

Oracle® Cloud

Implementing Oracle Internet of Things Cloud Service



17.3.5
E80978-08
September 2017

ORACLE®

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	v
Documentation Accessibility	v
Related Documents	v
Conventions	vi

1 Setting Up Your Cloud Service Instance

Before You Use the Cloud Service	1-1
Using the ssh-keygen Utility to Generate an SSH Key Pair	1-2
Using the PuTTYgen Program to Generate an SSH Key Pair	1-2
Workflow for Implementing the Oracle Internet of Things Cloud Service	1-3
Creating an Oracle Internet of Things Cloud Service Instance	1-4
Creating an Oracle Internet of Things Cloud Service Instance with Analytics	1-6
Securing Your Data	1-9
Registering a Custom Domain Name with a Third-Party Registration Vendor	1-9
Updating Your Application Environment to Use a Custom Domain Name	1-10
Getting an SSL Certificate from a Certificate Authority	1-11
Creating a Self-Signed SSL Certificate	1-13
Installing an SSL Certificate Provided by a Certificate Authority	1-14
Accessing the Management Console	1-15

2 Activating Oracle Internet of Things Cloud Service SaaS Applications

Creating an Oracle IoT Asset Monitoring Cloud Service Instance	2-1
Creating an Oracle IoT Production Monitoring Cloud Service Instance	2-4
Creating an Oracle IoT Fleet Monitoring Cloud Service Instance	2-7
Creating an Oracle IoT Connected Worker Cloud Service Instance	2-9

3 Managing Users

Adding a User Account	3-1
-----------------------	-----

Editing a User Account	3-2
Removing a User Account	3-2

4 Troubleshooting Oracle Internet of Things Cloud Service

RSA Key Size Should be 1024 Bits	4-1
Unable to Delete Oracle Internet of Things Cloud Service Instance	4-1
Unable to Receive Data when Using an Apache Spark Cluster and the Kafka Handler	4-3
How to Get Support	4-4

Preface

The Oracle Internet of Things Cloud Service Implementation Guide provides information and procedures for implementing Oracle Internet of Things Cloud Service. Oracle Internet of Things Cloud Service lets you connect, analyze, and integrate device data into your business processes and applications, enabling your business to deliver innovative new services faster and with less risk. To implement Oracle Internet of Things Cloud Service, you create a Database Cloud Service instance and then a Oracle Java Cloud Service instance.

Topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Audience

The *Oracle Internet of Things Cloud Service Implementation Guide* is intended for system administrators who are responsible for implementing Oracle Internet of Things Cloud Service.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, see these Oracle resources:

- Oracle Cloud at <http://cloud.oracle.com>
- *Getting Started with Oracle Cloud*
- *Using Oracle Business Intelligence Cloud Service*

- [Getting Started with Oracle Stream Explorer](#)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Setting Up Your Cloud Service Instance

To set up a new cloud service, complete the procedures in the order they're presented. You'll need to do this when you purchase a new subscription.

Topics

- [Before You Use the Cloud Service](#)
- [Workflow for Implementing the Oracle Internet of Things Cloud Service](#)
- [Creating an Oracle Internet of Things Cloud Service Instance](#)
- [Creating an Oracle Internet of Things Cloud Service Instance with Analytics](#)
- [Securing Your Data](#)
- [Accessing the Management Console](#)

Before You Use the Cloud Service

Before you use Oracle Internet of Things Cloud Service for the first time:

- Purchase a subscription to Database Cloud Service. See [Buying a Metered Subscription to an Oracle Cloud Service](#) in *Getting Started with Oracle Cloud*.
- Purchase a subscription to Oracle Java Cloud Service. See [Buying a Metered Subscription to an Oracle Cloud Service](#) or [Buying a Non-Metered Subscription to an Oracle Cloud Service](#) in *Getting Started with Oracle Cloud*.
- Purchase a subscription to Oracle Internet of Things Cloud Service. See [Buying a Metered Subscription to an Oracle Cloud Service](#) in *Getting Started with Oracle Cloud*.
- (Optional) Purchase a subscription to Oracle Big Data Cloud Service - Compute Edition and Oracle Event Hub Cloud Service. These services are required for analytics functionality. See [Buying a Metered Subscription to an Oracle Cloud Service](#) or [Buying a Non-Metered Subscription to an Oracle Cloud Service](#) in *Getting Started with Oracle Cloud*.
- Create an 1024 bit SSH public/private key pair for Oracle Java Cloud Service. The SSH public key is used for authentication of the Oracle Internet of Things Cloud Service instance. When you create the Oracle Internet of Things Cloud Service instance, you must provide a Oracle Java Cloud Service private key that matches the Oracle Java Cloud Service public key. See [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#). When creating the SSH public/private key pair, do not use a passphrase.

Using the ssh-keygen Utility to Generate an SSH Key Pair

An SSH public key is used for authentication when you use an SSH client to connect to the Database Cloud Service instance. These procedures are specific to UNIX and UNIX-like operating systems.

For procedures that are specific to the Microsoft Windows operating system, see [Using the PuTTYgen Program to Generate an SSH Key Pair](#).

1. Open a command prompt and run the `cd $HOME` command to browse to your home directory.
2. Run this command to create the SSH public key:

```
ssh-keygen -b 1024 -t rsa filename
```

Replace *filename* with a unique filename for your SSH public key.

3. Enter the file to which the key pair should be saved when the Enter file in which to save the key prompt appears.
4. Leave the Enter passphrase (empty for no passphrase) and Enter the same passphrase again prompts empty.

This message appears:

```
Your identification has been saved in filename.
Your public key has been saved in filename.pub.
The key fingerprint is:
<fingerprint code>
The key's randomart image is:
<randomart image>
```

Using the PuTTYgen Program to Generate an SSH Key Pair

An SSH public key is used for authentication when you use an SSH client to connect to the Database Cloud Service instance. These procedures are specific to the Microsoft Windows operating system.

For procedures that are specific to UNIX and UNIX-like operating systems, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#).

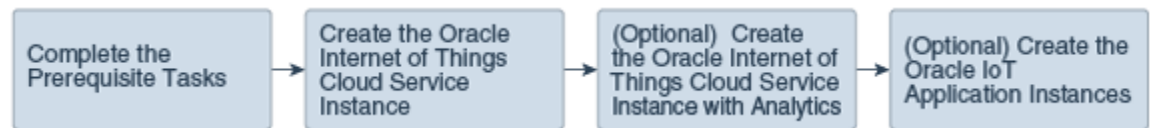
1. Download and install PuTTY from <http://www.putty.org/>.
2. On your computer, click **Start, All Programs, PuTTY**, and then **PuTTYgen**.
3. Select **SSH-2 RSA** in the **Parameters** area.
4. Enter **1024** in the **Number of bits in a generated key** field.
5. Click **Generate** and then move the cursor around the blank area of the **Key** area to generate the random characters that create a unique key.
6. Leave the **Key passphrase** and **Confirm passphrase** fields empty.
7. Export the SSH private key:
 - a. Click **Conversions** and then **Export OpenSSH key**.
 - b. Click **Yes** when the **PuTTYgen Warning** dialog appears.
 - c. Enter a name for the SSH private key file, change the file extension to **.openssh**, and then click **Save**.

