



# ITOC Integration

Software version: 4.80

Document release date: January 2017

Software release date: January 2017

# Contents

<b>Introduction</b>	<b>3</b>
Basic concepts	3
CSA role	3
ITOC role	3
<b>Environment configuration</b>	<b>4</b>
Configure ITOC in CSA	4
Consumer Organizations Setup	4
<b>CSA – ITOC Mapping Configuration</b>	<b>5</b>
List of default ITOC Resource Types names and attributes is listed in Appendix C: Default ITOC Resource Type Hierarchy and Attributes .Mapping of Platforms credentials for ITOC agent installation	6
Mapping File	6
<b>CSA - ITOC Integration UI</b>	<b>7</b>
Policy and Maintenance Windows Configuration on Offering	7
Compliance Score Results	7
<b>End-to-end scenario</b>	<b>9</b>
Prerequisites	9
ITOC Policies and Maintenance Windows	9
CSA Service design	10
CSA Service Offering	12
CSA MPP Requesting	12
CSA Operation Console	13
ITOC View of CSA Subscription	13
<b>Known problems and limitations</b>	<b>14</b>
ITOC Integration Failure does not fail subscription	14
List of ITOC Resource Types and Attributes of Resource Type	14
Remediation maintenance windows are not supported	14
<b>Appendix A: Configuration of CSA 4.80 to Integrated with ITOC 1.20</b>	<b>15</b>
<b>Appendix B: Establishing trust between CSA and ITOC</b>	<b>17</b>
<b>Appendix C: Default ITOC Resource Type Hierarchy and Attributes</b>	<b>18</b>
<b>Appendix D: Consumer Organization Setup for illustration Purposes</b>	<b>21</b>
<b>Send documentation feedback</b>	<b>22</b>
<b>Legal notices</b>	<b>22</b>

# Introduction

HPE IT Operations Compliance (ITOC) allows IT Operations users to track business service compliance against corporate and regulatory policies, making their environment compliant and therefore secure. ITOC can be integrated with HPE Cloud Service Automation (CSA), so that the CSA provisioned services are tracked by policies defined in ITOC.

This document describes the basic concepts of CSA-ITOC integration and the use cases provided by the integrated solution.

## Note:

- Two legacy integrations exist – one provided by ITOC, and the second provided by CSA as content. This document describes CSA-ITOC integration delivered in CSA 4.80 which compared to the legacy integrations – provides an end-to-end integrated experience.
- CSA upgraded servers: This CSA-ITOC integration is not upgradable from previous versions of CSA-ITOC integration as they are implemented as part of ITOC and not CSA. You can use previous version of CSA-ITOC integration, but it is not recommended to use both integration versions together.
- This step is necessary to redo only when ITOC setup is changed.

## Basic concepts

The following concepts are enumerated and then described in detail later in this document:

- CSA takes care of
  - Service definition, offering, fulfillment and subscription management.
  - Association of ITOC policies and maintenance windows with CSA offering.
  - Mapping of fulfilled service instance to ITOC resources and business service, and linking with ITOC policies and maintenance windows associated with CSA offering.
  - Displaying of ITOC compliance scores of subscriptions and organizations.
- ITOC takes care of
  - Management of compliance policies and maintenance windows.
  - Computing compliance score of mapped resources based on linked policies and maintenance windows.
- CSA communicates with ITOC using ITOC REST APIs
- Consumer organizations are defined in both CSA and ITOC IdM.

## CSA role

In the integrated solution, CSA plays the role of fulfillment engine. Service designs must be published in CSA and resource providers that are capable of providing the required resources must be configured.

Resource providers must be organized in CSA resource environments and assigned to catalogs of the organization in order to identify organization resource providers during fulfillment. In this way the CSA-ITOC integration supports multitenancy for resource providers. If multi tenancy support is not required by customers, then it is not required to configure resource environment

CSA offering can be associated not only with the design, but also with ITOC policies and maintenance windows. When such CSA offering is requested from MPP or using REST API, then at the end of fulfillment CSA maps CSA service instance to ITOC resources and creates ITOC business service representing CSA subscription, and creates ITOC statement of applicability for the business service and ITOC policies and maintenance windows as configured on the offering. CSA also synchronizes service instance to ITOC for modification and cancellation of subscription.

CSA displays ITOC compliance score for subscription in the operation console, and for organizations on the dashboard.

## ITOC role

ITOC is responsible for management of policies and maintenance windows, business service, resource management and statement of applicability and finally for computing the compliance score of mapped CSA service instances and subscriptions.

# Environment configuration

The integration is between CSA 4.80 and ITOC 1.20. Applying ITOC hotfix- QCCR1D233365 Installation and configuration guides for CSA and ITOC are available from HPE Software Support Online at [softwaresupport.hpe.com](https://softwaresupport.hpe.com).

Configuration is composed of following steps:

- Configure ITOC in CSA
- Create and configure consumer organizations in both ITOC and CSA

## Configure ITOC in CSA

In CSA the integration has to be enabled first, and ITOC has to be configured in CSA (CSA accesses ITOC REST APIs for retrieving various data of public tenant).

Create *integration* account in ITOC *public* tenant:

- Used to get list of ITOC policies and maintenance windows, resource type hierarchy and resource type attributes

ITOC permission needed for the account: *Viewers*

Configure ITOC as described in [Appendix A: Configuration of CSA 4.80 to Integrated with ITOC 1.20](#) , and establish trust between CSA and ITOC as described in [Appendix B: Establishing trust between CSA and ITOC](#) .

## Consumer Organizations Setup

CSA-ITOC integration is tenant aware, so service instance created in CSA organization X are mapped to ITOC organization X. In this way data is isolated between tenants and ITOC can compute compliance score per organization.

Integration maps consumer organizations using its names – consumer organizations must exist in both CSA and ITOC, and they have to have same *name* (case sensitive).

