InterConnect
2017

March 19–23
MGM Grand &
Mandalay Bay
Las Vegas, NV

IBM

Hands-on Lab
Session 2334

Watson IoT Platform Risk and Security Management

Mats Göthe
Senior Design Lead
IBM Watson IoT Platform Design

Cynthia Zhang
User Experience Designer
IBM Watson IoT Platform Design

This document is current as of the initial date of publication and may be changed by IBM at any time.

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.

Table of Contents

Introduction to this lab

The IBM Watson Internet of Things platform delivers advanced Risk and Security Management to enhance IBM Watson IoT Platform security by creating, enforcing, and reporting on device connection security.

Risk and Security Management adds support for certificates, TLS authentication, policies and a security dashboard for compliance reporting. Using the Risk and Security Management capabilities your organization will be able to perform the following actions:

1. Configure the platform to enable devices authenticating with certificates.
2. Import and activate either a new server certificate or generate a Certificate Signing Request (CSR) for messaging.
3. Configure the policy to specify the security level for device connection
4. Block access from specific IP addresses and/or countries by enforcing Blacklist or Whitelist policy.
5. Visualize critical IoT risks and security compliance through a security dashboard

The Risk and Security Management is included with parts in the Free Plan for fully available in the Advanced Security Plan.

In this lab you will be exploring hands-on the advanced Risk and Security Management features above in the IBM Watson IoT Platform.

Starting your Workstation

In this lab you will use an Ubuntu v14 virtual image as your Linux workstation. This workstation is only used in this lab to run your Firefox Web browser. All access to IBM Bluemix and IBM Watson Internet of Things Platform will be made using the Firefox Web browser.

At the start of this lab, all workstations should have been started and ready for you to use. If the workstation is locked, login as:

Username: “localuser”
Password: “passw0rd” – **Note the zero**

If you fail to log into your workstation, ask your lab facilitators for help.

Logging into Bluemix and Watson IoT Platform

IBM Bluemix is a cloud platform as a service (PaaS) developed by IBM. It supports several programming languages and services as well as integrated DevOps to build, run, deploy and manage applications on the cloud. Bluemix is based on Cloud Foundry open technology and runs on SoftLayer infrastructure.

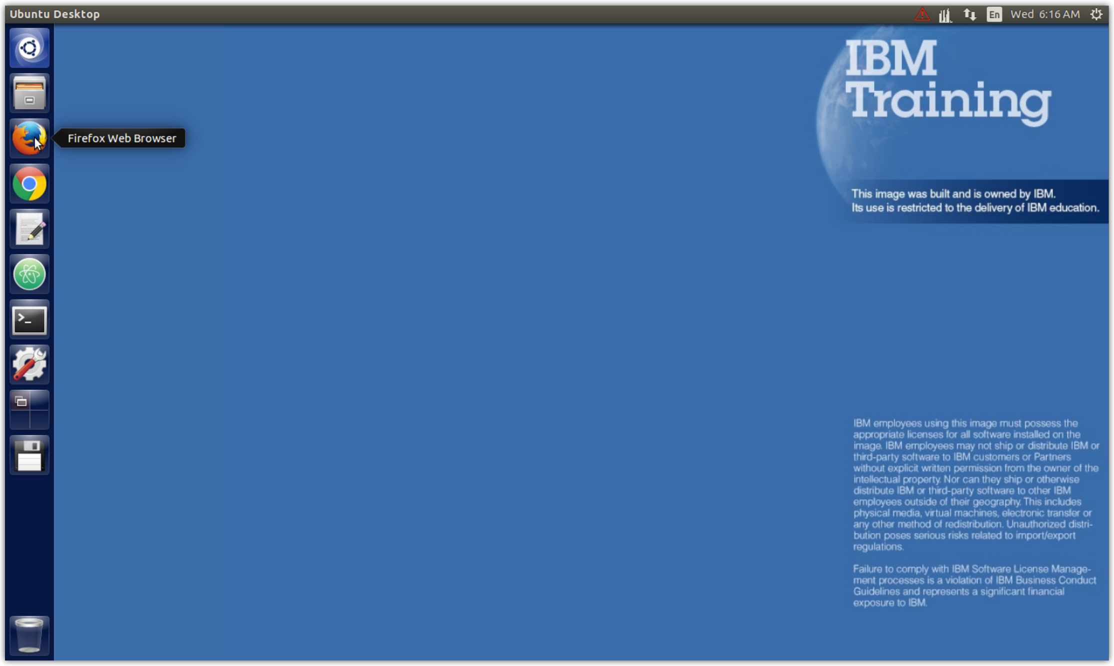
The IBM Watson Internet of Things Platform is a fully managed, cloud-hosted service available in IBM Bluemix, that makes it simple to derive value from Internet of Things (IoT) devices.

Devices can get connected and start sending data securely to the IBM Watson Internet of Things Platform cloud service using the open, lightweight MQTT messaging protocol. From there, you can setup and manage your devices using your online dashboard or our secure APIs, so that your apps can access live and historical data fast. With your devices connected to the IoT platform are now ready to start creating applications using your device data.

In this lab you will use the IBM Watson Internet of Things Platform service available in IBM Bluemix. To get access to the IoT platform you first have to log into IBM Bluemix and then browse to the IBM Watson Internet of Things Platform service.

Follow the steps below to log into IBM Bluemix and browse the Internet of Things Platform service.

1. Open the Firefox browser

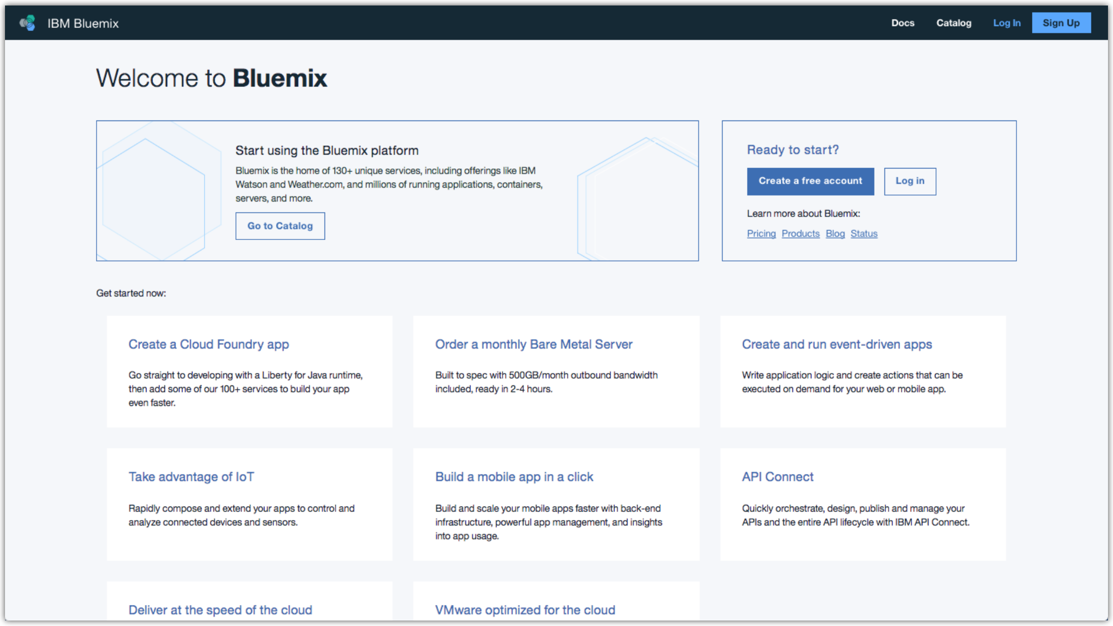


This image was built and is owned by IBM.
Its use is restricted to the delivery of IBM education.

IBM employees using this image must possess the appropriate licenses for all software installed on the image. IBM employees may not ship or distribute IBM or third-party software to IBM customers or Partners without explicit written permission from the owner of the intellectual property. Nor can they ship or otherwise distribute IBM or third-party software to other IBM employees outside of their geography. This includes physical media, virtual machines, electronic transfer or any other method of redistribution. Unauthorized distribution poses serious risks related to import/export regulations.

Failure to comply with IBM Software License Management processes is a violation of IBM Business Conduct Guidelines and represents a significant financial exposure to IBM.

2. Enter https://bluemix.net
   The Bluemix welcome page opens



Welcome to **Bluemix**

Start using the Bluemix platform

Bluemix is the home of 130+ unique services, including offerings like IBM Watson and Weather.com, and millions of running applications, containers, servers, and more.

Ready to start?

Learn more about Bluemix:

Get started now:

Create a Cloud Foundry app

Go straight to developing with a Liberty for Java runtime, then add some of our 100+ services to build your app even faster.

Order a monthly Bare Metal Server

Built to spec with 500GB/month outbound bandwidth included, ready in 2-4 hours.

Create and run event-driven apps

Write application logic and create actions that can be executed on demand for your web or mobile app.

Take advantage of IoT

Rapidly compose and extend your apps to control and analyze connected devices and sensors.

Build a mobile app in a click

Build and scale your mobile apps faster with back-end infrastructure, powerful app management, and insights into app usage.

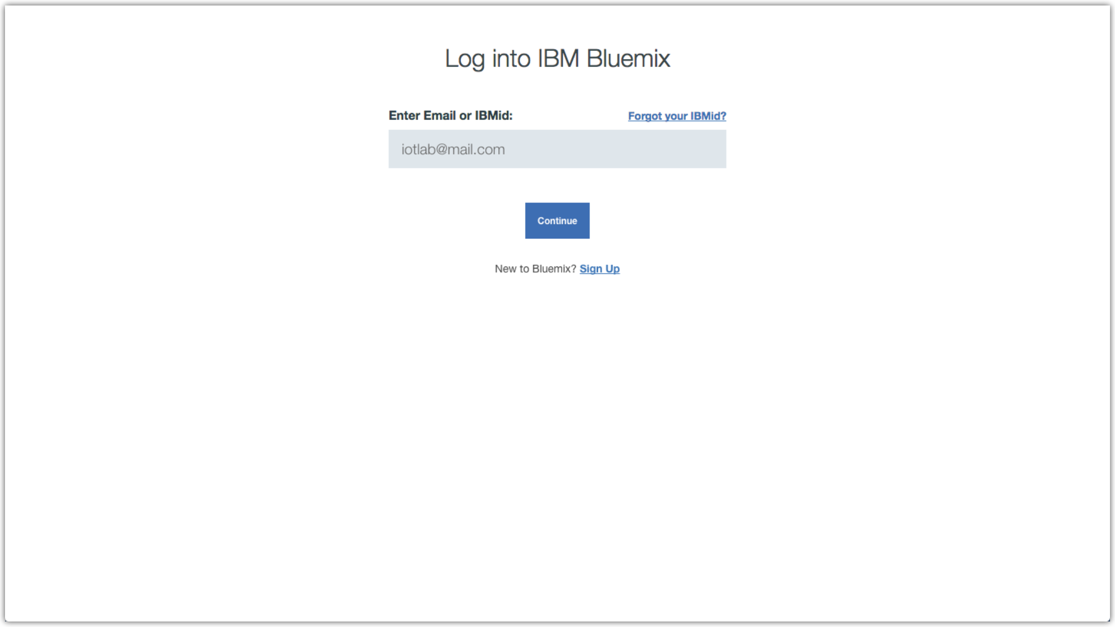
API Connect

Quickly orchestrate, design, publish and manage your APIs and the entire API lifecycle with IBM API Connect.

Deliver at the speed of the cloud

VMware optimized for the cloud

3. Click on **Login**
4. Enter the IBM ID “iotlab@mail.com”

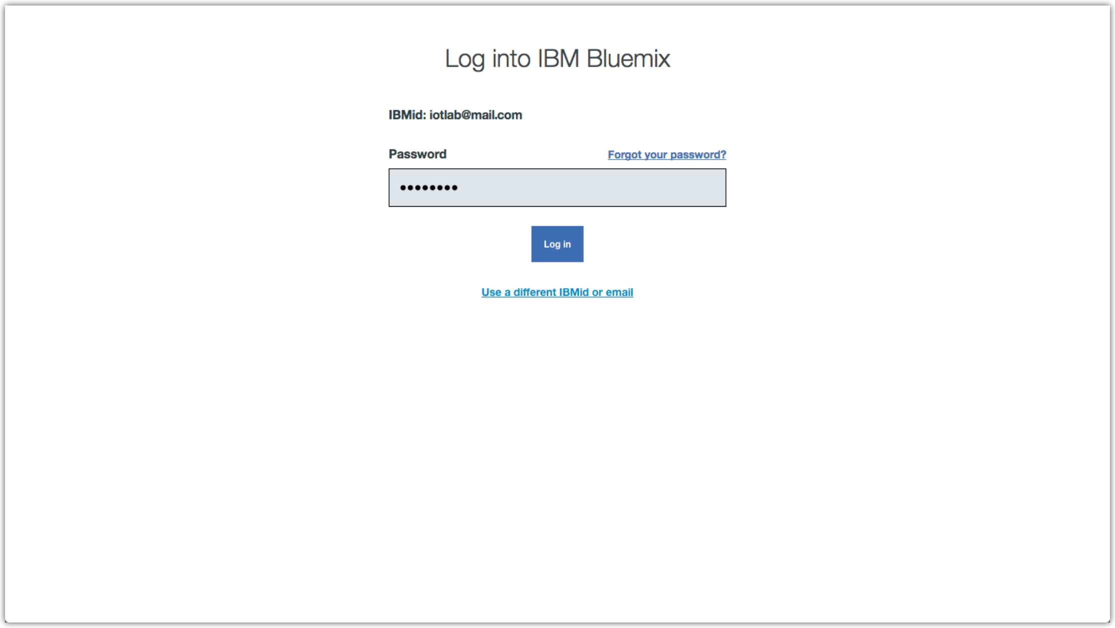


Log into IBM Bluemix

Enter Email or IBMid: iotlab@mail.com

New to Bluemix? Sign Up

5. Enter the password “Interconnect2017!”

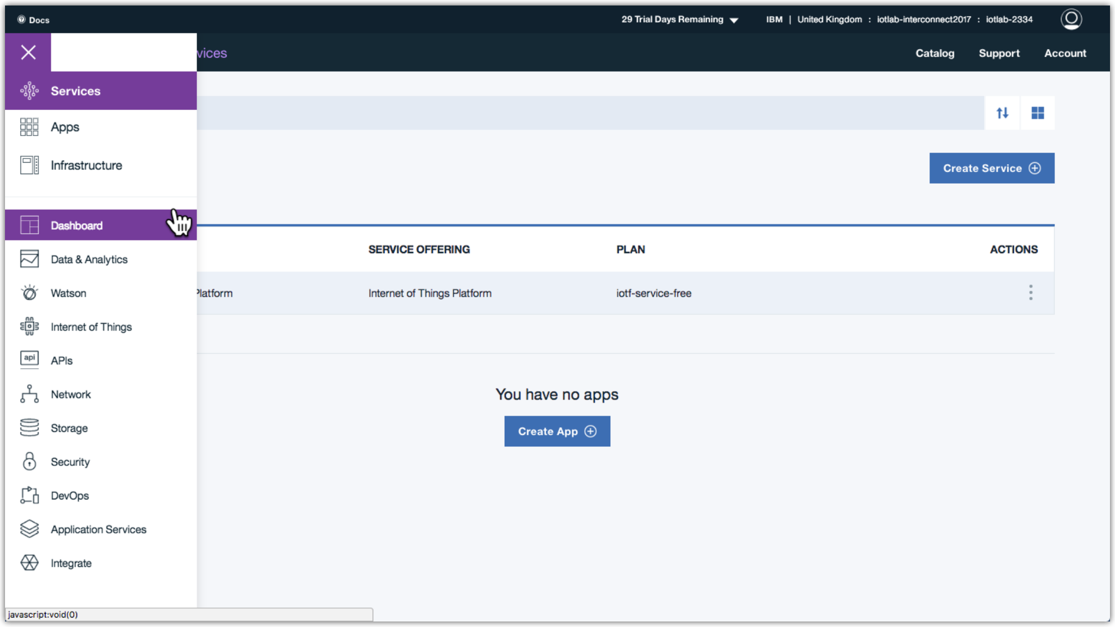


Log into IBM Bluemix

IBMid: iotlab@mail.com

Password: ••••••••

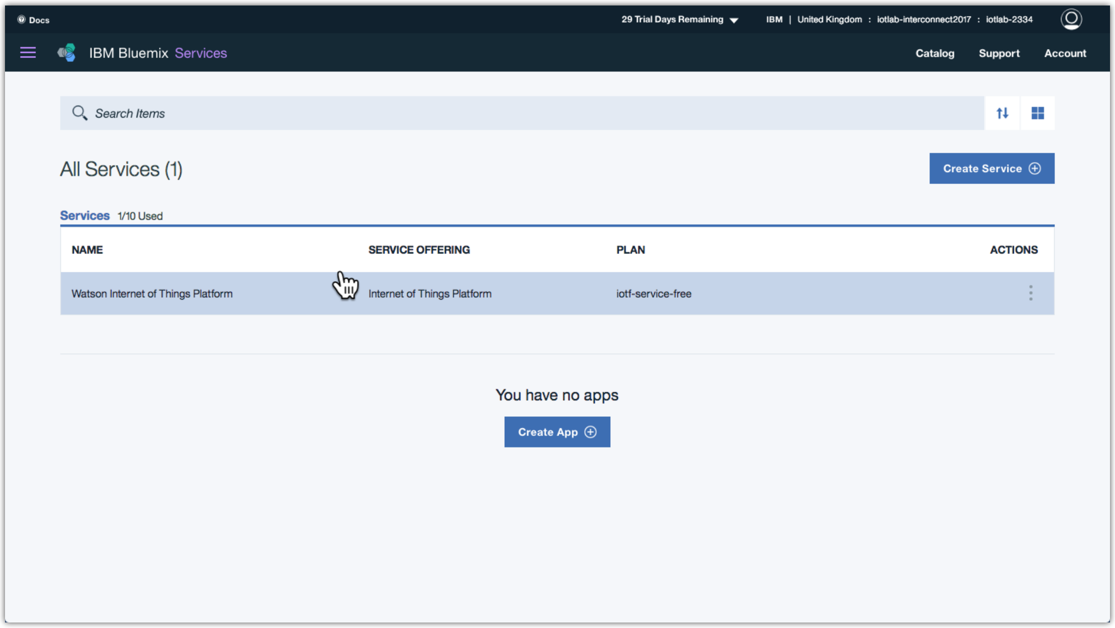
6. The IBM Bluemix Dashboard is loaded.
   From the menu bar, choose **Services** and **Dashboard**.