8. Select and copy all of the characters in the **Public key for pasting into OpenSSH authorized_keys file** area.
9. Open a text editor and paste the text you copied in step 8.
10. Save the SSH public key file in the same location as the SSH private key.
11. Enter a name for the SSH public key file, change the file extension to `.pub`, and then click **Save**.

Workflow for Implementing the Oracle Internet of Things Cloud Service

To implement Oracle Internet of Things Cloud Service, complete the tasks listed in the table.

This image represents the workflow for implementing Oracle Internet of Things Cloud Service:



Task	Description	More Information
Complete the prerequisite tasks.	Complete the prerequisite tasks to successfully complete the implementation.	Before You Use the Cloud Service
Create the Oracle Internet of Things Cloud Service instance.	Create the Oracle Internet of Things Cloud Service instance to manage and monitor devices and gateways.	Creating an Oracle Internet of Things Cloud Service Instance or Creating an Oracle Internet of Things Cloud Service Instance with Analytics
(Optional) Create the Oracle Internet of Things Applications	Create the optional cloud service instances. A subscription is required to create each application.	Activating Oracle Internet of Things Cloud Service SaaS Applications

Creating an Oracle Internet of Things Cloud Service Instance

Create a Oracle Internet of Things Cloud Service to manage and monitor devices and gateways.



Note:

When using Oracle Cloud Stack Manager to create Oracle cloud service instances, the cloud service instances cannot be used individually. For example, if Oracle Cloud Stack Manager is used to create the Database Cloud Service, Oracle Java Cloud Service, and Oracle Internet of Things Cloud Service instances, you cannot associate a standalone Oracle Internet of Things Cloud Service instance with a Oracle Java Cloud Service instance created with Oracle Cloud Stack Manager.

1. Sign in to Oracle Cloud:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.
 - b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.
 - c. Copy the user name displayed in the **Username** field and then paste it into the **User Name** field.
 - d. Copy the password displayed in the **Temporary Password** field and then paste it into the **Password** field.
 - e. Click **Sign In**.
 - f. If this is your first time accessing Oracle Cloud, create a new password and provide challenge questions to verify your access credentials. Click **Submit** after you create your password and provide your challenge questions.
 - g. Click **Continue** if a welcome dialog appears.
2. Locate and copy the Oracle Storage Cloud Service REST endpoint URL. This URL forms part of the name for the Cloud Storage Container and Content Storage Container fields that you complete later in this procedure.
 - a. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Storage** below **Monitoring Metrics**.
 - b. Click **Overview** in the left pane.
 - c. Copy the URL displayed in the **REST Endpoint (Permanent)** field and paste it into a text editor or word processing application.
3. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Oracle Cloud Stack**.
4. Click **Create Stack**.
5. Complete these fields in the **Stack Details** area:

- **Name:** Enter a unique name for the Oracle Internet of Things Cloud Service instance.
 - **Description:** (Optional) Enter a description for the Oracle Internet of Things Cloud Service instance.
 - **Template:** Select **Oracle-IOTEnterpriseApps-Template**.
 - **On Failure Retain Resources:** Select this option to retain the settings for the stack in case of failure.
6. Complete these fields in the **Service Details** area:
- **Installation Type:** Select **Production** to create a production instance, or select **Development** to create a development instance.
 - **Number of Named Users:** Enter **1** if you selected a development installation, or enter a value greater than one or accept the default value if you selected a production installation.
 - **Username for Cloud Services:** Accept the default value.
 - **Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **Confirm Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **SSH Public Key:** Click **Edit** and upload a SSH public key file or enter the SSH public key value used for Oracle Internet of Things Cloud Service authentication.



Note:

Do not select **Create a New Key** to auto-generate a SSH public/private key pair. The auto-generated key pair is 2048 bits and cannot be used for Oracle Internet of Things Cloud Service authentication. To manually create a SSH public/private key pair, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#). When creating the SSH public/private key pair, do not use a passphrase.

7. Complete these fields in the **Backup and Recovery Configuration** area:
- **Cloud Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackup.
 - **Cloud Storage Username:** Enter the user name you used to sign in to Oracle Cloud in step 1.
 - **Cloud Storage Password:** Enter the password you used to sign in to Oracle Cloud in step 1.
8. Complete these fields in the **Content Storage Container** area:
- **Content Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackupcontainer.
 - **Use same credentials as Cloud Storage Container:** Select **true** to use the credentials you specified in step 7 to access content storage, or select **false** to provide different access credentials.

- **Content Storage Username:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter a user name for Cloud Storage Container access.
 - **Content Storage Password:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter the password used to access the Cloud Storage Container.
9. Complete these fields in the **Oracle Internet of Things - Enterprise** area:
 - **Enter private key:** Paste the private key that matches the public key you uploaded in the **Service Details** area.
 - **Create spare JCS instance:** Select **true** to create an additional Oracle Java Cloud Service instance, or select **false** if you do not want to create an additional Oracle Java Cloud Service instance.
 - **Enable IoT Device Simulator:** Select **true** to create an Oracle Internet of Things Cloud Service device simulator, or select **false** if you do not want to create an Oracle Internet of Things Cloud Service device simulator. A device simulator can help you test communications between devices and your Oracle Internet of Things Cloud Service instance.
 10. Click **Next**.
 11. Click **Confirm**.

It can take 30 minutes or longer to activate the Oracle Internet of Things Cloud Service instance.

Creating an Oracle Internet of Things Cloud Service Instance with Analytics

Create a Oracle Internet of Things Cloud Service to manage and monitor devices and gateways. Activate analytics to access predictive analytics functionality.



Note:

When using Oracle Cloud Stack Manager to create Oracle cloud service instances, the cloud service instances cannot be used individually. For example, if Oracle Cloud Stack Manager is used to create the Database Cloud Service, Oracle Java Cloud Service, and Oracle Internet of Things Cloud Service instances, you cannot associate a standalone Oracle Internet of Things Cloud Service instance with a Oracle Java Cloud Service instance created with Oracle Cloud Stack Manager.

1. Sign in to Oracle Cloud:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.
 - b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.
 - c. Copy the user name displayed in the **Username** field and then paste it into the **User Name** field.

- d. Copy the password displayed in the **Temporary Password** field and then paste it into the **Password** field.
 - e. Click **Sign In**.
 - f. If this is your first time accessing Oracle Cloud, create a new password and provide challenge questions to verify your access credentials. Click **Submit** after you create your password and provide your challenge questions.
 - g. Click **Continue** if a welcome dialog appears.
2. Locate and copy the Oracle Storage Cloud Service REST endpoint URL. This URL forms part of the name for the Cloud Storage Container and Content Storage Container fields that you complete later in this procedure.
 - a. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Storage** below **Monitoring Metrics**.
 - b. Click **Overview** in the left pane.
 - c. Copy the URL displayed in the **REST Endpoint (Permanent)** field and paste it into a text editor or word processing application.
3. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Oracle Cloud Stack**.
4. Complete these fields in the **Stack Details** area:
 - **Name:** Enter a unique name for the Oracle Internet of Things Cloud Service instance.
 - **Description:** (Optional) Enter a description for the Oracle Internet of Things Cloud Service instance.
 - **Template:** Select **Oracle-IOTEnterpriseApps-Analytics-Template**.
 - **On Failure Retain Resources:** Select this option to retain the settings for the stack in case of failure.
5. Complete these fields in the **Service Details** area:
 - **Installation Type:** Select **Production** to create a production instance, or select **Development** to create a development instance.
 - **Number of Named Users:** Enter **1** if you selected a development installation, or enter a value greater than one or accept the default value if you selected a production installation.
 - **Username for Cloud Services:** Accept the default value.
 - **Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **Confirm Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **SSH Public Key:** Click **Edit** and upload a SSH public key file or enter the SSH public key value used for Oracle Internet of Things Cloud Service authentication.

