IT Operations Compliance

Software Version: 1.20

Linux, Solaris, AIX, HP-UX, and Windows

Integration Guide

Document Release Date: October 2016
Software Release Date: October 2016

Hewlett Packard Enterprise

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

© 2015 - 2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HP Passport login page.

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

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com/.

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/km/KM01702731.

Contents

HPE ITOC - HPE SA integration

This section discusses the use of HPE ITOC with HPE Server Automation (SA). HPE ITOC leverages HPE SA agents and gateway for remote execution.

HPE ITOC has a remote execution path that uses Salt agents to perform compliance scans on target servers. HPE SA also has its own agents that perform remote execution on target managed devices. For customers who already have HPE SA agents installed and want to use HPE ITOC to apply compliance on the same managed devices, HPE ITOCcan delegate remote execution through HPE SA agents instead of installing additional HPE ITOC agents on the servers.

The HPE ITOC Resource Manager Adapter delegates the responsibilities to HPE SA to execute scripts remotely. The Resource Manager Adapter sends HPE ITOC scanning and remediation jobs to HPE SA and triggers Run Server Script jobs in HPE SA.

HPE ITOC - HPE SA integration overview

HPE ITOC has a remote execution path that uses Salt agents to perform compliance scans on target servers. HPE SA also has its own agents that perform remote execution on target managed devices. For customers who already have HPE SA agents installed and want to use HPE ITOC to apply compliance on the same managed devices, HPE ITOCcan delegate remote execution through HPE SA agents instead of installing additional HPE ITOC agents on the servers.

The HPE ITOC Resource Manager Adapter delegates the responsibilities to HPE SA to execute scripts remotely. The Resource Manager Adapter sends HPE ITOC scanning and remediation jobs to HPE SA and triggers Run Server Script jobs in HPE SA.

Prerequisites

The following items are required to integrate HPE ITOC with HPE SA:

- Install HPE ITOC version 1.20.

   For information about installing HPE ITOC, see the *HPE ITOC 1.20 Installation Guide*.

- HPE SA version 10.20 or later or Data Center Automation Appliance (DCAA) version 1.0 with SSH enabled

For the matrix that details HPE ITOC-HPE SA integration, see the *HPE ITOC 1.20 Support Matrix*.

Prerequisites for installing the Resource Adapter

You must install an agent before you install the Resource Adapter. If you install the adapter before you install the agent, agent installation will fail.

For an HPE SA core installed using non-root user, the HPE ITOC agent and adapter need to be installed manually.

For more information, see "Install Agents on Resources Manually" in the *HPE ITOC 1.20 Installation Guide*.

Install the HPE ITOC agent and the adapter to HPE SA using the adapter_easy_install.sh script

1. From the HPE ITOC server, locate the `adapter_easy_install.sh` script in the `<itoc_install_directory>/adapters/packages/sa` directory.

2. From the HPE ITOC server, run the `adapter_easy_install.sh` script.
   Provide the SSH credential and SSH port of the HPE SA Slice host.

3. The `adapter_easy_install.sh script` will complete the installation of the HPE ITOC agent to HPE SA Slice, register the HPE ITOC agent, install the adapter to the HPE SA slice, and generate the key for the adapter in phases.

Install the ITOC agent and adapter manually to SA

1. Specify the HPE SA host name, SSH port, and SSH credential.

2. Copy the appropriate agent platform package from the `<itoc_install_directory>/salt/srv/salt` directory on the HPE server to the HPE SA Slice host where you plan to install the adapter.

3. Copy the `ITOC_SA_Lite-version_num` package from `<itoc_install_directory>/adapters/packages/sa` on the HPE ITOC server to the HPE SA Slice host.

4. On the HPE SA Slice, create a directory; for example, `/opt/hp/itoc`. Ensure that the user who

installs the agent in the next step has **Read**, **Write**, and **Execute** permissions on this directory.