	SERVICE OFFERING	PLAN	ACTIONS
Platform	Internet of Things Platform	iotf-service-free	⋮

You have no apps

7. In the list of Services, choose the **Watson Internet of Things Platform** service.
   The Watson Internet of Things Platform service opens.



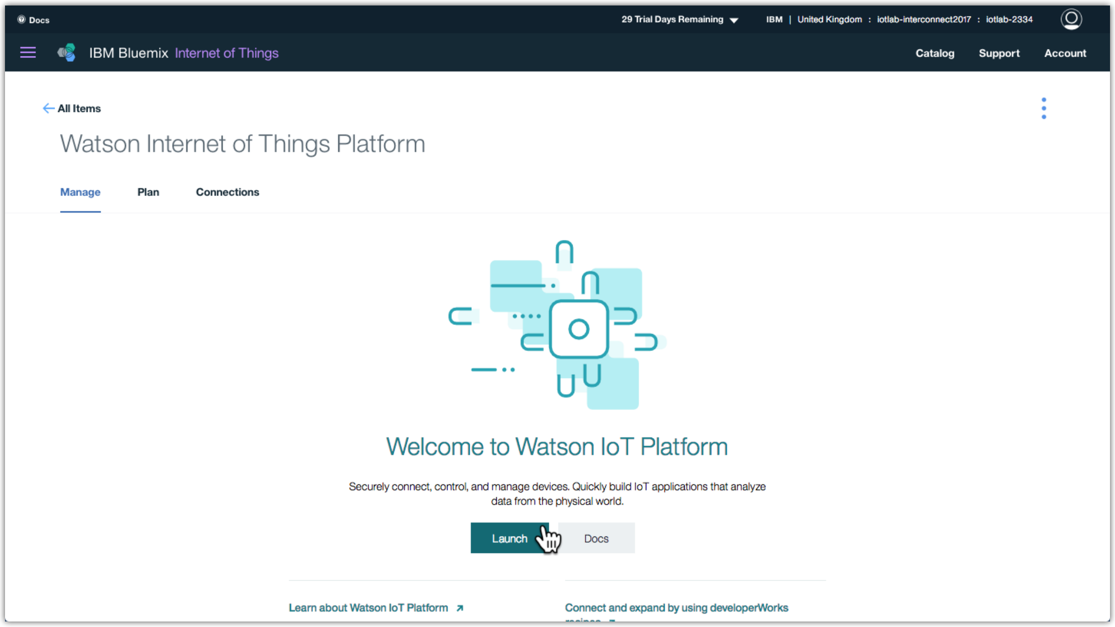
All Services (1)

Services 1/10 Used

NAME	SERVICE OFFERING	PLAN	ACTIONS
Watson Internet of Things Platform	Internet of Things Platform	iotf-service-free	⋮

You have no apps

8. Click **Launch** to open the IoT platform web interface.

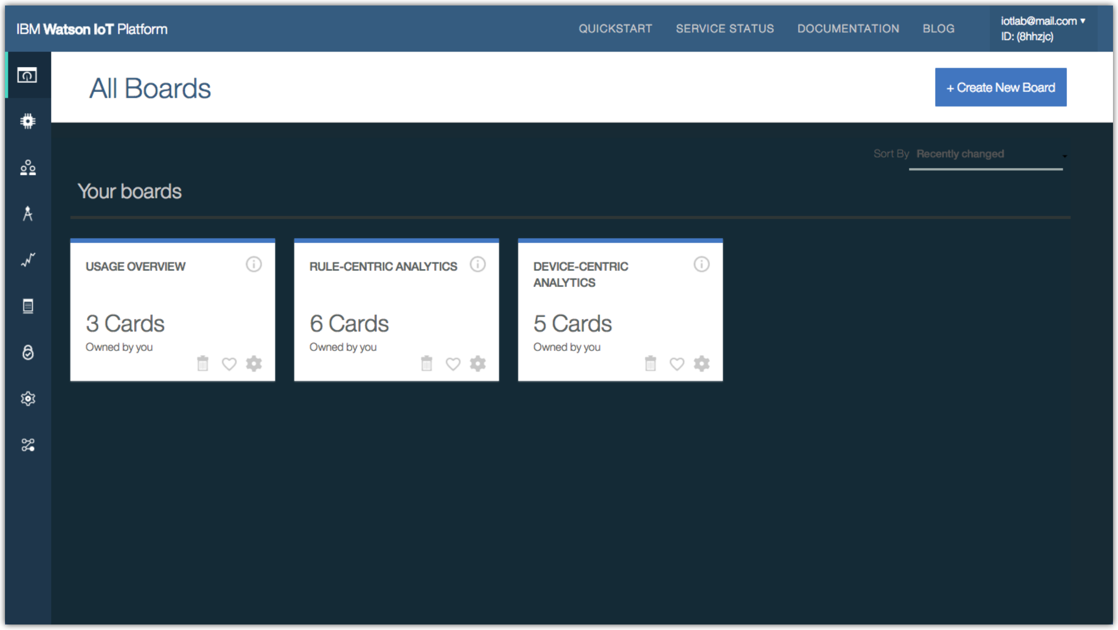

Docs
29 Trial Days Remaining
IBM | United Kingdom : iotlab-interconnect2017 : iotlab-2334
IBM Bluemix Internet of Things
Catalog
Support
Account
All Items
Manage
Plan
Connections
Launch
Docs
Learn about Watson IoT Platform
Connect and expand by using developerWorks

Watson Internet of Things Platform

Welcome to Watson IoT Platform

Securely connect, control, and manage devices. Quickly build IoT applications that analyze data from the physical world.

9. The Watson IoT Platform opens and shows the platform dashboard.



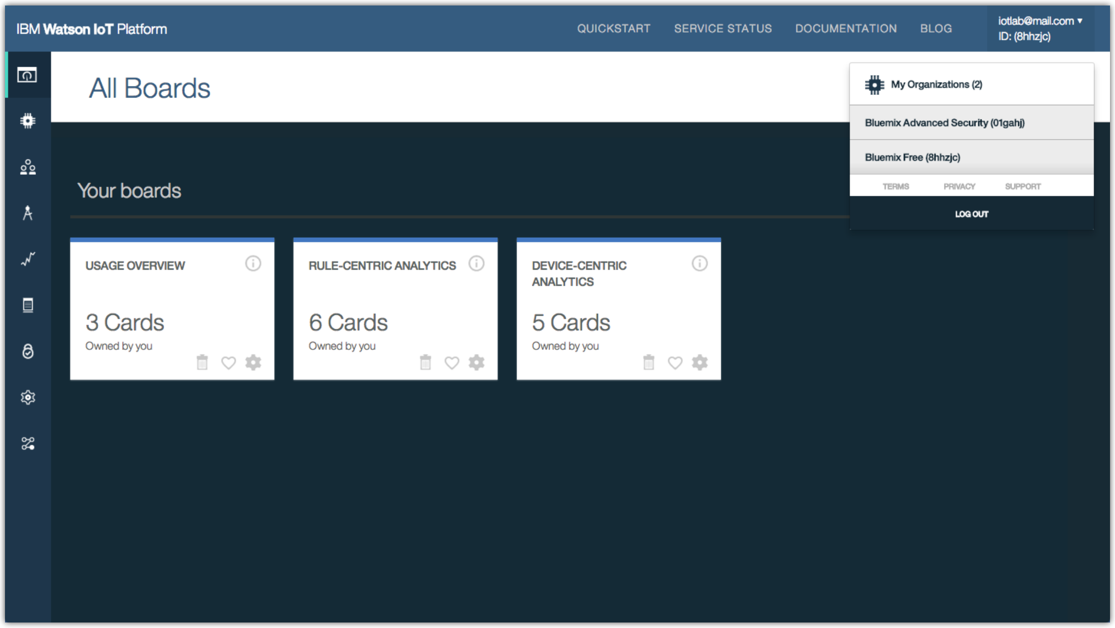
You have now successfully logged into IBM Bluemix and opened the IBM Watson IoT Platform service. You are now ready to switch to the IoT platform *organization* that you will use in this lab.

When you register with the Watson IoT Platform, you are given an organization ID. Your organization ID is a unique six-character identifier for your account. Organizations ensure that your data is organized and accessible by your devices and applications. An IoT platform organization is hence a workspace that independently of other organizations manages users, devices and device data.

For this lab we have registered and created one organization for each workstation. You will use an individually assigned IoT platform organization. By selecting your assigned organization, you will work in your own workspace and not make conflicting changes to other workstations.

Note: Look for the organization id that has been assigned to your workstation. Or ask one of the lab facilitators.

10. Click on the organization menu in the upper right hand corner of the application. In the list, choose the organization id that has been assigned to your workstation for this lab.



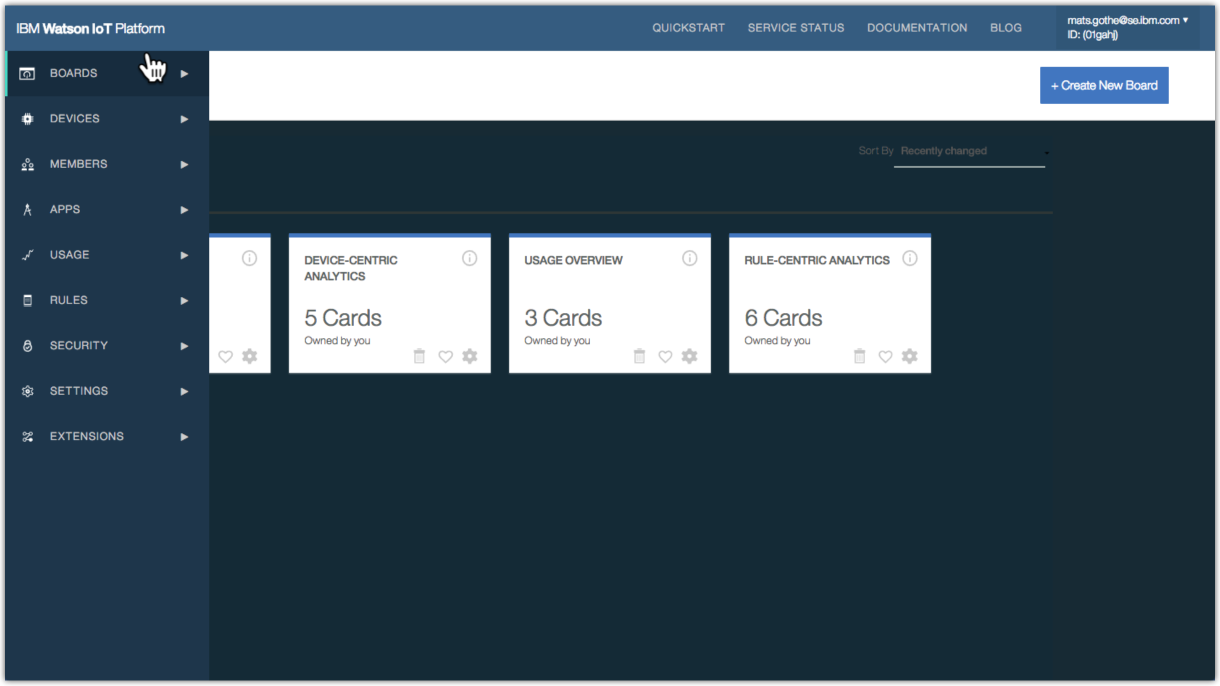
IBM Watson IoT Platform
QUICKSTART
SERVICE STATUS
DOCUMENTATION
BLOG
iotlab@mail.com ▾
ID: (8hhzjc)
All Boards
Your boards
USAGE OVERVIEW
3 Cards
Owned by you
RULE-CENTRIC ANALYTICS
6 Cards
Owned by you
DEVICE-CENTRIC ANALYTICS
5 Cards
Owned by you
My Organizations (2)
Bluemix Advanced Security (01gahj)
Bluemix Free (8hhzjc)
TERMS
PRIVACY
SUPPORT
LOG OUT

Overview of the Watson IoT Platform

IBM Watson IoT Platform provides powerful application access to IoT devices and device data to help you rapidly compose analytics applications, visualization dashboards, and mobile IoT apps.

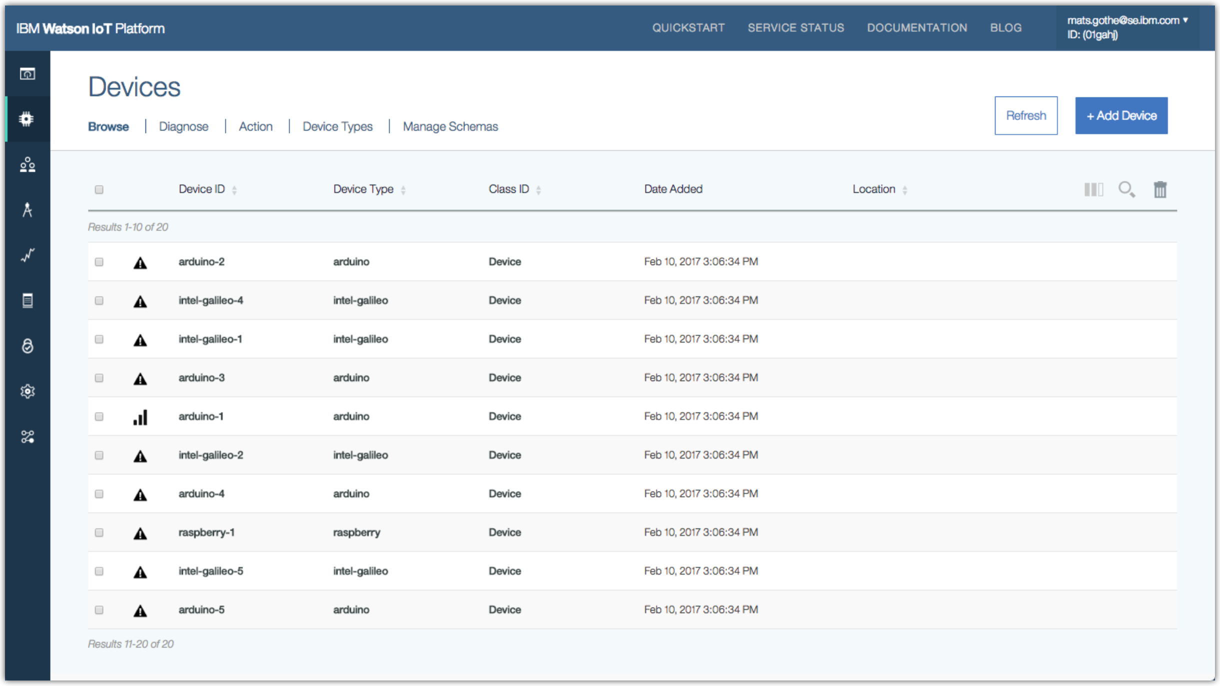
In this first section you will familiarize yourself with the IBM Watson IoT Platform user interface. The navigation bar on the left hand side provides access to the capabilities of the platform

- Boards – Opens the dashboard and shows the boards and cards
- Devices – Opens a browser for registered devices and their device types
- Members – User management
- Apps – API Key management
- Usage – Metrics of usage
- Rules – Analytics rules and actions
- Security – Risk and Security Policies. We will explore details later in this lab
- Settings – Administration settings. For example, client and server certificates.
- Extensions – Additional capabilities, optionally enabled



1. Move your mouse pointer to the left side navigation bar. The navigation menu slides out and shows the IoT platform capability sections.
2. From the navigation menu, choose **Devices**
   The Devices page opens. This view shows all devices registered in this organization.

Note: You can sort the list of devices, *e.g.* by Device ID and Device Type. Try it!