**Note:** it is recommended to create organization in CSA first, as it derives the *name* from the organization display name, and then create organization of the same *name* (case sensitive) in ITOC IdM management UI.

Two accounts in ITOC consumer organization are required:

- Administrator account
  - Used to manually configure ITOC organization– auto-approval of statement of applicability (see below)
  - ITOC permissions needed for the account: *Business Administrators*
- Integration account
  - Used by CSA to create/delete ITOC resource, business service and statements of applicability for mapping of CSA subscriptions.
  - ITOC permissions needed for the account: *Business Service Owners*

ITOC consumer organization must be manually configured using ITOC UI prior to it is used in the integration:

- Sign in to consumer organization using administrator account of the consumer organization
- Set Workflow as follows
  - Business Services: Auto-Approval
  - Statements of Applicability: Auto-Approval

Once ITOC consumer organization is created, then it has to be configured in CSA as described in [Appendix A: Configuration of CSA 4.80 to Integrated with ITOC 1.20](#)

**Notes:**

- Only consumer organizations with configured ITOC integration account in CSA are integrated.
- Adding new consumer organization requires CSA manual reconfiguration and restart.
- In the integration CSA SMC/MPP UIs and ITOC UI are not integrated, it is not necessary to configure SSO between CSA and ITOC.

## CSA – ITOC Mapping Configuration

Important part of CSA-ITOC integration is mapping of CSA subscription/service instance to ITOC business service/resource.

Following table describes mapping in detail

CSA Entity	ITOC Entity
<b>CSA Subscription</b>	<b>ITOC Business service</b>
<i>Policies and Maintenance Windows</i> set on offering	Statements of applicability is created for each <i>Policy</i> with all <i>maintenance windows</i>
Service Instance	Hierarchy of mapped ITOC resources
<b>Service Instance component</b>	<b>ITOC Resource</b>
<i>ITOCResourceType</i> property	<p>Defines type of created ITOC resource.</p> <p>If it is subtype of <i>Software</i>, then <i>Access Through</i> is set to parent resource if parent type is subtype of <i>Platform</i></p> <p>If it is subtype of <i>Platform</i>, then the integration will instruct ITOC to install agent on it. See below for more details.</p> <p>If <i>ITOCResourceType</i> does not exist, then <i>unknown</i> type is used.</p> <p>If type is invalid, then mapping fails</p>
Properties	<p>Attributes</p> <p>See property-attribute mapping description below</p>

Properties of CSA service instance components are mapped to ITOC resource attributes as follows:

CSA retrieves attribute list of the ITOC resource type, and set attribute value to CSA property value for each attribute is retrieved using following process:

- If *mapping file* defines attribute to property mapping, then property value is used
- or if CSA component contains property of attribute name, then the property value is used
- or If CSA component contains property named 'ITOC'+attribute name, then the property value is used
- Otherwise empty string is returned

## List of default ITOC Resource Types names and attributes is listed in [Appendix C: Default ITOC Resource Type Hierarchy and Attributes](#) .Mapping of Platforms credentials for ITOC agent installation

*Platform* represents machines with installed supported OS such as Windows, or Linux. ITOC executes policy rule controls on the machines using ITOC agent (based on *SaltStack* framework over *ssh* access protocol).

When CSA component is mapped to subtype of *ITOC Platform*, the integration will instruct ITOC to install *ITOC agent* on it. SSH credentials of the machine (i.e., *username* and *password*) are retrieved from built-in *sshUser* and *sshPass* ITOC attributes (they are not part of ITOC resource type attribute list) and passed to ITOC. FQN of machine can be also constructed using built-in *hostDomain* attribute – if defined, then it is appended to *Hostname* attribute of *ITOC Platform* type.

### Note:

- The Windows VM Templates which are deployed as part of CSA Subscriptions should have open SSH for CSA-ITOC Integration APIs to push ITOC agent onto it.
- Please refer ITOC documentation on ITOC agent installation requirements.

## Mapping File

Mapping file defines mapping of CSA property to ITOC attributes in following precedence.

- `<CSA-component-type>.<CSA-property-name> = <ITOC-attribute-name>`
- `<CSA-property-name> = <ITOC-attribute-name>`

Mapping also defines mapping of ITOC agent credentials and FQN hostname of machines:

- *sshUser* and *sshPass* represents credentials as ITOC attributes
- if ITOC *hostDomain* attribute is mapped (i.e., CSA component has corresponding property), then its value will be appended to *Hostname* attribute

