Cisco Connected Assets - Site Asset Management 1.0 Implementation Guide

November 2015

Cisco Validated Design

Building Architectures to Solve Business Problems

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Connected Assets - Site Asset Management 1.0 Implementation Guide

CHAPTER 1 **Overview of Solution** 1-1

CHAPTER 2 **Installation** 2-1

Prerequisites for Installation 2-1
  Procuring Cisco Software and Hardware 2-1
  Procuring Third-Party Software and Hardware 2-1

Cloud-Side Installation 2-1
  CAM Installation 2-2
    Installation of CAM Server 2-2
    Installation of CAM Controller 2-9
  ACP Installation 2-15
    Integration of CAM with ACP 2-15
    MQTT Photos Configuration 2-25
  Network Setup 2-28
    VPN Server Configuration 2-28

Remote Site installation 2-33
  Network Setup 2-33
    Deployment Option -1: Sensors Only with 3G as WAN Backup 2-33
    Deployment Model - 2: Sensors plus Camera with 4G as WAN Backup 2-35

Site Controller Installation 2-39
  External Modules Installation 2-39
  Internal Module Installation 2-39
  Basic Configuration of Site Controller 2-42
    Run Mosquito and Site Controller Application 2-42

Setting Up the Sensor Network 2-43
  Method of Slave Address Configuration 2-43
    Configure Slave Address using modpoll.exe 2-43
    Configure Slave Address using Adam Utility 2-44
    Configure ADAM-4117-AE 2-44
    Configure ADAM-4150-AE 2-47
    Configure Slave Address using DIP Switch 2-52
    Configure Slave Address using Jumper 2-52
  Standard Slave Address Plan 2-53
  General Wiring 2-54
    WattsOn-1100-MS360-500A and MS360 2-54
    DC Voltage Meter CE-AU11-34MS3-0.2/0-65V 2-55
    Fuel Sensor Mounting 2-55
  Connectivity Diagram 2-56

IP Camera Installation 2-57

CHAPTER 3 Site Configuration 3-1

New Site Template Creation 3-1

Adding a New Site and Applying a Site Template 3-10

Site Template Customization 3-13

Use-Case: Door Access 3-13

Door Access Work Flow Diagram 3-13

Configuration Detail 3-14

Providing User Access to Site by Using ACP 3-15

Editing Timer T2 Parameter for Door Access 3-18

Configuring Threshold for Service Comet_Humidity_Status 3-19

Use Case: Fuel Theft 3-21

Work Flow Diagram 3-21

Configuration Detail 3-22

Use Case: Picture Snapshot 3-23

Flow Diagram 3-23

Configuration Detail 3-24

Use Case: HVAC Management and Power Monitoring 3-25

CHAPTER 4 Monitoring and Reporting 4-1

Setting Up Dashboard 4-1

Prerequisites for Creating a Dashboard 4-1

Get DQL ID of Asset 4-1

Creation of Custom Report 4-5

Dashboard 4-12

Add Widget 4-14

Dashboard Customization 4-21

Creating Total Energy Consumption 4-21

Door Opening Log for the Last Seven Days 4-22

Total Energy Cost for COLT 4-24

Generator Status for the Last Seven Days 4-25

Camera View - Generator 4-27

Camera View - Alley 1 4-28

Floor Plan 4-29

Reports Customization 4-33

Use Cases for Notification using Policy 4-39

Energy Consumption 4-39

Generator Startup Problem 4-40

Temperature Warning for Door Status 4-40

Current Warning for Door Status 4-41

Multi-Tenant Setup 4-42

APPENDIX A Troubleshooting A-1

Information Flow A-1

Flow of Information When the System Starts A-1

Information Flow for a Data Acquisition Module A-1

Information Flow for Automatic Control-Based on Parameters A-2

Troubleshooting Scenario A-3

Services Show Timed Out in Cloud A-3

Services Show Wrong Value in Cloud A-4

Event Is Not Raised for Service A-5

CAM Shows Location Disconnected A-5

APPENDIX B Sensor - Data Sheets B-1

Sensor - Data Sheets B-1

Advantech Input/Output Modules B-1

Adam 4117 B-1

Adam 4150 B-2

WattsOn-1100-MS360-500A and MSCT2 B-2

DC Multiparameter CE AD11B-34GS4-1.0/0-250A*0-65V B-3

DC Voltage Meter CE-AU11-34MS3-0.2/0-65V B-4

Comet T3411 B-5

Analog Sensors B-5

Fuel Level Sensor: AST 4510 - 5PSI - Pressure Sensor B-5

AC On/Off Current Transducer i-Snail-S B-6

AC Current Transducer i-Snail-VC B-7

Use Case: Complete Door Access B-9

Configuration Detail B-9

CHAPTER 1

Overview of Solution

This CVD 1.0 addresses the design and implementation details of SAM. SAM solutions can be deployed for various use cases with unmanned remote site assets. Typical examples include the following:

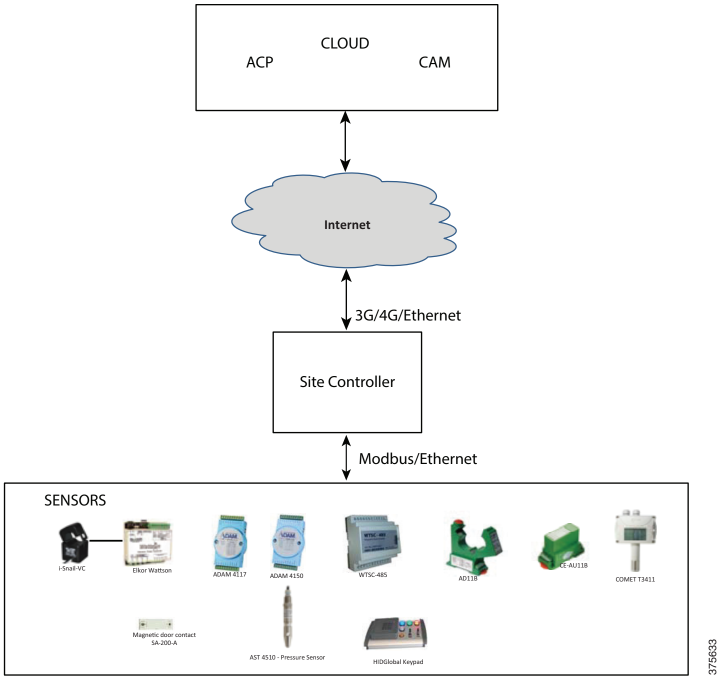
- Cell towers, COLT/COW (Cell on Light Truck, Cell on Wheel)
- Utility substations
- Oil and gas pump sites
- Remote branch offices

The overall solution consists of three major components:

- Cloud - CAM,VPN server and ACP
- Network connectivity with option Ethernet / 3G /4G
- Site Controller and Sensors

The Azeti Control Panel (ACP) and Cisco Asset Manager (CAM) are the front-end application servers hosted in the Cloud. CAM is used for reporting and analytic. ACP is used for provisioning sensors and collecting data from the site controller. The site controller is connected to the Cloud using either Ethernet or 3G/4G. The sensors communicate to site controller by using either Modbus or Ethernet. The data is secured over the internet Cloud by using IPSec VPN.

Figure 1-1 Deployment 1- Sensor Only System Setup



Installation

This section covers the installation process of the Cloud and remote site location. The following process is listed below:

- Prerequisites for Installation
- Cloud Side Installation
- Remote Site Installation
- Site Controller Installation
- Setting up Sensor Network
- IP Camera Installation

Prerequisites for Installation

The following sections discuss the prerequisites for installation.

Procuring Cisco Software and Hardware

Cisco software and hardware, along with licenses, can be procured from Cisco CCO.

Procuring Third-Party Software and Hardware

On receipt of the PO from the customer, Cisco will procure and supply required the s/w and h/w along with the required licenses to the customer. This includes software packages for ACP, site controller and sensor hardware.

Cloud-Side Installation

This section covers installation of CAM, ACP, and Network setup for the Cloud side.

CAM Installation

This section provides the steps for installation of Cloud CAM. Cloud CAM has two components: the CAM server and the CAM controller (standalone deployment).

Installation of CAM Server

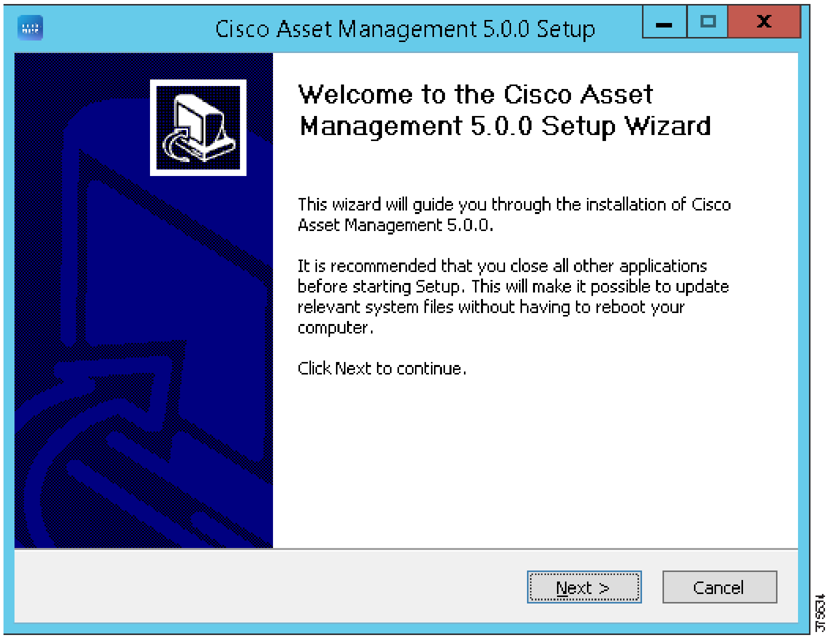
To install the CAM server, complete the following steps:

Step 1 The VM Machine is created in the Cloud with the Windows server 2012 operating system and two NIC cards. One NIC card is used to communicate with all other servers in the Cloud, such as ACP, and second NIC port is connected in Public IP pool. The customer manages the CAM server by using either Public IP address or Private IP address.

Step 2 Download the installation file of CAM (**CiscoAssetManagement_server_x64_40903_trunk**) from the following link: https://software.cisco.com/download/navigator.html.

Step 3 Select **Next**. Figure 2-1 shows the Setup Wizard Welcome screen.

Figure 2-1 Cisco Asset Management Setup Wizard



Cisco Asset Management 5.0.0 Setup

Welcome to the Cisco Asset Management 5.0.0 Setup Wizard

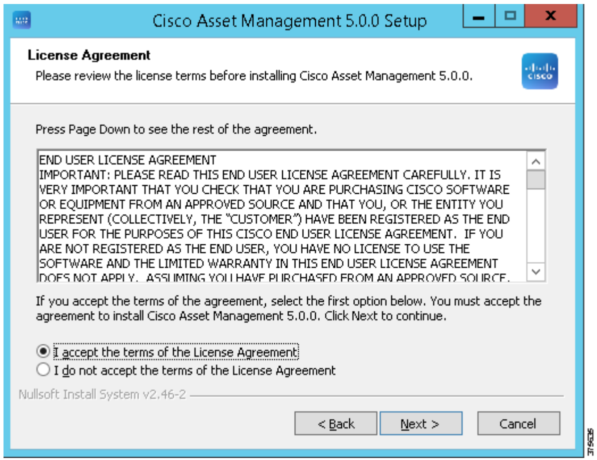
This wizard will guide you through the installation of Cisco Asset Management 5.0.0.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Step 4 Accept the terms of the license agreement, as shown in Figure 2-2.

Figure 2-2 License Agreement



License Agreement

Please review the license terms before installing Cisco Asset Management 5.0.0.

Press Page Down to see the rest of the agreement.

END USER LICENSE AGREEMENT
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER, YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE.

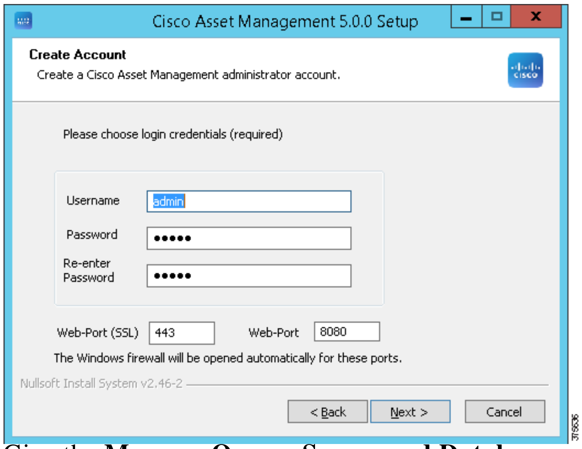
If you accept the terms of the agreement, select the first option below. You must accept the agreement to install Cisco Asset Management 5.0.0. Click Next to continue.

● I accept the terms of the License Agreement
○ I do not accept the terms of the License Agreement

Nullsoft Install System v2.46-2

Step 5 Give the new user name and password for the new account to be created, as shown in Figure 2-3.

Figure 2-3 Create Account



Create Account

Create a Cisco Asset Management administrator account.

Please choose login credentials (required)

Username: admin
Password: •••••
Re-enter Password: •••••

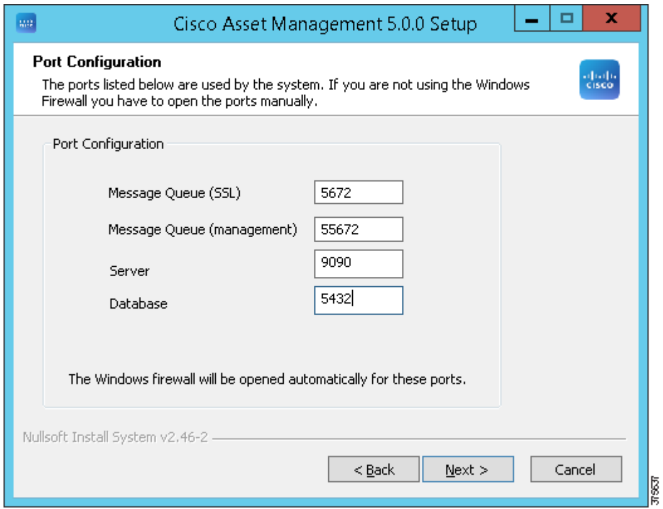
Web-Port (SSL): 443 Web-Port: 8080

The Windows firewall will be opened automatically for these ports.

Nullsoft Install System v2.46-2

Step 6 Give the **Message Queue, Server and Database** parameters under Port Configuration. Use the default port configuration.

Figure 2-4 Port Configuration



Cisco Asset Management 5.0.0 Setup

Port Configuration

The ports listed below are used by the system. If you are not using the Windows Firewall you have to open the ports manually.

Port Configuration

Message Queue (SSL): 5672

Message Queue (management): 55672

Server: 9090

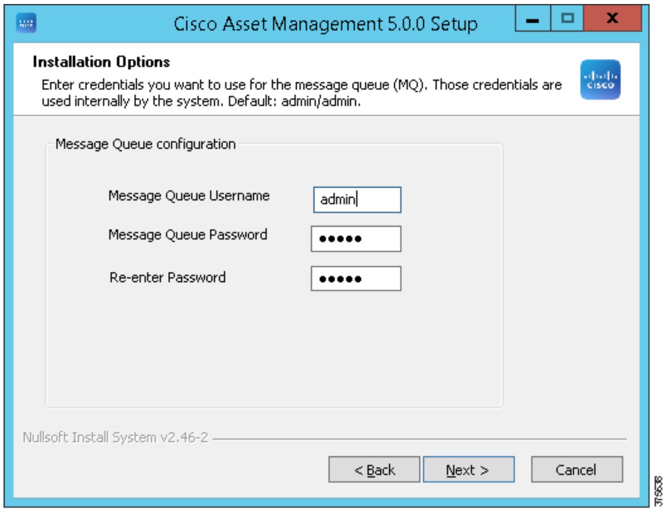
Database: 5432

The Windows firewall will be opened automatically for these ports.

Nullsoft Install System v2.46-2

Step 7 Give the username and password credentials to use for Message Queue (MQ), as shown in Figure 2-5.

Figure 2-5 Message Queue Credentials



Cisco Asset Management 5.0.0 Setup

Installation Options

Enter credentials you want to use for the message queue (MQ). Those credentials are used internally by the system. Default: admin/admin.

Message Queue configuration

Message Queue Username: admin

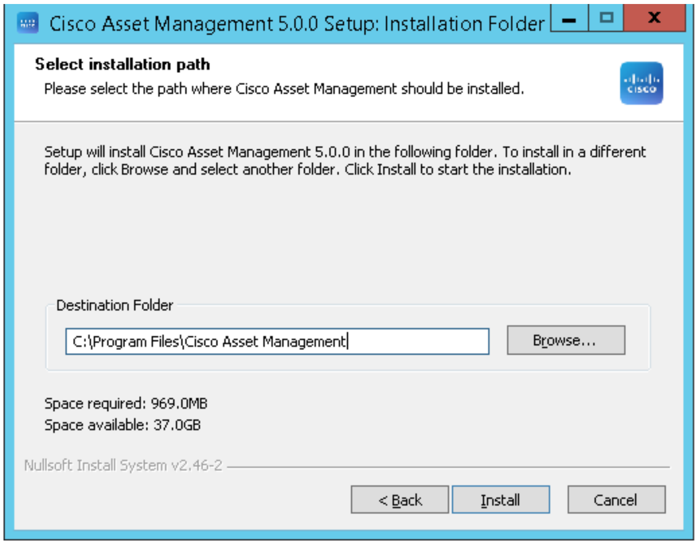
Message Queue Password: •••••

Re-enter Password: •••••

Nullsoft Install System v2.46-2

Step 8 Select the destination folder where the server has to be installed, as shown in Figure 2-6.

Figure 2-6 Server Installation Destination Folder



Cisco Asset Management 5.0.0 Setup: Installation Folder

Select installation path

Please select the path where Cisco Asset Management should be installed.

Setup will install Cisco Asset Management 5.0.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

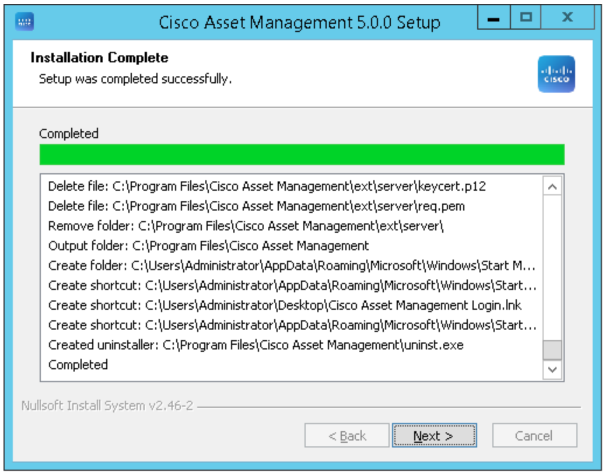
C:\Program Files\Cisco Asset Management

Space required: 969.0MB
Space available: 37.0GB

Nullsoft Install System v2.46-2

Step 9 Select **Next** after the installation gets completed, as shown in Figure 2-7.

Figure 2-7 Install Complete



Cisco Asset Management 5.0.0 Setup

Installation Complete

Setup was completed successfully.

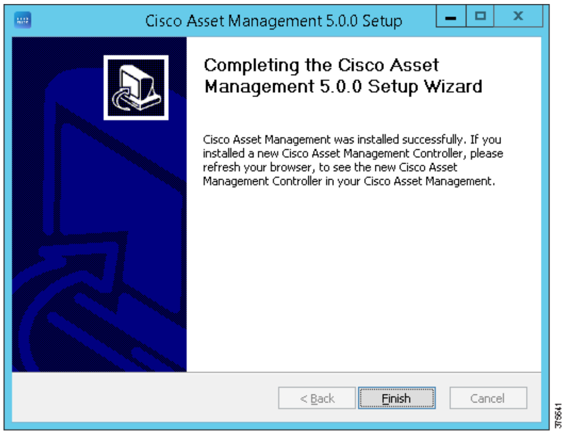
Completed

```
Delete file: C:\Program Files\Cisco Asset Management\ext\server\keycert.p12
Delete file: C:\Program Files\Cisco Asset Management\ext\server\req.pem
Remove folder: C:\Program Files\Cisco Asset Management\ext\server\
Output folder: C:\Program Files\Cisco Asset Management
Create folder: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start M...
Create shortcut: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start...
Create shortcut: C:\Users\Administrator\Desktop\Cisco Asset Management Login.lnk
Create shortcut: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start...
Created uninstaller: C:\Program Files\Cisco Asset Management\uninst.exe
Completed
```

Nullsoft Install System v2.46-2

Step 10 Finish the installation by selecting **Finish** option, as shown in Figure 2-8.

Figure 2-8 Completing the Setup Wizard

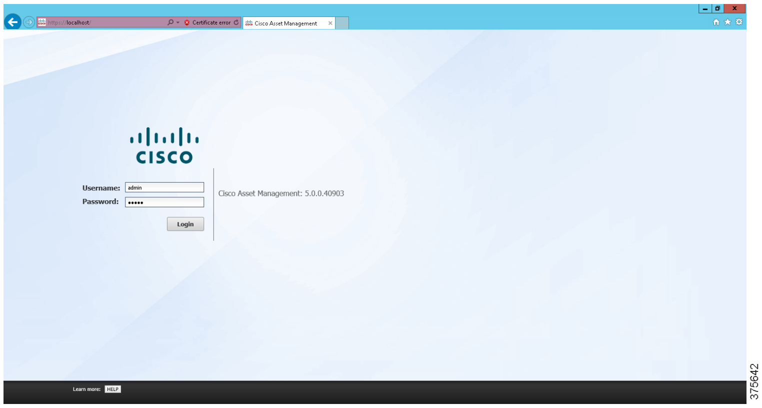


Completing the Cisco Asset Management 5.0.0 Setup Wizard

Cisco Asset Management was installed successfully. If you installed a new Cisco Asset Management Controller, please refresh your browser, to see the new Cisco Asset Management Controller in your Cisco Asset Management.

Step 11 Log in to the CAM webpage using **admin** as the username and its corresponding password set in Step 5, as shown in Figure 2-9.

Figure 2-9 Log in Credentials

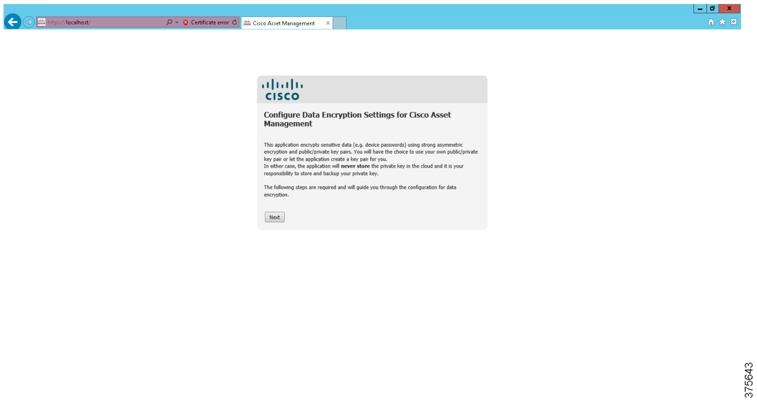


Username: admin
Password: •••••

Cisco Asset Management: 5.0.0.40903

Step 12 To configure data encryption settings for CAM, click **Next,** as shown in Figure 2-10.

Figure 2-10 Data Encryption



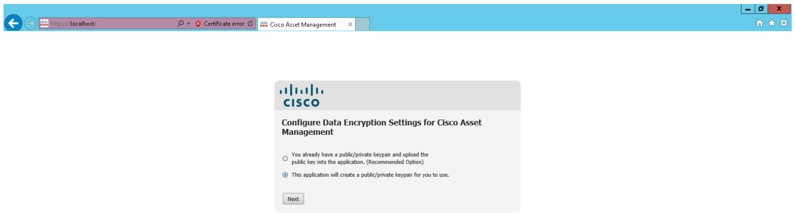
Configure Data Encryption Settings for Cisco Asset Management

This application encrypts sensitive data (e.g. device passwords) using strong asymmetric encryption and public/private key pairs. You will have the choice to use your own public/private key pair or let the application create a key pair for you.
In either case, the application will **never store** the private key in the cloud and it is your responsibility to store and backup your private key.

The following steps are required and will guide you through the configuration for data encryption.

Step 13 For a first time installation, there has to be a new public/private key pair, which needs to be generated, as shown in Figure 2-11. The generated key will be used in Step 4 of the CAM controller installation.

Figure 2-11 Public/Private Key Pair



Configure Data Encryption Settings for Cisco Asset Management

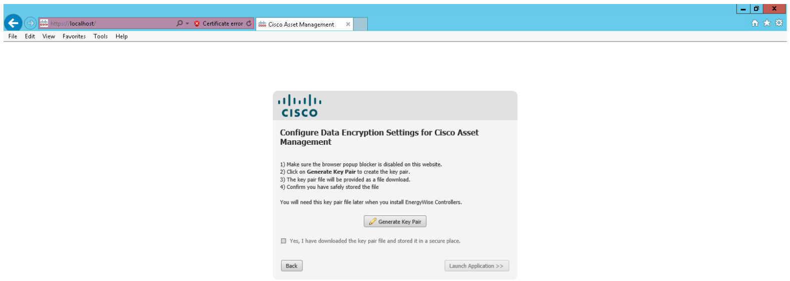
○ You already have a public/private keypair and upload the public key into the application. (Recommended Option)

● This application will create a public/private keypair for you to use.

Next

Step 14 Select the **Generate Key Pair** option to get a new key file, as shown in Figure 2-12.

Figure 2-12 Generate Key Pair



Configure Data Encryption Settings for Cisco Asset Management

1) Make sure the browser popup blocker is disabled on this website.
2) Click on **Generate Key Pair** to create the key pair.
3) The key pair file will be provided as a file download.
4) Confirm you have safely stored the file

You will need this key pair file later when you install EnergyWise Controllers.

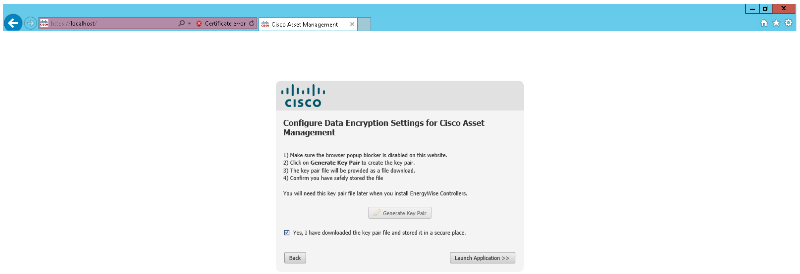
Generate Key Pair

□ Yes, I have downloaded the key pair file and stored it in a secure place.

Back Launch Application >>

Step 15 After the file is downloaded, select the option **Launch Application**, as shown in Figure 2-13.

Figure 2-13 Launch Application



Configure Data Encryption Settings for Cisco Asset Management

1) Make sure the browser popup blocker is disabled on this website.
2) Click on **Generate Key Pair** to create the key pair.
3) The key pair file will be provided as a file download.
4) Confirm you have safely stored the file

You will need this key pair file later when you install EnergyWise Controllers.

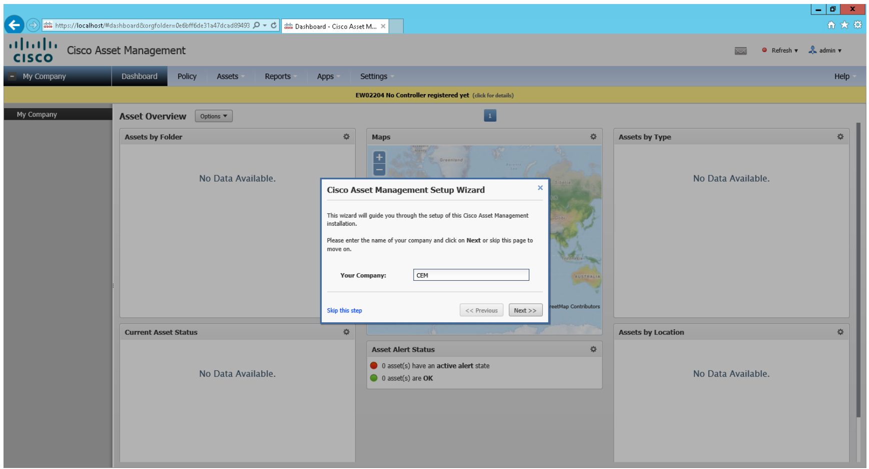
Generate Key Pair

☑ Yes, I have downloaded the key pair file and stored it in a secure place.

Back Launch Application >>

Step 16 Give a company name as shown in Figure 2-14.

Figure 2-14 Company Name



EW02204 No Controller registered yet (click for details)

Cisco Asset Management Setup Wizard

This wizard will guide you through the setup of this Cisco Asset Management installation.

Please enter the name of your company and click on **Next** or skip this page to move on.

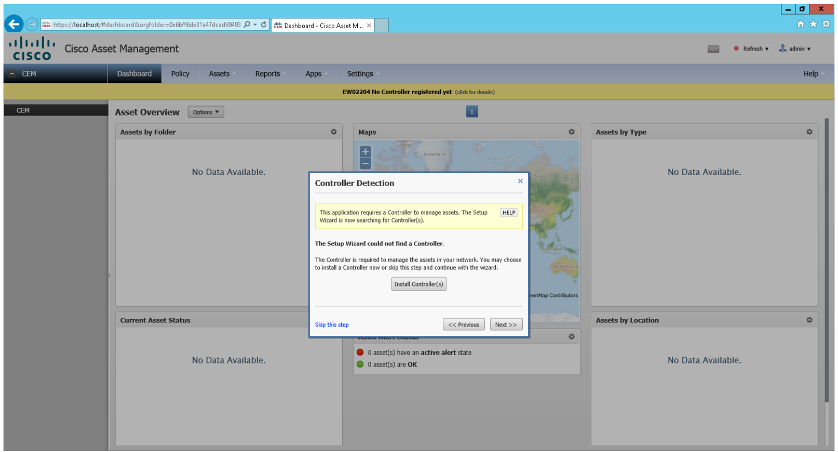
Your Company: CEM

Skip this step | << Previous | Next >>

0 asset(s) have an **active alert** state
0 asset(s) are **OK**

Step 17 Select **Install Controller** for the controller to be detected, as shown in Figure 2-15.

Figure 2-15 Controller Detection



EW02204 No Controller registered yet (click for details)

Controller Detection

This application requires a Controller to manage assets. The Setup Wizard is now searching for Controller(s). HELP

The Setup Wizard could not find a Controller.

The Controller is required to manage the assets in your network. You may choose to install a Controller now or skip this step and continue with the wizard.

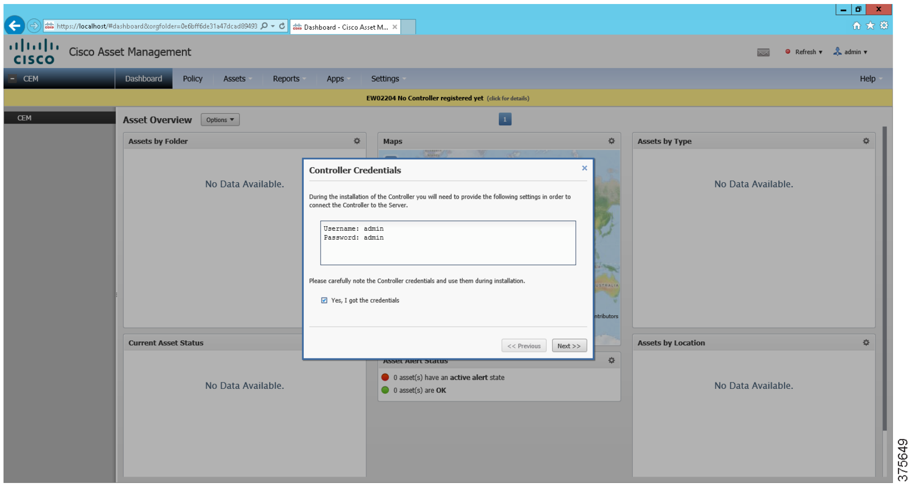
Install Controller(s)

Skip this step | << Previous | Next >>

0 asset(s) have an **active alert** state
0 asset(s) are **OK**

Step 18 Enter the Controller Credentials and select **Next**, as shown in Figure 2-16.

Figure 2-16 Controller Credentials



EW02204 No Controller registered yet (click for details)

Controller Credentials

During the installation of the Controller you will need to provide the following settings in order to connect the Controller to the Server.

```
Username: admin
Password: admin
```

Please carefully note the Controller credentials and use them during installation.

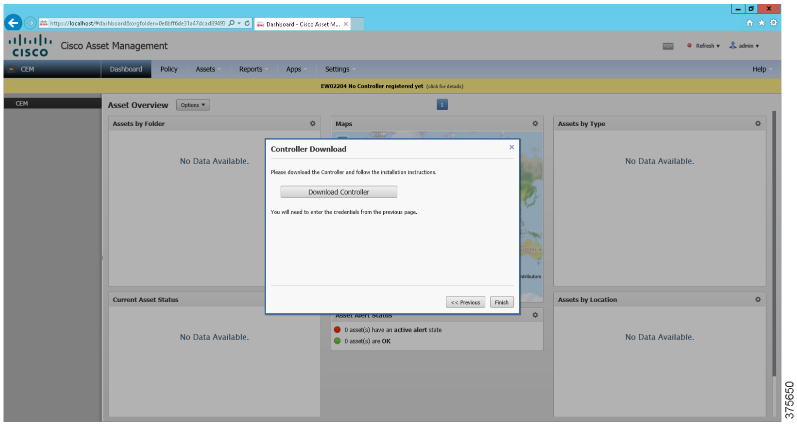
☑ Yes, I got the credentials

<< Previous | Next >>

0 asset(s) have an **active alert** state
0 asset(s) are **OK**

Step 19 Select Finish to finish the CAM server installation, as shown in Figure 2-17.

Figure 2-17 Finish CAM Server Install



EW02204 No Controller registered yet (click for details)

No Data Available.

Controller Download

Please download the Controller and follow the installation instructions.

You will need to enter the credentials from the previous page.

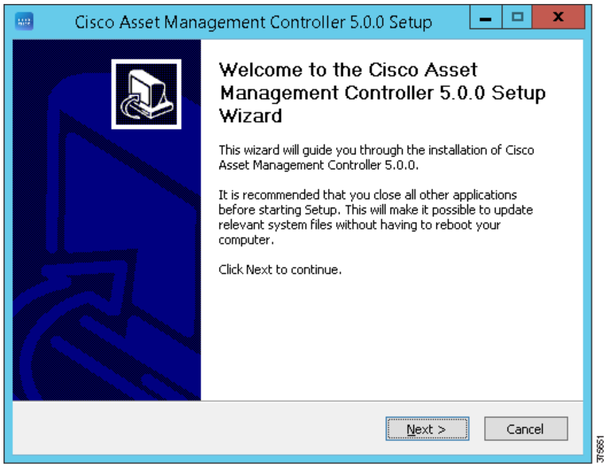
0 asset(s) have an **active alert** state

0 asset(s) are **OK**

Installation of CAM Controller

Step 1 Select the setup file named **CiscoAssetManagement_controller_x64_40903_trunk** to begin the controller installation. Click **Next** when Figure 2-18 appears.

Figure 2-18 Controller Setup Wizard



Welcome to the Cisco Asset Management Controller 5.0.0 Setup Wizard

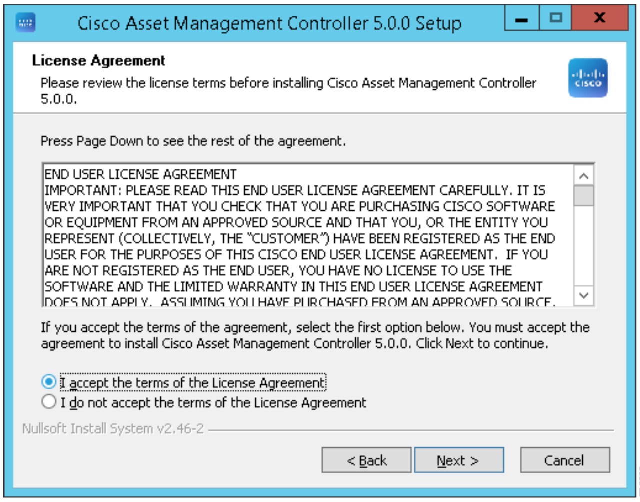
This wizard will guide you through the installation of Cisco Asset Management Controller 5.0.0.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Step 2 Accept the terms of the license agreement, as shown in Figure 2-19.

Figure 2-19 Controller License Agreement



Cisco Asset Management Controller 5.0.0 Setup

License Agreement

Please review the license terms before installing Cisco Asset Management Controller 5.0.0.

Press Page Down to see the rest of the agreement.

END USER LICENSE AGREEMENT
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER, YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE.

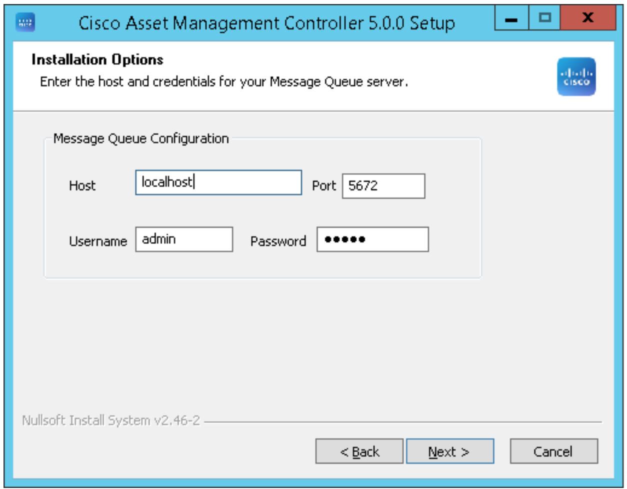
If you accept the terms of the agreement, select the first option below. You must accept the agreement to install Cisco Asset Management Controller 5.0.0. Click Next to continue.

● I accept the terms of the License Agreement
○ I do not accept the terms of the License Agreement

Nullsoft Install System v2.46-2

Step 3 Enter the credentials for the message queue server, as shown in Figure 2-20.

Figure 2-20 Controller Message Queue Credentials



Cisco Asset Management Controller 5.0.0 Setup

Installation Options

Enter the host and credentials for your Message Queue server.

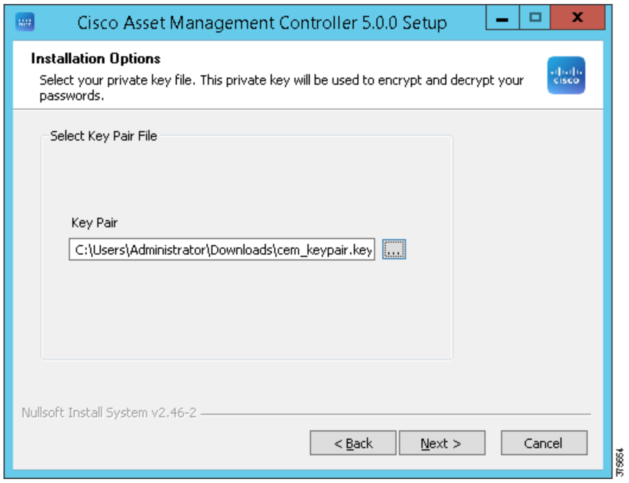
Message Queue Configuration

Host: localhost
Port: 5672
Username: admin
Password: •••••

Nullsoft Install System v2.46-2

Step 4 Select the key file that was downloaded during the server installation process, as shown in Figure 2-21.

