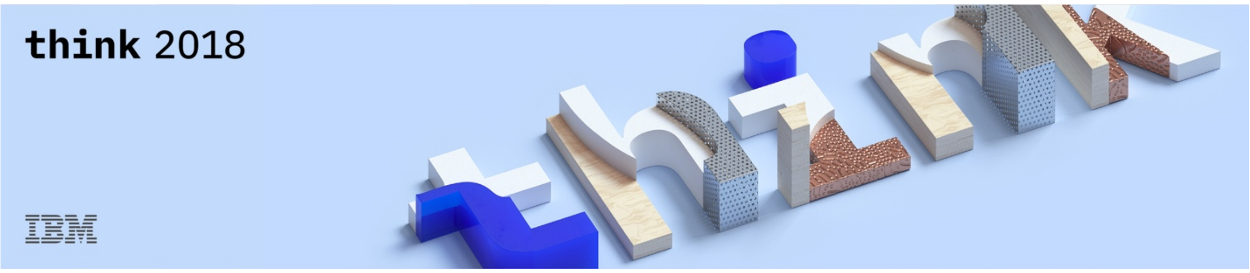


Lab Center – Hands-on Lab

Session 5009

Watson IoT Platform
Risk and Security Management

Mats Gothe
Senior Design Lead
Watson Content & IoT Platform

mats.gothe@se.ibm.com

Table of Contents

Disclaimer

IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results like those stated here.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

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 a Windows 7 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 with automatic login.

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

Logging into Bluemix and Watson IoT Platform

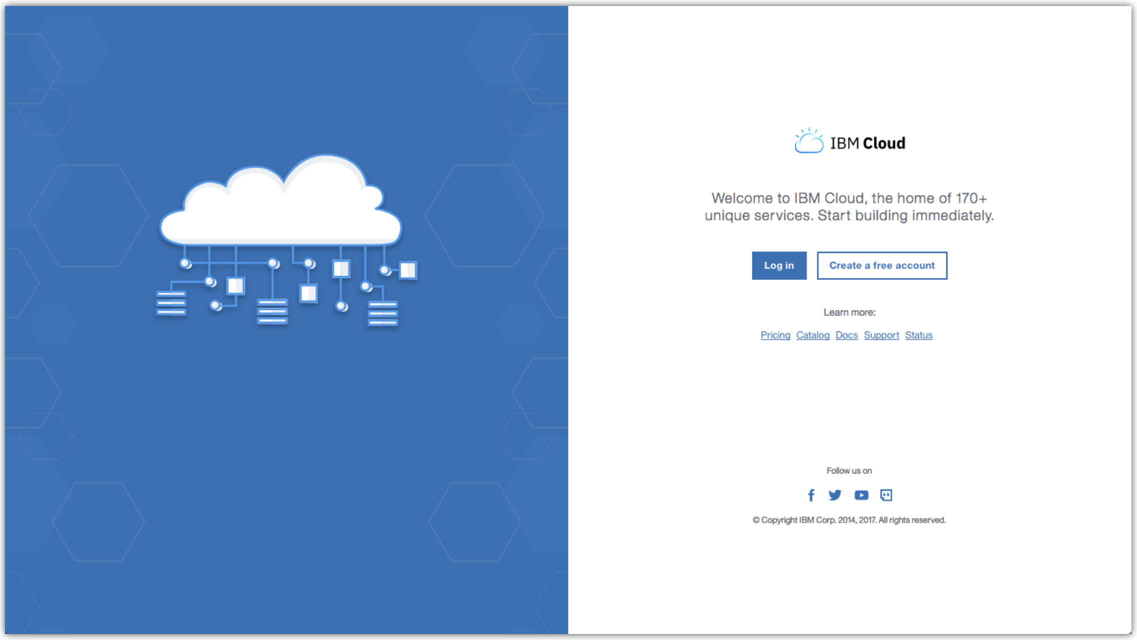
IBM Bluemix is a cloud platform as a service (PaaS) developed by IBM. It supports several programming languages and services as well as integrated DevOps to build, run, deploy and manage applications on the cloud. Bluemix is based on Cloud Foundry open technology and runs on SoftLayer infrastructure.

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.

1. Open the Firefox browser on your workstation
2. Enter https://bluemix.net
   The IBM Cloud welcome page opens

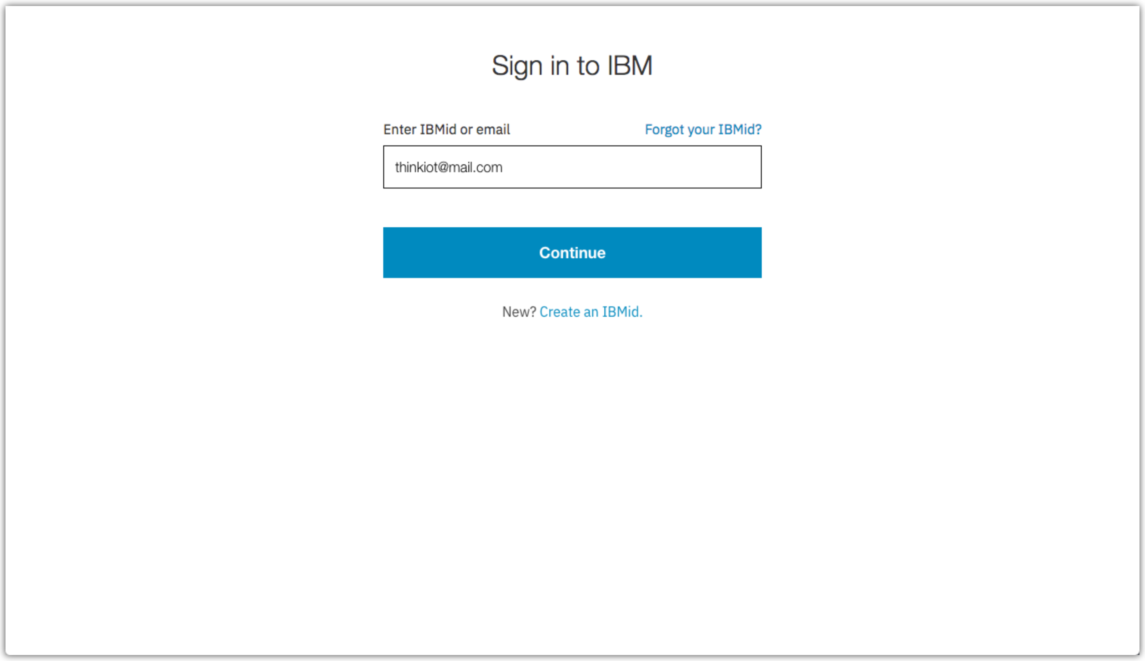


Welcome to IBM Cloud, the home of 170+ unique services. Start building immediately.

© Copyright IBM Corp. 2014, 2017. All rights reserved.

3. Click on **Log in**

4. Enter the IBM ID

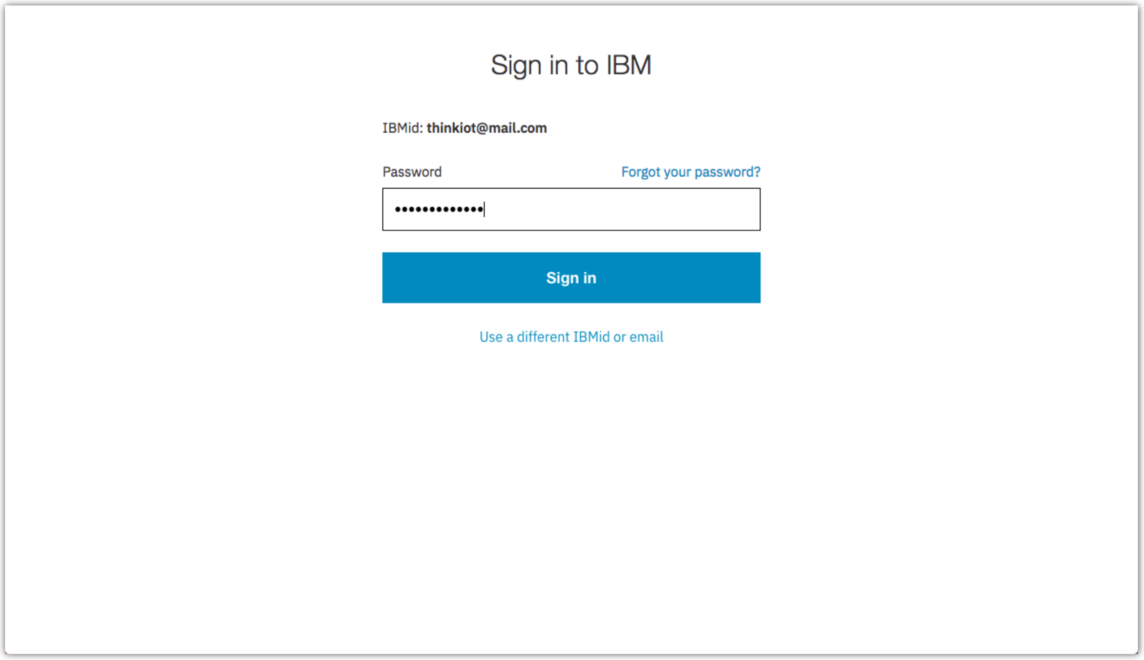


Sign in to IBM

Enter IBMid or email

thinkiot@mail.com

5. Enter the password and click **Sign in**



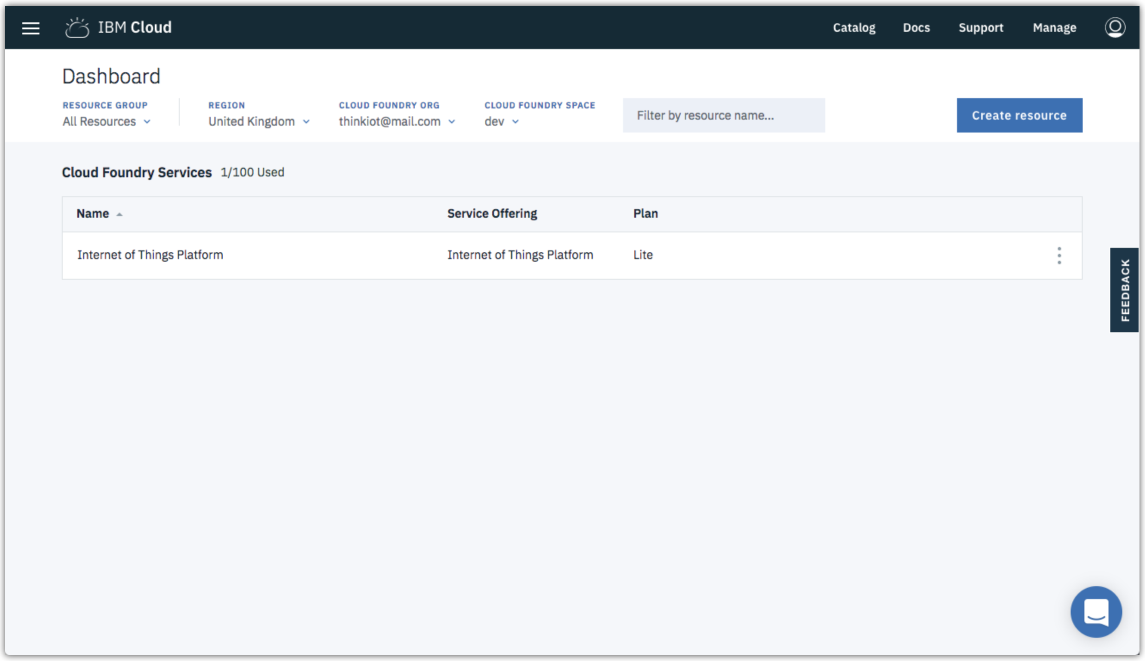
Sign in to IBM

IBMid: **thinkiot@mail.com**

Password

•••••••••••••

6. The IBM Bluemix Dashboard is loaded.



Dashboard

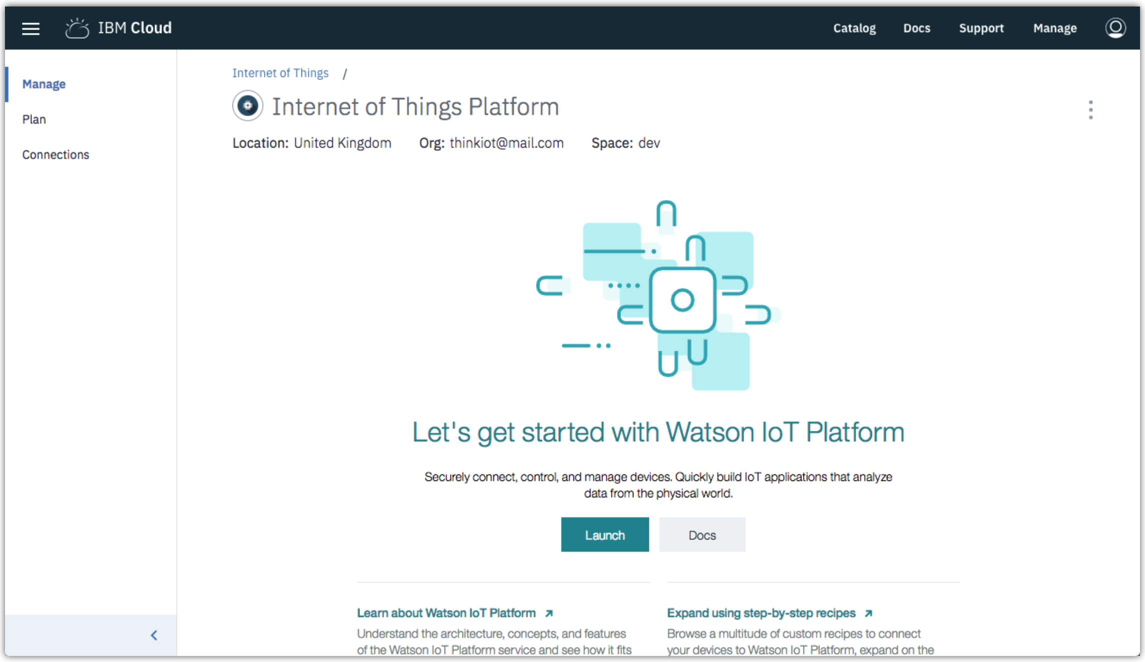
RESOURCE GROUP: All Resources
REGION: United Kingdom
CLOUD FOUNDRY ORG: thinkiot@mail.com
CLOUD FOUNDRY SPACE: dev

Filter by resource name...

Cloud Foundry Services 1/100 Used

Name	Service Offering	Plan
Internet of Things Platform	Internet of Things Platform	Lite

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



Internet of Things Platform

Location: United Kingdom Org: thinkiot@mail.com Space: dev

Let's get started with Watson IoT Platform

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

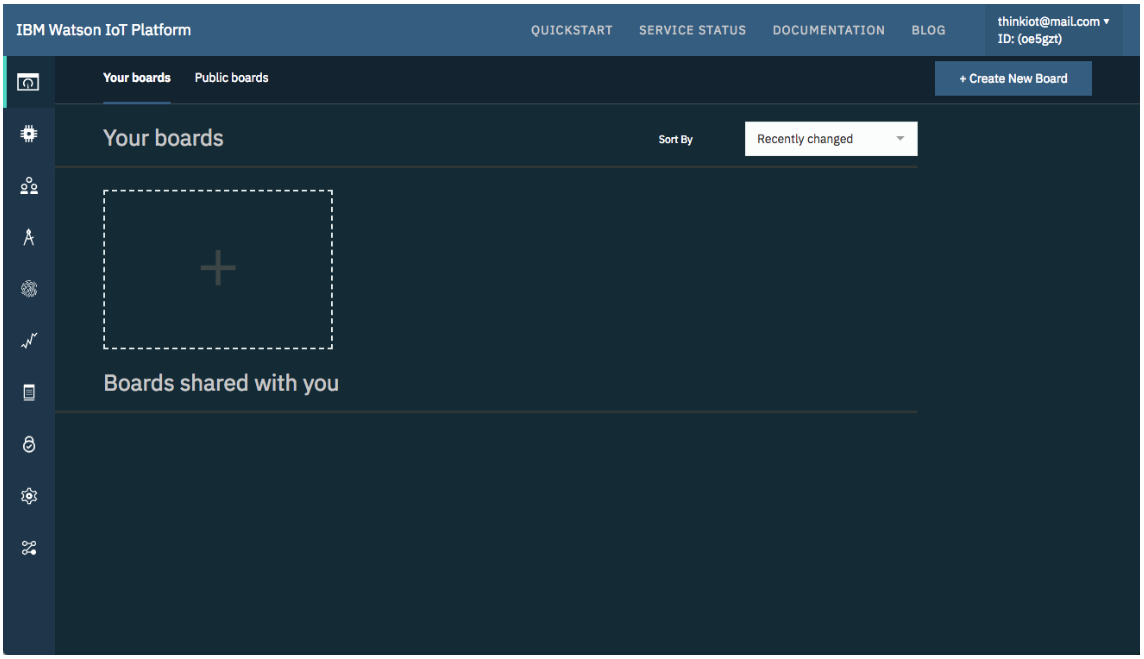
Learn about Watson IoT Platform ↗

Understand the architecture, concepts, and features of the Watson IoT Platform service and see how it fits

Expand using step-by-step recipes ↗

Browse a multitude of custom recipes to connect your devices to Watson IoT Platform, expand on the

8. Click **Launch** to open the IoT platform web interface.
   The Watson IoT Platform opens and shows the platform dashboard.



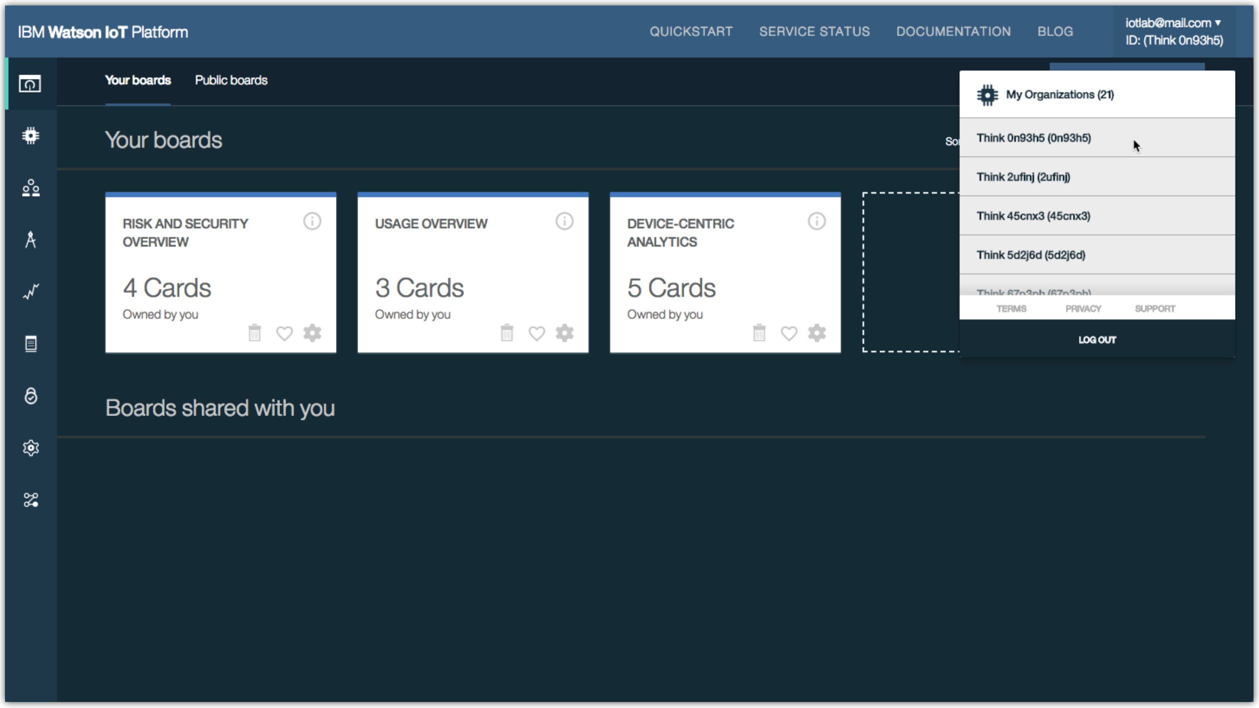
You have now successfully logged into IBM Bluemix and opened the IBM Watson IoT Platform service. You are now ready to switch to the IoT platform *organization* that you will use in this lab.

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.

- 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.

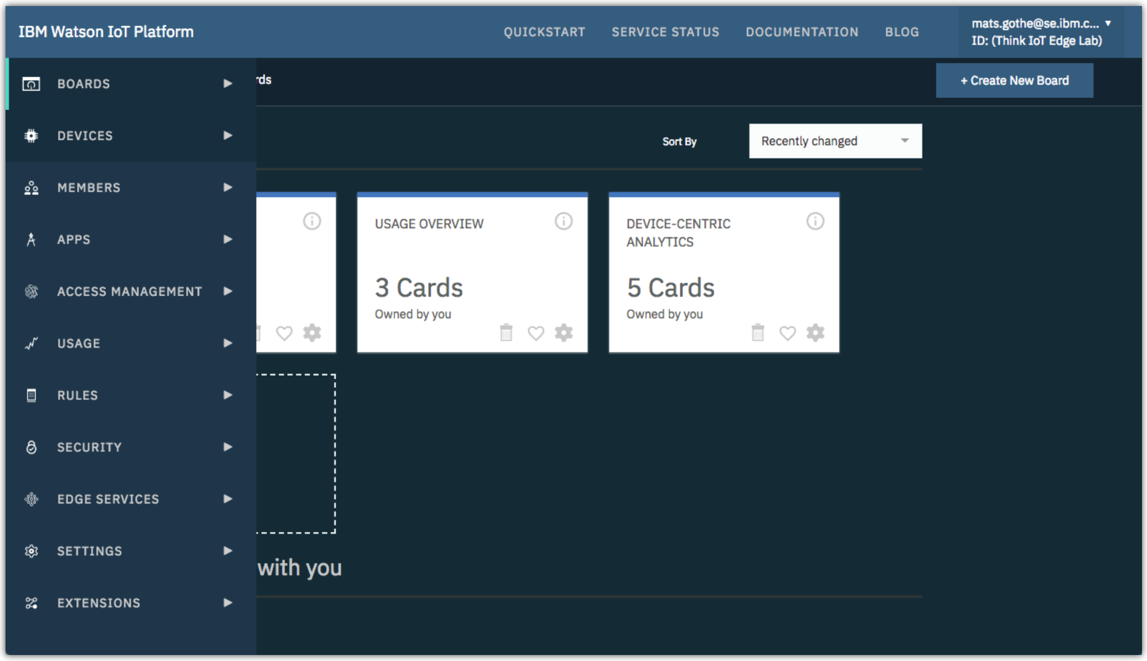


Overview of the Watson IoT Platform

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.

