



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Arrow Connect™ IoT Solution with Avaya Breeze™ – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Arrow Connect™ IoT solution with Avaya Breeze™. Arrow Connect IoT solution consists of dynamic tasks which can be used on Avaya Engagement Designer to create workflows.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to integrate Arrow Connect™ IoT (Internet of Things) solution with Avaya Breeze™ (Breeze).

Arrow Connect IoT solution is comprised of dynamic tasks created by Arrow Systems Integration. These dynamic tasks allow the power of Arrow Connect and IoT to be easily integrated into Breeze Snap-Ins. These tasks also greatly simplify the work required to speak to a myriad of sensors each with their protocols and reporting capabilities. Using these tasks, Snap-Ins can query sensors for their current values, run analytics on a sensor's data, and send device specific commands to those sensors. These sensors communicate to Arrow Connect IoT solution via an Arrow Connect Gateway application, which is available for iOS and Android devices. These dynamic tasks are used to create workflows on Avaya Engagement Designer. An example of a workflow is to turn on or off a LED light on a sensor device by calling a number. Avaya Engagement Designer is a Snap-in that is deployed on Breeze. Below is the list of tasks used during compliance testing:

- **Arrow Connect Action:** Arrow Connect Action is used to enable and disable Arrow Connect Actions. Actions are created for devices to dynamically launch Snap-Ins.
- **Arrow Connect Info:** Arrow Connect Info is used to retrieve information about a particular device.
- **Arrow Connect Snapshot:** Arrow Connect Snapshot is used to retrieve the last collected values in the Arrow Connect cloud for a particular device.
- **Arrow Connect State:** Arrow Connect State is used to make state changes to a particular device.
- **Arrow Connect Device:** Arrow Connect Device is used to send device specific commands for a particular device.
- **Arrow Connect Trends:** Arrow Connect Trends is used to retrieve analytics data for a particular sensor.

2. General Test Approach and Test Results

The interoperability compliance testing included feature testing. The feature testing involved, invoking the Arrow Connect dynamic tasks via Engagement Designer workflows.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Arrow Connect IoT solution utilized enabled capabilities of HTTPS.

2.1. Interoperability Compliance Testing

Compliance testing was mainly focused around Arrow Connect dynamic tasks' ability to use provided input data and return relevant results. Various workflows were created to invoke the following dynamic tasks and ensure each task performed as it was configured:

- Arrow Connect Action
- Arrow Connect Info
- Arrow Connect Snapshot
- Arrow Connect State
- Arrow Connect Device
- Arrow Connect Trend

2.2. Test Results

The Arrow Connect IoT solution successfully completed compliance testing.

2.3. Support

For Arrow Connect IoT solution support, Arrow can be reached using the following methods:

- **Web:** <https://www.arrow.com/en/iot>
- **Phone:** +1-855-326-4757
- **Email:** websupport@arrow.com

3. Reference Configuration

Figure 1 illustrates the lab configuration used to verify the Arrow Connect IoT solution with Avaya Breeze™. The configuration consists of an Avaya Aura® environment providing connectivity to the PSTN via an ISDN-PRI trunk, and a Breeze server. Arrow Connect dynamic tasks were deployed on Avaya Engagement Designer (running on Breeze).