Figure 2-21 Key Pair File



Cisco Asset Management Controller 5.0.0 Setup

Installation Options

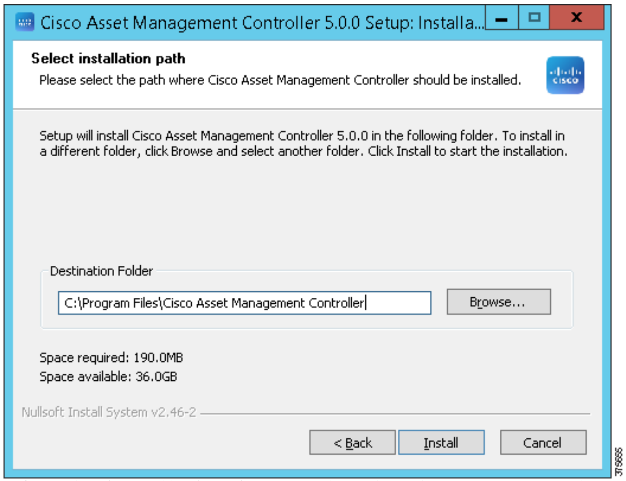
Select your private key file. This private key will be used to encrypt and decrypt your passwords.

Select Key Pair File

Key Pair: C:\Users\Administrator\Downloads\cem_keypair.key

Step 5 Select the destination path where the controller needs to be installed, as shown in Figure 2-22.

Figure 2-22 Controller Destination Path



Cisco Asset Management Controller 5.0.0 Setup: Installa...

Select installation path

Please select the path where Cisco Asset Management Controller should be installed.

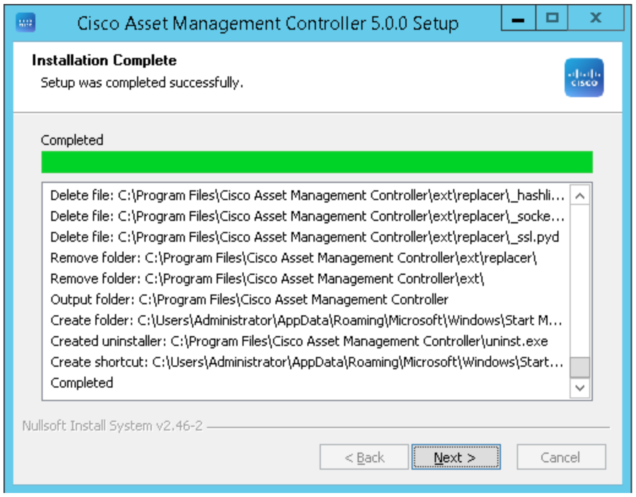
Setup will install Cisco Asset Management Controller 5.0.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\Cisco Asset Management Controller

Space required: 190.0MB
Space available: 36.0GB

Step 6 After the installation is completed, select **Next**, as shown in Figure 2-23.

Figure 2-23 Controller Installation Complete



Cisco Asset Management Controller 5.0.0 Setup

Installation Complete

Setup was completed successfully.

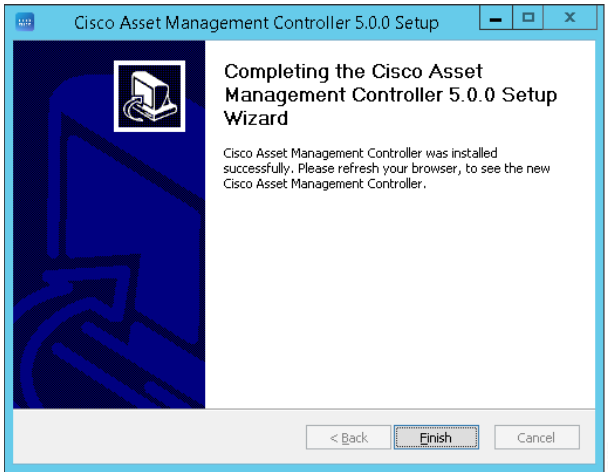
Completed

```
Delete file: C:\Program Files\Cisco Asset Management Controller\ext\replacer\_hashli...
Delete file: C:\Program Files\Cisco Asset Management Controller\ext\replacer\_socke...
Delete file: C:\Program Files\Cisco Asset Management Controller\ext\replacer\_ssl.pyd
Remove folder: C:\Program Files\Cisco Asset Management Controller\ext\replacer\
Remove folder: C:\Program Files\Cisco Asset Management Controller\ext\
Output folder: C:\Program Files\Cisco Asset Management Controller
Create folder: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start M...
Created uninstaller: C:\Program Files\Cisco Asset Management Controller\uninst.exe
Create shortcut: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start...
Completed
```

Nullsoft Install System v2.46-2

Step 7 Finish the installation by selecting Finish, as shown in Figure 2-24.

Figure 2-24 Finish Controller Installation



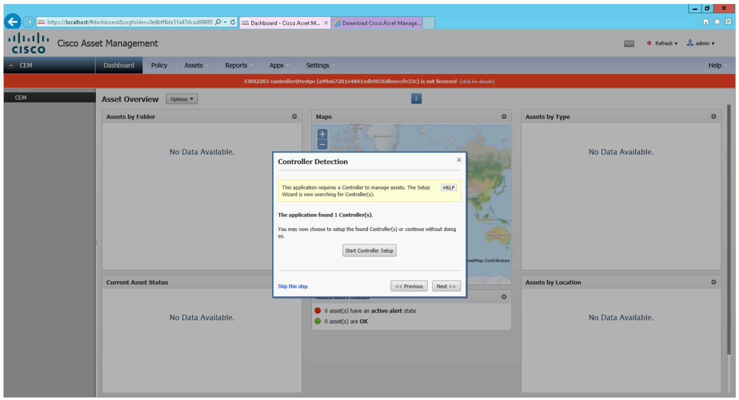
Cisco Asset Management Controller 5.0.0 Setup

Completing the Cisco Asset Management Controller 5.0.0 Setup Wizard

Cisco Asset Management Controller was installed successfully. Please refresh your browser, to see the new Cisco Asset Management Controller.

Step 8 The CAM application automatically detects the CAM controller; select the **Start Controller Setup** option, as shown in Figure 2-25.

Figure 2-25 Start Controller Setup



EW02203 controller@testpc (a99a67201e4841edb9036dbeeccfe33c) is not licensed (click for details)

Controller Detection

This application requires a Controller to manage assets. The Setup Wizard is now searching for Controller(s). HELP

The application found 1 Controller(s).

You may now choose to setup the found Controller(s) or continue without doing so.

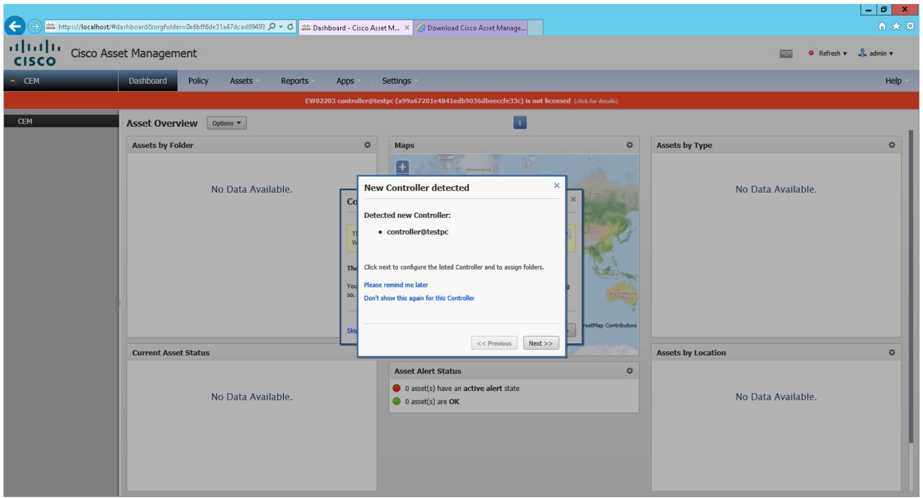
Start Controller Setup

Skip this step   << Previous   Next >>

0 asset(s) have an **active alert** state
0 asset(s) are **OK**

Step 9 Select **Next** after the name of the correct controller appears, as shown in Figure 2-26.

Figure 2-26 New Controller Detected



EW02203 controller@testpc (a99a67201e4841edb9036dbeeccfe33c) is not licensed (click for details)

New Controller detected

Detected new Controller:

- controller@testpc

Click next to configure the listed Controller and to assign folders.

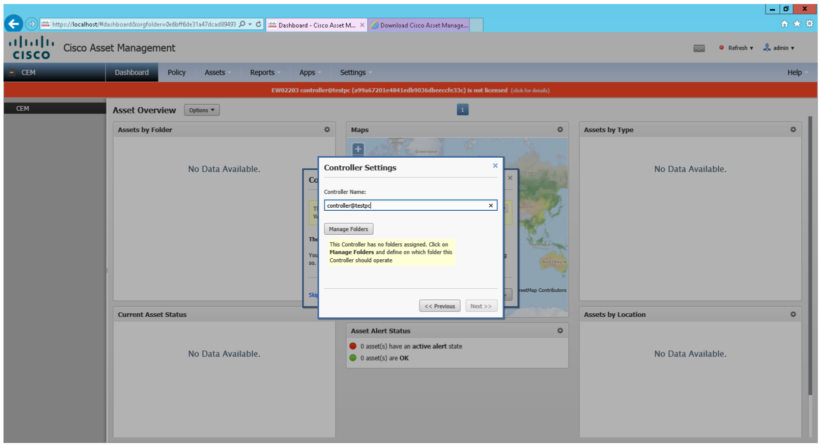
Please remind me later
Don't show this again for this Controller

<< Previous   Next >>

0 asset(s) have an **active alert** state
0 asset(s) are **OK**

Step 10 Select the **Manage Folders** option, as shown in Figure 2-27.

Figure 2-27 Manage Controller Folder Settings



EW02203 controller@testpc (a99a67201e4841edb9036dbeeccfe33c) is not licensed (click for details)

Controller Settings

Controller Name: controller@testpc

Manage Folders

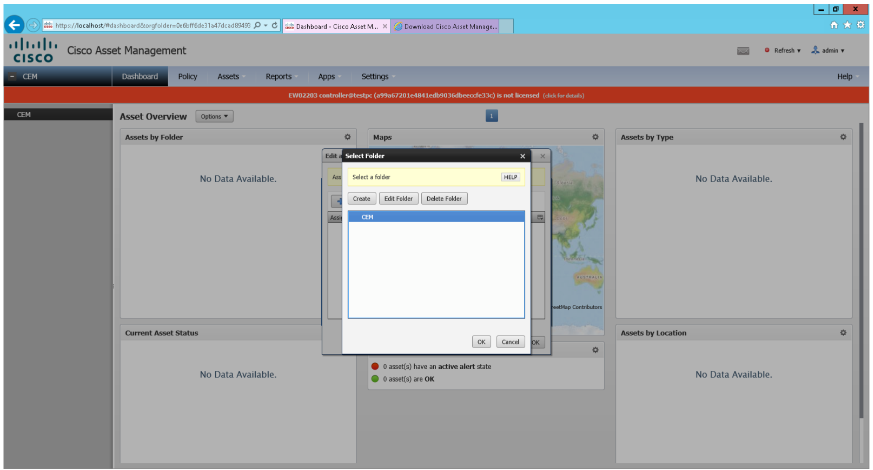
This Controller has no folders assigned. Click on **Manage Folders** and define on which folder this Controller should operate

<< Previous   Next >>

0 asset(s) have an **active alert** state
0 asset(s) are **OK**

Step 11 Select the appropriate folder, as shown in Figure 2-28, and select **OK** twice.

Figure 2-28 Select Folder



EW02203 controller@testpc (a99a67201e4841edb9036dbeeccfe33c) is not licensed (click for details)

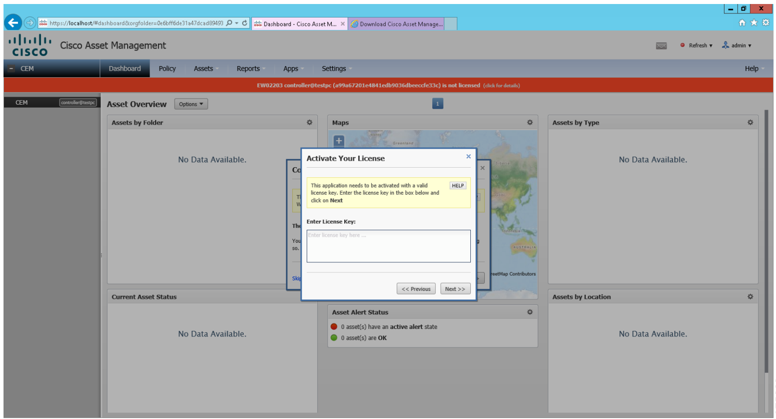
Select Folder

Select a folder

CEM

Step 12 Enter the license key to activate the controller, as shown in Figure 2-29. (When the order is booked on CCW, the license key is provided to the customer.)

Figure 2-29 Controller License Key



EW02203 controller@testpc (a99a67201e4841edb9036dbeeccfe33c) is not licensed (click for details)

Activate Your License

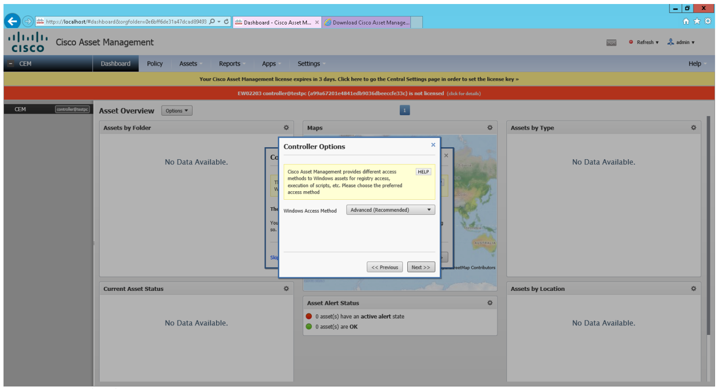
This application needs to be activated with a valid license key. Enter the license key in the box below and click on **Next**

Enter License Key:

Enter license key here ...

Step 13 Select the **Advanced (recommended)** option out of the three options available for the Window Access Method, as shown in Figure 2-30.

Figure 2-30 Controller Options



Your Cisco Asset Management license expires in 3 days. Click here to go the Central Settings page in order to set the license key »

EW02203 controller@testpc (a99a67201e4841edb9036dbeeccfe33c) is not licensed (click for details)

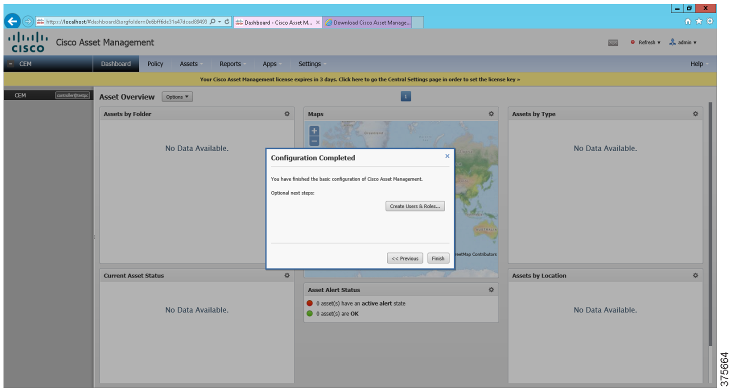
Controller Options

Cisco Asset Management provides different access methods to Windows assets for registry access, execution of scripts, etc. Please choose the preferred access method

Windows Access Method: Advanced (Recommended)

Step 14 Select **Finish** to end the configuration process, as shown in Figure 2-31.

Figure 2-31 Controller Configuration Completed



Your Cisco Asset Management license expires in 3 days. Click here to go the Central Settings page in order to set the license key »

Configuration Completed

You have finished the basic configuration of Cisco Asset Management.

Optional next steps:

0 asset(s) have an **active alert** state

0 asset(s) are **OK**

ACP Installation

Installation of ACP is directly done by the Cisco partner. The customer has to give the required Cloud credentials.

Integration of CAM with ACP

CAM is integrated with ACP to collect sensor details and corresponding values by using asset connectors. Every organization on CAM needs to have four asset connectors.

- REST API-based asset connector (one)
- MQTT-based asset connector (three)

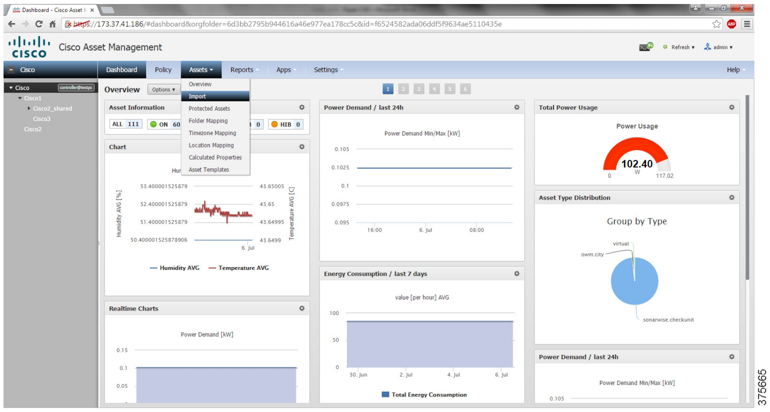
The configuration steps are captured as below:

REST API-Based Asset Connector (One)

Each organization has one REST API-based asset connector to collect a list of sensors that belongs to each organization and its latest value. It is executed on every 15 minutes.

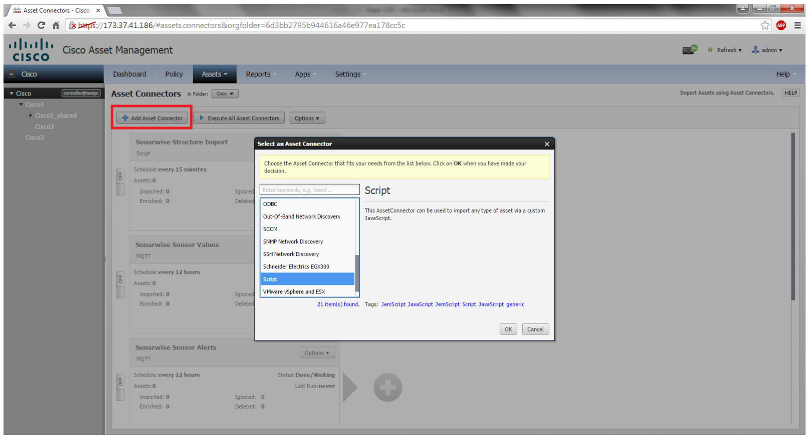
Step 1 Select the **Import** option from **Assets** in Cisco Asset Management, as shown in Figure 2-32.

Figure 2-32 Importing Process



Step 2 Select **Add Asset Connector** to decide the type of asset connector, as shown in Figure 2-33.

Figure 2-33 Selection of Script Asset Connector



Select an Asset Connector

Choose the Asset Connector that fits your needs from the list below. Click on **OK** when you have made your decision.

Enter keywords, e.g. 'cisco'...

- ODBC
- Out-Of-Band Network Discovery
- SCCM
- SNMP Network Discovery
- SSH Network Discovery
- Schneider Electrics EGX300
- Script
- VMware vSphere and ESX

21 item(s) found.

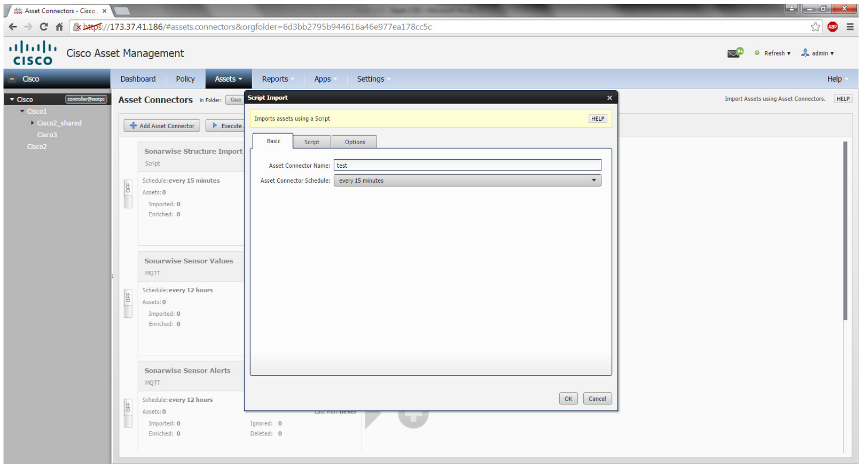
Script

This AssetConnector can be used to import any type of asset via a custom JavaScript.

Tags: JemScript JavaScript JemScript Script JavaScript generic

Step 3 Give the asset connector a name and corresponding schedule, as shown in Figure 2-34.

Figure 2-34 Script Name and Schedule



Script Import

Imports assets using a Script

Asset Connector Name: test

Asset Connector Schedule: every 15 minutes

Step 4 In the **Script** tab, the script can be edited. The customer has to copy and paste the script below. The customer needs to change value corresponding to **uname**, **host**, and **pword**. This detail is provided by the Cisco partner.

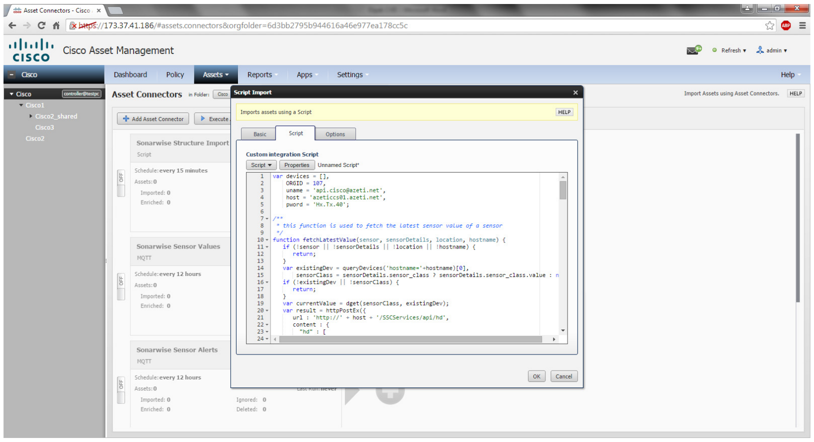
The full script is as shown below:

```
var devices = [],
    ORGID = 107,
    uname = 'api.cisco@azeti.net',
    host = '10.81.1.12',
    pword = 'Hx.Tx.40';


/**
 * this function is used to fetch the latest sensor value of a sensor
 */
function fetchLatestValue(sensor, sensorDetails, location, hostname) {
   if (!sensor || !sensorDetails || !location || !hostname) {
      return;
   }
   var existingDev = queryDevices('hostname='+hostname)[0],
       sensorClass = sensorDetails.sensor_class ? sensorDetails.sensor_class.value : null;
   if (!existingDev || !sensorClass) {
      return;
   }
   var currentValue = dget(sensorClass, existingDev);
   var result = httpPostEx({
      url : 'http://' + host + '/SSCServices/api/hd',
      content : {
        "hd" : [
          {
          "location" : location.guid,
          "sensor": sensor.id
          }
        ]
      },
      username : uname,
      password : pword,
      timeout : 10
   });
   if (result.StatusCode !== 200) {
      return;
   }
   var states = JSON.parse(result.Response);
   if (!states.length) {
      return;
   }
   // just use the first entry
   for (var i = 0; i < states.length; i++) {
      var entry = states[i];
      if (entry.name.indexOf('Value') !== -1) {
         if (!entry.points.length) {
            return;
         }
         // look up column index of value
         for (var h = 0; h < entry.columns.length; h++) {
            if (entry.columns[h] === 'value') {
               break;
            }
         }
         return entry.points[0][h];
      }
   }
}

/**
 * IMPORT BEGINS HERE
 */


// get all locations in the organization
var json = httpPost({
   url : 'http://' + host + '/SSCServices/api/config',
   content : { organization: ORGID },
   username : uname,
   password : pword,
   timeout : 60
});


var locations = JSON.parse(json)[0],
    locationMap = {};

// preparing data for the next request and in addition creating a map location guid ->
location
```

```
var locationPayload = locations.map(function(l) {
   locationMap[l.guid] = l;
   return { location: l.guid };
});

// get all sensors in each location
json = httpPost({
   url : 'http://' + host + '/SSCServices/api/config',
   content : locationPayload,
   contentType : 'application/json',
   username : uname,
   password : pword,
   timeout : 60
});

var sensorsPerLocation = JSON.parse(json),
    allSensorsInOne = [],
    locationToSensorsMap = {};

sensorsPerLocation.forEach(function(sensors) {
   sensors.forEach(function(s) {
      locationToSensorsMap[s.locationId] = locationToSensorsMap[s.locationId] || [];
      locationToSensorsMap[s.locationId].push(s);
   });
   allSensorsInOne = allSensorsInOne.concat(sensors);
});

var sensorPayload = allSensorsInOne.map(function(s) {
   return { sensor: s.id };
});

log(JSON.stringify(sensorPayload), "INFO");

// get all sensor details (details are not available for all sensors, some might be
missing)
var response = httpPost({
   url : 'http://' + host + '/SSCServices/api/config',
   content : sensorPayload,
   contentType : 'application/json',
   username : uname,
   password : pword,
   timeout : 240
});

var allSensorDetails = JSON.parse(response),
    allSensorDetailsMap = {};

allSensorDetails.forEach(function(json) {
   try {
      var details = JSON.parse(json);
      allSensorDetailsMap[details.guid] = details;
   }
   catch (e) {
      log('could not parse sensor details: ' + json + ' (skipping)', 'WARNING');
   }
});


// create the devices from the sensors
allSensorsInOne.forEach(function(sensor) {
   var location = locationMap[sensor.locationId],
       sensorDetails = allSensorDetailsMap[sensor.id] || {};

   var deviceHostname = location.name + '//' + sensor.name,
       latestValue,
       sensorClass;

   if (sensorDetails) {
      sensorClass = sensorDetails.sensor_class ? sensorDetails.sensor_class.value : null;
      latestValue = fetchLatestValue(sensor, sensorDetails, location, deviceHostname);
   }

   var device = {
      'sonarwise.structure' : 'CEM//' + location.name + '//' + sensor.name,
      'hostname' : deviceHostname,
      'mqtt.id' : sensor.id,
      'sonarwise.sensor.id' : sensor.id,
      'sonarwise.sensor.class' : sensorClass,
     'sonarwise.sensor.unit' : sensorDetails.unit ? sensorDetails.unit.value : "",
      'sonarwise.sensor.contenttype' : sensorDetails.binary,
      'sonarwise.location.id' : location.guid,
      'type' : 'sonarwise.checkunit',
      'dns.disabled' : '1',
      'measure.disabled' : '1',
      'scan.disabled': '1',
      'measure.interval': '',
      'scan.interval': ''
   };

   if (latestValue && sensorClass) {
      device[sensorClass] = latestValue;
      device["value"] = latestValue;
   }
   else {
      var dev = queryDevices("sonarwise.sensor.id=" + sensor.id)[0];
      if (dev) {
         if (sensorClass) {
            device[sensorClass] = dget(sensorClass, dev);
         }
         device["value"] = dget("value", dev);
      }
   }

   //log (JSON.stringify(device), "INFO");

   devices.push(device);
});
return devices;
```

Step 5 Execute the created asset connector by first saving the changes by clicking **Save Changes** and then Execute under Options, as shown in Figure 2-35.

Figure 2-35 Execution of the Rest of the API Script



```
var devices = [],
    ORGID = 107,
    uname = 'api.cisco@azeti.net',
    host = 'azeticcs01.azeti.net',
    pword = 'Hx.Tx.40';

/**
 * this function is used to fetch the latest sensor value of a sensor
 */
function fetchLatestValue(sensor, sensorDetails, location, hostname) {
   if (!sensor || !sensorDetails || !location || !hostname) {
      return;
   }
   var existingDev = queryDevices('hostname='+hostname)[0],
      sensorClass = sensorDetails.sensor_class ? sensorDetails.sensor_class.value : n
   if (!existingDev || !sensorClass) {
      return;
   }
   var currentValue = dget(sensorClass, existingDev);
   var result = httpPostEx({
      url : 'http://' + host + '/SSCServices/api/hd',
      content : {
        "hd" : [
```

MQTT-Based Asset Connector

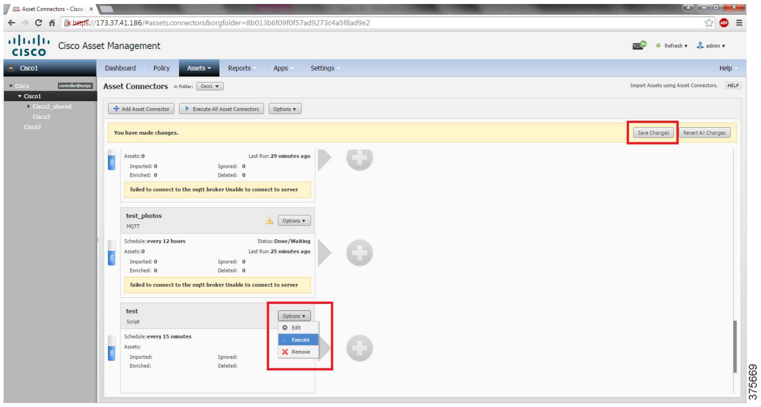
Each organization has the following three MQTT-based asset connectors to collect:

- Events - The events are collected by subscribing to MQTT topic of Cisco/outbound/events.
- Alerts - The alerts are collected by subscribing to MQTT topic of Cisco/outbound/hd.
- Photos - Photos are collected by subscribing to MQTT topic of Cisco/outbound/binary.

MQTT- Event Configuration

Step 1 Select the **MQTT** option in the **Add Asset Connector** and select **OK,** as shown in Figure 2-36.

Figure 2-36 Selection of MQTT Asset Connector



You have made changes.

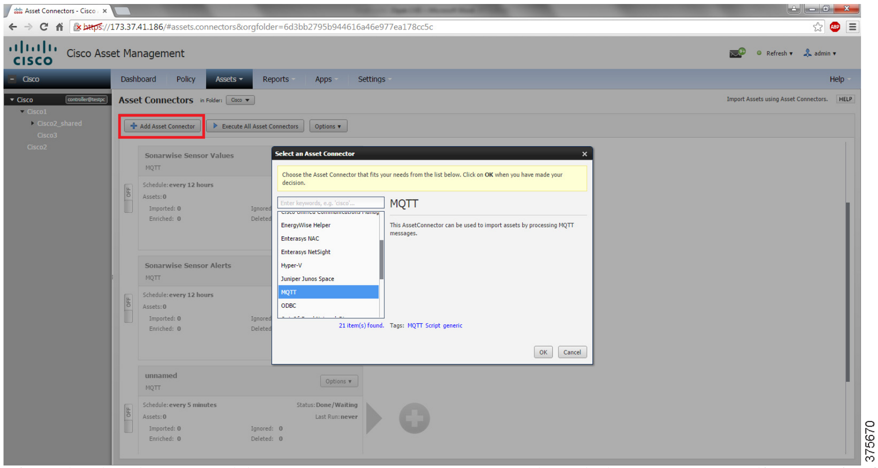
Assets: 0 Last Run: 29 minutes ago
Imported: 0 Ignored: 0
Enriched: 0 Deleted: 0
failed to connect to the mqtt broker Unable to connect to server

test_photos
MQTT
Schedule: every 12 hours Status: Done/Waiting
Assets: 0 Last Run: 25 minutes ago
Imported: 0 Ignored: 0
Enriched: 0 Deleted: 0
failed to connect to the mqtt broker Unable to connect to server

test
Script
Schedule: every 15 minutes

Step 2 Type the required asset connector name for events, as shown in Figure 2-37.

Figure 2-37 Event Name and Schedule



Select an Asset Connector

Choose the Asset Connector that fits your needs from the list below. Click on **OK** when you have made your decision.

Enter keywords, e.g. 'cisco'...

- EnergyWise Helper
- Enterasys NAC
- Enterasys NetSight
- Hyper-V
- Juniper Junos Space
- MQTT
- ODBC

MQTT

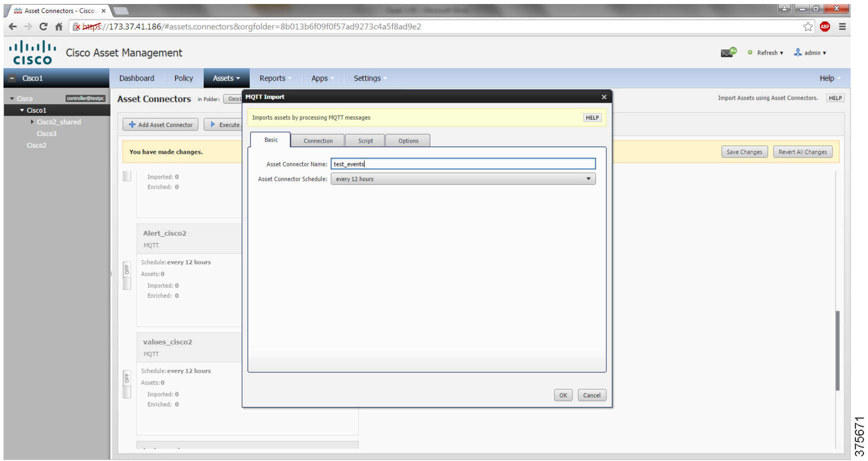
This AssetConnector can be used to import assets by processing MQTT messages.

21 item(s) found. Tags: MQTT Script generic

OK Cancel

Step 3 Give the broker IP address, user name, password and the corresponding topic for MQTT Events. The username and password is provided by the Cisco partner, as shown in Figure 2-38.

Figure 2-38 Event Connection Details



MQTT Import

Imports assets by processing MQTT messages HELP

Basic | Connection | Script | Options

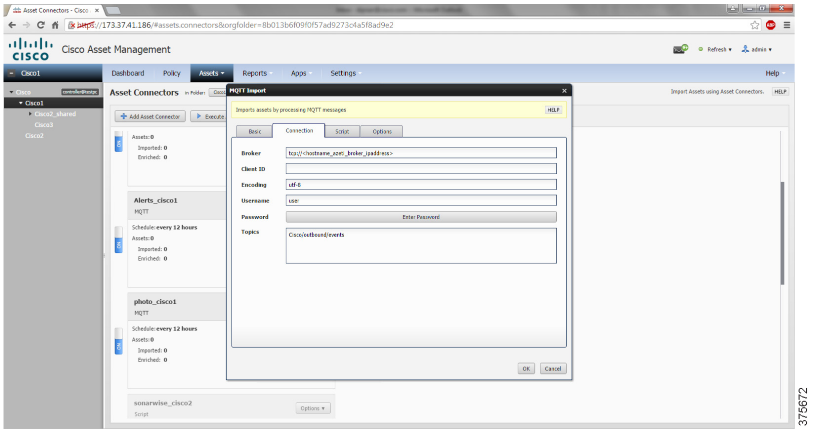
Asset Connector Name: test_events

Asset Connector Schedule: every 12 hours

OK Cancel

Step 4 Select the **Script** tab to put the required script, as shown in Figure 2-39.

Figure 2-39 Event Script



MQTT Import

Imports assets by processing MQTT messages HELP

Basic | Connection | Script | Options

Broker: tcp://<hostname_azeti_broker_ipaddress>

Client ID:

Encoding: utf-8

Username: user

Password: Enter Password

Topics: Cisco/outbound/events

OK Cancel

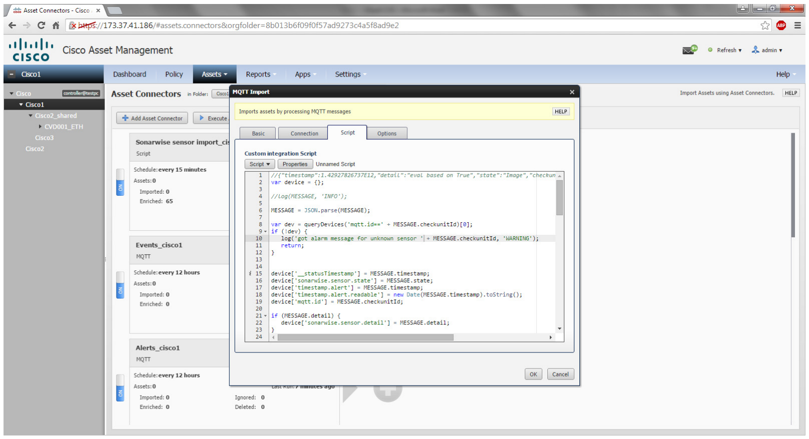
The full script is as shown below:

```
//{"timestamp":1.42927826737E12,"detail":"eval based on
True","state":"Image","checkunitId":"1505954f-dea3-4ff7-8e48-458218998406"}
var device = {};

//log(MESSAGE, 'INFO');

MESSAGE = JSON.parse(MESSAGE);


var dev = queryDevices('mqtt.id==' + MESSAGE.checkunitId)[0];
if (!dev) {
   log('got alarm message for unknown sensor ' + MESSAGE.checkunitId, 'WARNING');
   return;
}


device['__statusTimestamp'] = MESSAGE.timestamp;
device['sonarwise.sensor.state'] = MESSAGE.state;
device['timestamp.alert'] = MESSAGE.timestamp;
device['timestamp.alert.readable'] = new Date(MESSAGE.timestamp).toString();
device['mqtt.id'] = MESSAGE.checkunitId;

if (MESSAGE.detail) {
   device['sonarwise.sensor.detail'] = MESSAGE.detail;
}

// processing level
device['sonarwise.processing_level'] = MESSAGE.processing_level;
if (MESSAGE.processing_level > 0 && MESSAGE.processing_level <= 9) {
   device['issue'] = "sensor is unreachable";
   device['sonarwise.sensor.state'] = "UNREACHABLE";
} else {
   device['issue'] = '';
   if (device['sonarwise.sensor.state'] === "UNREACHABLE") {
      device['sonarwise.sensor.state'] = '';
   }
}

var alertStateToMessageSeverity = {
  "OK" : "info",
  "WARNING" : "warning",
  "CRITICAL" : "error"
};

var alertStateToFlag = {
  "WARNING": "yellow",
  "CRITICAL": "red"
};

device['flag'] = alertStateToFlag[MESSAGE.state] || '';
device["sonarwise.sensor.alert"] = MESSAGE;

var config = dget('sonarwise.service.config', dev) || {
   alerting: {
      createSystemMessage: true
   }
};
var createSystemMessage = MESSAGE.state !== "Image" && config.alerting &&
config.alerting.createSystemMessage !== false;


if (createSystemMessage) {
    var sensorPropertyName = dget('sonarwise.sensor.class', dev),
         sensorValue = sensorPropertyName ? dget(sensorPropertyName, dev) : "n/a",
         sensorValue = sensorValue == null ? "n/a" : sensorValue;

    var messageText = config.alerting ? config.alerting.messageText : '',
       messageTitle = config.alerting ? config.alerting.messageTitle : '';


    if (!messageText) {
      messageText = 'State of sensor is: ' + MESSAGE.state + '.\n' +
                     'Current sensor value is: ' + sensorValue + '.\n' +
                     'Alert message is: ' + MESSAGE.detail + '.';
    }

    if (!messageTitle) {
        messageTitle = dget('hostname', dev) || "";
    }

    var folder = dget('orgfolder', dev) || null;

    var systemMessage = {
        objecttype: 'message',
        orgfolder: folder,
        senderId: dget("id", dev),
        label: messageTitle,
        severity: alertStateToMessageSeverity[MESSAGE.state] || "information",
        text: messageText,
        createdMillisUtc: MESSAGE.timestamp,
        categories: [ 'alert' ]
    };

    createObject(systemMessage);
}

return device;
```

MQTT Alert Configuration

Step 1 Type the required asset connector name for alerts, as shown in Figure 2-40.