**Note:**

Do not select **Create a New Key** to auto-generate a SSH public/private key pair. The auto-generated key pair is 2048 bits and cannot be used for Oracle Internet of Things Cloud Service authentication. To manually create a SSH public/private key pair, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#). When creating the SSH public/private key pair, do not use a passphrase.

6. Complete these fields in the **Backup and Recovery Configuration** area:
 - **Cloud Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackup.
 - **Cloud Storage Username:** Enter the user name you used to sign in to Oracle Cloud in step 1.
 - **Cloud Storage Password:** Enter the password you used to sign in to Oracle Cloud in step 1.
7. Complete these fields in the **Content Storage Container** area:
 - **Content Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackupcontainer.
 - **Use same credentials as Cloud Storage Container:** Select **true** to use the credentials you specified in step 7 to access content storage, or select **false** to provide different access credentials.
 - **Content Storage Username:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter a user name for Cloud Storage Container access.
 - **Content Storage Password:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter the password used to access the Cloud Storage Container.
8. Complete these fields in the **Oracle Internet of Things Cloud Analytics** area:
 - **Enter private key:** Paste the private key that matches the public key you uploaded in the **Service Details** area.
 - **PSM URL:** Accept the default value.
 - **MyServices Username:** Enter the user name used to access the Oracle Platform as a Service Service Manager.
 - **MyServices Password:** Enter the password used to access the Oracle Platform as a Service Service Manager.
 - **Create spare JCS instance:** Select **true** to create an additional Oracle Java Cloud Service instance, or select **false** if you do not want to create an additional Oracle Java Cloud Service instance.
 - **Enable IoT Device Simulator:** Select **true** to create an Oracle Internet of Things Cloud Service device simulator, or select **false** if you do not want to create an Oracle Internet of Things Cloud Service device simulator. A device simulator can help you test communications between devices and your Oracle Internet of Things Cloud Service instance.

9. Click **Next**.
10. Click **Confirm**.

It can take 30 minutes or longer to activate the Oracle Internet of Things Cloud Service instance.

Securing Your Data

To make sure the data sent and received by your devices remains secure, Oracle recommends using the Secure Socket Layer (SSL) security protocol. To use an SSL certificate to secure your application data, you configure SSL between the device and the load balancer. The installation of an SSL certificate provided by a Certificate Authority is recommended for production deployments, and is mandatory if you are using the Oracle IoT Asset Monitoring Mobile Application or the Oracle IoT Fleet Monitoring Mobile Application. For development and testing, you can use a self-signed SSL certificate.



Note:

Before you can implement SSL, make sure that you have registered your custom domain name and activated the load balancer in the Oracle Java Cloud Service. To activate the load balancer, see [Disabling or Enabling the Load Balancer for an Oracle Java Cloud Service Instance](#). To register your custom domain name, see [Registering a Custom Domain Name with a Third-Party Registration Vendor](#).

Topics

- [Registering a Custom Domain Name with a Third-Party Registration Vendor](#)
- [Updating Your Application Environment to Use a Custom Domain Name](#)
- [Getting an SSL Certificate from a Certificate Authority](#)
- [Creating a Self-Signed SSL Certificate](#)
- [Installing an SSL Certificate Provided by a Certificate Authority](#)

Registering a Custom Domain Name with a Third-Party Registration Vendor

If you want to access your applications with a custom Uniform Resource Locator (URL) instead of a public Internet Protocol (IP) address, you register and then associate a custom “vanity” domain name with your application environment.

1. Create the Oracle Internet of Things Cloud Service instance. See [Creating an Oracle Internet of Things Cloud Service Instance](#) or [Creating an Oracle Internet of Things Cloud Service Instance with Analytics](#).
2. Record the load balancer public IP address. To view the public IP address:
 - a. Open a web browser and browse to <http://cloud.oracle.com>.
 - b. Click **Sign In**.

- c. Select the data center where your services are located in the **Select Data Center** list.
 - d. Click **My Services**.
 - e. Enter the identity domain provided and then click **Go**.
 - f. Enter your user name and your password and then click **Sign In**.
 - g. Click the **Menu** () icon next to Oracle Cloud My Services and then select Oracle Java Cloud Service.
 - h. Click a service in the **Services** list.
 - i. Expand **Load Balancer**.
The public IP address for the load balancer appears in the **Content endpoint** field.
3. Register your custom domain name through a third-party domain registration vendor.
 4. Resolve your domain name to the IP address of the Oracle Java Cloud Service load balancer, using the third-party domain registration vendor console.
- For more information, refer to the third-party domain registration documentation.

Updating Your Application Environment to Use a Custom Domain Name

You update the application to use the custom domain name after registering a custom domain name. Using a custom domain name lets users access your applications with a custom Uniform Resource Locator (URL) such as `example.com`.

Note:

By default, access to the administration consoles is disabled. If you did not enable console access when you set up your Oracle Java Cloud Service instance, see [Enabling Console Access in an Oracle Java Cloud Service Instance](#).

1. Open a web browser and browse to <http://cloud.oracle.com>.
2. Click **Sign In**.
3. Select the data center where your services are located in the **Select Data Center** list.
4. Click **My Services**.
5. Enter the identity domain provided and then click **Go**.
6. Enter your user name and your password and then click **Sign In**.
7. Click the **Menu** () icon next to Oracle Cloud My Services and then select Oracle Java Cloud Service.

8. Click the **Menu** () icon for a service in the **Services** list and then select **Open Load Balancer Console**.

If the server is protected with a self-signed certificate, you will be warned that this certificate is not trusted.

9. Accept the certificate if prompted and choose one of these options:
 - If you are using Firefox, click **Advanced** , click **Add Exception** and then click **Confirm Security Exception**.
 - If you are using Chrome, click **Advanced** and then click **Proceed**.
10. Log in to the load balancer console using the credentials you used when you provisioned your Oracle Java Cloud Service instance.

If you created your Oracle Java Cloud Service instance using the Oracle Java Cloud Service console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.

11. Click the **Target Navigation** () icon.
12. Expand **Traffic Director** in the left pane.
13. Click the virtual server name. For example, `opc-config`.
14. Click **Virtual Servers** in the left pane.
15. Click the virtual server in the **Name** column in the right pane. For example, `opc-config`.
16. Expand **General Settings** and enter the custom domain name (for example, `example.com`) in the **Hosts** field.

If there are multiple entries, separate each by a comma.
17. Click **Apply**.

Getting an SSL Certificate from a Certificate Authority

Use a SSL certificate issued by a Certificate Authority to encrypt the data that is sent and received by your devices. To obtain an SSL certificate from a Certificate Authority, you create a Certificate Signing Request (CSR) and then submit the CSR to the Certificate Authority vendor. The CSR includes the public key and other information that the Certificate Authority vendor needs to verify the identity of the load balancer server on which you want to enable SSL. The implementation of an SSL Certificate Authority certificate is recommended for production deployments and is mandatory if you are using the Oracle IoT Asset Monitoring Mobile Application or the Oracle IoT Fleet Monitoring Mobile Application.