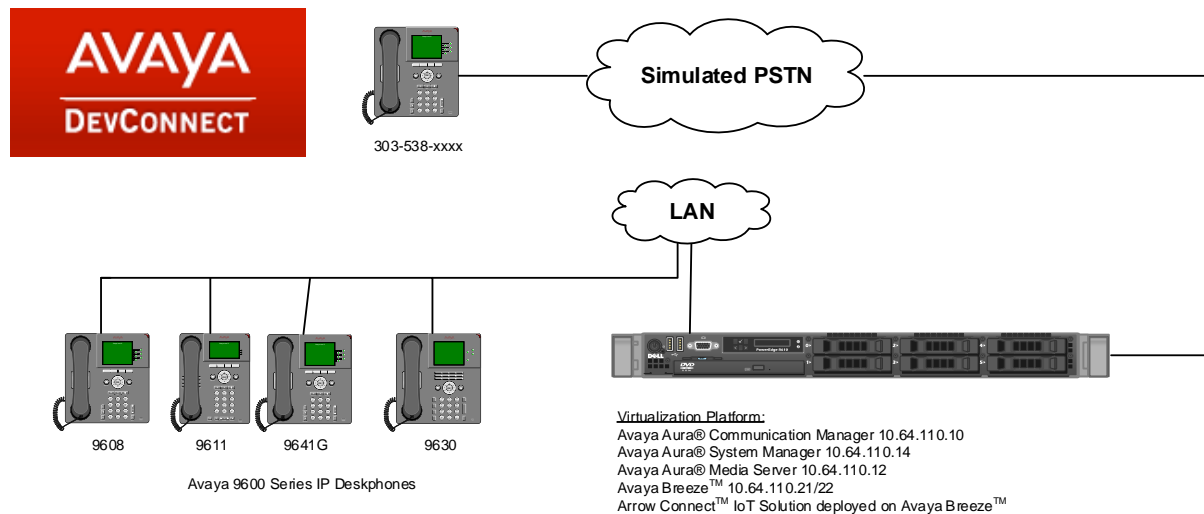


Figure 1: Lab Configuration

4. Equipment and Software Validated

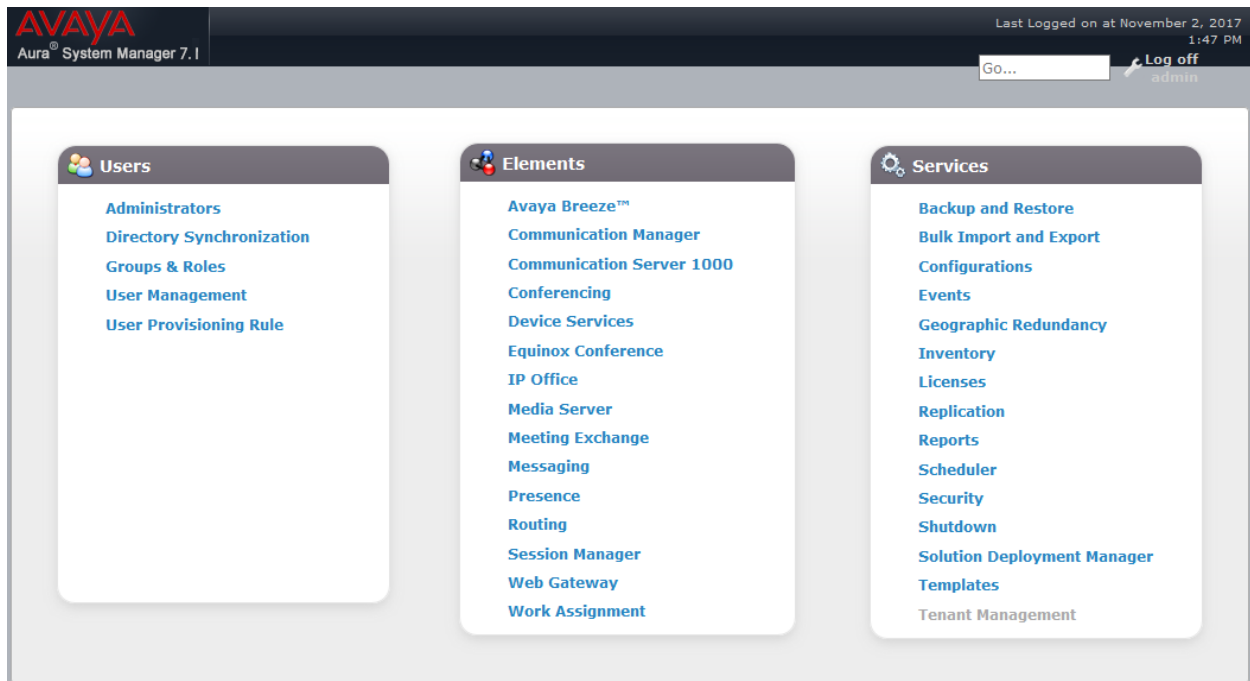
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	R017x.01.0.532.0
Avaya Aura® System Manager	7.1.1.0
Avaya Aura® Session Manager	7.1.1.0.711008
Avaya Aura® Media Server	7.8.0.333
Avaya Breeze™	3.3.1.1.331108
Avaya Engagement Designer	3.3.0.0.25042
Arrow Connect™ IoT Solution: <ul style="list-style-type: none">• Arrow Connect Action• Arrow Connect Info• Arrow Connect Snapshot• Arrow Connect State• Arrow Connect Device• Arrow Connect Trends• Arrow Connect Gateway app running on an iOS device	<ul style="list-style-type: none">• 1.0.0.0.5• 1.0.0.0.5• 1.0.0.0.8• 1.0.0.0.2• 1.0.0.0.6• 1.0.0.0.5• 1.1.11

5. Configure Avaya Breeze™

Configuration of Avaya Breeze™ is performed via Avaya Aura® System Manager. Access the System Manager Administration web interface by entering <https://<ip-address>/SMGR> as the URL in a web browser, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials.

Once logged in, the following screen is displayed.



5.1. Configure SIP Entities

Verify a SIP Entity for Avaya Breeze™ has been added. Navigate to **Home → Elements → Routing → SIP Entities** and click the **Edit** button (not shown).

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Scroll down to the **Entity Links** section. Verify that the Session Manager SIP Entity is set as **SIP Entity 1**, and that this Avaya Breeze™ SIP Entity is set as **SIP Entity 2**. Set the **Protocol** and **Port** (i.e TLS/5061).

Entity Links

Override Port & Transport with DNS SRV: ☐

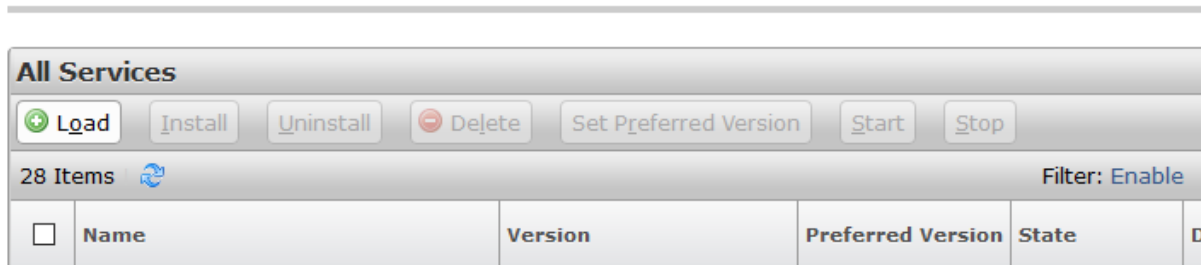
Add		Remove					
1 Item		Filter: Enable					
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* asm_abrz_5061_TLS	asm	TLS	* 5061	abrz	* 5061	trusted