Figure 2-40 Alert Name and Schedule



Asset Connectors - Cisco
https://173.37.41.186/#assets.connectors&orgfolder=8b013b6f09f0f57ad9273c4a5f8ad9e2

Cisco Asset Management

Asset Connectors in Folder: Cisco1

Sonarwise sensor import_cis
Script
Schedule: every 15 minutes
Assets: 0
Imported: 0
Enriched: 65

Events_cisco1
MQTT
Schedule: every 12 hours
Assets: 0
Imported: 0
Enriched: 0

Alerts_cisco1
MQTT
Schedule: every 12 hours
Assets: 0
Imported: 0
Enriched: 0
Ignored: 0
Deleted: 0

MQTT Import

Imports assets by processing MQTT messages

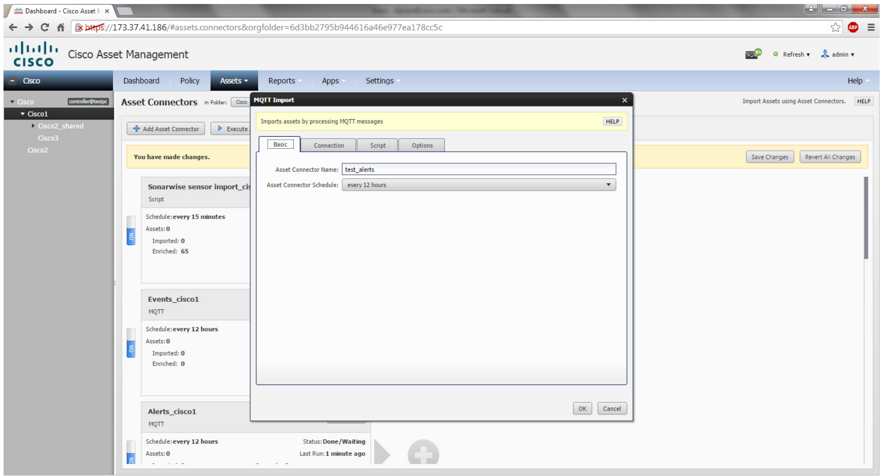
Custom integration Script

Unnamed Script

```
//{"timestamp":1.42927826737E12,"detail":"eval based on True","state":"Image","checkun
var device = {};

//log(MESSAGE, 'INFO');

MESSAGE = JSON.parse(MESSAGE);

var dev = queryDevices('mqtt.id==' + MESSAGE.checkunitId)[0];
if (!dev) {
   log('got alarm message for unknown sensor ' + MESSAGE.checkunitId, 'WARNING');
   return;
}


device['__statusTimestamp'] = MESSAGE.timestamp;
device['sonarwise.sensor.state'] = MESSAGE.state;
device['timestamp.alert'] = MESSAGE.timestamp;
device['timestamp.alert.readable'] = new Date(MESSAGE.timestamp).toString();
device['mqtt.id'] = MESSAGE.checkunitId;

if (MESSAGE.detail) {
   device['sonarwise.sensor.detail'] = MESSAGE.detail;
}
```

Step 2 Give the broker IP address, user name, password and the corresponding topic for MQTT Events. The username and password is provided by Cisco partner, as shown in Figure 2-41.

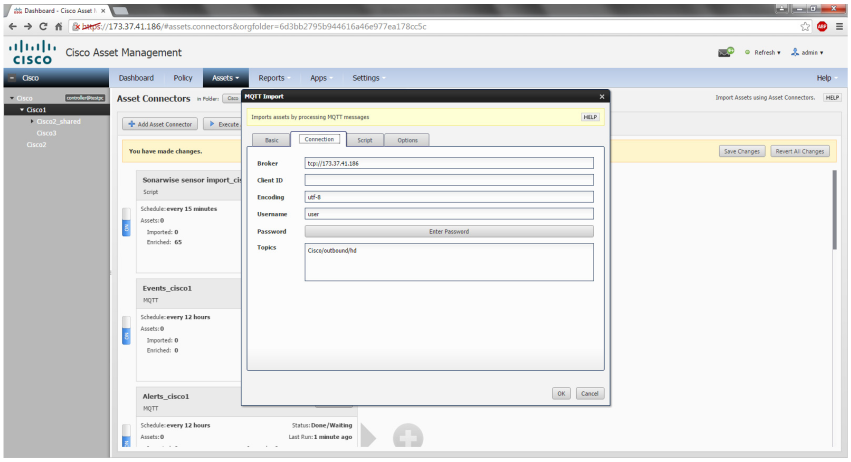
Figure 2-41 Alert Connection Details



Asset Connector Name: test_alerts
Asset Connector Schedule: every 12 hours

Step 3 Select the **Script** tab to put the required script, as shown in Figure 2-42.

Figure 2-42 Alert Script



Broker: tcp://173.37.41.186
Client ID:
Encoding: utf-8
Username: user
Password: Enter Password
Topics: Cisco/outbound/hd

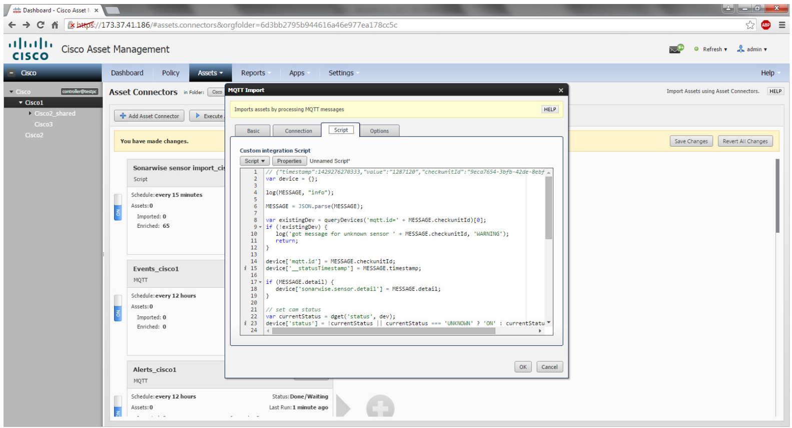
The full script is as shown below:

```
//
{"timestamp":1429276270333,"value":"1287120","checkunitId":"9eca7654-3bfb-42de-8ebf-696aa7
a16915"}
var device = {};

log(MESSAGE, "info");


MESSAGE = JSON.parse(MESSAGE);

var existingDev = queryDevices('mqtt.id=' + MESSAGE.checkunitId)[0];
if (!existingDev) {
   log('got message for unknown sensor ' + MESSAGE.checkunitId, 'WARNING');
   return;
}

device['mqtt.id'] = MESSAGE.checkunitId;
device['__statusTimestamp'] = MESSAGE.timestamp;

if (MESSAGE.detail) {
   device['sonarwise.sensor.detail'] = MESSAGE.detail;
}

// set cam status
var currentStatus = dget('status', dev);
device['status'] = !currentStatus || currentStatus === 'UNKNOWN' ? 'ON' : currentStatus;

// processing level
device['sonarwise.processing_level'] = MESSAGE.processing_level;
if (MESSAGE.processing_level > 0 && MESSAGE.processing_level <= 9) {
   device['issue'] = "sensor is unreachable";
   device['sonarwise.sensor.state'] = "UNREACHABLE";
} else {
   device['issue'] = '';
   if (device['sonarwise.sensor.state'] === "UNREACHABLE") {
      device['sonarwise.sensor.state'] = '';
   }
}

var value = MESSAGE.value;
if (!isNaN(value)) {
   value = Math.round(parseFloat(value) * 100) / 100;
}

device['value'] = value;
device['timestamp.measure'] = MESSAGE.timestamp;
device['timestamp.measure.readable'] = new Date(MESSAGE.timestamp).toString();

// check for the real sensor class and update it
var clazz = dget('sonarwise.sensor.class', existingDev);
if (clazz) {
   device[clazz] = value != null ? value : '';
}
return device;
```

MQTT Photos Configuration

Step 1 Type the required asset connector name for photos, as shown in Figure 2-43.

Figure 2-43 Photo Name and Schedule



You have made changes.

Imports assets by processing MQTT messages

Custom integration Script

Unnamed Script*

```
// {"timestamp":1429276270333,"value":"1287120","checkunitId":"9eca7654-3bfb-42de-8ebf
var device = {};

log(MESSAGE, "info");

MESSAGE = JSON.parse(MESSAGE);

var existingDev = queryDevices('mqtt.id=' + MESSAGE.checkunitId)[0];
if (!existingDev) {
   log('got message for unknown sensor ' + MESSAGE.checkunitId, 'WARNING');
   return;
}

device['mqtt.id'] = MESSAGE.checkunitId;
device['__statusTimestamp'] = MESSAGE.timestamp;

if (MESSAGE.detail) {
   device['sonarwise.sensor.detail'] = MESSAGE.detail;
}

// set cam status
var currentStatus = dget('status', dev);
device['status'] = !currentStatus || currentStatus === 'UNKNOWN' ? 'ON' : currentStatu
```

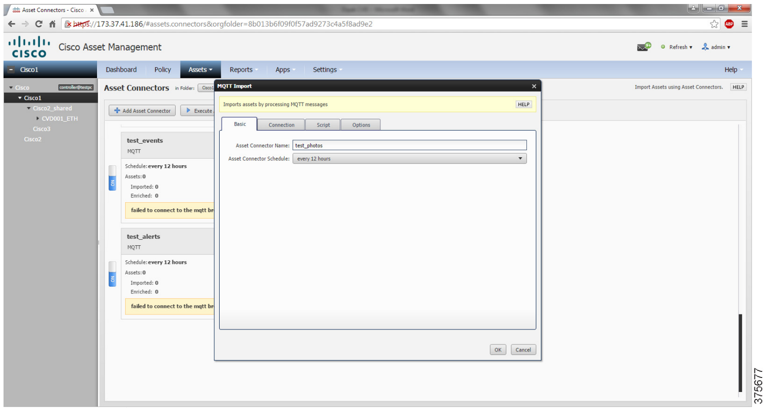
Sonarwise sensor import_ci
Script
Schedule: every 15 minutes
Assets: 0
Imported: 0
Enriched: 65

Events_cisco1
MQTT
Schedule: every 12 hours
Assets: 0
Imported: 0
Enriched: 0

Alerts_cisco1
MQTT
Schedule: every 12 hours
Assets: 0
Status: Done/Waiting
Last Run: 1 minute ago

Step 2 Give the broker IP address, user name, password and the corresponding topic for MQTT Events, as shown in Figure 2-44. The username and password are provided by Cisco partner.

Figure 2-44 Photo Connection Details



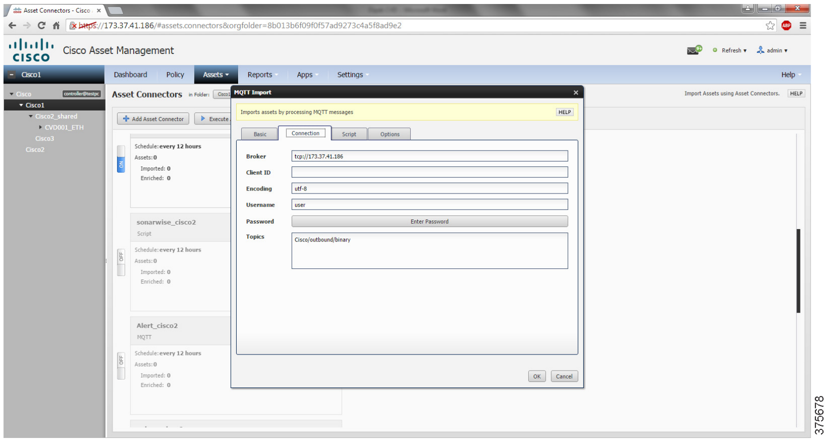
Imports assets by processing MQTT messages

Asset Connector Name: test_photos

Asset Connector Schedule: every 12 hours

Step 3 Select the **Script** tab to put the required script, as shown in Figure 2-45.

Figure 2-45 Photo Script



Imports assets by processing MQTT messages

Broker tcp://173.37.41.186

Client ID

Encoding utf-8

Username user

Password

Topics Cisco/outbound/binary

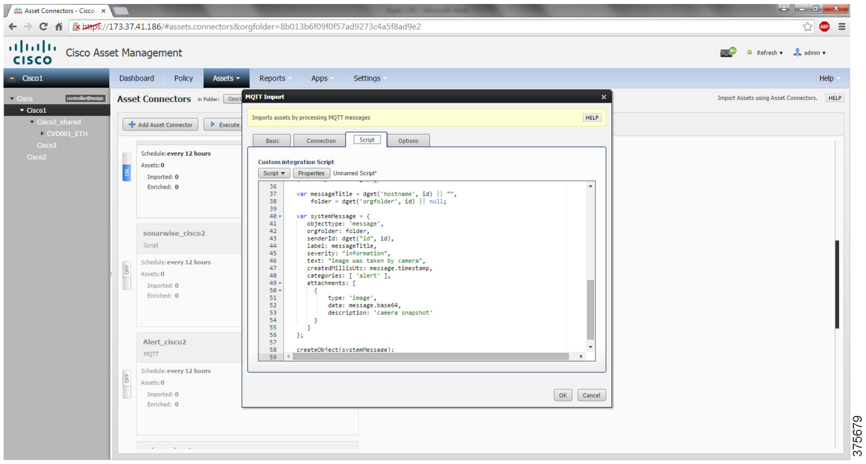
The full script is as shown below:

```
/*
{
    "action_id": "Snap_123_virtual",
    "sensor": "f705ce27-c95a-4c70-908e-669e65da4c5e",
    "timestamp": 1428987655000,
    "exec_uid": "8512db19-3f7d-4226-8e8f-38961c661a30",
    "base64": "/9j/4AAQSkZJRgABAQEASABIAAD/4QCMRXhp etc etc etc etc",
    "location": "7eb14020-73a8-411f-87e5-4b2ccdf115d7",
    "device_id": "cisco_cam_virtual_123",
    "sensor_id": "timed_result"
}
*/

//log(MESSAGE,"INFO");

// the MESSAGE variable contains the raw MQTT message
var message = JSON.parse(MESSAGE);

var id = queryDevices("sonarwise.sensor.id=" + message.sensor)[0];
if (!id) {
   log("got image data for unknown device:" + MESSAGE, "INFO");
   return;
}
```

```
// save image
sysset("image_" + id, message.base64);

// process message if configured
var config = dget('sonarwise.service.config', id) || {
   alerting: {
      createSystemMessage: true
   }
};

var createSystemMessage = config.alerting && config.alerting.createSystemMessage !==
false;

if (createSystemMessage) {

    var messageTitle = dget('hostname', id) || "",
        folder = dget('orgfolder', id) || null;

    var systemMessage = {
        objecttype: 'message',
        orgfolder: folder,
        senderId: dget("id", id),
        label: messageTitle,
        severity: "information",
        text: "image was taken by camera",
        createdMillisUtc: message.timestamp,
        categories: [ 'alert' ],
        attachments: [
        {
            type: 'image/script',
            data: "httpPost({" +
                  "url: 'http://10.81.1.12/SSCServices/api/binary'," +
                  "username: getenv('azeti_rest_username')," +
                  "password: getenv('azeti_rest_password')," +
                  "timeout: 10," +
                  "responseEncoding: 'base64'," +
                  "contentType: 'application/json'," +
                 "content: JSON.stringify({ location: '" + message.location  +"', sensor:
'"+message.sensor+"', timestamp: " +message.timestamp+" })" +
               "})",
            description: 'camera snapshot'
        }
       ]
    };

    createObject(systemMessage);
}
```

Step 4 To deploy any of the events, alerts or photos, select **Execute** from **Options** for the corresponding asset connectors after saving the changes, as shown in Figure 2-46.

Figure 2-46 Execution of MQTT Asset Connectors



```
var messageTitle = dget('hostname', id) || "",
    folder = dget('orgfolder', id) || null;

var systemMessage = {
   objecttype: 'message',
   orgfolder: folder,
   senderId: dget("id", id),
   label: messageTitle,
   severity: "information",
   text: "image was taken by camera",
   createdMillisUtc: message.timestamp,
   categories: [ 'alert' ],
   attachments: [
     {
        type: 'image',
        data: message.base64,
        description: 'camera snapshot'
     }
   ]
};

createObject(systemMessage);
```

Network Setup

This section provides configuration details for the VPN server configured in the Cloud. CSR1Kv is used as the VPN server. The solution has two deployment options based on connectivity, as shown in Table 2-1 and Table 2-2.

Table 2-1 Deployment Option - 1: Sensors Only with 3G as WAN Backup

Device	Role
IR910	Sensor gateway
IR910	Transport router

Table 2-2 Deployment Model - 2: Sensors plus Camera with 4G as WAN Backup

Device	Role
IR910	Sensor gateway
CISCO899G	Transport router

VPN Server Configuration

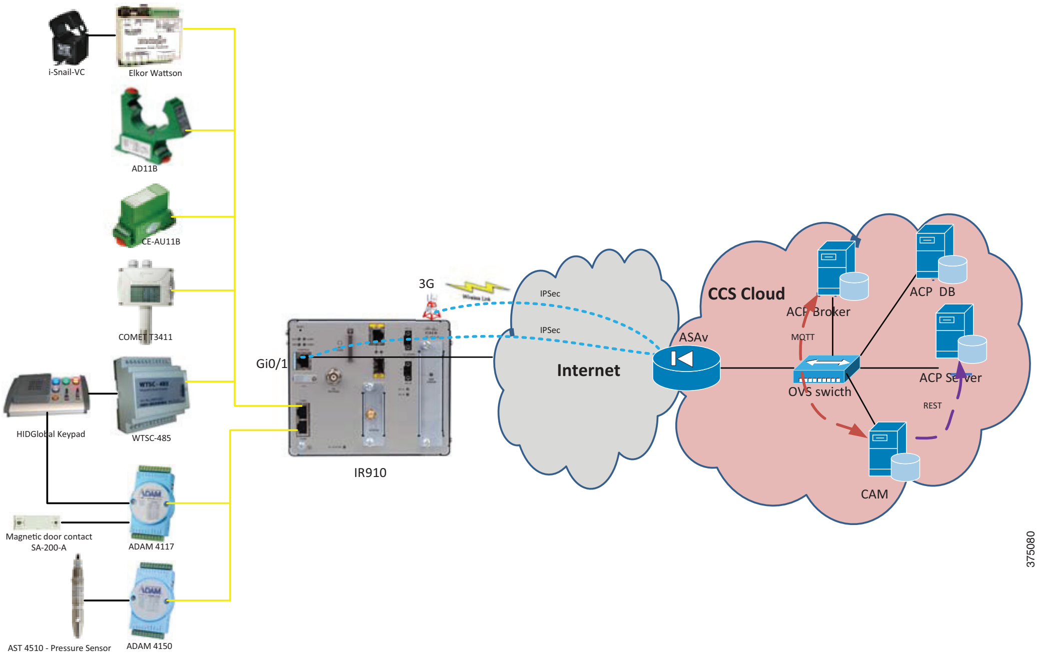
This section provides configuration details VPN server configuration on CSR1IK for Deployment option -1 and Deployment option-2.

Deployment Option -1: Sensors Only with 3G as WAN Backup

The sensor gateway is connected to all Modbus sensors by using COM1 and COM2. The site controller application is running on IR910 and fetches all required sensor parameters. It supports two WAN connections: Gigabit Ethernet and Cellular. An IPSEC tunnel is created from the sensor gateway to CSR1Kv to send MQTT messages. The WAN connection Gigabit Ethernet is used as primary and cellular is used as secondary. Once an IPSEC tunnel is established, CSR1Kv assigns an IP address to the sensor gateway dynamically. The sensor gateway is sending all information to the Azeti control panel by using an assigned IP address. The required configuration is categorized as a cell site configuration and a Cloud-side configuration. The cell site configuration section covers network configuration details of the sensor gateway (IR910). The Cloud-side configuration covers details of CSR1Kv.

Figure 2-47 shown the deployment 1 - sensor only system setup.

Figure 2-47 Deployment 1- Sensor Only System Setup



Cloud-Side Configuration - CSR1Kv

The Cloud-side configuration for CSR1Kv is shown below:

```
!*** aaa configuration ***
aaa new-model
!
!
!*** Create aaa network authorization with a name  ***

aaa authorization network ikev1 local
!
aaa session-id common

!
!*** Create Keyring with address any and a key name  ***

crypto keyring key1
  pre-shared-key address 0.0.0.0 0.0.0.0 key <1234567>
!
!
!*** Create IKEV1 policy  ***


crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!

!
```

```
!*** Create isakamp client group with a name ***

crypto isakmp client configuration group <ikev1>
!*** Set Key and ip pool for client ***
 key <1234567>
 domain cisco.com
 pool pool1

!

!*** Create isakamp Profile with a name ***
crypto isakmp profile <p1>
   keyring key1
   match identity address 0.0.0.0
!*** Map aaa authorization, Client group and addesss respond pool ***
   isakmp authorization list <ikev1>
   client configuration address respond
   client configuration group <ikev1>
!
!*** create Tranform-set for IPSEC ***

crypto ipsec transform-set TS2 esp-aes esp-sha-hmac
 mode tunnel
!
!
!*** create Dynamic MAP ***

crypto dynamic-map <DMAP> 1
 set transform-set <TS2>
 set isakmp-profile <p1>
 reverse-route
!
!
!*** Map dynamic map to static MAP
crypto map CMAP 1 ipsec-isakmp dynamic DMAP

!*** create ip pool to assign ip address on IR910 ***

ip local pool pool1 10.100.100.1 10.100.100.254

!*** DMZ Interface configuration Connect to ACP Broker ***!
 interface GigabitEthernet1
 description Connected_Cloud_server
 ip address 10.81.1.14 255.255.255.0
!


!*** Outside Interface configuration Connect to Internet cloud ***
interface GigabitEthernet2
 ip address 173.39.224.174 255.255.255.0
 negotiation auto
!*** Apply crypto map to interface ***
 crypto map CMAP
!


!


!***  add Ipsec ikev1 on outside interface ***

crypto ikev1 enable outside

!***  create ikev1 policy ***
```

```
!*** Routing to reach INTERNET CLOUD ***
ip route 0.0.0.0 0.0.0.0 173.39.224.1
```

Table 2-3 shows layer 2 and IP addressing for deployment 1.

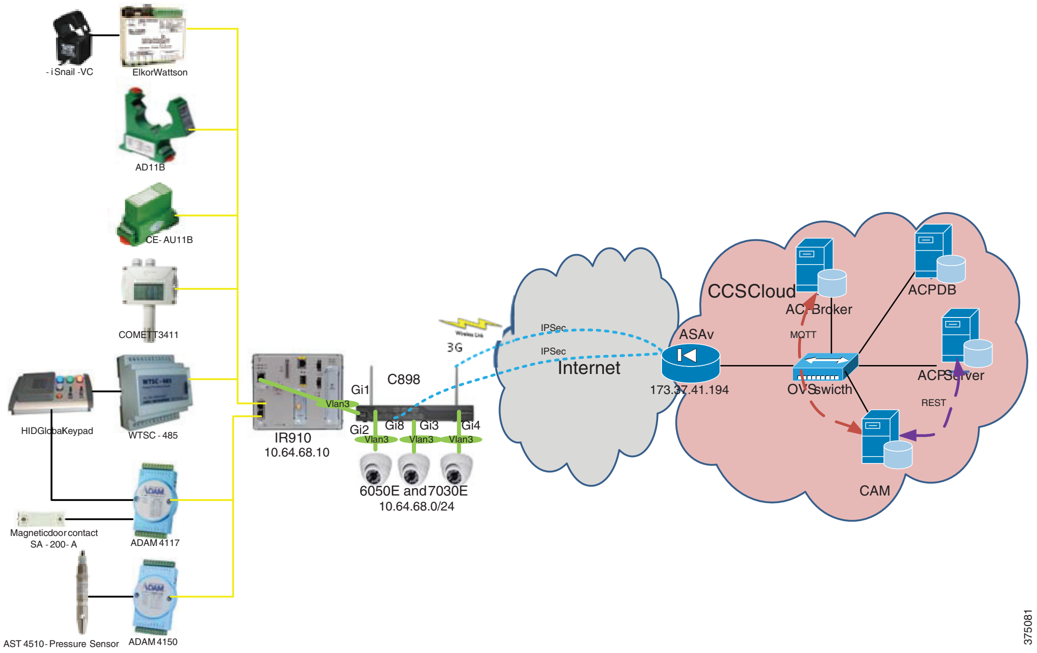
Table 2-3 Layer 2 and IP Addressing (VLANs) - Deployment I Sensor Only

Network/Mask	Purpose	VLAN/Port
10.105.248.175/24	IR910	Gi 0/1
10.81.1.14	CSR1Kv - Cloud Server	Gi1
173.39.224.174	CSR1Kv -Internet Cloud	Gi2
10.81.1.10, 10.81.1.11, 10.81.1.12	Azeti control Panel	Gi0
10.81.1.5	CAM	Gi0

Deployment Model -2: Sensors plus Camera with 4G as WAN Backup

Figure 2-48 shows deployment model 2.

Figure 2-48 Deployment - 2 Sensor plus IP Camera



Cloud Side Configuration - CSR1Kv

The Cloud-side configuration for CSR1Kv is shown below:

```
!*** aaa configuration ***
aaa new-model
!
!
aaa authorization network local-group local
!
```

```
!*** create ikev2 authorization policy and is used in psk under crypto profile ***

crypto ikev2 authorization policy <local-pol>
 route set access-list 10
!

!*** create ikev2 proposal ***
crypto ikev2 proposal <p1>
 encryption 3des
 integrity md5
 group 2
!

!*** create ikev2 policy and match proposal ***
crypto ikev2 policy <p1>
 proposal <p1>
!


!*** create ikev2 Keyring and macth identity of peer address. if peer address changes, use
fqdn ***
crypto ikev2 keyring <key>
 peer peer
  address 0.0.0.0 0.0.0.0
  pre-shared-key local <cisco>
  pre-shared-key remote <cisco>
 !
!
!
!*** create ikev2 profile and match aaa authorization list and keyring ***
crypto ikev2 profile <prof1>
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local <key>
 aaa authorization group psk list local-group local-pol
 virtual-template 1
!
!
!
!
!
!*** Create IPSEC transform-set ***

crypto ipsec transform-set <trans> esp-3des esp-md5-hmac
 mode tunnel

!

!*** Create IPSEC profile and match tranform-set and ikev2 profile ***

crypto ipsec profile <prof>
 set transform-set <trans>
 set ikev2-profile <prof1>


!*** Interface configuration ***
!
!*** Interface connected to cloud server ***
interface GigabitEthernet1
 ip address 10.81.1.14 255.255.255.0
 negotiation auto
```

```
!*** Interface connected to Internet_cloud ***
 !
interface GigabitEthernet2
 ip address 173.39.224.174 255.255.255.0

!*** create virtual template and map ipsec profile
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile <prof>
!
!*** Routing configuration ***
ip route 0.0.0.0 0.0.0.0 173.39.224.1
!*** acccess-list used for sending network to spoke ***
access-list 10 permit 10.81.1.0 0.0.0.255
```

Table 2-4 shows layer 2 and IP addressing for VLANs.

Table 2-4 Layer 2 and IP Addressing (VLANs) - Deployment 2 - Sensor Only

Network/Mask	Purpose	VLAN/Port
10.64.68.10/24	IR910	Vlan 3
10.105.248.180	Cisco 898 GA	Gi8
10.81.1.14	CSR1Kv - Cloud server	Gi1
173.39.224.174	CSR1Kv - Internet Cloud	Gi2
10.81.1.10,10.81.1.11,10.81.1.12	Azeti Control Panel	Gi0
10.81.1.5	CAM	Gi0

Remote Site installation

This section covers installation of the network setup, Site controller, and the IP camera, as well as, setting up the sensor network, for the remote site.

Network Setup

This section provides configuration details for Deployment option -1 and Deployment option -2. It has configuration detail of the IR910 and Cisco899G

Deployment Option -1: Sensors Only with 3G as WAN Backup

This section covers the configuration of the IR910. The following are the parameters for cell site configuration - IR910:

- Interface configuration
- Cellular - 3G/4G
- IPSEC
- IP routing

Cell Site Configuration - IR910

```
!*** Gigabit Ethernet interface Configuration ***
```

```
interface GigabitEthernet 0/1
mtu 1200
speed 100
duplex full
description InternetCloud
ip address 10.105.248.175 255.255.255.0
exit

!*** Cellular Configuration Chat script ***

chat-script gsm "" "ATDT*99*1#" TIMEOUT 30 "CONNECT"

!

!*** 3G cellular Configuration ***
interface cellular 0
 ip address negotiated
 dialer string gsm
 exit
!



!*** IPSEC Configuration ***

crypto isakmp profile IPSecRAVPN
!*** Configure Peer Ip address as IPSEC server IP address ***
 set peer address 173.37.41.194
!*** Configure user-fqdn value matches group created in CiscoASAv***
 self-identity user-fqdn <DefaultRAGroup>

 !*** IPSEC method - Remote-access***
 match address remote-access
!*** IPSEC x-auth username and password ***
 xauth-identity <usrname>xauth-password <pwd>
!*** IPSEC mode- aggressive***
 initiate mode aggressive
 pre-share-key <presharedkey>
 policy authentication pre-share
 exit

!
!*** start ipsec***
crypto vpn ipsec IPSecRAVPN
!*** Routing Configuration ***
ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 10.105.248.177
ip route 0.0.0.0 0.0.0.0 cellular 0 Metric 250
```

Note Manual switchover is needed from the cellular interface to the Gigabit Ethernet interface.

Table 2-5 shows layer and IP addressing for VLANs.

Table 2-5 Layer 2 and IP Addressing (VLANs) - Deployment I Sensor Only

Network/Mask	Purpose	VLAN/Port
10.105.248.175/24	IR910	Gi 0/1
10.81.1.14	CSR1Kv - Cloud Server	Gi1
173.39.224.174	CSR1Kv - Internet Cloud	Gi2

Table 2-5 Layer 2 and IP Addressing (VLANs) - Deployment I Sensor Only

Network/Mask	Purpose	VLAN/Port
10.81.1.10, 10.81.1.11, 10.81.1.12	Azeti Control Panel	Gi0
10.81.1.5	CAM	Gi0

Deployment Model - 2: Sensors plus Camera with 4G as WAN Backup

This section covers configuration details for deployment option -1. It covers the following:

- Cell site configuration - IR910
  - Interface configuration on IR910
  - IP routing
- Cell site configuration - Cisco889G
- AAA
- Cellular - 3G/4G
- IPSEC
- IP SLA
- IP routing
- LAN /VLAN configuration

Cell Site Configuration - IR910

Cell site Configuration - C899G

```
!*** Gigabit Ethernet interface Configuration ***

interface GigabitEthernet 0/1
mtu 1200
speed 100
duplex full
description InternetCloud
ip address 10.64.68.10 255.255.255.0
exit

!*** Routing Configuration ***

ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 10.64.68.1
```

Cell Site Configuration - C899G

```
!*** AAA configuration ***
aaa new-model
!
!
aaa authorization network local-group local
!

!
aaa session-id common

!
!*** cellular configuration
```

```
!*** chat-srcipt for LTE ***
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"

!*** Configure interesting traffic***
access-list 1 permit any
dialer-list 1 protocol ip list 1
!

!*** Configure Cellular0***
interface Cellular0
 ip address negotiated
 ip virtual-reassembly in
 encapsulation slip
 dialer in-band
 dialer idle-timeout 60
 dialer string lte
 dialer-group 1
 async mode interactive
!!*** Configure Line 3 mapped to cellular 0***

line 3
 exec-timeout 0 0
 script dialer lte
 modem InOut
 no exec
!

!*** crypto configuration ***

!*** create ikev2 authorization policy ***
crypto ikev2 authorization policy <client-pol>
 route set interface
!*** Access-list map LAN subnet ***
 route set access-list 90
!
!*** create IKEV2 Proposal ***
crypto ikev2 proposal <p1>
 encryption 3des
 integrity md5
 group 2
!
!*** create IKEV2 Policy and map proposal ***
crypto ikev2 policy <p1>
 proposal <p1>
!
!*** create IKEV2 Keyringl ***
crypto ikev2 keyring <key>
  peer peer
  address 0.0.0.0 0.0.0.0
  pre-shared-key <cisco>
 !
!

!*** create IKEV2 profile and map aaa list and client group ***
crypto ikev2 profile <prof>
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local key
 aaa authorization group psk list local-group client-pol


!
```

```
!*** create isakmp Policy ***
crypto isakmp policy 1
hash md5
 authentication pre-share
 group 2
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 group 2
!

!*** create ipsec tranform-set ***
!
crypto ipsec transform-set <trans> esp-3des esp-md5-hmac
 mode tunnel
!
!

!*** create ipsec profile  ***
crypto ipsec profile <prof>
 set transform-set <trans>
 set ikev2-profile <prof>
!

!*** create flex vpn client with source of Tunnel using primary interface (Gi8) ***

crypto ikev2 client flexvpn easy
  peer 1 173.39.224.174
  client connect Tunnel0
!
!*** create flex vpn client with source of Tunnel using secondary interface (Cellular0)
***
crypto ikev2 client flexvpn easy1
  peer 1 173.39.224.174
  client connect Tunnel1
!
!
!*** Create vlan 3 database ***
vlan 3
!
!*** IPSLA configuration with route ***
!
ip sla 1
 icmp-echo 3.3.3.3 source-interface GigabitEthernet8
ip sla schedule 1 life forever start-time now
track 11 ip sla 1
!



!
!
!
!*** Interface configuration ***
!
!
!*** Interface tunnel0 as primary tunnel ***
interface Tunnel0
 ip unnumbered GigabitEthernet8
 tunnel source GigabitEthernet8
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile <prof>
```

```
!
!*** Interface tunnel1 as secondary tunnel ***
interface Tunnel1
 ip unnumbered Cellular0
 tunnel source dynamic
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile <prof>


!*** Interface connected to Internet cloud***
!
interface GigabitEthernet8
 ip address 10.105.248.180 255.255.255.0
  duplex auto
 speed auto
!*** Interface connected to Site controllers and Camera ***

interface Vlan3
 ip address 10.64.68.1 255.255.255.0

!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!*** IPROUTE Configuration ***
ip route 0.0.0.0 0.0.0.0 10.105.248.177 track 10
ip route 0.0.0.0 0.0.0.0 Cellular0 100
ip route 3.3.3.3 255.255.255.255 10.105.248.177
!



access-list 90 permit 10.64.68.0 0.0.0.255
!

!*** LAN side configuration ***



interface GigabitEthernet1
description Connected_IR910
 switchport access vlan 3
 no ip address
!
interface GigabitEthernet2
description Connected_Camera_1
 switchport access vlan 3
 no ip address
!
interface GigabitEthernet3
 description Connected_Camera_2
 switchport access vlan 3
!
interface GigabitEthernet4
description Connected_Camera_3
 switchport access vlan 3
 no ip address
!
```

Table 2-6 shows layer 2 and IP addressing for deployment 1 sensors and the IP camera.

Table 2-6 Layer 2 and IP Addressing (VLANs)- Deployment I Sensor and IP camera

Network/Mask	Purpose	VLAN/Port
10.64.68.10/24	IR910	Vlan 3
10.64.68.201/24	IP Camera 7030E	Vlan 3
10.64.68.202/24	IP Camera 6400	Vlan 3
10.105.248.180	Cisco 898 GA	Gi8
10.81.1.14	CSR1Kv -Cloud Server	Gi1
173.39.224.174	CSR1Kv -Internet Cloud	Gi2
10.81.1.10,10.81.1.11,10.81.1.12	Azeti Control Panel	Gi0
10.81.1.5	CAM	Gi0

Site Controller Installation

This section provides installation step for the site controller on the IR910.

External Modules Installation

There are necessary modules to be installed for functionality, such as, the watchdog module. Install them as part of your initial installation procedure, by completing the following steps:

Step 1 SSH to IR910 by using "system" as user and it's corresponding password.

Step 2 Make an /mnt/data directory in the sensor gateway: **mkdir /mnt/data.**

Step 3 The following modules need to be uploaded to IR910 by using the scp protocol.

```
psutil-2.2.1.linux-armv5tel.tar-1.gz
pycrypto-2.6.1.linux-armv5tel.tar-1.gz
scp system@scp_server_ip:/mnt/data/psutil-2.2.1.linux-armv5tel.tar-1.gz /mnt/data
scp system@ scp_server_ip:/mnt/data/pycrypto-2.6.1.linux-armv5tel.tar-1.gz /mnt/data
```

Step 4 Unpack and install these. If you have a site controller running already, you will need to restart it.

```
cd /mnt/data/azeti/SiteController/lib
tar -xvzf /mnt/data/psutil-2.2.1.linux-armv5tel.tar.gz
tar -xvzf /mnt/data/pycrypto-2.6.1.linux-armv5tel.tar.gz
```

Internal Module Installation

The following steps are required for the installation of internal module:

Step 1 Copy the mosquitto and site controller installation file to a folder by using the SCP protocol where there is enough space. (Roughly 12 MB are required for the files and110 MB for the installation, so around 122 MB of space is required.)

```
scp system@scp_server_ip:/mnt/data/mosquitto-firmware1.2.tar /mnt/data
scp system@scp_server_ip:/mnt/data/SiteController-install-xxxxx.tar.gz   /mnt/data
```

Step 2 Install the mosquito application by completing the following steps:

a. Decompress the file with the following command:

```
cd /mnt/data/
tar xvzf mosquitto-firmware1.2.tar (Example: tar xvzf  mosquitto-firmware1.2.tar)
```

b. Go to the created folder with the same name of the compressed file.

c. Execute the script **./setup.sh** in order to proceed to install the mosquitto MQTT broker.

d. Proceed to the installation of the site controller without starting the broker.