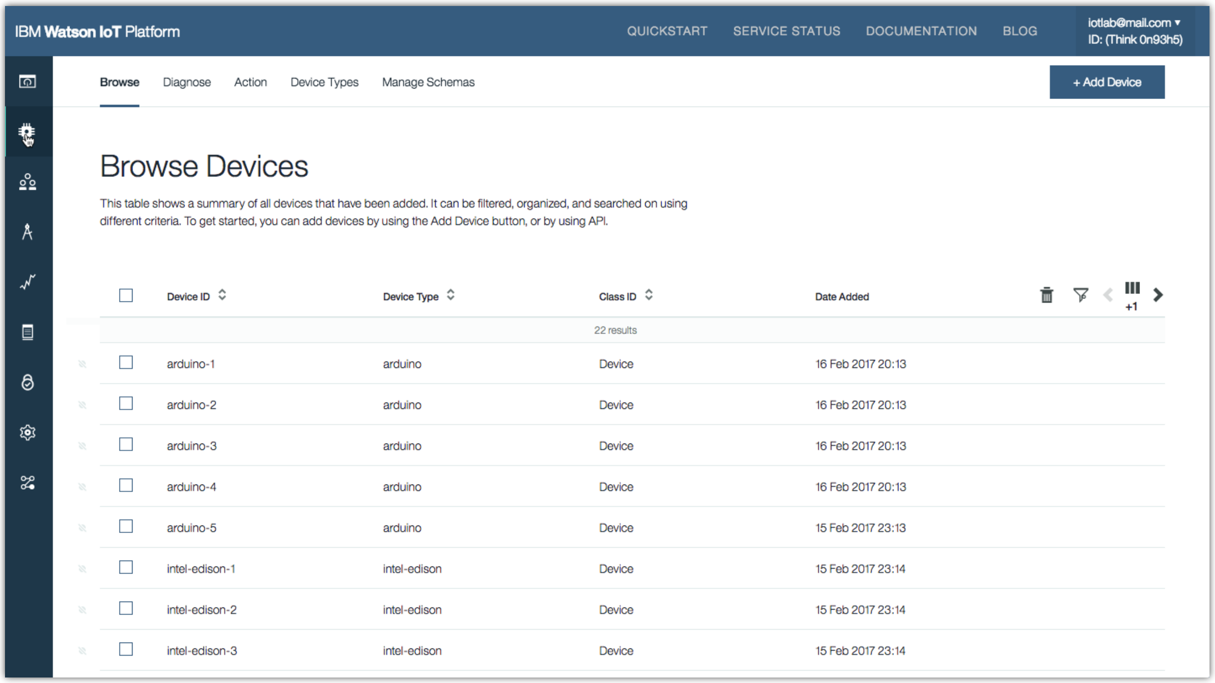
In this first section you will familiarize yourself with the IBM Watson IoT Platform user interface. The navigation bar on the left-hand side provides access to the capabilities of the platform

- 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
- Access Management – Roles and Permissions
- Usage – Metrics of usage
- Rules – Analytics rules and actions
- Security – Risk and Security Policies. We will explore details later in this lab
- Edge Services – Catalog of Services configurable to run on edge gateways
- 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 or Device Type. Try it!

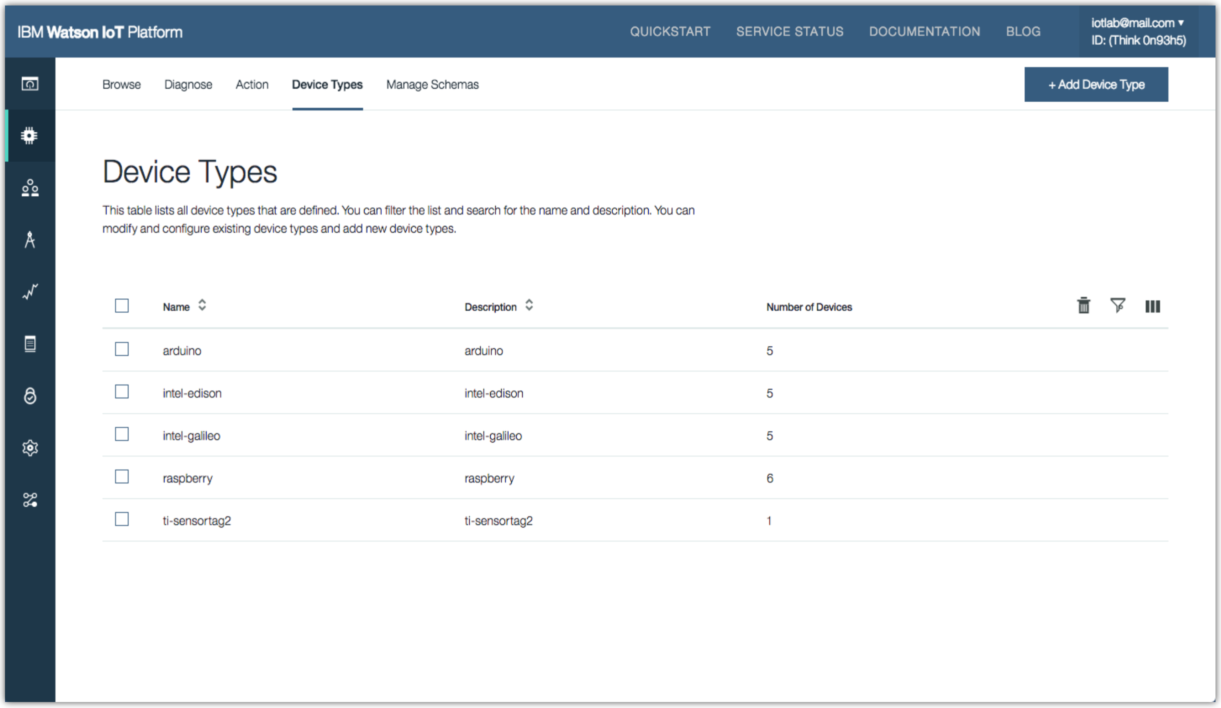


Browse Devices

This table shows a summary of all devices that have been added. It can be filtered, organized, and searched on using different criteria. To get started, you can add devices by using the Add Device button, or by using API.

□	Device ID	Device Type	Class ID	Date Added
			22 results	
□	arduino-1	arduino	Device	16 Feb 2017 20:13
□	arduino-2	arduino	Device	16 Feb 2017 20:13
□	arduino-3	arduino	Device	16 Feb 2017 20:13
□	arduino-4	arduino	Device	16 Feb 2017 20:13
□	arduino-5	arduino	Device	15 Feb 2017 23:13
□	intel-edison-1	intel-edison	Device	15 Feb 2017 23:14
□	intel-edison-2	intel-edison	Device	15 Feb 2017 23:14
□	intel-edison-3	intel-edison	Device	15 Feb 2017 23:14

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.

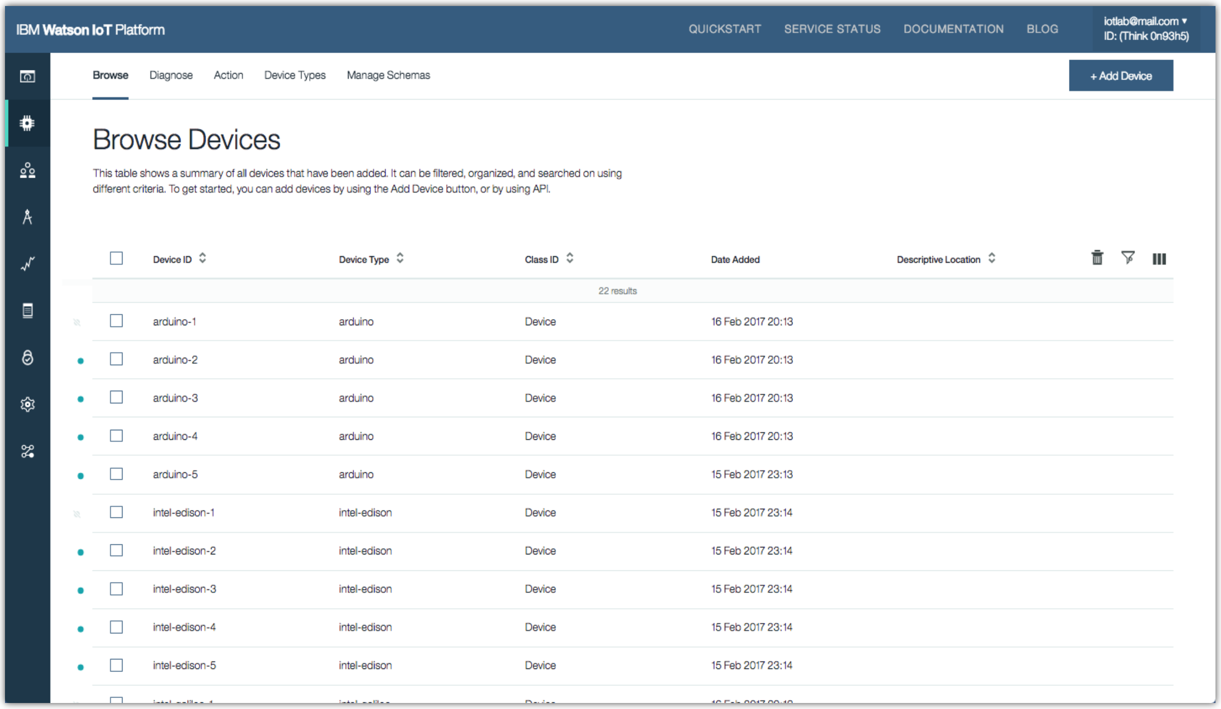


Device Types

This table lists all device types that are defined. You can filter the list and search for the name and description. You can modify and configure existing device types and add new device types.

□	Name	Description	Number of Devices
□	arduino	arduino	5
□	intel-edison	intel-edison	5
□	intel-galileo	intel-galileo	5
□	raspberry	raspberry	6
□	ti-sensortag2	ti-sensortag2	1

4. Return to the Devices page by clicking on **Browse**. Locate the device named “Arduino-5” in the list.



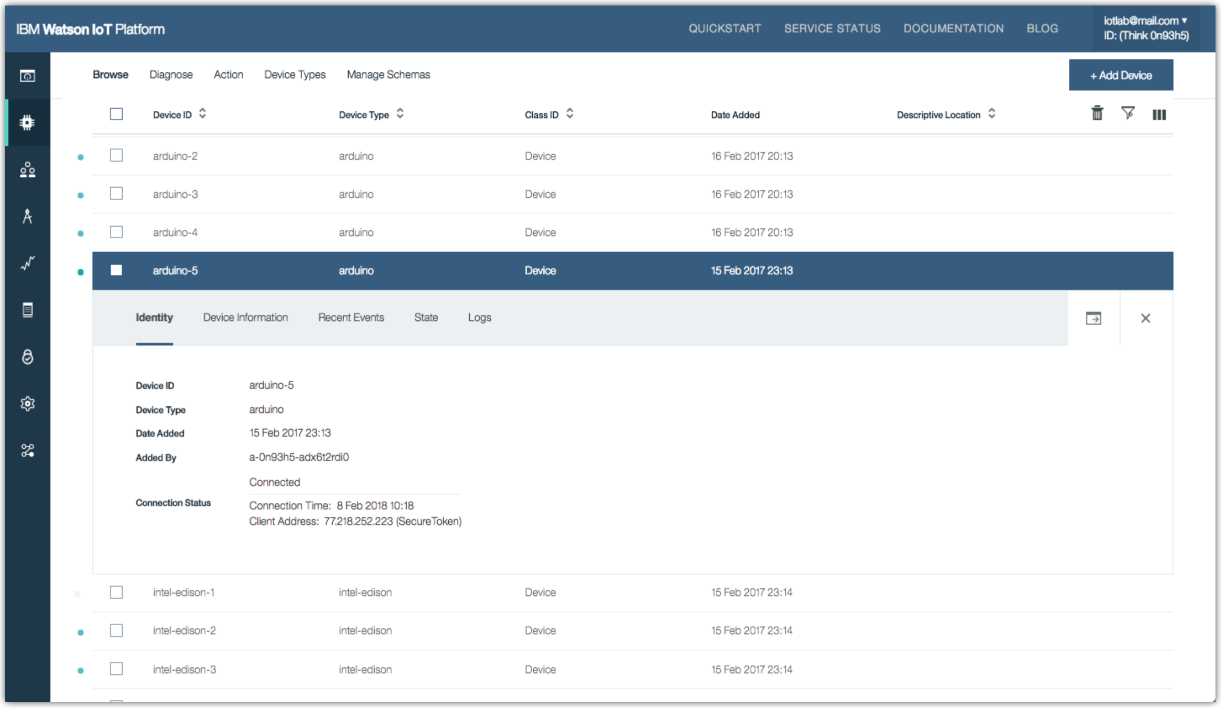
Browse Devices

This table shows a summary of all devices that have been added. It can be filtered, organized, and searched on using different criteria. To get started, you can add devices by using the Add Device button, or by using API.

22 results

	□	Device ID	Device Type	Class ID	Date Added	Descriptive Location
	□	arduino-1	arduino	Device	16 Feb 2017 20:13	
●	□	arduino-2	arduino	Device	16 Feb 2017 20:13	
●	□	arduino-3	arduino	Device	16 Feb 2017 20:13	
●	□	arduino-4	arduino	Device	16 Feb 2017 20:13	
●	□	arduino-5	arduino	Device	15 Feb 2017 23:13	
	□	intel-edison-1	intel-edison	Device	15 Feb 2017 23:14	
●	□	intel-edison-2	intel-edison	Device	15 Feb 2017 23:14	
●	□	intel-edison-3	intel-edison	Device	15 Feb 2017 23:14	
●	□	intel-edison-4	intel-edison	Device	15 Feb 2017 23:14	
●	□	intel-edison-5	intel-edison	Device	15 Feb 2017 23:14	

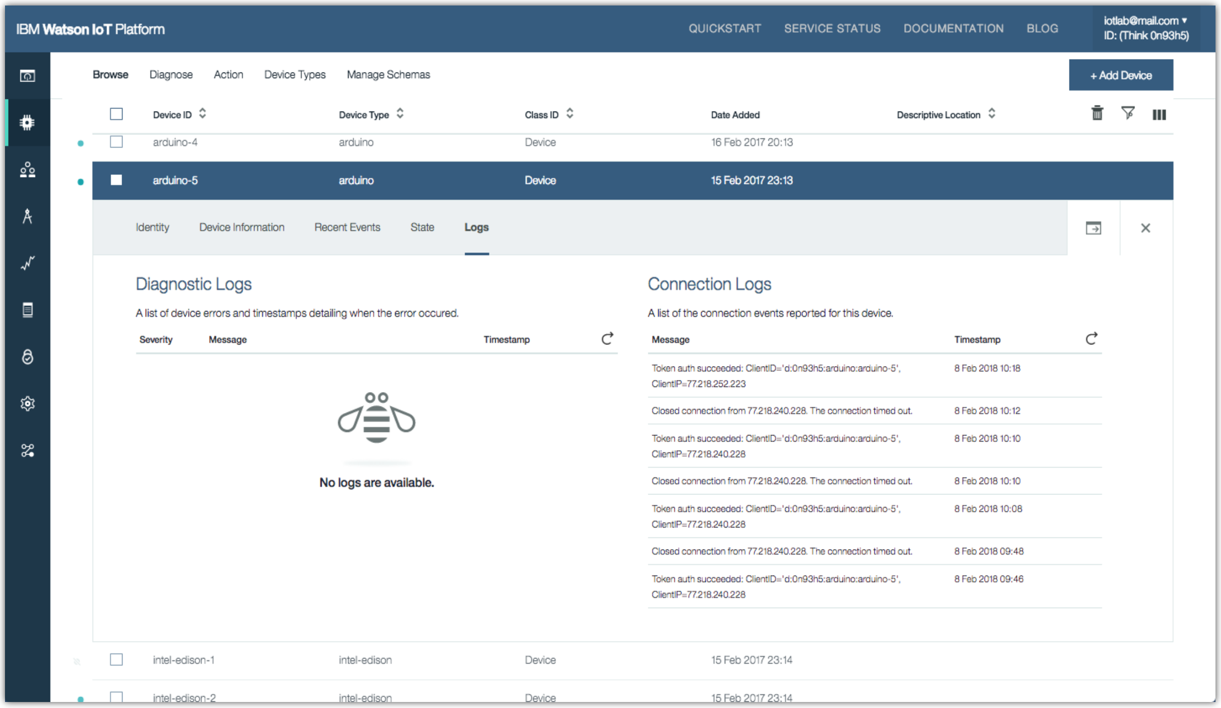
5. Click on the “Arduino-5” row in the list to open the Device Details card.



☐	Device ID	Device Type	Class ID	Date Added	Descriptive Location
☐	arduino-2	arduino	Device	16 Feb 2017 20:13	
☐	arduino-3	arduino	Device	16 Feb 2017 20:13	
☐	arduino-4	arduino	Device	16 Feb 2017 20:13	
■	arduino-5	arduino	Device	15 Feb 2017 23:13	
☐	intel-edison-1	intel-edison	Device	15 Feb 2017 23:14	
☐	intel-edison-2	intel-edison	Device	15 Feb 2017 23:14	
☐	intel-edison-3	intel-edison	Device	15 Feb 2017 23:14	

Device ID	arduino-5
Device Type	arduino
Date Added	15 Feb 2017 23:13
Added By	a-0n93h5-adx6t2rdl0
Connection Status	Connected Connection Time: 8 Feb 2018 10:18 Client Address: 77.218.252.223 (SecureToken)

6. On the **Identity** tab, look in the **Connection Status** section. Name a note of the **Client Address** the Arduino-5 device is connecting from. You will use this information later in this lab.
7. Select the **Logs** tab. View the connection history and the authentication information for the device.



	Device ID	Device Type	Class ID	Date Added	Descriptive Location
□	arduino-4	arduino	Device	16 Feb 2017 20:13	
■	arduino-5	arduino	Device	15 Feb 2017 23:13	
□	intel-edison-1	intel-edison	Device	15 Feb 2017 23:14	
□	intel-edison-2	intel-edison	Device	15 Feb 2017 23:14	

Diagnostic Logs

A list of device errors and timestamps detailing when the error occured.

Severity	Message	Timestamp

No logs are available.

Connection Logs

A list of the connection events reported for this device.

Message	Timestamp
Token auth succeeded: ClientID='d:0n93h5:arduino:arduino-5', ClientIP=77.218.252.223	8 Feb 2018 10:18
Closed connection from 77.218.240.228. The connection timed out.	8 Feb 2018 10:12
Token auth succeeded: ClientID='d:0n93h5:arduino:arduino-5', ClientIP=77.218.240.228	8 Feb 2018 10:10
Closed connection from 77.218.240.228. The connection timed out.	8 Feb 2018 10:10
Token auth succeeded: ClientID='d:0n93h5:arduino:arduino-5', ClientIP=77.218.240.228	8 Feb 2018 10:08
Closed connection from 77.218.240.228. The connection timed out.	8 Feb 2018 09:48
Token auth succeeded: ClientID='d:0n93h5:arduino:arduino-5', ClientIP=77.218.240.228	8 Feb 2018 09:46

8. 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.

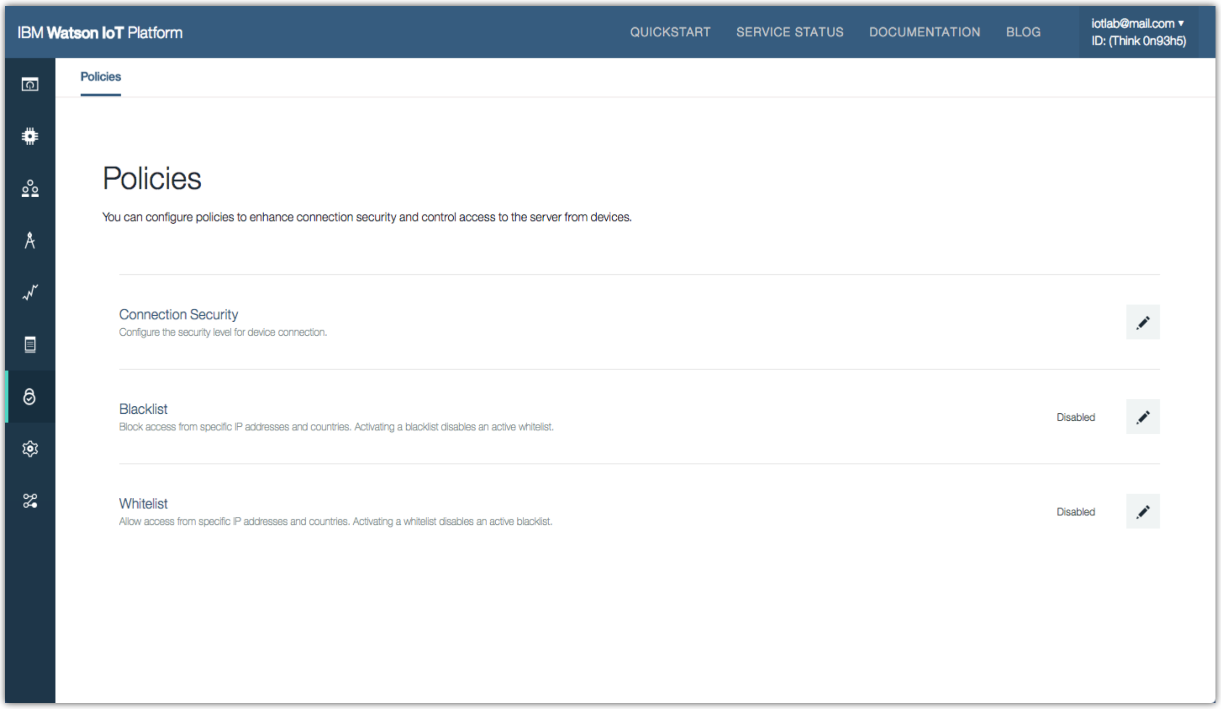
Configuring a Connection Security Policy

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

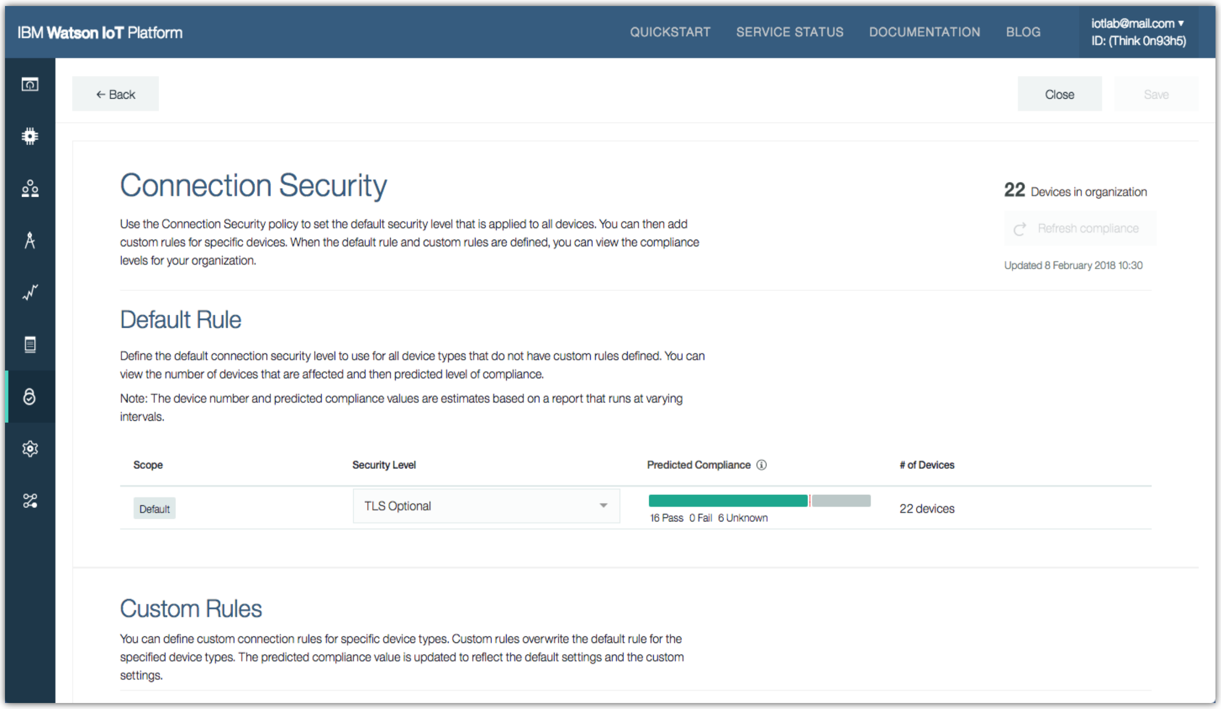
You can configure policies to enhance connection security and control access to the server from devices.