Select : All, None

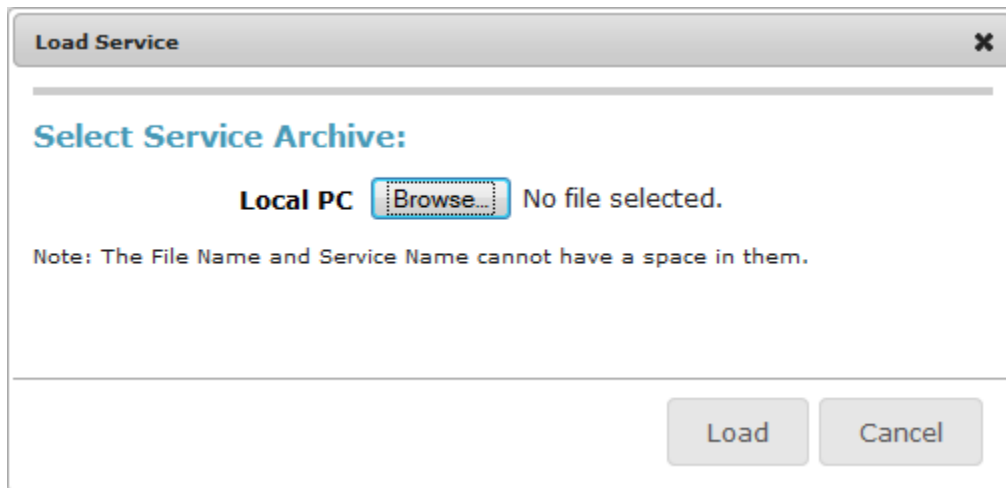
5.2. Deploy Avaya Engagement Designer

Obtain the Engagement Designer Snap-in and save the file to a local system. Navigate to **Home** → **Elements** → **Avaya Breeze™** → **Service Management**. Click the **Load** button.

Service Management



Click the **Browse** button, navigate to the Engagement Designer Snap-in svar file saved on the local system, and select it. Click the **Load** button to load the service.



The screen below shows **EngagementDesigner** has been loaded. Select the radio button to the left of the service and then click the **Install** button.

All Services						
<div> <div>Load</div> <div>Install</div> <div>Uninstall</div> <div>Delete</div> <div>Set Preferred Version</div> <div>Start</div> <div>Stop</div> </div>						
37 Items			Filter: Enable			
<input type="checkbox"/>	Name	Version	Preferred Version	State	Deployment Type	License Mode
<input type="checkbox"/>	AdminDataCollector	3.3.0.0.70501		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	AgentControllerService	3.3.0.0.70501		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	AuthorizationService	3.3.1.1.331105		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	AutomationController	3.3.0.0.70501		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	CallEventControl	3.3.1.1.331105		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	CCAManager	3.3.0.0.70501		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	CSCService	3.3.0.0.70501		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	CSManager	3.3.0.0.70501		✓ Installed	Java	✓
<input type="checkbox"/>	CSQuery	3.3.0.0.70501		✓ Installed	Java	✓
<input type="checkbox"/>	CSRest	3.3.0.0.70501		✓ Installed	Java	✓
<input type="checkbox"/>	CustomerControllerService	3.3.0.0.70501		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	CustomerManagement	3.3.0.0.70501		✓ Installed	Java	✓
<input type="checkbox"/>	EmailConnector	3.3.1.1.331105		✓ Loaded	Java	Not Applicable
<input type="checkbox"/>	EmailService	3.3.0.0.70501		✓ Installed	Java	Not Applicable
<input type="checkbox"/>	EngagementDesigner	3.3.0.0.25040		✓ Installed	Java	✓
<input checked="" type="checkbox"/>	EngagementDesigner	3.3.0.0.25042		✓ Loaded	Java	✓

During compliance testing, the service was installed on a single Breeze server within a cluster named **GeneralPurpose**. Select the cluster of server where the service will be installed and click the **Commit** button.

Confirm Install service: EngagementDesigner-3.3.0.0.25042

4 Items

Filter: Enable

<input type="checkbox"/>	Cluster Name
<input type="checkbox"/>	PresenceCluster
<input type="checkbox"/>	OceanaCluster1
<input type="checkbox"/>	OceanaCluster3
<input checked="" type="checkbox"/>	GeneralPurpose

Select : All, None

Commit

Cancel

Wait until the Engagement Designer Snap-in is **Installed** state.

<input type="checkbox"/>	EngagementDesigner	3.3.0.0.25042		✓ Installed	Java	✓	✓
<input type="checkbox"/>	EventingConnector	3.3.1.1.331105		✓ Installed	Java	Not Applicable	✓
						Not	Not

5.3. Install Arrow Connect™ Certificate

A certificate needs to be installed on Breeze cluster for the Arrow Connect tasks to work with Engagement Designer. Obtain the certificate from Arrow. Continuing from above, select **Cluster Administration** (not shown). Check box for the cluster where Engagement Designer is deployed and select **Certificate Management** → **Install Trust Certificate (All Avaya Breeze Instances)**.

	Details	Cluster Name	Cluster IP	Cluster Profile	Cluster State	Alarms	Activity	Cluster Database	Data Replic
<input checked="" type="checkbox"/>	Show	GeneralPurpose	10.64.110.42	General Purpose	Accepting [1/1]	0/0/0	0	[3/1.4G]	
<input type="checkbox"/>	Show	OceanaCluster1	10.64.111.9	Customer Engagement	Accepting [2/3]	0/0/0	0	[27/2.1G]	

Browse to the location of the certificate obtained from Arrow and select **Retrieve Certificate**. Select **Commit** to save the certificate.

Install Trusted Certificate

Bulk install trust certificate on all Avaya Breeze instances

Commit **Cancel**

Select Store Type to install trusted certificate All

*Please select a file Browse... No file selected.