Step 3 Install the site controller by completing the foll:

a. Uncompress the file with the command

```
tar xvzf SiteController-install-xxxxx.tar.gz
```

(Example: tar xvzf SiteController-install-2015-02-20 output):

```
./SiteController-install/
./SiteController-install/lib/
./SiteController-install/lib/six-1.9.0.tar.gz
./SiteController-install/lib/futures-2.1.6.tar.gz
./SiteController-install/lib/pyasn1-0.1.7.tar.gz
./SiteController-install/lib/pycrypto-2.6.1.tar.gz
./SiteController-install/lib/unicodedata.so
./SiteController-install/lib/uart
./SiteController-install/lib/tzlocal-1.1.1.tar.gz
./SiteController-install/lib/pytz-2014.7.tar.gz
./SiteController-install/lib/pyftpdlib-1.4.0.tar.gz
./SiteController-install/lib/psutil-2.2.1.tar.gz
./SiteController-install/lib/modbus-tk-0.4.2.tar.gz
./SiteController-install/lib/setuptools-12.2.tar.gz
./SiteController-install/lib/APScheduler-3.0.0.tar.gz
./SiteController-install/lib/pyserial-2.7.tar.gz
./SiteController-install/lib/bitstring-3.1.3.tar.gz
./SiteController-install/lib/PyXB-1.2.3.tar.gz
./SiteController-install/lib/pysnmp-4.2.5.tar.gz
./SiteController-install/lib/paho-mqtt-1.1.tar.gz
./SiteController-install/lib/Requirements.txt
./SiteController-install/run_SiteController.sh
./SiteController-install/src/
./SiteController-install/src/RawResultsDeMux.py
./SiteController-install/src/ConfigProvider.py
./SiteController-install/src/trapd.py
./SiteController-install/src/result.py
./SiteController-install/src/ac_config.py
./SiteController-install/src/commons.py
./SiteController-install/src/deleteAllPersistantMsg.py
./SiteController-install/src/DataAcquisition_SimulatedResultsDaemon.py
./SiteController-install/src/VS_filesize.py
./SiteController-install/src/DataAcquisition_ResultGeneratorServer.py
./SiteController-install/src/mod.py
./SiteController-install/src/FileReader.py
./SiteController-install/src/action_cfg.py
./SiteController-install/src/gpio_dio.py
./SiteController-install/src/VS_tank_simulator.py
./SiteController-install/src/run_SiteController.py
./SiteController-install/src/VS_access_control.py
./SiteController-install/src/VS_flow_rate.py
./SiteController-install/src/JobProcessor.py
./SiteController-install/src/tcpserver.py
./SiteController-install/src/cloudConnector.py
./SiteController-install/src/serial_line_daemon.py
./SiteController-install/src/azeti_logging.py
./SiteController-install/src/jobs_updateConfig.py
```

```
./SiteController-install/src/test_mqtt_basic_integration.py
./SiteController-install/src/VS_fill_quantity.py
./SiteController-install/src/acli.py
./SiteController-install/src/ftphandler.py
./SiteController-install/src/CalibResultsEvaluator.py
./SiteController-install/src/VS_HistoryAnalyser.py
./SiteController-install/src/rule_cfg.py
./SiteController-install/src/imgfetcher.py
./SiteController-install/src/snmpgetd.py
./SiteController-install/src/test_lib_installed.py
./SiteController-install/src/DataAcquisition_Digital_IO_Simulator.py
./SiteController-install/src/sensor_cfg.py
./SiteController-install/src/UDPserver_AdvantechAdam60xx.py
./SiteController-install/src/DataAcquisition_Numerical_Simulator.py
./SiteController-install/src/test_ftpd.py
./SiteController-install/src/raw_results_to_gnuplot.py
./SiteController-install/src/http_server.py
./SiteController-install/src/Watchdog.py
./SiteController-install/src/wtsc_simulator.py
./SiteController-install/src/AutomationController.py
./SiteController-install/src/persistord.py
./SiteController-install/src/HD2CloudExporter.py
./SiteController-install/src/md5sum.py
./SiteController-install/src/device_cfg.py
./SiteController-install/src/ModbusDaemon/
./SiteController-install/src/ModbusDaemon/ModbusResult.py
./SiteController-install/src/ModbusDaemon/__init__.py
./SiteController-install/src/ModbusDaemon/ModbusSensorBase.py
./SiteController-install/src/ModbusDaemon/ModbusMaster.py
./SiteController-install/src/ModbusDaemon/ModbusGlobals.py
./SiteController-install/src/ModbusDaemon/ModbusDevice.py
./SiteController-install/src/ModbusDaemon/ModbusActuator.py
./SiteController-install/src/ModbusDaemon/Defines.py
./SiteController-install/src/ModbusDaemon/ModbusSensor.py
./SiteController-install/src/ModbusDaemon/MqttHandler.py
./SiteController-install/src/sensor_config.py
./SiteController-install/src/extract_conf_section.py
./SiteController-install/src/VS_battery_details.py
./SiteController-install/src/unittesttest3.py
./SiteController-install/src/VirtualSensorProvider.py
./SiteController-install/SiteController.lsm
./SiteController-install/SiteController-rev-info.txt
./SiteController-install/config/
./SiteController-install/config/azeti_logging.cfg
./SiteController-install/config/SiteController.cfg
./SiteController-install/md5sums.txt
./SiteController-install/setup.sh
```

b. Go to the created folder with the name **SiteController-install**.

```
cd SiteController-install.
```

c. Execute the script **./setup.sh** to proceed to install the site controller modules and all the necessary python libraries.

d. You will be asked for a serial number. This will be the identifier of the system on the Cloud, so choose it according to your infrastructure needs. Just alphanumeric characters are allowed.

e. Read the installation.log file generated in order to check that there were no errors during the installation.

Basic Configuration of Site Controller

Once you finish the installation process, you have a basic site controller system installed. The system has to be configured in order to do the necessary tasks. You can adjust some configuration, for deciding which modules will run in Site Controller to select some parameters of the different modules. Please read carefully the guides about Site Controller before proceeding to change any configuration of the system. A wrong configuration may cause a failure in the monitoring/actuation system that can affect the overall solution.

The required configuration is shown below.

Change the MQTT Folder. Edit the file **/opt/azeti/SiteController/SiteController.conf:** and change the path of the mosquitto folder:

```
MOSQUITTO_FOLDER=/mnt/apps
```

Step 1 Cloud connection: address and username/password for the cloud connection. You will need to edit the file **/mnt/data/azeti/SiteController/config/SiteController.cfg**.

The host, user_id and password are provided to customer from the Azeti for each organization. See an example configuration below.

```
[ExternalBroker]
host=10.0.0.72
sub_topics=cloud/%SYSID%/#
user_id=cvd.cisco@azeti.net
password=password
```

Step 2 To activate TLS connections, edit the file **/mnt/data/azeti/SiteController/config/SiteController.cfg.**

a. Copy the ***.pem** files provided to you by azeti to %SiteController%/config.

b. Edit the port setting in the [ExternalBroker] section in the file cloudConnector.cfg to 8883.

c. Change the setting tls_enable in the [ExternalBroker] section in the file cloudConnector.cfg to True. An example configuration is below:

```
#azetibroker02 azeti organization
tls_enable=True
host=azetibroker02.azeti.net
user_id=user.just.test@azeti.net
password=doNotTryIsFake
port=8883
```

Run Mosquito and Site Controller Application

To run mosquito and the site controller application, complete the following steps:

Step 1 Start the mosquito application with the following command:

```
/mnt/data/azeti/SiteController/run_SiteController.sh start_mosquitto
```

Step 2 Start the site controller application with the following command:

```
/mnt/data/azeti/SiteController/run_SiteController.sh start
```

Step 3 Check the status of the site controller and mosquitto with the following command:

```
/mnt/data/azeti/SiteController/run_SiteController.sh status
```

Output:

```
it shows different modules involved in Site controller
serial of this installation: Lab-Demo01
Main version of this installation: 1.1.0_(Build:895_fd622f9)
Checking installation ... OK.
```

```
ConfigProvider.py is running with PID (15170)
RawResultsDeMux.py is running with PID (15195)
CalibResultsEvaluator.py is running with PID (15206)
JobProcessor.py is running with PID (15219)
Watchdog.py is running with PID (15226)
imgfetcher.py is running with PID (15233)
cloudConnector.py is running with PID (15240)
HD2CloudExporter.py is running with PID (15247)
AutomationController.py is running with PID (15254)
VirtualSensorProvider.py is running with PID (15266)
ModbusDaemon/ModbusMaster.py is running with PID (15291)
UDPserver_AdvantechAdam60xx.py is running with PID (15305)
trapd.py is running with PID (15312)
snmpgetd.py is running with PID (15329)
persistord.py is running with PID (15336)
Mosquitto daemon is running with PID (15141)
```

Setting Up the Sensor Network

This section describes setting up the sensors and interfacing with the sensor gateway. The sensors interface with the sensor gateway using Modbus RTU. The sensor gateway acts as the Modbus server and the sensors are the Modbus clients. Some sensors support Modbus natively and others interfaces via Modbus Adapter. RS485 is the physical connectivity between the sensor gateway and the sensors/adapters. All sensors are powered using DC power. The data sheet of each sensor is covered in section Sensor - Data sheet in Appendix. This section covers following topics:

- Method of slave address configuration
- Slave address plan for CVD
- General wiring
- Connectivity diagram

Method of Slave Address Configuration

The site controller communicates to sensors by using slave address. The slave address of sensors used in our CVD1.0 can be configured in four ways and is given below:

- Configure slave address using modpoll.exe (sensor: AD11B-34GS4-1.0/0-50A*0-65V and CE-AU11-34MS3-0.2/0-65V).
- Configure slave address using Adam utility (sensor: ADAM-4117-AE and ADAM 4150-AE).
- Configure slave address based on Dip switch (sensor: ELKOR WattsOn).
- Configure slave address by using jumper (sensor: Comet T3411).

Configure Slave Address using modpoll.exe

This method is used to configure sensors, such as, AD11B-34GS4-1.0/0-50A*0-65V and CE-AU11-34MS3-0.2/0-65V. Complete the following steps:

Step 1 Connect the device to the PC (with Window or Linux) using a USB/RS485 converter (with the appropriate drivers) or RS232/RS485 (only if the PC has a serial connector) converter.

Step 2 Download Modpoll software and copy the appropriate file to the PC (in the case of windows, the file win32/modpoll.exe):

http://www.modbusdriver.com/modpoll.html

Step 3 Identify the COM port by selecting **Control Panel > System > Device Manager > Port (COM and LTP)**. If using the RS232/RS485 converter plugged to a serial port, it will be the number of the physical port (typically COM1).

Step 4 Open a command line (typing **cmd** on the init menu), go to the folder where modpoll.exe is placed and execute the following command (address a number between 1 and 253, and COM1 the right COM port):

```
modpoll -a 1 -b 9600 -d 8 -p none -s 1 -t 4 -0 -o 3 -1 -r 0x20 COM1 0xAddress06
```

(This address is the new address to be configured in hexadecimal.)

Configure Slave Address using Adam Utility

This method is used to configure sensors, such as, ADAM-4117-AE and ADAM 4150-AE. Complete the following steps:

Configure ADAM-4117-AE

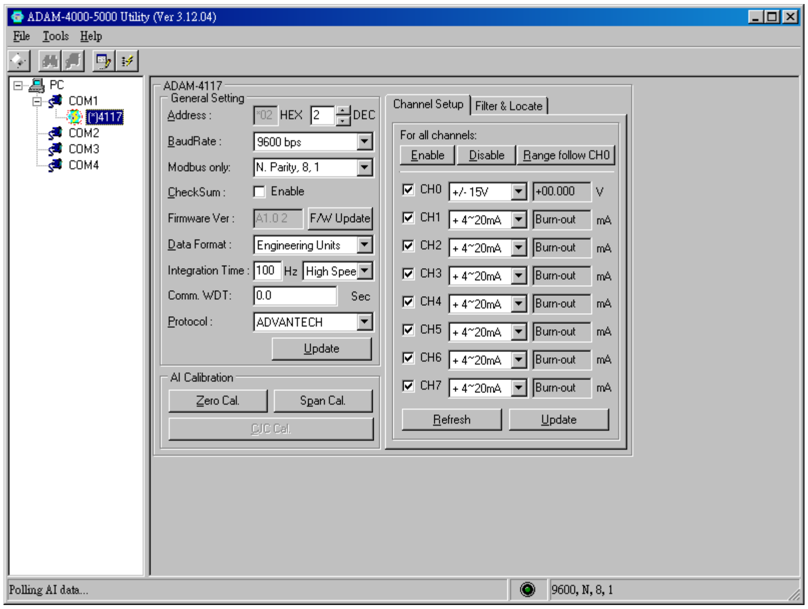
The ADAM-4117 is a 16-bit, 8-channel analog input module that provides programmable input ranges for all channels. Configuration of ADAM-4117 is divided into the following four sections:

- General Setting
- AI Calibration
- Channel Setup
- Filter and Locate

Step 1 Download the ADAM-4000-5000 Utility software from the following link: http://support.advantech.com/support/new_default.aspx

Step 2 Figure 2-49 shows the overview of the ADAM-4000-5000 Utility software.

Figure 2-49 Overview of ADAM-4000-5000 Utility Software



ADAM-4117

General Setting

Address : 02 HEX 2 DEC

BaudRate : 9600 bps

Modbus only: N. Parity, 8, 1

CheckSum : □ Enable

Firmware Ver : A1.02

Data Format : Engineering Units

Integration Time : 100 Hz High Spee

Comm. WDT: 0.0 Sec

Protocol : ADVANTECH

AI Calibration

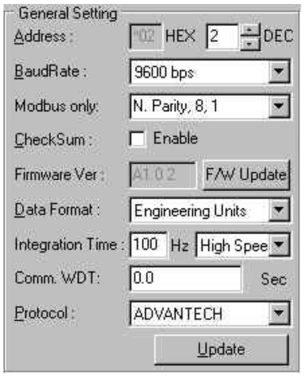
For all channels:

☑ CH0	+/- 15V	+00.000	V
☑ CH1	+ 4~20mA	Burn-out	mA
☑ CH2	+ 4~20mA	Burn-out	mA
☑ CH3	+ 4~20mA	Burn-out	mA
☑ CH4	+ 4~20mA	Burn-out	mA
☑ CH5	+ 4~20mA	Burn-out	mA
☑ CH6	+ 4~20mA	Burn-out	mA
☑ CH7	+ 4~20mA	Burn-out	mA

Polling AI data... 9600, N, 8, 1

Step 3 In **General Settings**, set the Address, Baud rate, Data Format and Checksum status, as shown in Figure 2-50.

Figure 2-50 General Settings



General Setting

Address : 02 HEX 2 DEC

BaudRate : 9600 bps

Modbus only: N. Parity, 8, 1

CheckSum : □ Enable

Firmware Ver : A1.02

Data Format : Engineering Units

Integration Time : 100 Hz High Spee

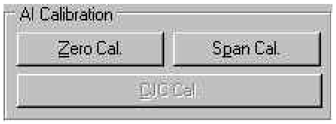
Comm. WDT: 0.0 Sec

Protocol : ADVANTECH

Step 4 There are two types of calibrations (as shown in Figure 2-51):

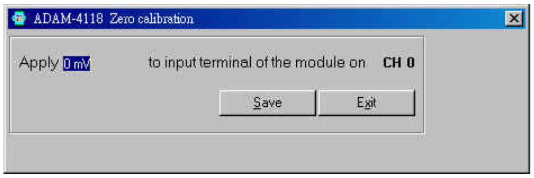
- Zero Calibration
- Span Calibration

Figure 2-51 A1 Calibration



Zero Calibration: Calibrates an analog input module to correct for offset errors, as shown in Figure 2-52.

Figure 2-52 Zero Calibrations

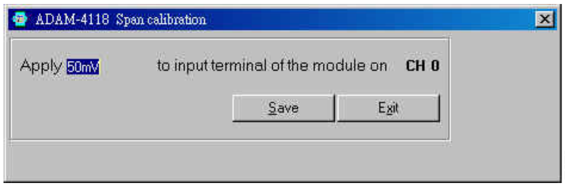


ADAM-4118 Zero calibration

Apply 0 mV to input terminal of the module on CH 0

Span Calibration: Calibrates an analog input module to correct for gain errors, as shown in Figure 2-53.

Figure 2-53 Span Calibration

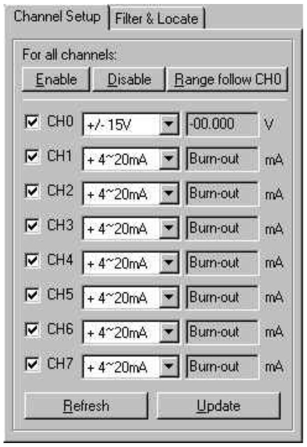


ADAM-4118 Span calibration

Apply 50mV to input terminal of the module on CH 0

Step 5 In **Channel Setup,** click **Refresh** to refresh all channel values, status and range. Select **Update** to set a channel, enable/disable, and input range, as shown in Figure 2-54.

Figure 2-54 Channel Setup

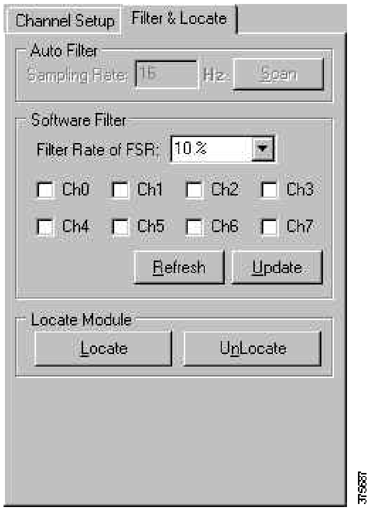


☑ CH0	+/- 15V	-00.000	V
☑ CH1	+ 4~20mA	Burn-out	mA
☑ CH2	+ 4~20mA	Burn-out	mA
☑ CH3	+ 4~20mA	Burn-out	mA
☑ CH4	+ 4~20mA	Burn-out	mA
☑ CH5	+ 4~20mA	Burn-out	mA
☑ CH6	+ 4~20mA	Burn-out	mA
☑ CH7	+ 4~20mA	Burn-out	mA

Step 6 For Filter & Locate, the following options are available (as shown in Figure 2-55):

- Auto Filter - When Integration time is selected, the auto-filter will auto scan major noise and filter it actively.
- Software Filter - Used to ignore the sudden noise.

Figure 2-55 Filter and Locate



Sampling Rate: 15 Hz

Filter Rate of FSR: 10 %

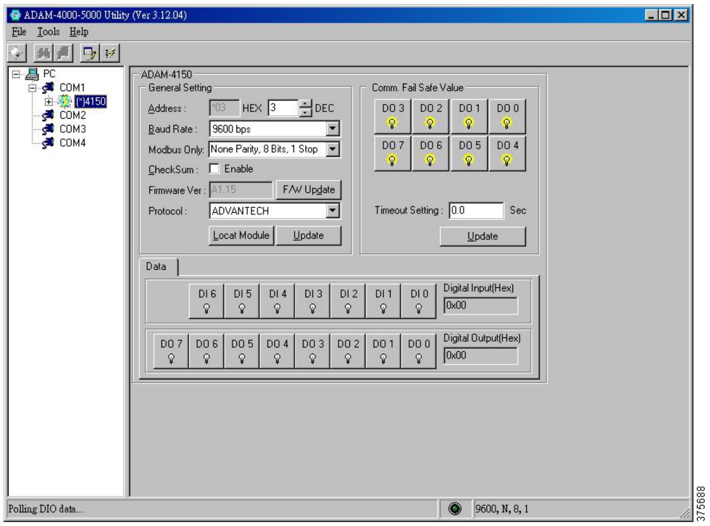
Configure ADAM-4150-AE

The ADAM-4150 features a seven digital input and eight digital output channels. The outputs are open-collector transistor switches that you can control from the host computer. Configuration of ADAM-4150 is divided into the following five sections:

- General setting
- Safety Value setting
- Data Area
- Digital Input Channel
- Digital Output Channel

Step 1 Figure 2-56 shows the overview of the ADAM-4150.

Figure 2-56 Overview of ADAM-4150



Address : *03 HEX 3 DEC

Baud Rate : 9600 bps

Modbus Only: None Parity, 8 Bits, 1 Stop

CheckSum : □ Enable

Firmware Ver : A1.15

Protocol : ADVANTECH

Timeout Setting : 0.0 Sec

Digital Input(Hex) 0x00

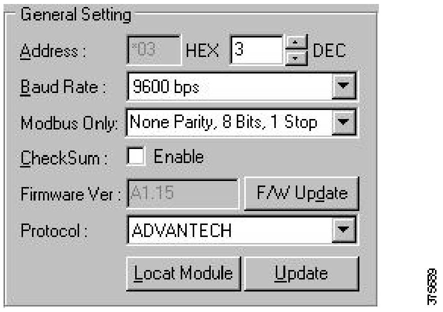
Digital Output(Hex) 0x00

Polling DIO data...

9600, N, 8, 1

Step 2 Select the **General** setting to set the address, baud rate, data format and checksum status, as shown in Figure 2-57.

Figure 2-57 General Setting


General Setting

Address : *03 HEX 3 DEC

Baud Rate : 9600 bps

Modbus Only: None Parity, 8 Bits, 1 Stop

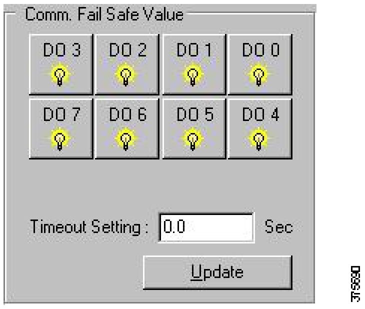
CheckSum : □ Enable

Firmware Ver : A1.15

Protocol : ADVANTECH

Step 3 In the Safety Value setting, the **Communication Fail Safety** value is to force the DO channels to safety status when communication is in time-out and over pre-defined period, as shown in Figure 2-58.

Figure 2-58 Safety Value Setting

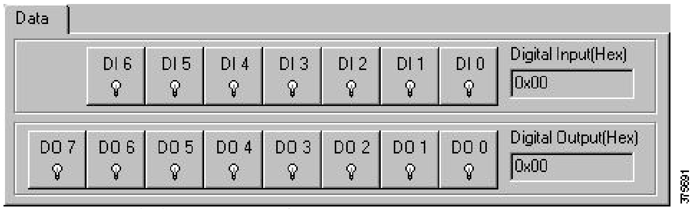

Comm. Fail Safe Value

Timeout Setting : 0.0 Sec

Step 4 In the **Data Area**, configure the following (as shown in Figure 2-59):

- DI Light: Digital data input channel status.
- DO Light: Click to set digital data output channel on or off.

Figure 2-59 Data Area Settings

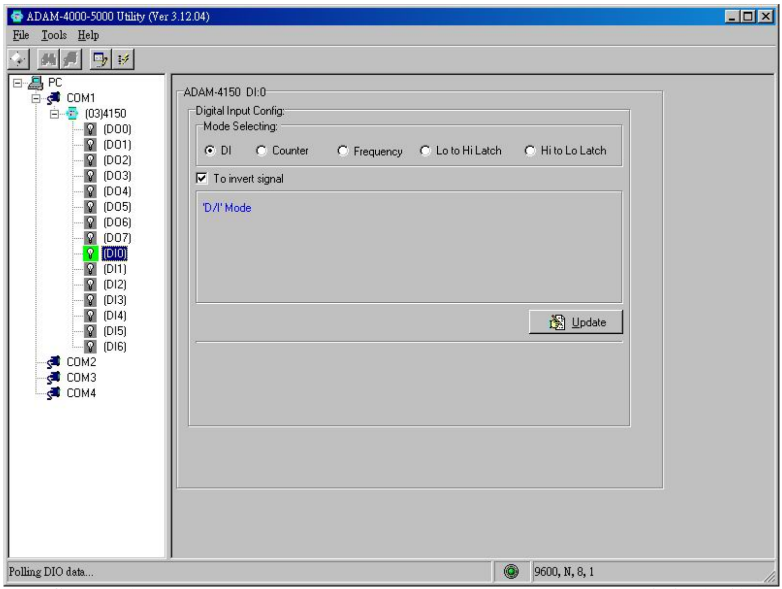

Data

Digital Input(Hex) 0x00

Digital Output(Hex) 0x00

Step 5 Configure **Digital Input Channel**, which can support five types of input: DI, Counter, Frequency, Low to High latch and High to Low latch, as shown in Figure 2-60.

Figure 2-60 Data Input Channel



ADAM-4150 DI:0

Digital Input Config:

Mode Selecting: ● DI ○ Counter ○ Frequency ○ Lo to Hi Latch ○ Hi to Lo Latch

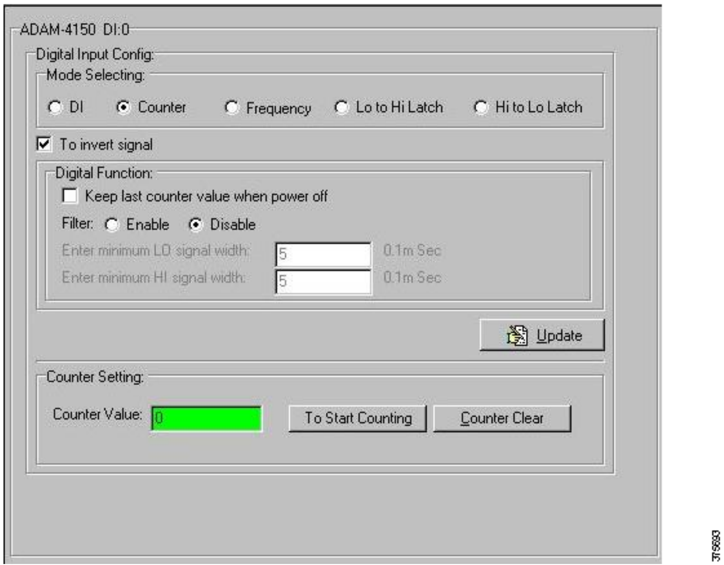
☑ To invert signal

'D/I' Mode

Polling DIO data... 9600, N, 8, 1

Step 6 Configure the Counter Mode.Counter Mode supports the Digital Filter function and can set the minimum width of low and high signal to filter unwanted noise, as shown in Figure 2-61.

Figure 2-61 Counter Mode



ADAM-4150 DI:0

Digital Input Config:

Mode Selecting: ○ DI ● Counter ○ Frequency ○ Lo to Hi Latch ○ Hi to Lo Latch

☑ To invert signal

Digital Function:

☐ Keep last counter value when power off

Filter: ○ Enable ● Disable

Enter minimum LO signal width: 5 0.1m Sec

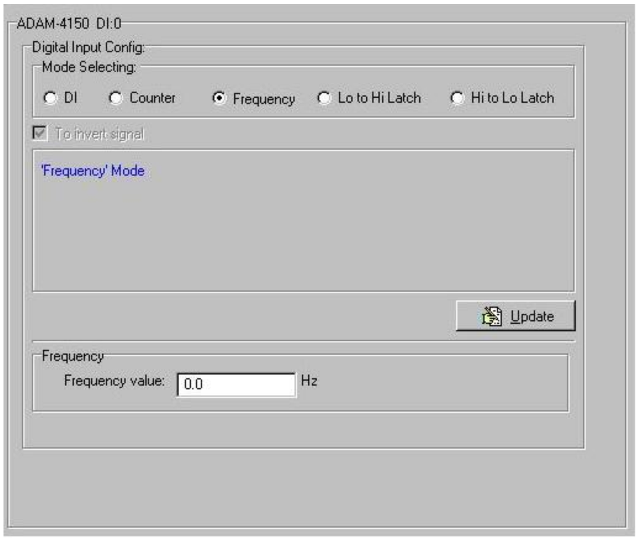
Enter minimum HI signal width: 5 0.1m Sec

Counter Setting:

Counter Value: 0

Step 7 Set the Frequency mode, which can read the frequency value of input signal, as shown in Figure 2-62.

Figure 2-62 Frequency Mode



ADAM-4150 DI:0

Digital Input Config:

Mode Selecting:

○ DI ○ Counter ● Frequency ○ Lo to Hi Latch ○ Hi to Lo Latch

☑ To invert signal

'Frequency' Mode

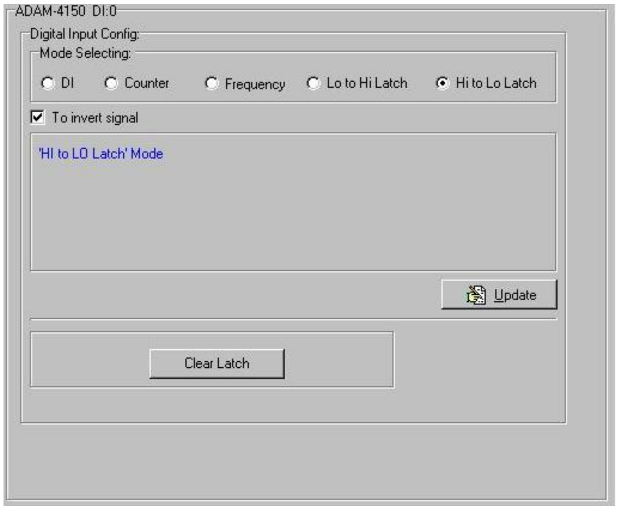
Update

Frequency

Frequency value: 0.0 Hz

Step 8 Configure the Low to High latch and High to Low latch, which can set the high and low latch when the status is changed, as shown in Figure 2-63.

Figure 2-63 Configure the Latch



ADAM-4150 DI:0

Digital Input Config:

Mode Selecting:

○ DI ○ Counter ○ Frequency ○ Lo to Hi Latch ● Hi to Lo Latch

☑ To invert signal

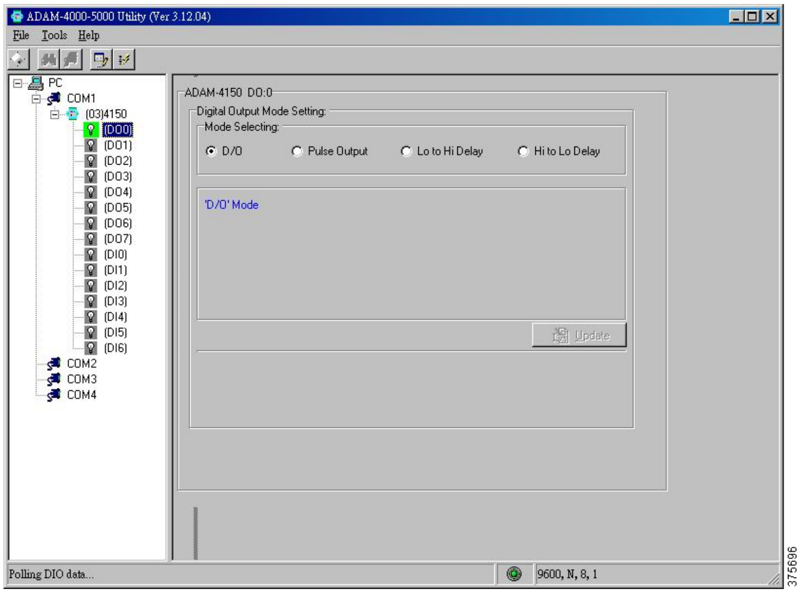
'HI to LO Latch' Mode

Update

Clear Latch

Step 9 The Digital Output Channel can support four types of input: DO, Pulse Output, Low to High delay and High to Low delay, as shown in Figure 2-64.

Figure 2-64 Digital Output Channel



ADAM-4150 DO:0

Digital Output Mode Setting:

Mode Selecting:

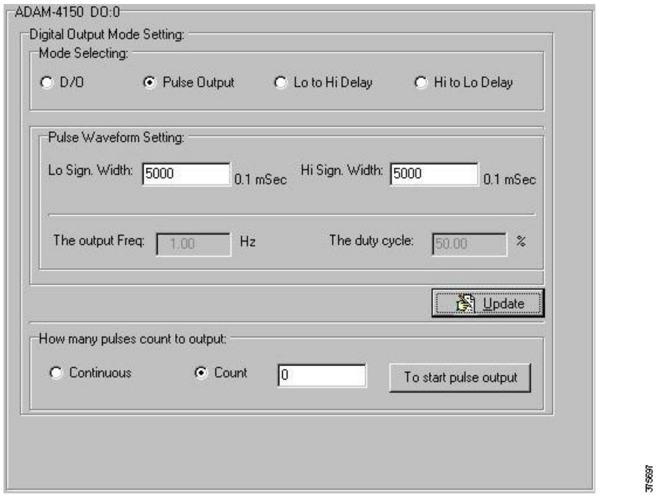
● D/O ○ Pulse Output ○ Lo to Hi Delay ○ Hi to Lo Delay

'D/O' Mode

Polling DIO data... 9600, N, 8, 1

Step 10 Pulse output mode can set the pulse width of low and high signals to determine the output frequency; it also can select the pulses count to output, as shown in Figure 2-65.

Figure 2-65 Pulse Output Mode



ADAM-4150 DO:0

Digital Output Mode Setting:

Mode Selecting:

○ D/O ● Pulse Output ○ Lo to Hi Delay ○ Hi to Lo Delay

Pulse Waveform Setting:

Lo Sign. Width: 5000 0.1 mSec Hi Sign. Width: 5000 0.1 mSec

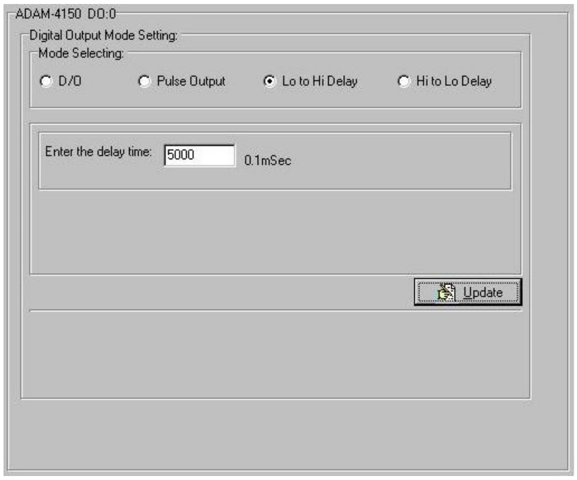
The output Freq: 1.00 Hz The duty cycle: 50.00 %

How many pulses count to output:

○ Continuous ● Count 0

Step 11 Low to High delay and High to Low delay can set the delay time to determine the opportune moment of status change, as shown in Figure 2-66.

Figure 2-66 Set the Delay Time



ADAM-4150 DO:0

Digital Output Mode Setting:

Mode Selecting:

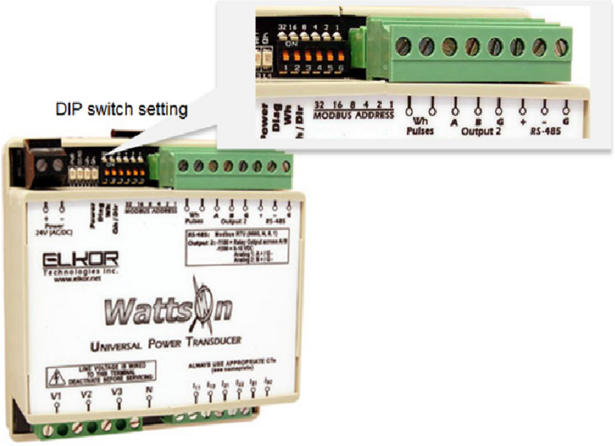
○ D/O ○ Pulse Output ● Lo to Hi Delay ○ Hi to Lo Delay

Enter the delay time: 5000 0.1mSec

Configure Slave Address using DIP Switch

This method is used to configure slave address for ELKOR WattsOn devices. The DIP switch position determines the slave address. It has seven DIP switches and its positioning starts from the right to the left, as shown in Figure 2-67.

Figure 2-67 DIP Switches



Configure Slave Address using Jumper

Complete the following steps to configure sensors, such as, Comet T3411:

Step 1 Open the device and close the jumper.

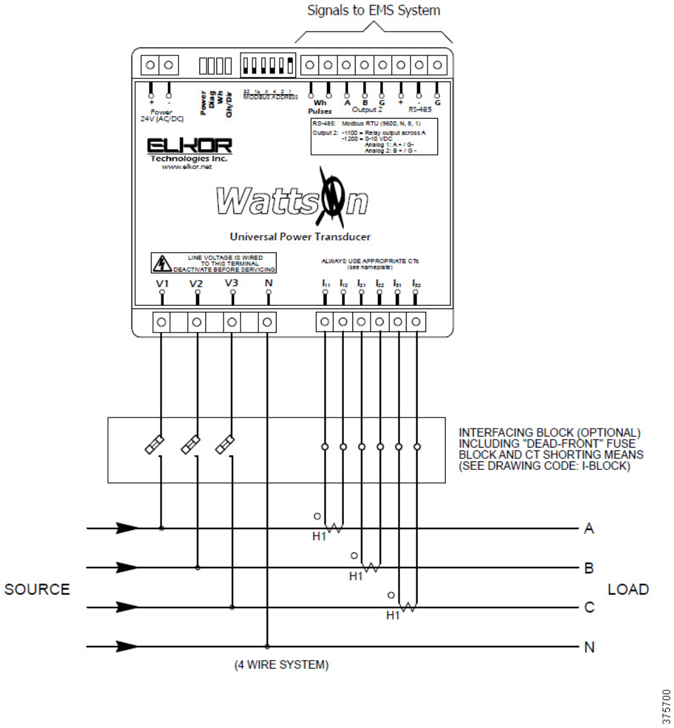
Step 2 Connect the device to the PC using the USB/RS485 converter.

Step 3 Power on the device.

Step 4 Launch the Tsensor software from Comet at the following link: http://www.cometsystem.com/products/tsensor/reg-TSensor#download

Step 5 Leave the standard communications settings. Change the address based on requirements.

Figure 2-68 Communications Settings


Signals to EMS System
+
-
Power
24V (AC/DC)
Power
Diag
Wh
Qh/Dir
32 16 8 4 2 1
MODBUS ADDRESS
Wh
Pulses
A
B
G
Output 2
+
-
G
RS-485
RS-485: Modbus RTU (9600, N, 8, 1)
Output 2: -1100 = Relay output across A
-1200 = 0-10 VDC
Analog 1: A + / G-
Analog 2: B + / G -
ELKOR
Technologies Inc.
www.elkor.net
WattsOn
Universal Power Transducer
LINE VOLTAGE IS WIRED TO THIS TERMINAL DEACTIVATE BEFORE SERVICING
ALWAYS USE APPROPRIATE CTs (see nameplate)
V1
V2
V3
N
I11
I12
I21
I22
I31
I32
INTERFACING BLOCK (OPTIONAL) INCLUDING "DEAD-FRONT" FUSE BLOCK AND CT SHORTING MEANS (SEE DRAWING CODE: I-BLOCK)
H1
H1
H1
A
B
C
N
SOURCE
LOAD
(4 WIRE SYSTEM)
375700

Step 6 Once the device is found, set the new parameters and save.

Standard Slave Address Plan

Table 2-7 shows the suggested slave address plan. This plan is meant to be a guideline to follow, but can be changed if necessary.

Table 2-7 Standard Slave Address Plan

Vendor	Device	Baud Rate	Port	Address
Advantech	ADAM-4051-BE	115200	1	51
Advantech	ADAM-4117-AE	115200	1	17
Advantech	ADAM 4150-AE	115200	1	50
Elkor	(B4) WattsOn-1100-MSCT2-600A	9600	2	2
Elkor	(B5) WattsOn-1100-MSCT2-600A	9600	2	3
CE-Transducers	AD11B-34GS4-1.0/0-250A*0-65V	9600	2	10
CE-Transducers	CE-AU11-34MS3-0.2/0-65V	9600	2	11
Comet	T3411	9600	2	20

If more sensors are needed, the address should be the next on each category. For example, if a new Voltage Meter (AU11) is needed, the address should be 21. If a new AC Meter is needed (WattsOn), it should have the 4 address.

General Wiring

Each of the sensors requires a power supply and serial RS485-based MODBUS connection. The RS485 physical connection is daisy chained across all MODBUS devices, since this is a shared bus serial protocol. The power source can also be shared among multiple devices, but check power consumption of the devices plus sensors when searching for the power source. The devices are powered through 24V DC. Use a standard three core cable to provide the MODBUS data connection (2 wires + 1 GND) and the V+,V- 24V DC power supply.

WattsOn-1100-MS360-500A and MS360

In order to properly measure the AC power, the WattsOn has to be connected to the voltage and current transformers. The typical wiring (3-phase) is shown in Figure 2-69.