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 the pen icon ✎ on **Connection Security** policy.
   The Connection Security Policy page loads.



IBM **Watson IoT** Platform

QUICKSTART SERVICE STATUS DOCUMENTATION BLOG

iotlab@mail.com ▾
ID: (Think 0n93h5)

← Back

Close Save

Connection Security

22 Devices in organization

Refresh compliance

Updated 8 February 2018 10:30

Use the Connection Security policy to set the default security level that is applied to all devices. You can then add custom rules for specific devices. When the default rule and custom rules are defined, you can view the compliance levels for your organization.

Default Rule

Define the default connection security level to use for all device types that do not have custom rules defined. You can view the number of devices that are affected and then predicted level of compliance.

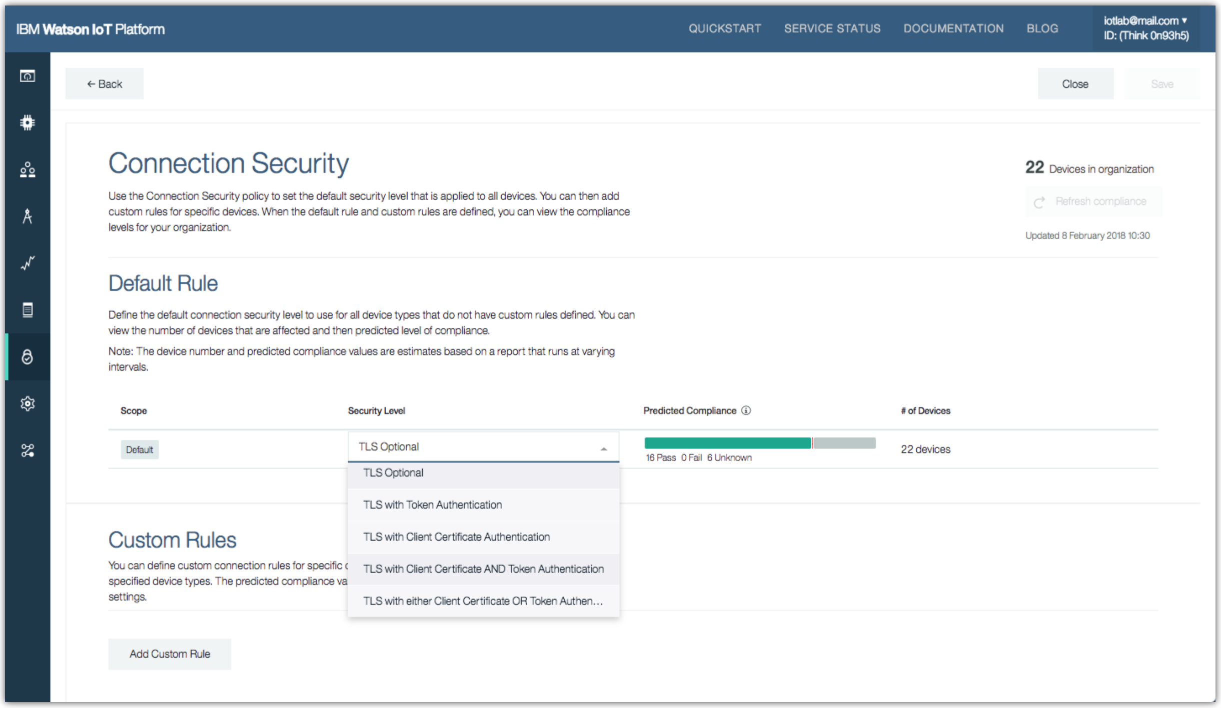
Note: The device number and predicted compliance values are estimates based on a report that runs at varying intervals.

Scope	Security Level	Predicted Compliance ⓘ	# of Devices
Default	TLS Optional ▾	16 Pass 0 Fail 6 Unknown	22 devices

Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

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



IBM **Watson IoT** Platform

QUICKSTART SERVICE STATUS DOCUMENTATION BLOG

iotlab@mail.com ▾
ID: (Think 0n93h5)

← Back

Close Save

Connection Security

22 Devices in organization

Refresh compliance

Updated 8 February 2018 10:30

Use the Connection Security policy to set the default security level that is applied to all devices. You can then add custom rules for specific devices. When the default rule and custom rules are defined, you can view the compliance levels for your organization.

Default Rule

Define the default connection security level to use for all device types that do not have custom rules defined. You can view the number of devices that are affected and then predicted level of compliance.

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

Scope	Security Level	Predicted Compliance ⓘ	# of Devices
Default	TLS Optional ▴	16 Pass 0 Fail 6 Unknown	22 devices

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 Authen…

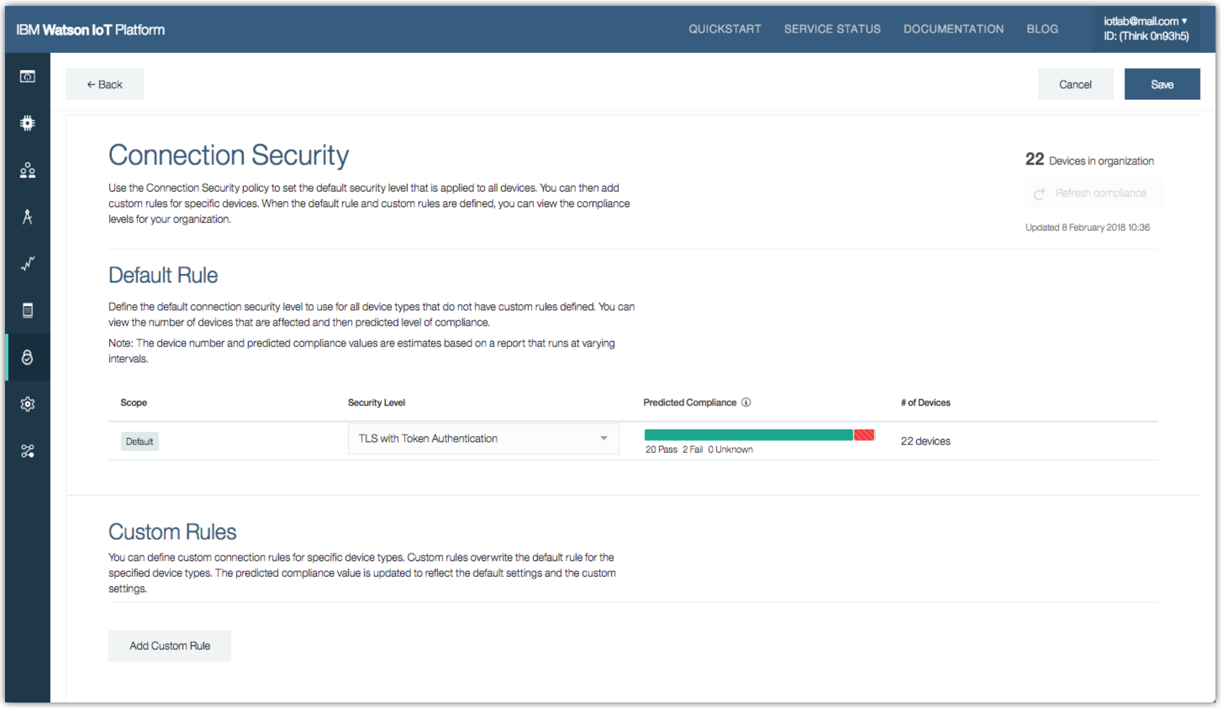
Custom Rules

You can define custom connection rules for specific c… specified device types. The predicted compliance va… settings.

Add Custom Rule

4. Try different Security Levels, like “TLS with Token Authentication”. After a new security level is selected, click **Refresh Compliance** button in the **Predicted Compliance** column.

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



Connection Security

Use the Connection Security policy to set the default security level that is applied to all devices. You can then add custom rules for specific devices. When the default rule and custom rules are defined, you can view the compliance levels for your organization.

22 Devices in organization

Updated 8 February 2018 10:36

Default Rule

Define the default connection security level to use for all device types that do not have custom rules defined. You can view the number of devices that are affected and then predicted level of compliance.

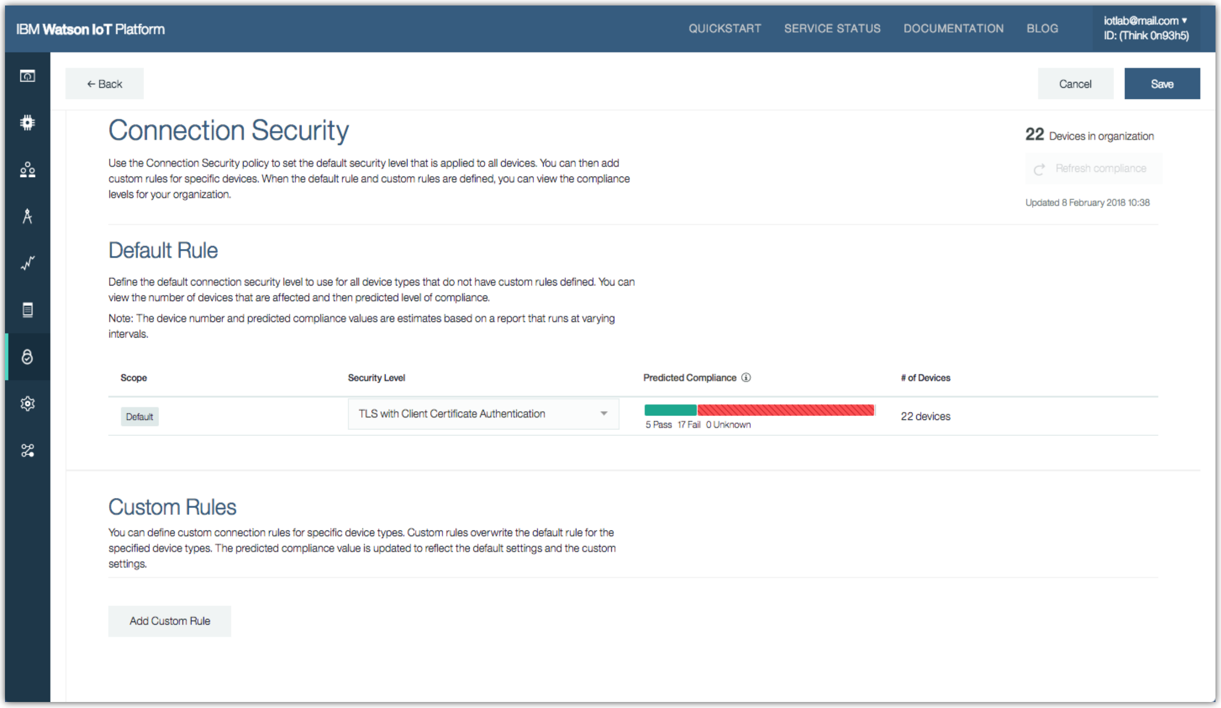
Note: The device number and predicted compliance values are estimates based on a report that runs at varying intervals.

Scope	Security Level	Predicted Compliance ⓘ	# of Devices
Default	TLS with Token Authentication ▾	20 Pass 2 Fail 0 Unknown	22 devices

Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

5. After trying different settings, set the Default Security Level to “TLS with Client Certificate Authentication”



Connection Security

Use the Connection Security policy to set the default security level that is applied to all devices. You can then add custom rules for specific devices. When the default rule and custom rules are defined, you can view the compliance levels for your organization.

22 Devices in organization

Updated 8 February 2018 10:38

Default Rule

Define the default connection security level to use for all device types that do not have custom rules defined. You can view the number of devices that are affected and then predicted level of compliance.

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

Scope	Security Level	Predicted Compliance ⓘ	# of Devices
Default	TLS with Client Certificate Authentication ▾	5 Pass 17 Fail 0 Unknown	22 devices

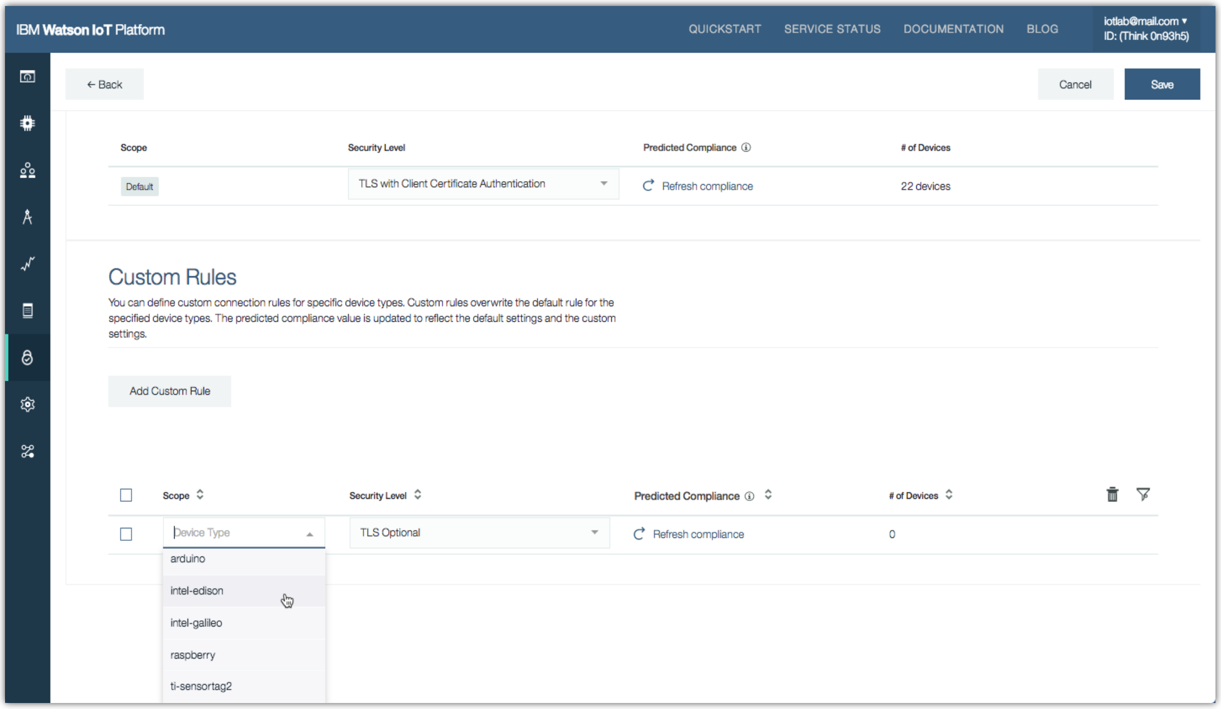
Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

Applying Custom Connection Security Rules

The custom connection rules 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 Rules, click on **Add Custom Rule**. A new row is added to the table below.



Scope	Security Level	Predicted Compliance ⓘ	# of Devices
Default	TLS with Client Certificate Authentication ▾	Refresh compliance	22 devices

Custom Rules

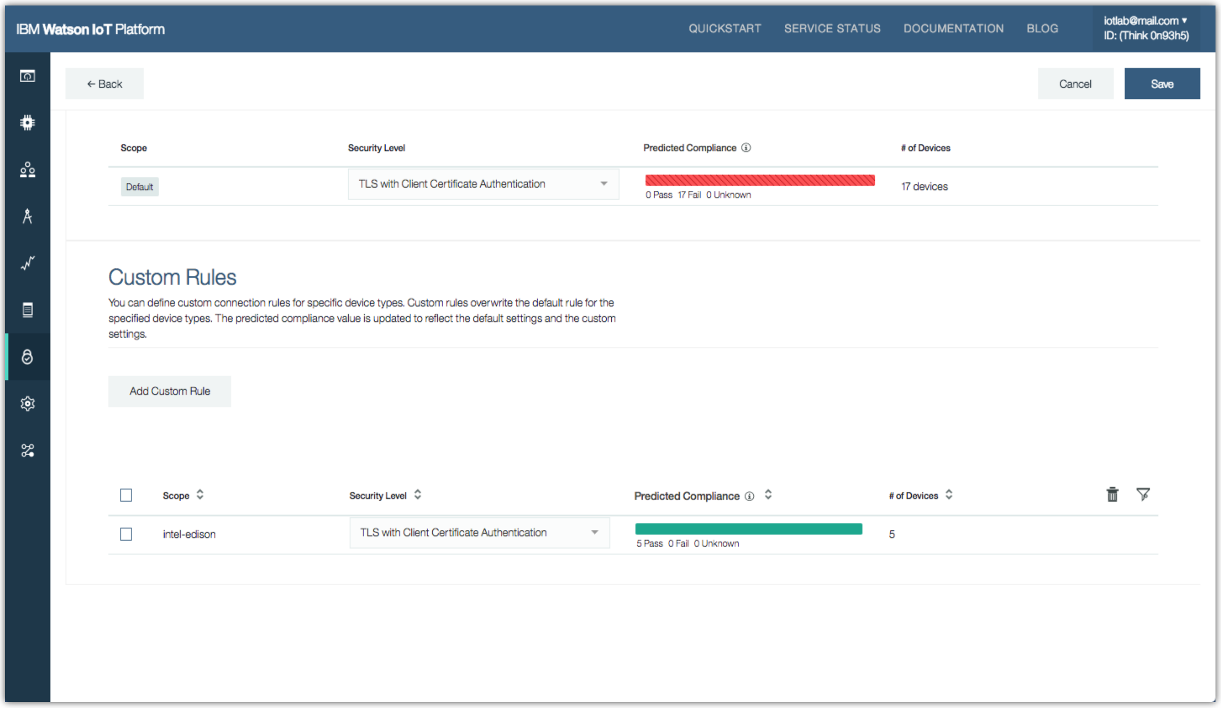
You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

□	Scope	Security Level	Predicted Compliance ⓘ	# of Devices
□	Device Type ▴	TLS Optional ▾	Refresh compliance	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.



Scope	Security Level	Predicted Compliance ⓘ	# of Devices
Default	TLS with Client Certificate Authentication ▾	🟥 0 Pass 17 Fail 0 Unknown	17 devices

Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

□	Scope	Security Level	Predicted Compliance ⓘ	# of Devices
□	intel-edison	TLS with Client Certificate Authentication ▾	🟩 5 Pass 0 Fail 0 Unknown	5

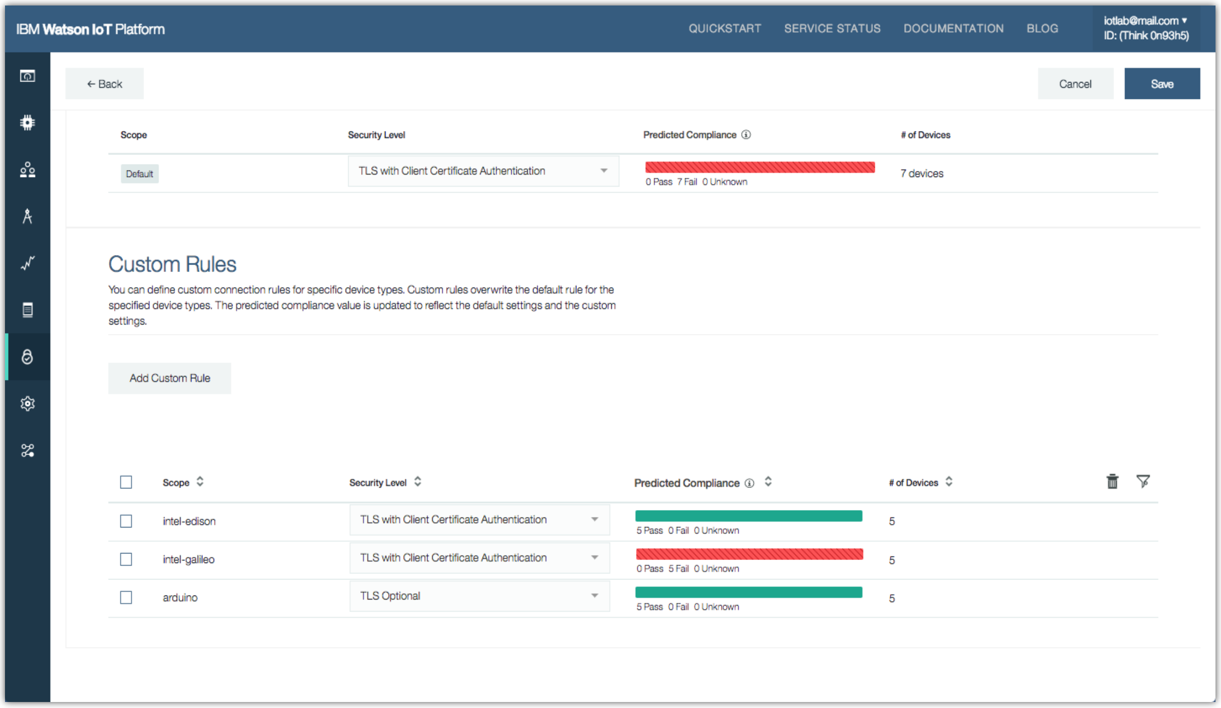
4. Repeat the step and add a custom connection security for the “intel-galileo” device type. Set the security level to “TLS with Client Certificate Authentication”.

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.