1. Log in to the Oracle Java Cloud Service:
 - a. Open a web browser and browse to <http://cloud.oracle.com>.
 - b. Click **Sign In**.
 - c. Select the data center where your services are located in the **Select Data Center** list.
 - d. Click **My Services**.
 - e. Enter the identity domain provided and then click **Go**.

- f. Enter your user name and your password and then click **Sign In**.
 - g. Click the **Menu** () icon next to Oracle Cloud My Services and then select Oracle Java Cloud Service.
2. Click the **Menu** () icon for a service in the **Services** list and then select **Open Load Balancer Console**.

If the server is protected with a self-signed certificate, you will be warned that this certificate is not trusted.
 3. Accept the certificate if prompted and choose one of these options:
 - If you are using Firefox, click **Advanced** , click **Add Exception** and then click **Confirm Security Exception**.
 - If you are using Chrome, click **Advanced** and then click **Proceed**.
 4. Log in to the load balancer console using the credentials you used when you provisioned your Oracle Java Cloud Service instance.

If you created your Oracle Java Cloud Service instance using the Oracle Java Cloud Service console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.
 5. Click the **Target Navigation** () icon.
 6. Expand **Traffic Director** in the left pane.
 7. Click the virtual server name. For example, `opc-config`.
 8. Click the **Traffic Director Configuration** menu in the top left, select **Security**, and then **Manage Certificates**.
 9. Select an alias in the **Alias** list.
 10. Click **Generate CSR** .
 11. Click **Export CSR** and save the CSR file as a .txt file.
 12. Click **Close**.
 13. Send the CSR to your Certificate Authority vendor and request a new SSL certificate. Include this information with your request:
 - Your custom domain name.
 - Public information associated with the domain confirming you as the owner.
 - Email address associated with the custom domain for verification.
 - The load balancer public IP address. To locate the load balancer public IP address, see [Registering a Custom Domain Name with a Third-Party Registration Vendor](#).
 - The fully qualified domain name (FQDN) for the load balancer. To identify the FQDN, open an SSH client, connect to the load balancer, and then run the `hostname -f` command.

For more information about submitting the CSR, refer to the documentation provided by your Certificate Authority vendor.

Creating a Self-Signed SSL Certificate

Use a self-signed SSL certificate to encrypt the data that is sent and received by your devices. The implementation of a self-signed SSL certificate is recommended for development and testing. The implementation of an SSL certificate provided by a Certificate Authority is recommended for production deployments and is mandatory if you are using the Oracle IoT Asset Monitoring Mobile Application or the Oracle IoT Fleet Monitoring Mobile Application.

1. Log in to the Oracle Java Cloud Service:
 - a. Open a web browser and browse to <http://cloud.oracle.com>.
 - b. Click **Sign In**.
 - c. Select the data center where your services are located in the **Select Data Center** list.
 - d. Click **My Services**.
 - e. Enter the identity domain provided and then click **Go**.
 - f. Enter your user name and your password and then click **Sign In**.
 - g. Click the **Menu** () icon next to Oracle Cloud My Services and then select Oracle Java Cloud Service.
2. Click the **Menu** () icon for a service in the **Services** list and then select **Open Load Balancer Console**.

If the server is protected with a self-signed certificate, you will be warned that this certificate is not trusted.
3. Accept the certificate if prompted and choose one of these options:
 - If you are using Firefox, click **Advanced** , click **Add Exception** and then click **Confirm Security Exception**.
 - If you are using Chrome, click **Advanced** and then click **Proceed**.
4. Log in to the load balancer console using the credentials you used when you provisioned your Oracle Java Cloud Service instance.

If you created your Oracle Java Cloud Service instance using the Oracle Java Cloud Service console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.
5. Click the **Target Navigation** () icon.
6. Expand **Traffic Director** in the left pane.
7. Click the virtual server name. For example, `opc-config`.
8. Click the **Traffic Director Configuration** menu in the top left, select **Security**, and then **Manage Certificates**.
9. Select an alias in the **Alias** list.
10. Click **Generate Keypair** .
11. Complete the mandatory and optional fields for the key pair and then click **OK**.

Installing an SSL Certificate Provided by a Certificate Authority

Use a self-signed SSL certificate to encrypt the data that is sent and received by your devices. The implementation of a self-signed SSL certificate is recommended for development and testing. The implementation of an SSL certificate provided by a Certificate Authority is recommended for production deployments and is mandatory if you are using the Oracle IoT Asset Monitoring Mobile Application or the Oracle IoT Fleet Monitoring Mobile Application.

1. Log in to the Oracle Java Cloud Service:
 - a. Open a web browser and browse to <http://cloud.oracle.com>.
 - b. Click **Sign In**.
 - c. Select the data center where your services are located in the **Select Data Center** list.
 - d. Click **My Services**.
 - e. Enter the identity domain provided and then click **Go**.
 - f. Enter your user name and your password and then click **Sign In**.
 - g. Click the **Menu** () icon next to Oracle Cloud My Services and then select Oracle Java Cloud Service.
2. Click the **Menu** () icon for a service in the **Services** list and then select **Open Load Balancer Console**.

If the server is protected with a self-signed certificate, you will be warned that this certificate is not trusted.
3. Accept the certificate if prompted and choose one of these options:
 - If you are using Firefox, click **Advanced**, click **Add Exception** and then click **Confirm Security Exception**.
 - If you are using Chrome, click **Advanced** and then click **Proceed**.
4. Log in to the load balancer console using the credentials you used when you provisioned your Oracle Java Cloud Service instance.

If you created your Oracle Java Cloud Service instance using the Oracle Java Cloud Service console, the user name and password default to the Oracle WebLogic Server Administration Console user name and password.
5. Click the **Target Navigation** () icon.
6. Expand **Traffic Director** in the left pane.
7. Click the virtual server name. For example, `opc-config`.
8. Click the **Traffic Director Configuration** menu in the top left, select **Security**, and then **Manage Certificates**.
9. Select an alias in the **Alias** list.
10. Import the trusted certificate:
 - a. Click **Import**.

- b. Select **Trusted Certificate** in the **Certificate Type** list.
- c. Enter a name for the SSL certificate in the **Alias** field.
- d. Select **Select a file that contains the Certificate or Certificate Chain**.
- e. Click **Browse** and browse to the location of the SSL certificate provided by the Certificate Authority.
- f. Select the SSL certificate and then click **Open**.
- g. Click **OK**.

Accessing the Management Console

Access the Oracle Internet of Things Cloud Service management console to manage your Oracle Internet of Things Cloud Service instance. This procedure assumes that you have created your Oracle Internet of Things Cloud Service instance.

1. Sign in to Oracle Cloud:
 - a. Open a web browser and browse to <http://cloud.oracle.com>.
 - b. Click **Sign In**.
 - c. Select the data center where your services are located in the **Select Data Center** list.
 - d. Click **My Services**.
 - e. Enter the identity domain provided in your welcome email and then click **Go**.
 - f. Enter your user name and your password and then click **Sign In**.
2. Select **Internet of Things** in the **My Oracle Services** area.

2

Activating Oracle Internet of Things Cloud Service SaaS Applications

Follow these procedures to create the optional Oracle Internet of Things Cloud Service Software as a Service (SaaS) applications. A subscription is required to create each application.