Mapping can be specified on CSA component level using file `[csa]/jboss-as/standalone/deployments/csa.war/WEB-INF/lib/apis-04.80.000-SNAPSHOT.jar! itocResourceMapping.properties` . If file is modified, then CSA has to be restarted.Below there is default content of the mapping file. It contains default mapping for CSA *Server* to ITOC *Platform* subtypes.

```
# This file contains CSA - ITOC mappings where:
# - key is CSA component property name,
# - optionally it can contain COMPONENT_TYPE prefix (e.g. "SERVER.hostName=Hostname") to apply only to some
types
# - value is ITOC resource attribute name

# VMware vCenter
SERVER.hostName=Hostname

# OpenStack
serverName=Hostname

# Agent installation properties (applies only to "Platform" ITOC resource types)
username=sshUser
password=sshPass
# agentInstallPath=agentInstallPath - optional, default is '/opt/hp/itoc'
# sshPort=sshPort - optional, default is 22

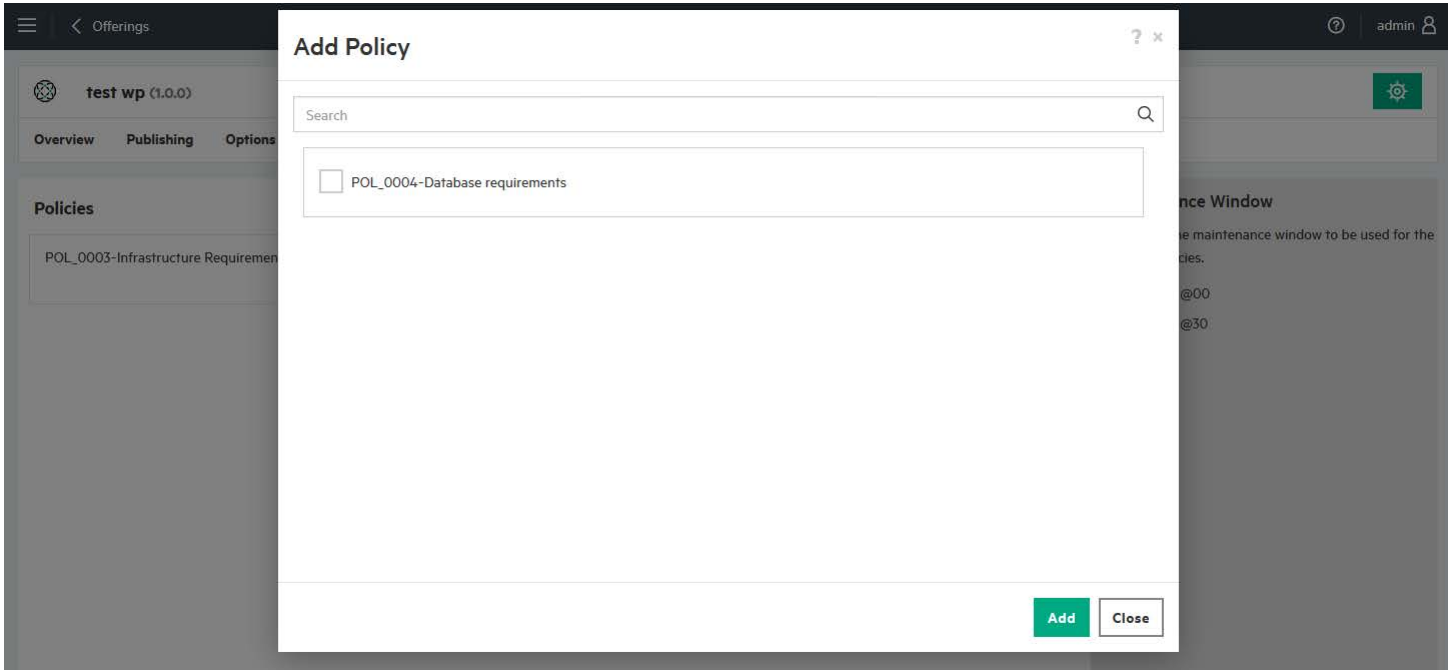
# 'hostDomain' is optional
# - if value is found (e.g. "host.com")
# - and when 'hostName' is not FQDN (e.g. "vm123")
# - then 'hostDomain' will be appended to 'hostName' (e.g. "vm123.host.com")
domainName=hostDomain
```

# CSA - ITOC Integration UI

When integration is configured, CSA SMC UI integration use cases are enabled. It allows to setup policies and maintenance windows on offerings, and to display compliance score of provisioned services

## Policy and Maintenance Windows Configuration on Offering

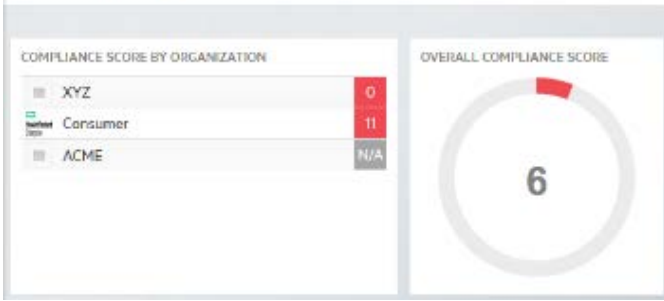
Service offering manager can select policies and maintenance windows on CSA offering. When offering is being provisioned (e.g., requested from MPP), configured policies and maintenance windows are converted to ITOC statement-of-applicability on created ITOC business service. ITOC can start scan to compute compliance score at given maintenance windows.



## Compliance Score Results

When integration is enabled, ITOC compliance score is displayed for subscription and tenant. Following table lists displayed values.

UI	Compliance score: N/A	Compliance score: 0 - 100 %
Subscription detail	subscription is in tenant without configured integration, or mapping failed	compliance score returned by ITOC of mapped business service
Subscription in operation console subscription list	subscription is in tenant without configured integration, or mapping failed	compliance score returned by ITOC of mapped business service
Dashboard – compliance score by organization	Integration is not configured for tenant	Tenant compliance score returned by ITOC
Dashboard – overall compliance score	Compliance score is not available	Average of return tenant compliance scores



Consumer ⚙️

✖️ 0
🕒 0
🔊 0
🛑 0
🕒 0
👤 1

Subscriptions Submitted On ▾ 🔍

Subscription Details	User Name	Submitted On	Subscription Period	Subscription Status	Service Instance Status	Compliance
wp (1.0.0) <small>wp (Global Shared Catalog)</small>	consumer <small>consumer@csaconsumer.com</small>	12/13/2016 9:44:02 am	12/13/2016 - no end date	Active	Online	33

wp (1.0.0)

[Overview](#)
[Events](#)
[Topology](#)
[Providers](#)

---

**Display Name**  
wp (1.0.0)

---

**Service Offering (Service Catalog)**  
wp 1.0.0 (Global Shared Catalog)

---

**Design Name**  
wp (1.0.0)

---

**Subscriber**  
consumer (consumer@csaconsumer.com)

---

**Submitted On**  
12/13/2016 9:44:02 am

---

**Subscription Period**  
12/13/2016 - no end date

---

**Subscription Cost**  
\$0.00 and \$0.00 Weekly

---

**Compliance Score**  
N/A



# End-to-end scenario

This section describes a common end-to-end scenario starting with creating a service design through publishing offerings to service management. Users with different roles perform different actions during this process. The process and the actions are elaborated in detail in the following text.