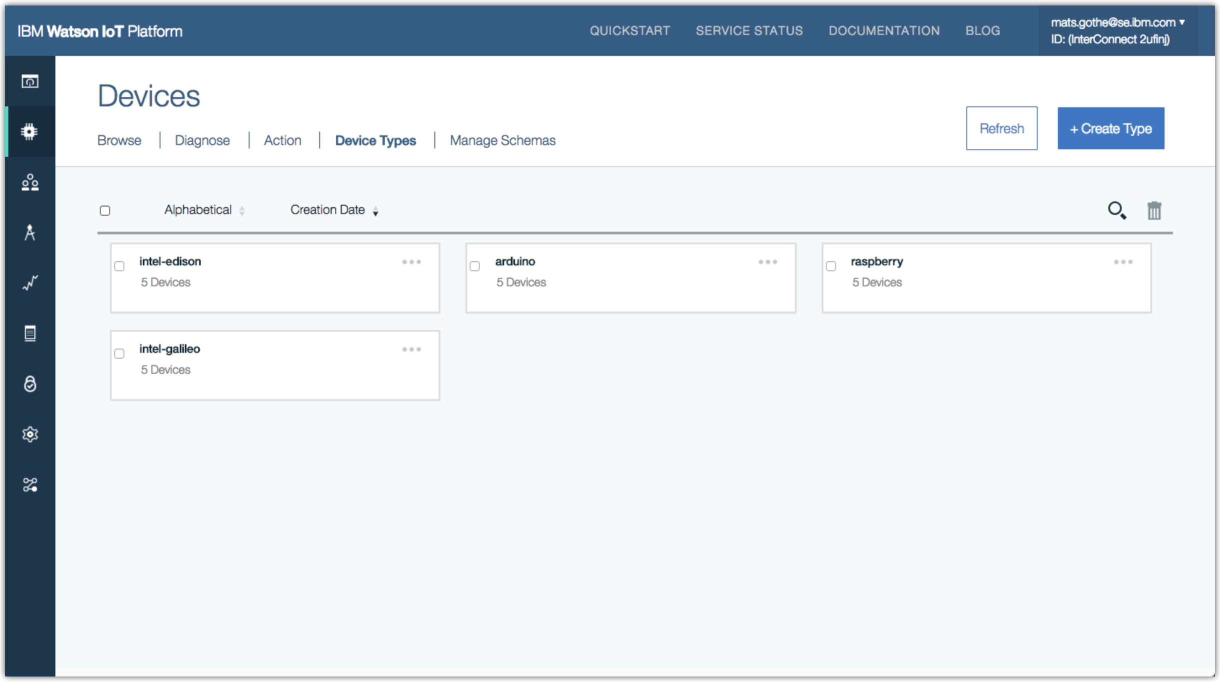


Results 1-10 of 20

□		Device ID	Device Type	Class ID	Date Added	Location
□	⚠	arduino-2	arduino	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	intel-galileo-4	intel-galileo	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	intel-galileo-1	intel-galileo	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	arduino-3	arduino	Device	Feb 10, 2017 3:06:34 PM	
□	▂▄▆	arduino-1	arduino	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	intel-galileo-2	intel-galileo	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	arduino-4	arduino	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	raspberry-1	raspberry	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	intel-galileo-5	intel-galileo	Device	Feb 10, 2017 3:06:34 PM	
□	⚠	arduino-5	arduino	Device	Feb 10, 2017 3:06:34 PM	

Results 11-20 of 20

3. From the section tabs on the page, choose **Device Types**
   The Device Types page opens. This page shows all device types registered in this organization.



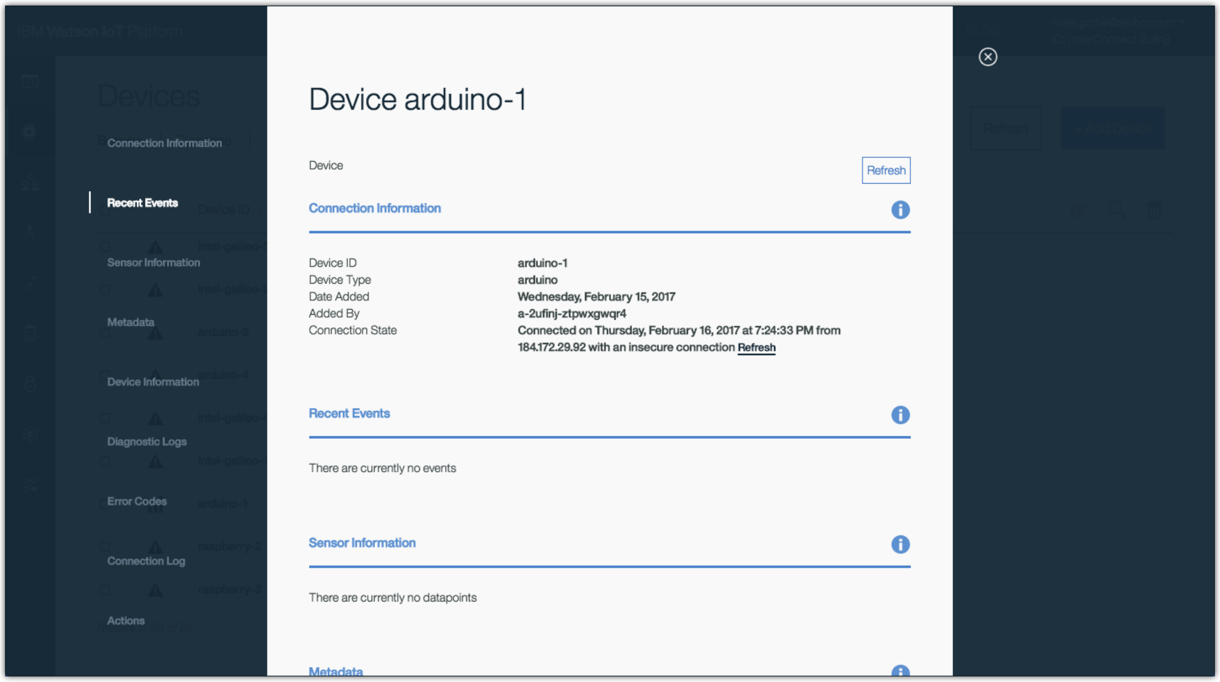
□ intel-edison
5 Devices

□ arduino
5 Devices

□ raspberry
5 Devices

□ intel-galileo
5 Devices

4. Return to the Devices page by clicking on **Browse**. Locate the device named “Arduino-1” in the list. Click on the device to open the Device Details page.



Device arduino-1

Device

Connection Information

Device ID	arduino-1
Device Type	arduino
Date Added	Wednesday, February 15, 2017
Added By	a-2ufinj-ztpwxgwqr4
Connection State	Connected on Thursday, February 16, 2017 at 7:24:33 PM from 184.172.29.92 with an insecure connection Refresh

Recent Events

There are currently no events

Sensor Information

There are currently no datapoints

Metadata

5. The IP address of the "Arduino-1" device is shown un the Connection Information section. Write down below the IP address the Arduino-1 device is connecting from. You will use this information later in this lab.

   The IP address to the Arduino-1 device is: ______________________________

6. Browse the other sections on the details page.

You have now explored the Devices and their Device Types currently registered in your IoT platform organization.

You will now proceed to the Risk and Security Management capability and explore connection policies, client and server certificates and reporting using the IoT platform dashboard.

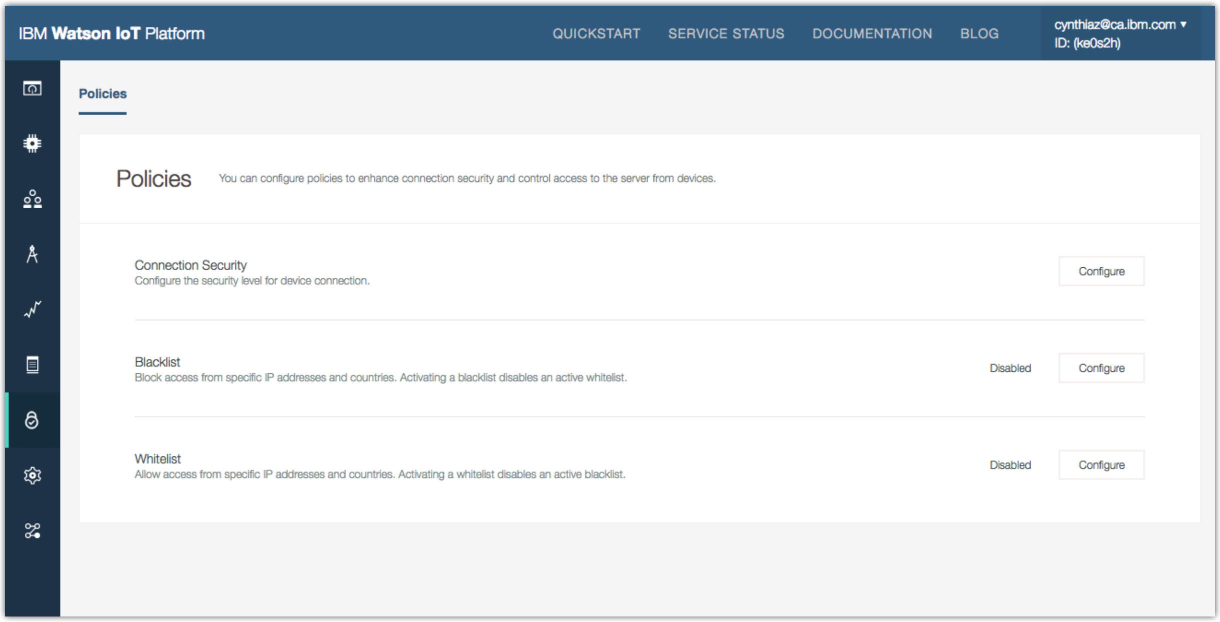
Configuring a Connection Security Policy

The Risk and Security Management capability enables organizations to enhance IoT platform security by creating, enforcing, and reporting on device connection security. Certificates and transport layer security (TLS) authentication are used, on top of the user IDs and tokens that are used by Watson IoT Platform to determine how and where devices connect with the platform.

The Connection Security policy enforces how devices connect to the platform. You can set up default connection policies for all device types, as well as custom settings for specific device types. The policy can be set to allow unencrypted connections, to enforce only transport layer security (TLS) connections, and to enable devices to authenticate with client-side certificates. When client-side certificates are being used, the security policy provides an additional option of using only the certificate for client authentication or using a combination of both a client certificate and client ID and authentication token pair.

Using the connection security policy, you can set the default security level of the required authentication method that is applied to all devices. You can then add custom security settings for specific devices.

1. From the left menu, select **Security** to navigate to the policies page



Policies

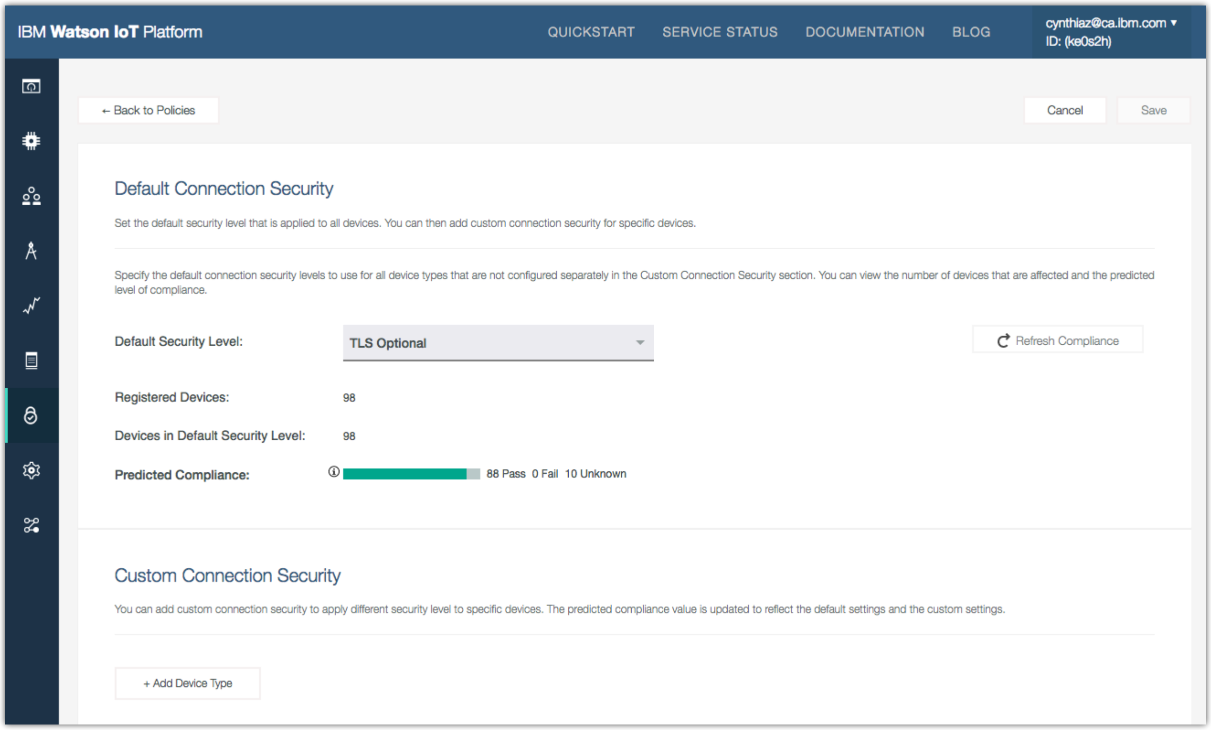
You can configure policies to enhance connection security and control access to the server from devices.

Connection Security
Configure the security level for device connection.

Blacklist
Block access from specific IP addresses and countries. Activating a blacklist disables an active whitelist.
Disabled

Whitelist
Allow access from specific IP addresses and countries. Activating a whitelist disables an active blacklist.
Disabled

2. Click **Configure** on **Connection Security** policy.
   The Connection Security Policy page loads.



Default Connection Security

Set the default security level that is applied to all devices. You can then add custom connection security for specific devices.

Specify the default connection security levels to use for all device types that are not configured separately in the Custom Connection Security section. You can view the number of devices that are affected and the predicted level of compliance.

Default Security Level: TLS Optional

Registered Devices: 98

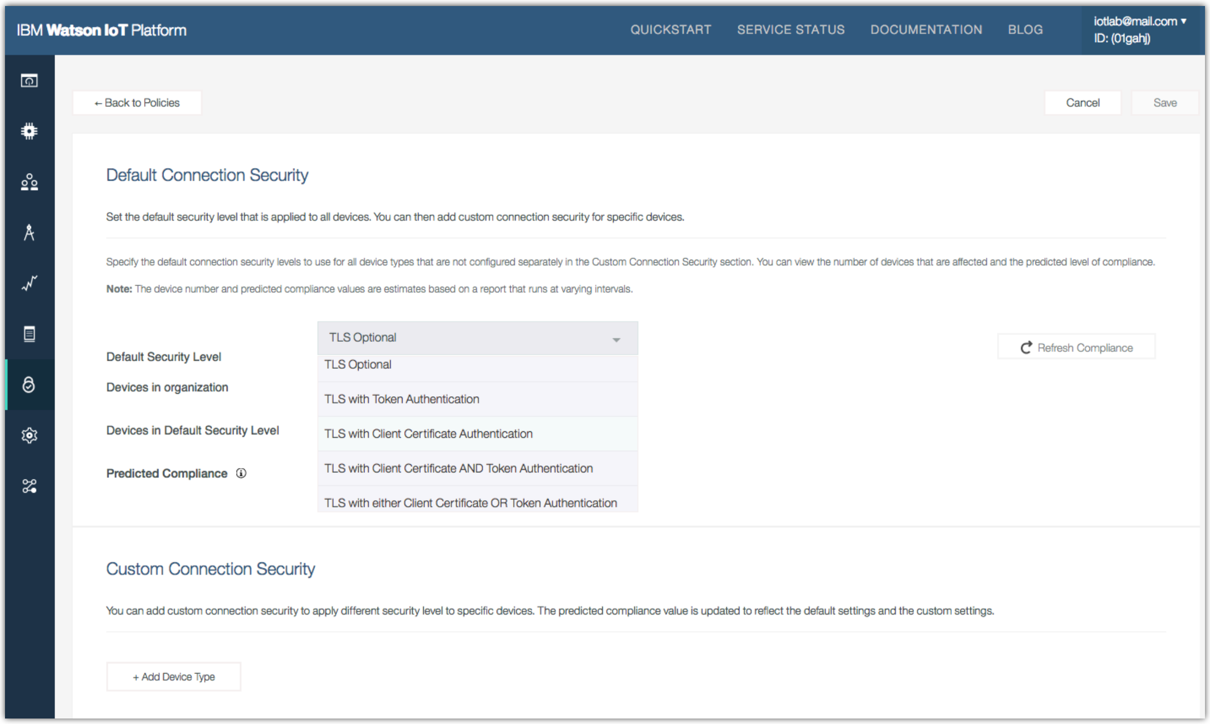
Devices in Default Security Level: 98

Predicted Compliance: 88 Pass 0 Fail 10 Unknown

Custom Connection Security

You can add custom connection security to apply different security level to specific devices. The predicted compliance value is updated to reflect the default settings and the custom settings.

3. Click open the dropdown menu and browse all the security level options



Default Connection Security

Set the default security level that is applied to all devices. You can then add custom connection security for specific devices.