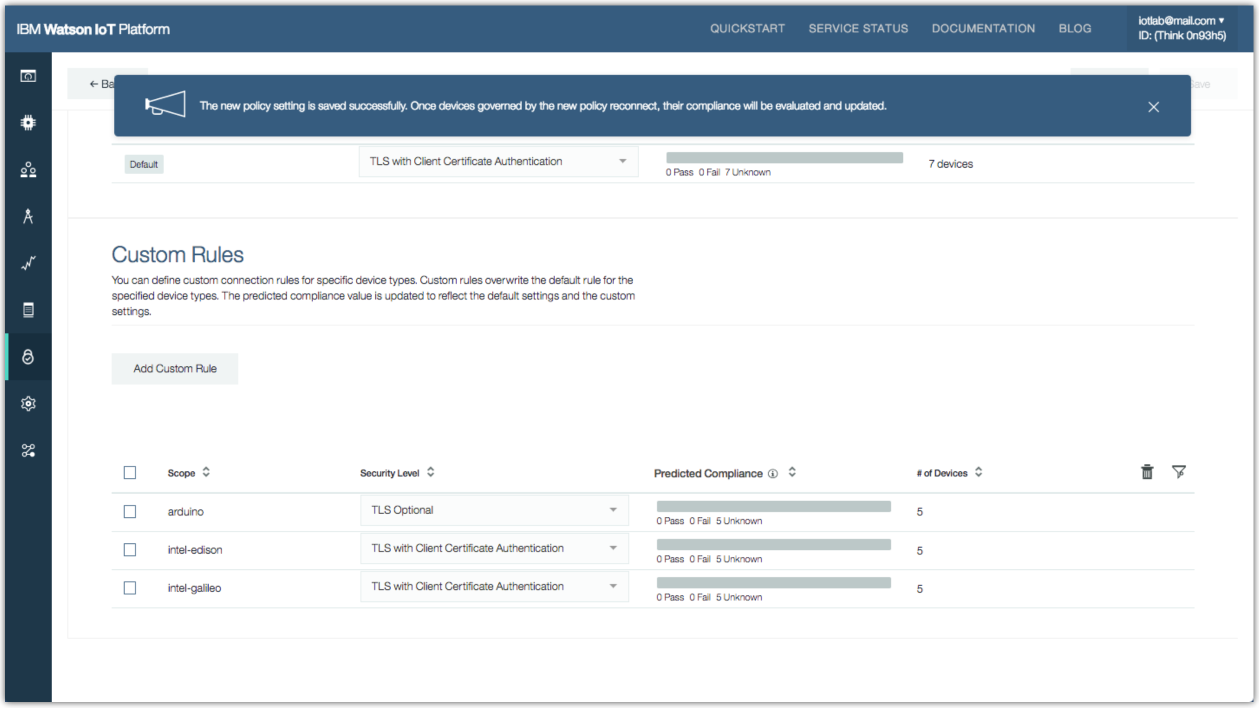
Scope	Security Level	Predicted Compliance ⓘ	# of Devices
Default	TLS with Client Certificate Authentication	0 Pass 7 Fail 0 Unknown	7 devices

Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

□	Scope	Security Level	Predicted Compliance ⓘ	# of Devices
□	intel-edison	TLS with Client Certificate Authentication	5 Pass 0 Fail 0 Unknown	5
□	intel-galileo	TLS with Client Certificate Authentication	0 Pass 5 Fail 0 Unknown	5
□	arduino	TLS Optional	5 Pass 0 Fail 0 Unknown	5

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



The new policy setting is saved successfully. Once devices governed by the new policy reconnect, their compliance will be evaluated and updated.

Default	TLS with Client Certificate Authentication	0 Pass 0 Fail 7 Unknown	7 devices

Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

□	Scope	Security Level	Predicted Compliance	# of Devices
□	arduino	TLS Optional	0 Pass 0 Fail 5 Unknown	5
□	intel-edison	TLS with Client Certificate Authentication	0 Pass 0 Fail 5 Unknown	5
□	intel-galileo	TLS with Client Certificate Authentication	0 Pass 0 Fail 5 Unknown	5

8. Note the message after saving.

> The new policy setting is saved successfully. Once devices governed by the new policy reconnect, their compliance will be evaluated and updated.

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).

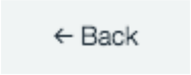
You have now completed the steps to preview and update the connection security policy. While your IoT platform organization is updating the device connection information you will explore the Blacklist and Whitelist Policy.

Configuring a Blacklist / Whitelist Policy

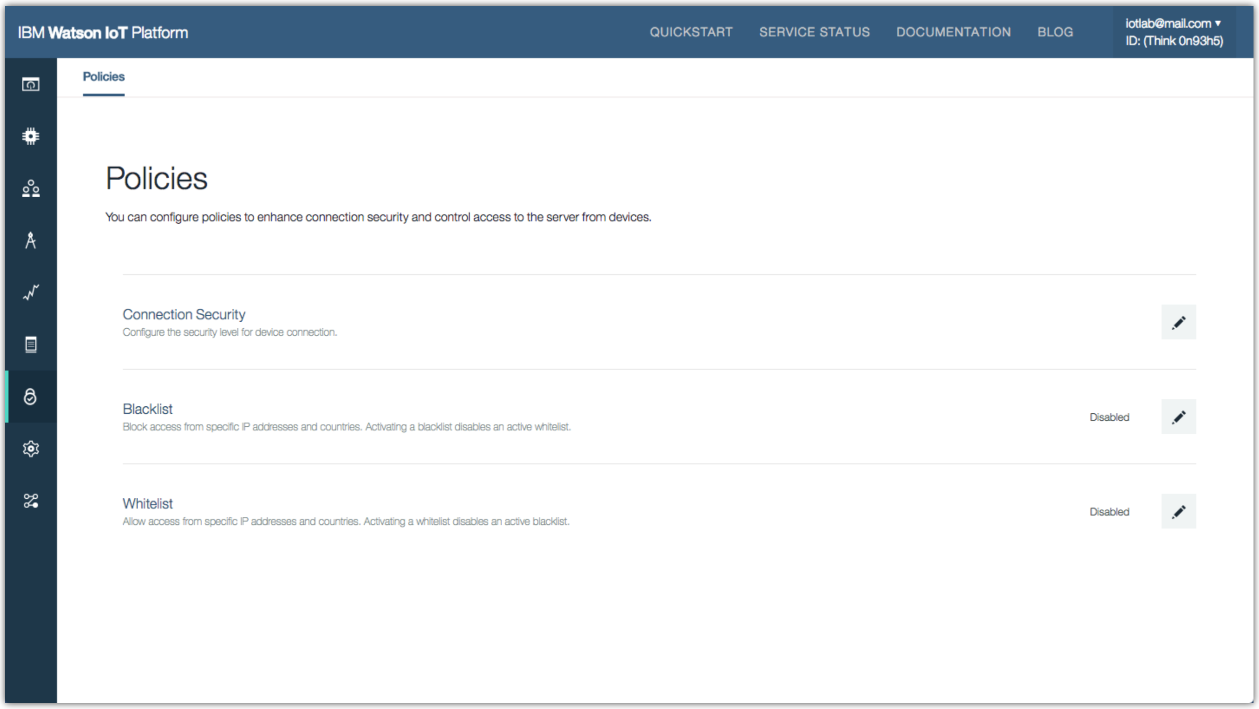
Your organization can restrict access to the server from certain devices by using a blacklist or a whitelist to grant server access to specific devices. A blacklist identifies all of the IP addresses, CIDRs, or countries that are to be denied server access, while a whitelist gives explicit access to 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. Click the **Back** button, or Choose **Security** from the left-hand navigator



2. Open **Blacklist** policy by clicking on the pen icon ✏



Policies

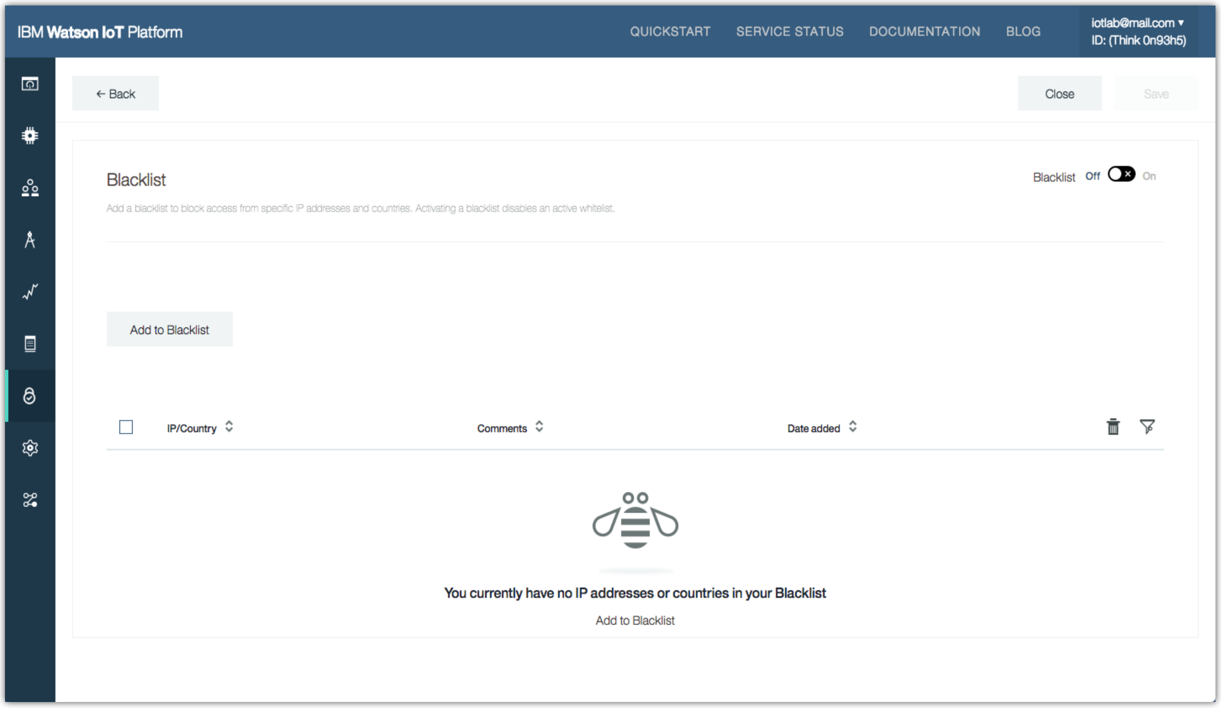
You can configure policies to enhance connection security and control access to the server from devices.

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

3. On the Blacklist policy, click **Add to Blacklist**.



IBM Watson IoT Platform QUICKSTART SERVICE STATUS DOCUMENTATION BLOG iotlab@mail.com ▾ ID: (Think 0n93h5)

← Back Close Save

Blacklist

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

Blacklist Off On

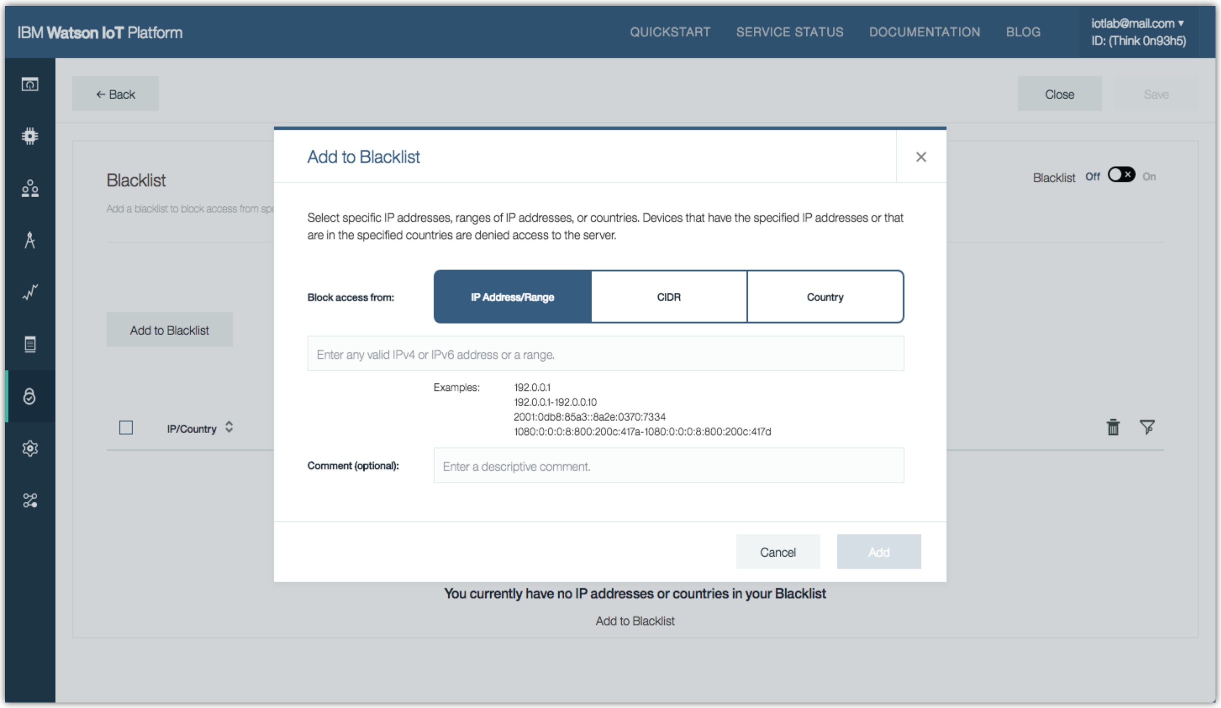
Add to Blacklist

□ IP/Country Comments Date added

You currently have no IP addresses or countries in your Blacklist

Add to Blacklist

4. 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

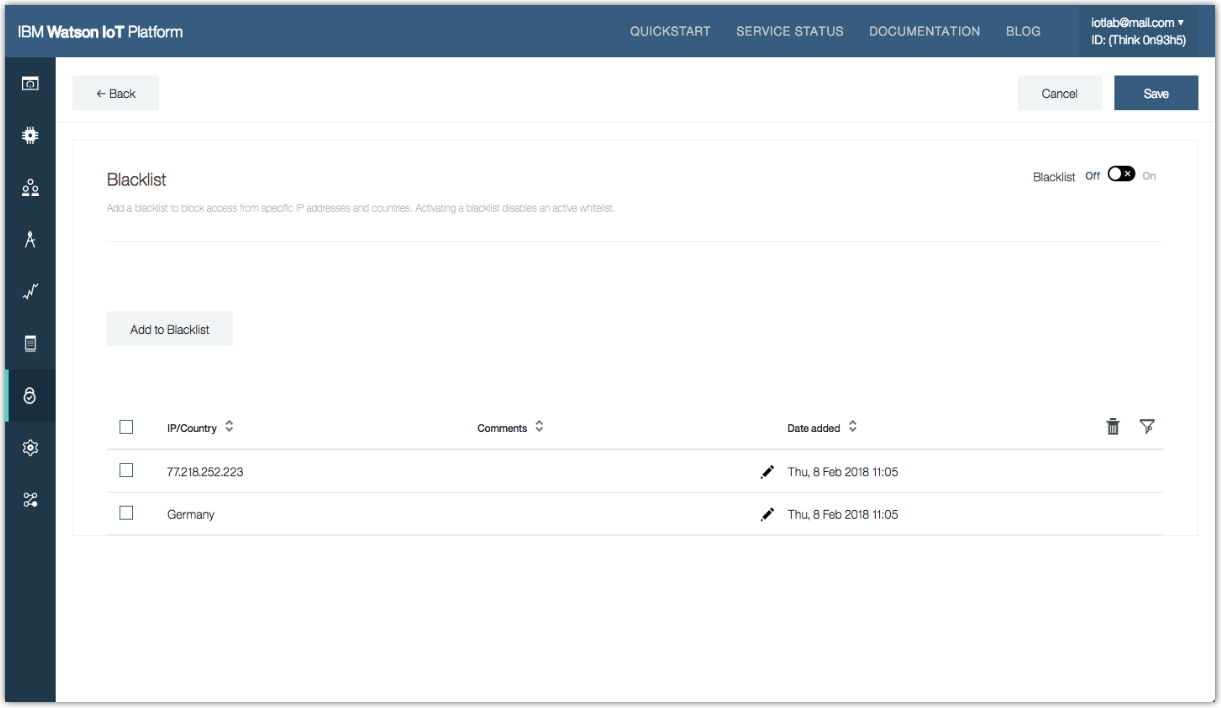
Enter any valid IPv4 or IPv6 address or a range.

Examples: 192.0.0.1
192.0.0.1-192.0.0.10
2001:0db8:85a3::8a2e:0370:7334
1080:0:0:0:8:800:200c:417a-1080:0:0:0:8:800:200c:417d

Comment (optional): Enter a descriptive comment.

Cancel Add

5. On the **IP Address/Range** tab, enter the IP address to the “arduino-5” device that you made a note of in an earlier section of the lab.
6. Click **Add** to block devices connect from this IP address.



Blacklist

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

Blacklist Off ● On

□	IP/Country	Comments	Date added
□	77.218.252.223		Thu, 8 Feb 2018 11:05
□	Germany		Thu, 8 Feb 2018 11:05

Note: There are options to block an IP rage or a Country.

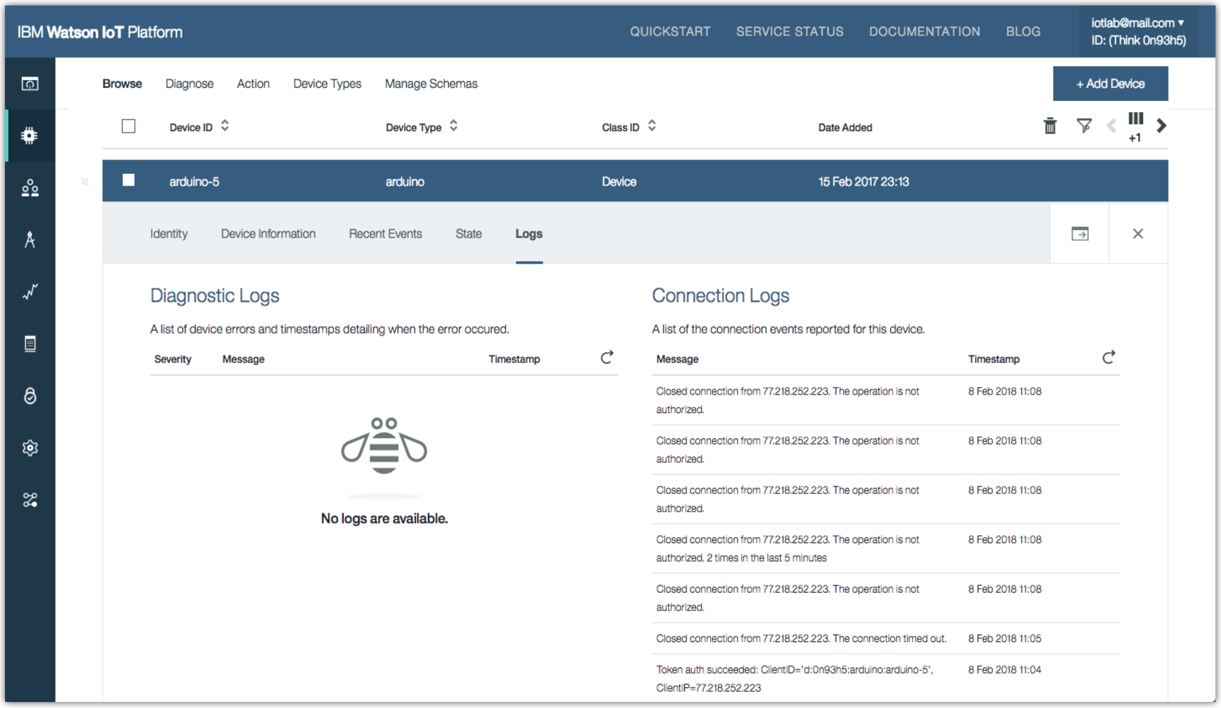
- Use the **CIDR** tab to enter a Classless Inter-Domain Routing (CIDR) notated block.
- Use the **Country** tab, enter or select countries from which you want to block all devices.

7. Once you have completed the blacklist settings, flip the **Enable Blacklist** switch to On.
8. Click **Save**.

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

9. Return to the device details for the ‘Arduino-5’ device.
   Select the **Devices** section in the navigator, choose **Browse**, locate and select the ‘Arduino-5’ device in the list of devices.
10. On the ‘Arduino-5’ device, select the **Logs** tab.
11. View the **Connection Logs** section.

    Note: The connections from the ‘Arduino-5’ device are now rejected by the IoT Platform as the IP address has been blocked.



□	Device ID	Device Type	Class ID	Date Added
■	arduino-5	arduino	Device	15 Feb 2017 23:13

Diagnostic Logs

A list of device errors and timestamps detailing when the error occured.

Severity	Message	Timestamp

No logs are available.

Connection Logs

A list of the connection events reported for this device.

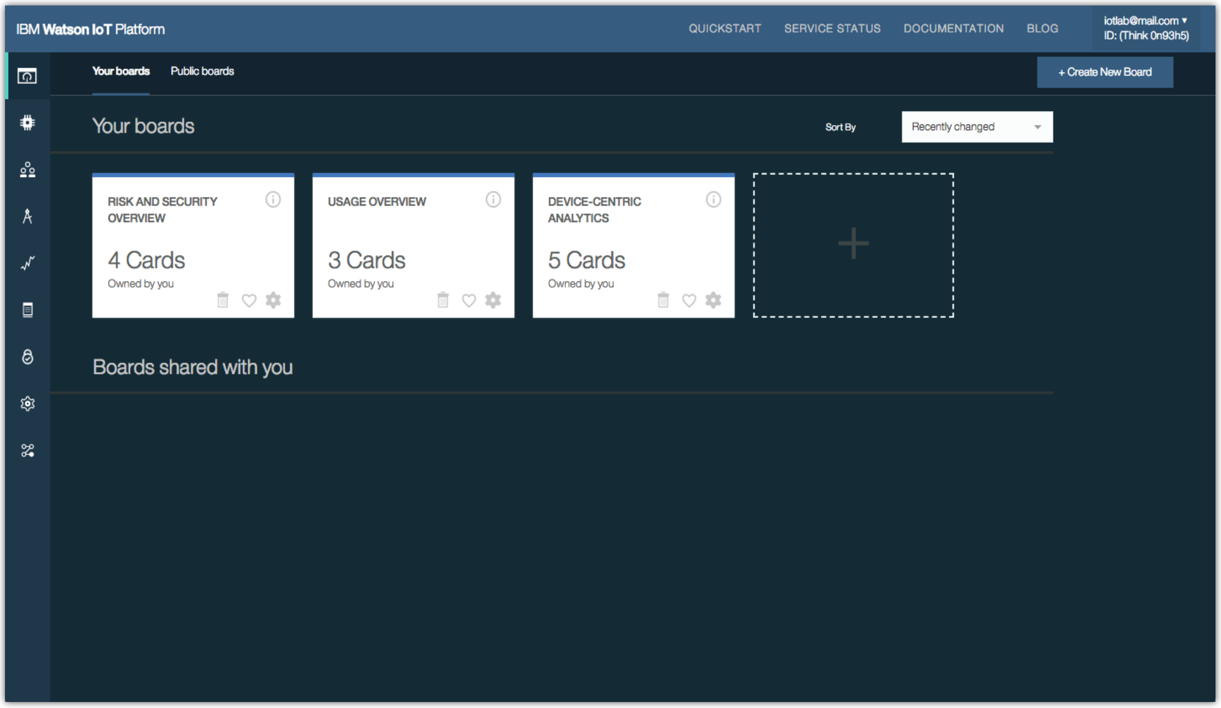
Message	Timestamp
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized. 2 times in the last 5 minutes	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The connection timed out.	8 Feb 2018 11:05
Token auth succeeded: ClientID='d:0n93h5:arduino:arduino-5', ClientIP=77.218.252.223	8 Feb 2018 11:04

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.