5. From the HPE SA Slice, install the agent:

   `./<platform>_minion-version -- -d <full_path> -f <itoc_server_FQDN>`

6. From the HPE ITOC server, register the agent installed in step 5:

   `<itoc_install_directory>/scripts/minion_reg.sh -a <agent_key>`

7. From the HPE SA Slice, `cd` to the directory to which the packages were copied. Run the following command to install the adapter:

   `./ITOC_SA_Lite<-ver_num> -- -d <agent_install_directory>/adapter -f <SA_Slice_Host_FQDN>`

   > **Note:** A path relative to the agent install path must to be specified in the `-d` option.

   > **Note:** The end directory of adapter installation path must be `adapter`, as shown in step 7.

8. From the HPE SA Slice, copy the public key in the `<SA_Slice Hostname>-public.pem` file from the
   `<agent_install_directory>/adapter` directory (as the file or copy the file content from `stdout`)
   to the HPE ITOCserver directory: `<itoc_install_directory>/adapters/keys`

Create a Resource Manager - HPE SA

1. Log in to HPE ITOCas a user with the Business Administrators role.

2. Navigate to the **Resource Managers** list under the Administration tab.

3. From **Actions**, select **New Resource Manager**.

4. The **New Resource Manager** dialog appears

New Resource

Name:

Resource Manager

Resource Type:

HPE Server Automation

Description:

Resource Manager for SA

Version:

10.5

Host:

123.755.693.945

Port:

443

User:

itocuser

Password:

••••

Adapter Host:

557.294.934.853

OK   Cancel

5. Complete the following fields:

- ○ **Name:** (required) - User-specified name.

- ○ **Resource Type:** (required) - Select **HPE Server Automation**.

Enter resource attribute information:

- **Description:** (optional) - A detailed description of the HPE SA core with which you are integrating.

- **Version:** (optional) - The HPE SA version being used.

- **Host:** (required) - The host name for the HPE SA core. This host name matches the host name registered with the Salt server.

  Note: Make sure the value you enter in the **Host** field matches exactly to the value you specified for the Slice host name during adapter installation.

- **Port:** (required) - The port of the HPE SA Slice's configuration gateway tunnel port. The default is 443.

- **User:** (required) - An HPE SA integration user with the following permissions:
  - Run Ad hoc scripts.

  - Run Ad hoc & Saved Server Scripts as Super User.

  - Managed Servers and Groups

  - Read and write permission on the resource (facility, customer, or device group) to which the managed server belongs.

- **Password:** (required) - HPE SA user password.

- **Adapter Host:** (optional) - The host on which the adapter is installed. If this information is not provided, the default is the HPE SA core host name provided above.

Create a resource managed by HPE SA in HPE ITOC

Create a resource for the server that is managed by HPE SA in HPE ITOC.

1. Navigate to the **Resources** list.

2. Click **Actions**, and select **New Resource**.

3. The **New Resource** dialog appears:

  ○ **Name** - Name of the server.

  ○ **Resource Type** - The OS platform of the SA managed server.

  ○ **Server Identifier** - The object ID of the managed server in SA.

  ○ **Choose the Access Through Resource:** - Uncheck the **Use self** box.

  ○ **Type is:** Choose **Server Automation**.

  ○ **Name contains:** Enter the full or partial name of the Resource Manager to use, and press **Search**. Select the resource manager you want to use.

4. Press **OK**.

New Resource

Name:

test

Resource Type:

MS Windows Server 2008

Server Identifier:

30001

Choose the Access Through Resource: Use self

  Status is:

  Active Resources

  Type is:

  HPE Server Automation

  Name contains:

  1 Resource(s) found: Search

OK   Cancel

For information about creating a resource, see the *HPE ITOC 1.20 User Guide*.

Uninstall the resource adapter

1. Locate the following scripts on the HPE SA slice on which the adapter was installed. These scripts should be in the home directory of the UNIX user specified for adapter installation. If `root` was specified, these scripts will be in `/root`.

   `.uninstall_itoc_adapter.sh`

   `.uninstall_itoc_minion.sh`

2. Run the `.uninstall_itoc_adapter.sh` script.

3. Manually remove the following files. If the adapter installation was done using the `adapter_easy_install.sh` script, these files will be in the `/tmp` directory:

   - `ITOC_SA_Lite-<version>`

   - `minion_easy_install`

   - `<platform>_minion-<version>`

4. Uninstall the HPE ITOCagent from the HPE SA Slice. You must uninstall the adapter before you uninstall the HPE ITOC agent.