The scenario will be presented on CSA design composed of *Server* and *MySQL* components. To make the illustration simple and fast, none of these components will be deployed – instead of that design will represent existing machine whose hostname, credentials and running MySQL DB parameters will be part of subscriber options. In ITOC there will be a policy checking a file and MySQL user. The policy will be set on the CSA offering, so when consumer will request the offering, ITOC will start to compute compliance score of the instance.

## Prerequisites

- Instance of CSA 4.80
- Instance of ITOC 1.20 with hotfix
- Populate ITOC 1.20 instance with control libraries
  - Control libraries are available on [ITOC HPLN page under following names. Consult ITOC documentation for import steps.](#)
    - `itocSoftwareControlLibrary-5118-20160128.zip`
    - `itocUnixControlLibrary-5024-20151203.zip`
- Setup and configure ITOC and CSA as described in Environment configuration.
  - At least one consumer organization must be created and configured. For illustration you can follow [Appendix D: Consumer Organization Setup for illustration Purposes](#)
- Running RHEL 6.x server  
server will be used during illustration–ITOC policy will be computing compliance score here
  - ITOC will install agent on this machine. Consult *HPE IT Operations Compliance User Guide* for agent requirements.
  - Prepare server's FQN hostname, and *root* user password

## ITOC Policies and Maintenance Windows

The ITOC administrator must provide policies (i.e., *what*) and maintenance windows (i.e., *when*) in order to start compute compliance score in public tenant.

Two policies will be created for this end-to-end scenario:

- Infrastructure requirements
  - It validates whether file `/tmp/required-itoc-file` exists and its content is *ITOC*
  - Tip: create this file manually on the RHEL 6.x server, so ITOC marks this policy as compliant – it will increase the score
- Database requirements
  - It validates whether MySQL DB is running under *mysql* user.

Tip: install MySQL 5.6 and start it on the RHEL 6.x server, so ITOC marks this policy as compliant – it will increase the score

As *public* tenant administrator create:

- ITOC policy *Infrastructure Requirements*  
this policy will check if server has file `/tmp/required-itoc-file` with content *ITOC*
  - Create requirement *filesystem* with following rule
    - Control: *CTRL\_000327: File Contents*
    - Scope: *RHEL 6*
    - Evaluation input parameters:
      - Directory or File: `/tmp/required-itoc-file`
      - expectedValue: *ITOC*
  - Submit and approve the policy
- ITOC policy *Database requirements*
  - Create requirement *mysql* with following rule
    - Control: *CTRL\_000029: Verify account used for MySQL Daemon*
    - Scope: *MySQL Community Server 5.6*
    - Evaluation input parameters
      - expectedValue: *0*
  - Submit and approve the policy
- Maintenance Window *hourly@00* and *hourly@30*  
these maintenance windows will start compliance score computation every 30 minutes
  - Window Type: *Scan*
  - Start time: choose time with 00 minutes, respectively 30 minutes
  - Duration: *1 hour*
  - Recurrence Type: *Hourly: Every 1 hour(s)*

**Edit Rule**

Type: Evaluation

Scope: RHEL 6

Control: CTRL\_000327 - File Contents

Rule Name: File Contents

Evaluation Input Parameters		
Name	Source	Value
Directory or File	Custom Value	/tmp/required-itoc-file
expectedValue	Custom Value	ITOC

OK Cancel

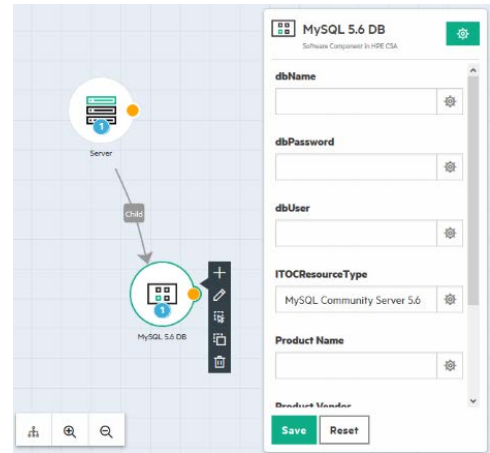
## CSA Service design

The service designer is responsible for designing service blueprints in CSA. Two approaches are supported: topology and sequence designs. Service design creation methodology is different for each of these two types, but both types of designs are supported in CSA-ITOC integration.