Specify the default connection security levels to use for all device types that are not configured separately in the Custom Connection Security section. You can view the number of devices that are affected and the predicted level of compliance.

Note: The device number and predicted compliance values are estimates based on a report that runs at varying intervals.

Default Security Level: TLS Optional

- TLS Optional
- TLS with Token Authentication
- TLS with Client Certificate Authentication
- TLS with Client Certificate AND Token Authentication
- TLS with either Client Certificate OR Token Authentication

Devices in organization

Devices in Default Security Level

Predicted Compliance ⓘ

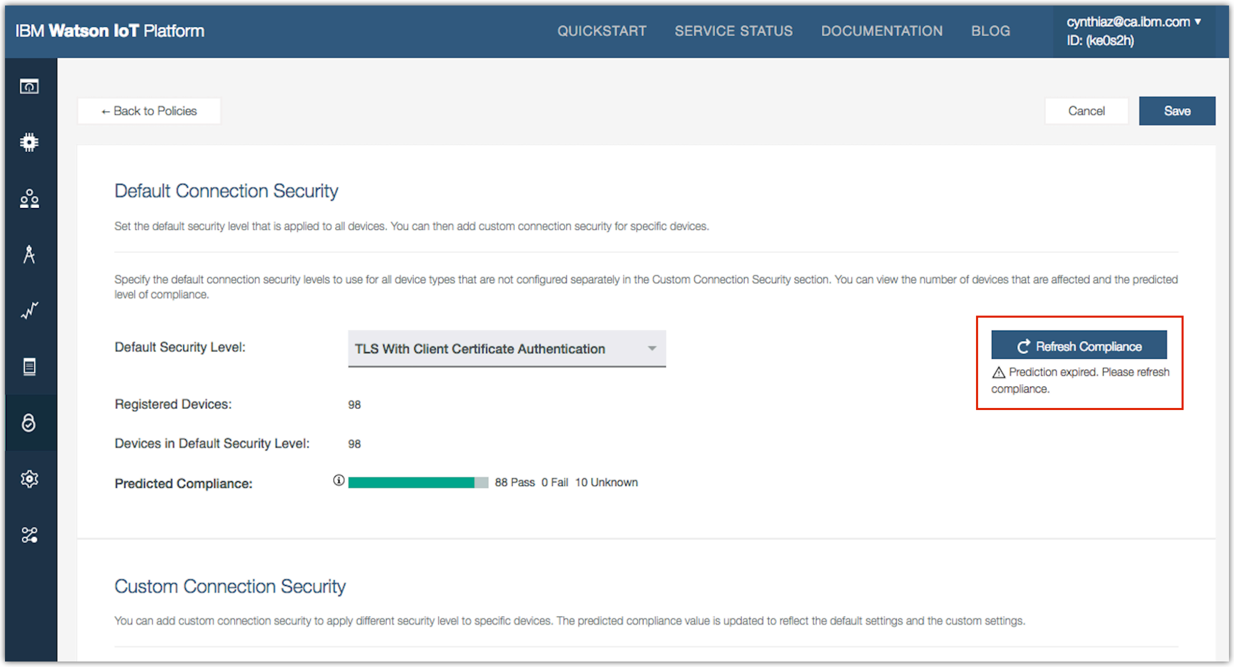
Custom Connection Security

You can add custom connection security to apply different security level to specific devices. The predicted compliance value is updated to reflect the default settings and the custom settings.

1. Try different Security Levels, like “TLS with Token Authentication” or “TLS with Client Certificate Authentication”. After a new security level is selected, click **Refresh Compliance** button to preview the predicted compliance.

   Note: The Predicted Compliance will be update and show the predicted numbers of devices that will Pass and Fail with the new setting.

2. After trying different settings, set the Default Security Level to ““TLS with Token Authentication”



Default Connection Security

Set the default security level that is applied to all devices. You can then add custom connection security for specific devices.

Specify the default connection security levels to use for all device types that are not configured separately in the Custom Connection Security section. You can view the number of devices that are affected and the predicted level of compliance.

Default Security Level: TLS With Client Certificate Authentication

⚠ Prediction expired. Please refresh compliance.

Registered Devices: 98

Devices in Default Security Level: 98

Predicted Compliance: 88 Pass 0 Fail 10 Unknown

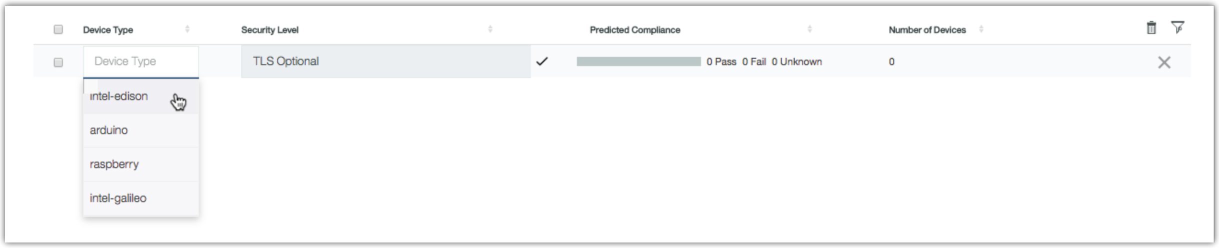
Custom Connection Security

You can add custom connection security to apply different security level to specific devices. The predicted compliance value is updated to reflect the default settings and the custom settings.

Applying Custom Connection Security

The custom connection security setting allows you to specify a different security level than the default setting to a specific device type. All devices of this type will be enforced by this setting. The predicted compliance value will be updated to reflect changes resulting from the custom security settings.

1. Under Custom Connection Security, click on **Add Device Type**.
   A new row is added.



□	Device Type	Security Level		Predicted Compliance	Number of Devices	
□	Device Type	TLS Optional	✓	0 Pass 0 Fail 0 Unknown	0	×

2. Choose the “intel-edison” device type.

Note: The sample used in this lab has devices registered of the following types; ‘raspberry’, ‘intel-galileo', 'arduino’ and ‘intel-edison’. In this step, add one or more of these types for your custom connection security settings.

3. Choose the “TLS with Client Certificate Authentication” security level for the “intel-edison” device type. Click **Refresh Compliance** button to preview the predicted compliance.

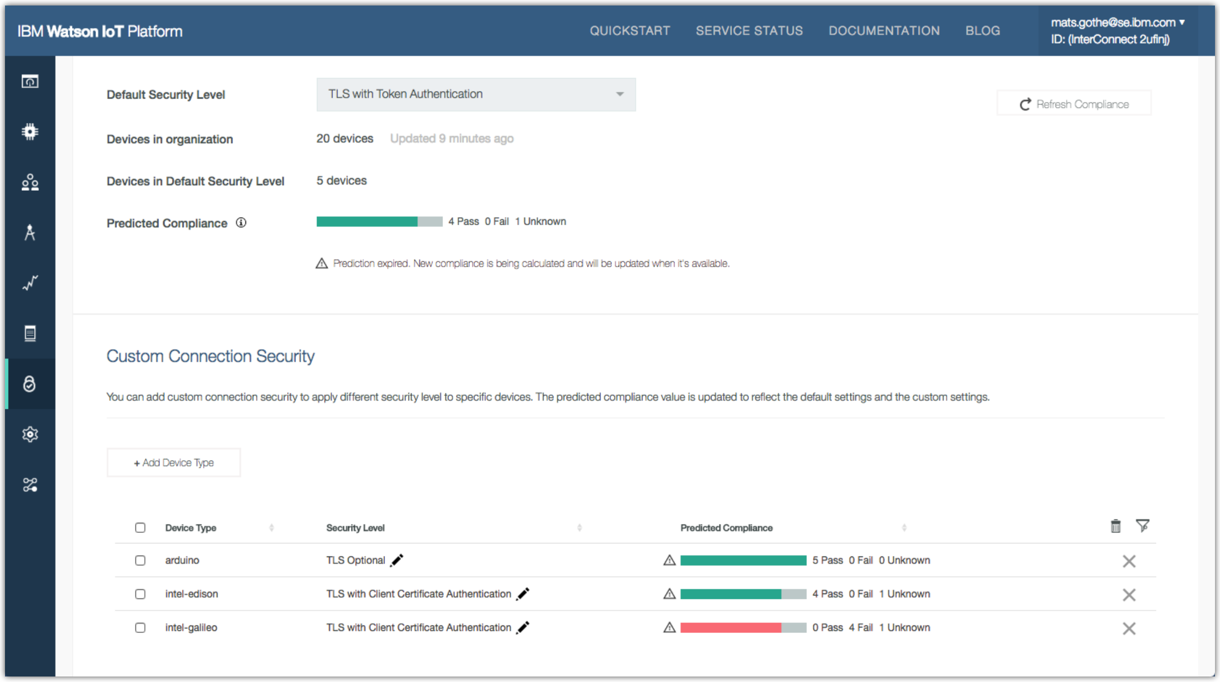
4. Repeat the step and add a custom connection security for the “intel-galileo” device type. Set the security level to “TLS with Token Authentication”.

5. Repeat the step and add a custom connection security for the “arduino” device type. Set the security level to “TLS optional”.

6. Click **Refresh Compliance** button to preview the predicted compliance.

Note: With these settings we have achieved the following

- The “intel-edison” devices are now required to present a valid client certificate to be allowed to connect. The prediction is that all devices will pass.
- The “intel-galileo” devices do not yet have client certificates and will not be allowed to connect. All devices will fail.
- The “arduino” devices are not required to have a client token or certificate when connecting. All devices will pass.



Default Security Level: TLS with Token Authentication

Devices in organization: 20 devices Updated 9 minutes ago

Devices in Default Security Level: 5 devices

Predicted Compliance: 4 Pass 0 Fail 1 Unknown

Prediction expired. New compliance is being calculated and will be updated when it's available.

Custom Connection Security

You can add custom connection security to apply different security level to specific devices. The predicted compliance value is updated to reflect the default settings and the custom settings.

□	Device Type	Security Level	Predicted Compliance
□	arduino	TLS Optional	5 Pass 0 Fail 0 Unknown
□	intel-edison	TLS with Client Certificate Authentication	4 Pass 0 Fail 1 Unknown
□	intel-galileo	TLS with Client Certificate Authentication	0 Pass 4 Fail 1 Unknown

7. Click **Refresh Compliance** to update the report.

8. Click **Save** to apply the changes.

   Note: After policy is saved, all applicable devices need to reconnect in order to be evaluated against the new policy setting. New compliance will be updated and displayed when it’s available (usually the evaluation takes up to 15 minutes depending on the organization’s size).

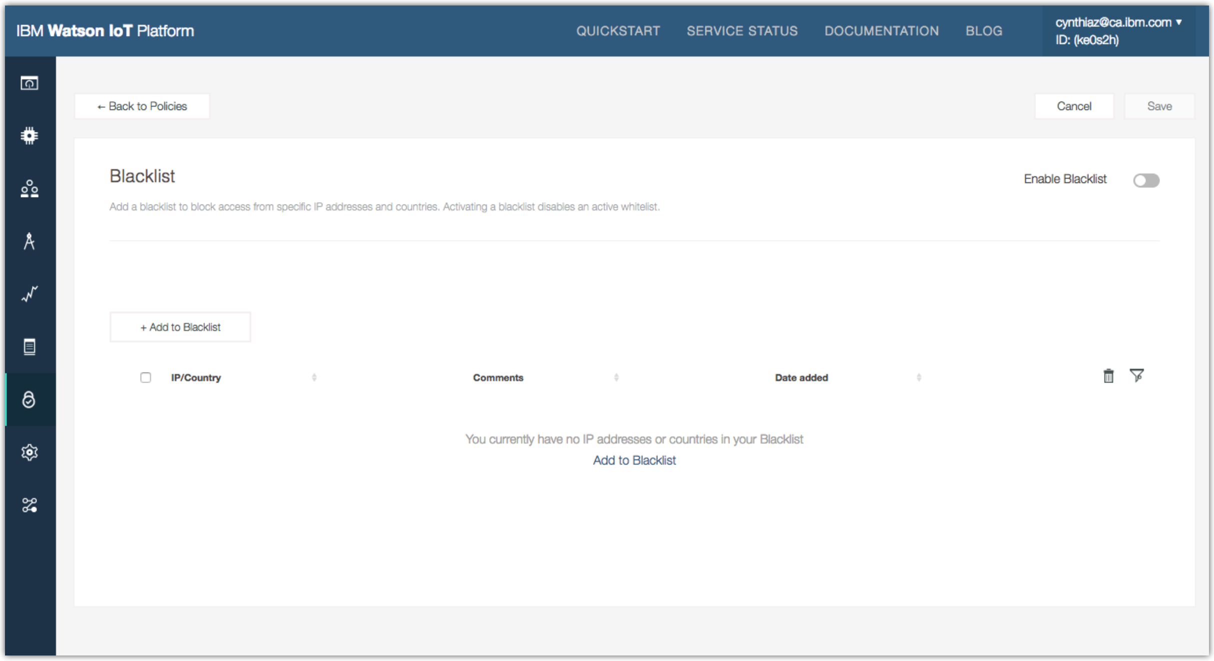
You have now completed the steps to preview and update the connection security policy. While your IoT platform organization is updating the device connection information you will explore the Blacklist and Whitelist Policy.

Configuring a Blacklist / Whitelist Policy

Your organization can restrict access to the server from certain devices by using a blacklist or a whitelist to grant server access to specific devices. A blacklist identifies all of the IP addresses, CIDRs, or countries that are to be denied server access, while a whitelist gives explicit access to specific IP addresses, CIDRs or countries. They cannot be used together. In this scenario, you will be setting up the Blacklist.

You will learn to use the Blacklist to block access from devices, and you can apply the same work flow to Whitelist.

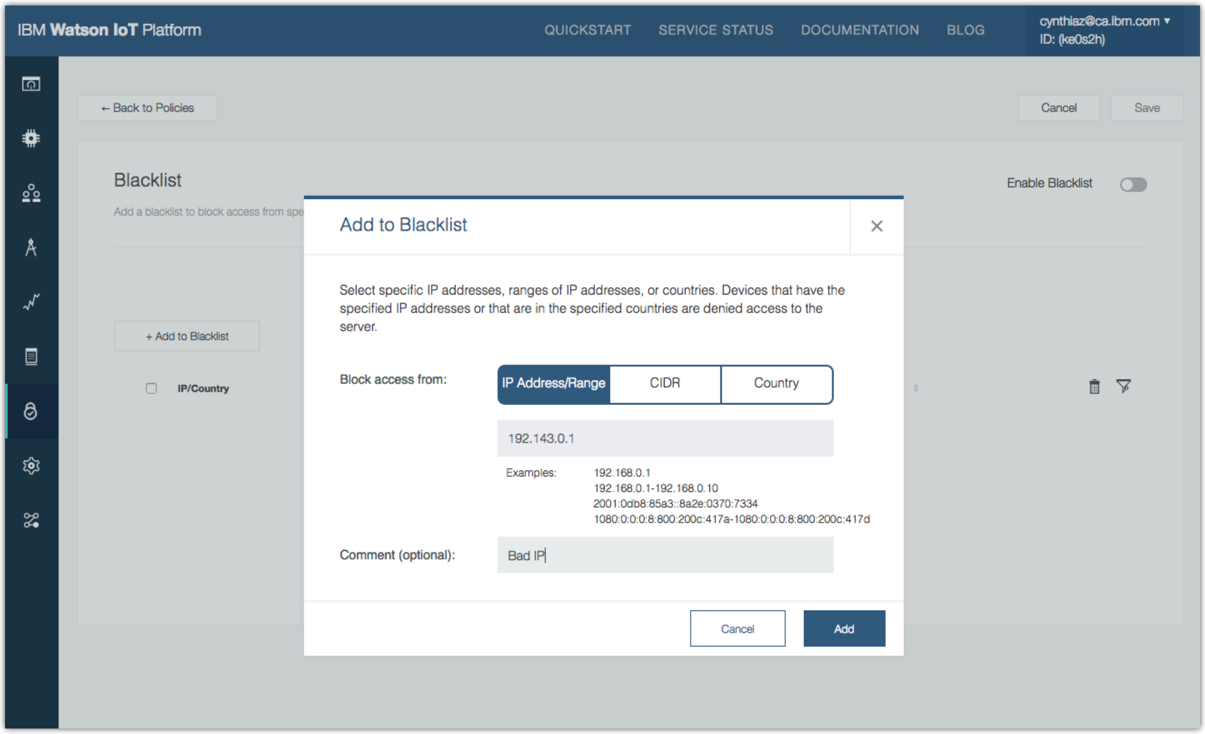
1. Open Blacklist policy, and click **Add to Blacklist**.



Add a blacklist to block access from specific IP addresses and countries. Activating a blacklist disables an active whitelist.

You currently have no IP addresses or countries in your Blacklist

2. Click **Add to Blacklist**. The Add to Blacklist dialog opens.



Add to Blacklist

Select specific IP addresses, ranges of IP addresses, or countries. Devices that have the specified IP addresses or that are in the specified countries are denied access to the server.