   For more information about uninstalling an agent, see the "Uninstall an agent" section in the *HPE ITOC 1.20 Installation Guide*.

5. From the HPE ITOC server, remove the adapter key in the `<itoc_install_directory>/adapters/keys` directory.

6. From the HPE ITOC server, unregister the HPE ITOC agent of the HPE SA Slice host by running the following:

   `<itoc_install_directory>/scripts/minion_reg.sh -d <agent_key>`

7. From the HPE ITOC UI, log in as `itocadmin`. Navigate to the **Resource Manager** list, and delete the HPE SA resource manager instance.

HPE ITOC - HPE CSA integration

Cloud Service Automation (CSA) orchestrates the deployment of infrastructure to provide private cloud, public cloud, or hybrid cloud for end users. ITOC is a compliance management solution designed for ensuring business service compliance against corporate and regulatory policies, making your environment compliant and secure. This section discusses HPE ITOCintegration on the HPE CSA platform.

You can configure HPE CSA and HPE ITOC so that when a new service instance is instantiated in HPE CSA, HPE ITOC receives a notification (as an invocation of a rest API call) from HPE CSA. This notification is delivered to the HPE ITOC integration user (for example, "csauser" in a "public" organization) along with the HPE CSA's Service Instance ID. The customer should have the correct LDAP and the same definition of organizations in HPE ITOC as that of HPE CSA in order for the integration to work.

When HPE CSA notifies HPE ITOC of a new service instance:

1. HPE CSA looks up the `csa.properties` file to discover the HPE ITOC endpoint and initiates a REST API call to HPE ITOC using the HPE ITOC user name/password and tenant name configured in the `csa.properties` file. (For information about configuring the csa.properties file, see "Configure HPE CSA" on page 16.)

2. This API call to HPE ITOC initiates the search for a Resource Manager of type Cloud Service Automation. HPE ITOC searches this list of resource managers for the one with the `serviceURL` that matches the HPE CSA instance that initiated this API call. This Resource Manager provides the user, password, and tenant credentials to HPE ITOC to communicate with the HPE CSA service.

3. Once two-way communication between HPE CSA and HPE ITOC is established, HPE ITOCexamines the service instance reported by HPE CSA and determines if the instance should be created, modified, or canceled (obsoleted) in HPE ITOC.

   a. If no existing service definition is found, a new HPE ITOC instance is created.

   b. If a previous definition is found, the HPE ITOC instance is modified and updated.

   c. If HPE CSA reports a canceled instance, HPE ITOC searches for that instance and obsoletes the service and attached resources.

4. When steps 1, 2, and 3 are completed, the HPE ITOC user receives an email notification detailing whether each instance was created, modified, or canceled.

The HPE ITOC-HPE CSA usage flow is as follows:

1. Configure HPE CSA to send service instantiation, modification, and cancellation data (notifications) to an HPE ITOCinstance.

2. Configure HPE ITOC to communicate with HPE CSA on receipt of the HPE CSA data.

3. Configure HPE CSA service designs to provide necessary information for integration with HPE ITOC.

4. HPE CSA notifies HPE ITOC by calling the HPE ITOC REST API when a HPE CSA service instance is instantiated, modified, or canceled.

HPE ITOC - HPE CSA integration overview

You can configure HPE CSA and HPE ITOC so that when a new service instance is instantiated in HPE CSA, HPE ITOC receives a notification (as an invocation of a rest API call) from HPE CSA. This notification is delivered to the HPE ITOC integration user (for example, "csauser" in a "public" organization) along with the HPE CSA's Service Instance ID. The customer should have the correct LDAP and the same definition of organizations in HPE ITOC as that of HPE CSA in order for the integration to work.

When HPE CSA notifies HPE ITOC of a new service instance:

1. HPE CSA looks up the `csa.properties` file to discover the HPE ITOC endpoint and initiates a REST API call to HPE ITOC using the HPE ITOC user name/password and tenant name configured in the `csa.properties` file. (For information about configuring the csa.properties file, see "Configure HPE CSA" on page 16.)