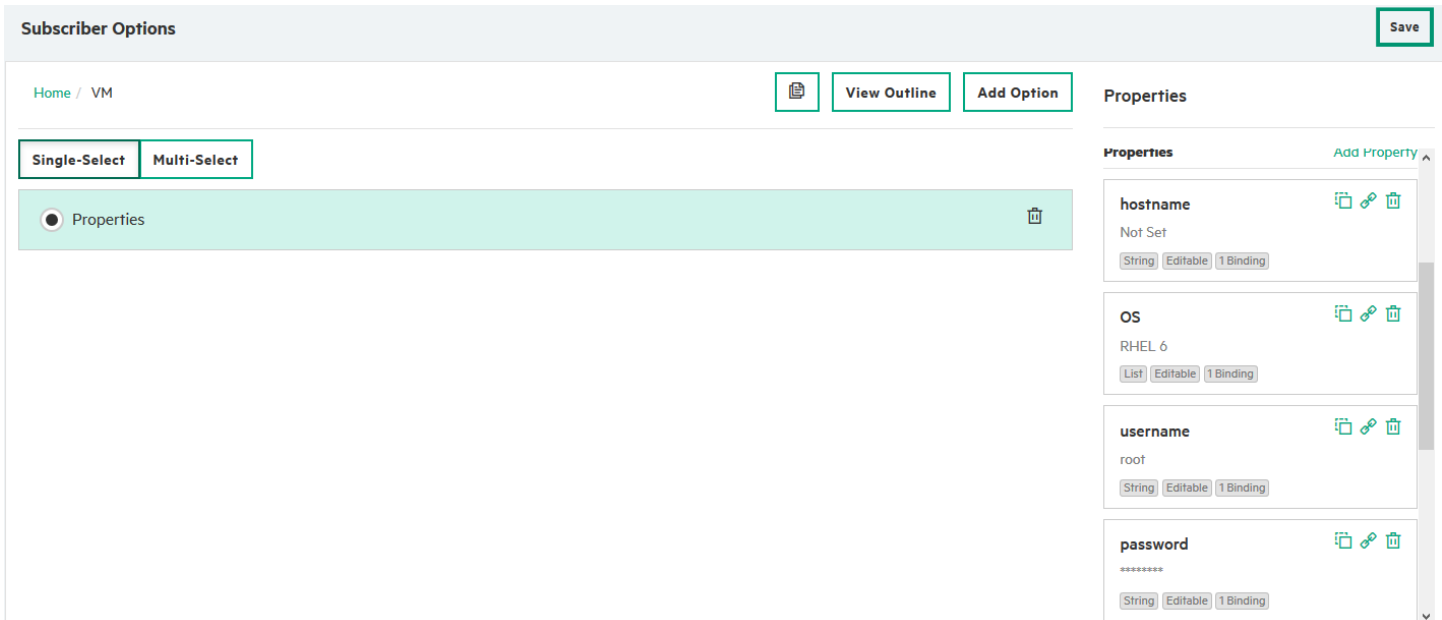
In end-to-end scenario following simple sequenced design will be used. It does not use neither resource offering nor resource providers, so real instance of Server and DB will not be created outside CSA.

Create CSA design with following content, and then publish it:

- Design components
  - Server component (*Blank Server*)
    - Properties
      - *ITOCResourceType*, String, consumer visible
      - *username*: String, consumer visible
      - *password*: String, confidential, consumer visible
  - MySQL 5.6 DB component (*Blank Software Component*)
    - Properties
      - *ITOCResourceType*, String, consumer visible, default value "*MySQL Community Server 5.6*"
      - *dbName*, *dbUser*, *dbPassword*: String, consumer visible



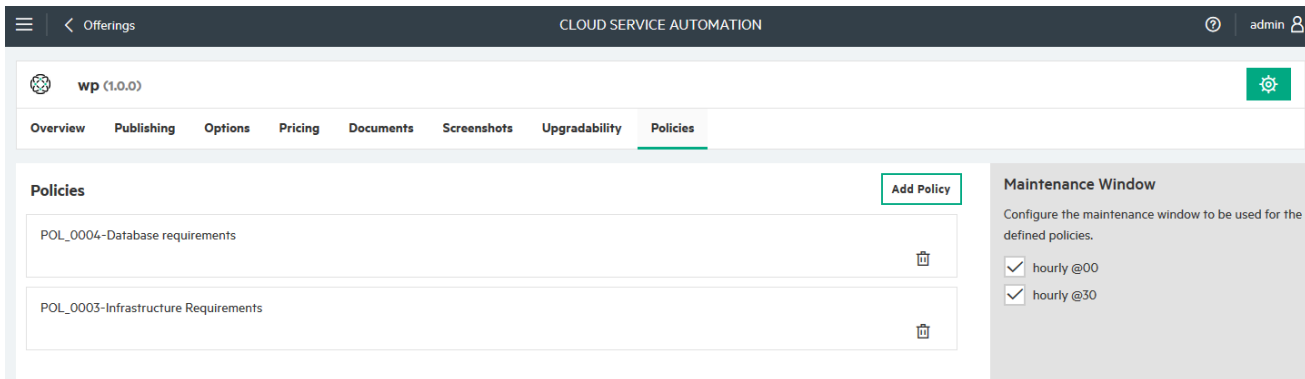
- Design subscriber options
  - Create an option set with one option. Add following properties  
note: you can provide default values
    - *hostname*: String, required, mapped to *Server.hostname*
    - OS: List, String, required, mapped to *Server.ITOCResourceType*
      - Static list item: "RHEL 6"
    - *username*: String, required, mapped to *Server.username*
    - *password*: String, required, confidential, mapped to *Server.password*
    - *dbName*: String, required, mapped to *MySQL 5.6 DB.dbName*
    - *dbUser*: String, required, mapped to *MySQL 5.6 DB.dbUser*
    - *dbPassword*: String, required, mapped to *MySQL 5.6 DB.dbPassword*



## CSA Service Offering

Now service offering can be created – it will bound together CSA design with ITOC policies. When the ITOC integration is enabled, new tab *Policy* is displayed on CSA offering. Using *Policy* tab, user can configure what ITOC policies will be used to compute compliance score, and when policies will be scanned by selecting ITOC maintenance windows.

Create CSA offering for design created above. Add both ITOC policies and maintenance windows. Then publish the offering.