To view compliance

1. Choose **Boards** from the navigator. The IoT Platform dashboard loads



IBM Watson IoT Platform

QUICKSTART SERVICE STATUS DOCUMENTATION BLOG

iotlab@mail.com ▾
ID: (Think 0n93h5)

Your boards Public boards

+ Create New Board

Your boards

Sort By Recently changed

RISK AND SECURITY OVERVIEW
4 Cards
Owned by you

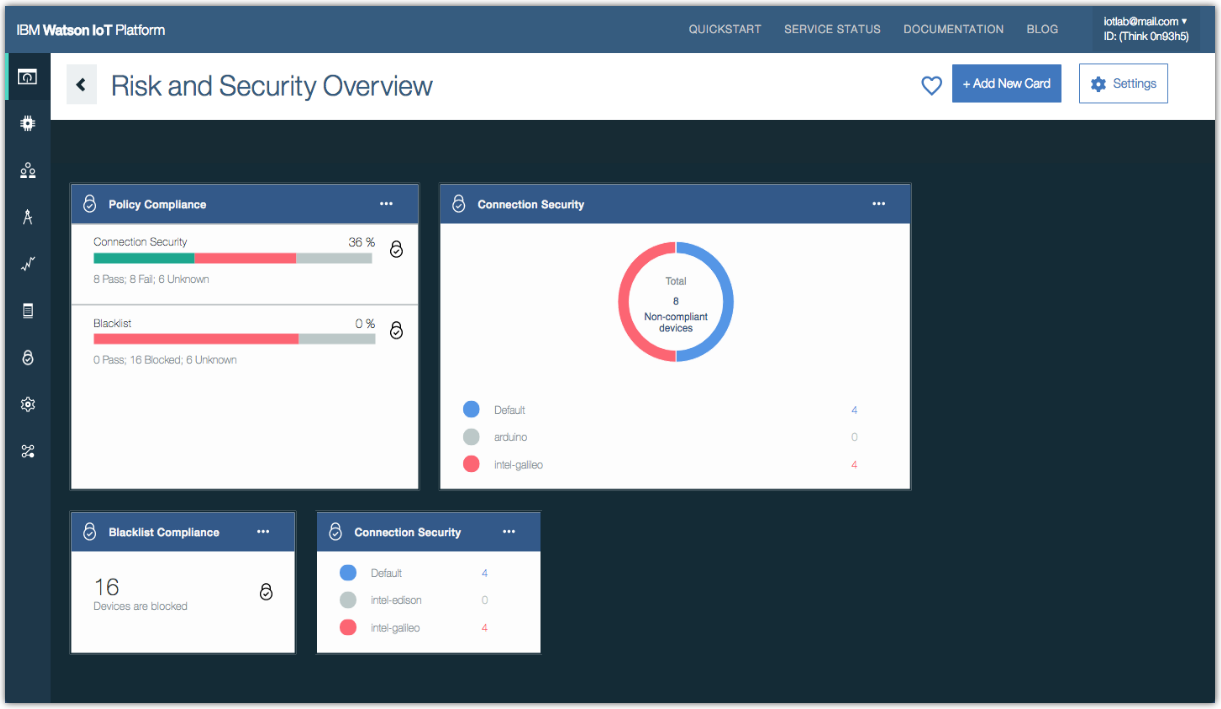
USAGE OVERVIEW
3 Cards
Owned by you

DEVICE-CENTRIC ANALYTICS
5 Cards
Owned by you

+

Boards shared with you

2. Click on the **Risk and Security Overview** board.



IBM Watson IoT Platform

QUICKSTART SERVICE STATUS DOCUMENTATION BLOG

iotlab@mail.com ▾
ID: (Think 0n93h5)

Risk and Security Overview

+ Add New Card Settings

Policy Compliance

Connection Security 36 %
8 Pass; 8 Fail; 6 Unknown

Blacklist 0 %
0 Pass; 16 Blocked; 6 Unknown

Connection Security

Total
8
Non-compliant devices

● Default	4
● arduino	0
● intel-galileo	4

Blacklist Compliance

16
Devices are blocked

Connection Security

● Default	4
● intel-edison	0
● intel-galileo	4

3. A summary of the Policy Compliance is shown on the cards.

You have now completed the steps to configure Blacklist and Whitelist Policy.

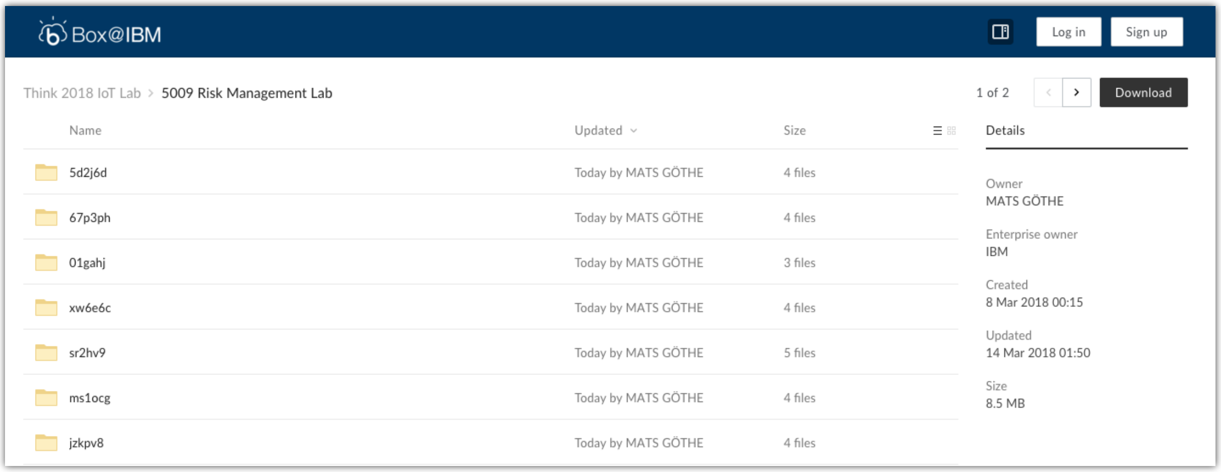
Downloading your Certificates

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/thinkiot

   The Box shared folder page opens
3. Open the folder **5009 Risk Management Lab**
4. A subfolder has been created for each organization. Look for a folder with the organization id that has been assigned to your workstation.



Think 2018 IoT Lab > 5009 Risk Management Lab

Name	Updated	Size
5d2j6d	Today by MATS GÖTHE	4 files
67p3ph	Today by MATS GÖTHE	4 files
01gahj	Today by MATS GÖTHE	3 files
xw6e6c	Today by MATS GÖTHE	4 files
sr2hv9	Today by MATS GÖTHE	5 files
ms1ocg	Today by MATS GÖTHE	4 files
jzkpv8	Today by MATS GÖTHE	4 files

Details

Owner
MATS GÖTHE

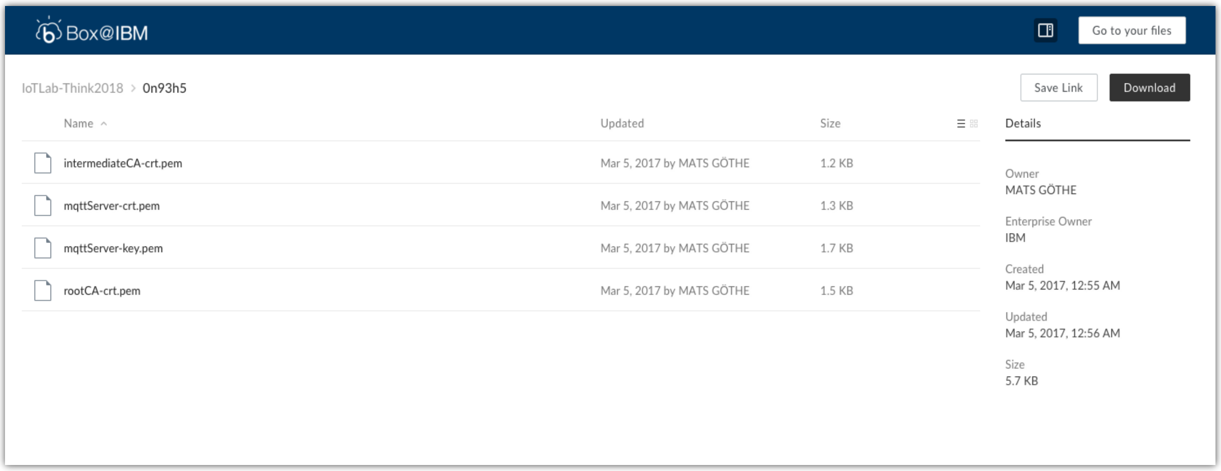
Enterprise owner
IBM

Created
8 Mar 2018 00:15

Updated
14 Mar 2018 01:50

Size
8.5 MB

5. **Click on the folder** have of your organization id.



IoTLab-Think2018 > 0n93h5

Name	Updated	Size
intermediateCA-crt.pem	Mar 5, 2017 by MATS GÖTHE	1.2 KB
mqttServer-crt.pem	Mar 5, 2017 by MATS GÖTHE	1.3 KB
mqttServer-key.pem	Mar 5, 2017 by MATS GÖTHE	1.7 KB
rootCA-crt.pem	Mar 5, 2017 by MATS GÖTHE	1.5 KB

Details

Owner
MATS GÖTHE

Enterprise Owner
IBM

Created
Mar 5, 2017, 12:55 AM

Updated
Mar 5, 2017, 12:56 AM

Size
5.7 KB

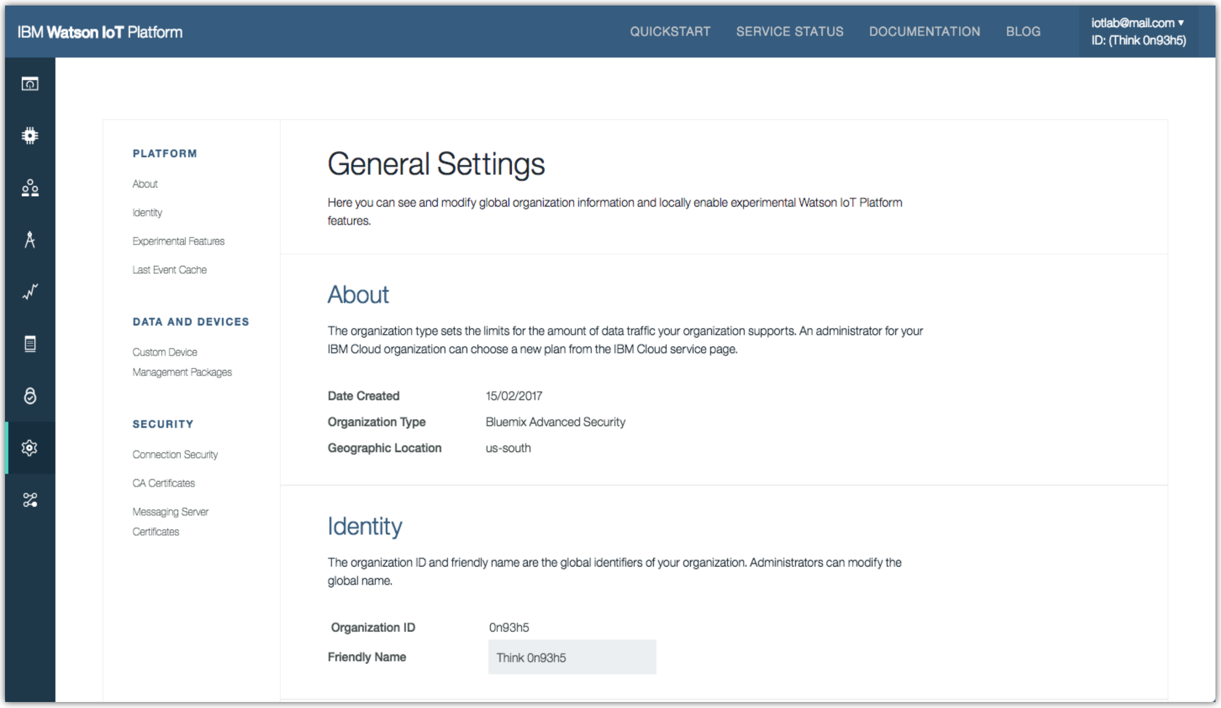
6. Click the **Download** link on the first file.
7. On the following dialog, choose **Save File** and save the file to your ‘Downloads’ directory
8. Repeat the steps above to download all files in the shared directory

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. Choose **Settings** section from the left-hand navigator



General Settings

Here you can see and modify global organization information and locally enable experimental Watson IoT Platform features.

About

The organization type sets the limits for the amount of data traffic your organization supports. An administrator for your IBM Cloud organization can choose a new plan from the IBM Cloud service page.

Date Created	15/02/2017
Organization Type	Bluemix Advanced Security
Geographic Location	us-south

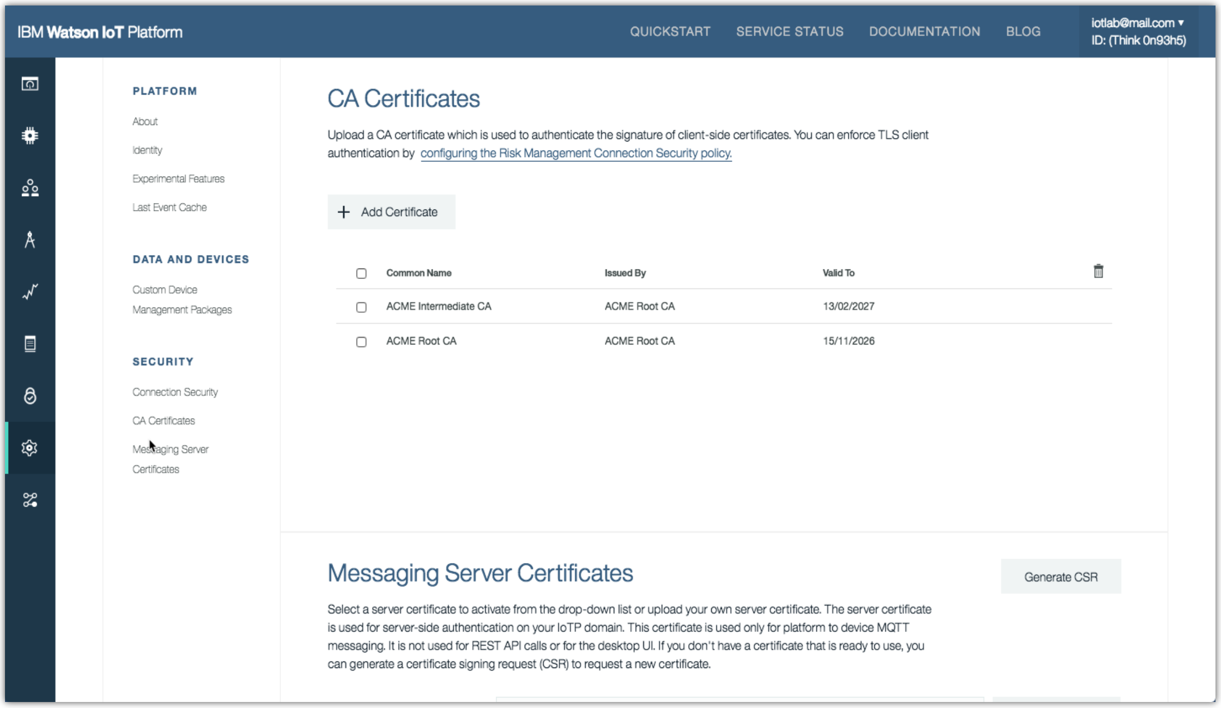
Identity

The organization ID and friendly name are the global identifiers of your organization. Administrators can modify the global name.

Organization ID	0n93h5
Friendly Name	Think 0n93h5

2. On the **General Settings** page, 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

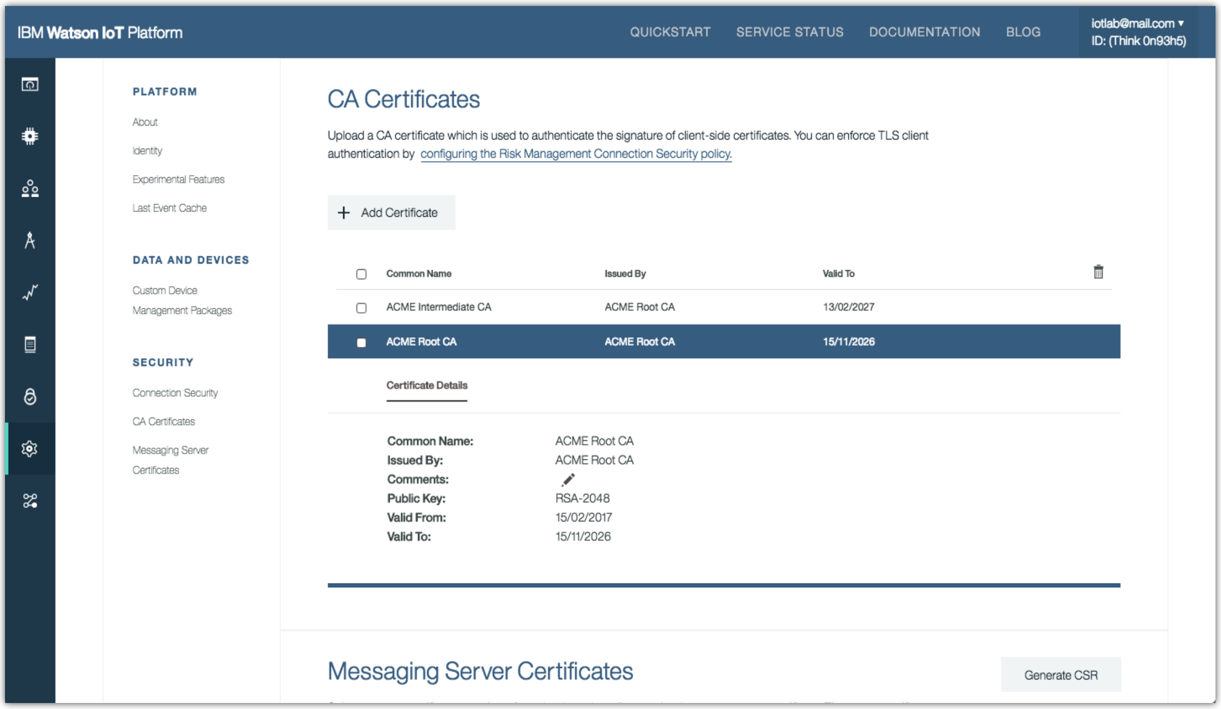
Upload a CA certificate which is used to authenticate the signature of client-side certificates. You can enforce TLS client authentication by configuring the Risk Management Connection Security policy.

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

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.

3. 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.

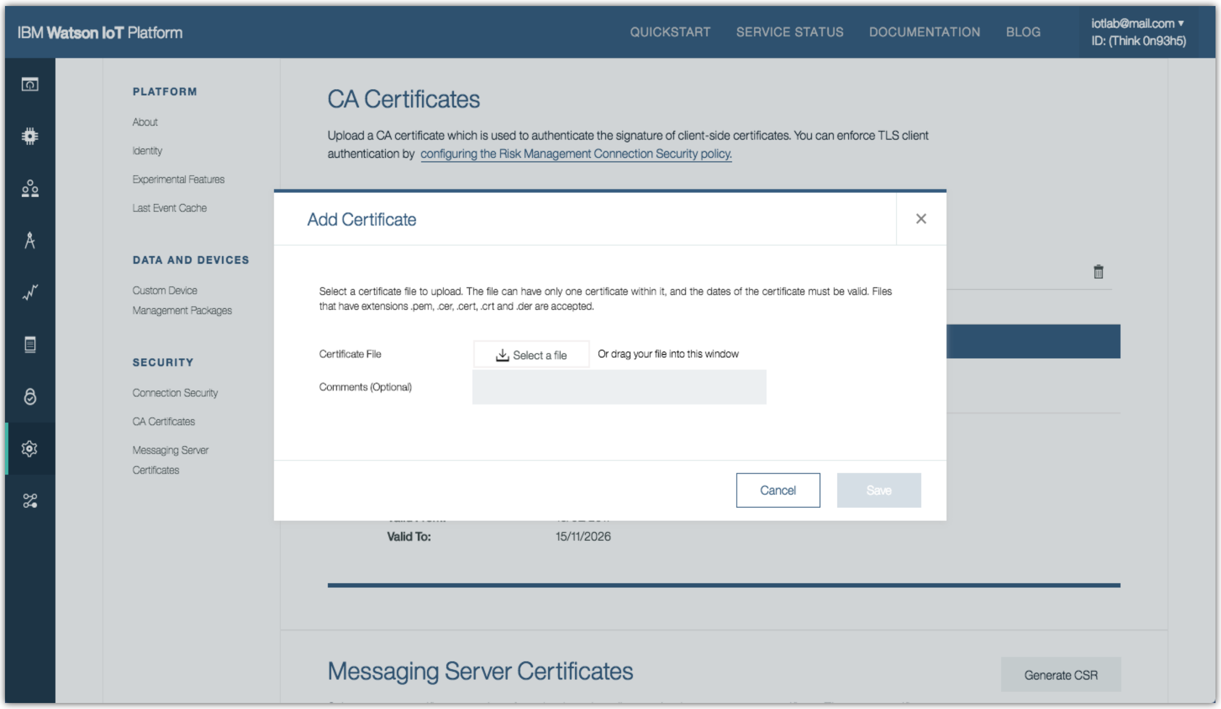
	Common Name	Issued By	Valid To
□	ACME Intermediate CA	ACME Root CA	13/02/2027
■	ACME Root CA	ACME Root CA	15/11/2026

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

Messaging Server Certificates

4. **Optionally**, Remove the "ACME Intermediate CA" certificate by checking the box on the certificate and click the trash can icon.

5. Click **Add Certificate** to upload a new 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.

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, .crt and .der are accepted.

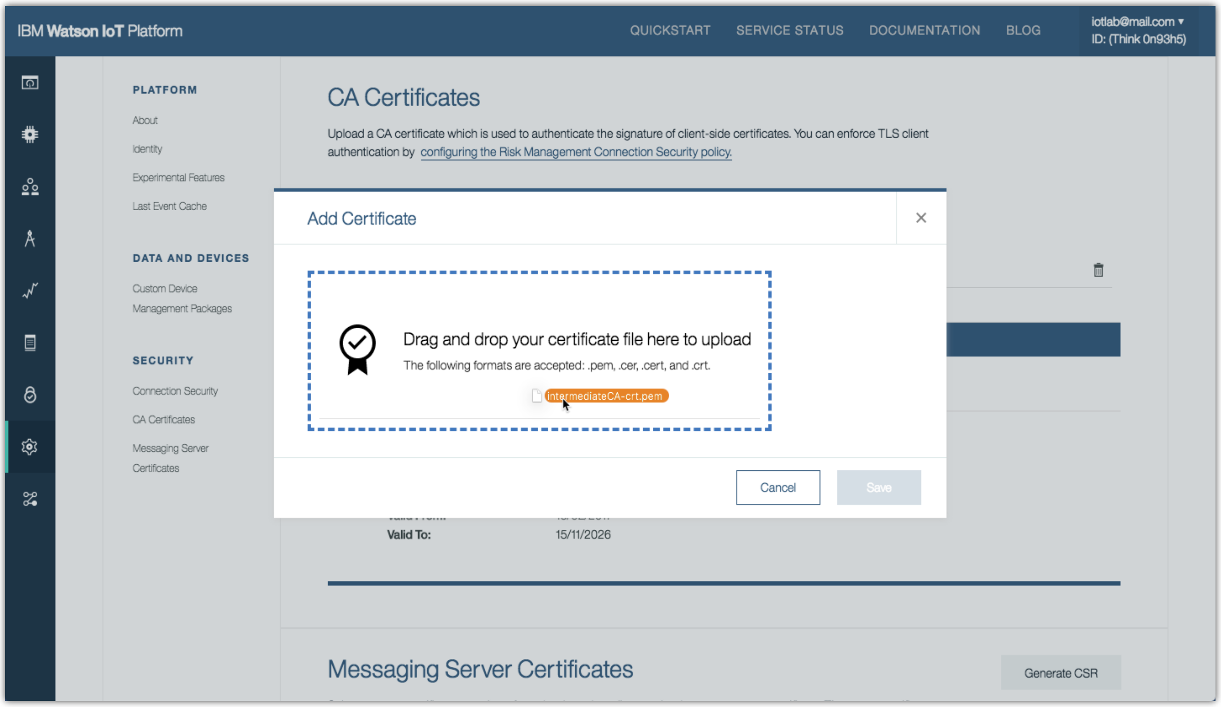
Certificate File — Select a file — Or drag your file into this window

Comments (Optional)

Valid To: 15/11/2026

Messaging Server Certificates

6. Upload the ‘intermediateCA-crt.pem’ certificate for your IoT platform organization that you downloaded from Box. Browse to select a certificate file to upload or drag and drop a file in the **Add Certificate** pop-up.