Block access from: IP Address/Range | CIDR | Country

192.143.0.1

Examples:
192.168.0.1
192.168.0.1-192.168.0.10
2001:0db8:85a3::8a2e:0370:7334
1080:0:0:0:8:800:200c:417a-1080:0:0:0:8:800:200c:417d

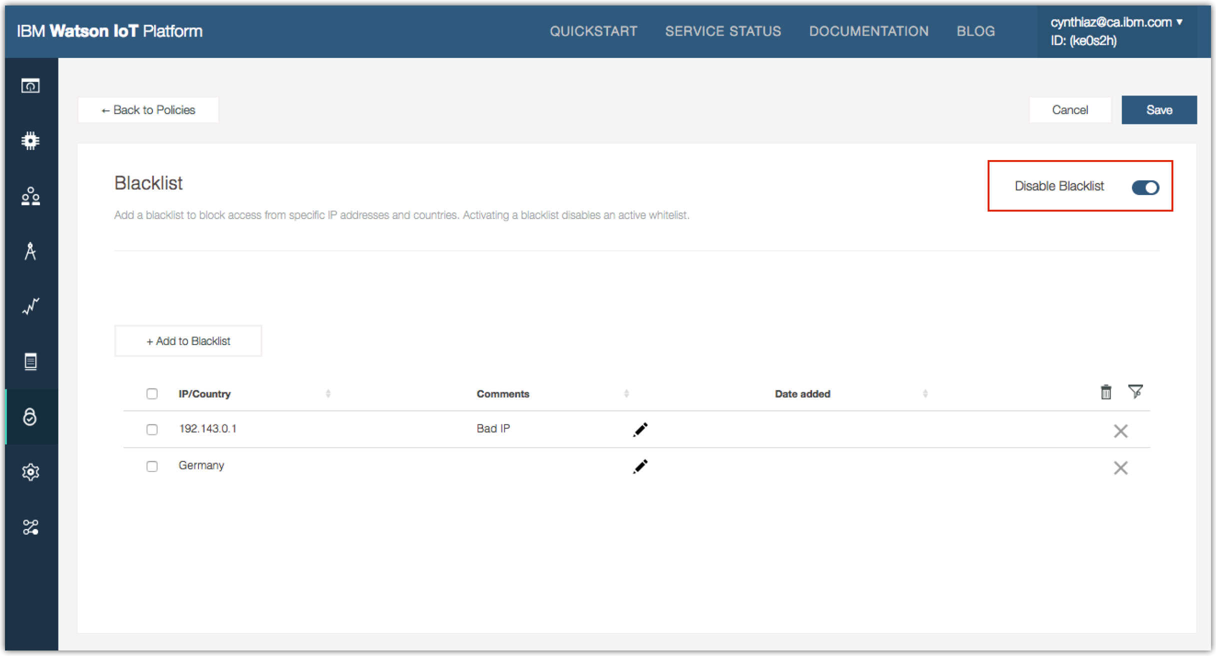
Comment (optional): Bad IP

3. On the **IP Address/Range** tab, enter the IP address to the “arduino-1” device that you made a note of in an earlier section of the lab.

   Note: There are options to block an IP rage or a Country.
   - Use the **CIDR** tab to enter a Classless Inter-Domain Routing (CIDR) notated block.
   - Use the **Country** tab, enter or select countries from which you want to block all devices.

4. Once you have complete the blacklist settings, flip the **Enable Blacklist** switch to On. Click **Save**.

   Tip: you can maintain your blacklist without enforcing it by keeping it disabled.

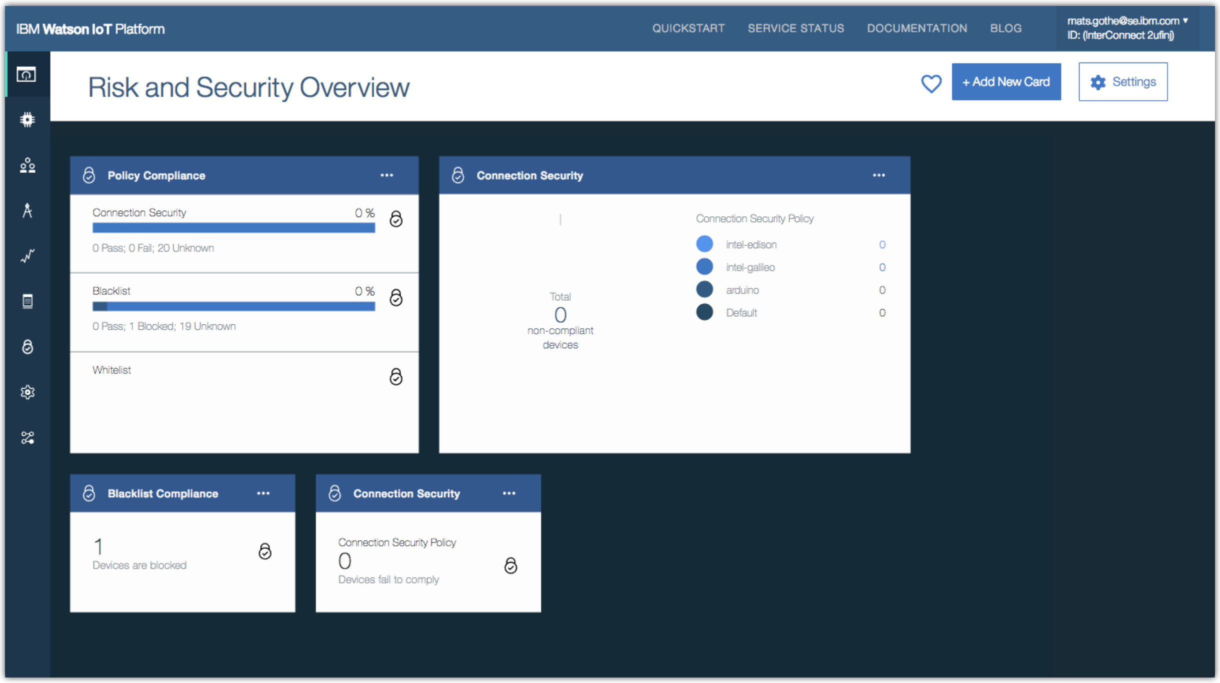


Blacklist

Add a blacklist to block access from specific IP addresses and countries. Activating a blacklist disables an active whitelist.

□	IP/Country	Comments	Date added
□	192.143.0.1	Bad IP	
□	Germany		

5. When the device tries to reconnect from the same IP, the connection will be rejected. This information will also be reflected on the **Blacklist Compliance card** in the **Risk and Security Overview** board.



Risk and Security Overview

Policy Compliance

Connection Security 0 %
0 Pass; 0 Fail; 20 Unknown

Blacklist 0 %
0 Pass; 1 Blocked; 19 Unknown

Whitelist

Connection Security

Total
0
non-compliant devices

Connection Security Policy	
● intel-edison	0
● intel-galileo	0
● arduino	0
● Default	0

Blacklist Compliance

1
Devices are blocked

Connection Security

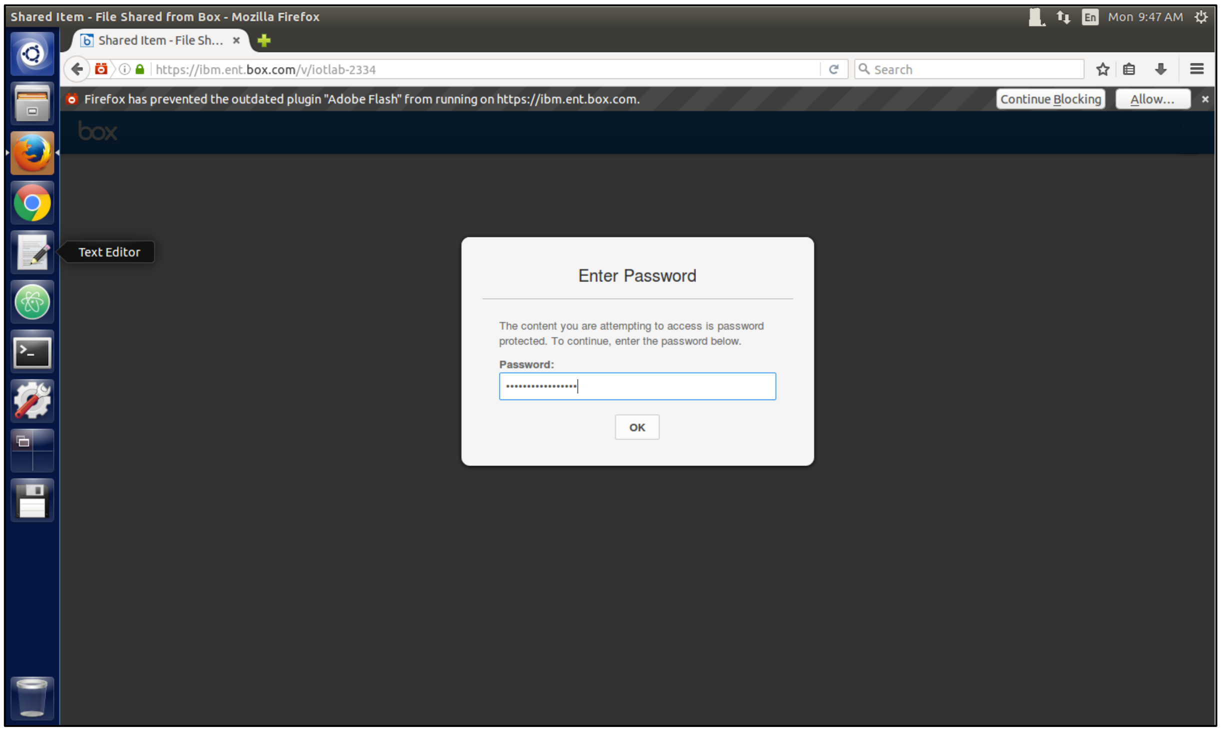
Connection Security Policy
0
Devices fail to comply

Downloading your Certificates

In the next sections of this lab you will work with client and server certificates. As certificates are ensuring secure access for your devices to your organization they are individually generated for each IoT platform organization in this lab.

To access your certificates and keys you have to log into Box and download your certificates.

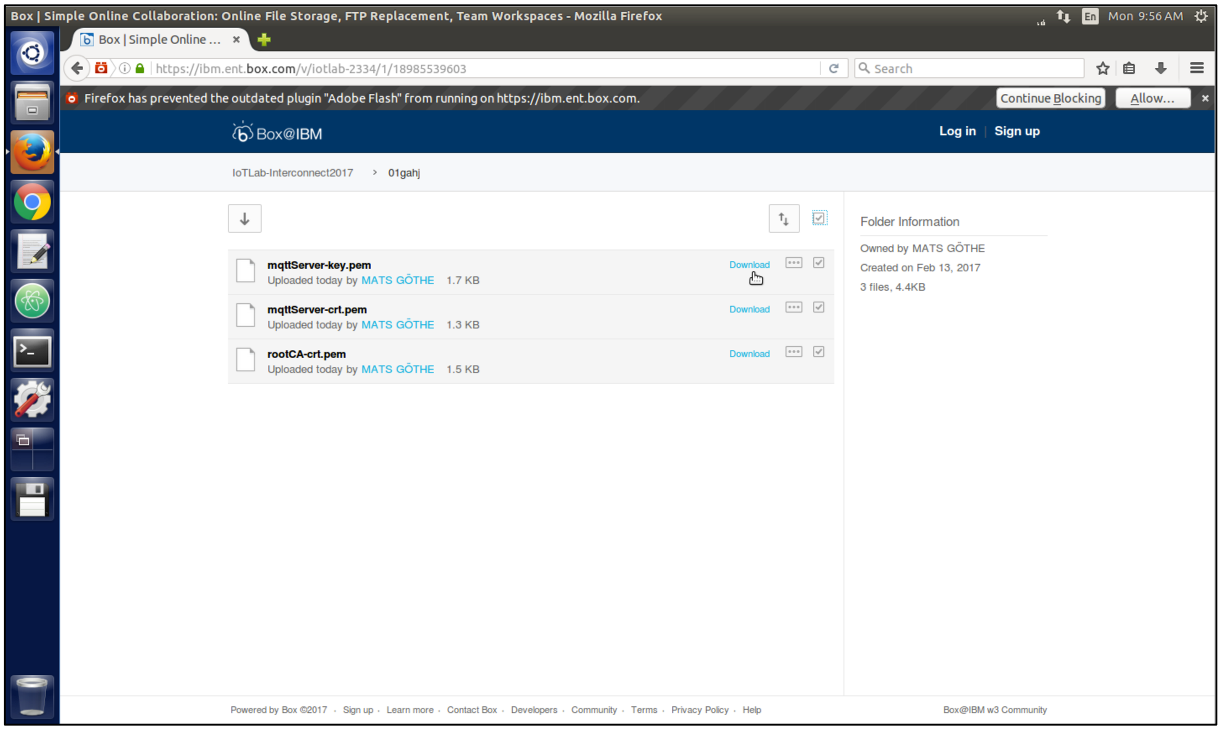
1. Open a new browser window in Firefox
2. Enter https://ibm.box.com/v/iotlab-2334
   The Box shared folder page opens and ask for a Password.
3. Enter password “Interconnect2017!”



Firefox has prevented the outdated plugin "Adobe Flash" from running on https://ibm.ent.box.com.

The content you are attempting to access is password protected. To continue, enter the password below.

4. A folder has been created for each organization. Look for a folder with the organization id that has been assigned to your workstation.
5. **Click on the folder** have of your organization id.



Box | Simple Online Collaboration: Online File Storage, FTP Replacement, Team Workspaces - Mozilla Firefox

https://ibm.ent.box.com/v/iotlab-2334/1/18985539603

Firefox has prevented the outdated plugin "Adobe Flash" from running on https://ibm.ent.box.com.

IoTLab-Interconnect2017 › 01gahj

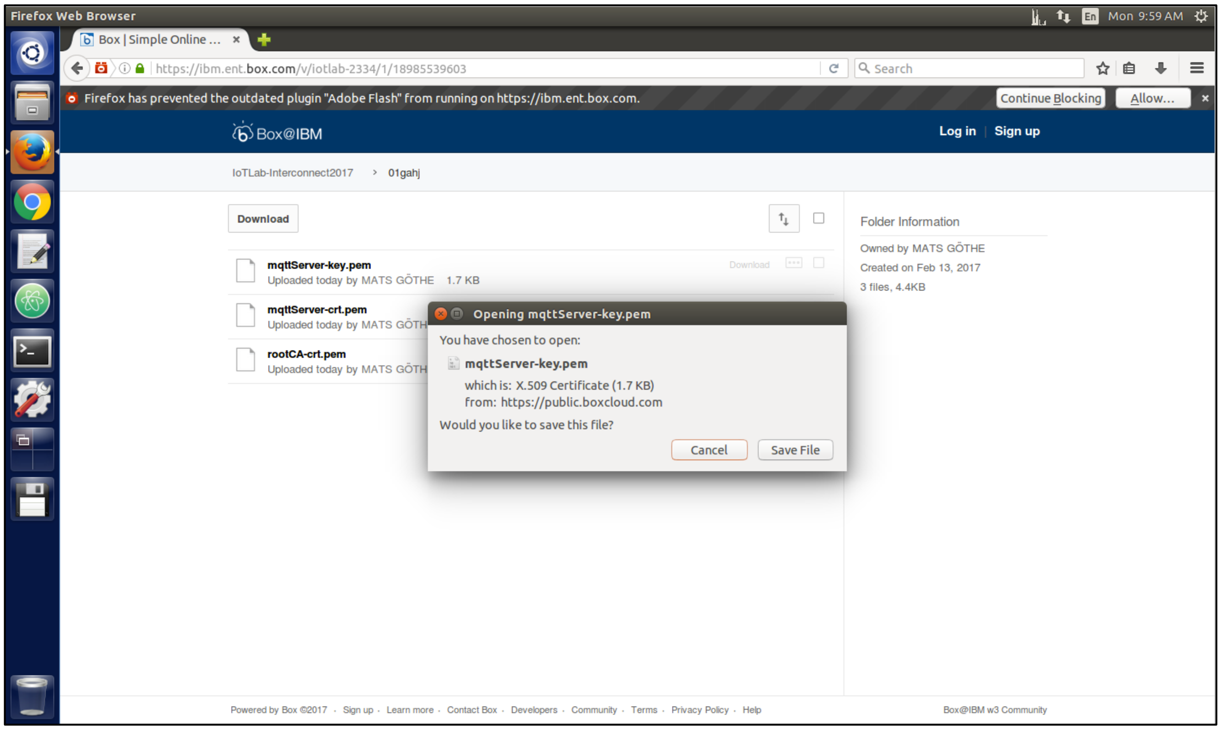
mqttServer-key.pem
Uploaded today by MATS GÖTHE 1.7 KB

mqttServer-crt.pem
Uploaded today by MATS GÖTHE 1.3 KB

rootCA-crt.pem
Uploaded today by MATS GÖTHE 1.5 KB

Folder Information
Owned by MATS GÖTHE
Created on Feb 13, 2017
3 files, 4.4KB

6. Click the **Download** link on the first file.
7. On the following dialog, choose **Save File**



Firefox Web Browser

https://ibm.ent.box.com/v/iotlab-2334/1/18985539603

Firefox has prevented the outdated plugin "Adobe Flash" from running on https://ibm.ent.box.com.