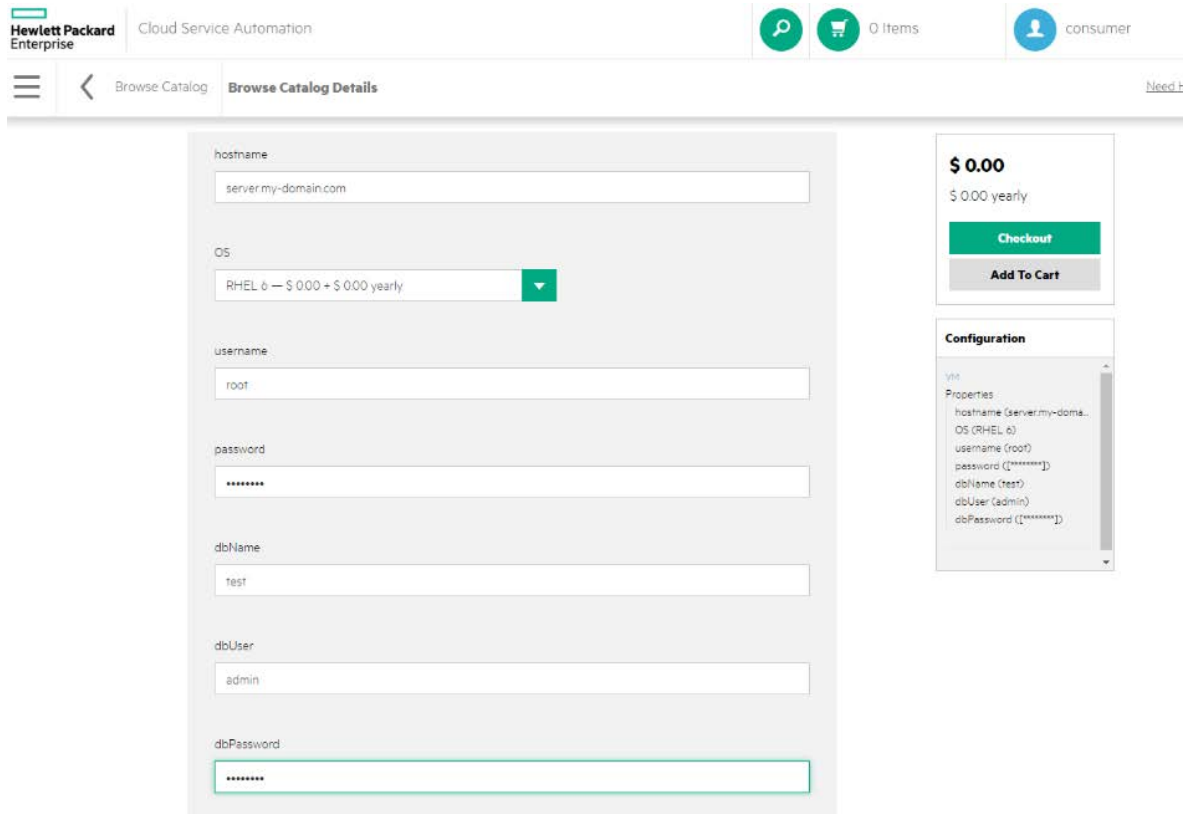


The screenshot shows the 'Policies' tab in the Cloud Service Automation interface. The top navigation bar includes 'Offerings' and 'CLOUD SERVICE AUTOMATION'. The main content area is titled 'wp (1.0.0)' and has tabs for 'Overview', 'Publishing', 'Options', 'Pricing', 'Documents', 'Screenshots', 'Upgradability', and 'Policies'. Under the 'Policies' tab, there is a list of policies: 'POL\_0004-Database requirements' and 'POL\_0003-Infrastructure Requirements'. An 'Add Policy' button is visible. To the right, there is a 'Maintenance Window' section with a description and two checked options: 'hourly @00' and 'hourly @30'.

## CSA MPP Requesting

Requesting the CSA offering does not differ from the ordinary request. In our case just enter RHEL 6.x server's FQN hostname and credentials, and database credentials (if MySQL 5.6 is installed and running on RHEL 6.x server).

Once the request is sent, the subscriber options values are mapped to properties of service instance component. Then corresponding ITOC entities are created, so ITOC can start compute compliance score.

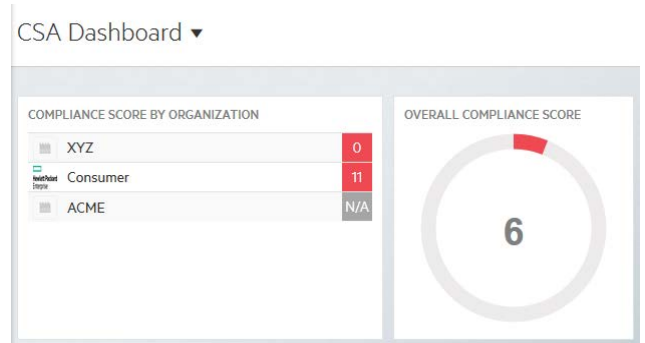


The screenshot shows the configuration form for a service offering in the Cloud Service Automation interface. The form includes fields for 'hostname' (server.my-domain.com), 'OS' (RHEL 6), 'username' (root), 'password' (masked), 'dbName' (test), 'dbUser' (admin), and 'dbPassword' (masked). The price is shown as '\$ 0.00' with a note '\$ 0.00 yearly'. There are 'Checkout' and 'Add To Cart' buttons. A 'Configuration' section shows the properties of the service instance component, including hostname, OS, username, password, dbName, dbUser, and dbPassword.

## CSA Operation Console

Once the ITOC starts compute compliance scores, and CSA displays it in following places

- CSA Dashboard
  - Two new widgets are displayed if the integration is enabled:
    - Compliance score by organization
    - Overall compliance score
- CSA Operations console – list of subscriptions and subscription detail



It takes some time to display compliance score because ITOC will start scan at times defined by maintenance windows.

## ITOC View of CSA Subscription

You can inspect mapped CSA subscription in ITOC UI. Because CSA UI and ITOC UI are not integrated on user-level it is not possible to sign in as user who requested CSA offering. You have to sign-in as *integration user* to inspect mapped CSA subscriptions.

You can find there mapped resources (with attributes), compliance score scan results, check if agent was installed, run compliance scan, etc.

**Note:** You can manually start scan if you use *jobrunner* account and starts the scan manually in ITOC UI.

The screenshot shows the ITOC UI for a CSA subscription. At the top, it displays 'Hewlett Packard Enterprise IT Operations Compliance' and the user 'serviceowner'. The subscription ID is 'SVC\_00252 - wp (1.0.0) (901c05d658f7544e0158f75a60d90113)' and the revision is '1 (Production)'. The compliance status is shown as a bar chart: 33% Compliant (green), 34% Non-Compliant (within RSLO) (yellow), and 33% Unknown (grey). Below this is a table of 'Statements of Applicability'.