2. This API call to HPE ITOC initiates the search for a Resource Manager of type Cloud Service Automation. HPE ITOC searches this list of resource managers for the one with the `serviceURL` that matches the HPE CSA instance that initiated this API call. This Resource Manager provides the user, password, and tenant credentials to HPE ITOC to communicate with the HPE CSA service.

3. Once two-way communication between HPE CSA and HPE ITOC is established, HPE ITOCexamines the service instance reported by HPE CSA and determines if the instance should be created, modified, or canceled (obsoleted) in HPE ITOC.

   a. If no existing service definition is found, a new HPE ITOC instance is created.

   b. If a previous definition is found, the HPE ITOC instance is modified and updated.

   c. If HPE CSA reports a canceled instance, HPE ITOC searches for that instance and obsoletes the service and attached resources.

4. When steps 1, 2, and 3 are completed, the HPE ITOC user receives an email notification detailing whether each instance was created, modified, or canceled.

The HPE ITOC-HPE CSA usage flow is as follows:

1. Configure HPE CSA to send service instantiation, modification, and cancellation data (notifications) to an HPE ITOCinstance.

2. Configure HPE ITOC to communicate with HPE CSA on receipt of the HPE CSA data.

3. Configure HPE CSA service designs to provide necessary information for integration with HPE ITOC.

4. HPE CSA notifies HPE ITOC by calling the HPE ITOC REST API when a HPE CSA service instance is instantiated, modified, or canceled.

Prerequisites

To integrate HPE ITOC and HPE CSA, you must have:

- HPE CSA version 4.7 with one or more of the following two providers:

  Note: HPE CSA - HPE ITOC integration supports only the following in Release 1.20.

  - vCenter
  - OpenStack

Create a Resource Manager - HPE CSA

1. Log in to HPE ITOC as a user with the Business Administrators role.

2. Navigate to the **Resource Managers** list.

3. From **Actions**, select **New Resource Manager**.

4. The **New Resource Manager** dialog appears:

New Resource

Name:

New Resource Manager

Resource Type:

Cloud Service Automation

Description:

New Resource Manager for CSA

Version:

4.7

User:

itocuser

Password:

••••

CSA Service URL:

https://<csaServer>:<csaPort>/csa/

Organization:

CSA-Provider

OK   Cancel

Complete the following fields:

○ **Name:** (required) - User-specified name.

○ **Resource Type:** (required) - Select **Cloud Service Automation**.

Enter resource attribute information:

- **Description:** (optional) - A detailed description of the HPE CSA core with which you are integrating.

- **Version:** (optional) - The HPE CSA version being used.

- **User** (required) - The HPE CSA user.

- **Password:** (required) - HPE CSA user password.

- **CSA Service URL:** (required) - `https://<csaServer>:<csaPort>/csa/`
  Note: The Service URL must end with `/csa/`, as shown above.

- **Organization:** (required) - The organization of the user.
  Note: If you created the HPE CSA instance using the defaults, this value would be **CSA-Provider**.

Configure HPE CSA

An Admin user configures the HPE ITOC integration endpoint that the HPE CSA instance will contact.

1. Log in to the HPE CSA server and navigate to the `<csaInstallDir>/csa/jboss-as/standalone/deployments/csa.war/WEBINF/classes/csa.properties` file.

2. Modify the `csa.properties` file (see the following examples):

   ○ `csa.ITOC.Integration.enabled=true`

   ○ `csa.ITOC.Notification.BaseUri=https://itocserver:itoc port/` - The `itocport` value typically is 7771 for default ITOC installs.

   ○ `csa.ITOC.Notification.username=integuser` - The `integuser` must belong to a special HPE ITOCrole called "INTEGRATION_USER". The same user must be known in HPE ITOC.

   ○ `csa.ITOC.Notification.password=iupassword` - The `integuser`'s password. The password value must be encrypted as shown in the "Encrypt a Password" section in the *CSA Configuration Guide*.

   ○ `csa.ITOC.Notification.tenant=public` - The organization of the `integuser`.

   > **NOTE:** This organization must match the corresponding organization in HPE ITOC; otherwise, the import fails.