Topics

- [Creating an Oracle IoT Asset Monitoring Cloud Service Instance](#)
- [Creating an Oracle IoT Production Monitoring Cloud Service Instance](#)
- [Creating an Oracle IoT Fleet Monitoring Cloud Service Instance](#)
- [Creating an Oracle IoT Connected Worker Cloud Service Instance](#)

Creating an Oracle IoT Asset Monitoring Cloud Service Instance

If you have subscribed to Oracle IoT Asset Monitoring Cloud Service, use this procedure to create the application.

Note:

When using Oracle Cloud Stack Manager to create Oracle cloud service instances, the cloud service instances cannot be used individually. For example, if Oracle Cloud Stack Manager is used to create the Database Cloud Service, Oracle Java Cloud Service, and Oracle Internet of Things Cloud Service instances, you cannot associate a standalone Oracle Internet of Things Cloud Service instance with a Oracle Java Cloud Service instance created with Oracle Cloud Stack Manager.

1. Sign in to Oracle Cloud:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.
 - b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.
 - c. Copy the user name displayed in the **Username** field and then paste it into the **User Name** field.
 - d. Copy the password displayed in the **Temporary Password** field and then paste it into the **Password** field.
 - e. Click **Sign In**.

- f. If this is your first time accessing Oracle Cloud, create a new password and provide challenge questions to verify your access credentials. Click **Submit** after you create your password and provide your challenge questions.
 - g. Click **Continue** if a welcome dialog appears.
2. Locate and copy the Oracle Storage Cloud Service REST endpoint URL. This URL forms part of the name for the Cloud Storage Container and Content Storage Container fields that you complete later in this procedure.
 - a. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Storage** below **Monitoring Metrics**.
 - b. Click **Overview** in the left pane.
 - c. Copy the URL displayed in the **REST Endpoint (Permanent)** field and paste it into a text editor or word processing application.
3. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Oracle Cloud Stack**.
4. Complete these fields in the **Stack Details** area:
 - **Name:** Enter a unique name for the Oracle IoT Asset Monitoring Cloud Service instance.
 - **Description:** (Optional) Enter a description for the Oracle IoT Asset Monitoring Cloud Service instance.
 - **Template:** Select **Oracle-IOTAssetMon-Analytics-Template**.
 - **On Failure Retain Resources:** Select this option to retain the settings for the stack in case of failure.
5. Complete these fields in the **Service Details** area:
 - **Installation Type:** Select **Production** to create a production instance, or select **Development** to create a development instance.
 - **Number of Named Users:** Enter **1** if you selected a development installation, or enter a value greater than one or accept the default value if you selected a production installation.
 - **Username for Cloud Services:** Accept the default value.
 - **Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **Confirm Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **SSH Public Key:** Click **Edit** and upload a SSH public key file or enter the SSH public key value used for Oracle Internet of Things Cloud Service authentication.

 Note:

Do not select **Create a New Key** to auto-generate a SSH public/private key pair. The auto-generated key pair is 2048 bits and cannot be used for Oracle Internet of Things Cloud Service authentication. To manually create a SSH public/private key pair, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#). When creating the SSH public/private key pair, do not use a passphrase.

6. Complete these fields in the **Backup and Recovery Configuration** area:
 - **Cloud Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackup.
 - **Cloud Storage Username:** Enter the user name you used to sign in to Oracle Cloud in step 1.
 - **Cloud Storage Password:** Enter the password you used to sign in to Oracle Cloud in step 1.
7. Complete these fields in the **Content Storage Container** area:
 - **Content Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackupcontainer.
 - **Use same credentials as Cloud Storage Container:** Select **true** to use the credentials you specified in step 6 to access content storage, or select **false** to provide different access credentials.
 - **Content Storage Username:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter a user name for Cloud Storage Container access.
 - **Content Storage Password:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter the password used to access the Cloud Storage Container.
8. Complete these fields in the **Oracle IoT Asset Monitoring Cloud Service** area:
 - **Enter private key:** Paste the private key that matches the public key you uploaded in the **Service Details** area.
 - **PSM URL:** Accept the default value.
 - **MyServices Username:** Enter the user name used to access the Oracle Platform as a Service Service Manager.
 - **MyServices Password:** Enter the password used to access the Oracle Platform as a Service Service Manager.
 - **Create spare JCS instance:** Select **true** to create an additional Oracle Java Cloud Service instance, or select **false** if you do not want to create an additional Oracle Java Cloud Service instance.
 - **Enable IoT Device Simulator:** Select **true** to create an Oracle Internet of Things Cloud Service device simulator, or select **false** if you do not want to create an Oracle Internet of Things Cloud Service device simulator. A device simulator can help you test communications between devices and your Oracle Internet of Things Cloud Service instance.

9. Click **Next**.

10. Click **Confirm**.

It can take 30 minutes or longer to activate the Oracle Internet of Things Cloud Service instance.

Creating an Oracle IoT Production Monitoring Cloud Service Instance

If you have subscribed to Oracle IoT Production Monitoring Cloud Service, use this procedure to create the application.



Note:

When using Oracle Cloud Stack Manager to create Oracle cloud service instances, the cloud service instances cannot be used individually. For example, if Oracle Cloud Stack Manager is used to create the Database Cloud Service, Oracle Java Cloud Service, and Oracle Internet of Things Cloud Service instances, you cannot associate a standalone Oracle Internet of Things Cloud Service instance with a Oracle Java Cloud Service instance created with Oracle Cloud Stack Manager.

1. Sign in to Oracle Cloud:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.
 - b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.
 - c. Copy the user name displayed in the **Username** field and then paste it into the **User Name** field.
 - d. Copy the password displayed in the **Temporary Password** field and then paste it into the **Password** field.
 - e. Click **Sign In**.
 - f. If this is your first time accessing Oracle Cloud, create a new password and provide challenge questions to verify your access credentials. Click **Submit** after you create your password and provide your challenge questions.
 - g. Click **Continue** if a welcome dialog appears.
2. Locate and copy the Oracle Storage Cloud Service REST endpoint URL. This URL forms part of the name for the Cloud Storage Container and Content Storage Container fields that you complete later in this procedure.
 - a. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Storage** below **Monitoring Metrics**.
 - b. Click **Overview** in the left pane.
 - c. Copy the URL displayed in the **REST Endpoint (Permanent)** field and paste it into a text editor or word processing application.
3. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Oracle Cloud Stack**.

4. Complete these fields in the **Stack Details** area:
 - **Name:** Enter a unique name for the Oracle IoT Production Monitoring Cloud Service instance.
 - **Description:** (Optional) Enter a description for the Oracle IoT Production Monitoring Cloud Service instance.
 - **Template:** Select **Oracle-IOTProdMonitoring-Analytics-Template**.
 - **On Failure Retain Resources:** Select this option to retain the settings for the stack in case of failure.
5. Complete these fields in the **Service Details** area:
 - **Installation Type:** Select **Production** to create a production instance, or select **Development** to create a development instance.
 - **Number of Named Users:** Enter **1** if you selected a development installation, or enter a value greater than one or accept the default value if you selected a production installation.
 - **Username for Cloud Services:** Accept the default value.
 - **Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **Confirm Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **SSH Public Key:** Click **Edit** and upload a SSH public key file or enter the SSH public key value used for Oracle Internet of Things Cloud Service authentication.

 Note:

Do not select **Create a New Key** to auto-generate a SSH public/private key pair. The auto-generated key pair is 2048 bits and cannot be used for Oracle Internet of Things Cloud Service authentication. To manually create a SSH public/private key pair, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#). When creating the SSH public/private key pair, do not use a passphrase.