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.

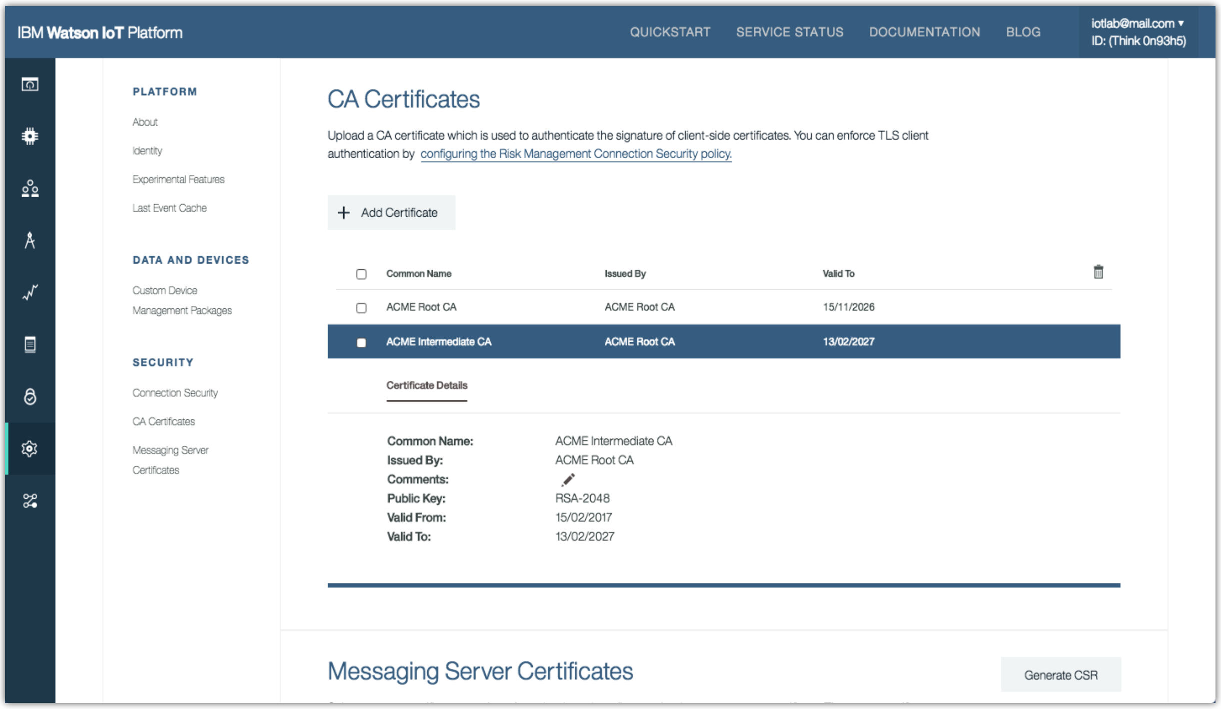
Drag and drop your certificate file here to upload

The following formats are accepted: .pem, .cer, .cert, and .crt.

Valid To: 15/11/2026

Messaging Server Certificates

7. Enter an optional comment and click **Save**. The certificate is added to your IoT platform organization, activated and listed in the table.
8. 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.

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

Common Name:	ACME Intermediate CA
Issued By:	ACME Root CA
Comments:	✎
Public Key:	RSA-2048
Valid From:	15/02/2017
Valid To:	13/02/2027

Messaging Server Certificates

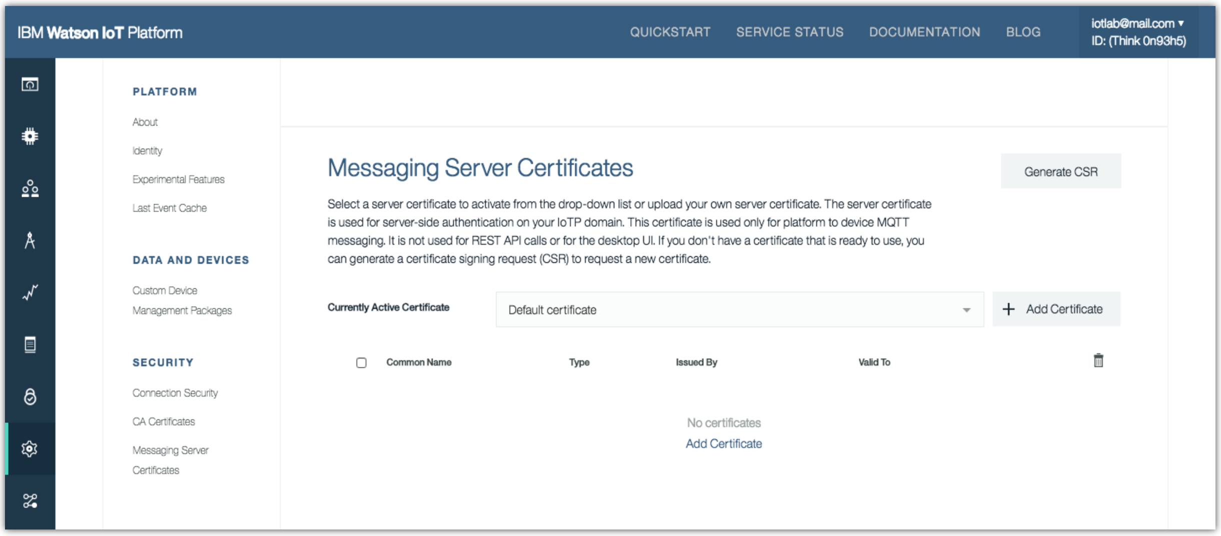
Requesting a new server certificate

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.

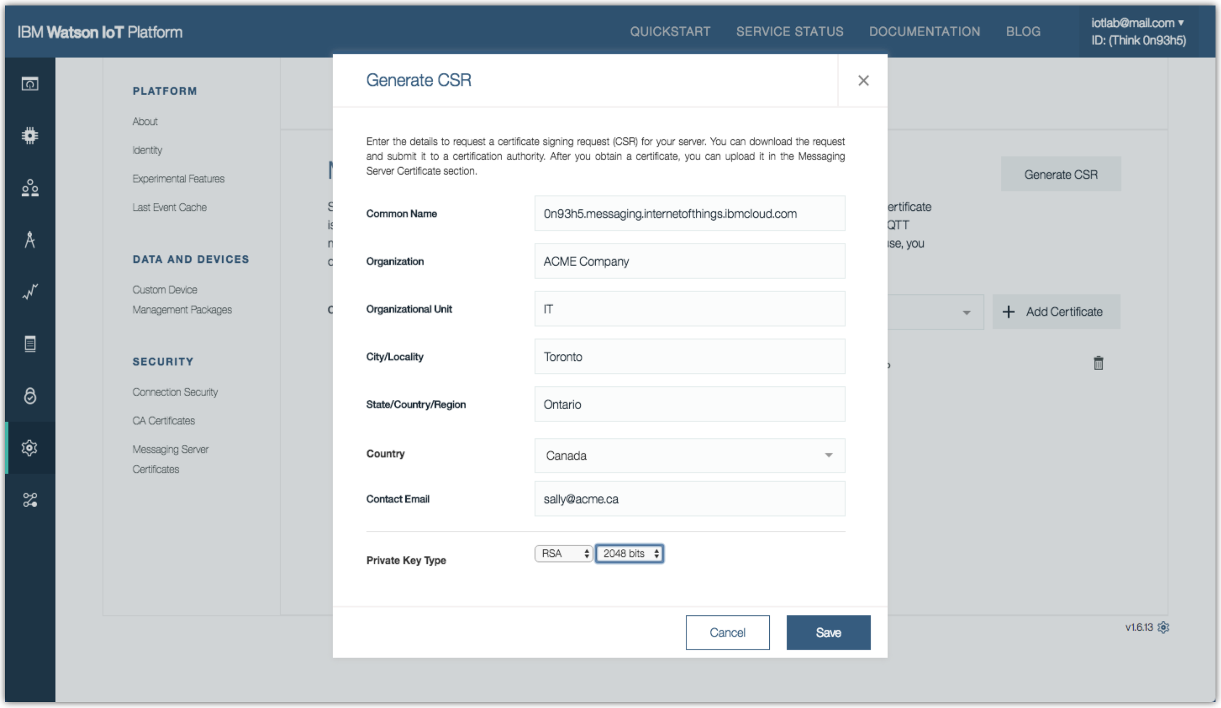
Currently Active Certificate: Default certificate

□	Common Name	Type	Issued By	Valid To

No certificates
Add Certificate

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**



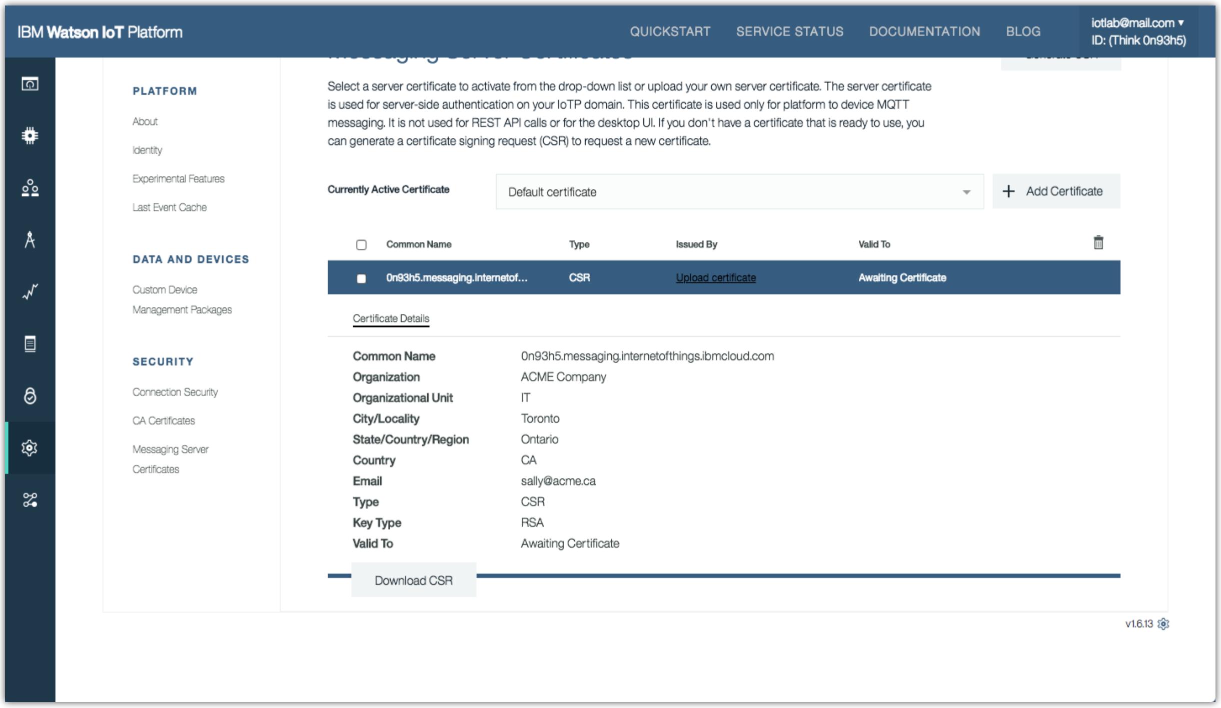
Generate CSR

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	0n93h5.messaging.internetofthings.ibmcloud.com
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

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.



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
■	0n93h5.messaging.internetof...	CSR	Upload certificate	Awaiting Certificate

Certificate Details

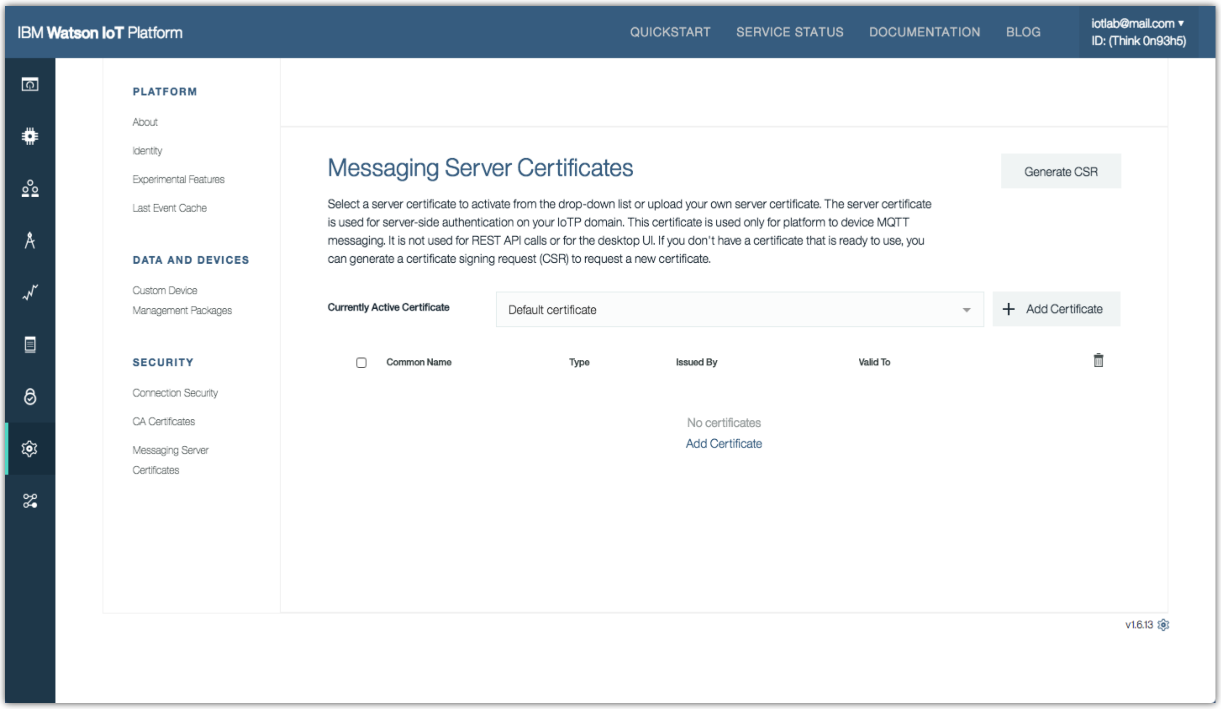
Common Name	0n93h5.messaging.internetofthings.ibmcloud.com
Organization	ACME Company
Organizational Unit	IT
City/Locality	Toronto
State/Country/Region	Ontario
Country	CA
Email	sally@acme.ca
Type	CSR
Key Type	RSA
Valid To	Awaiting Certificate

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.

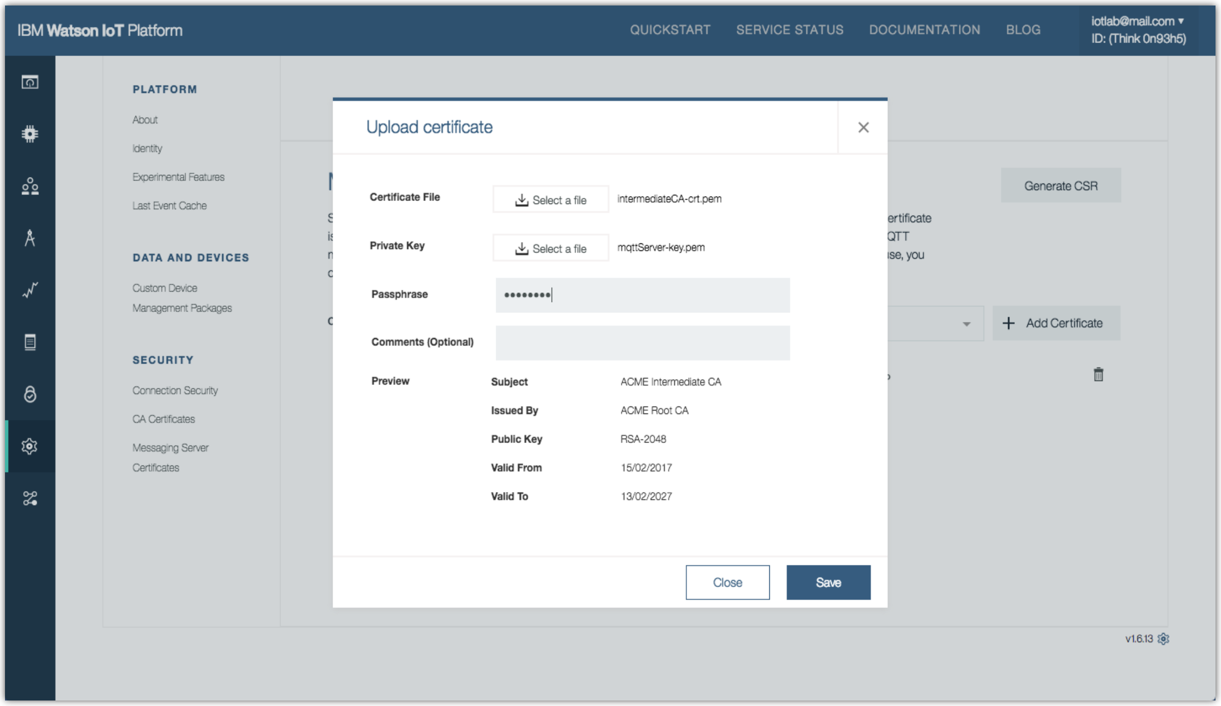


Messaging Server Certificates

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

2. Upload the ‘mqttServer-crt.pem’ certificate file to the **Certificate File** section in the **Add Certificate** window.
3. Upload the ‘mqttServer-key.pem’ private key file to the **Private Key** section the **Add Certificate** window.
4. Enter the passphrase “password” of the private key



Upload certificate

Certificate File: intermediateCA-crt.pem

Private Key: mqttServer-key.pem

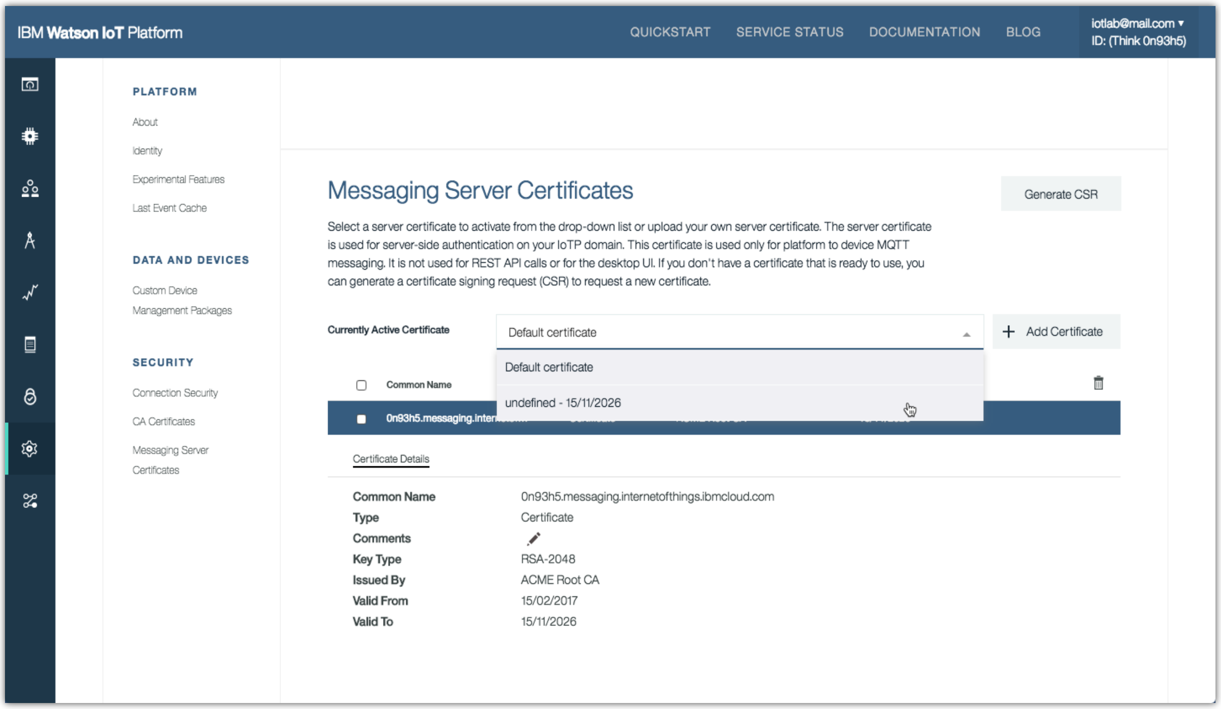
Passphrase: ••••••••

Comments (Optional):

Preview

Subject	ACME Intermediate CA
Issued By	ACME Root CA
Public Key	RSA-2048
Valid From	15/02/2017
Valid To	13/02/2027

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

- Default certificate
- undefined - 15/11/2026

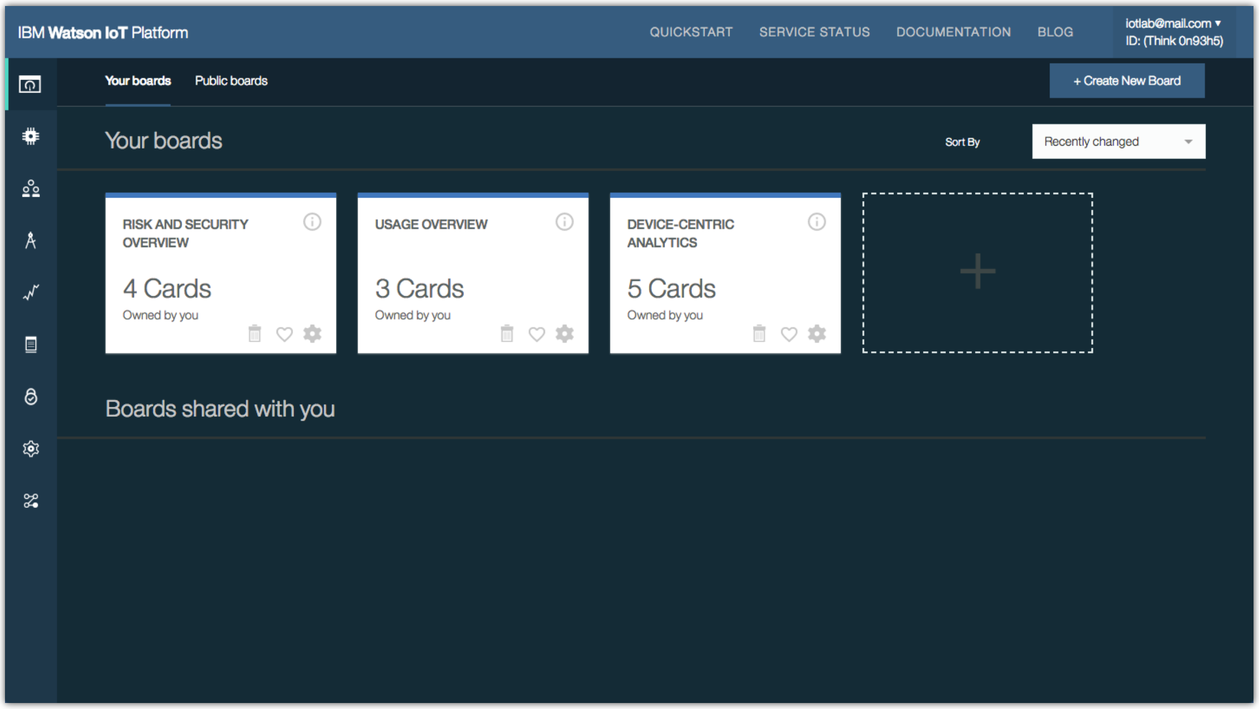
□	Common Name
□	0n93h5.messaging.inter

Common Name	0n93h5.messaging.internetofthings.ibmcloud.com
Type	Certificate
Comments	
Key Type	RSA-2048
Issued By	ACME Root CA
Valid From	15/02/2017
Valid To	15/11/2026