You must click the Retrieve certificate button and review the certificate details before you can continue. **Retrieve Certificate**

Certificate Details	
Subject Details	CN=*.arrowconnect.io, OU=Technology, O="Arrow El
Valid From	Sun Jul 02 18:00:00 MDT 2017
Valid To	Wed Sep 11 06:00:00 MDT 2019
Key Size	2048
Issuer Name	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc,
Certificate Fingerprint	2f1e8d7063aee427a3fc4ca3c84a0c32e551c66c
CA Certificate	No

5.4. Install Arrow Connect™ Dynamic Tasks on Avaya Engagement Designer

Continuing from above, select **Cluster Administration** (not shown). Select the **Service URL** drop down for the cluster where Engagement Designer was deployed in previous section and click **Admin Console URL**.

Cluster Administration

This page allows you to view, edit and delete Avaya Breeze clusters.

Avaya Breeze Clusters

Edit

New

Delete

Certificate Management

Cluster State

Backup and Restore

4 Items

Filter: Enable

<input type="checkbox"/>	Details	Cluster Name	Cluster IP	Cluster Profile	Cluster State	Alarms	Activity	Cluster Database	Data Replication	Service Install Status	Tests Pass	Data Grid Status	Overload Status	Service URL
<input type="checkbox"/>	Show	GeneralPurpose	10.64.110.42	General Purpose	Accepting [1/1]	0/0/0	0	[1/998M]	✖	⚠	✓	Up [1/1]	✓	<div>Select</div>
<input type="checkbox"/>	Show	OceanaCluster1	10.64.111.9	Customer Engagement	Accepting [2/3]	0/0/0	0	[36/1.3G]	✖	✓	✓	Up [3/3]	✓	<div>Select</div>
<input type="checkbox"/>	Show	OceanaCluster3	10.64.111.24	Customer Engagement	Denying [0/1]	0/0/0	0	Disabled	✖	✓	✓	Up [1/1]	✓	<div>Admin Console URL</div>
<input type="checkbox"/>	Show	PresenceCluster	10.64.110.23	Core Platform	Accepting [1/1]	0/0/0	4	[5/53M]	✖	✓	✓	Up [1/1]	✓	<div>Designer Console URL</div>

Select : All, None

User Task Portal URL

Engagement Designer Admin Console will open in a new tab; log in using System Manager credentials. Select the **Bundles** tab at the top.