Figure 2-69 Typical 3-Phase Wiring

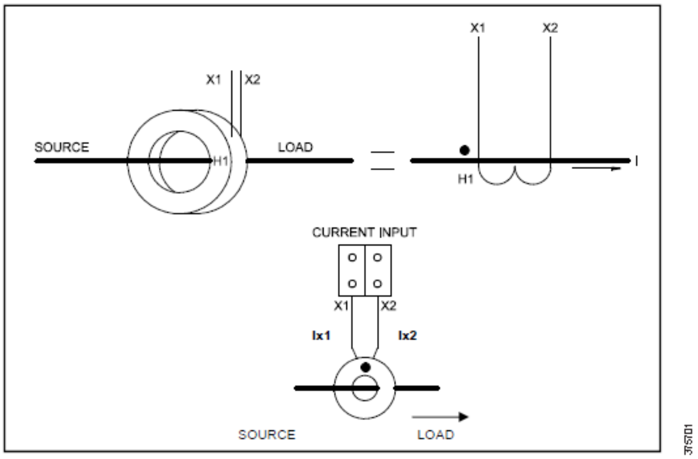
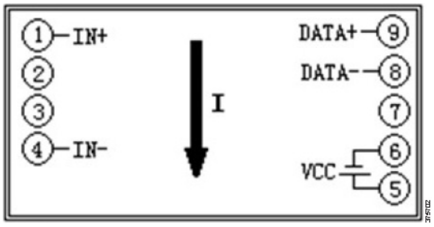
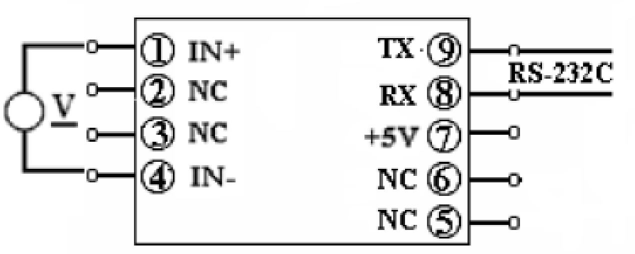


*Figure 2-70 DC Multi-Parameter CE AD11B-34GS4-1.0/0-250A*0-65V*



The AD11B is a multi-parameter device that measures voltage, current and power. The voltage is measured through contacts 1 and 4 on the device base. Current is measured through the split core CT, as shown in Figure 2-71.

Figure 2-71 AD11B Device



- Terminal 1: Positive signal input (Voltage to be measured.)
- Terminal 4: Negative signal input (Voltage to be measured.)
- Terminal 5: Positive power supply (+24VDC)
- Terminal 6: Negative power supply (Ground)
- Terminal 8: Modbus, DATA - (b)
- Terminal 9: Modbus, DATA + (a)

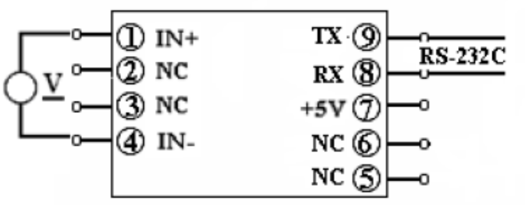
Note

- To open/close the split core, press and move the orange bolt to the open/close direction.
- The conductor carrying the input current should pass through the center of the aperture as perpendicularly as possible and lock the bolt.

DC Voltage Meter CE-AU11-34MS3-0.2/0-65V

The CE AU11 is a DC voltage meter that can measure DC Voltage through contacts 1 and 4.

Figure 2-72 CE AU11

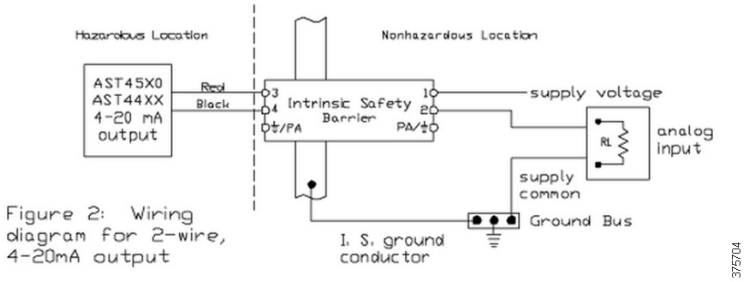


- Terminal 1: Positive signal input (Voltage to be measured)
- Terminal 4: Negative signal input (Voltage to be measured)
- Terminal 5: Positive power supply (+24VDC)
- Terminal 6: Negative power supply (Ground)
- Terminal 8: Modbus, DATA - (b)
- Terminal 9: Modbus, DATA + (a)

Fuel Sensor Mounting

The AS4510 fuel sensor must be mounted to use the 4-20mA ouput. The connection diagram is shown in Figure 2-73.

Figure 2-73 Fuel Sensor Mounting Connection Diagram



The analog input must be connected to one of the T3-32I inputs, which has previously been configured as a 0-20mA input.

The red cable has to be connected to a +24V DC power supply.

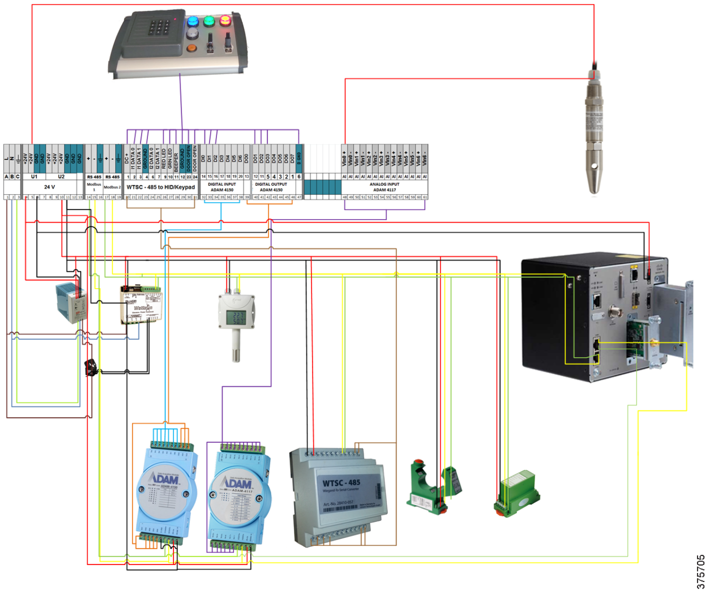
The black cable has to be connected to the analog input of the Adam 4117. The negative one has to be connected to ground. For example, if using Input 0, the black cable has to be connected to the IN0+ and ground to the IN0-.

The translucent tube should not be obstructed, since it is used for compensate the atmospheric pressure. It is also important to make sure that the sensor is placed at the bottom of the tank.

Connectivity Diagram

Figure 2-74 shows connectivity between all sensor and IR910.

Figure 2-74 Connectivity Diagram



The site controller collects data from different types of sensors. shows the sensors that have been tested.

Table 2-8 Site Controller Data

Vendor	Device	Use Cases
Advantech	ADAM-4117-AE	Analog to digital converter (pressure-voltage - digital)
Advantech	ADAM 4150-AE	Switch on/off, sense dry contact
Elkor	WattsOn-1100-MS160-120A	AC voltage, frequency, AC power, and power consumption
Elkor	i-Snail-S	AC Current
CE-Transducers	AD11B-34GS4-1.0/0-50A*0-65V	DC Current FLOW
CE-Transducers	CE-AU11-34MS3-0.2/0-65V	DC Voltage, DC current, DC power, and DC power consumption
Comet	Magnetic door contact SA-200-A	Door open/close sensor
Comet	T3411	Temperature/humidity
AST sensors	AST 4510 - Pressure Sensor	Fuel level, fuel leakage, fuel theft
Infranet	WTSC-485 Wiegand to RS-485 converter (for keypad)	Door access/control
HIDGlobal	Keypad HIDGlobal Proxpro 5355 including WTSC-485 converter	Door access/control

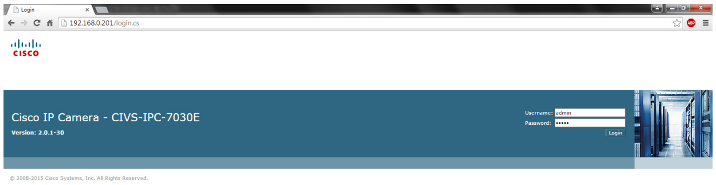
IP Camera Installation

This section explains installing the IP camera. All IP cameras are configured with static a IP address. The IP default gateway is configured with the IP address of G899G. All IP cameras are powered up by using POE interface.

The following steps need to be performed for integration of IP camera:

Step 1 Log in to the IP camera's webpage using its current/default IP address, as shown in Figure 2-75.

Figure 2-75 Camera Login Page



Login

192.168.0.201/login.cs

Cisco IP Camera - CIVS-IPC-7030E
Version: 2.0.1-30

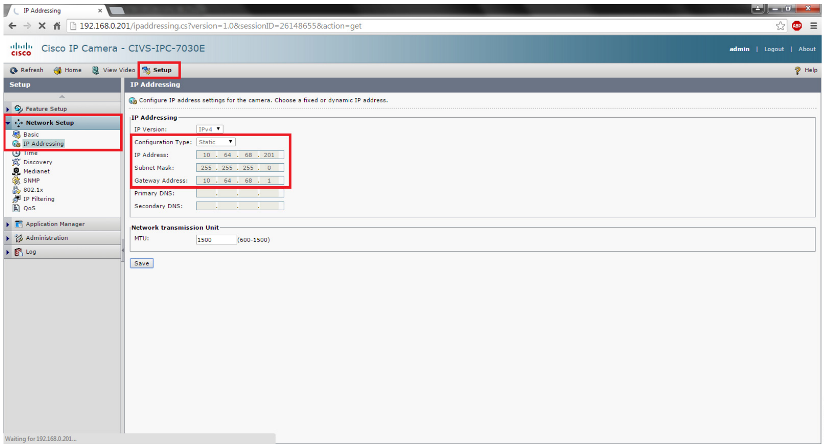
Username: admin
Password: •••••
Login

© 2008-2015 Cisco Systems, Inc. All Rights Reserved.

375706

Step 2 In the **Setup** tab, select the **IP Addressing** option under the **Network Setup** option to configure the static IP address, subnet mask, and gateway address, as shown in Figure 2-76.

Figure 2-76 Static IP Address Configuration



IP Addressing

192.168.0.201/ipaddressing.cs?version=1.0&sessionID=26148655&action=get

Cisco IP Camera - CIVS-IPC-7030E — admin | Logout | About

Refresh | Home | View Video | Setup | Help

Setup

- Feature Setup
- **Network Setup**
  - Basic
  - IP Addressing
  - Time
  - Discovery
  - Medianet
  - SNMP
  - 802.1x
  - IP Filtering
  - QoS
- Application Manager
- Administration
- Log

IP Addressing

Configure IP address settings for the camera. Choose a fixed or dynamic IP address.

IP Addressing

IP Version: IPv4
Configuration Type: Static
IP Address: 10 . 64 . 68 . 201
Subnet Mask: 255 . 255 . 255 . 0
Gateway Address: 10 . 64 . 68 . 1
Primary DNS: . . .
Secondary DNS: . . .

Network transmission Unit

MTU: 1500 (600-1500)

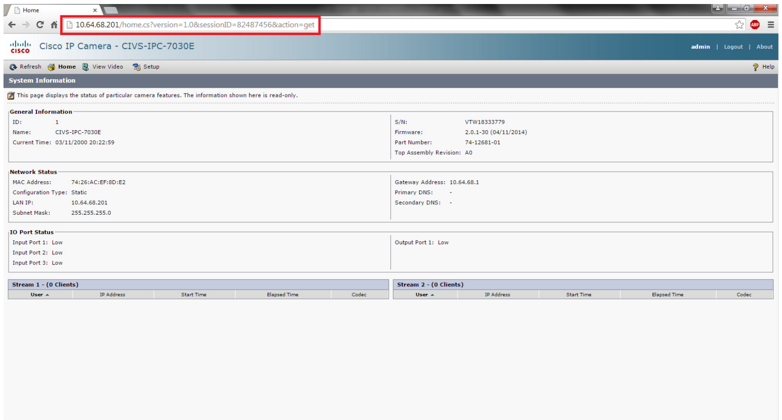
Save

Waiting for 192.168.0.201...

375707

Step 3 Now the log in can be done using the new static IP address, as shown in Figure 2-77.

Figure 2-77 Log in Camera with New IP Address



Home

10.64.68.201/home.cs?version=1.0&sessionID=82487456&action=get

Cisco IP Camera - CIVS-IPC-7030E — admin | Logout | About

Refresh | Home | View Video | Setup | Help

System Information

This page displays the status of particular camera features. The information shown here is read-only.

General Information

ID: 1
Name: CIVS-IPC-7030E
Current Time: 03/11/2000 20:22:59

S/N: VTW18333779
Firmware: 2.0.1-30 (04/11/2014)
Part Number: 74-12681-01
Top Assembly Revision: A0

Network Status

MAC Address: 74:26:AC:EF:8D:E2
Configuration Type: Static
LAN IP: 10.64.68.201
Subnet Mask: 255.255.255.0

Gateway Address: 10.64.68.1
Primary DNS: -
Secondary DNS: -

IO Port Status

Input Port 1: Low
Input Port 2: Low
Input Port 3: Low

Output Port 1: Low

Stream 1 - (0 Clients)

User ▲	IP Address	Start Time	Elapsed Time	Codec

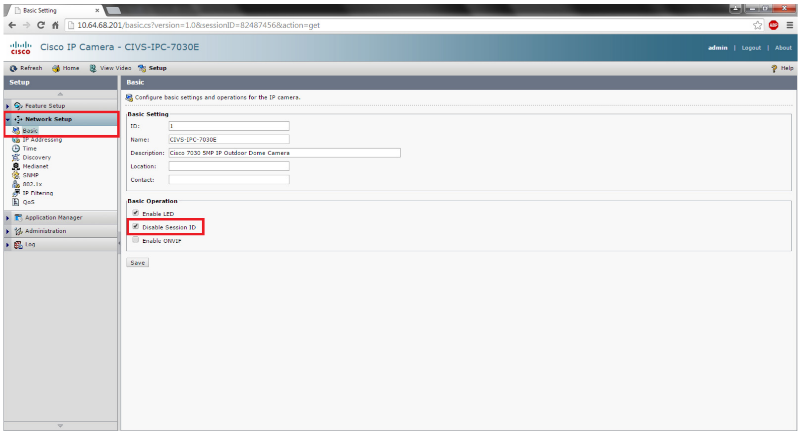
Stream 2 - (0 Clients)

User ▲	IP Address	Start Time	Elapsed Time	Codec

375708

Step 4 Select the **Disable Session ID** check box under the **Basic** option of **Networking** to disable the session ID, as shown in Figure 2-78.

Figure 2-78 Disabling Session ID



Basic

Configure basic settings and operations for the IP camera.

Basic Setting

ID: 1

Name: CIVS-IPC-7030E

Description: Cisco 7030 5MP IP Outdoor Dome Camera

Location:

Contact:

Basic Operation

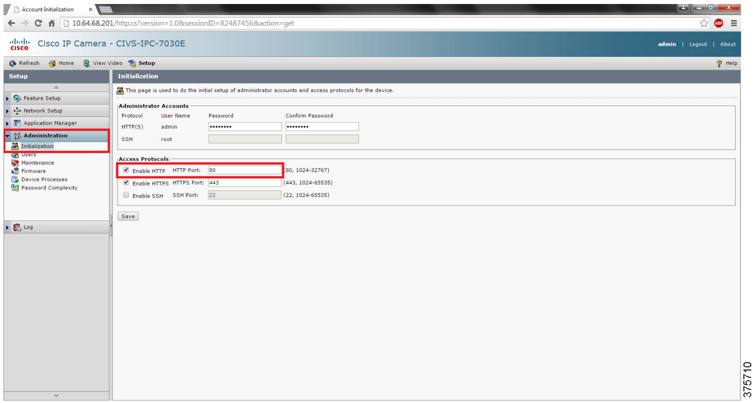
☑ Enable LED

☑ Disable Session ID

☐ Enable ONVIF

Step 5 Select the **Enable HTTP** check box under the **Initialization** option of **Administration** to enable HTTP access to the camera, as shown in Figure 2-79.

Figure 2-79 Enabling HHTP Access



Initialization

This page is used to do the initial setup of administrator accounts and access protocols for the device.

Administrator Accounts

Protocol	User Name	Password	Confirm Password
HTTP(S)	admin	••••••••	••••••••
SSH	root		

Access Protocols

☑ Enable HTTP HTTP Port: 80 (80, 1024-32767)

☑ Enable HTTPS HTTPS Port: 443 (443, 1024-65535)

☐ Enable SSH SSH Port: 22 (22, 1024-65535)

Step 6 The test to check that the API is working can be done by accessingthe following link: http://10.64.68.201/StreamingSetting?version=1.0&action=getPicture&ChannelID=1&ChannelName=Channel1&userName=admin&password=Admin@123&SnapShotImageType=2

Site Configuration

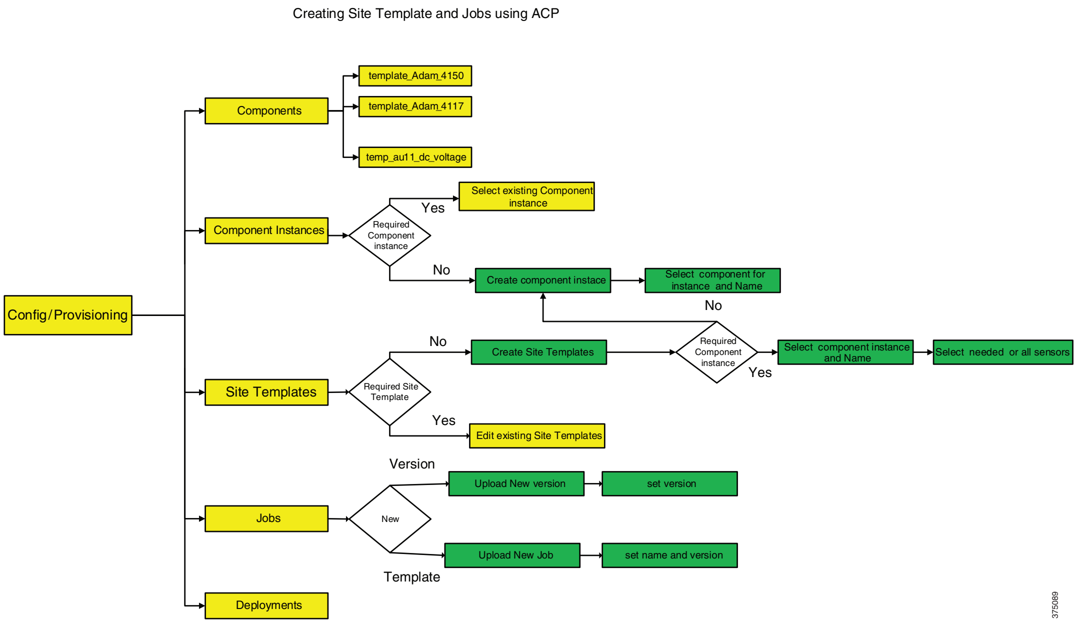
This section covers provisioning of various services on the site controller by using ACP. This chapter covers following sections:

- Adding the site controller on ACP
- Provisioning of services on the site controller using ACP

New Site Template Creation

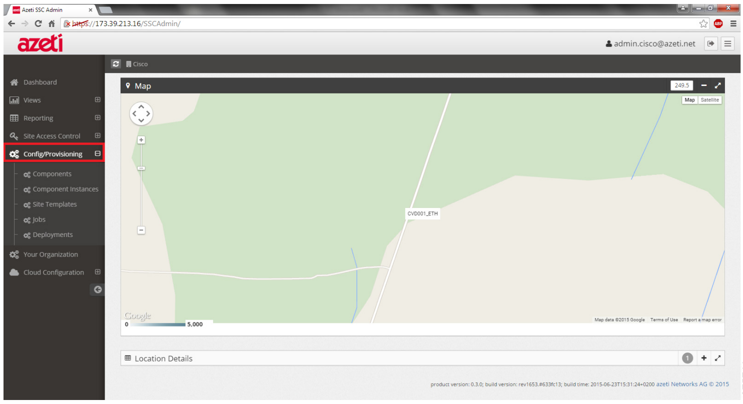
This section explains about the procedure to provision service on the site controller. The work flow diagram for it is shown in Figure 3-1.

Figure 3-1 Flow Chart of Creating Site Template and Jobs using ACP



Step 1 Select **Config/Provisioning** to start provisioning, as shown in Figure 3-2.

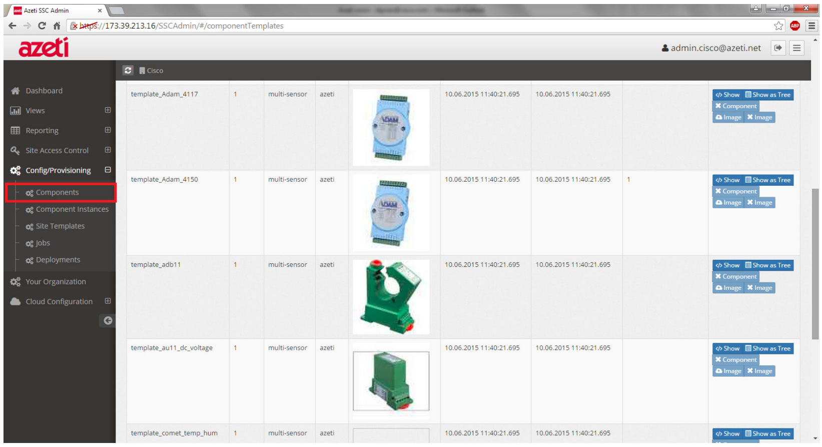
Figure 3-2 Config/Provisioning Option



product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 2 Select **Components** to see a list of supporting components, as shown in Figure 3-3.

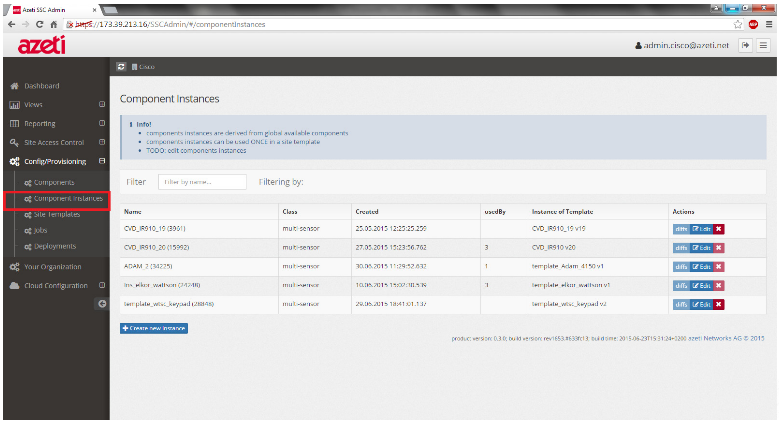
Figure 3-3 List of Components



template_Adam_4117	1	multi-sensor	azeti		10.06.2015 11:40:21.695	10.06.2015 11:40:21.695		Show Show as Tree Component Image Image
template_Adam_4150	1	multi-sensor	azeti		10.06.2015 11:40:21.695	10.06.2015 11:40:21.695	1	Show Show as Tree Component Image Image
template_adb11	1	multi-sensor	azeti		10.06.2015 11:40:21.695	10.06.2015 11:40:21.695		Show Show as Tree Component Image Image
template_au11_dc_voltage	1	multi-sensor	azeti		10.06.2015 11:40:21.695	10.06.2015 11:40:21.695		Show Show as Tree Component Image Image
template_comet_temp_hum	1	multi-sensor	azeti		10.06.2015 11:40:21.695	10.06.2015 11:40:21.695		Show Show as Tree

Step 3 Create a new component instance with available components, as shown in Figure 3-4.

Figure 3-4 Component Instances



Component Instances

Info!
- components instances are derived from global available components
- components instances can be used ONCE in a site template
- TODO: edit components instances

Filter: Filter by name... Filtering by:

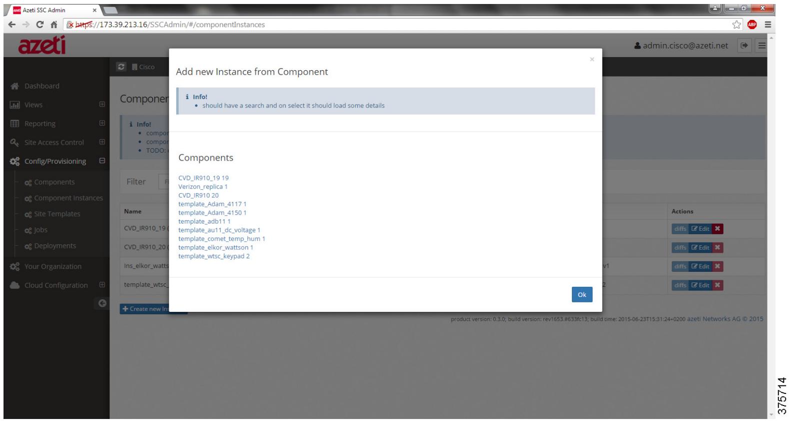
Name	Class	Created	usedBy	Instance of Template	Actions
CVD_IR910_19 (3961)	multi-sensor	25.05.2015 12:25:25.259		CVD_IR910_19 v19	diffs Edit ✖
CVD_IR910_20 (15992)	multi-sensor	27.05.2015 15:23:56.762	3	CVD_IR910 v20	diffs Edit ✖
ADAM_2 (34225)	multi-sensor	30.06.2015 11:29:52.632	1	template_Adam_4150 v1	diffs Edit ✖
Ins_elkor_wattson (24248)	multi-sensor	10.06.2015 15:02:30.539	3	template_elkor_wattson v1	diffs Edit ✖
template_wtsc_keypad (28848)	multi-sensor	29.06.2015 18:41:01.137		template_wtsc_keypad v2	diffs Edit ✖

+ Create new Instance

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 4 Select **Create New Instance**, as shown in Figure 3-5.

Figure 3-5 *Creating New Instances*



Add new Instance from Component

Info!
- should have a search and on select it should load some details

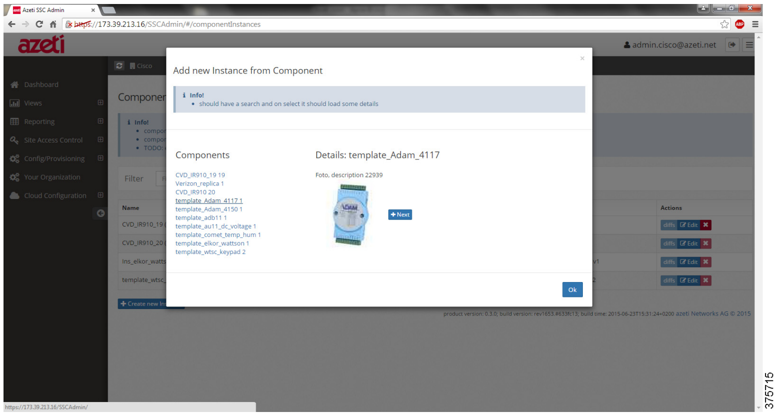
Components

CVD_IR910_19 19
Verizon_replica 1
CVD_IR910 20
template_Adam_4117 1
template_Adam_4150 1
template_adb11 1
template_au11_dc_voltage 1
template_comet_temp_hum 1
template_elkor_wattson 1
template_wtsc_keypad 2

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 5 Select one of the components to be added, as shown in Figure 3-6.

Figure 3-6 *Adding New Components*



Add new Instance from Component

Info!
- should have a search and on select it should load some details

Components

CVD_IR910_19 19
Verizon_replica 1
CVD_IR910 20
template_Adam_4117 1
template_Adam_4150 1
template_adb11 1
template_au11_dc_voltage 1
template_comet_temp_hum 1
template_elkor_wattson 1
template_wtsc_keypad 2

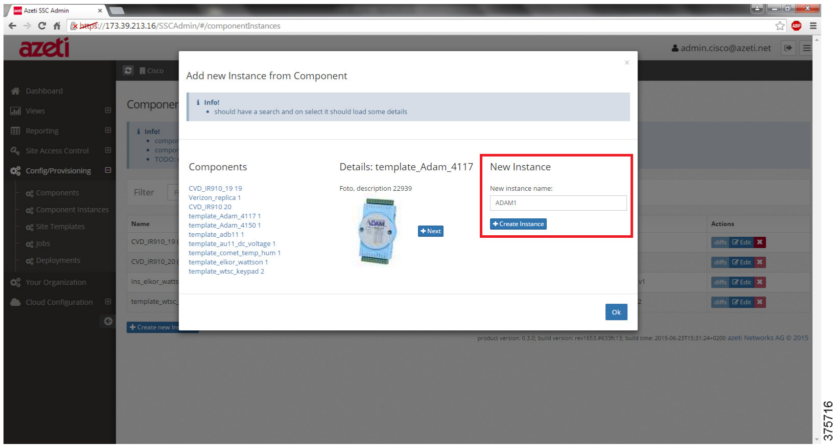
Details: template_Adam_4117

Foto, description 22939

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 6 Name the new instance and select **Create Instance**, as shown in Figure 3-7.

Figure 3-7 *Naming the New Instance*



Add new Instance from Component

Info!
- should have a search and on select it should load some details

Components

CVD_IR910_19 19
Verizon_replica 1
CVD_IR910 20
template_Adam_4117 1
template_Adam_4150 1
template_adb11 1
template_au11_dc_voltage 1
template_comet_temp_hum 1
template_elkor_wattson 1
template_wtsc_keypad 2

Details: template_Adam_4117

Foto, description 22939

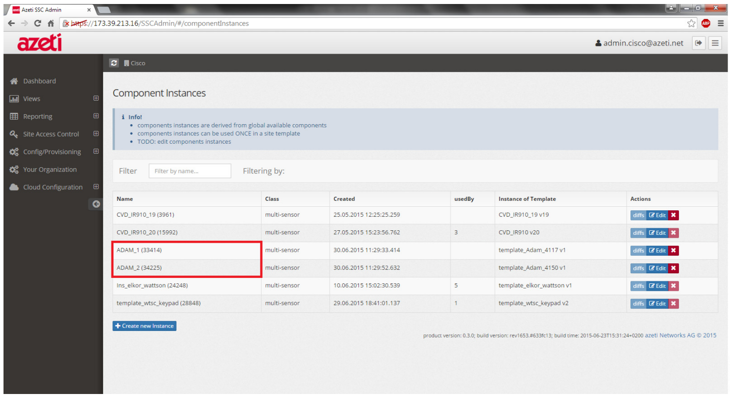
New Instance

New instance name: ADAM1

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 7 The list of new component instances will be visible now, as shown in Figure 3-8.

Figure 3-8 List of Newly Created Component Instances



Component Instances

Info!
- components instances are derived from global available components
- components instances can be used ONCE in a site template
- TODO: edit components instances

Filter: Filter by name... Filtering by:

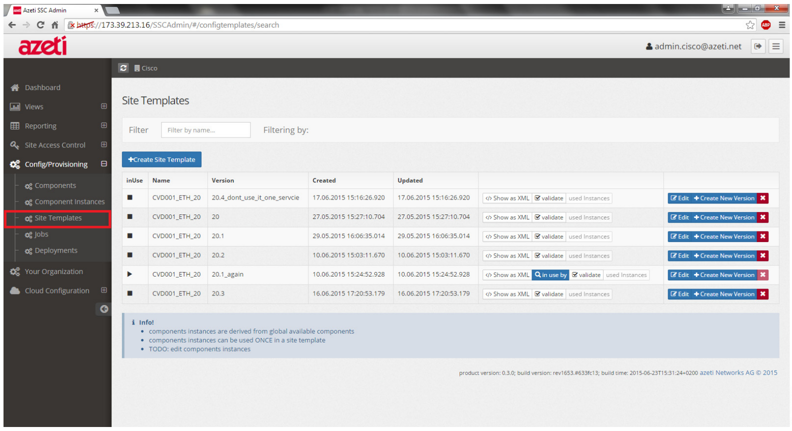
Name	Class	Created	usedBy	Instance of Template	Actions
CVD_IR910_19 (3961)	multi-sensor	25.05.2015 12:25:25.259		CVD_IR910_19 v19	diffs Edit ✖
CVD_IR910_20 (15992)	multi-sensor	27.05.2015 15:23:56.762	3	CVD_IR910 v20	diffs Edit ✖
ADAM_1 (33414)	multi-sensor	30.06.2015 11:29:33.414		template_Adam_4117 v1	diffs Edit ✖
ADAM_2 (34225)	multi-sensor	30.06.2015 11:29:52.632		template_Adam_4150 v1	diffs Edit ✖
Ins_elkor_wattson (24248)	multi-sensor	10.06.2015 15:02:30.539	5	template_elkor_wattson v1	diffs Edit ✖
template_wtsc_keypad (28848)	multi-sensor	29.06.2015 18:41:01.137	1	template_wtsc_keypad v2	diffs Edit ✖

+ Create new Instance

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 8 Create a new site template with a selection of multiple component instances, as shown in Figure 3-9.

Figure 3-9 Site Templates



Site Templates

Filter: Filter by name... Filtering by:

+Create Site Template

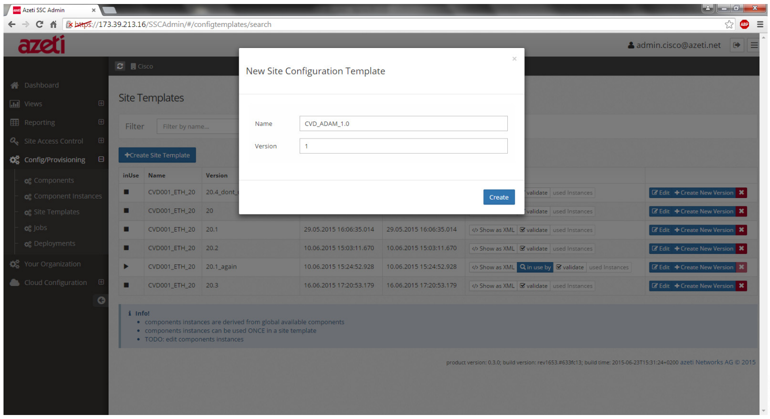
inUse	Name	Version	Created	Updated		
■	CVD001_ETH_20	20.4_dont_use_it_one_servcie	17.06.2015 15:16:26.920	17.06.2015 15:16:26.920	Show as XML validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20	27.05.2015 15:27:10.704	27.05.2015 15:27:10.704	Show as XML validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20.1	29.05.2015 16:06:35.014	29.05.2015 16:06:35.014	Show as XML validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20.2	10.06.2015 15:03:11.670	10.06.2015 15:03:11.670	Show as XML validate used Instances	Edit + Create New Version ✖
▶	CVD001_ETH_20	20.1_again	10.06.2015 15:24:52.928	10.06.2015 15:24:52.928	Show as XML in use by validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20.3	16.06.2015 17:20:53.179	16.06.2015 17:20:53.179	Show as XML validate used Instances	Edit + Create New Version ✖

Info!
- components instances are derived from global available components
- components instances can be used ONCE in a site template
- TODO: edit components instances

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 9 Select the Create Site Template option to create a new site template, as shown in Figure 3-10.

Figure 3-10 Create a New Site Template



New Site Configuration Template

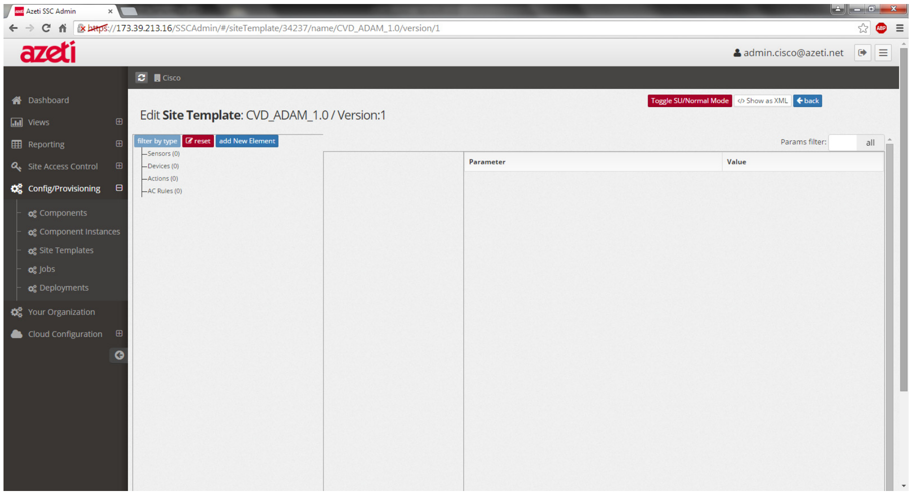
Name: CVD_ADAM_1.0

Version: 1

Create

Step 10 Select the **Edit** option for the new site template to edit it by using the required component instances, as shown in Figure 3-11.

Figure 3-11 Edit Site Templates

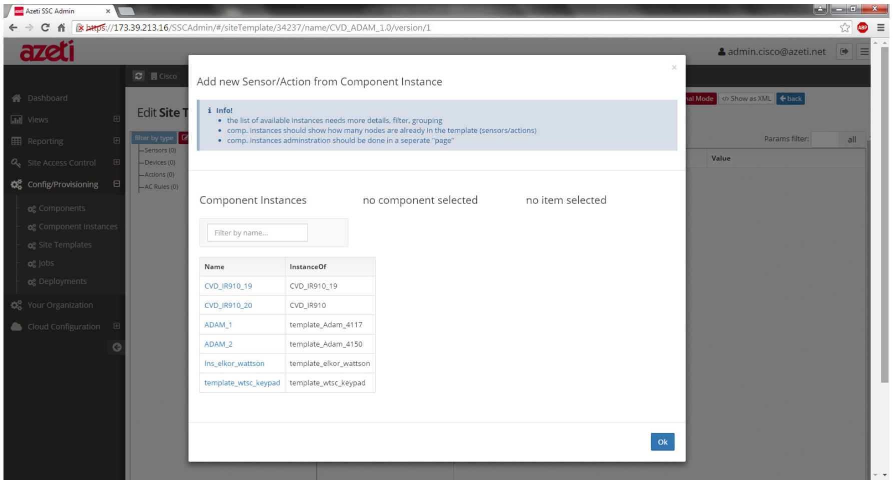


Edit **Site Template**: CVD_ADAM_1.0 / Version:1

375099

Step 11 Select the **Add New Element** option to add the component instances to that site template, as shown in Figure 3-12.

Figure 3-12 Component Instance Selection



Add new Sensor/Action from Component Instance

Info!