ID	Policy	Compliance Score	Meeting MSLO	Meeting RSLO	Revision	Last Compliance Scan
STMT_0000502	Database requirements (Public)	0	No	Yes	1 (Production)	12/15/16 12:12 PM
STMT_0000501	Infrastructure Requirements (Public)	100	Yes	Yes	1 (Production)	12/13/16 10:07 AM

# Known problems and limitations

There are issues with the CSA – ITOC integration that are not addressed in this release.

## ITOC Integration Failure does not fail subscription

Failed integration (i.e., mapping of CSA entities to ITOC entities) does not fail CSA subscription. Failure can be detected by displaying N/A in column *score* of operation console list of subscriptions, and in the CSA *csa.log* file.

## List of ITOC Resource Types and Attributes of Resource Type

There is not list of ITOC resource types and their attributes available in ITOC UI. For up-to-date names use ITOC REST API. In [Appendix C: Default ITOC Resource Type Hierarchy and Attributes](#) there is a list of names of out-of-box installed ITOC resource types and attributes.

## Remediation maintenance windows are not supported

Do not use maintenance windows of window type *Scan & Remediation*, and *Remediation*. For such windows ITOC fails to compute compliance score (e.g., if controls of policy does not support remediation).

# Appendix A: Configuration of CSA 4.80 to Integrated with ITOC

## 1.20

Following table contains CSA configuration of CSA-ITOC integration as stored in [csa]/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties.

**Note:** every configuration change requires CSA restart

Example configuration:

```
### Start of ITOC Integration v.2 configuration #####
#Set this property to true if you want to integrate CSA with ITOC (IT Operation Compliance)
#csa.ITOC.IntegrationV2.enabled=true
csa.ITOC.IntegrationV2.enabled=true

#ITOCBaseUri, by replacing the <itoc_host> and <port> with the hostname and port used by ITOC instance
#default port 7771
#csa.ITOC.IntegrationV2.ITOCBaseUri=https://<itoc_host>:<port>/
csa.ITOC.IntegrationV2.ITOCBaseUri=https://my-itoc.mydomain.net:7771/

#ITOC integration users;
#there must be integration user for 'public' tenant
#and integration user for consumer tenants
#csa.ITOC.IntegrationV2.public.<user>=<password>
#csa.ITOC.IntegrationV2.<tenant>.<user>=<password>

#integration account of ITOC public tenant
csa.ITOC.IntegrationV2.public.viewer=ENC(1yDl/K4bwHJt3vBPONqXxw==)

#integration account of ITOC consumer tenant CONSUMER
csa.ITOC.IntegrationV2.CONSUMER.serviceowner=ENC(aETP/+KiAVM21NiDp0FAOQ==)

#the connection timeout to ITOC server (in milliseconds); if not configured default (10000) is used
csa.ITOC.IntegrationV2.timeout=10000

### End of ITOC Integration v.2 configuration #####
```

Table 1. CSA configuration

Item	Comments
csa.ITOC.IntegrationV2.enabled	Optional. Enable or disable integration v2 between CSA and ITOC. To enable, this property must be uncommented and set to true. To disable, either comment out the property or set it to false. Default: (disabled)
csa.ITOC.IntegrationV2.ITOCBaseUri	Required if integration v2 between CSA and ITOC is enabled. To enable, this property must be uncommented and set to the endpoint of the ITOC instance. The endpoint is the URL for connecting to the ITOC instance where <protocol> is the protocol used to communicate with the ITOC instance (for example, http or https), <itoc_host> is the hostname of the ITOC instance, and <port> is the port used to connect to the system on which ITOC is running. Default: (disabled)
csa.ITOC.IntegrationV2.public.<user>=<password>	Required if integration v2 between CSA and ITOC is enabled. To enable, this property must be uncommented and set to ITOC integration credentials. It is used to access ITOC public tenant to get the list of policies and maintenance windows.

	<p>Username is part of the configuration key and encrypted password is value of the configuration key.</p> <p>Password is encrypted using <i>PasswordUtil</i> tool.</p> <p>An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses.</p> <p>Default: (disabled)</p>
csa.ITOC.IntegrationV2.<tenant>.<user>=<password>	<p>Required if integration v2 between CSA and ITOC is enabled. To enable, this property must be uncommented and set to integration credentials for each consumer tenant of ITOC. Tenant is part of the configuration key, username is part of the configuration key and encrypted password is value of the configuration key.</p> <p>Password is encrypted using <i>PasswordUtil</i> tool.</p> <p>An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses.</p> <p>Default: (disabled)</p>
csa.ITOC.IntegrationV2.timeout=10000	<p>Required if integration v2 between CSA and ITOC is enabled. . To enable, this property must be uncommented and set to connection timeout in milliseconds.</p> <p>Default: (disabled)</p>



# Appendix B: Establishing trust between CSA and ITOC

Certificates of ITOC must be trusted by CSA order to establish mutual trust.

## Importing the ITOC certificate to CSA

Steps:

1. On the ITOC server export ITOC certificate from ITOC keystore located in `/opt/hp/itoc/wildfly-8.1.0.Final/standalone/configuration`

```
$ keytool -exportcert -keystore selfcacerts -alias itoc_self_signed -file itoc_self_signed.crt
```

The default ITOC password is *changeit*

Copy `itoc_self_signed.crt` to CSA server

2. On the CSA server, import ITOC certificate to the CSA keystore, which is found at `<CSA>/openjre/lib/security/cacerts`.

```
$ keytool -importcert -file itoc_self_signed.crt -alias ITOC -keystore cacerts -trustcacerts
```

The default CSA keystore password is *changeit*.

3. Restart the CSA service

# Appendix C: Default ITOC Resource Type Hierarchy and Attributes

Following table contains list of names of ITOC 1.20 default resource types and attributes. Use ITOC documentation and ITOC product for description of types and attributes.