6. Complete these fields in the **Backup and Recovery Configuration** area:
 - **Cloud Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackup.
 - **Cloud Storage Username:** Enter the user name you used to sign in to Oracle Cloud in step 1.
 - **Cloud Storage Password:** Enter the password you used to sign in to Oracle Cloud in step 1.
7. Complete these fields in the **Content Storage Container** area:
 - **Content Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackupcontainer.

- **Use same credentials as Cloud Storage Container:** Select **true** to use the credentials you specified in step 6 to access content storage, or select **false** to provide different access credentials.
 - **Content Storage Username:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter a user name for Cloud Storage Container access.
 - **Content Storage Password:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter the password used to access the Cloud Storage Container.
8. Complete these fields in the **Oracle IoT Production Monitoring Cloud Service** area:
- **Enter private key:** Paste the private key that matches the public key you uploaded in the **Service Details** area.
 - **PSM URL:** Accept the default value.
 - **MyServices Username:** Enter the user name used to access the Oracle Platform as a Service Service Manager.
 - **MyServices Password:** Enter the password used to access the Oracle Platform as a Service Service Manager.
 - **Create spare JCS instance:** Select **true** to create an additional Oracle Java Cloud Service instance, or select **false** if you do not want to create an additional Oracle Java Cloud Service instance.
 - **Enable IoT Device Simulator:** Select **true** to create an Oracle Internet of Things Cloud Service device simulator, or select **false** if you do not want to create an Oracle Internet of Things Cloud Service device simulator. A device simulator can help you test communications between devices and your Oracle Internet of Things Cloud Service instance.
9. Click **Next**.
10. Click **Confirm**.

It can take 30 minutes or longer to activate the Oracle Internet of Things Cloud Service instance.

Creating an Oracle IoT Fleet Monitoring Cloud Service Instance

If you have subscribed to Oracle IoT Fleet Monitoring Cloud Service, use this procedure to create the application.

Note:

When using Oracle Cloud Stack Manager to create Oracle cloud service instances, the cloud service instances cannot be used individually. For example, if Oracle Cloud Stack Manager is used to create the Database Cloud Service, Oracle Java Cloud Service, and Oracle Internet of Things Cloud Service instances, you cannot associate a standalone Oracle Internet of Things Cloud Service instance with a Oracle Java Cloud Service instance created with Oracle Cloud Stack Manager.

1. Sign in to Oracle Cloud:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.
 - b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.
 - c. Copy the user name displayed in the **Username** field and then paste it into the **User Name** field.
 - d. Copy the password displayed in the **Temporary Password** field and then paste it into the **Password** field.
 - e. Click **Sign In**.
 - f. If this is your first time accessing Oracle Cloud, create a new password and provide challenge questions to verify your access credentials. Click **Submit** after you create your password and provide your challenge questions.
 - g. Click **Continue** if a welcome dialog appears.
2. Locate and copy the Oracle Storage Cloud Service REST endpoint URL. This URL forms part of the name for the Cloud Storage Container and Content Storage Container fields that you complete later in this procedure.
 - a. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Storage** below **Monitoring Metrics**.
 - b. Click **Overview** in the left pane.
 - c. Copy the URL displayed in the **REST Endpoint (Permanent)** field and paste it into a text editor or word processing application.
3. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Oracle Cloud Stack**.
4. Complete these fields in the **Stack Details** area:
 - **Name:** Enter a unique name for the Oracle IoT Fleet Monitoring Cloud Service instance.

- **Description:** (Optional) Enter a description for the Oracle IoT Fleet Monitoring Cloud Service instance.
 - **Template:** Select **Oracle-IOTFleetMon-Analytics-Template**.
 - **On Failure Retain Resources:** Select this option to retain the settings for the stack in case of failure.
5. Complete these fields in the **Service Details** area:
- **Installation Type:** Select **Production** to create a production instance, or select **Development** to create a development instance.
 - **Number of Named Users:** Enter **1** if you selected a development installation, or enter a value greater than one or accept the default value if you selected a production installation.
 - **Username for Cloud Services:** Accept the default value.
 - **Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **Confirm Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **SSH Public Key:** Click **Edit** and upload a SSH public key file or enter the SSH public key value used for Oracle Internet of Things Cloud Service authentication.



Note:

Do not select **Create a New Key** to auto-generate a SSH public/private key pair. The auto-generated key pair is 2048 bits and cannot be used for Oracle Internet of Things Cloud Service authentication. To manually create a SSH public/private key pair, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#). When creating the SSH public/private key pair, do not use a passphrase.

6. Complete these fields in the **Backup and Recovery Configuration** area:
- **Cloud Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackup.
 - **Cloud Storage Username:** Enter the user name you used to sign in to Oracle Cloud in step 1.
 - **Cloud Storage Password:** Enter the password you used to sign in to Oracle Cloud in step 1.
7. Complete these fields in the **Content Storage Container** area:
- **Content Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackupcontainer.
 - **Use same credentials as Cloud Storage Container:** Select **true** to use the credentials you specified in step 6 to access content storage, or select **false** to provide different access credentials.

- **Content Storage Username:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter a user name for Cloud Storage Container access.
 - **Content Storage Password:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter the password used to access the Cloud Storage Container.
8. Complete these fields in the **Oracle IoT Fleet Monitoring Cloud Service** area:
- **Enter private key:** Paste the private key that matches the public key you uploaded in the **Service Details** area.
 - **PSM URL:** Accept the default value.
 - **MyServices Username:** Enter the user name used to access the Oracle Platform as a Service Service Manager.
 - **MyServices Password:** Enter the password used to access the Oracle Platform as a Service Service Manager.
 - **Create spare JCS instance:** Select **true** to create an additional Oracle Java Cloud Service instance, or select **false** if you do not want to create an additional Oracle Java Cloud Service instance.
 - **Enable IoT Device Simulator:** Select **true** to create an Oracle Internet of Things Cloud Service device simulator, or select **false** if you do not want to create an Oracle Internet of Things Cloud Service device simulator. A device simulator can help you test communications between devices and your Oracle Internet of Things Cloud Service instance.
9. Click **Next**.
10. Click **Confirm**.

It can take 30 minutes or longer to activate the Oracle Internet of Things Cloud Service instance.

Creating an Oracle IoT Connected Worker Cloud Service Instance

If you have subscribed to Oracle IoT Connected Worker Cloud Service, use this procedure to create the application.

Note:

When using Oracle Cloud Stack Manager to create Oracle cloud service instances, the cloud service instances cannot be used individually. For example, if Oracle Cloud Stack Manager is used to create the Database Cloud Service, Oracle Java Cloud Service, and Oracle Internet of Things Cloud Service instances, you cannot associate a standalone Oracle Internet of Things Cloud Service instance with a Oracle Java Cloud Service instance created with Oracle Cloud Stack Manager.