- the list of available instances needs more details, filter, grouping
- comp. instances should show how many nodes are already in the template (sensors/actions)
- comp. instances adminstration should be done in a seperate "page"

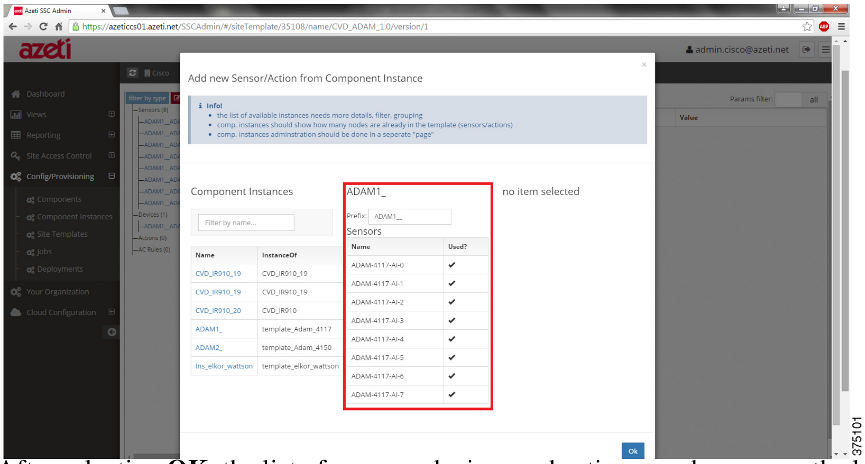
Component Instances no component selected no item selected

Name	InstanceOf
CVD_IR910_19	CVD_IR910_19
CVD_IR910_20	CVD_IR910
ADAM_1	template_Adam_4117
ADAM_2	template_Adam_4150
Ins_elkor_wattson	template_elkor_wattson
template_wtsc_keypad	template_wtsc_keypad

375100

Step 12 Select the sensors required and name a prefix, as shown in Figure 3-13.

Figure 3-13 Sensor and Prefix Selection



Add new Sensor/Action from Component Instance

Info!

- the list of available instances needs more details, filter, grouping
- comp. instances should show how many nodes are already in the template (sensors/actions)
- comp. instances adminstration should be done in a seperate "page"

Component Instances

Filter by name...

Name	InstanceOf
CVD_IR910_19	CVD_IR910_19
CVD_IR910_19	CVD_IR910_19
CVD_IR910_20	CVD_IR910
ADAM1_	template_Adam_4117
ADAM2_	template_Adam_4150
Ins_elkor_wattson	template_elkor_wattson

ADAM1_

Prefix: ADAM1__

Sensors

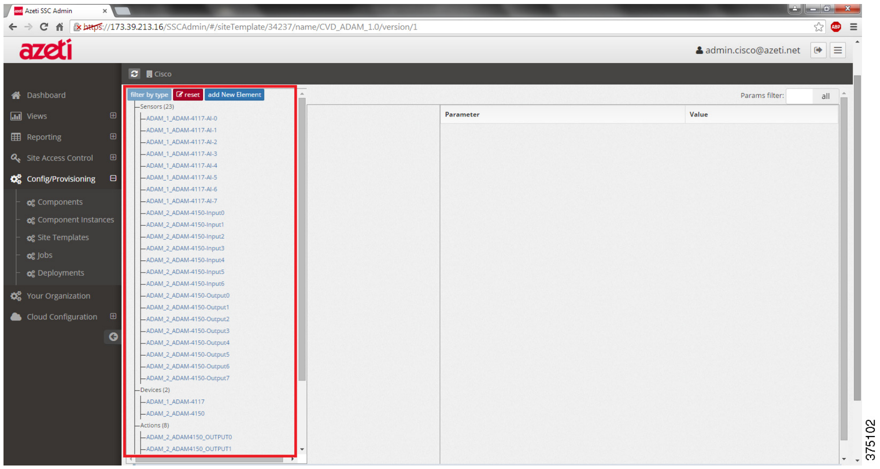
Name	Used?
ADAM-4117-AI-0	✓
ADAM-4117-AI-1	✓
ADAM-4117-AI-2	✓
ADAM-4117-AI-3	✓
ADAM-4117-AI-4	✓
ADAM-4117-AI-5	✓
ADAM-4117-AI-6	✓
ADAM-4117-AI-7	✓

no item selected

Ok

Step 13 After selecting **OK**, the list of sensors, devices and actions can be seen on the left side column, as shown in Figure 3-14.

Figure 3-14 List of Sensors, Devices, Actions, and ACLs



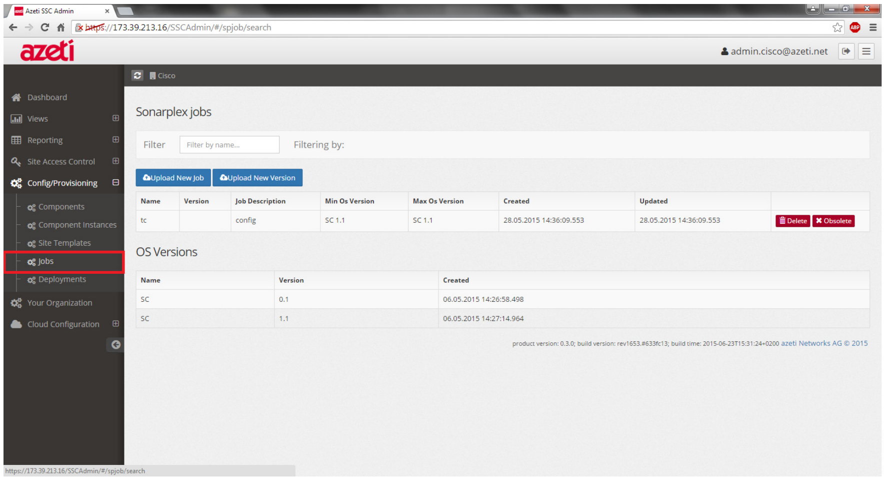
Sensors (23)
- ADAM_1_ADAM-4117-AI-0
- ADAM_1_ADAM-4117-AI-1
- ADAM_1_ADAM-4117-AI-2
- ADAM_1_ADAM-4117-AI-3
- ADAM_1_ADAM-4117-AI-4
- ADAM_1_ADAM-4117-AI-5
- ADAM_1_ADAM-4117-AI-6
- ADAM_1_ADAM-4117-AI-7
- ADAM_2_ADAM-4150-Input0
- ADAM_2_ADAM-4150-Input1
- ADAM_2_ADAM-4150-Input2
- ADAM_2_ADAM-4150-Input3
- ADAM_2_ADAM-4150-Input4
- ADAM_2_ADAM-4150-Input5
- ADAM_2_ADAM-4150-Input6
- ADAM_2_ADAM-4150-Output0
- ADAM_2_ADAM-4150-Output1
- ADAM_2_ADAM-4150-Output2
- ADAM_2_ADAM-4150-Output3
- ADAM_2_ADAM-4150-Output4
- ADAM_2_ADAM-4150-Output5
- ADAM_2_ADAM-4150-Output6
- ADAM_2_ADAM-4150-Output7

Devices (2)
- ADAM_1_ADAM-4117
- ADAM_2_ADAM-4150

Actions (8)
- ADAM_2_ADAM4150_OUTPUT0
- ADAM_2_ADAM4150_OUTPUT1

Step 14 Create a job by using the new site template, as shown in Figure 3-15.

Figure 3-15 Jobs Creation or Editing



Sonarplex jobs

Name	Version	Job Description	Min Os Version	Max Os Version	Created	Updated	
tc		config	SC 1.1	SC 1.1	28.05.2015 14:36:09.553	28.05.2015 14:36:09.553	Delete Obsolete

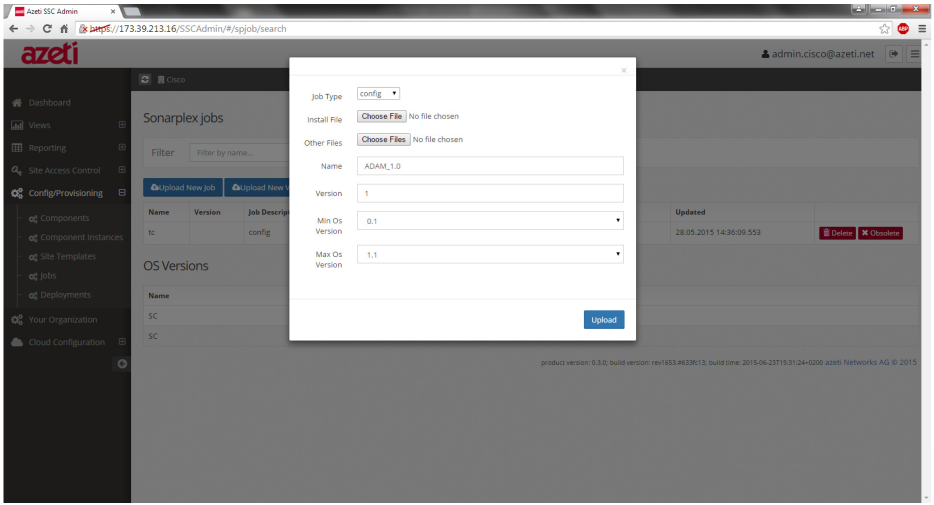
OS Versions

Name	Version	Created
SC	0.1	06.05.2015 14:26:58.498
SC	1.1	06.05.2015 14:27:14.964

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 15 Select the **Upload New Job** option and give an appropriate name and version, as shown in Figure 3-16.

Figure 3-16 Upload a New Job



Job Type: config

Install File: No file chosen

Other Files: No file chosen

Name: ADAM_1.0

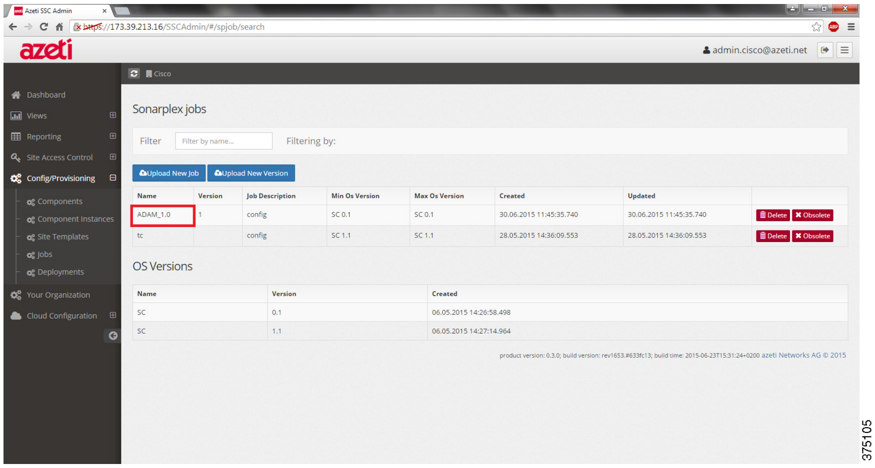
Version: 1

Min Os Version: 0.1

Max Os Version: 1.1

Step 16 The new job created can be seen in the Jobs list, as shown in Figure 3-17.

Figure 3-17 List of New Jobs



Sonarplex jobs

Filter: Filter by name... Filtering by:

Name	Version	Job Description	Min Os Version	Max Os Version	Created	Updated	
ADAM_1.0	1	config	SC 0.1	SC 0.1	30.06.2015 11:45:35.740	30.06.2015 11:45:35.740	Delete Obsolete
tc		config	SC 1.1	SC 1.1	28.05.2015 14:36:09.553	28.05.2015 14:36:09.553	Delete Obsolete

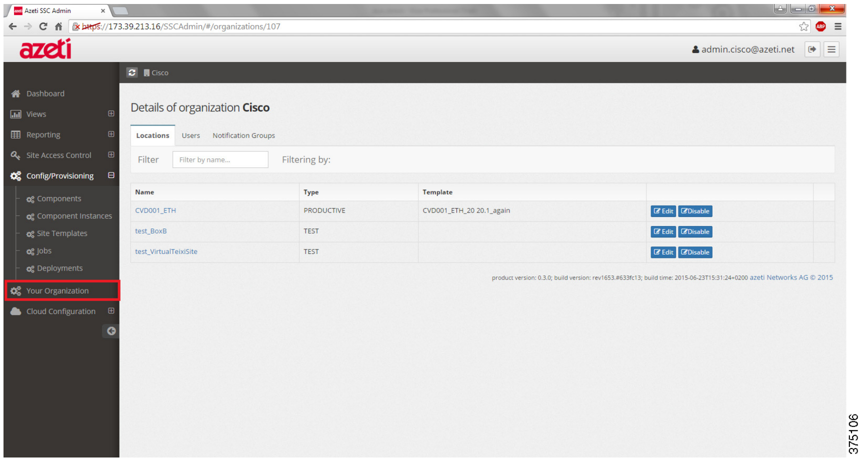
OS Versions

Name	Version	Created
SC	0.1	06.05.2015 14:26:58.498
SC	1.1	06.05.2015 14:27:14.964

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 17 Select the Your Organization option, as shown in Figure 3-18.

Figure 3-18 Editing the Destination Location



Details of organization **Cisco**

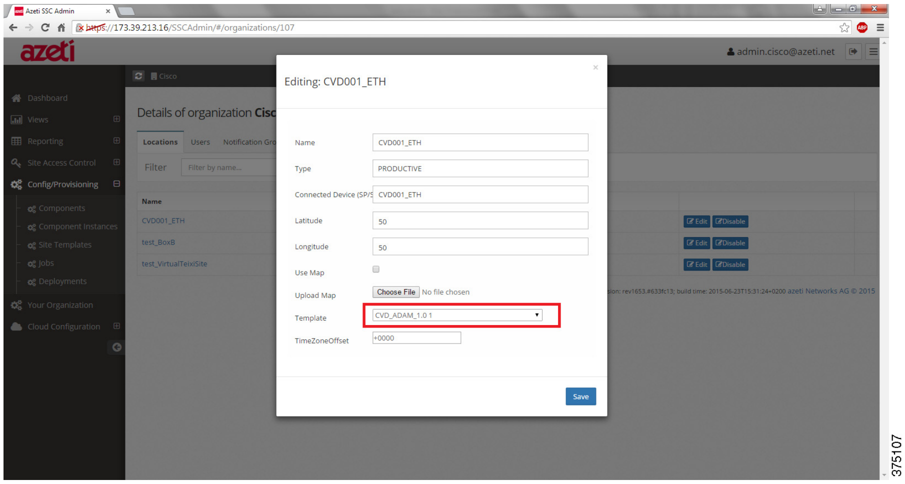
Filter: Filter by name... Filtering by:

Name	Type	Template	
CVD001_ETH	PRODUCTIVE	CVD001_ETH_20 20.1_again	Edit Disable
test_BoxB	TEST		Edit Disable
test_VirtualTeixiSite	TEST		Edit Disable

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 18 Select the **Edit** option for the desired location and then select the required template and save it, as shown in Figure 3-19.

Figure 3-19 ***Select the Destination***



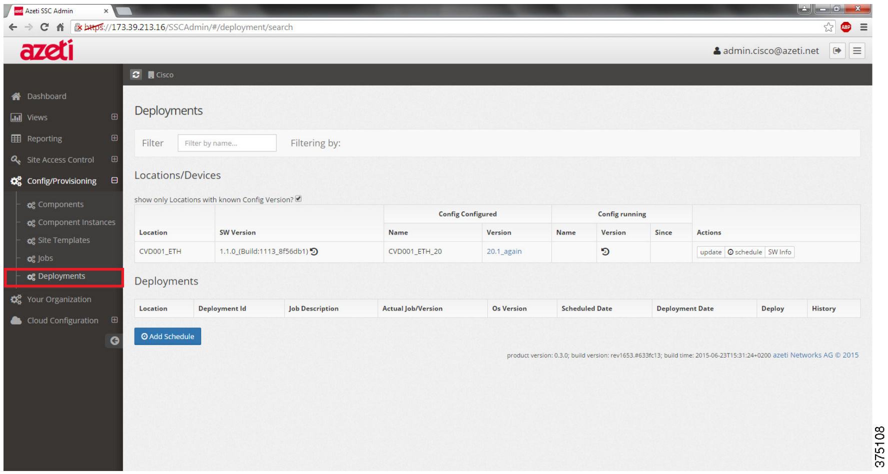
Editing: CVD001_ETH

Name	CVD001_ETH
Type	PRODUCTIVE
Connected Device (SP/S	CVD001_ETH
Latitude	50
Longitude	50
Use Map	□
Upload Map	Choose File No file chosen
Template	CVD_ADAM_1.0 1
TimeZoneOffset	+0000

Save

Step 19 Provision the services on the site controller, as shown in Figure 3-20.

Figure 3-20 ***Deployment of Job***



Deployments

Locations/Devices

show only Locations with known Config Version? ☑

		Config Configured		Config running			
Location	SW Version	Name	Version	Name	Version	Since	Actions
CVD001_ETH	1.1.0_(Build:1113_8f56db1)	CVD001_ETH_20	20.1_again				update schedule SW Info

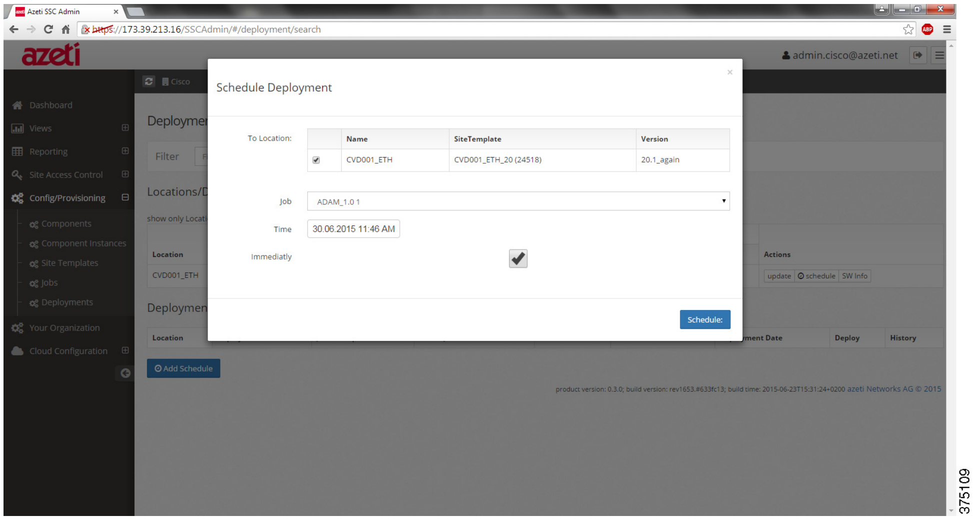
Deployments

Location	Deployment Id	Job Description	Actual Job/Version	Os Version	Scheduled Date	Deployment Date	Deploy	History

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 20 Select the **Add Schedule** option to decide the date and time to schedule the deployment, as shown in Figure 3-21.

Figure 3-21 Scheduling the Deployment



Schedule Deployment

To Location:

	Name	SiteTemplate	Version
☑	CVD001_ETH	CVD001_ETH_20 (24518)	20.1_again

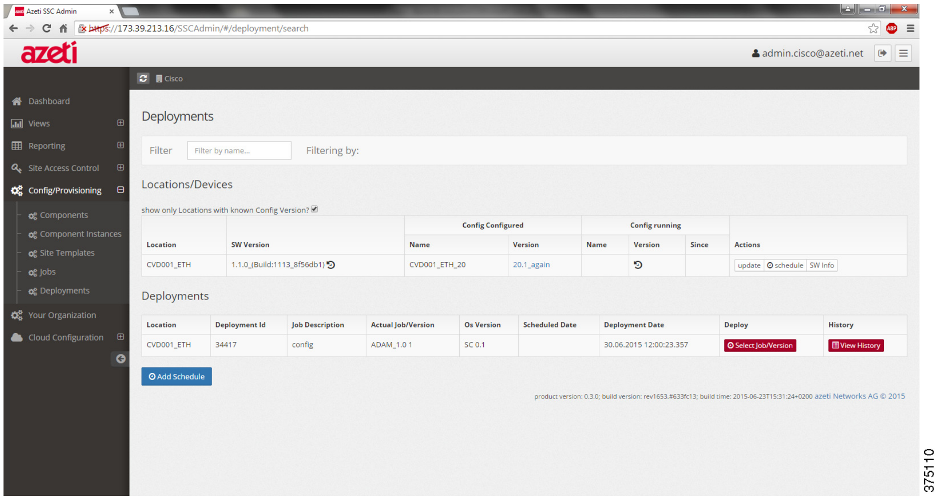
Job: ADAM_1.0 1

Time: 30.06.2015 11:46 AM

Immediatly: ☑

Step 21 The new list of deployments is available, with their scheduled date and time, as shown in Figure 3-22.

Figure 3-22 List of Scheduled Deployment



Deployments

Filter: Filter by name... Filtering by:

Locations/Devices

show only Locations with known Config Version? ☑

		Config Configured		Config running			
Location	SW Version	Name	Version	Name	Version	Since	Actions
CVD001_ETH	1.1.0_(Build:1113_8f56db1)	CVD001_ETH_20	20.1_again				update / schedule / SW Info

Deployments

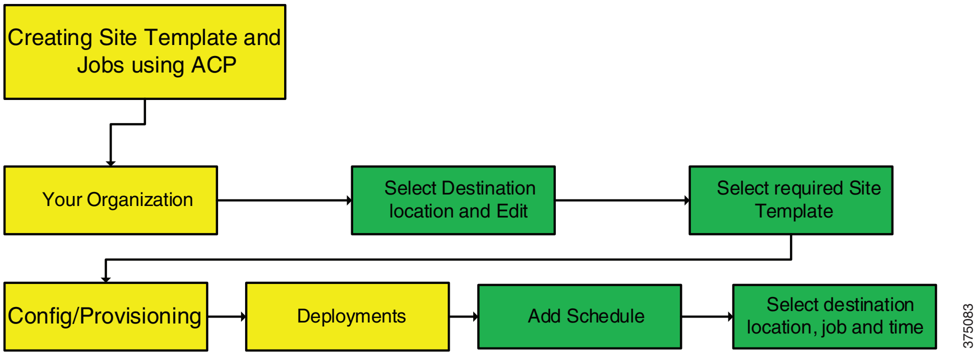
Location	Deployment Id	Job Description	Actual Job/Version	Os Version	Scheduled Date	Deployment Date	Deploy	History
CVD001_ETH	34417	config	ADAM_1.0 1	SC 0.1		30.06.2015 12:00:23.357	Select Job/Version	View History

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Adding a New Site and Applying a Site Template

This section explains the procedure to add a site controller on ACP. The flowchart is shown in Figure 3-23.

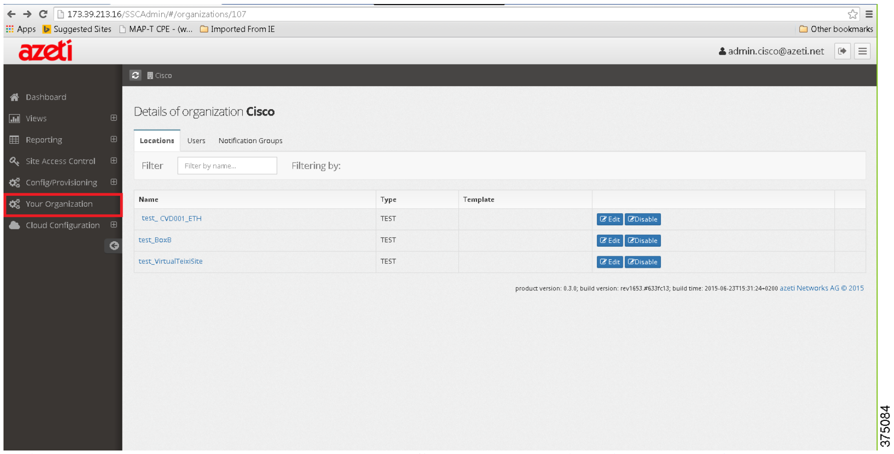
Figure 3-23 Flow Chart for Adding Site Controller on ACP


Creating Site Template and Jobs using ACP
Your Organization
Select Destination location and Edit
Select required Site Template
Config/Provisioning
Deployments
Add Schedule
Select destination location, job and time
375083

To add a site controller on ACP, complete the following steps:

Step 1 See the newly added site controller and select **Your Organization,** as shown in Figure 3-24.

Figure 3-24 Details of Organization



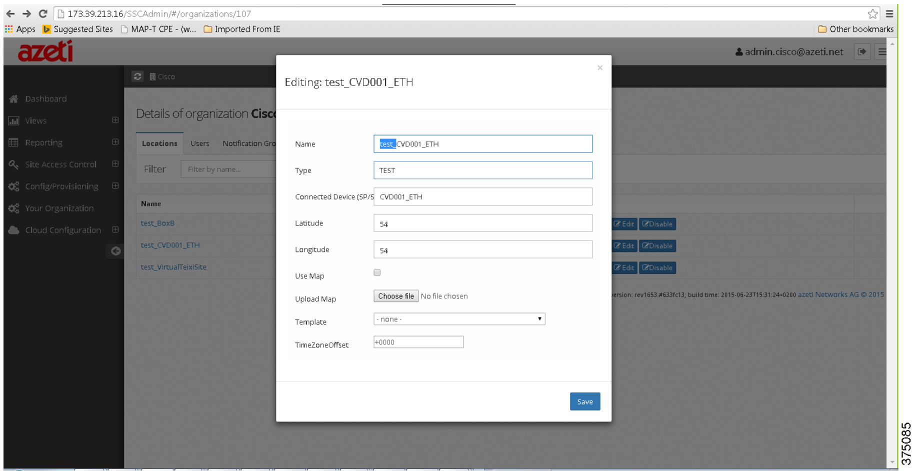
Details of organization **Cisco**

Name	Type	Template	
test_ CVD001_ETH	TEST		Edit Disable
test_BoxB	TEST		Edit Disable
test_VirtualTeixiSite	TEST		Edit Disable

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 2 Give a new name to see test as a prefix, as shown in Figure 3-25.

Figure 3-25 Editing Organization

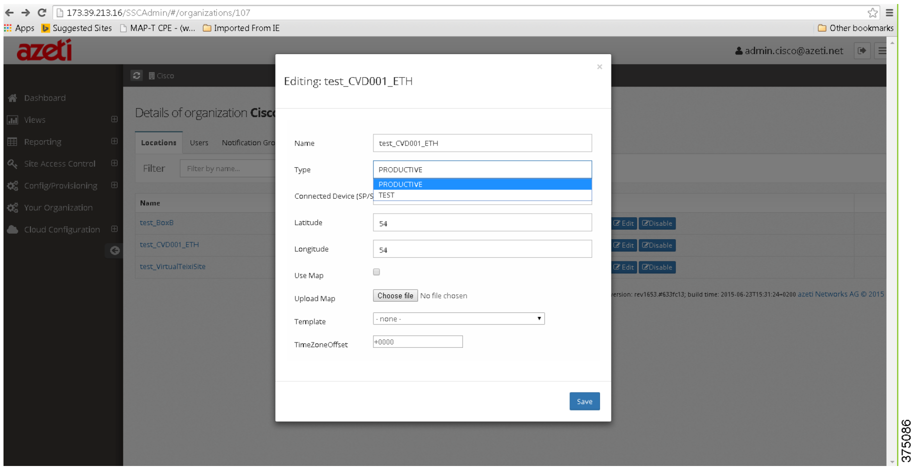


Editing: test_CVD001_ETH

Name	test_CVD001_ETH
Type	TEST
Connected Device (SP/S	CVD001_ETH
Latitude	54
Longitude	54
Use Map	□
Upload Map	No file chosen
Template	- none -
TimeZoneOffset	+0000

Step 3 Change the type to **Productive**, as shown in Figure 3-26.

Figure 3-26 Type Selection

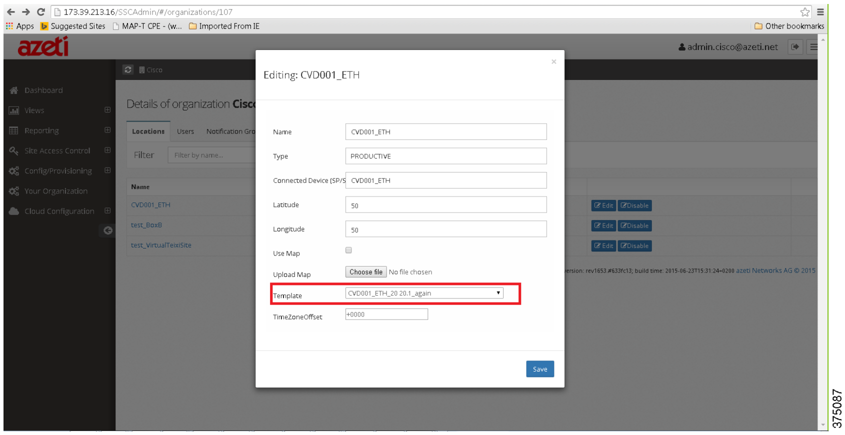


Editing: test_CVD001_ETH

Name: test_CVD001_ETH
Type: PRODUCTIVE (PRODUCTIVE / TEST)
Connected Device (SP/S
Latitude: 54
Longitude: 54
Use Map: □
Upload Map: Choose file No file chosen
Template: - none -
TimeZoneOffset: +0000
Save

Step 4 Change the template to **CVD001_ETH_20 20.1_again**, as shown in Figure 3-27.

Figure 3-27 Template Selection

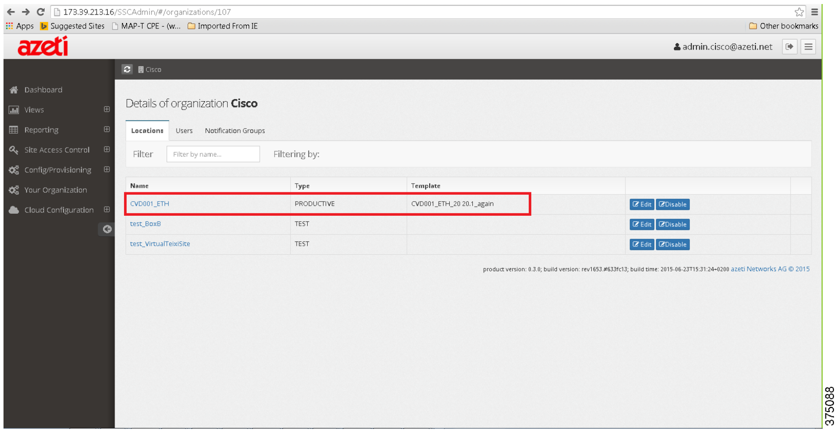


Editing: CVD001_ETH

Name: CVD001_ETH
Type: PRODUCTIVE
Connected Device (SP/S: CVD001_ETH
Latitude: 50
Longitude: 50
Use Map: □
Upload Map: Choose file No file chosen
Template: CVD001_ETH_20 20.1_again
TimeZoneOffset: +0000
Save

Step 5 The new details about the organization are visible, as shown in Figure 3-28.

Figure 3-28 Edited Details of Organization



Details of organization **Cisco**

Name	Type	Template	
CVD001_ETH	PRODUCTIVE	CVD001_ETH_20 20.1_again	Edit Disable
test_BoxB	TEST		Edit Disable
test_VirtualTeixiSite	TEST		Edit Disable

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Site Template Customization

This section explains the work flow diagram and configuration details of three use-cases: Door Access, Fuel Theft and Picture Snapshot.

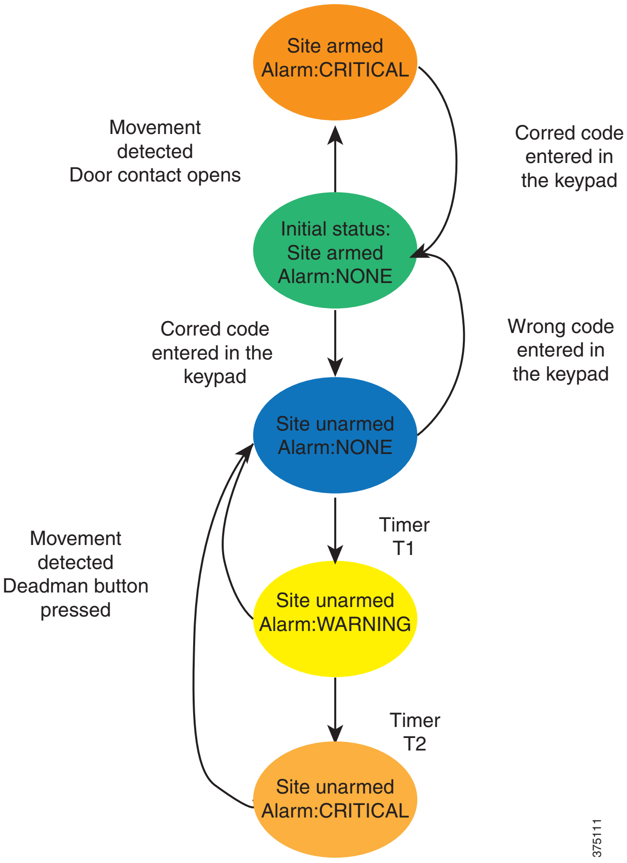
Use-Case: Door Access

This is an example of the access management use case. It describes the Door Access Control (DAC) solution using the site controller. The DAC is created as a solution to control the access to a facility. It covers flows and configuration details of each service involved in the door access use case.

Door Access Work Flow Diagram

This section explains the various steps of the work flow for the use case Door Access Control. Figure 3-29 shows alarm states are triggered based on different site states.

Figure 3-29 Door Access Work Flow



Step 1 This is the initial (resting) status of the system. The site is armed and there is no alarm. The door lock is closed. At this point, any movement detected in the facility will cause an immediate alarm.

Step 2 After the correct code is entered, the system signals with a short beep and a green light in the keypad. The door lock is opened for 5 seconds (signaled by switching on the white LED), so that the operator can enter the facility. After that time, the light of the keypad returns to red and the door locks again (signaled by the white led switching off).

Step 3 In this status the system is unarmed. The system will continue in this status while it detects movement. If no movement is detected during the time established for the timer T1, the system will raise an alarm. (In this console we simulate movement with the switch labeled **movement**; normally you connect a PIR to a digital input.)

Step 4 In this status, the system has an alarm because no movement was detected during the T1 timer. A siren (in this case a small buzzer) signals the operator that he needs to indicate that he is alive by pressing the dead man button.

Step 5 If there is no signal before the timer T2 finishes, the system will start the critical alarm. To restore the system to the initial status, the site must be armed and unarmed using the keypad, or the NOC must send a signal to switch off the lights.

Step 6 The brute force attack is signaled with an orange LED. When the system receives a number of wrong codes, it will block the keypad for some time and set the LED to orange to indicate that it is disabled.

Note Not all keypads are configured to use this color code. If you have any doubt, review your installation manual for the keypad in order to enable the orange LED.

Configuration Detail

This section provides configuration details for access of the remote site, including required services and their corresponding action and ACL rules. The complete list of services, rules, and actions for all use cases are detailed in Appendix.

Table 3-1 shows the configuration details for door access control.

Table 3-1 Door Access Control Configuration Details

Service	Device	Purpose
Access_Control_Door1	VirtualSensorProvider	Validate PIN entered on keypad. It can be either granted or denied, or idle or brute force attack.
ADAM-4150-LED BLUE	ADAM-4150	Indicates Armed (ON) or unarmed (OFF) on BLUE light.
BTS_arm_state	VirtualSensorProvider	Indicates ARMED or UNARMED in text.
Door1_Status	ADAM-4150	Indicates status of door open or closed.
WTSC_Keypad_Door_PIN_1	M2M_WTSC_Door_Controller	Entering PIN.
WTSC_Keypad_Relay	M2M_WTSC_Door_Controller	Door lock controlled using this relay.

Table 3-2 shows a list of actions to be performed on the services.

Table 3-2 List of Actions

Action	Purpose
ClearAlertsAndLights	Fire rule to clear alerts and lights.
SiteArming	Changing ARM state.
Switch_ARM_LED_0	Switch ON/OFF BLUE light.
Switch_M2M_WTSC_default	RESET keypad.
Switch_M2M_WTSC_DO_3_Beep_short	Make beep short.
Switch_M2M_WTSC_Relay	Make relay ON /OFF.

Table 3-3 shows a list of ACLs.

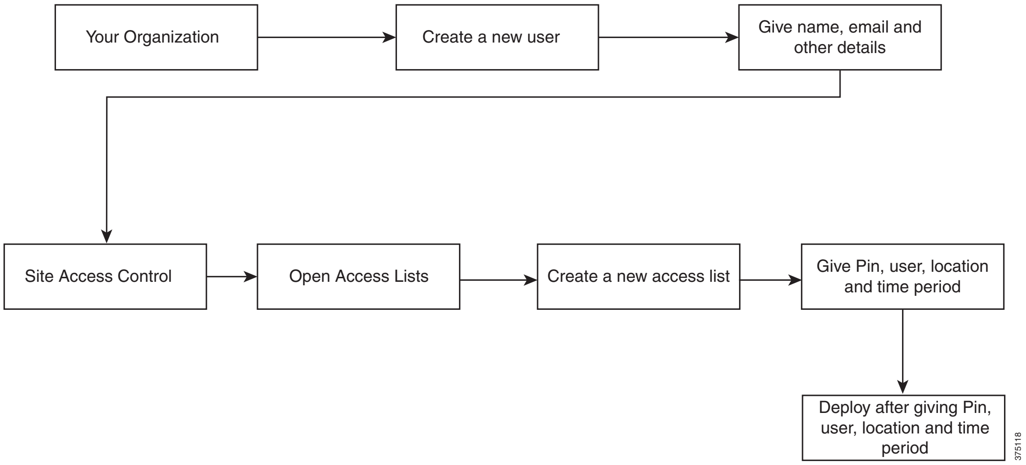
Table 3-3 List of ACLs

ACL Rule	Description
ArmState	Change the arm-state based on the result of Access_Control_Door1 sensor.
door1control	Fire actions to change LED colors based on Access_Control_Door1.

Providing User Access to Site by Using ACP

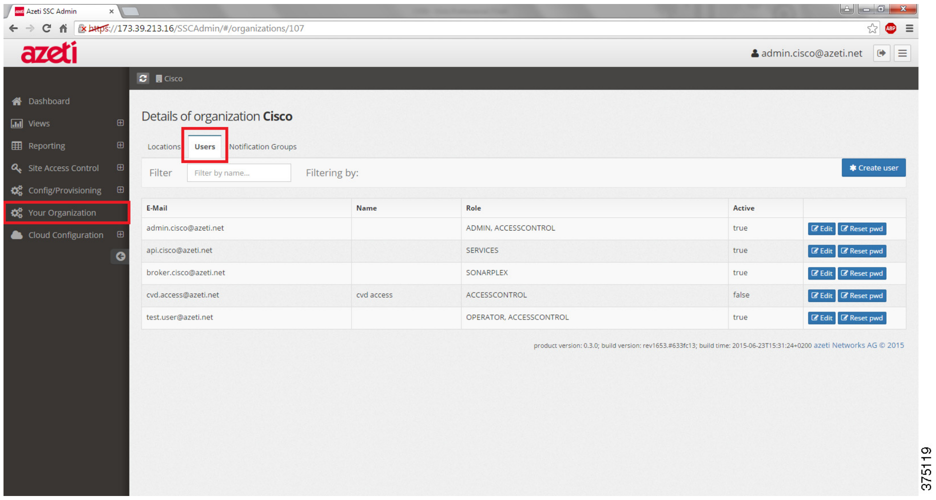
This section provides the flow (shown in Figure 3-30) to configure user access to the site by using ACP.

Figure 3-30 User Access to Site Using ACP


Your Organization
Create a new user
Give name, email and other details
Site Access Control
Open Access Lists
Create a new access list
Give Pin, user, location and time period
Deploy after giving Pin, user, location and time period
375118

Step 1 Select **Users** from **Your Organization** to create new user or to use an existing one, as shown in Figure 3-31.