IoTLab-Interconnect2017 › 01gahj

mqttServer-key.pem
Uploaded today by MATS GÖTHE 1.7 KB

mqttServer-crt.pem
Uploaded today by MATS GÖTH

rootCA-crt.pem
Uploaded today by MATS GÖTH

Folder Information
Owned by MATS GÖTHE
Created on Feb 13, 2017
3 files, 4.4KB

Opening mqttServer-key.pem

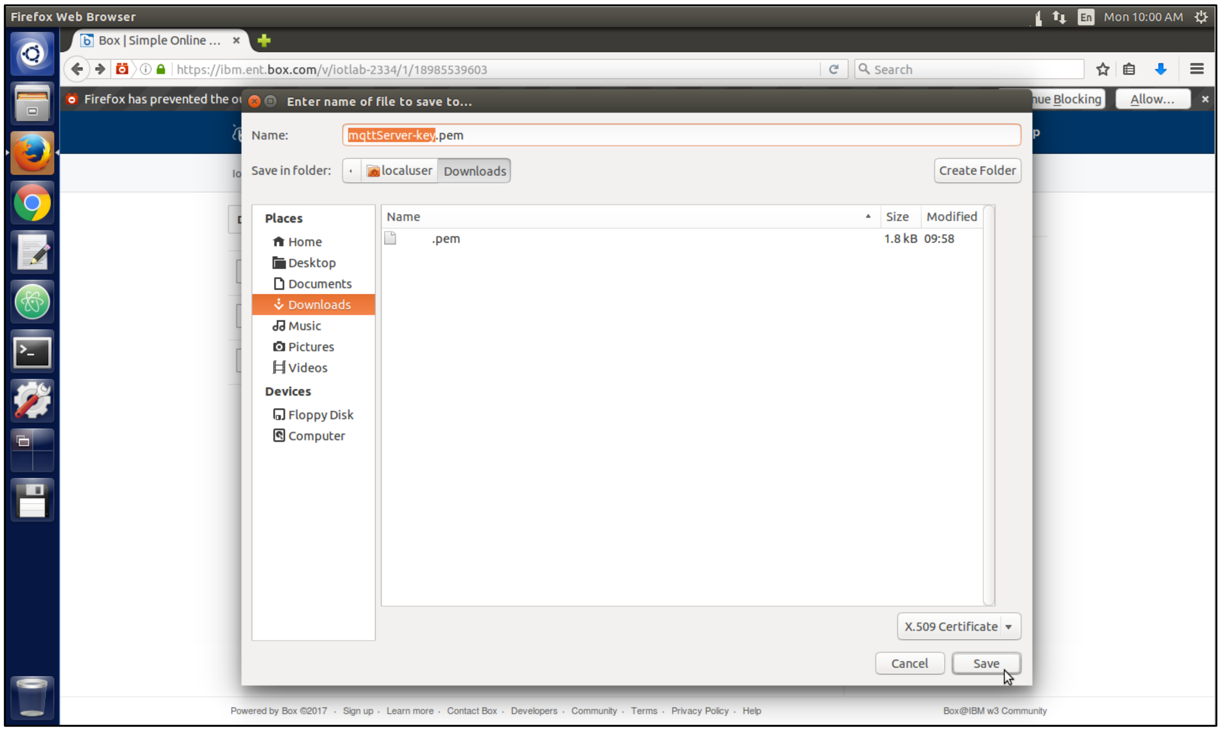
You have chosen to open:

mqttServer-key.pem

which is: X.509 Certificate (1.7 KB)
from: https://public.boxcloud.com

Would you like to save this file?

8. Choose the **Download** directory


Firefox Web Browser
Mon 10:00 AM
Box | Simple Online ...
https://ibm.ent.box.com/v/iotlab-2334/1/18985539603
Search
Firefox has prevented the o
ue Blocking
Allow...
Enter name of file to save to...
Create Folder
Places
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices
Floppy Disk
Computer
Cancel
Save
Powered by Box ©2017 · Sign up · Learn more · Contact Box · Developers · Community · Terms · Privacy Policy · Help
Box@IBM w3 Community

Name: mqttServer-key.pem

Save in folder: localuser Downloads

Name	Size	Modified
.pem	1.8 kB	09:58

X.509 Certificate

9. Choose the **Download** directory
10. Repeat the steps above to download all files in the shared directory

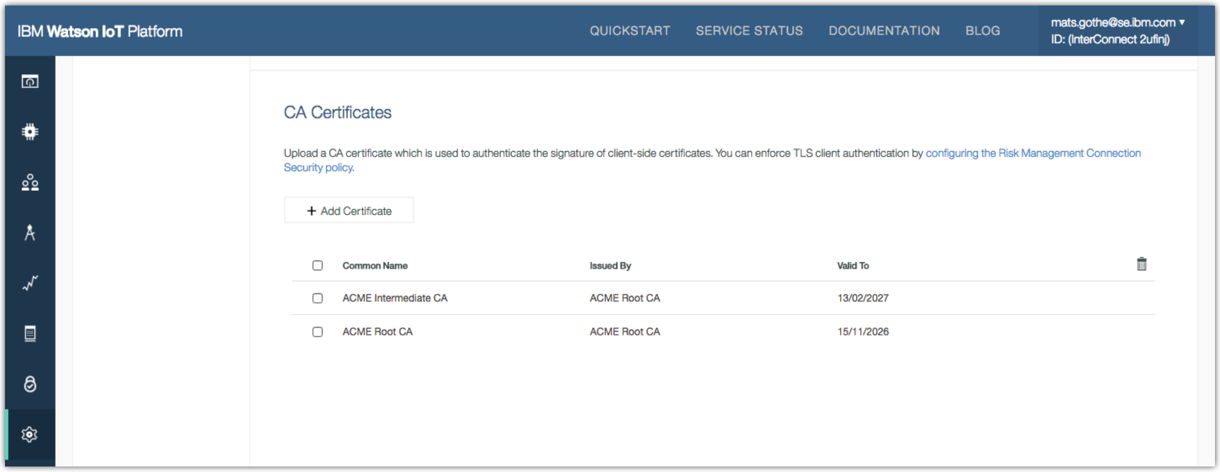
Client Certificate Management

Certificates are used for device authentication. Any devices that do not have valid signed certificates are denied access and cannot communicate with the server.

To configure certificates and server access for devices, you can register the associated certificate authority (CA) certificates into the Watson IoT Platform. CA certificates enable the organization to recognize the client certificates on devices as trusted so that devices can connect to the server.

1. Navigate to **General Settings**, click **CA Certificates** in the Security section**.**

Note: There are two certificates installed in the organization. One Root certificate and one Intermediate Certificate.

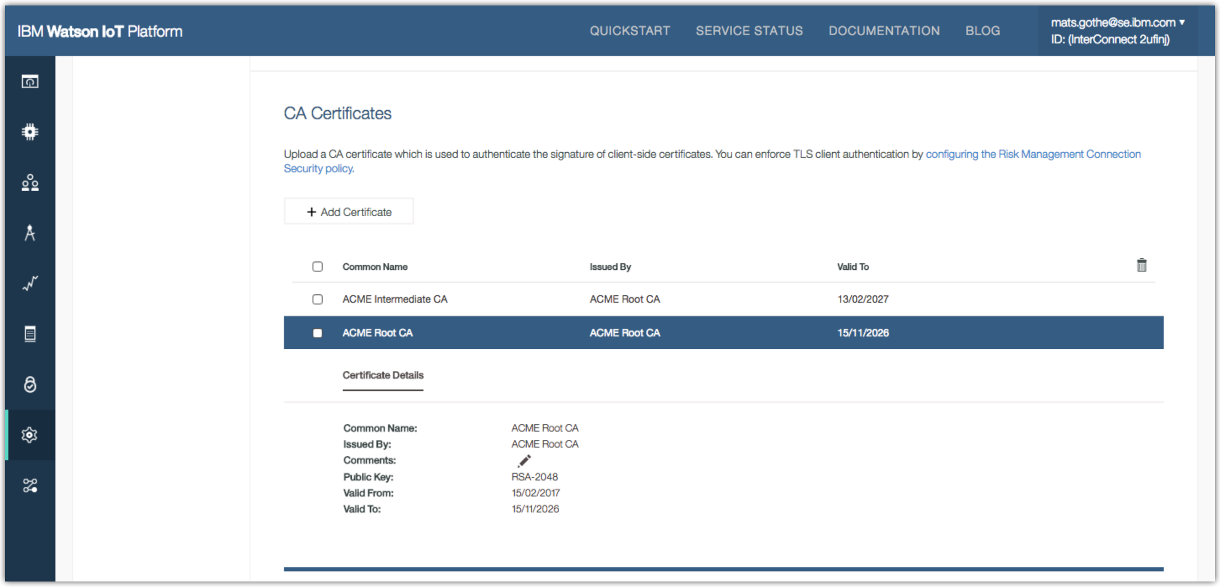


CA Certificates

Upload a CA certificate which is used to authenticate the signature of client-side certificates. You can enforce TLS client authentication by configuring the Risk Management Connection Security policy.

□	Common Name	Issued By	Valid To
□	ACME Intermediate CA	ACME Root CA	13/02/2027
□	ACME Root CA	ACME Root CA	15/11/2026

2. Click on one of the certificates. A detail view of the certificate is shown.



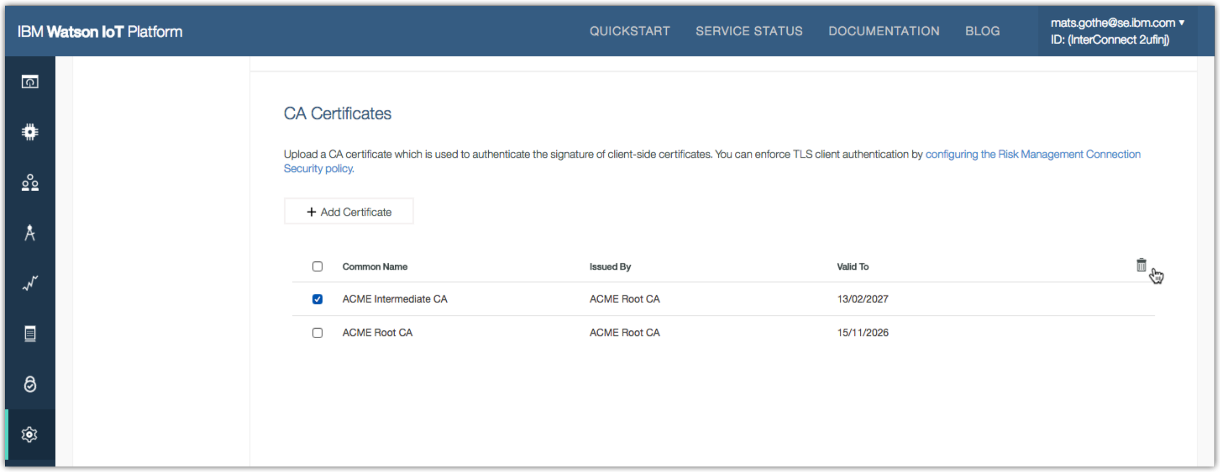
CA Certificates

Upload a CA certificate which is used to authenticate the signature of client-side certificates. You can enforce TLS client authentication by configuring the Risk Management Connection Security policy.

☐	Common Name	Issued By	Valid To
☐	ACME Intermediate CA	ACME Root CA	13/02/2027
■	ACME Root CA	ACME Root CA	15/11/2026

Common Name:	ACME Root CA
Issued By:	ACME Root CA
Comments:	
Public Key:	RSA-2048
Valid From:	15/02/2017
Valid To:	15/11/2026

3. **Optionally**, Remove the “ACME Intermediate CA” certificate by checking the box on the certificate and click the trash can icon.



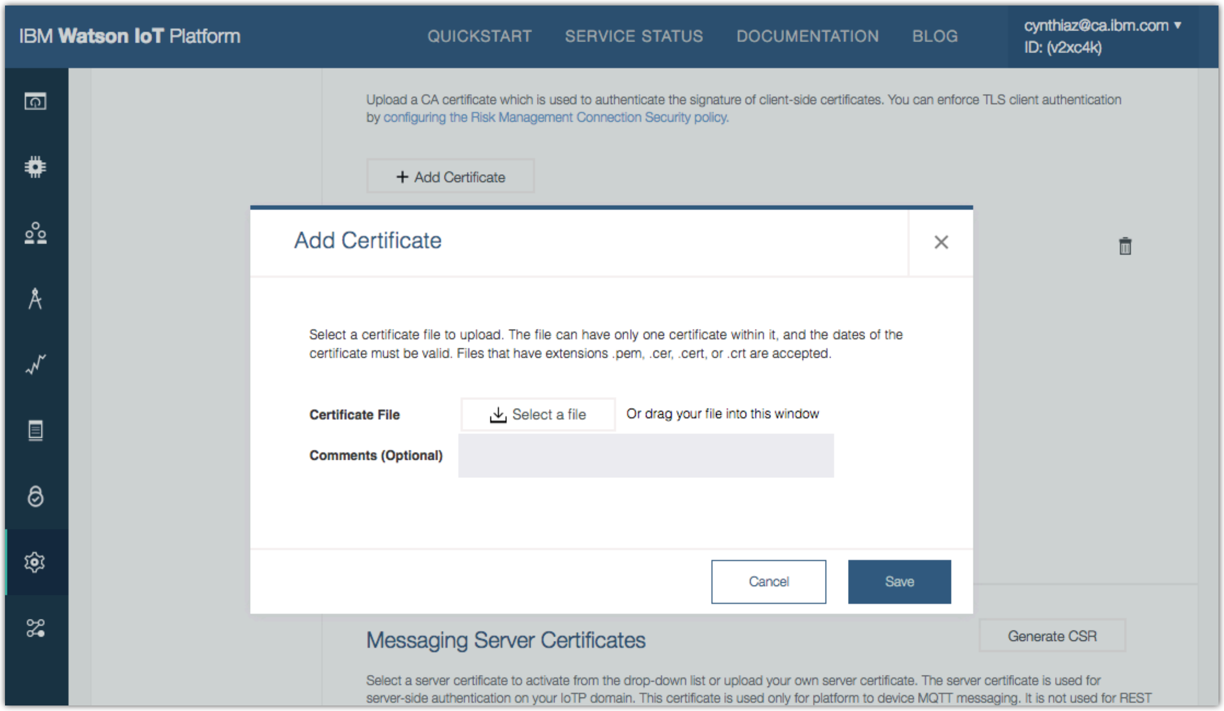
CA Certificates

Upload a CA certificate which is used to authenticate the signature of client-side certificates. You can enforce TLS client authentication by configuring the Risk Management Connection Security policy.

☐	Common Name	Issued By	Valid To
☑	ACME Intermediate CA	ACME Root CA	13/02/2027
☐	ACME Root CA	ACME Root CA	15/11/2026

4. Browse to select a certificate file to upload, or drag and drop a file in the **Add Certificate** window.

Note: Upload the ‘intermediateCA-crt.pem’ certificate for your IoT platform organization that you downloaded from Box.



Upload a CA certificate which is used to authenticate the signature of client-side certificates. You can enforce TLS client authentication by configuring the Risk Management Connection Security policy.

Select a certificate file to upload. The file can have only one certificate within it, and the dates of the certificate must be valid. Files that have extensions .pem, .cer, .cert, or .crt are accepted.

Certificate File Or drag your file into this window

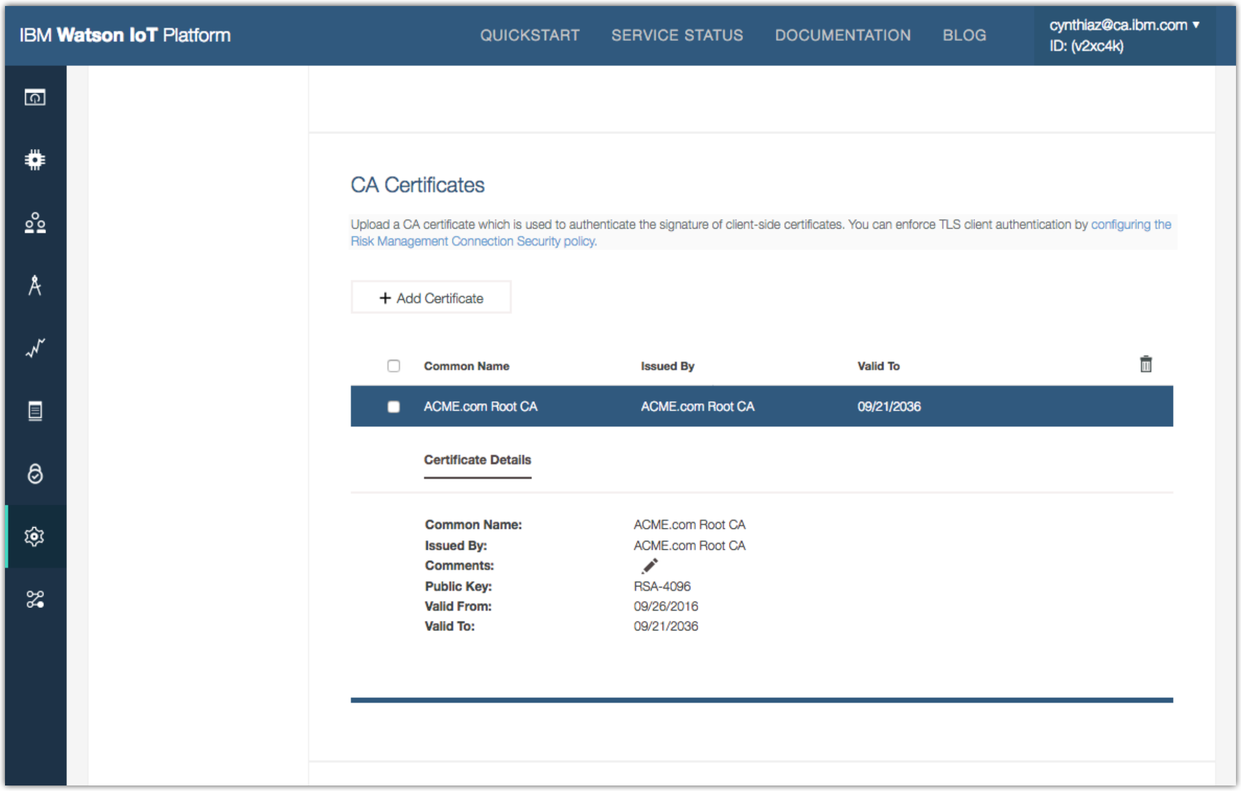
Comments (Optional)

Messaging Server Certificates

Select a server certificate to activate from the drop-down list or upload your own server certificate. The server certificate is used for server-side authentication on your IoTP domain. This certificate is used only for platform to device MQTT messaging. It is not used for REST

5. Enter an optional comment and click **Save**.
   The certificate is added to your IoT platform organization, activated and listed in the table.