AVAYA

Engagement Designer

Administration Console

User Task PortalEngagement Designer

WorkflowsWorkflow DraftsInstancesEvent CatalogBundlesRouting

+ Create Instance

Undeploy Workflow

Attributes

Search

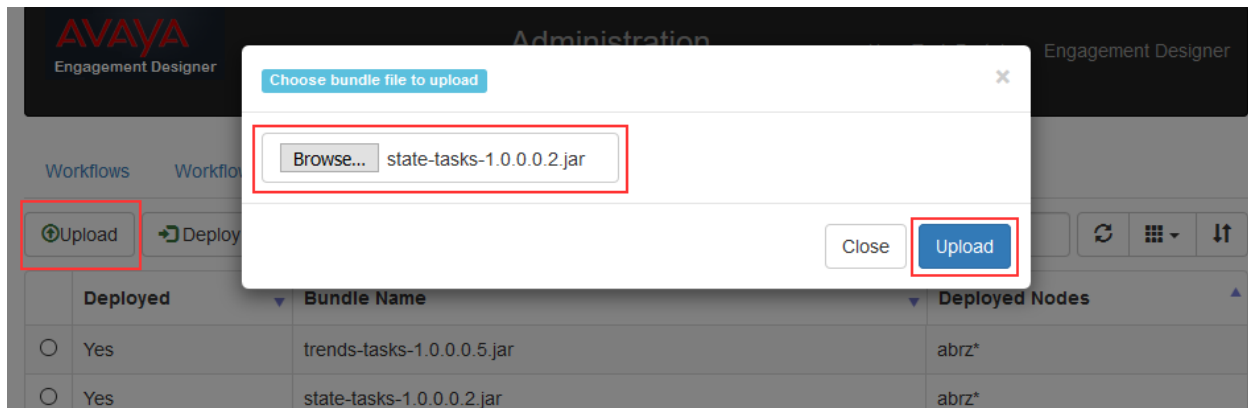
↺

⌵

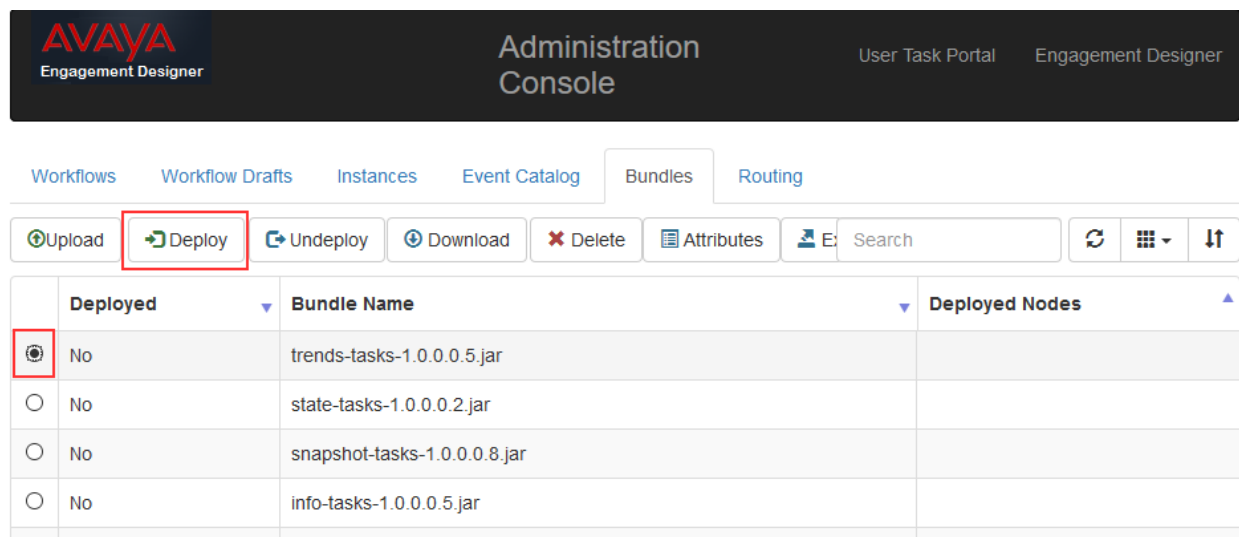
↻

	Workflow Name	Version	Description	Deployed By	Deployed On	Actions
<input type="radio"/>	Start_Thunder	6		admin	2017/10/27 13:45:46.045	<div><div></div><div></div></div>
<input type="radio"/>	Start_Thunder	5		admin	2017/10/27 13:30:23.030	<div><div></div><div></div></div>

Before proceeding, ensure all the tasks files for **Arrow Connect** have been obtained. Select **Upload** and **Browse** the task file; select **Upload**.



Follow same steps and upload all the Arrow Connect tasks. Once uploaded, select the radio button for a task and select **Deploy**.



Follow same steps and deploy all the Arrow Connect tasks.

AVAYA
Engagement Designer

Administration
Console

User Task PortalEngagement Designer

WorkflowsWorkflow DraftsInstancesEvent CatalogBundlesRouting

UploadDeployUndeployDownloadDeleteAttributes

Search

	Deployed	Bundle Name	Deployed Nodes
<input type="radio"/>	Yes	trends-tasks-1.0.0.0.5.jar	abrz*
<input type="radio"/>	Yes	state-tasks-1.0.0.0.2.jar	abrz*
<input type="radio"/>	Yes	snapshot-tasks-1.0.0.0.8.jar	abrz*
<input type="radio"/>	Yes	info-tasks-1.0.0.0.5.jar	abrz*
<input type="radio"/>	Yes	deviceMgmt-tasks-1.0.0.0.6.jar	abrz*
<input type="radio"/>	Yes	action-tasks-1.0.0.0.5.jar	abrz*
<input type="radio"/>	Yes	EngagementDesignerTasks-3.3.0.0.25042.jar	abrz*

5.5. Create an Avaya Engagement Designer Workflow

Before generating a workflow, perform the steps in **Section 6**. Via System Manager Web Console, navigate to **Home → Avaya Breeze™ → Cluster Administration**. Select the **Service URL** drop down for the cluster where Engagement Designer was deployed in previous section and click **Designer Console URL**.

Cluster Administration

This page allows you to view, edit and delete Avaya Breeze clusters.

Avaya Breeze Clusters

Edit

New

Delete

Certificate Management

Cluster State

Backup and Restore

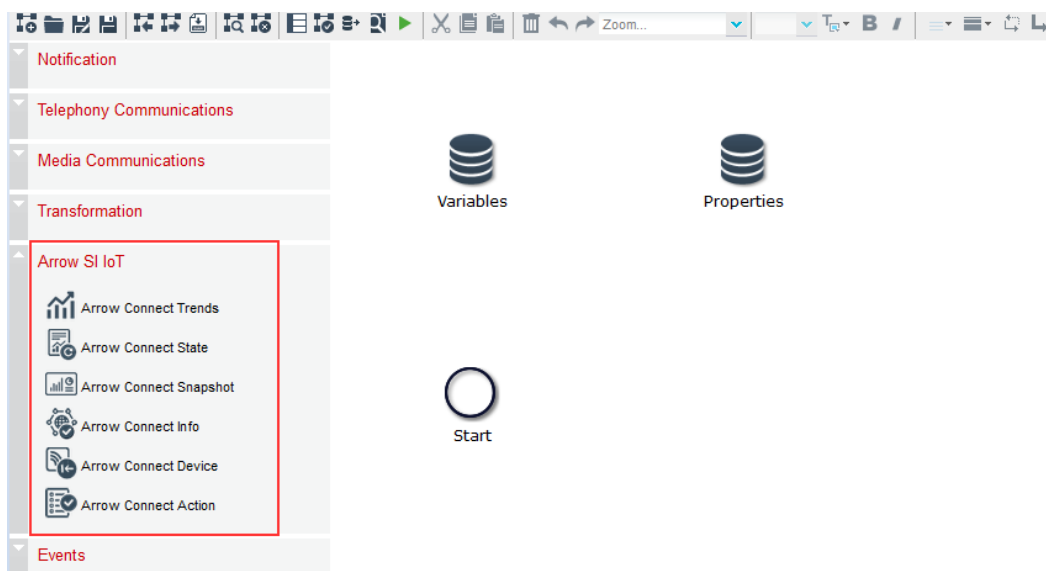
4 Items

Filter: Enable

<input type="checkbox"/>	Details	Cluster Name	Cluster IP	Cluster Profile	Cluster State	Alarms	Activity	Cluster Database	Data Replication	Service Install Status	Tests Pass	Data Grid Status	Overload Status	Service URL
<input type="checkbox"/>	Show	GeneralPurpose	10.64.110.42	General Purpose	Accepting [1/1]	0/0/0	0	[1/998M]	✖	⚠	✓	Up [1/1]	✓	Select
<input type="checkbox"/>	Show	OceanaCluster1	10.64.111.9	Customer Engagement	Accepting [2/3]	0/0/0	0	[36/1.3G]	✖	✓	✓	Up [3/3]	✓	Select
<input type="checkbox"/>	Show	OceanaCluster3	10.64.111.24	Customer Engagement	Denying [0/1]	0/0/0	0	Disabled	✖	✓	✓	Up [1/1]	✓	Admin Console URL
<input type="checkbox"/>	Show	PresenceCluster	10.64.110.23	Core Platform	Accepting [1/1]	0/0/0	4	[5/53M]	✖	✓	✓	Up [1/1]	✓	Designer Console URL