3. Restart the HPE CSA instance, and run:

```
/etc/init.d/csa restart
```

Configure HPE CSA component for an HPE ITOC resource

All applicable resource attributes for a resource type need to be defined on the HPE CSA component used in a topology design to be instantiated and imported to HPE ITOC in order for the imported HPE ITOC resource to be successfully scanned or remediated.

To make a HPE CSA component property available to HPE ITOC, you can perform one of the following tasks:

- Ensure that the existing HPE CSA component property name is the same as the HPE ITOC resource attribute name.
  For example, if the HPE CSA component has a property "Hostname," then its value is taken as the HPE ITOC resource attribute "Hostname" value.

- Map the existing HPE CSA component property name to the HPE ITOC resource attribute name in the `resource.properties` file on the HPE ITOC server (in the same folder as the `application.properties` file).
  For example, if the existing HPE CSA resource property "serverName" has the value of the HPE ITOC resource attribute "Hostname," configure the mapping in `resource.properties` file as follows:

  `serverName=Hostname`

  where the HPE CSA property name is the key in the mapping, and the HPE ITOC resource attribute name is the value.

- Add the HPE ITOC resource attribute to the HPE CSA component property and prefix the attribute with "ITOC."
  You may define ITOCHostname in the HPE CSA component property that has the value of HPE ITOC resource attribute "Hostname."

Configure HPE CSA designs for import into HPE ITOC

Configure HPE CSA designs so that HPE CSA instances can be imported into HPE ITOC:

1. Ensure that every resource component that is part of the HPE CSA service has following attribute set: `ITOCResourceType`

2. The value specified for `ITOCResourceType` must be of type string and have a valid 1:1 mapping to HPE ITOC-supported resource types. If not specified, the resource type (when imported into HPE ITOC) will be "Unknown."

3. All applicable properties for a given resource type in HPE ITOC must be available on the HPE CSA resource also and have the exact same name and value.

4. All HPE CSA services to be imported into HPE ITOC require a tag attached to the HPE CSA design in the following format:

   `ITOCPolicy_POL_ 0001:MW_12`

   in which `POL_0001` is the applicable business ID of the policy and `12` is the ID of the maintenance window that will run the jobs for this service. The user can include multiple Maintenance Windows in a tag as follows:

   `ITOCPolicy_POL_ 0001:MW_12:MW_14:MW_xx`

   If the policy or maintenance window names are missing, no statement is created.

5. HPE ITOC supports the `ITOCDomainName` user-defined property in HPE CSA services to specify the optional domain name for a resource.

HPE ITOC import

When HPE ITOC successfully imports the HPE CSA service and associated resource instances, it also automatically:

- Creates the corresponding Business Service and all associated resources.

- Promotes the business service to production.

- Ensures that the policy specified by the `ITOCPolicy_` tag is available in the same org as the user that initiated the service in HPE CSA and in production.

- Ensures the maintenance window is available and in the same org as the user that initiated the service in HPE CSA.

- Creates and promotes to production a new statement that ties the newly imported service with the specified policy and maintenance window.

Import the server certificate from HPE CSA to HPE ITOC

This section describes how to import a server certificate from HPE CSA to HPE ITOC for HTTPS communication.

Prerequisites

This process must be performed by a user with privileges to log in to both the HPE CSA and HPE ITOC servers and access the install location.

On the HPE CSA server

1. On the HPE CSA server, verify the certificate is available in the keystore. Use the alias `csa` to narrow your choices:

   ```
   # <csa_server>/csa/openjre/bin/keytool -list -alias csa -v -keystore
   <csa_server>/csa/openjre/lib/security/cacerts
   Enter keystore password:
   Alias name: csa
   Creation date: May 27, 2015
   Entry type: trustedCertEntry

   Owner: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
   Issuer: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
   Serial number: 7a8bdee
   Valid from: Wed May 27 02:38:51 PDT 2015 until: Thu Sep 24 02:38:51 PDT 2015
   Certificate fingerprints:
   MD5: 1E:35:CB:E0:B6:93:B9:21:8C:17:BF:57:C5:61:B0:70
   SHA1: 85:54:F8:E8:A3:D5:6C:7B:5A:5D:AF:AA:14:A9:03:E3:67:F9:2A:39
   SHA256: 9B:AB:E7:77:4F:84:C7:54:D2:7D:F0:4B:2F:EE:37:30:56:1F:66:72:
   A9:30:43:62:22:AF:7A:49:80:D1:94:5A
   Signature algorithm name: SHA256withRSA
   Version: 3
   ```

```
Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 40 41 77 C8 53 D2 F7 CB 6B 42 66 9F D7 3F 25 AA  @Aw.S...kBf..?%.
0010: 9E 43 09 30                                      .C.0
]
]
#
```

2. Export the certificate to a file, using the default Java keystore password `changeit` when prompted.

    ```
     # <csa_server>/csa/openjre/bin/keytool -export -alias csa -file /tmp/csa.crt -
    keystore
    <csa_server>/csa/openjre/lib/security/cacerts
    Enter keystore password:
    Certificate stored in file </tmp/csa.crt>
    #
    ```

3. On the HPE ITOC server, copy the exported certificate file `csa.crt` from the HPE CSA server to the HPE ITOC server and import the certificate.

    o   Use the default Java keystore password `changeit` when prompted.

    o   Enter yes when prompted: `Trust this certificate?`

    ```
    # <itoc_server>/openjre/bin/keytool -importcert -alias csa -file /tmp/csa.crt -
    keystore <itoc_server>/wildfly-8.1.0.Final/standalone/configuration/selfcacerts
    Enter keystore password:
    Owner: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
    Issuer: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
    Serial number: 7a8bdee
    Valid from: Wed May 27 02:38:51 PDT 2015 until: Thu Sep 24 02:38:51 PDT 2015
    Certificate fingerprints:
    MD5:
    1E:35:CB:E0:B6:93:B9:21:8C:17:BF:57:C5:61:B0:70
    SHA1: 85:54:F8:E8:A3:D5:6C:7B:5A:5D:AF:AA:14:A9:03:E3:67:F9:2A:39
    SHA256: 9B:AB:E7:77:4F:84:C7:54:D2:7D:F0:4B:2F:EE:37:30:56:1F:
    66:72:A9:30:43:62:22:AF:7A:49:80:D1:94:5A
    Signature algorithm name: SHA256withRSA
    Version: 3
    ```

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 40 41 77 C8 53 D2 F7 CB 6B 42 66 9F D7 3F 25
AA @Aw.S...kBf..?%.
0010: 9E 43 09 30   .C.0
]
]
Trust this certificate? [no]: yes
Certificate was added to keystore
#

List the certificate to confirm

<itoc_server>/openjre/bin/keytool -list -alias csa -v -keystore
/opt/hp/itoc/wildfly-8.1.0.Final/standalone/configuration/selfcacerts
Enter keystore password:
Alias name: csa
Creation date: Jul 28, 2015
Entry type: trustedCertEntry
Owner: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Issuer: CN=csa.server.domain.net, OU=TEST, O=TEST, L=Palo Alto, ST=CA, C=US
Serial number: 7a8bdee
Valid from: Wed May 27 02:38:51 PDT 2015 until: Thu Sep 24 02:38:51 PDT 2015
Certificate fingerprints:
MD5: 1E:35:CB:E0:B6:93:B9:21:8C:17:BF:57:C5:61:B0:70
SHA1: 85:54:F8:E8:A3:D5:6C:7B:5A:5D:AF:AA:14:A9:03:E3:67:F9:2A:39
SHA256: 9B:AB:E7:77:4F:84:C7:54:D2:7D:F0:4B:2F:EE:37:30:56:
1F:66:72:A9:30:43:62:22:AF:7A:49:80:D1:94:5A
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [

```
0000: 40 41 77 C8 53 D2 F7 CB 6B 42 66 9F D7 3F 25 AA  @Aw.S...kBf..?%.
0010: 9E 43 09 30  .C.0
]
]
#
```

4. Restart the HPE ITOC server.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Integration Guide (IT Operations Compliance 1.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_itoc_docs@hpe.com.

We appreciate your feedback!