6. Click on the new entry to view more information on the certificate.



CA Certificates

Upload a CA certificate which is used to authenticate the signature of client-side certificates. You can enforce TLS client authentication by configuring the Risk Management Connection Security policy.

+ Add Certificate

□	Common Name	Issued By	Valid To
□	ACME.com Root CA	ACME.com Root CA	09/21/2036

Certificate Details

Common Name:	ACME.com Root CA
Issued By:	ACME.com Root CA
Comments:	
Public Key:	RSA-4096
Valid From:	09/26/2016
Valid To:	09/21/2036

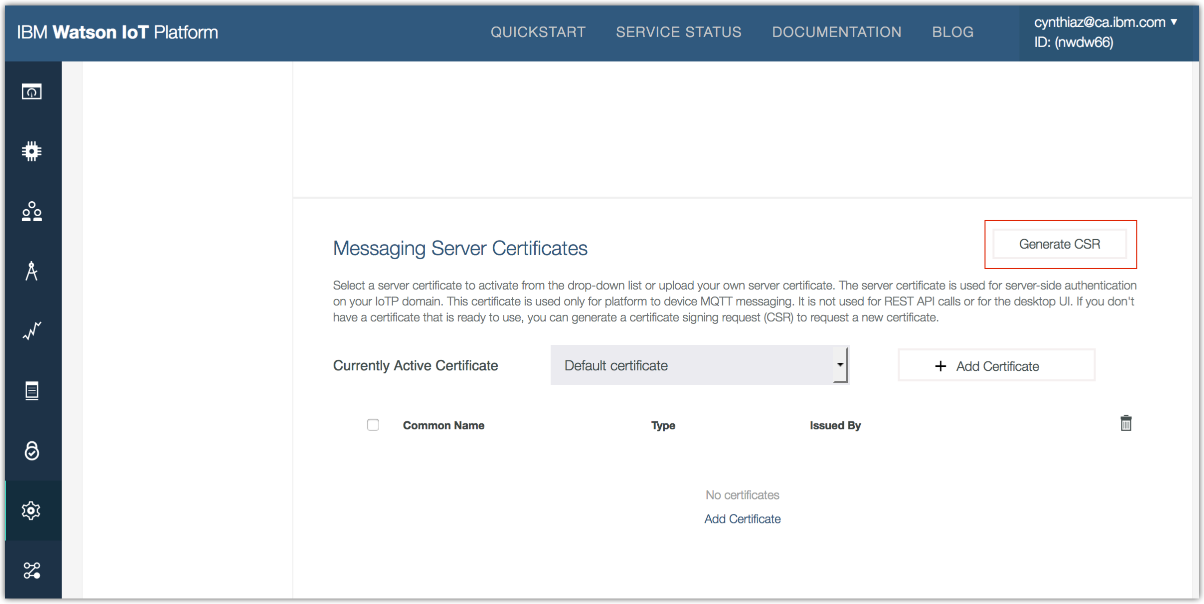
Requesting a new server certificate

Watson IoT Platform provides a default server. You can use the default certificate or request and upload a new server certificate for your organization. If you do not yet have a certificate to use, you can create a request for a new certificate. After you receive the new certificate, you must have it signed and then upload it to the platform.

In the case if your organization doesn't have a certificate that is ready to use, you can generate a certificate signing request (CSR) to request a new certificate. The platform will generate a pairing private key and it will remain in the platform and cannot be downloaded.

In this section of the lab you will make a Certificate Signing Request.

1. In the **Security** section of **General Settings**, under **Messaging Server Certificates**, click **Generate CSR**.



Messaging Server Certificates

Select a server certificate to activate from the drop-down list or upload your own server certificate. The server certificate is used for server-side authentication on your IoTP domain. This certificate is used only for platform to device MQTT messaging. It is not used for REST API calls or for the desktop UI. If you don't have a certificate that is ready to use, you can generate a certificate signing request (CSR) to request a new certificate.

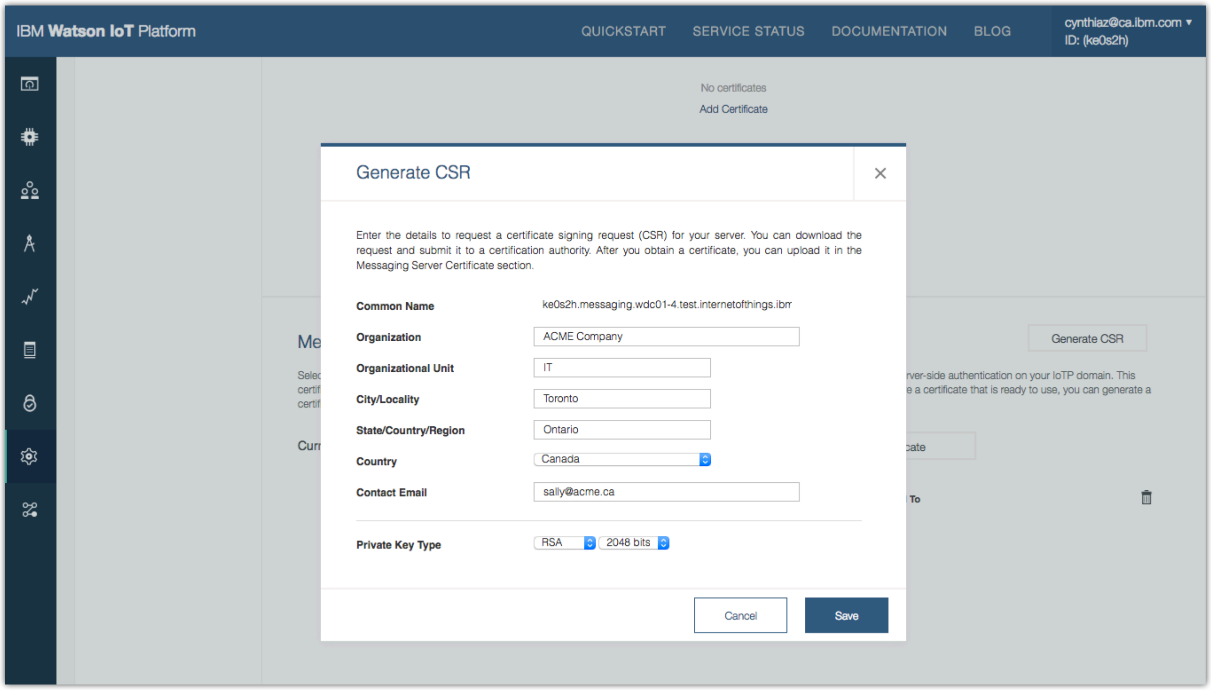
Currently Active Certificate: Default certificate

□	Common Name	Type	Issued By

No certificates

2. Enter the details to request a CSR for your server, and click **Generate**. You can use your own data or the information provided below.

   Organization: **ACME Company**
   Organizational Unit: **IT**
   City / Locality: **Toronto**
   State / Country / Region: **Ontario**
   Country: **Canada**
   Contact Email: **sally@acme.ca**
   Private Key Type: **RSA 2048 bits**



Generate CSR

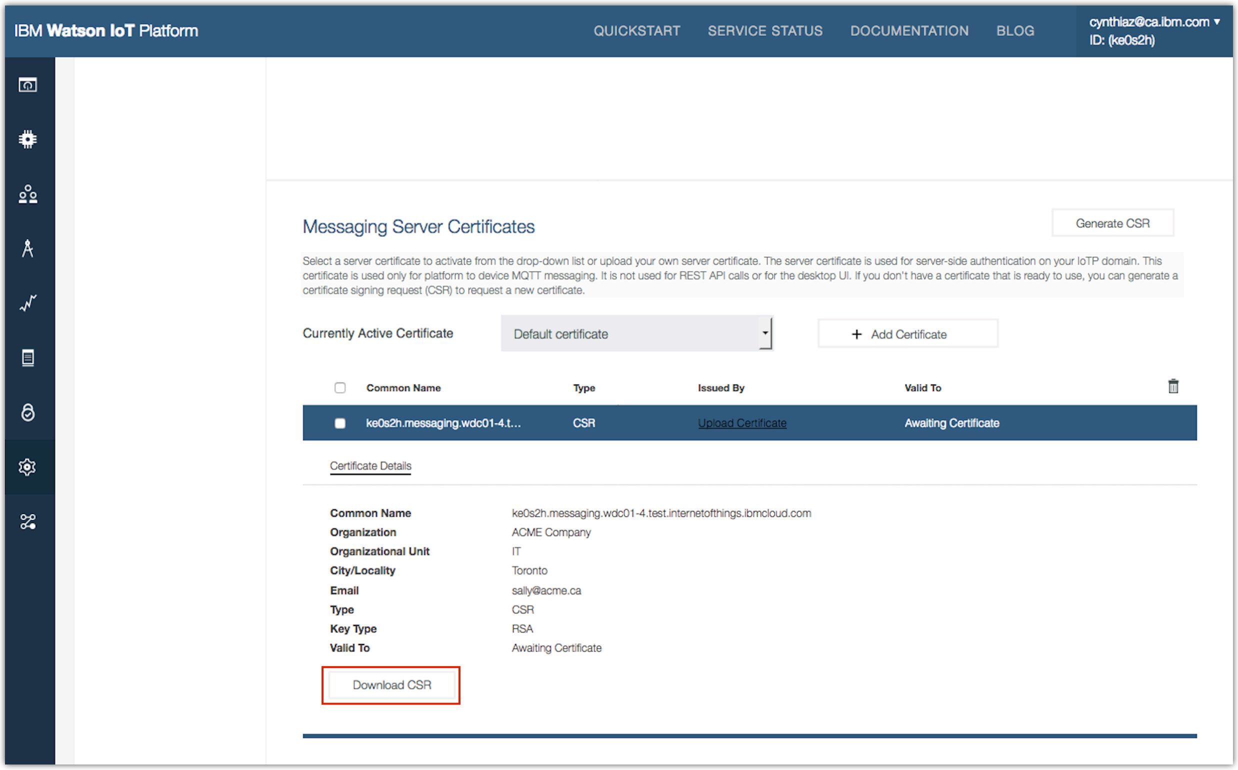
Enter the details to request a certificate signing request (CSR) for your server. You can download the request and submit it to a certification authority. After you obtain a certificate, you can upload it in the Messaging Server Certificate section.

Common Name	ke0s2h.messaging.wdc01-4.test.internetofthings.ibm
Organization	ACME Company
Organizational Unit	IT
City/Locality	Toronto
State/Country/Region	Ontario
Country	Canada
Contact Email	sally@acme.ca
Private Key Type	RSA 2048 bits

Cancel Save

3. Click **Download CSR** to get the request.

   Note: You would submit your CSR to a certification authority for signing.
   In this lab you will be given a server certificate and a key that has been generated for this lab.



Messaging Server Certificates

Select a server certificate to activate from the drop-down list or upload your own server certificate. The server certificate is used for server-side authentication on your IoTP domain. This certificate is used only for platform to device MQTT messaging. It is not used for REST API calls or for the desktop UI. If you don't have a certificate that is ready to use, you can generate a certificate signing request (CSR) to request a new certificate.

Currently Active Certificate: Default certificate

□	Common Name	Type	Issued By	Valid To
□	ke0s2h.messaging.wdc01-4.t...	CSR	Upload Certificate	Awaiting Certificate

Certificate Details

Common Name	ke0s2h.messaging.wdc01-4.test.internetofthings.ibmcloud.com
Organization	ACME Company
Organizational Unit	IT
City/Locality	Toronto
Email	sally@acme.ca
Type	CSR
Key Type	RSA
Valid To	Awaiting Certificate

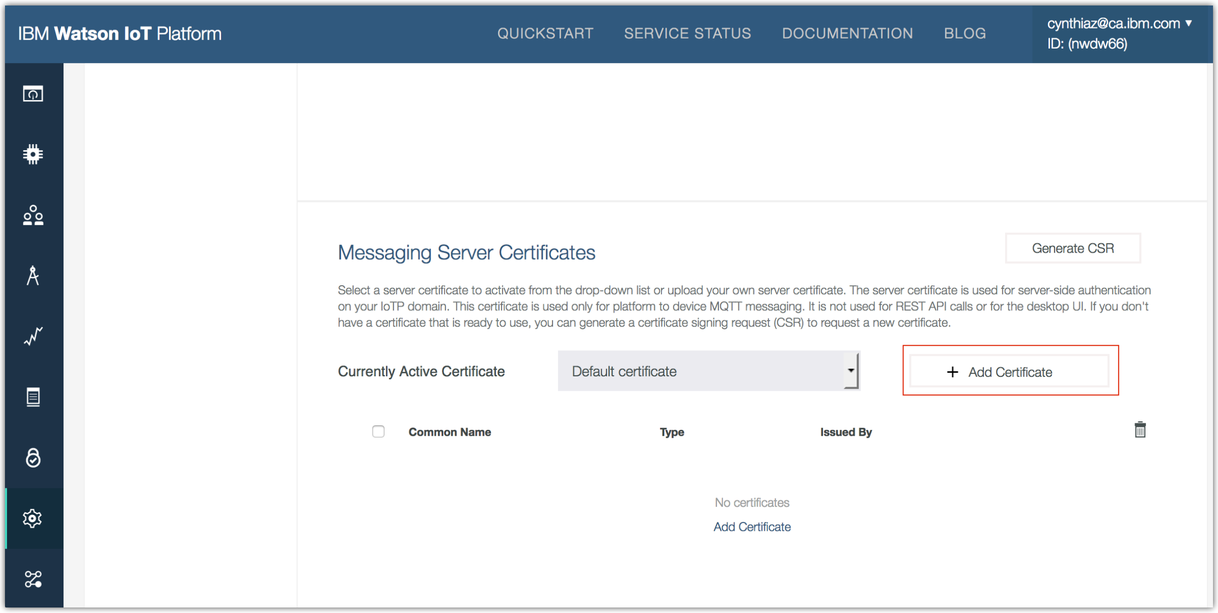
Download CSR

You have now completed the Certificate Service Request. In a real-life situation, you will obtain a certificate. In this lab we have generated certificates for you to upload into the platform as part of next lab section.

Server Certificate Management

As earlier mentioned, Watson IoT Platform provides a default server certificate. You can use this default certificate or upload one from your organization.

1. In the **Security** section of **General Settings**, under **Messaging Server Certificates**, click **Add Certificate**.



Messaging Server Certificates

Generate CSR

Select a server certificate to activate from the drop-down list or upload your own server certificate. The server certificate is used for server-side authentication on your IoTP domain. This certificate is used only for platform to device MQTT messaging. It is not used for REST API calls or for the desktop UI. If you don't have a certificate that is ready to use, you can generate a certificate signing request (CSR) to request a new certificate.