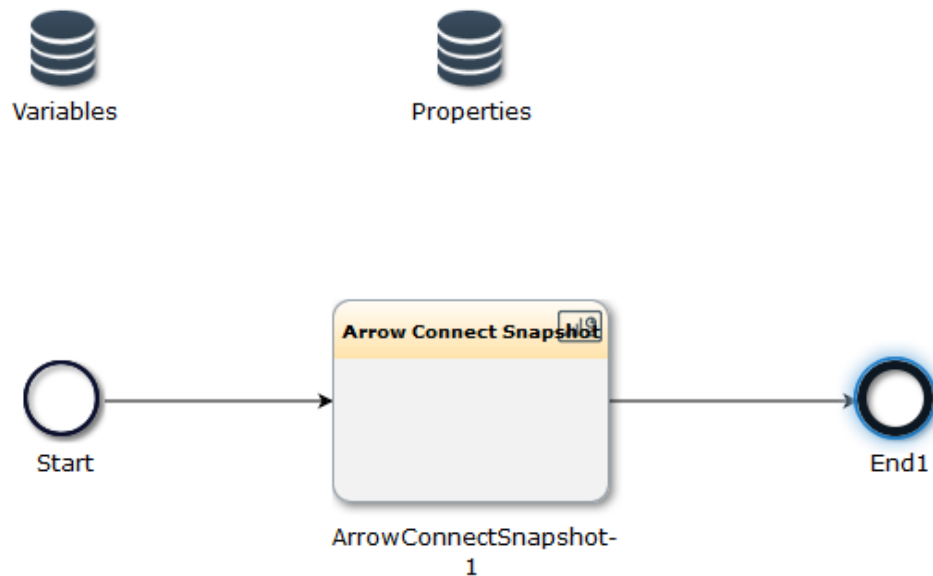
Select : All, None

On the left pane, ensure all the Arrow Connect tasks deployed via Engagement Designer are available.

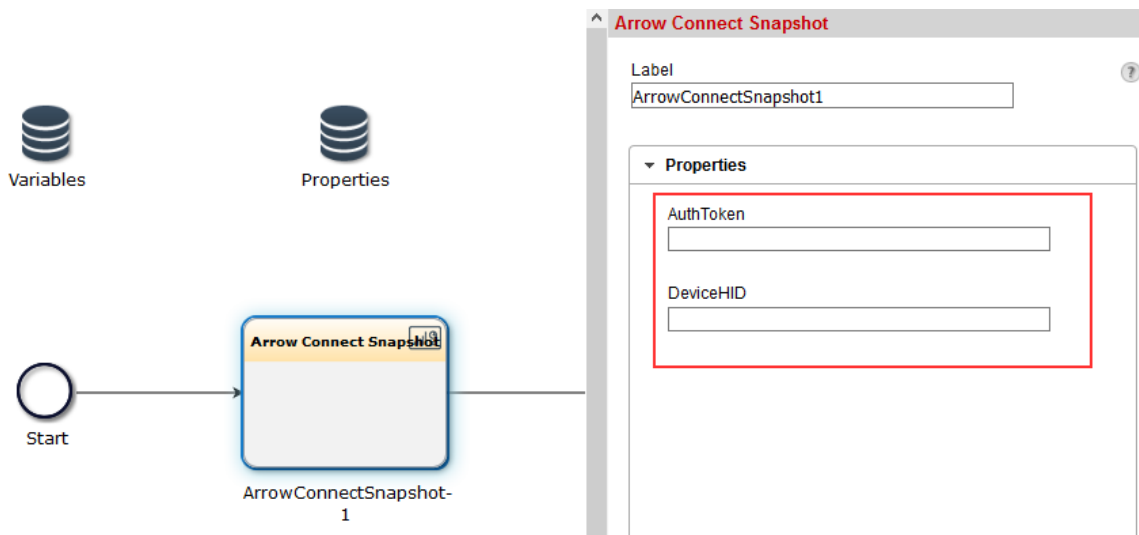


To create a simple workflow:

- Drag an Arrow Connect task to the designer board; **Arrow Connect Snapshot** in this case. Arrow Connect Snapshot is used to retrieve the last collected values in the Arrow Connect cloud for a particular device.
- From the **Events** (not shown), drag **End** to the designer board.
- Connect the tasks.



Depending on the Arrow Connect task, different values will need to be configured. Arrow Connect Snapshot requires the values highlighted below; enter the values. Save the workflow.



6. Configure Arrow Connect™ IoT Solution

An account will need to be created to manage Arrow Connect Gateway and sensor devices. Via a browser navigate to the Arrow Connect Portal, <https://portal.arrowconnect.io>, enter pertinent information and select **Sign up** to complete registration.

Arrow Connect™


ARROW IOT

SIGN IN

SIGN UP


IoT Arrow Connect - Arrow.com

Arrow Connect



ARROW | Internet of Things

Rapid sensor to cloud development, flexible data platform options and comprehensive IoT solution management are just a few clicks away.