Figure 3-31 Users under the Organization



Azeti SSC Admin

~~https~~://173.39.213.16/SSCAdmin/#/organizations/107

admin.cisco@azeti.net

Cisco

Details of organization **Cisco**

Locations | Users | Notification Groups

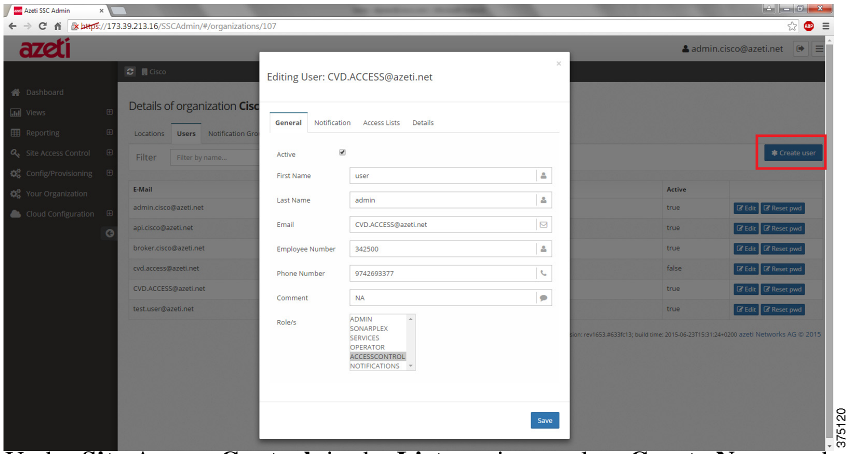
Filter: Filter by name... Filtering by:

E-Mail	Name	Role	Active	
admin.cisco@azeti.net		ADMIN, ACCESSCONTROL	true	Edit Reset pwd
api.cisco@azeti.net		SERVICES	true	Edit Reset pwd
broker.cisco@azeti.net		SONARPLEX	true	Edit Reset pwd
cvd.access@azeti.net	cvd access	ACCESSCONTROL	false	Edit Reset pwd
test.user@azeti.net		OPERATOR, ACCESSCONTROL	true	Edit Reset pwd

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 2 shows the creation of a new user by selecting **Create User** and **ACCESSCONTROL** as the role.

Figure 3-32 Create a New User



Editing User: CVD.ACCESS@azeti.net

General | Notification | Access Lists | Details

Active ☑

First Name: user

Last Name: admin

Email: CVD.ACCESS@azeti.net

Employee Number: 342500

Phone Number: 9742693377

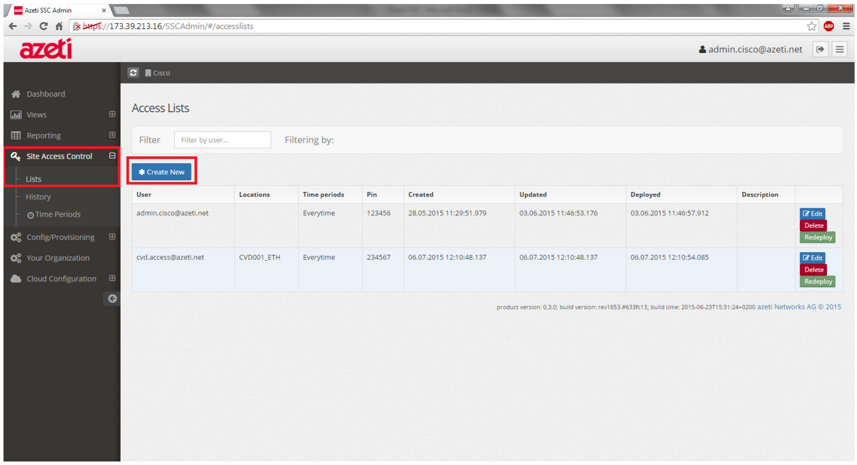
Comment: NA

Role/s: ADMIN, SONARPLEX, SERVICES, OPERATOR, ACCESSCONTROL (selected), NOTIFICATIONS

Save

Step 3 Under **Site Access Control**, in the **Lists** options, select **Create New**, as shown in Figure 3-33.

Figure 3-33 Existing Access Lists



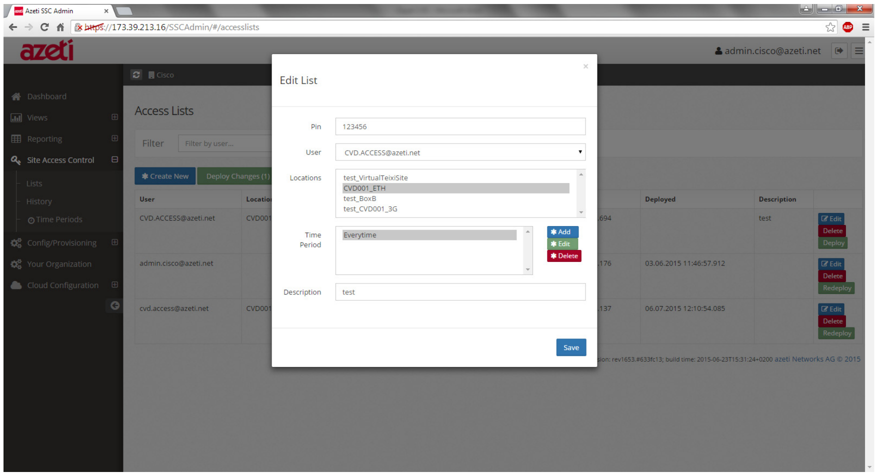
Access Lists

User	Locations	Time periods	Pin	Created	Updated	Deployed	Description	
admin.cisco@azeti.net		Everytime	123456	28.05.2015 11:29:51.979	03.06.2015 11:46:53.176	03.06.2015 11:46:57.912		Edit Delete Redeploy
cvd.access@azeti.net	CVD001_ETH	Everytime	234567	06.07.2015 12:10:48.137	06.07.2015 12:10:48.137	06.07.2015 12:10:54.085		Edit Delete Redeploy

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 4 Give the required PIN, user, location, and time period for the deployment, as shown in Figure 3-34.

Figure 3-34 Editing the Parameters for the Access List



Edit List

Pin: 123456

User: CVD.ACCESS@azeti.net

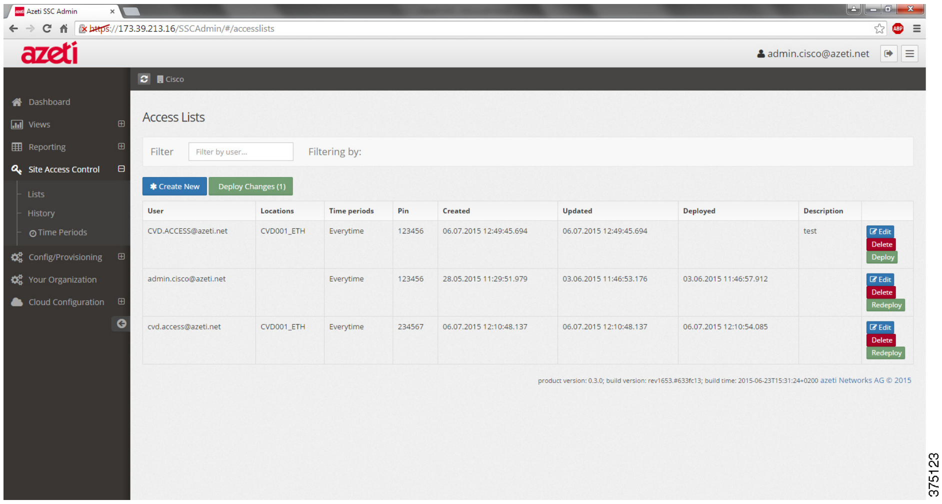
Locations:
test_VirtualTeixiSite
CVD001_ETH
test_BoxB
test_CVD001_3G

Time Period: Everytime

Description: test

Step 5 The new user can be seen in the list, as shown in Figure 3-35.

Figure 3-35 Deploy the Changes



Access Lists

Filter | Filter by user... | Filtering by:

Create New | Deploy Changes (1)

User	Locations	Time periods	Pin	Created	Updated	Deployed	Description	
CVD.ACCESS@azeti.net	CVD001_ETH	Everytime	123456	06.07.2015 12:49:45.694	06.07.2015 12:49:45.694		test	Edit Delete Deploy
admin.cisco@azeti.net		Everytime	123456	28.05.2015 11:29:51.979	03.06.2015 11:46:53.176	03.06.2015 11:46:57.912		Edit Delete Redeploy
cvd.access@azeti.net	CVD001_ETH	Everytime	234567	06.07.2015 12:10:48.137	06.07.2015 12:10:48.137	06.07.2015 12:10:54.085		Edit Delete Redeploy

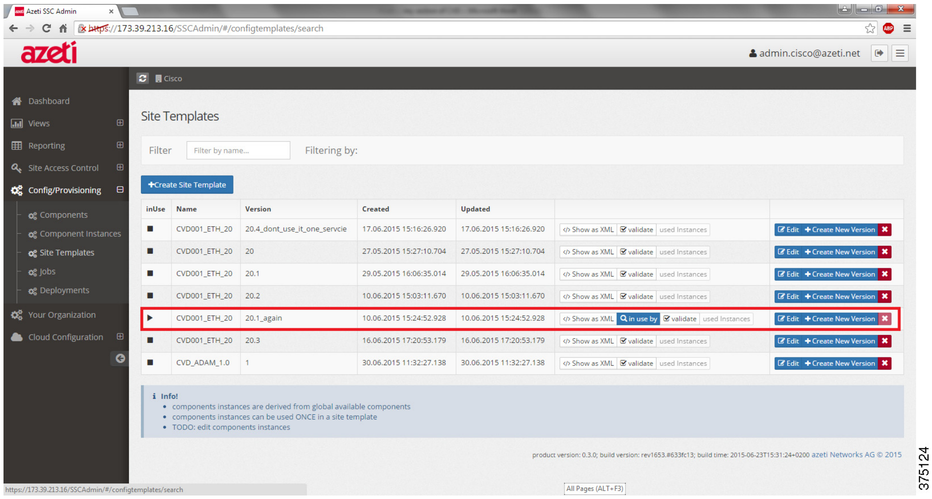
product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Editing Timer T2 Parameter for Door Access

A standard site template is available in ACP. This example shows how to change the T2 parameter of door access.

Step 1 Select the **Edit** option for the required site template to edit its parameters, as shown in Figure 3-36.

Figure 3-36 Selection of Required Site Template for Editing



Site Templates

Filter | Filter by name... | Filtering by:

Create Site Template

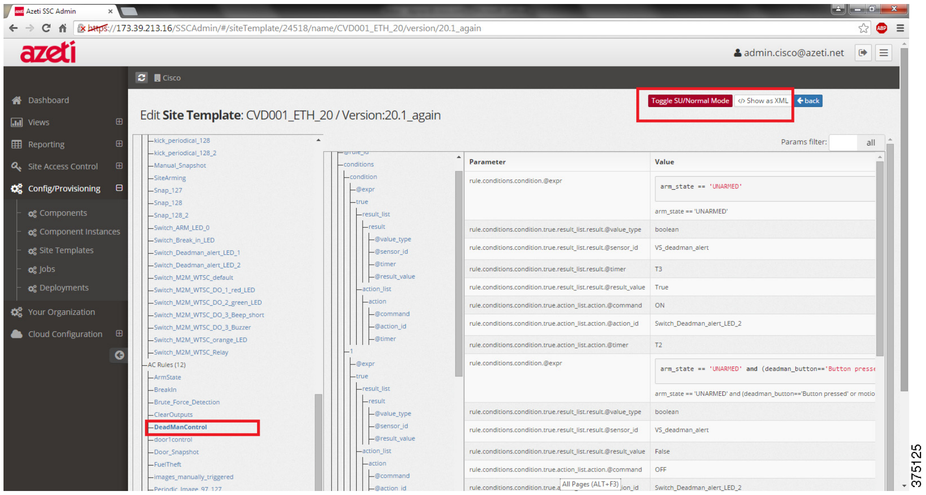
inUse	Name	Version	Created	Updated		
■	CVD001_ETH_20	20.4_dont_use_it_one_servcie	17.06.2015 15:16:26.920	17.06.2015 15:16:26.920	Show as XML, validate, used Instances	Edit, Create New Version, ✖
■	CVD001_ETH_20	20	27.05.2015 15:27:10.704	27.05.2015 15:27:10.704	Show as XML, validate, used Instances	Edit, Create New Version, ✖
■	CVD001_ETH_20	20.1	29.05.2015 16:06:35.014	29.05.2015 16:06:35.014	Show as XML, validate, used Instances	Edit, Create New Version, ✖
■	CVD001_ETH_20	20.2	10.06.2015 15:03:11.670	10.06.2015 15:03:11.670	Show as XML, validate, used Instances	Edit, Create New Version, ✖
▶	CVD001_ETH_20	20.1_again	10.06.2015 15:24:52.928	10.06.2015 15:24:52.928	Show as XML, in use by, validate, used Instances	Edit, Create New Version, ✖
■	CVD001_ETH_20	20.3	16.06.2015 17:20:53.179	16.06.2015 17:20:53.179	Show as XML, validate, used Instances	Edit, Create New Version, ✖
■	CVD_ADAM_1.0	1	30.06.2015 11:32:27.138	30.06.2015 11:32:27.138	Show as XML, validate, used Instances	Edit, Create New Version, ✖

Info!
- components instances are derived from global available components
- components instances can be used ONCE in a site template
- TODO: edit components instances

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Step 2 Select the **Toggle SU/normal Mode** option for the action **DeadManControl**, as shown in Figure 3-37.

Figure 3-37 Selection of Access List to Be Edited

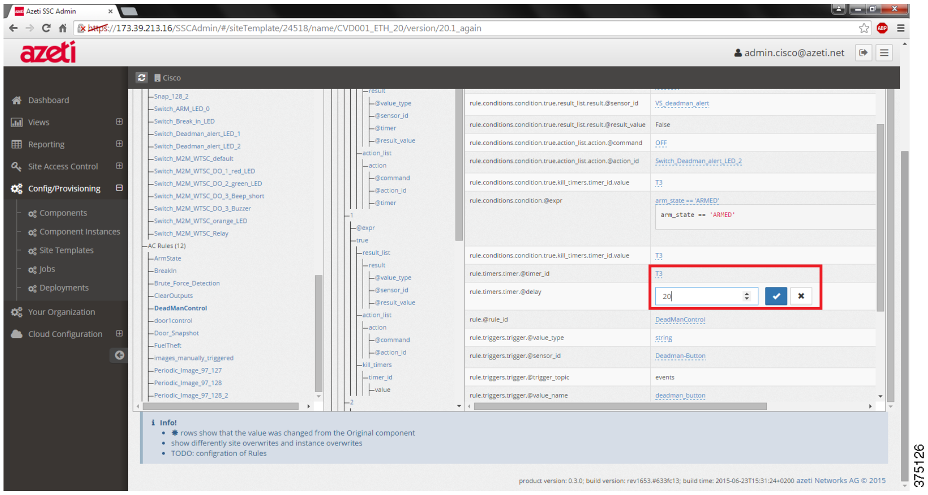


Edit **Site Template**: CVD001_ETH_20 / Version:20.1_again

Parameter	Value
rule.conditions.condition.@expr	`arm_state == 'UNARMED'` arm_state == 'UNARMED'
rule.conditions.condition.true.result_list.result.@value_type	boolean
rule.conditions.condition.true.result_list.result.@sensor_id	VS_deadman_alert
rule.conditions.condition.true.result_list.result.@timer	T3
rule.conditions.condition.true.result_list.result.@result_value	True
rule.conditions.condition.true.action_list.action.@command	ON
rule.conditions.condition.true.action_list.action.@action_id	Switch_Deadman_alert_LED_2
rule.conditions.condition.true.action_list.action.@timer	T2
rule.conditions.condition.@expr	`arm_state == 'UNARMED' and (deadman_button=='Button presse` arm_state == 'UNARMED' and (deadman_button=='Button pressed' or motio
rule.conditions.condition.true.result_list.result.@value_type	boolean
rule.conditions.condition.true.result_list.result.@sensor_id	VS_deadman_alert
rule.conditions.condition.true.result_list.result.@result_value	False
rule.conditions.condition.true.action_list.action.@command	OFF
rule.conditions.condition.true.a ion_id	Switch_Deadman_alert_LED_2

Step 3 The T2 Timer Value can be edited, as shown in Figure 3-38.

Figure 3-38 Changing the T2 Value



Parameter	Value
rule.conditions.condition.true.result_list.result.@sensor_id	VS_deadman_alert
rule.conditions.condition.true.result_list.result.@result_value	False
rule.conditions.condition.true.action_list.action.@command	OFF
rule.conditions.condition.true.action_list.action.@action_id	Switch_Deadman_alert_LED_2
rule.conditions.condition.true.kill_timers.timer_id.value	T3
rule.conditions.condition.@expr	arm_state == 'ARMED' `arm_state == 'ARMED'`
rule.conditions.condition.true.kill_timers.timer_id.value	T3
rule.timers.timer.@timer_id	T3
rule.timers.timer.@delay	20
rule.@rule_id	DeadManControl
rule.triggers.trigger.@value_type	string
rule.triggers.trigger.@sensor_id	Deadman-Button
rule.triggers.trigger.@trigger_topic	events
rule.triggers.trigger.@value_name	deadman_button

ℹ Info!

- ✱ rows show that the value was changed from the Original component
- show differently site overwrites and instance overwrites
- TODO: configration of Rules

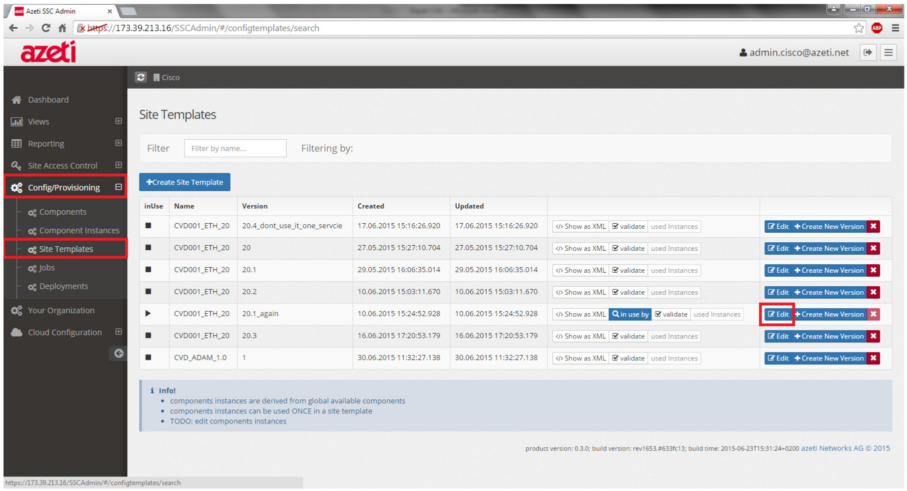
product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

Configuring Threshold for Service Comet_Humidity_Status

The standard site template is available in ACP. This example shows how to configure various threshold levels, such as, CRITICAL, WARNING, and OK, for the service **Comet_Humidity_Status**. This use case is an example of environmental monitoring (operational continuity).

Step 1 Select the **Edit** option, for the site template that contains the required sensor, in the **Config/Provisioning** main option, as shown in Figure 3-39.

Figure 3-39 Selection of Site Template to Change Threshold Values



Site Templates

inUse	Name	Version	Created	Updated		
■	CVD001_ETH_20	20.4_dont_use_it_one_servcie	17.06.2015 15:16:26.920	17.06.2015 15:16:26.920	Show as XML ☑ validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20	27.05.2015 15:27:10.704	27.05.2015 15:27:10.704	Show as XML ☑ validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20.1	29.05.2015 16:06:35.014	29.05.2015 16:06:35.014	Show as XML ☑ validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20.2	10.06.2015 15:03:11.670	10.06.2015 15:03:11.670	Show as XML ☑ validate used Instances	Edit + Create New Version ✖
▶	CVD001_ETH_20	20.1_again	10.06.2015 15:24:52.928	10.06.2015 15:24:52.928	Show as XML in use by ☑ validate used Instances	Edit + Create New Version ✖
■	CVD001_ETH_20	20.3	16.06.2015 17:20:53.179	16.06.2015 17:20:53.179	Show as XML ☑ validate used Instances	Edit + Create New Version ✖
■	CVD_ADAM_1.0	1	30.06.2015 11:32:27.138	30.06.2015 11:32:27.138	Show as XML ☑ validate used Instances	Edit + Create New Version ✖

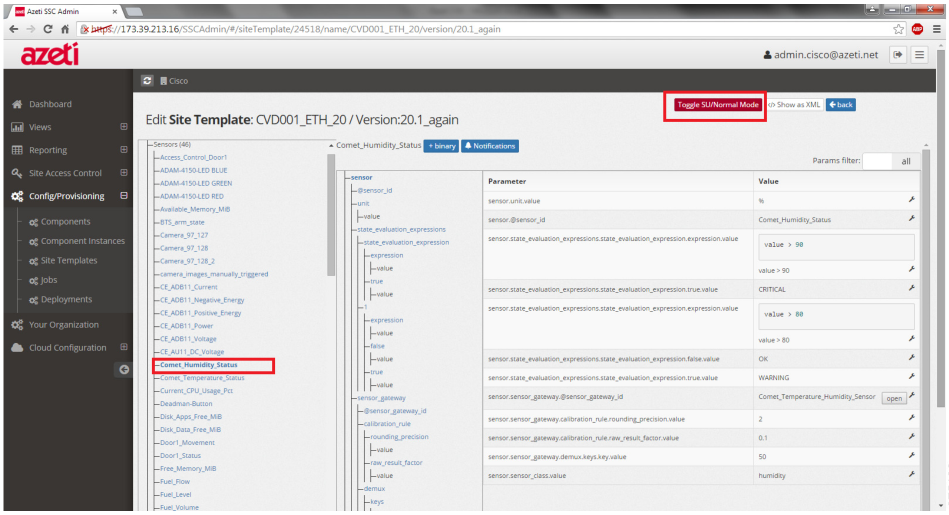
Info!
- components instances are derived from global available components
- components instances can be used ONCE in a site template
- TODO: edit components instances

product version: 0.3.0; build version: rev1653.#633fc13; build time: 2015-06-23T15:31:24+0200 azeti Networks AG © 2015

https://173.39.213.16/SSCAdmin/#/configtemplates/search

Step 2 Select the **Toggle SU/Normal** mode for the **Comet_Humidity_Status** sensor, as shown in Figure 3-40.

Figure 3-40 Section of Sensor to Be Edited

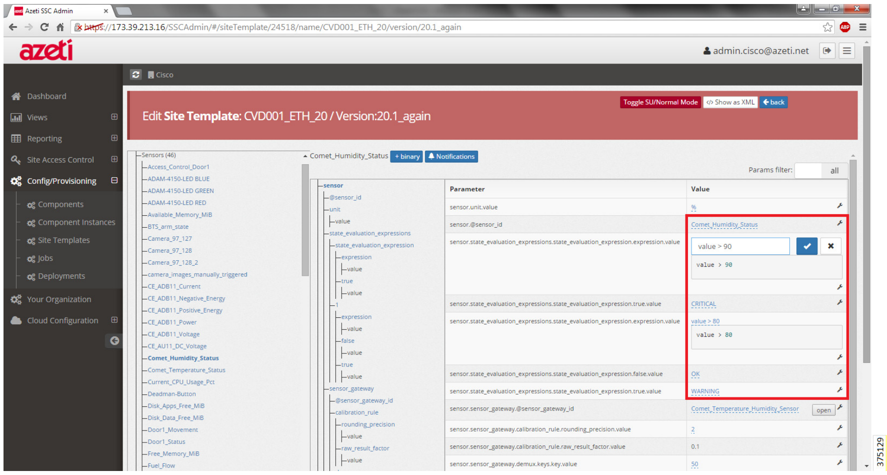


Edit **Site Template**: CVD001_ETH_20 / Version:20.1_again

Parameter	Value
sensor.unit.value	%
sensor.@sensor_id	Comet_Humidity_Status
sensor.state_evaluation_expressions.state_evaluation_expression.expression.value	value > 90 value > 90
sensor.state_evaluation_expressions.state_evaluation_expression.true.value	CRITICAL
sensor.state_evaluation_expressions.state_evaluation_expression.expression.value	value > 80 value > 80
sensor.state_evaluation_expressions.state_evaluation_expression.false.value	OK
sensor.state_evaluation_expressions.state_evaluation_expression.true.value	WARNING
sensor.sensor_gateway.@sensor_gateway_id	Comet_Temperature_Humidity_Sensor open
sensor.sensor_gateway.calibration_rule.rounding_precision.value	2
sensor.sensor_gateway.calibration_rule.raw_result_factor.value	0.1
sensor.sensor_gateway.demux.keys.key.value	50
sensor.sensor_class.value	humidity

Step 3 Select the **sensor.state_evaluation_expressions.state_evaluation_expression.expression.value** and the **sensor.state_evaluation_expressions.state_evaluation_expression.true.value** to set the threshold value and true/false states respectively, as shown in Figure 3-41.

Figure 3-41 Edit the Threshold Value for Parameters



Edit **Site Template:** CVD001_ETH_20 / Version:20.1_again

Parameter	Value
sensor.unit.value	%
sensor.@sensor_id	Comet_Humidity_Status
sensor.state_evaluation_expressions.state_evaluation_expression.expression.value	value > 90 value > 90
sensor.state_evaluation_expressions.state_evaluation_expression.true.value	CRITICAL
sensor.state_evaluation_expressions.state_evaluation_expression.expression.value	value > 80 value > 80
sensor.state_evaluation_expressions.state_evaluation_expression.false.value	OK
sensor.state_evaluation_expressions.state_evaluation_expression.true.value	WARNING
sensor.sensor_gateway.@sensor_gateway_id	Comet_Temperature_Humidity_Sensor
sensor.sensor_gateway.calibration_rule.rounding_precision.value	2
sensor.sensor_gateway.calibration_rule.raw_result_factor.value	0.1
sensor.sensor_gateway.demux.keys.key.value	50

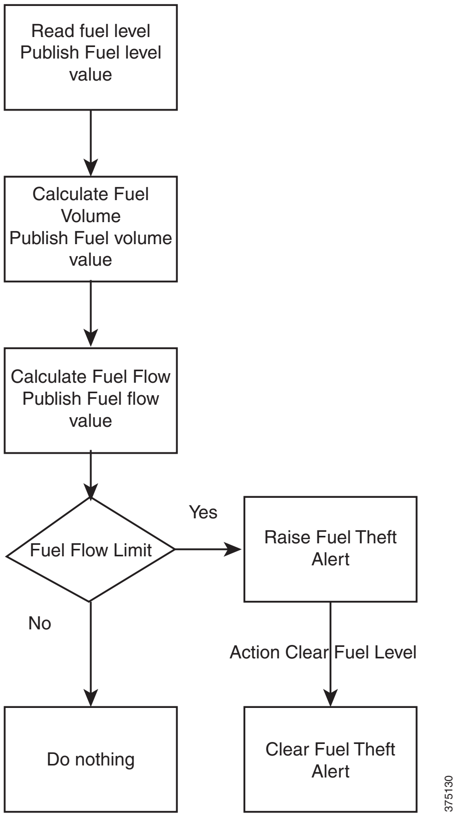
Use Case: Fuel Theft

This section describes the fuel theft module using the site controller. Fuel theft is created as a solution to control the fuel flow, and possible theft, in a facility. It covers the flow and configuration details of each service involved in the fuel theft use case.

Work Flow Diagram

Figure 3-42 is the flow diagram, which shows the different states of the sensors in the fuel solution.

Figure 3-42 Fuel Theft Work Flow Diagram



Configuration Detail

This section provides configuration detail of each services, action and ACL rules of fuel theft.

Table 3-4 shows the list of services and the corresponding devices.

Table 3-4 Configuration Details for Fuel Theft

Service	Device	Purpose
Fuel_Level	ADAM-4150	Read the fuel level with a pressure sensor.
Fuel_Volume	VirtualSensorProvider-VS_fill_quantity	Calculates the volume of the fuel based on level and the tank geometry.
Fuel_Flow	VirtualSensorProvider- VS_flow_rate	Calculates the flow rate based on changes on fuel volume.
FuelTheft_alarm	VirtualSensorProvider	Indicates if there has been an alarm (state CRITICAL) raised in Fuel_flow.

Table 3-5 shows the action to be performed on the services for fuel theft.

Table 3-5 List of Actions for Fuel Theft

Action	Purpose
FuelTheft_clear	Clear Fuel Theft alarm

Table 3-6 shows the ACL for Fuel Theft.

Table 3-6 ACL for Fuel Theft

ACL Rule	Description
FuelTheft	A CRITICAL fuel flow (over a certain value per minute), raises the alarm FuelTheft_alarm in the NOC.

Editing a Parameter for Fuel Theft Service

A standard site template available in ACP. To change a parameter of Fuel Theft service, in the **Site Template** option, select **Toggle SU/normal mode** and edit the parameter, as shown in Figure 3-43.

Figure 3-43 Editing Fuel Theft Parameter

Use Case: Picture Snapshot

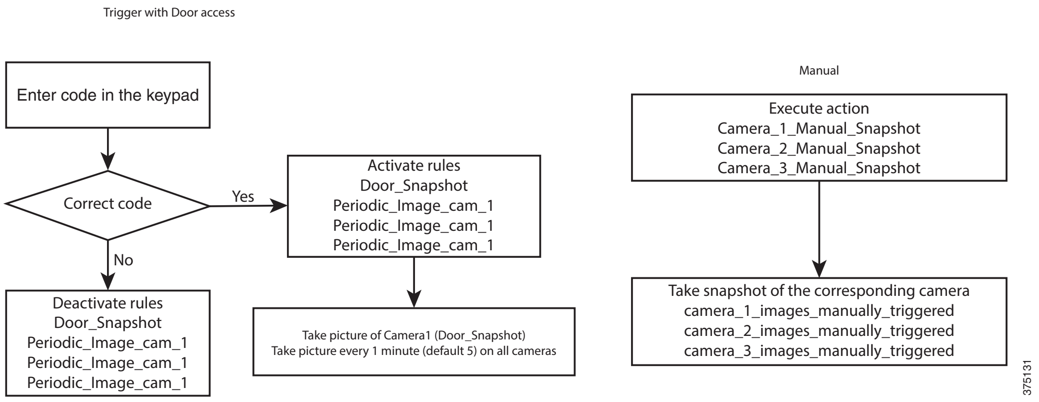
This is the example for Security Management usecase. It describes the picture snapshot configuration using the Site Controller. The uses information of the door access control solution to get image captures at certain points.

Note The sensors, actions and rules that are specific for the cameras configuration are shown. There is some dependence on the door control sensors and rules. We do not detail them here to avoid redundancies.

Flow Diagram

Figure 3-44 shows the flow diagram, which illustrates the different states of the picture snapshot use case. When the keypad access is granted, there is a picture snapshot after 3 seconds. Once the facility is unarmed, there is a picture snapshot every 5 minutes. Manual snapshots for every camera are possible.

Figure 3-44 Picture Snapshot Work Flow Diagram



Configuration Detail

This section provides configuration details for each service, action, and ACL rules of door access control. Table 3-7 shows the list of services and the corresponding devices.

Table 3-7 Configuration Details for Picture Snapshot

Service	Device	Purpose
Camera_1	VirtualSensorProvider	Show images for Camera 1 that are captured when the facility is unarmed, and after, at regular intervals.
Camera_2	VirtualSensorProvider	Show images for Camera 2 that are captured when the facility is unarmed and after it at regular intervals.
Camera_3	VirtualSensorProvider	Show images for Camera 3 that are captured when the facility is unarmed and after it at regular intervals.
camera_1_images_manually_triggered	VirtualSensorProvider	Show images for Camera 1 that are triggered manually.
camera_2_images_manually_triggered	VirtualSensorProvider	Show images for Camera 2 that are triggered manually.
camera_3_images_manually_triggered	VirtualSensorProvider	Show images for Camera 3 that are triggered manually.

Table 3-8 shows a list of action to be performed for Picture Snapshot.

Table 3-8 List of Actions to Be Performed for Picture Snapshot

Action	Purpose
Camera_1_Manual_Snapshot	Perform a manual snapshot in the camera_1.
Camera_2_Manual_Snapshot	Perform a manual snapshot in the camera_2.
Camera_3_Manual_Snapshot	Perform a manual snapshot in the camera_3.
Snap_1	Make an image shot in camera_1.
Snap_2	Make an image shot in camera_2.
Snap_3	Make an image shot in camera_3.

Table 3-9 shows a list of ACLs for Picture Snapshot.

Table 3-9 List of ACLs for Picture Snapshot

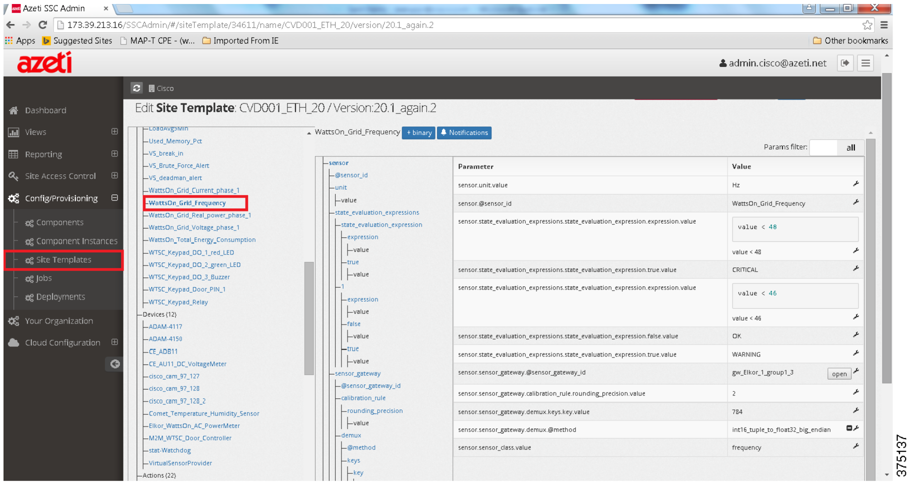
ACL Rule	Description
Door_Snapshot	Take a snapshot in case there is an access granted in the door (correct keypad code written).
Periodic_Image_cam_1	Whenever the facility is unarmed, it takes a picture and a schedule to take a picture every T minutes (default 5) until it is armed again.
Periodic_Image_cam_2	Whenever the facility is unarmed, it takes a picture and a schedule to take a picture every T minutes (default 5) until it is armed again.
Periodic_Image_cam_3	Whenever the facility is unarmed, it takes a picture and a schedule to take a picture every T minutes (default 5) until it is armed again.
camera_1_images_manually_triggered	Take a snapshot and publish the result to the corresponding sensor when the user executes the Camera_1_Manual_Snapshot action.
camera_2_images_manually_triggered	Take a snapshot and publish the result to the corresponding sensor when the user executes the Camera_2_Manual_Snapshot action.
camera_3_images_manually_triggered	Take a snapshot and publish the result to the corresponding sensor when the user executes the Camera_3_Manual_Snapshot action.

Use Case: HVAC Management and Power Monitoring

This section explains the use cases of HVAC Management and Power Monitoring.

Step 1 From **Sensors,** under the **Site Templates** option, select **WattsOn_Grid_Frequency** to view and edit its frequency parameters, as shown in Figure 3-45.

Figure 3-45 Editing Frequency Parameter



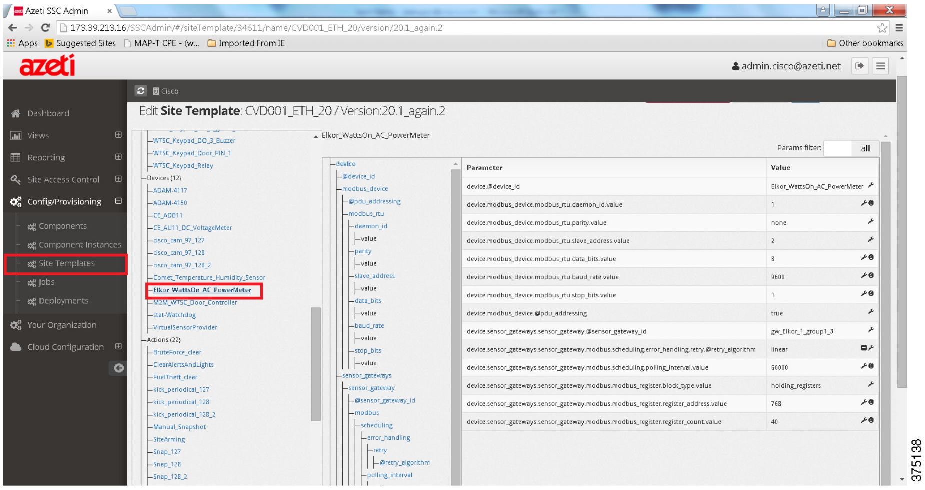
Edit **Site Template**: CVD001_ETH_20 / Version:20.1_again.2

WattsOn_Grid_Frequency

Parameter	Value
sensor.unit.value	Hz
sensor.@sensor_id	WattsOn_Grid_Frequency
sensor.state_evaluation_expressions.state_evaluation_expression.expression.value	value < 48
sensor.state_evaluation_expressions.state_evaluation_expression.true.value	CRITICAL
sensor.state_evaluation_expressions.state_evaluation_expression.expression.value	value < 46
sensor.state_evaluation_expressions.state_evaluation_expression.false.value	OK
sensor.state_evaluation_expressions.state_evaluation_expression.true.value	WARNING
sensor.sensor_gateway.@sensor_gateway_id	gw_Elkor_1_group1_3
sensor.sensor_gateway.calibration_rule.rounding_precision.value	2
sensor.sensor_gateway.demux.keys.key.value	784
sensor.sensor_gateway.demux.@method	int16_tuple_to_float32_big_endian
sensor.sensor_class.value	frequency

Step 2 From **Devices** under **Site Templates**, select **Elkor WattsOn Ac PowerMeter** to edit the power parameters, as shown in Figure 3-46.

Figure 3-46 Editing Power Parameters



Edit **Site Template**: CVD001_ETH_20 / Version:20.1_again.2

Elkor_WattsOn_AC_PowerMeter

Parameter	Value
device.@device_id	Elkor_WattsOn_AC_PowerMeter
device.modbus_device.modbus_rtu.daemon_id.value	1
device.modbus_device.modbus_rtu.parity.value	none
device.modbus_device.modbus_rtu.slave_address.value	2
device.modbus_device.modbus_rtu.data_bits.value	8
device.modbus_device.modbus_rtu.baud_rate.value	9600
device.modbus_device.modbus_rtu.stop_bits.value	1
device.modbus_device.@pdu_addressing	true
device.sensor_gateways.sensor_gateway.@sensor_gateway_id	gw_Elkor_1_group1_3
device.sensor_gateways.sensor_gateway.modbus.scheduling.error_handling.retry.@retry_algorithm	linear
device.sensor_gateways.sensor_gateway.modbus.scheduling.polling_interval.value	60000
device.sensor_gateways.sensor_gateway.modbus.modbus_register.block_type.value	holding_registers
device.sensor_gateways.sensor_gateway.modbus.modbus_register.register_address.value	768
device.sensor_gateways.sensor_gateway.modbus.modbus_register.register_count.value	40

CHAPTER 4

Monitoring and Reporting

Monitoring and reporting is done by CAM.