ITOC Resource Type Name	Attribute Names of ITOC Resource Type
Business Service	
Device	Vendor,
Compute	Vendor,BiosUUID
Server	Vendor,BiosUUID
Group	
Platform	Hostname
Microsoft (MS) Windows	Hostname
MS Windows 7	Hostname
MS Windows 8	Hostname
MS Windows 8.1	Hostname
MS Windows Server 2008	Hostname
MS Windows Server 2008 R2	Hostname
MS Windows Server 2012	Hostname
MS Windows Server 2012 R2	Hostname
Unix	Hostname
HP-UX	Hostname
HP-UX 11.31	Hostname
IBM AIX	Hostname
IBM AIX 7.1	Hostname
Linux	Hostname
RHEL Compatibles	Hostname
RHEL 5 Compatibles	Hostname
CentOS 5	Hostname
OEL 5	Hostname
RHEL 5	Hostname
RHEL 6 Compatibles	Hostname
CentOS 6	Hostname
OEL 6	Hostname

RHEL 6	Hostname
RHEL 7 Compatibles	Hostname
CentOS 7	Hostname
OEL 7	Hostname
RHEL 7	Hostname
SUSE Compatibles	Hostname
OpenSUSE	Hostname
OpenSUSE 12	Hostname
OpenSUSE 13	Hostname
SUSE Linux Enterprise Server (SLES)	Hostname
SLES 10	Hostname
SLES 11	Hostname
Ubuntu Compatibles	Hostname
Debian	Hostname
Debian 7	Hostname
Ubuntu	Hostname
Ubuntu 12.04 LTS	Hostname
Ubuntu 14.04 LTS	Hostname
Oracle Solaris	Hostname
Oracle Solaris 11	Hostname
Oracle Solaris 11.1	Hostname
Resource Manager	description,version
Cloud Service Automation	description,version,user,password,serviceURL,tenant
HPE Server Automation	description,version,host,port,user,password,adapterHost
Software	
Application Server	
J2EE Server	
JBoss	JBOSS_HOME
JBoss Application Server 7	JBOSS_HOME
WebLogic	
Websphere	
Database	
DB2 Database Server	dbUser,dbPassword,dbName,DASUser,latestVersion(withFixPack)
DB2 Database Server 10.5	dbUser,dbPassword,dbName,DASUser,latestVersion(withFixPack)

DB2 Database Server 8	dbUser,dbPassword,dbName,DASUser,latestVersion(withFixPack)
DB2 Database Server 9	dbUser,dbPassword,dbName,DASUser,latestVersion(withFixPack)
DB2 Database Server 9.5	dbUser,dbPassword,dbName,DASUser,latestVersion(withFixPack)
MS SQL Server	dbUser,dbPassword,dbName
MSSQL Server 2005	dbUser,dbPassword,dbName
MYSQL	dbUser,dbPassword,dbName
MySQL Community Server 5.6	dbUser,dbPassword,dbName
Oracle	instanceName,instanceHome
Oracle 10g	instanceName,instanceHome
Oracle 11g	instanceName,instanceHome
Web Server	
Apache HTTP Server	APACHE_PREFIX,DOCROOT,HTTPD_ROOT
Apache HTTP Server 2.4	APACHE_PREFIX,DOCROOT,HTTPD_ROOT
Apache Tomcat	CATALINA_HOME,CATALINA_BASE
Apache Tomcat 6	CATALINA_HOME,CATALINA_BASE
NGINX	
Unknown	

# Appendix D: Consumer Organization Setup for illustration Purposes

This section describes setup of ITOC to connect to CSA out-of-box *CONSUMER* consumer organization for CSA-ITOC integration.

**Note:** this setup is for illustration purposes only, not for production.

Out-of-box CSA has preinstalled *CONSUMER* consumer organization, and ITOC has preinstalled *CSA\_CONSUMER* consumer organization. Using following steps ITOC *CSA\_CONSUMER* organization will be renamed to *CONSUMER*, and configured, so the integration supports integration of *CONSUMER* organization.

## Steps:

- On ITOC machine edit file

```
/opt/hp/itoc/wildfly-8.1.0.Final/standalone/deployments/idm-service.war/WEB-INF/classes/seededorgs.properties
```

- Change

```
CSA_CONSUMER=csa-consumer-users.properties
```

To

```
CONSUMER=csa-consumer-users.properties
```

- Restart ITOC using

```
$ /opt/hp/itoc/scripts/itoc restart
```

- Configure CSA-ITOC integration using users using table below and restart CSA
- Wait several minutes to restart of both CSA and ITOC
- Use username *csauser* and password *hpitoc* to sign in to ITOC and follow Consumer Organizations Setup

Product	Organization	Username	Password	Role
ITOC	CONSUMER	serviceowner	hpitoc	integration user
ITOC	CONSUMER	csauser	hpitoc	administrator user
ITOC	CONSUMER	jobrunner	hpitoc	user capable to run compliance score and remediation manually from ITOC UI
CSA	CONSUMER	consumer	cloud	CSA MPP consumer user requesting published offerings
ITOC	public	itocadmin	<specified during installation>	integration user for <i>public</i> tenant user capable of creating ITOC policies and maintenance windows
CSA	Provider	admin	cloud	user capable to create and publish designs and offerings

**Note:** to sign-in to ITOC *CONSUMER* organization note

- Open <https://<itoc-machine>:9000/org/public> and click on *Login* button
- When sign-in dialog is opened, then in browser location input change URL's query parameter *tenant* value to *CONSUMER*:
  - *tenant=public -> tenant=CONSUMER*
- Press enter in browser location input to reload sign-in dialog
- Now you can sign-in to *CONSUMER* organization

# 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 LP

### 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: <https://softwaresupport.hpe.com>.

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://softwaresupport.hpe.com>.