- Support for up to 50 concurrent devices

DEVELOPER REGISTRATION

Email*

First Name*

Last Name*

Title*

Company Name*


Company Web Site*

Project Description*

Referral Code

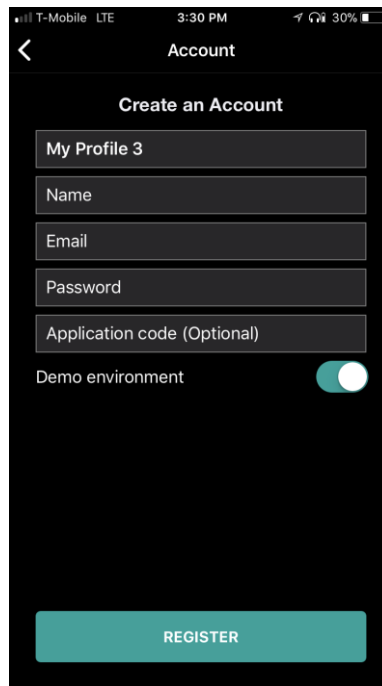
Event Code

☐ I'm not a robot


reCAPTCHA
Privacy - Terms

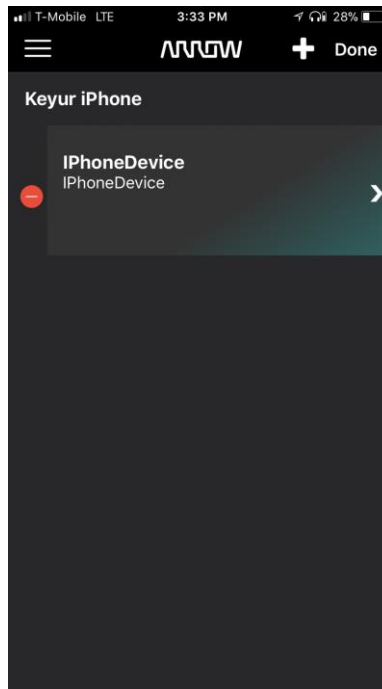
Sign up

Once an account is created, download the **Arrow Connect Gateway** app on an iOS or Android device. Once downloaded, open the app and finish registration using the same credentials as above.

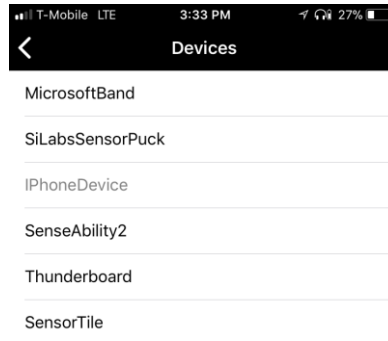


The screenshot shows the 'Create an Account' screen of the Arrow Connect Gateway app. The status bar at the top indicates 'T-Mobile LTE', '3:30 PM', and '30%' battery. The screen has a dark background with white text. At the top, there is a back arrow and the title 'Account'. Below this is the heading 'Create an Account'. The form contains five input fields: 'My Profile 3', 'Name', 'Email', 'Password', and 'Application code (Optional)'. Below the fields is a toggle switch for 'Demo environment', which is currently turned on. At the bottom of the screen is a large teal button labeled 'REGISTER'.

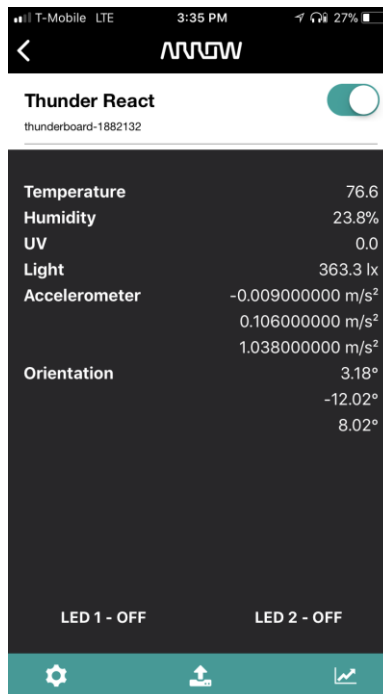
Select the pencil icon on the left top to add a device (not shown); followed by + icon. The iPhoneDevice shown below is a previously added device.



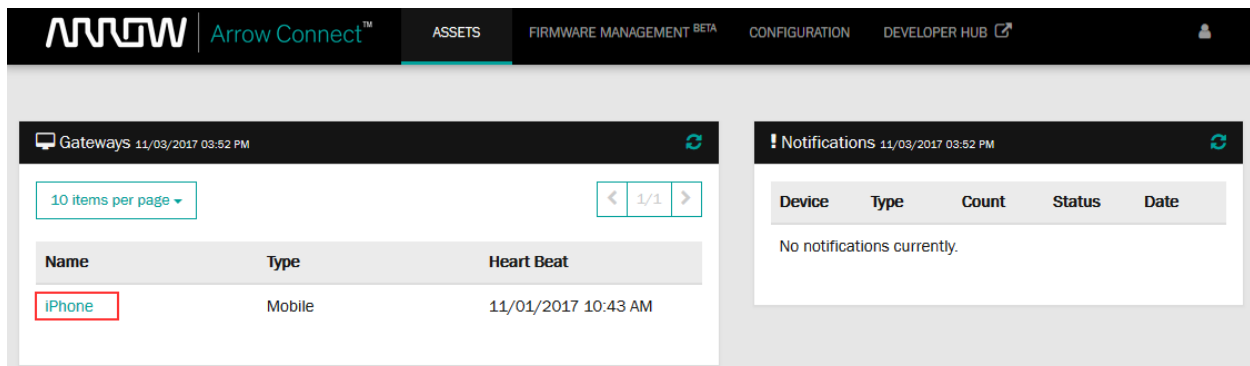
In this case, **Thunderboard** was selected; select **Done** (not shown). During compliance testing, **Thunderboard** and **SiLabSensorPuck** were used. These devices communicate to the Gateway app via Bluetooth.



Select **Thunderboard**. Turn on the physical Thunder Board device by tapping on the power button and in the Gateway app to turn it on. Verify the app is receiving data from Thunder Board.



A few values need to be obtained via Arrow Connect Portal. Log onto the Arrow Connect Portal. To obtain the AuthToken and GatewayHID values, select the gateway; **iPhone** in our case.