1. Sign in to Oracle Cloud:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.

- b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.
 - c. Copy the user name displayed in the **Username** field and then paste it into the **User Name** field.
 - d. Copy the password displayed in the **Temporary Password** field and then paste it into the **Password** field.
 - e. Click **Sign In**.
 - f. If this is your first time accessing Oracle Cloud, create a new password and provide challenge questions to verify your access credentials. Click **Submit** after you create your password and provide your challenge questions.
 - g. Click **Continue** if a welcome dialog appears.
2. Locate and copy the Oracle Storage Cloud Service REST endpoint URL. This URL forms part of the name for the Cloud Storage Container and Content Storage Container fields that you complete later in this procedure.
 - a. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Storage** below **Monitoring Metrics**.
 - b. Click **Overview** in the left pane.
 - c. Copy the URL displayed in the **REST Endpoint (Permanent)** field and paste it into a text editor or word processing application.
3. Click the **Menu** (≡) icon next to Oracle CLOUD My services, and then click **Oracle Cloud Stack**.
4. Complete these fields in the **Stack Details** area:
 - **Name:** Enter a unique name for the Oracle IoT Fleet Monitoring Cloud Service instance.
 - **Description:** (Optional) Enter a description for the Oracle IoT Fleet Monitoring Cloud Service instance.
 - **Template:** Select **Oracle-IOTConnectedWrker-Analytics-Template**.
 - **On Failure Retain Resources:** Select this option to retain the settings for the stack in case of failure.
5. Complete these fields in the **Service Details** area:
 - **Installation Type:** Select **Production** to create a production instance, or select **Development** to create a development instance.
 - **Number of Named Users:** Enter **1** if you selected a development installation, or enter a value greater than one or accept the default value if you selected a production installation.
 - **Username for Cloud Services:** Accept the default value.
 - **Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **Confirm Password (to access all services in Stack):** Enter the password used to access the Database Cloud Service instance.
 - **SSH Public Key:** Click **Edit** and upload a SSH public key file or enter the SSH public key value used for Oracle Internet of Things Cloud Service authentication.

 Note:

Do not select **Create a New Key** to auto-generate a SSH public/private key pair. The auto-generated key pair is 2048 bits and cannot be used for Oracle Internet of Things Cloud Service authentication. To manually create a SSH public/private key pair, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#). When creating the SSH public/private key pair, do not use a passphrase.

6. Complete these fields in the **Backup and Recovery Configuration** area:
 - **Cloud Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackup.
 - **Cloud Storage Username:** Enter the user name you used to sign in to Oracle Cloud in step 1.
 - **Cloud Storage Password:** Enter the password you used to sign in to Oracle Cloud in step 1.
7. Complete these fields in the **Content Storage Container** area:
 - **Content Storage Container:** Enter the REST endpoint URL you copied in step 2 and append it with a storage container name. For example, <REST endpoint URL>/mybackupcontainer.
 - **Use same credentials as Cloud Storage Container:** Select **true** to use the credentials you specified in step 6 to access content storage, or select **false** to provide different access credentials.
 - **Content Storage Username:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter a user name for Cloud Storage Container access.
 - **Content Storage Password:** (Optional) If you selected **false** in the **Use same credentials as Cloud Storage Container** field, enter the password used to access the Cloud Storage Container.
8. Complete these fields in the **Oracle IoT Connected Worker Cloud Service** area:
 - **Enter private key:** Paste the private key that matches the public key you uploaded in the **Service Details** area.
 - **PSM URL:** Accept the default value.
 - **MyServices Username:** Enter the user name used to access the Oracle Platform as a Service Service Manager.
 - **MyServices Password:** Enter the password used to access the Oracle Platform as a Service Service Manager.
 - **Create spare JCS instance:** Select **true** to create an additional Oracle Java Cloud Service instance, or select **false** if you do not want to create an additional Oracle Java Cloud Service instance.
 - **Enable IoT Device Simulator:** Select **true** to create an Oracle Internet of Things Cloud Service device simulator, or select **false** if you do not want to create an Oracle Internet of Things Cloud Service device simulator. A device simulator can help you test communications between devices and your Oracle Internet of Things Cloud Service instance.

9. Click **Next**.

10. Click **Confirm**.

It can take 30 minutes or longer to activate the Oracle Internet of Things Cloud Service instance.

3

Managing Users

Add user accounts to assign access privileges to your Oracle Internet of Things Cloud Service instance. Remove a user account when it is no longer required.

Topics

- [Adding a User Account](#)
- [Editing a User Account](#)
- [Removing a User Account](#)

Adding a User Account

Add a user account to assign a user Oracle Internet of Things Cloud Service access privileges.

1. Log in to the Oracle WebLogic Server instance associated with your Oracle Internet of Things Cloud Service instance.
2. Click **Security Realms** in the **Domain Structure** pane.
3. Click **myrealm** in the **Realms** list in the right pane.
4. Click the **Users and Groups** tab at the top of the right pane.
5. Click **New** at the top of the **Users** list and then complete these fields:
 - **Name:** Enter a name for the user account. Do not add tabs or these characters: semicolon (;), comma (,), plus sign (+), equal sign (=), single backslash (\), apostrophe ('), double quote ("). Do not precede the name with a pound (#) or double quote (").
 - **Description:** (Optional) Enter a description for the user account.
 - **Provider:** Select **DefaultAuthenticator**.
 - **Password:** Enter a password for the user account.
 - **Confirm Password:** Re-enter the user password.
6. Click **OK**.
7. Click the user name you entered in step 5 in the **Users** list.
8. Click the **Groups** tab.
9. Select one or more of these options in the **Available** list:
 - **lotAdministratorsGroup:** Select this option to assign administrator privileges to the user group.
 - **lotOperatorsGroup:** Select this option to assign operator privileges to the user account.
 - **lotUsersGroup:** Select this option to assign user privileges to the user account.

10. Click the **Move** (➤) icon.
11. Click **Save**.

Editing a User Account

Edit a user account to add or change the account description, change the account password, or add or remove access or privileges.

1. Log in to the Oracle WebLogic Server instance associated with your Oracle Internet of Things Cloud Service instance.
2. Click **Security Realms** in the **Domain Structure** pane.
3. Click **myrealm** in the **Realms** list in the right pane.
4. Click the **Users and Groups** tab at the top of the right pane.
5. Click a user name in the **Name** column of the **Users** list.
6. (Optional) Edit or add a user account description:
 - a. Click the **General** tab.
 - b. Edit or add a user a description for the user account in the **Description** field.
 - c. Click **Save**.
7. (Optional) Change the user account password:
 - a. Click the **Passwords** tab.
 - b. Enter a new password in the **New Password** field.
 - c. Re-enter the password in the **Confirm New Password** field.
 - d. Click **Save**.
8. (Optional) Add or remove access privileges:
 - a. Click the **Groups** tab.
 - b. To add privileges, select **lotAdministratorsGroup**, **lotClientsGroup**, **lotDeviceManagersGroup**, **lotOperatorsGroup**, or **lotUsersGroup** in the **Available** list, click the **Move Right** (➤) icon, and then click **Save**.
 - c. To remove privileges, select a privilege in the **Chosen** list, click the **Move Left** (➤) icon, and then click **Save**.

Removing a User Account

Remove a user when you no longer want them to have Oracle Internet of Things Cloud Service access or privileges.

1. Log in to the Oracle WebLogic Server instance associated with your Oracle Internet of Things Cloud Service instance.
2. Click **Security Realms** in the **Domain Structure** pane.
3. Click **myrealm** in the **Realms** list in the right pane.
4. Click the **Users and Groups** tab at the top of the right pane.

5. Select the check box next to the user you want to remove in the **Users** list.
6. Click **Delete**.
7. Click **Yes**.

4

Troubleshooting Oracle Internet of Things Cloud Service

Review the following topics to resolve issues with Oracle Internet of Things Cloud Service.