Currently Active Certificate: Default certificate

+ Add Certificate

□	Common Name	Type	Issued By

No certificates

Add Certificate

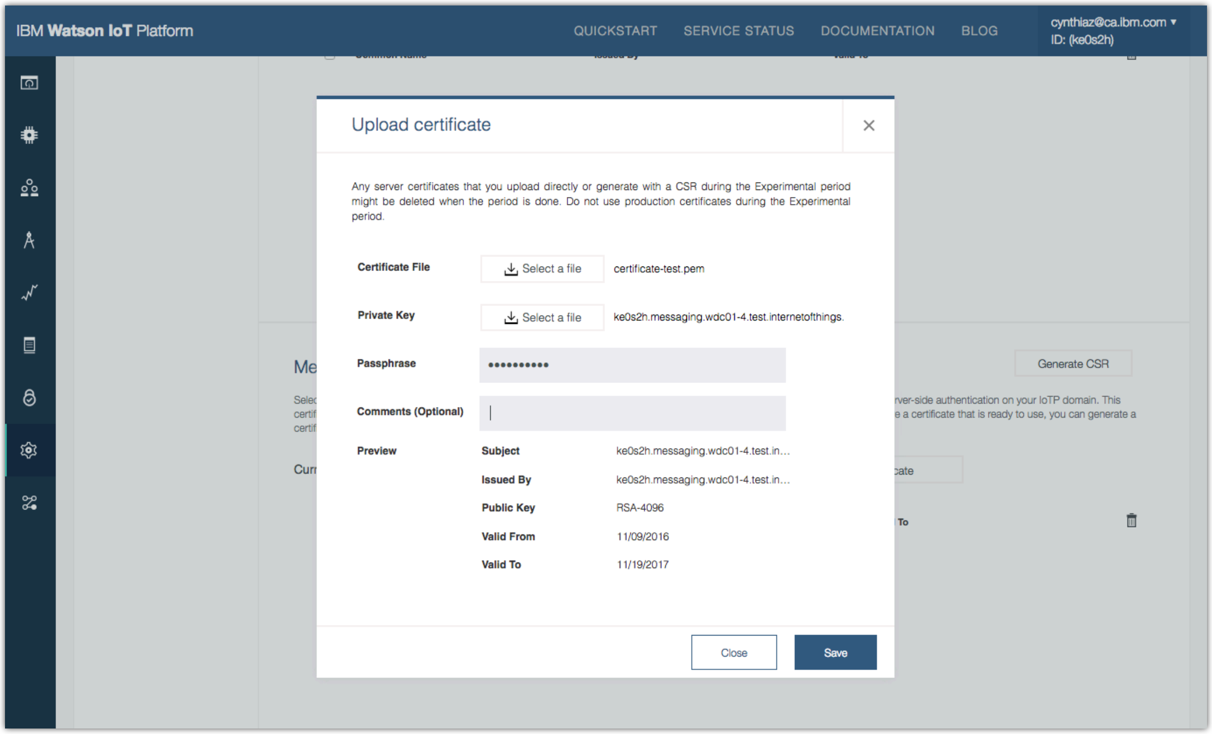
2. Browse to select a certificate file to upload, or drag and drop a file in the **Add Certificate** window.

3. Browse to select the private key file to upload, or drag and drop a file in the **Add Certificate** window.

   Note: Upload the ‘mqttServer-crt.pem’ certificate for your IoT platform organization that you downloaded from Box.

4. Enter the passphrase of the private key, if the private key was encrypted with a passphrase.

   Note: Upload the ‘mqttServer-key.pem’ key for your IoT platform organization that you downloaded from Box.

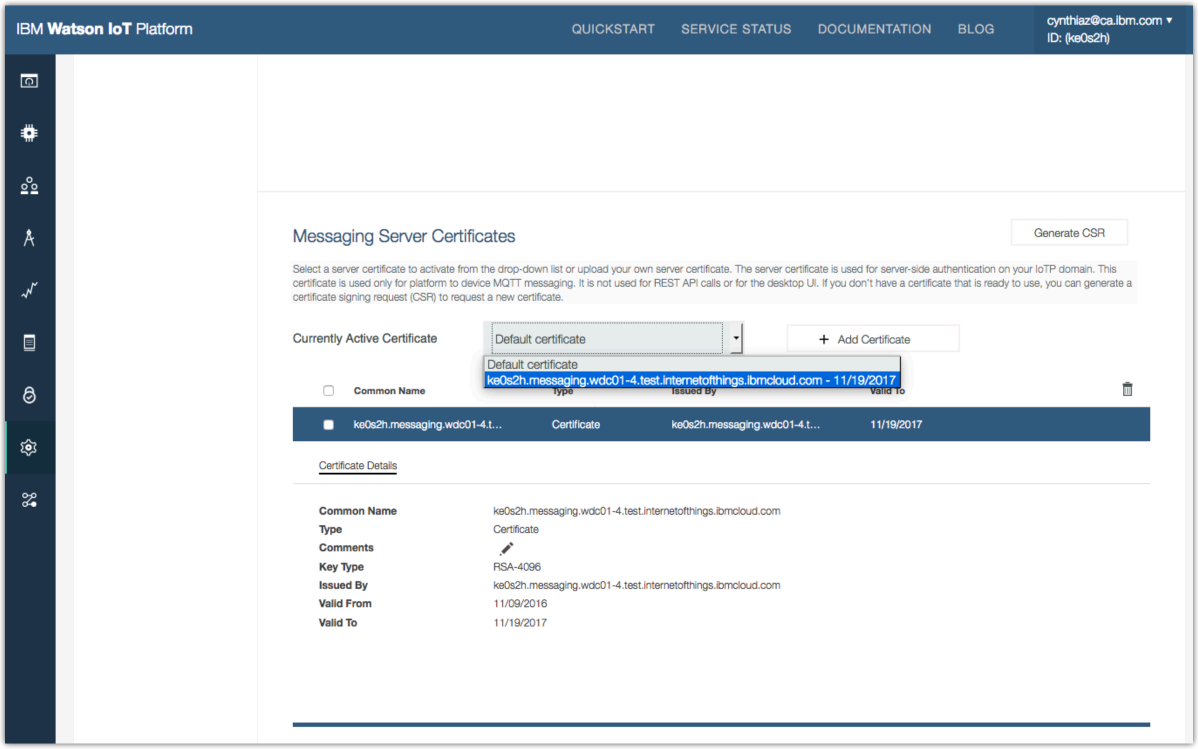


Upload certificate

Any server certificates that you upload directly or generate with a CSR during the Experimental period might be deleted when the period is done. Do not use production certificates during the Experimental period.

Certificate File	Select a file	certificate-test.pem
Private Key	Select a file	ke0s2h.messaging.wdc01-4.test.internetofthings.
Passphrase	••••••••••	
Comments (Optional)		
Preview	Subject	ke0s2h.messaging.wdc01-4.test.in...
	Issued By	ke0s2h.messaging.wdc01-4.test.in...
	Public Key	RSA-4096
	Valid From	11/09/2016
	Valid To	11/19/2017

5. Select the newly uploaded certificate from the **Default messaging server certificate** drop-down list. The selected certificate is listed in the table as the active certificate.



Messaging Server Certificates

Select a server certificate to activate from the drop-down list or upload your own server certificate. The server certificate is used for server-side authentication on your IoTP domain. This certificate is used only for platform to device MQTT messaging. It is not used for REST API calls or for the desktop UI. If you don't have a certificate that is ready to use, you can generate a certificate signing request (CSR) to request a new certificate.

Currently Active Certificate: Default certificate

+ Add Certificate
Default certificate
ke0s2h.messaging.wdc01-4.test.internetofthings.ibmcloud.com - 11/19/2017

□	Common Name	Type	Issued By	Valid To
□	ke0s2h.messaging.wdc01-4.t...	Certificate	ke0s2h.messaging.wdc01-4.t...	11/19/2017

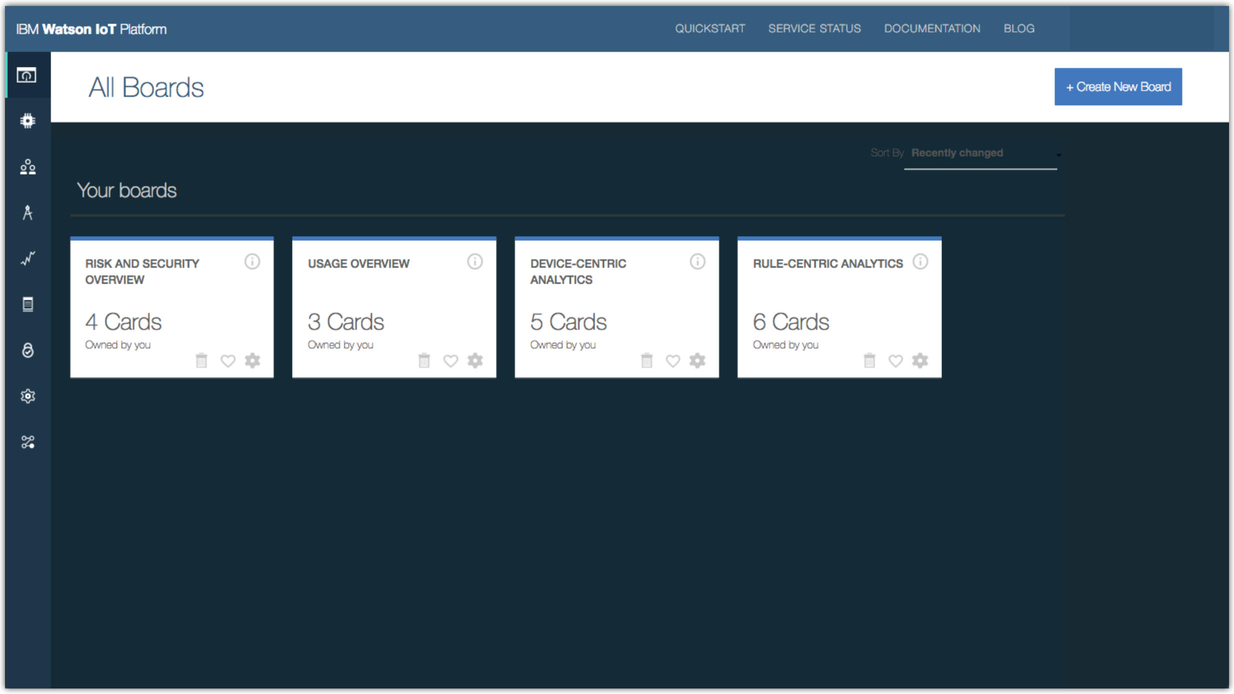
Certificate Details

Common Name	ke0s2h.messaging.wdc01-4.test.internetofthings.ibmcloud.com
Type	Certificate
Comments	
Key Type	RSA-4096
Issued By	ke0s2h.messaging.wdc01-4.test.internetofthings.ibmcloud.com
Valid From	11/09/2016
Valid To	11/19/2017

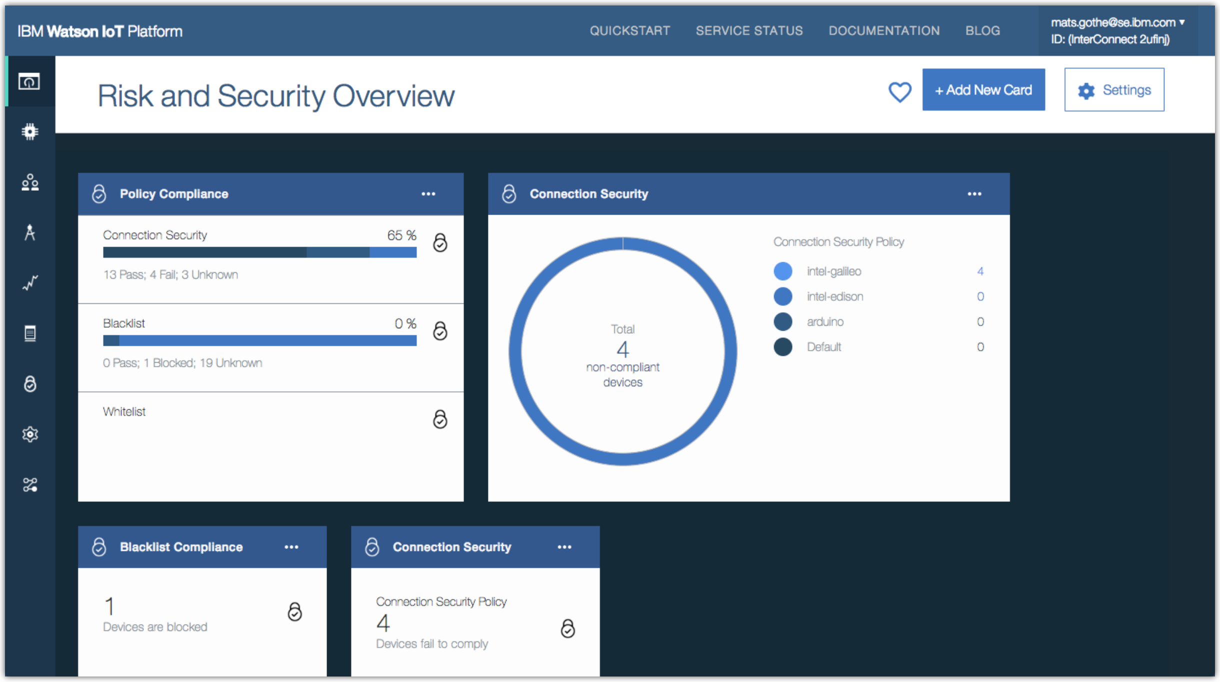
Monitoring the overall security posture and policy compliance

A new “Risk and Security Overview” board is already added on your dashboard with pre-configured cards. It provides an instant overview of the security state of your organization. As a security analyst, you can use the dashboard to visualize the policy compliance and any critical risks and be able to drill into the policy details for root- causes.

1. Go to **Boards** from the main menu, and open **Risk and Security Overview** board



2. Explore each individual card to understand the current risks and policy compliance, hover over the compliance bar to see the breakdown



Risk and Security Overview

Policy Compliance

Connection Security 65 %

13 Pass; 4 Fail; 3 Unknown

Blacklist 0 %

0 Pass; 1 Blocked; 19 Unknown

Whitelist

Connection Security

Total 4 non-compliant devices

Connection Security Policy

intel-galileo	4
intel-edison	0
arduino	0
Default	0

Blacklist Compliance

1 Devices are blocked

Connection Security

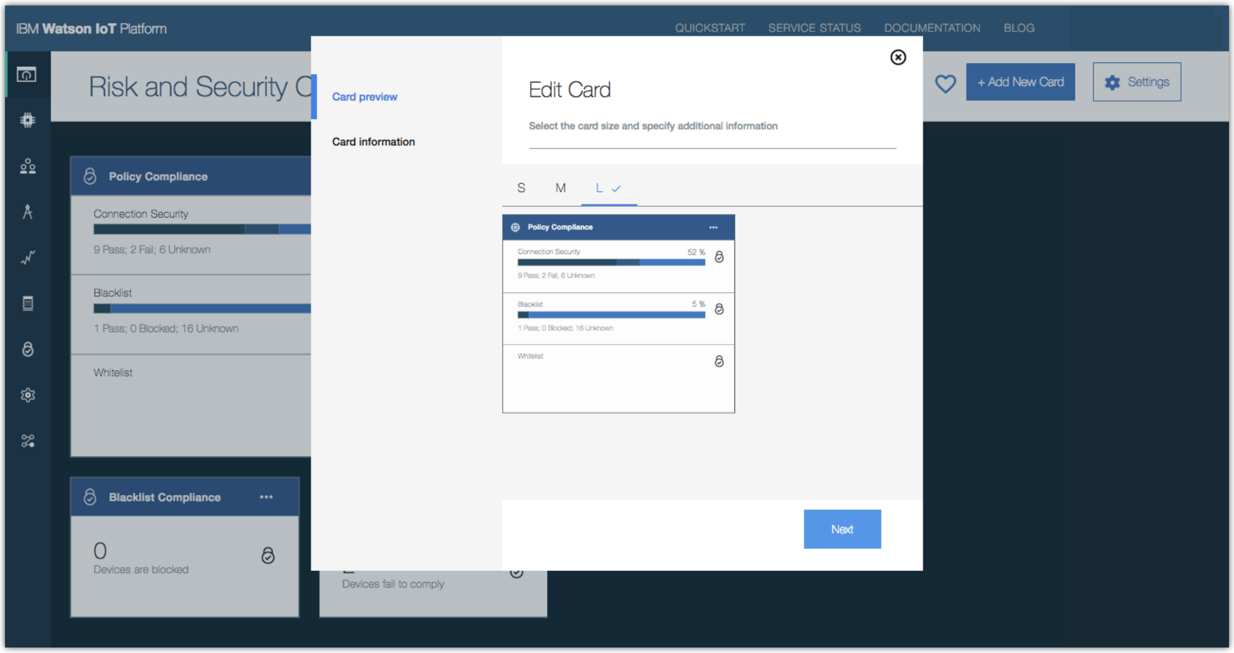
Connection Security Policy
4
Devices fail to comply

Note: You can change the size of the card to promote or demote details.

3. Click on the card **settings icon** on the top right corner of the card. The card menu opens.

4. Click on the **setting icon**. The Edit Card dialog opens.

5. Preview different card sizes by clicking on **S**, **M**, **L** or **XL**. Click **Next** and conform changes



Edit Card

Select the card size and specify additional information

Summary of this lab

You have now completed the Watson IoT Platform Risk and Security Management lab.

In this lab you have deepened your understanding of the Risk and Security Management capabilities in the IoT platform.

- Configure the platform to enable devices authenticating with certificates.
- Import and activate either a new server certificate or generate a Certificate Signing Request (CSR) for messaging.
- Configure the policy to specify the security level for device connection
- Block access from specific IP addresses and/or countries by enforcing Blacklist or Whitelist policy.
- Visualize critical IoT risks and security compliance through a security dashboard

To further explore, sign up for a trial account on IBM Bluemix, create the IBM Watson IoT Platform service and start connecting your IoT devices.