On the left pane, select **Access Keys** followed by the key under **Raw Api Key**.

The screenshot shows the Arrow Connect web interface. On the left sidebar, the 'Access Keys' menu item is highlighted with a red box. The main content area displays the 'iPhone' device page. Below the device name, there is a list of access keys. The first key is highlighted with a red box in the 'Raw Api Key' column.

Raw Api Key	Name	Owner	Expired	Expiration Date
860e66d1f7...		Gateway: iPhone	false	07/29/2037 02:13:40 PM

Showing 1 to 1 of 1 access keys

Copy the **Raw Api Key** into a word editor; this value is the AuthToken. At the bottom of the page under **Privileges**, copy the value after **arw:pgs:gwyr:** into a word editor; this value is GatewayHID. For security reasons, these values have been blurred.

Name

Name is required

Expiration Date

07/29/2037 02:13:40 PM

Expire No

Raw Api Key

Privileges

Add

Level	PRI	Name	Actions
OWNER	arw:pgs:gwyr: [blurred]	Gateway: iPhone	

Continuing from above, navigate to **ASSETS → Devices → Thunder React → Developer**. As shown below, copy the value into a word editor; this value is DeviceHID.

Telemetry

Export Telemetry

Device State

Firmware Management

Audit Logs

Developer

Test Results

INGESTION

ACCESS KEYS

COMMAND

Device

Device Type: silabs-thunderboard-react

UID: thunderboard-1882132

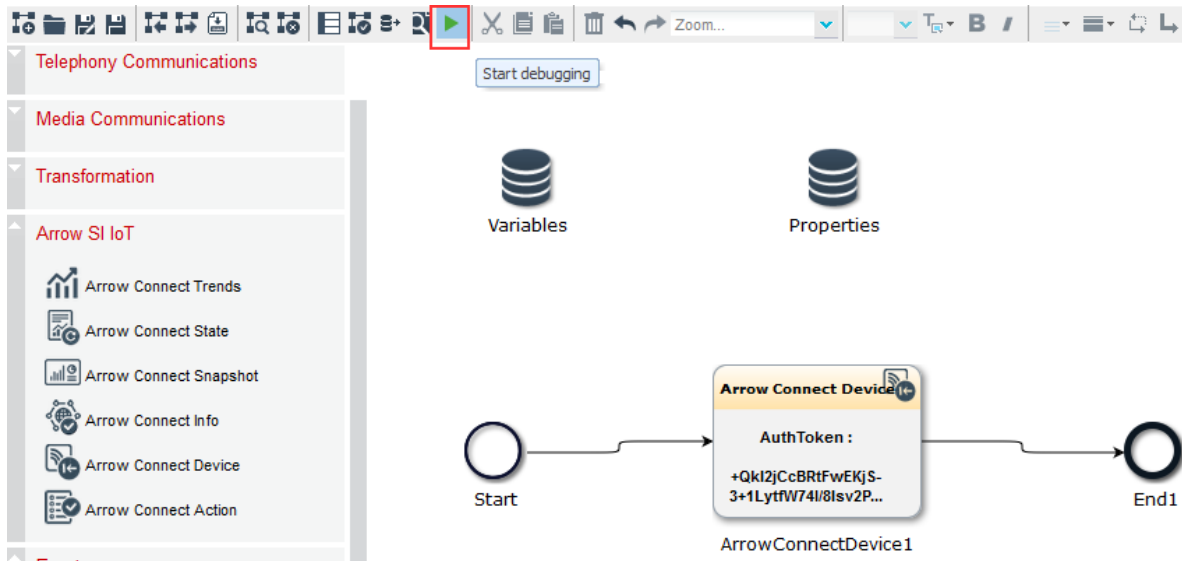
HID: [blurred]

Feed

7. Verification Steps

This section includes steps that can be followed to verify the configuration.

Log onto Engagement Designer portal and open the workflow created in this document. To verify the configured Arrow Connect tasks, select **Start Debugging**.



Select the Play icon to continue debugging, and wait until completed. Once completed, select the Arrow Connect task. Under the **Debugger Console**, verify the **Output result** is **Success**. This validates that the Arrow Connect task was executed successfully.

The screenshot displays the Arrow IoT Studio interface. At the top, a toolbar contains various icons, with the 'Play' icon (a green triangle) highlighted by a red box. Below the toolbar, the workflow canvas shows a sequence of nodes: a 'Start' node, an 'Arrow Connect Device' node, and an 'End1' node. The 'Arrow Connect Device' node is highlighted with a red box and contains the following details:

- AuthToken :**
- +Qk12jCcBRtFwEKjS-3+1YtFw74l/8IsV2P...**
- ArrowConnectDevice1**

To the right of the workflow canvas is the 'Debugger Console' panel. It displays the following information:

- Instance status :** Completed
- Selected node status**

Name	ArrowConnectDevice1
State	Completed
- Variables:**

system	system Expand
--------	-----------------------------------
- Output data:**

Output	OutputSchema Collapse result Success
--------	--

8. Conclusion

The Arrow Connect IoT solution completed compliance testing. These Application Notes describe the configuration steps required to integrate Arrow Connect IoT solution with Avaya Breeze™ (Breeze).

9. Additional References

Product documentation for Avaya products may be found at: <http://support.avaya.com>.

[1] Administering Avaya Aura® Avaya Breeze™, Release 3.3, Issue 2, June 2017

[2] Avaya Engagement Designer Reference, Release 3.3, Issue 2, September 2017

Product documentation for Arrow Connect™ may be obtained directly from Arrow:

[3] Arrow Systems Integration IoT and Zang™ Integration Toolkit V3.0

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.