Topics:

- [RSA Key Size Should be 1024 Bits](#)
- [Unable to Delete Oracle Internet of Things Cloud Service Instance](#)
- [Unable to Receive Data when Using an Apache Spark Cluster and the Kafka Handler](#)
- [How to Get Support](#)

RSA Key Size Should be 1024 Bits

The error message RSA key size should be 1024 bits appears when the SSH key length exceeds 1024 bits. This error message typically appears when entering the private key for the Oracle Java Cloud Service instance on the Oracle Internet of Things Cloud Service Service Details page. This issue can be caused when an auto-generated key pair is used for authentication. The auto-generated key pair is 2048 bits and cannot be used for Oracle Internet of Things Cloud Service authentication.

To manually create a 1024 bit SSH public/private key pair, see [Using the ssh-keygen Utility to Generate an SSH Key Pair](#) or [Using the PuTTYgen Program to Generate an SSH Key Pair](#).

Unable to Delete Oracle Internet of Things Cloud Service Instance

When you attempt to delete an Oracle Internet of Things Cloud Service instance, the instance is not deleted and the error message Last Activity DELETE_SERVICE <date and time> failed. See Activity Log for Details appears in Oracle Cloud Service. The cause of this issue is the removal of the `installiot` folder in Oracle Java Cloud Service.

To resolve this issue, reinstall the `installiot` folder and then delete the Oracle Internet of Things Cloud Service instance again.

1. Log in to Oracle Cloud Service:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.
 - b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.

- c. Enter your user name and password.
- d. Click **Sign In**.
2. Click the **Menu** (≡) icon, and then click Oracle Java Cloud Service.
3. Click the Oracle Java Cloud Service instance associated with the Oracle Internet of Things Cloud Service instance.
4. Record the host name and IP address for the Oracle Java Cloud Service instance.
5. On UNIX and UNIX-like platforms, use the standard OpenSSH command (ssh) to connect to the Oracle Java Cloud Service instance as the opc user.

Provide the following:

- The path to the private key corresponding to the public key used at the time of provisioning.
- The Administration Server public IP address.
- The Managed Server host name.

in this format:

```
ssh -i path_to_private_key -o ProxyCommand="ssh -W %h:%p -i path_to_private_key
opc@admin_server_IP_address" opc@managed_server_host_name
```

For example:

```
ssh -i /home/myuser/id_rsa -o ProxyCommand="ssh -W %h:%p -i /home/myuser/id_rsa
opc@111.111.111.111" opc@myjcs-wls-2
```

6. On Windows, use PuTTY or a similar SSH client, to connect to the Oracle Java Cloud Service instance as the opc user:

To download PuTTY, go to <http://www.putty.org/> and click the **You can download PuTTY here** link.

- a. Launch PuTTY. If your private key was defined with a passphrase, then you must use the pageant utility to launch PuTTY:

```
pageant "path to private key" -c "path to putty"
```

For example:

```
c:\PuTTY\pageant "c:\oracle\rsa.ppk" -c "c:\PuTTY\putty"
```

- b. If you used pageant to start PuTTY, enter the passphrase for the private key.
- c. In the **Host Name (or IP address)** field, enter the host name of the Managed Server.
- d. Expand **Connection** in the **Category** pane and then click **Data**.
- e. Enter **opc** in the **Auto-login username** field.
- f. Select **Prompt** in the **When username is not specified** field.
- g. Click **Proxy** below **Connection** in the **Category** pane.
- h. Select **Local** in the **Proxy type** area.
- i. Enter the IP address of the Administration Server in the **Proxy hostname** field.
- j. Enter **22** in the **Port** field.
- k. Enter this value in the **Telnet command or local proxy command** field :

```
plink -i "path to private key" opc@%proxyhost -nc %host:%port
```

For example:

```
plink -i "c:\\oracle\\rsa.ppk" opc@%proxyhost -nc %host:%port
```

- l.** Expand **SSH** below **Connection** in the **Category** pane and then click **Auth**.
- m.** Click **Browse** in the **Private key file for authentication** field.
- n.** Browse to the location of your private key file, select it, and then click **Open**.

 Note:

The .ppk file extension indicates that the private key is in PuTTY's proprietary format. You must use a key of this format when using PuTTY. If you have to use a key saved in a different format, see the PuTTY documentation.

- o.** Click **Open** to open the connection to the Oracle Java Cloud Service instance.

 Note:

You can optionally save this session configuration by navigating to the Session panel and clicking **Save**. When you open PuTTY the next time, you can load this configuration by selecting it and clicking **Load**.

- 7.** Open a command prompt and run this command to copy the private key on the host computer: - vi id_rsa.
- 8.** Run this command to paste the content of the private key to the host computer: - chmod 400 id_rsa.
- 9.** Run this command: ssh -i id_rsa opc@<IoT OEP host>.
- 10.** Run this command: sudo cd /u01/app/oracle/tools/ieas/OEP/vm-scripts/.
- 11.** Run this command: vi setup/iot-setup.sh.
- 12.** Add this comment: // \$JAVA_HOME/bin/java \$@
weblogic.WLST \$CONFIGURE_DEPLOY_PY \$DEPLOY_MODE \$iota_enable \$DOMAIN_HOME
sh ./installiot.sh.
- 13.** Delete the Oracle Internet of Things Cloud Service instance:
 - a.** Repeat step 1 to log in to Oracle Cloud Service.
 - b.** Click the **Menu** (≡) icon, and then click Oracle Internet of Things Cloud Service.
 - c.** Click **Delete**.

Unable to Receive Data when Using an Apache Spark Cluster and the Kafka Handler

If you are using an Apache Spark Cluster and the Kafka handler, data cannot be sent to an Oracle Internet of Things Cloud Service instance with analytics enabled.

To resolve this issue, create a custom Oracle Event Hub Cloud Service access rule.

1. Log in to Oracle Cloud Service:
 - a. Open the subscription notification email sent by Oracle. Typically, this email includes the subject line **Welcome to Oracle Cloud**.
 - b. Right-click the URL displayed in the **My Services URL** field and select **Open in new tab**.
 - c. Enter your user name and password.
 - d. Click **Sign In**.
2. Click the **Menu** (☰) icon, and then click Oracle Event Hub Cloud Service.
3. Select the Kafka instance to which you want to add the access rule.
4. Click the **Menu** (☰) icon and then select **Access Rules**.
5. Click **Create Rule**.
6. Complete these fields:
 - **Rule Name**: Enter a name for the access rule.
 - **Description**: (Optional) Enter a description for the access rule.
 - **Source**: Enter PUBLIC-INTERNET.
 - **Destination**: Enter kafka_KAFKA_SERVER
 - **Destination Port(s)**: Enter 6667
 - **Protocol**: Enter TCP.
7. Click **Create**.
8. Confirm the access rule appears in the **Access Rules** list. If it does not, repeat steps 5 to 7.

How to Get Support

Use these resources to resolve problems:

- Review [Troubleshooting Oracle Internet of Things Cloud Service](#).
- Click the **Contact Us** (☎) icon in the Oracle My Services management console and then select a support option.
- Visit the Oracle Help Center at <http://docs.oracle.com/en/>.
- If you're an Oracle Premier Support Customer, then visit [My Oracle Support](#).
- Contact Oracle Technical Support. See Contacting Oracle Support in *Getting Started with Oracle Cloud*.