Monitoring the overall security posture and policy compliance

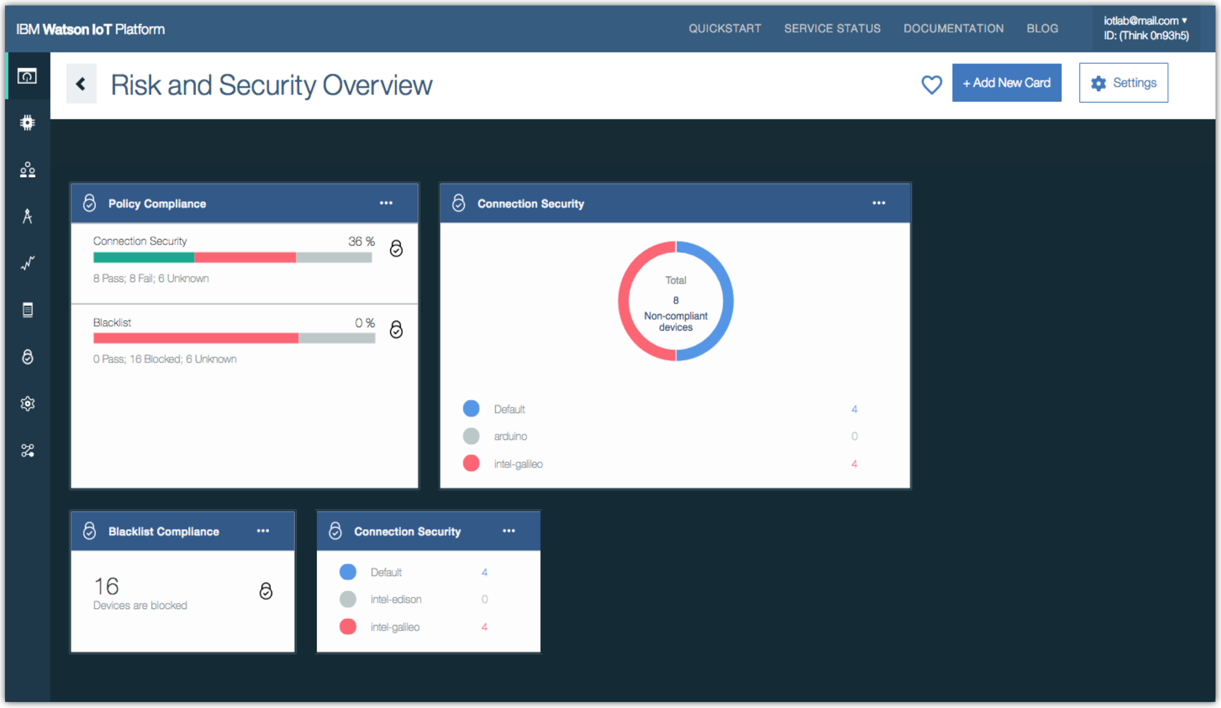
A new “Risk and Security Overview” board is already added on your dashboard with pre-configured cards. It provides an instant overview of the security state of your organization. As a security analyst, you can use the dashboard to visualize the policy compliance and any critical risks and be able to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

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



Policy Compliance

Connection Security 36 %
8 Pass; 8 Fail; 6 Unknown

Blacklist 0 %
0 Pass; 16 Blocked; 6 Unknown

Connection Security

Total
8
Non-compliant devices

Default	4
arduino	0
intel-galileo	4

Blacklist Compliance

16
Devices are blocked

Connection Security

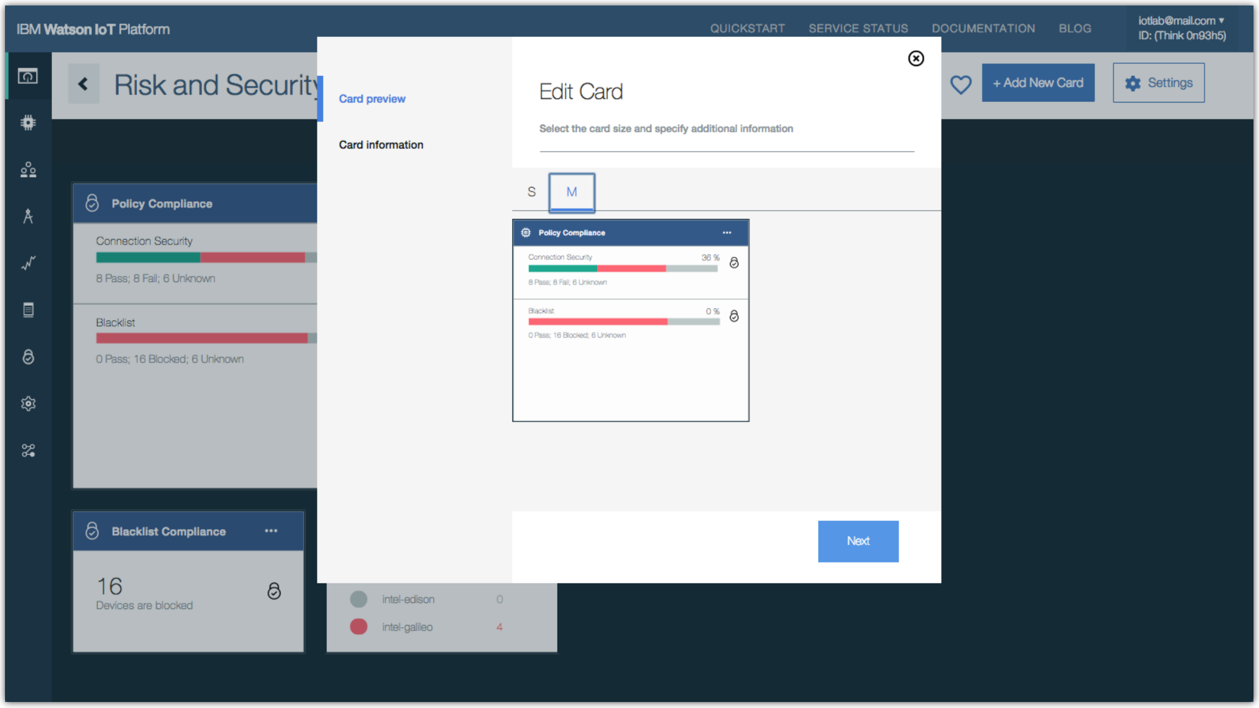
Default	4
intel-edison	0
intel-galileo	4

3. Click on the card **settings icon** on the top right corner of the card to open the menu.
   •••

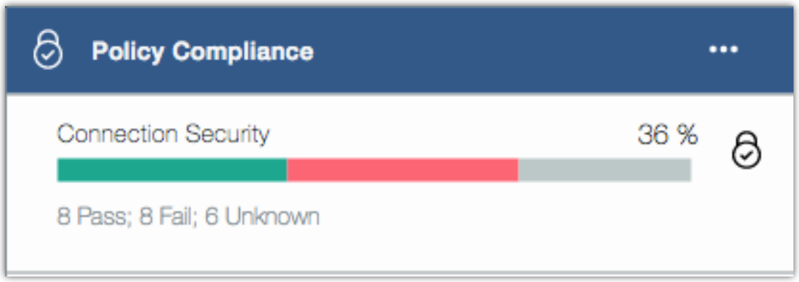
4. Click on the **setting icon**. The Edit Card dialog opens.

5. Preview different card sizes by clicking on **S** or **M**. Click **Next** and conform changes.
6. Clock **Next** and **Submit** to save any changes.

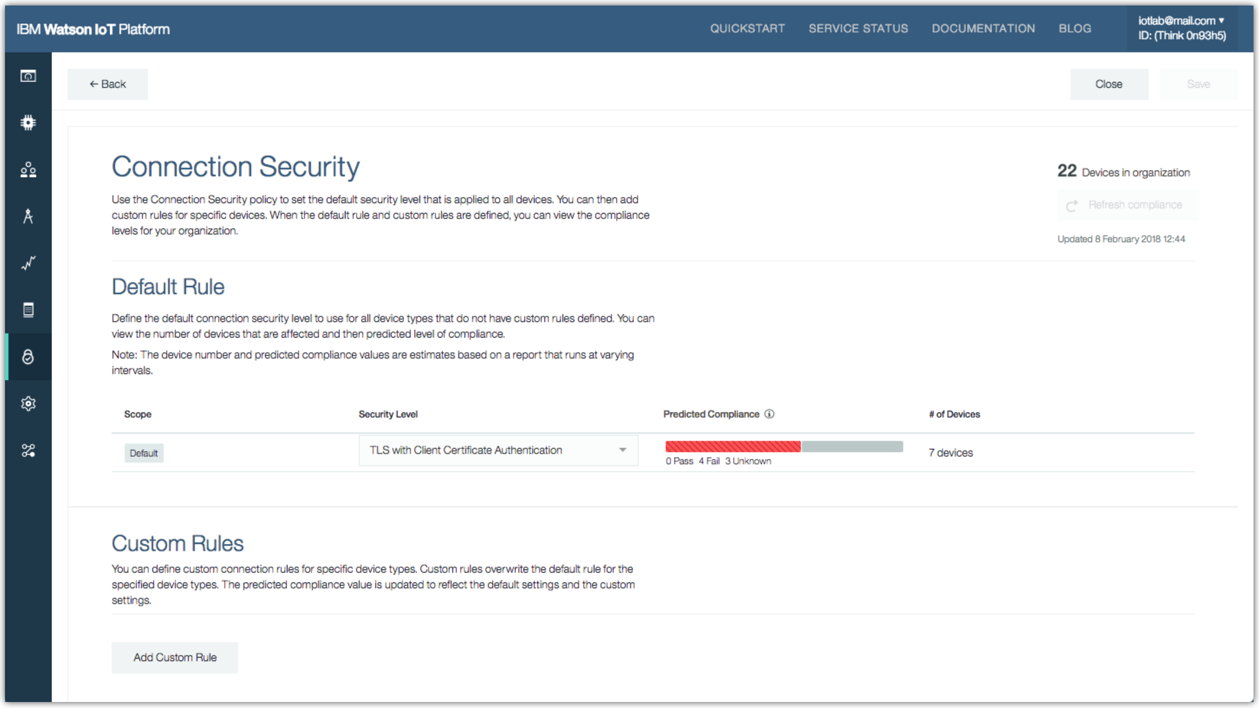
think
2018



7. On the Policy Compliance card, click on the padlock icon 🔒 to open to the Policy Editor.



8. The Connection Security Policy editor opens.



Connection Security

Use the Connection Security policy to set the default security level that is applied to all devices. You can then add custom rules for specific devices. When the default rule and custom rules are defined, you can view the compliance levels for your organization.

22 Devices in organization

Updated 8 February 2018 12:44

Default Rule

Define the default connection security level to use for all device types that do not have custom rules defined. You can view the number of devices that are affected and then predicted level of compliance.

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

Scope	Security Level	Predicted Compliance	# of Devices
Default	TLS with Client Certificate Authentication	0 Pass 4 Fail 3 Unknown	7 devices

Custom Rules

You can define custom connection rules for specific device types. Custom rules overwrite the default rule for the specified device types. The predicted compliance value is updated to reflect the default settings and the custom settings.

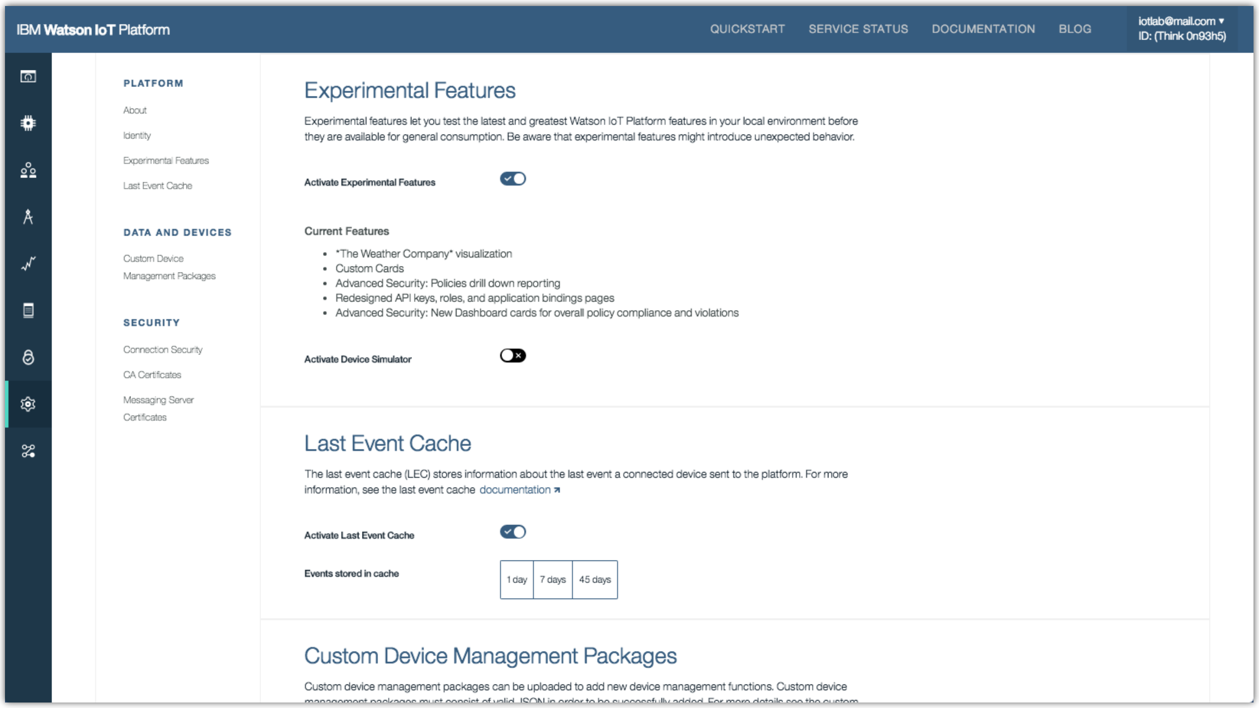
You have now completed the exploration of policy reporting using the Watson IoT Platform dashboard.

Advanced Security – Policy Drill-Down Reporting

A new experimental feature is currently available in the Watson IoT Platform. This new feature allows you to.

To enable Experimental Features

1. Choose **Settings** from left-hand navigator, and go to the **Experimental Features** section
2. Enable **Experimental Features** by moving the switch to On.



Experimental Features

Experimental features let you test the latest and greatest Watson IoT Platform features in your local environment before they are available for general consumption. Be aware that experimental features might introduce unexpected behavior.

Activate Experimental Features ✓

Current Features

- *The Weather Company* visualization
- Custom Cards
- Advanced Security: Policies drill down reporting
- Redesigned API keys, roles, and application bindings pages
- Advanced Security: New Dashboard cards for overall policy compliance and violations

Activate Device Simulator ✕

Last Event Cache

The last event cache (LEC) stores information about the last event a connected device sent to the platform. For more information, see the last event cache documentation ↗

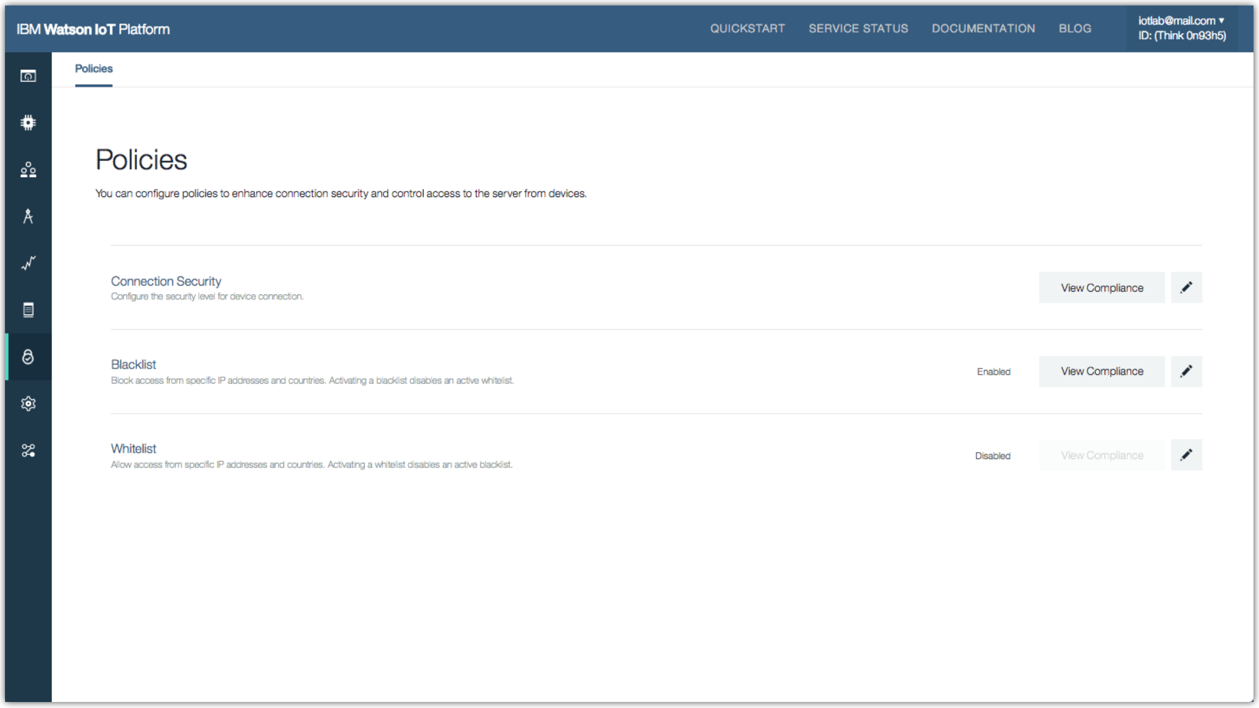
Activate Last Event Cache ✓

Events stored in cache: 1 day | 7 days | 45 days

Custom Device Management Packages

Custom device management packages can be uploaded to add new device management functions. Custom device management packages must consist of valid JSON in order to be successfully added. For more details see the custom

3. Return to the Policies section by choosing **Security** in the left-hand navigator.



Policies

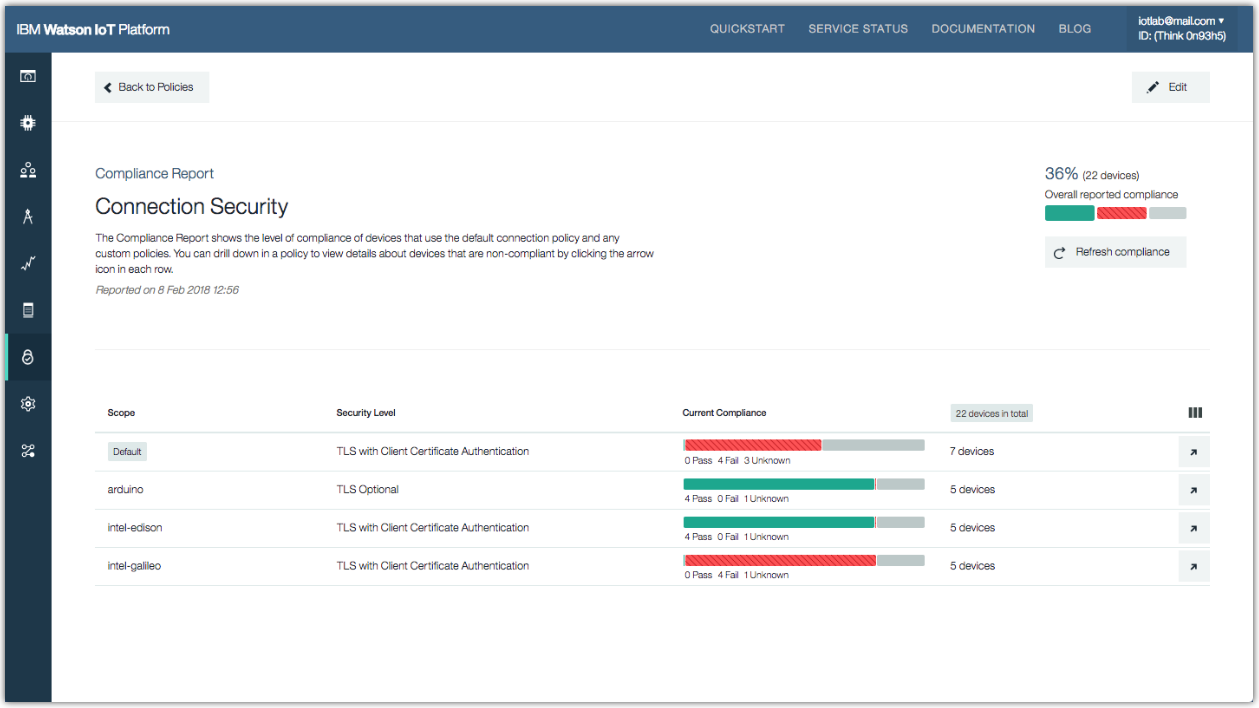
You can configure policies to enhance connection security and control access to the server from devices.

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.

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

4. Clock on **View Compliance** on the Connection Security row.
   The compliance report for loads.



Compliance Report

Connection Security

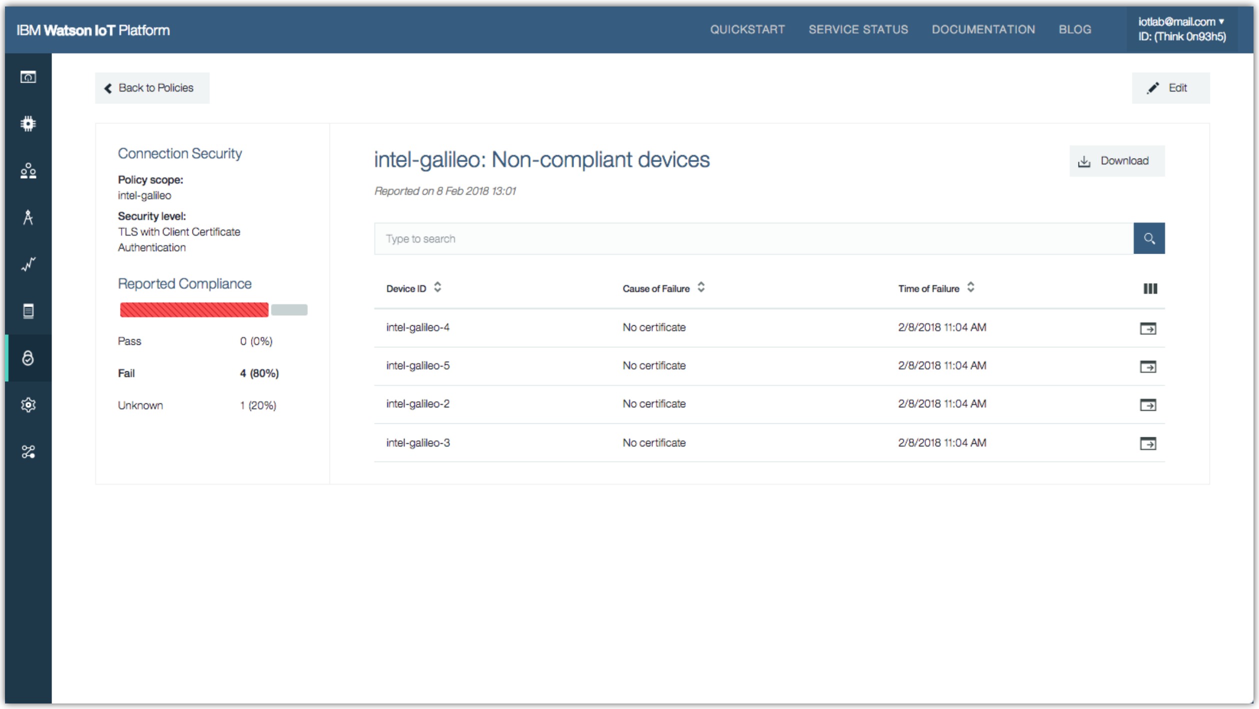
The Compliance Report shows the level of compliance of devices that use the default connection policy and any custom policies. You can drill down in a policy to view details about devices that are non-compliant by clicking the arrow icon in each row.

Reported on 8 Feb 2018 12:56

36% (22 devices)
Overall reported compliance

Scope	Security Level	Current Compliance	22 devices in total
Default	TLS with Client Certificate Authentication	0 Pass 4 Fail 3 Unknown	7 devices
arduino	TLS Optional	4 Pass 0 Fail 1 Unknown	5 devices
intel-edison	TLS with Client Certificate Authentication	4 Pass 0 Fail 1 Unknown	5 devices
intel-galileo	TLS with Client Certificate Authentication	0 Pass 4 Fail 1 Unknown	5 devices

5. To drill into details on the report, click the browse icon on the report row for the 'intel-galileo' devices.



Connection Security

Policy scope:
intel-galileo

Security level:
TLS with Client Certificate Authentication

Reported Compliance

Pass	0 (0%)
Fail	**4 (80%)**
Unknown	1 (20%)

intel-galileo: Non-compliant devices

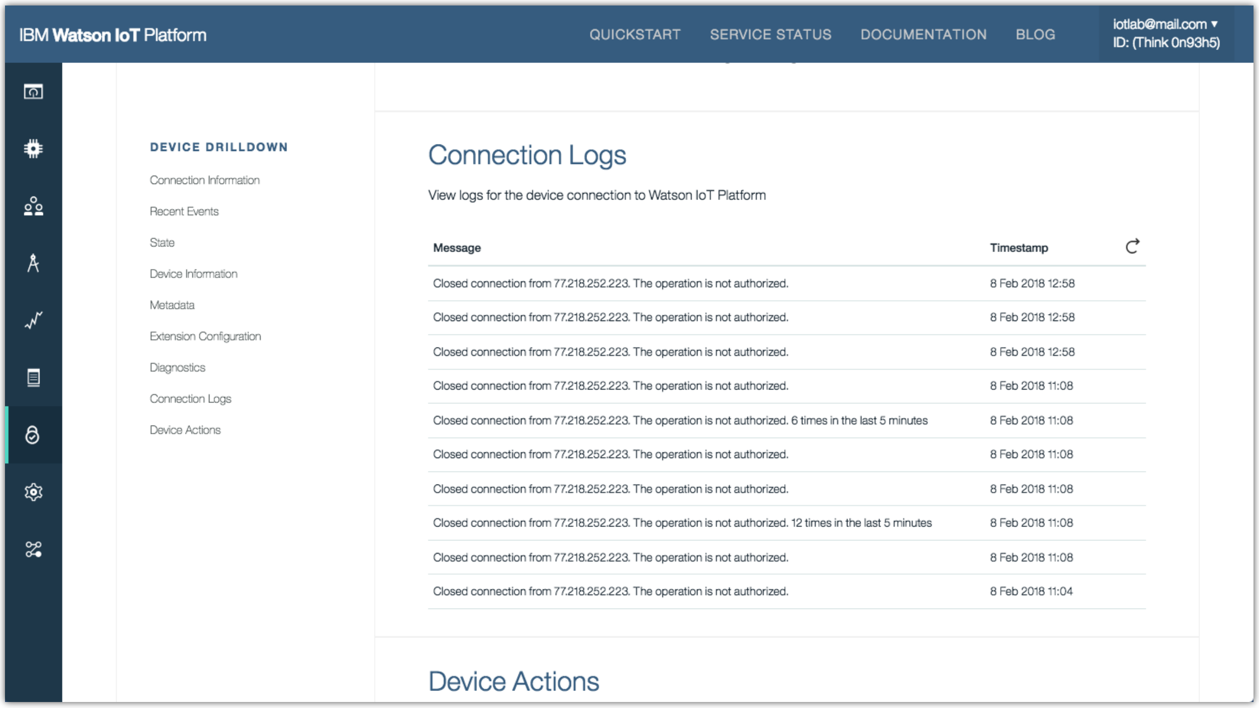
Reported on 8 Feb 2018 13:01

Device ID	Cause of Failure	Time of Failure
intel-galileo-4	No certificate	2/8/2018 11:04 AM
intel-galileo-5	No certificate	2/8/2018 11:04 AM
intel-galileo-2	No certificate	2/8/2018 11:04 AM
intel-galileo-3	No certificate	2/8/2018 11:04 AM

6. The report provides detailed information on the compliance by device and on connection failures.

7. To view the device state of the device and the connection log, click on the browse button, for example 'intel-galileo'-5'.

8. The Device Drilldown page opens. Click on the **Connection Log** section to view any connection failures.



Connection Logs

View logs for the device connection to Watson IoT Platform

Message	Timestamp
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 12:58
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 12:58
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 12:58
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized. 6 times in the last 5 minutes	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized. 12 times in the last 5 minutes	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:08
Closed connection from 77.218.252.223. The operation is not authorized.	8 Feb 2018 11:04

Device Actions

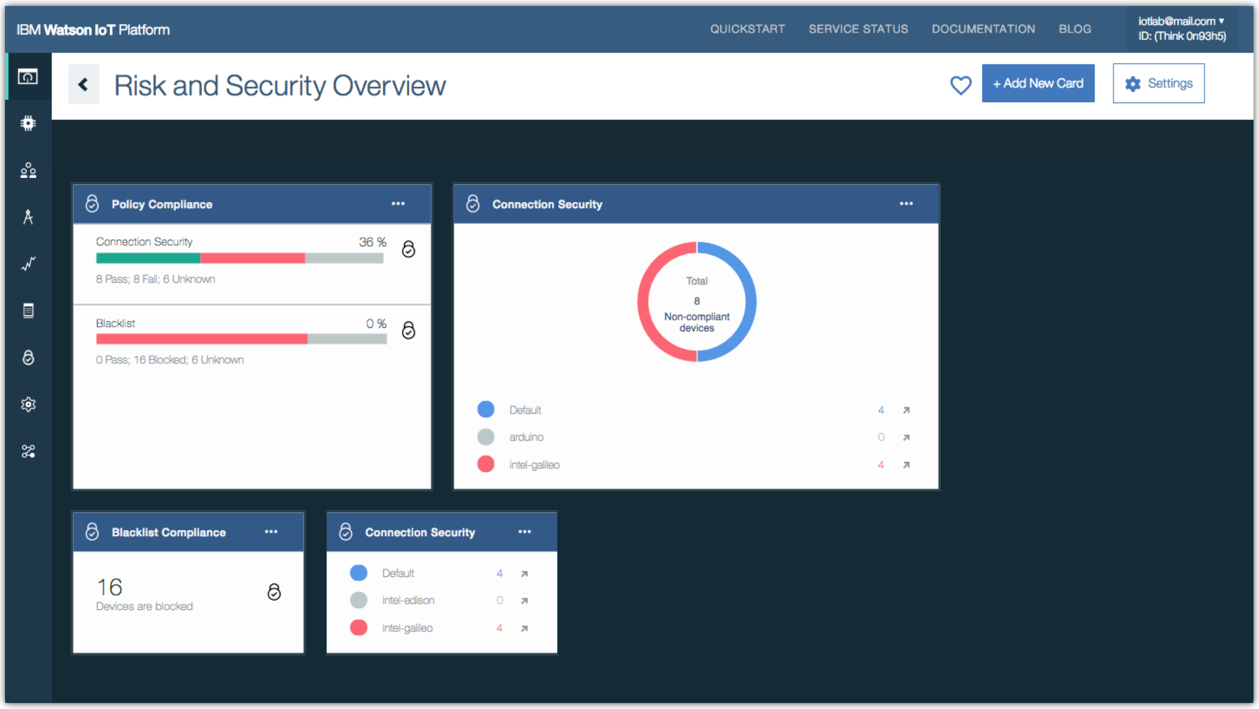
9. Optionally, generate other reports and browse other devices to explore the reporting feature.

Advanced Security – Policy Reporting Cards

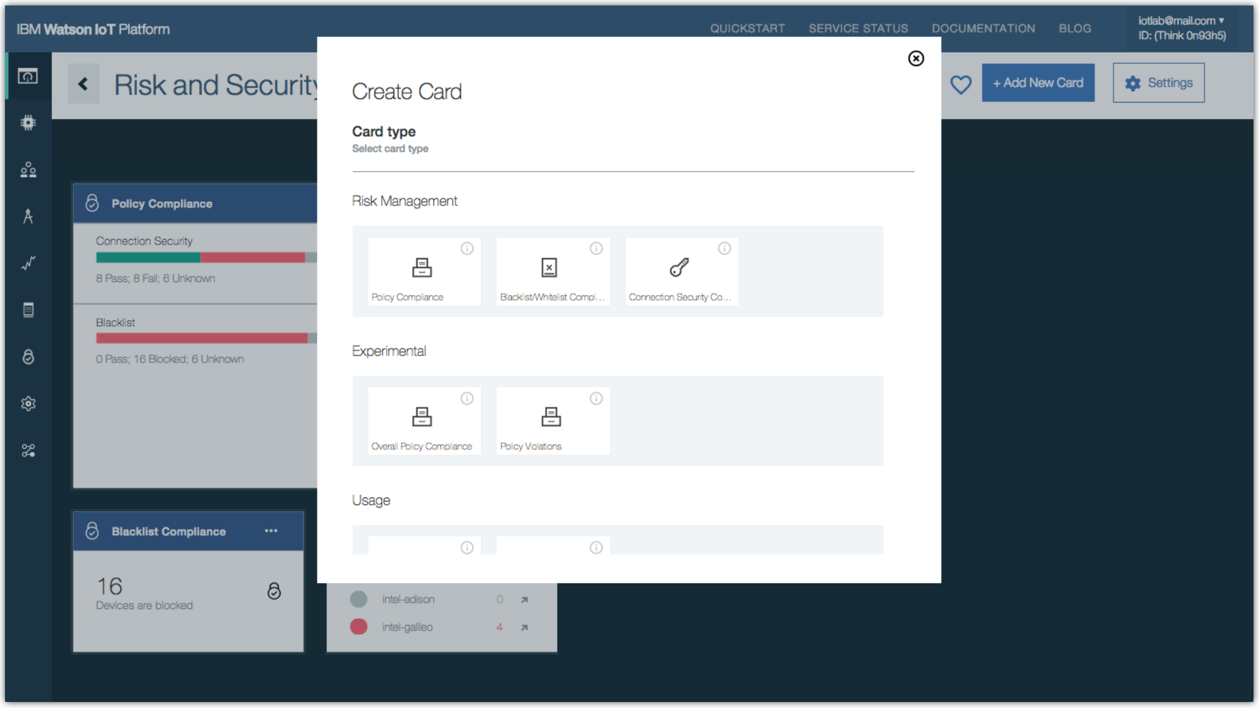
A new experimental feature is currently available in the Watson IoT Platform. This new feature allows you to view and browse Policy Reports on the dashboard.

To add policy reporting cards to your dashboard

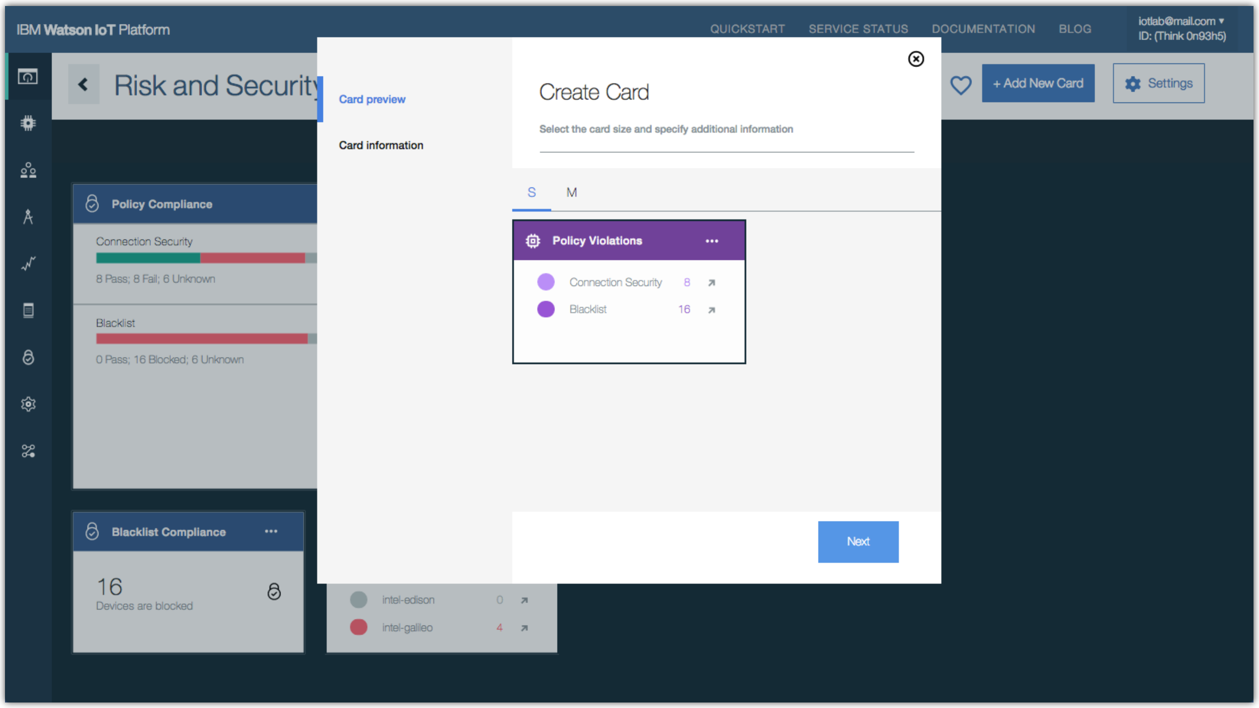
1. Go to the IoT Platform dashboard.
   Open the Risk and Security Overview card.



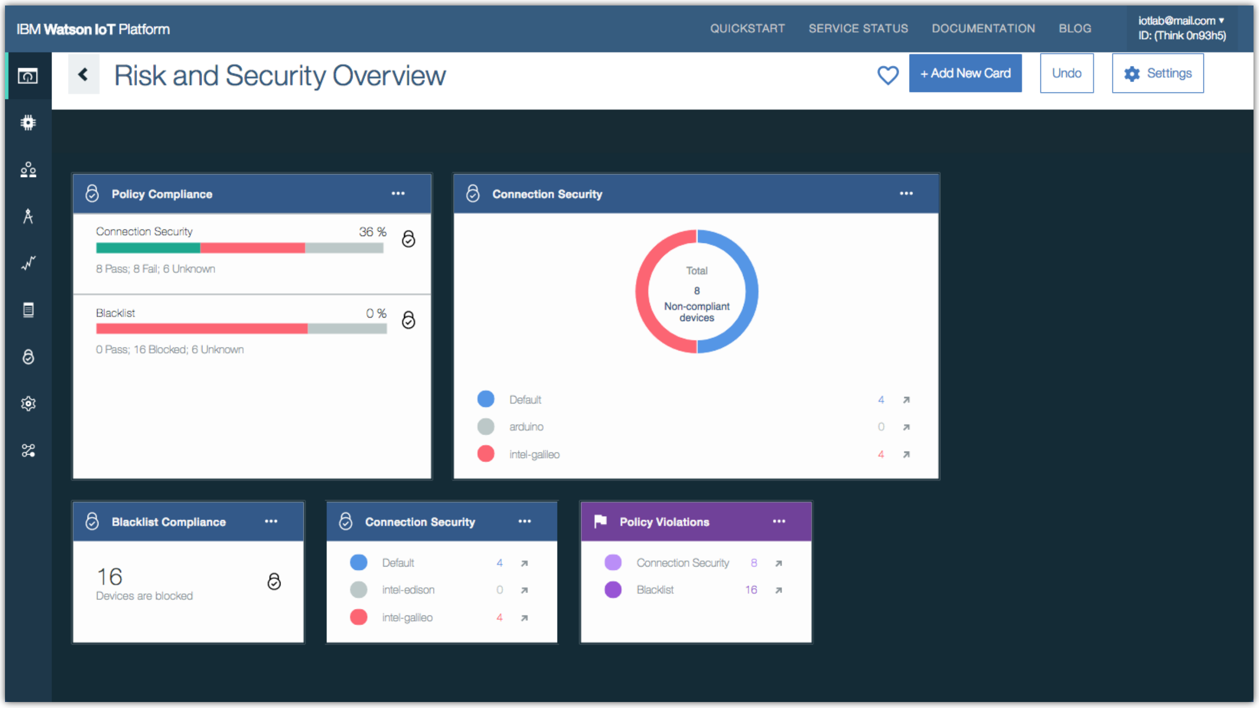
2. Click the **Add New Card** button on the title bar.
   The Create Card guide opens.



3. Click on Policy Violations to add a new card to the dashboard.



4. Keep the S size. Click Next and Finish to place the card on the board.



Risk and Security Overview

Policy Compliance

Connection Security 36 %

8 Pass; 8 Fail; 6 Unknown

Blacklist 0 %

0 Pass; 16 Blocked; 6 Unknown

Connection Security

Total 8 Non-compliant devices

Default	4
arduino	0
intel-galileo	4

Blacklist Compliance

16 Devices are blocked

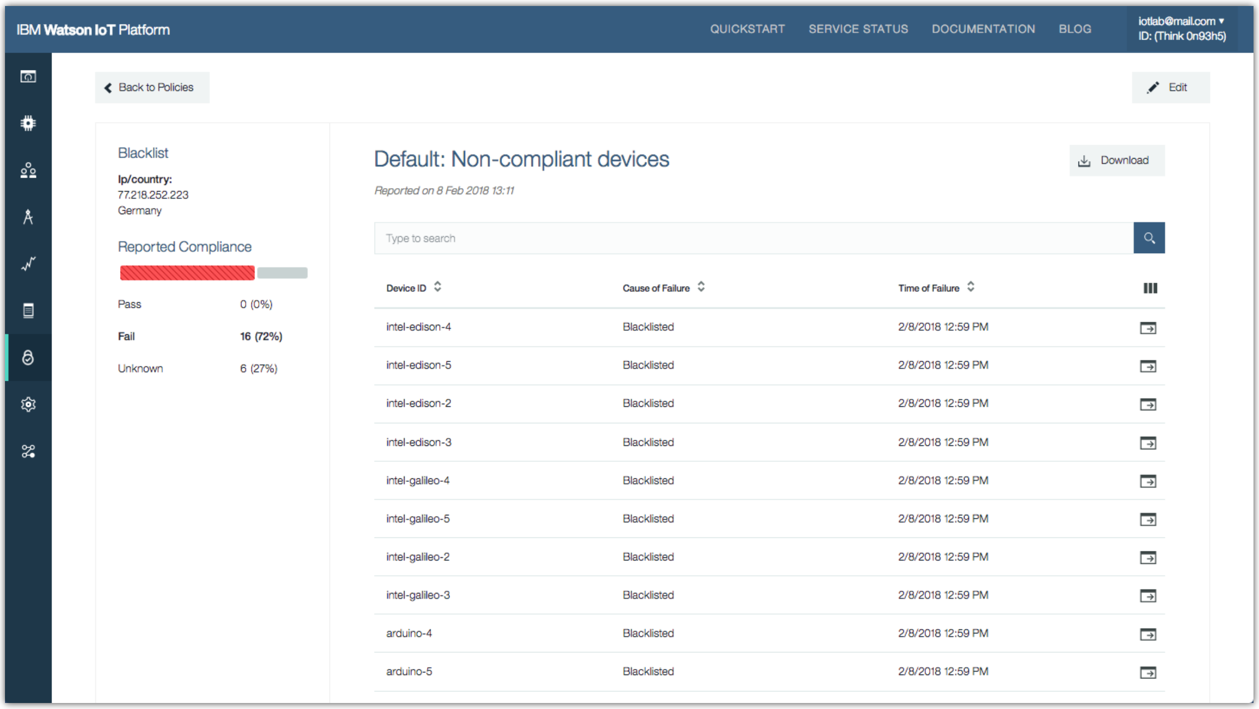
Connection Security

Default	4
intel-edison	0
intel-galileo	4

Policy Violations

Connection Security	8
Blacklist	16

5. Optionally, drag the card to a new position on the board.
6. On the new card, click the Blacklist row.



Blacklist

Ip/country:
77.218.252.223
Germany

Reported Compliance

Pass	0 (0%)
Fail	**16 (72%)**
Unknown	6 (27%)

Default: Non-compliant devices

Reported on 8 Feb 2018 13:11

Device ID	Cause of Failure	Time of Failure
intel-edison-4	Blacklisted	2/8/2018 12:59 PM
intel-edison-5	Blacklisted	2/8/2018 12:59 PM
intel-edison-2	Blacklisted	2/8/2018 12:59 PM
intel-edison-3	Blacklisted	2/8/2018 12:59 PM
intel-galileo-4	Blacklisted	2/8/2018 12:59 PM
intel-galileo-5	Blacklisted	2/8/2018 12:59 PM
intel-galileo-2	Blacklisted	2/8/2018 12:59 PM
intel-galileo-3	Blacklisted	2/8/2018 12:59 PM
arduino-4	Blacklisted	2/8/2018 12:59 PM
arduino-5	Blacklisted	2/8/2018 12:59 PM

7. The drill-in report for the Blacklist is shown.
   Optionally, drill into individual device for more information.

You have now completed the exploration of the new experimental feature for policy reporting using the Watson IoT Platform dashboard.

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.

We Value Your Feedback!

- Don’t forget to submit your Think 2018 session and speaker feedback! Your feedback is very important to us – we use it to continually improve the conference.
- Access the Think 2018 agenda tool to quickly submit your surveys from your smartphone, laptop or conference kiosk.