Setting Up Dashboard

This section provides configuration detail for integrating CAM with ACP and explains various uses cases reporting. This chapter includes the following sections:

- Integration of CAM with ACP
- Prerequisites for creating Dashboard use cases
- Use cases: Dashboard Monitoring
- Use cases: Reporting

Prerequisites for Creating a Dashboard

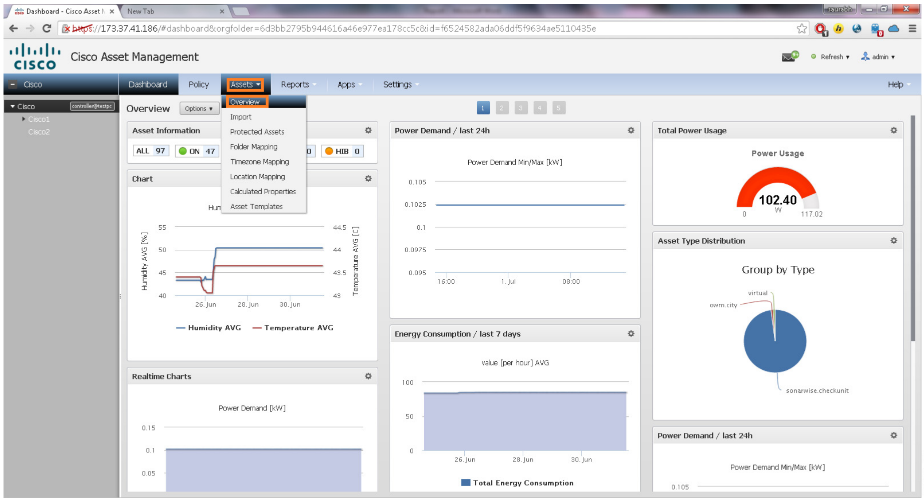
In this section, the prerequisites required in the use cases for Dashboard Monitoring and Reporting are discussed.

Get DQL ID of Asset

For DQL ID of an asset, complete the following steps:

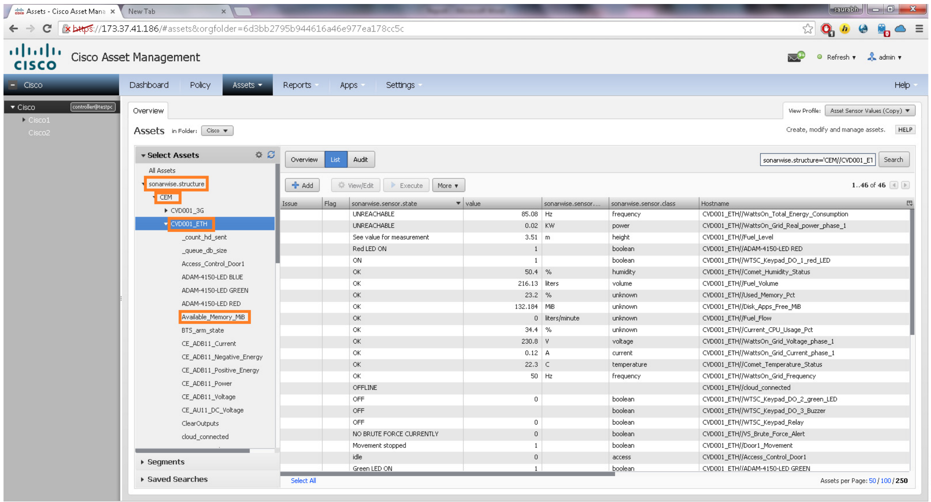
Step 1 Select **Overview** from the **Assets** menu, as shown in Figure 4-1.

Figure 4-1 Selection of Overview Page



Step 2 Select **Sonarwise > Structure > CEM > Device > Asset**. shows CVD001_ETH as **Device** and Available_Memory_MB as **Asset,** as shown in Figure 4-2.

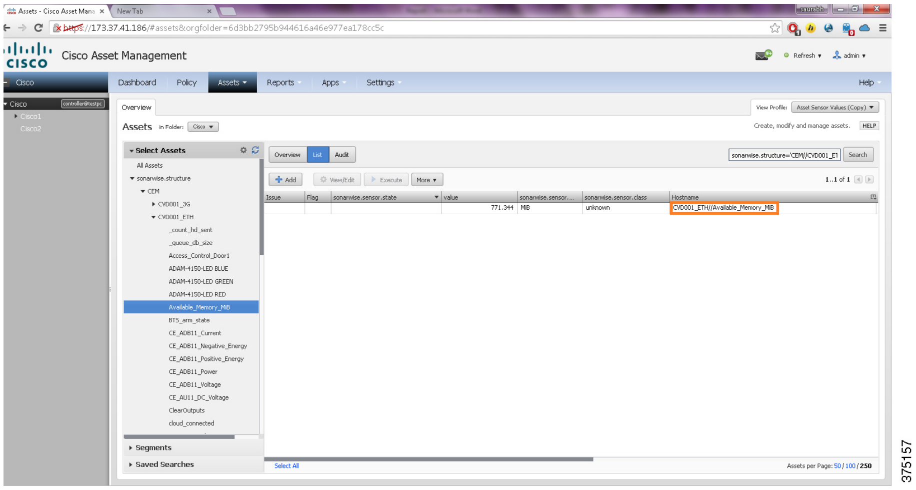
Figure 4-2 Selection of Asset from Device



Issue	Flag	sonarwise.sensor.state	value	sonarwise.sensor....	sonarwise.sensor.class	Hostname
		UNREACHABLE	85.08	Hz	frequency	CVD001_ETH//WattsOn_Total_Energy_Consumption
		UNREACHABLE	0.02	KW	power	CVD001_ETH//WattsOn_Grid_Real_power_phase_1
		See value for measurement	3.51	m	height	CVD001_ETH//Fuel_Level
		Red LED ON	1		boolean	CVD001_ETH//ADAM-4150-LED RED
		ON	1		boolean	CVD001_ETH//WTSC_Keypad_DO_1_red_LED
		OK	50.4	%	humidity	CVD001_ETH//Comet_Humidity_Status
		OK	216.13	liters	volume	CVD001_ETH//Fuel_Volume
		OK	23.2	%	unknown	CVD001_ETH//Used_Memory_Pct
		OK	132.184	MiB	unknown	CVD001_ETH//Disk_Apps_Free_MiB
		OK	0	liters/minute	unknown	CVD001_ETH//Fuel_Flow
		OK	34.4	%	unknown	CVD001_ETH//Current_CPU_Usage_Pct
		OK	230.8	V	voltage	CVD001_ETH//WattsOn_Grid_Voltage_phase_1
		OK	0.12	A	current	CVD001_ETH//WattsOn_Grid_Current_phase_1
		OK	22.3	C	temperature	CVD001_ETH//Comet_Temperature_Status
		OK	50	Hz	frequency	CVD001_ETH//WattsOn_Grid_Frequency
		OFFLINE				CVD001_ETH//cloud_connected
		OFF	0		boolean	CVD001_ETH//WTSC_Keypad_DO_2_green_LED
		OFF			boolean	CVD001_ETH//WTSC_Keypad_DO_3_Buzzer
		OFF	0		boolean	CVD001_ETH//WTSC_Keypad_Relay
		NO BRUTE FORCE CURRENTLY	0		boolean	CVD001_ETH//VS_Brute_Force_Alert
		Movement stopped	1		boolean	CVD001_ETH//Door1_Movement
		idle	0		access	CVD001_ETH//Access_Control_Door1
		Green LED ON	1		boolean	CVD001_ETH//ADAM-4150-LED GREEN

Step 3 Click on the selected asset. After clicking on the asset, asset information is displayed, as shown in Figure 4-3.

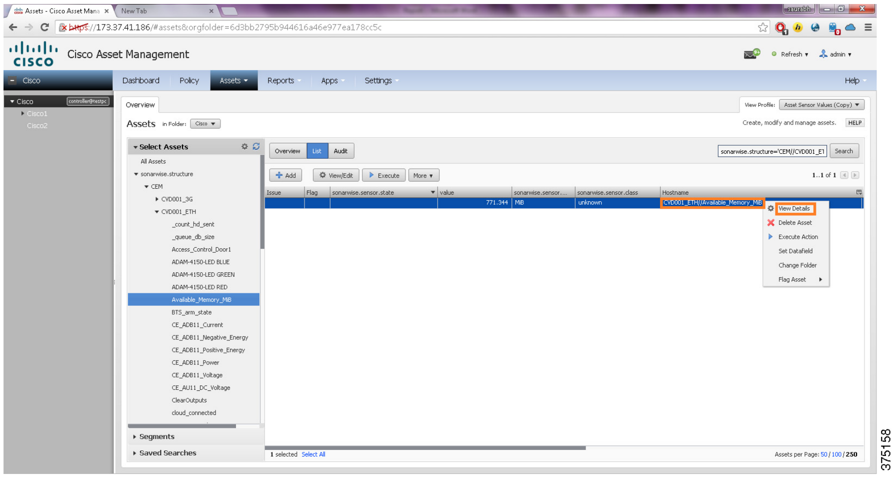
Figure 4-3 Summary of Asset



Issue	Flag	sonarwise.sensor.state	value	sonarwise.sensor....	sonarwise.sensor.class	Hostname
			771.344	MB	unknown	CVD001_ETH//Available_Memory_MB

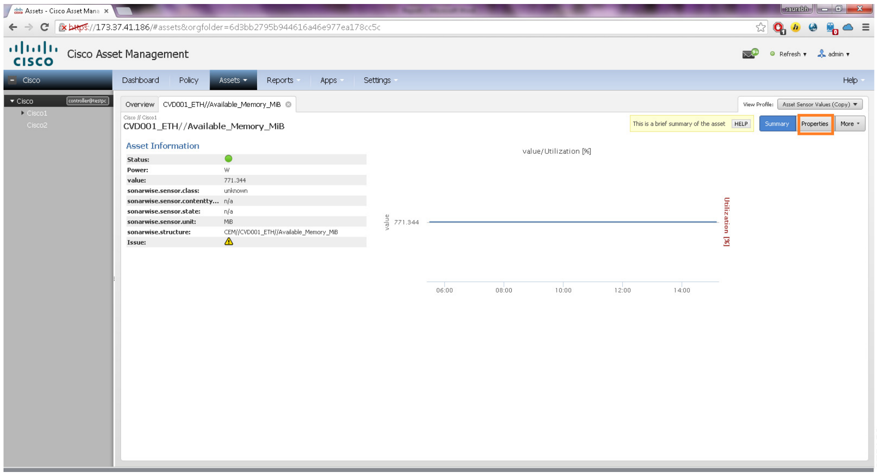
Step 4 Right-click on the **Hostname** value and select **View Details**, as shown in Figure 4-4.

Figure 4-4 Selection of Detail Information of Asset



Step 5 Summary information of the device appears. For DQL ID, select the **Property** option, as shown in Figure 4-5.

Figure 4-5 Selections of Properties of Asset

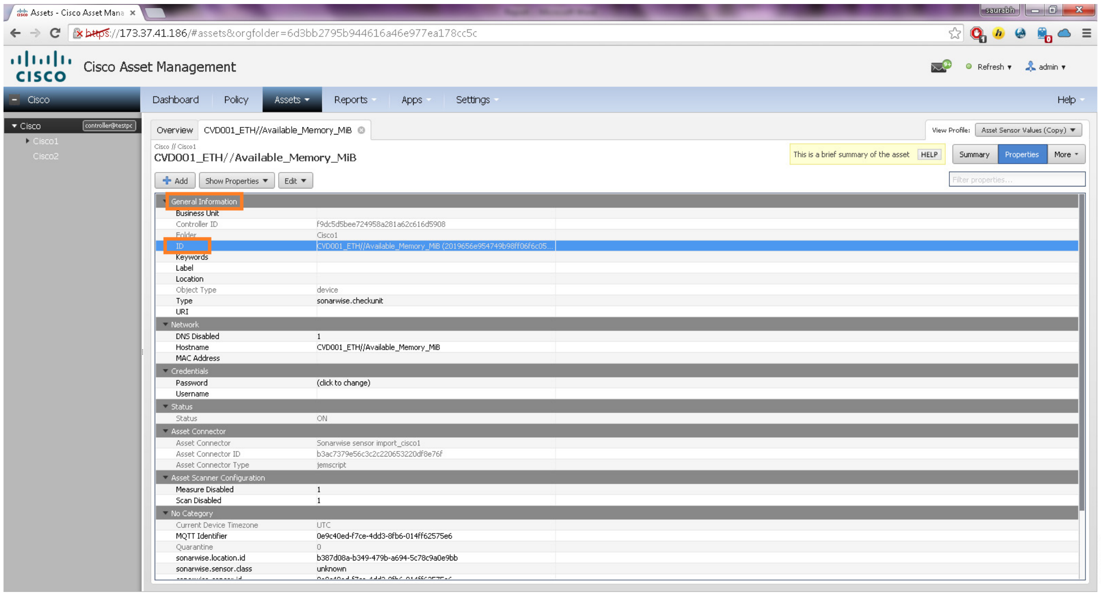


Asset Information

Status:	●
Power:	W
value:	771.344
sonarwise.sensor.class:	unknown
sonarwise.sensor.contentty...	n/a
sonarwise.sensor.state:	n/a
sonarwise.sensor.unit:	MiB
sonarwise.structure:	CEM//CVD001_ETH//Available_Memory_MiB
Issue:	⚠

Step 6 The **ID** option under the **General Information** option appears, as shown in Figure 4-6.

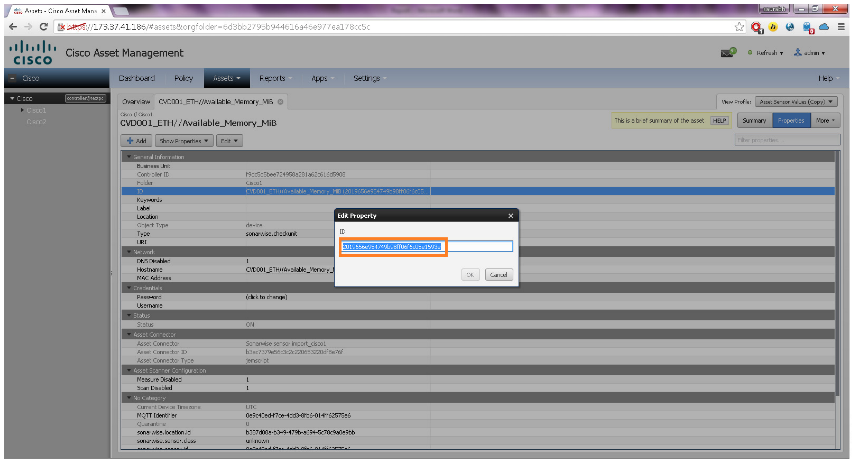
Figure 4-6 Properties of Asset



General Information	
Business Unit	
Controller ID	f9dc5d5bee724958a281a62c616d5908
Folder	Cisco1
ID	CVD001_ETH//Available_Memory_MiB (2019656e954749b98ff06f6c05...
Keywords	
Label	
Location	
Object Type	device
Type	sonarwise.checkunit
URI	
Network	
DNS Disabled	1
Hostname	CVD001_ETH//Available_Memory_MiB
MAC Address	
Credentials	
Password	(click to change)
Username	
Status	
Status	ON
Asset Connector	
Asset Connector	Sonarwise sensor import_cisco1
Asset Connector ID	b3ac7379e56c3c2c220653220df8e76f
Asset Connector Type	jemscript
Asset Scanner Configuration	
Measure Disabled	1
Scan Disabled	1
No Category	
Current Device Timezone	UTC
MQTT Identifier	0e9c40ed-f7ce-4dd3-8fb6-014ff62575e6
Quarantine	0
sonarwise.location.id	b387d08a-b349-479b-a694-5c78c9a0e9bb
sonarwise.sensor.class	unknown

Step 7 Double-click on the **ID** value. The Edit Property window appears. Select the **ID** value from **ID** option, as shown in Figure 4-7.

Figure 4-7 ***DQL ID of Asset***



General Information	
Business Unit	
Controller ID	f9dc5d5bee724958a281a62c616d5908
Folder	Cisco1
ID	CVD001_ETH//Available_Memory_MiB (2019656e954749b98ff06f6c05...
Keywords	
Label	
Location	
Object Type	device
Type	sonarwise.checkunit
URI	
Network	
DNS Disabled	1
Hostname	CVD001_ETH//Available_Memory_
MAC Address	
Credentials	
Password	(click to change)
Username	
Status	
Status	ON
Asset Connector	
Asset Connector	Sonarwise sensor import_cisco1
Asset Connector ID	b3ac7379e56c3c2c220653220df8e76f
Asset Connector Type	jemscript
Asset Scanner Configuration	
Measure Disabled	1
Scan Disabled	1
No Category	
Current Device Timezone	UTC
MQTT Identifier	0e9c40ed-f7ce-4dd3-8fb6-014ff62575e6
Quarantine	0
sonarwise.location.id	b387d08a-b349-479b-a694-5c78c9a0e9bb
sonarwise.sensor.class	unknown

Edit Property

ID: 2019656e954749b98ff06f6c05e1593e

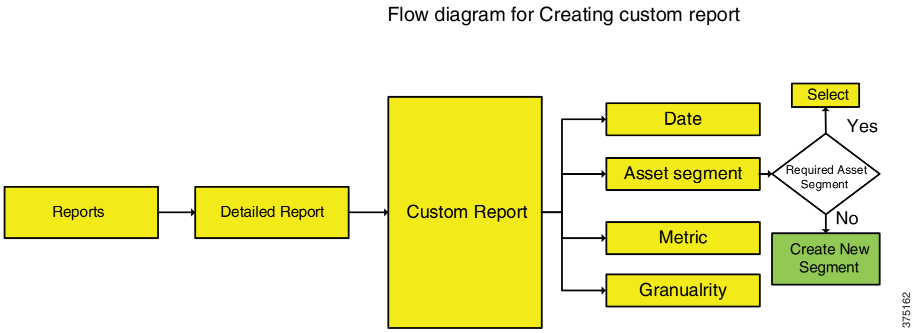
OK Cancel

Creation of Custom Report

This section explains how to get custom report of any asset based on user requirements.

Figure 4-8 shows the flow diagram for creating a custom report.

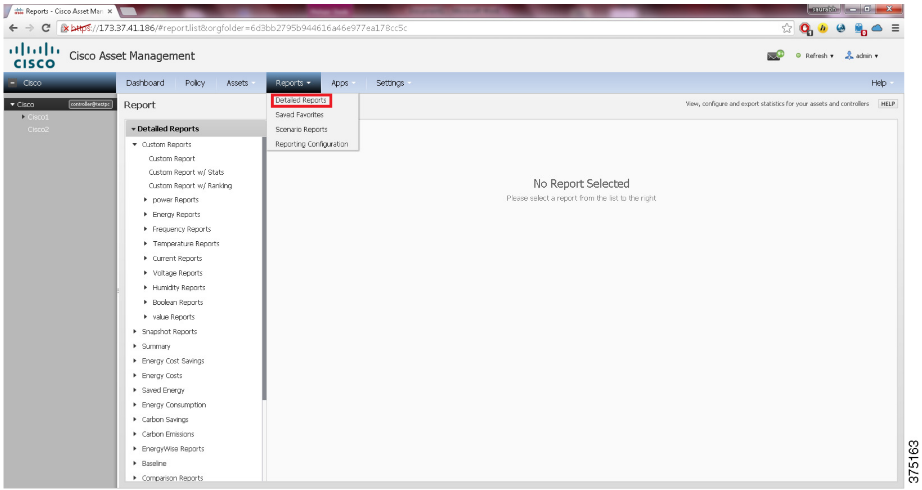
Figure 4-8 ***Flow Diagram for Creating Custom Report***



Complete the following steps to create a custom report.

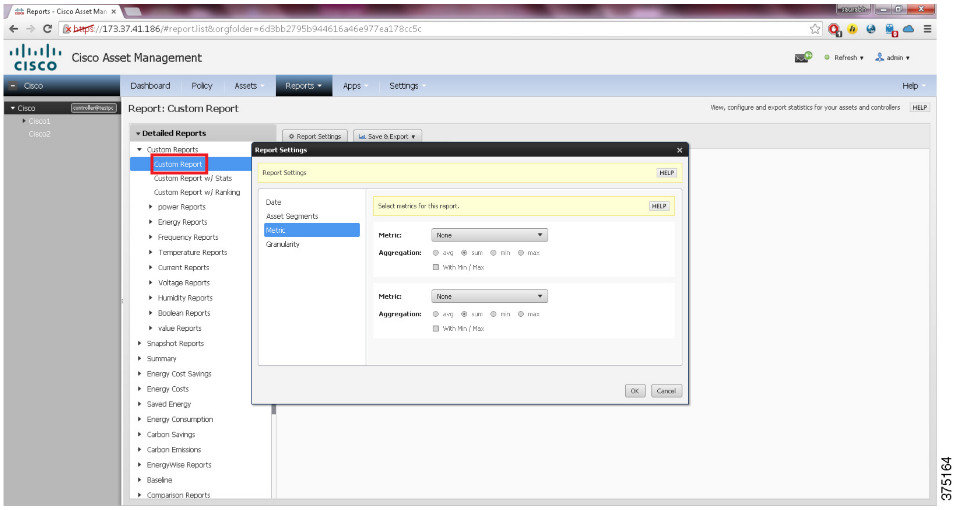
Step 1 Select **Detailed Reports** from the **Reports** menu, as shown in Figure 4-9.

Figure 4-9 Selection of Detailed Reports Page



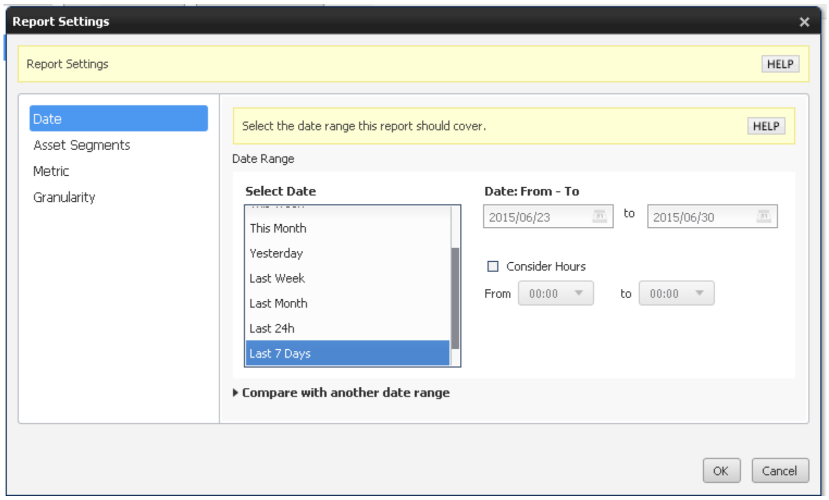
Step 2 Select **Custom Report**. The Report Settings window appears, as shown in Figure 4-10. Select date, asset segment, metric and granularity in the **Report** settings.

Figure 4-10 Selection of Custom Report



a. For **Select Date**, select the required date range that should be covered in the report, as shown in Figure 4-11.

Figure 4-11 Selection of Date Range



Select the date range this report should cover.

Date Range

Select Date: This Month, Yesterday, Last Week, Last Month, Last 24h, Last 7 Days (selected)

Date: From - To: 2015/06/23 to 2015/06/30

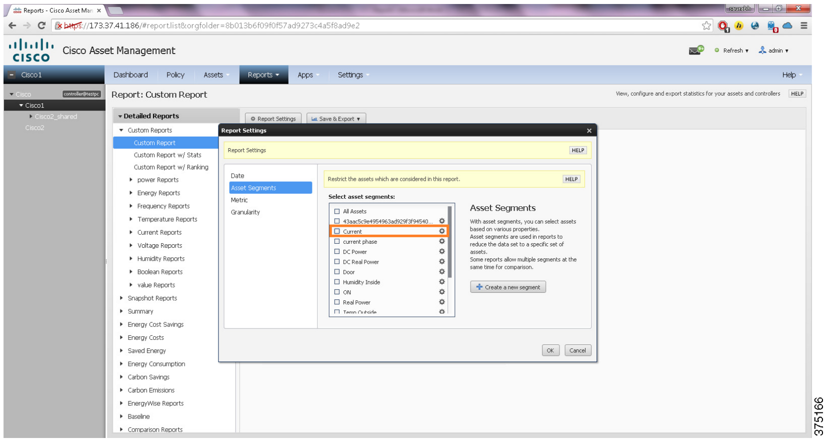
□ Consider Hours

From 00:00 to 00:00

Compare with another date range

b. **Asset Segments** gives two options for selecting an asset segment: either select a required Asset Segment from available list (see Figure 4-12) or select **Create a new Segment** from the **Asset Segments** option (see Figure 4-13 and Figure 4-14).

Figure 4-12 Selection of Required Asset Segment from Available List



Report: Custom Report

View, configure and export statistics for your assets and controllers

Restrict the assets which are considered in this report.

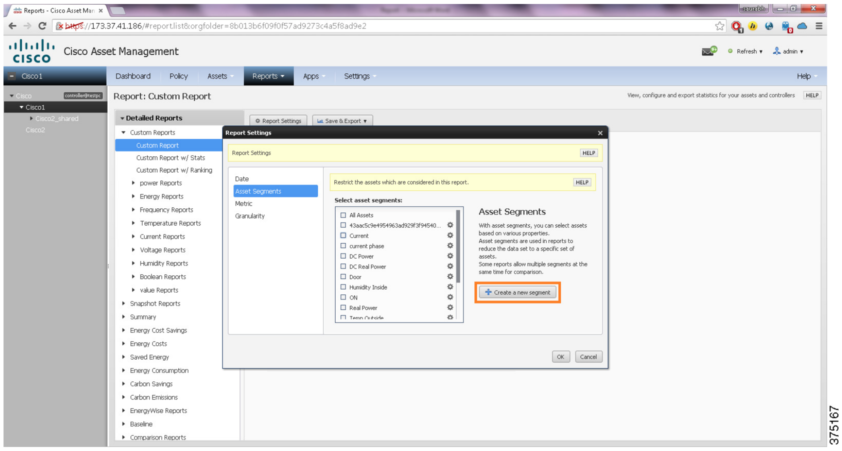
Select asset segments:

- □ All Assets
- □ 43aac5c9e4954963ad929f3f94540...
- □ Current
- □ current phase
- □ DC Power
- □ DC Real Power
- □ Door
- □ Humidity Inside
- □ ON
- □ Real Power
- □ Temp Outside

Asset Segments

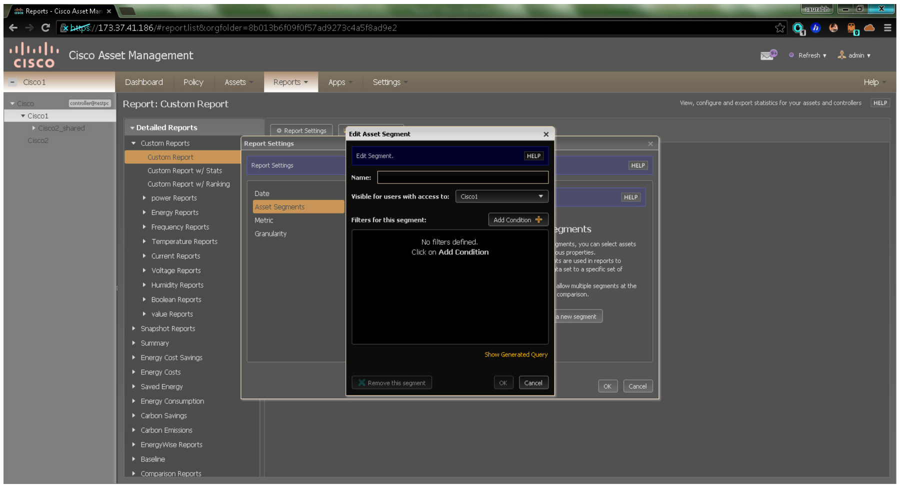
With asset segments, you can select assets based on various properties.
Asset segments are used in reports to reduce the data set to a specific set of assets.
Some reports allow multiple segments at the same time for comparison.

Figure 4-13 Create a New Segment



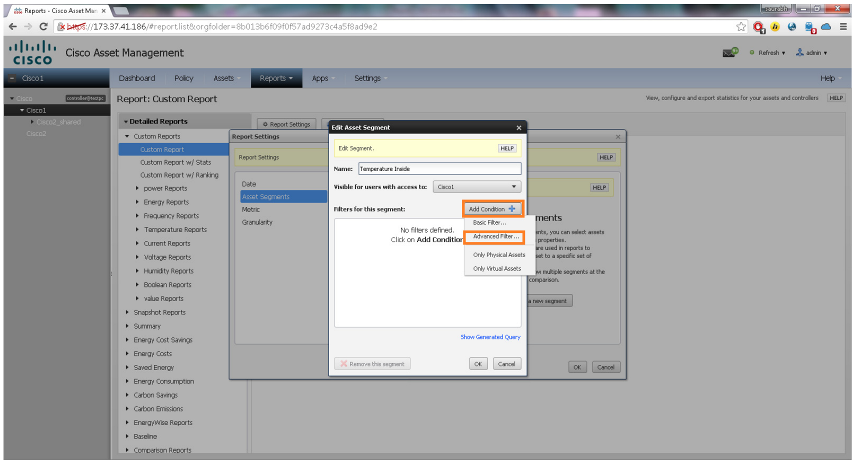
With asset segments, you can select assets based on various properties. Asset segments are used in reports to reduce the data set to a specific set of assets. Some reports allow multiple segments at the same time for comparison.

Figure 4-14 Edit Asset Segment Window



c. To create new segments, select **Create a new Segment** from the **Asset Segments** section. The Edit Asset Segment window appears. In the **Edit Asset Segment** window (see Figure 4-15), put the name of segment in the **Name** field (for example Temperature Inside). To filter this segment, select **Advance Filter** from the **Add Condition** option. A new window, Advance Filter, appears (see Figure 4-16). In the **Advance Filter** field, put the DQL ID of the sensor and select **OK** (see Figure 4-17).

Figure 4-15 Selection of Advance Filter



Edit Asset Segment

Edit Segment.

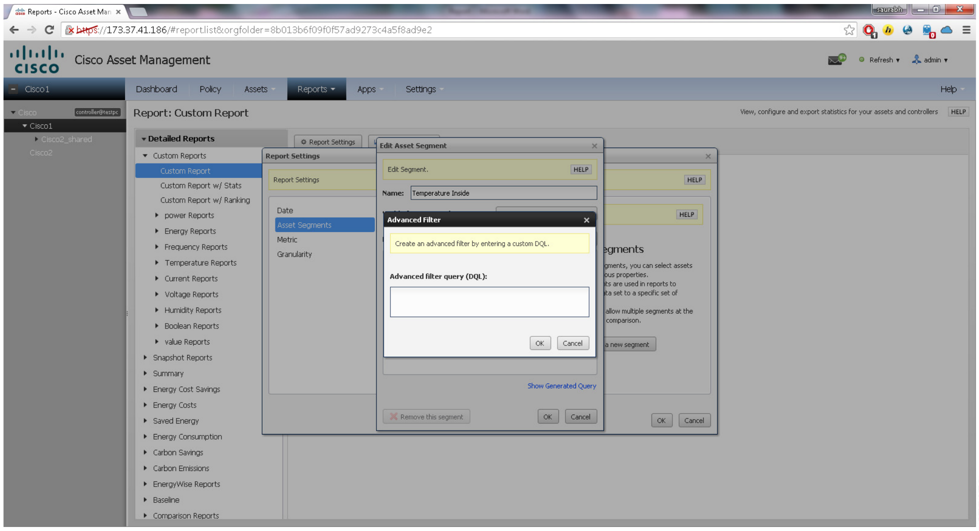
Name: Temperature Inside

Visible for users with access to: Cisco1

Filters for this segment:

No filters defined.
Click on Add Condition

Figure 4-16 DQL as an Advance Filter Query



Edit Asset Segment

Edit Segment.

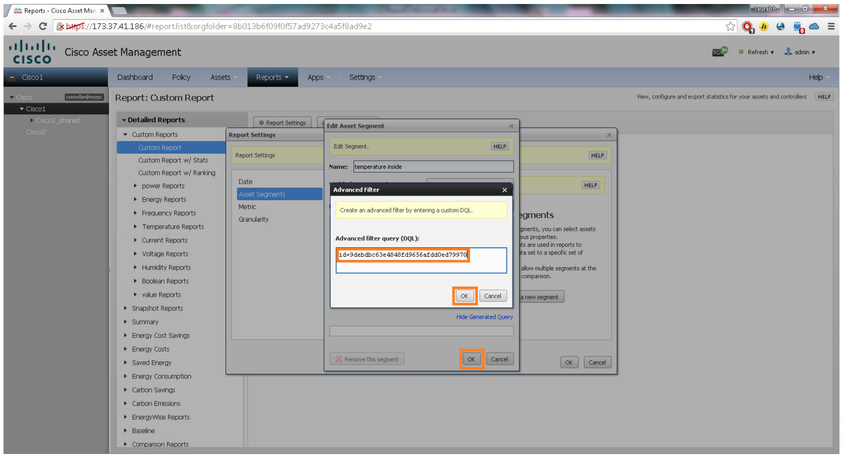
Name: Temperature Inside

Advanced Filter

Create an advanced filter by entering a custom DQL.

Advanced filter query (DQL):

Figure 4-17 Selection of DQL ID of Asset as an Advance Filter Query



Edit Asset Segment

Edit Segment.

Name: temperature inside

Advanced Filter

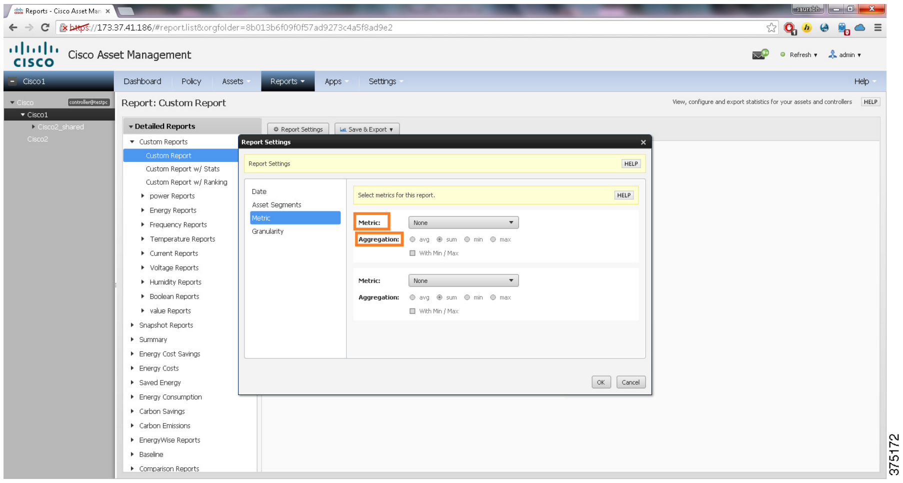
Create an advanced filter by entering a custom DQL.

Advanced filter query (DQL):

```
id=9debdbc63e4848fd9656afdd0ed79970
```

d. For Metric, select a Metric value and an Aggregation value based on the requirement, as shown in Figure 4-18.

Figure 4-18 Selection of Metric and Aggregation Value



e. For Granularity, there are four values (Dynamic, Hourly, Daily and Monthly). Select one value based on your requirement (see Figure 4-19). The default value is Dynamic. Select **OK**. A graph for the given metric and asset appears, as shown in Figure 4-20.

Figure 4-19 Selection of Granularity

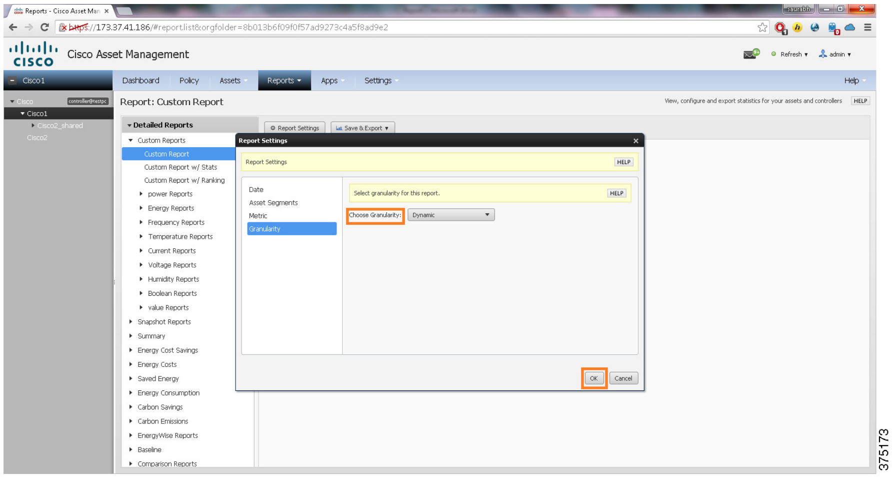
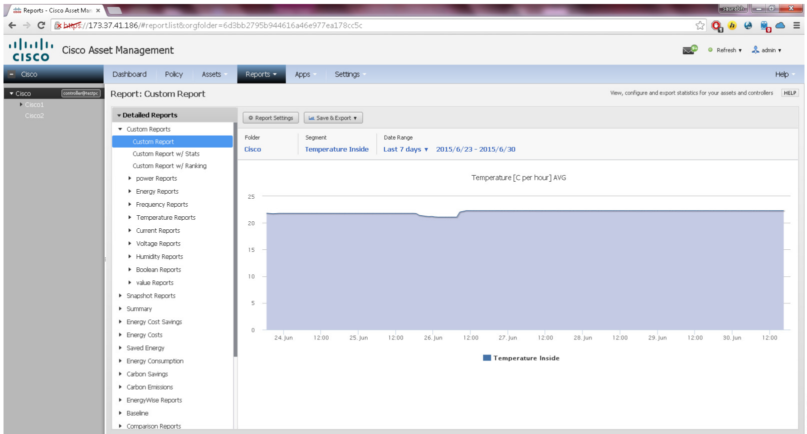


Figure 4-20 Graph of Custom Report



Step 3 Save and export the data from the **Save & Export** option. For example, if the user wants to get the data in JSON format, select **Export as JSON** (see Figure 4-21) from the **Save & Export** drop-down list. JSON data appears in a new window, as shown in Figure 4-22.

Figure 4-21 Selection of Custom Report in JSON Format

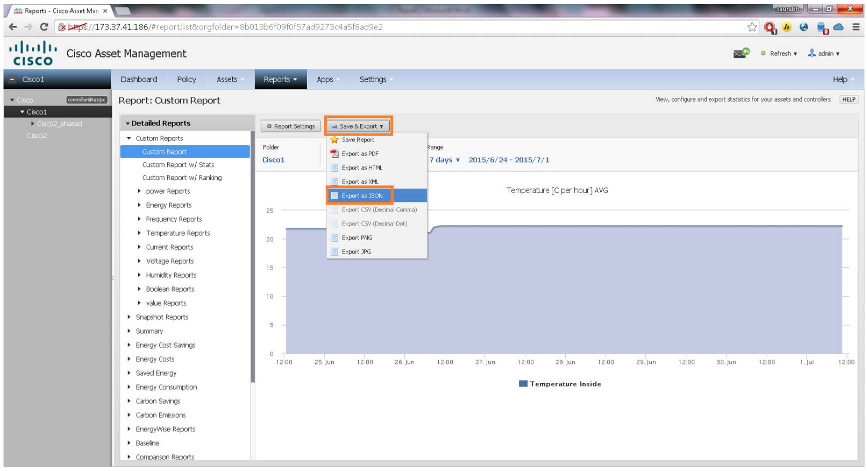
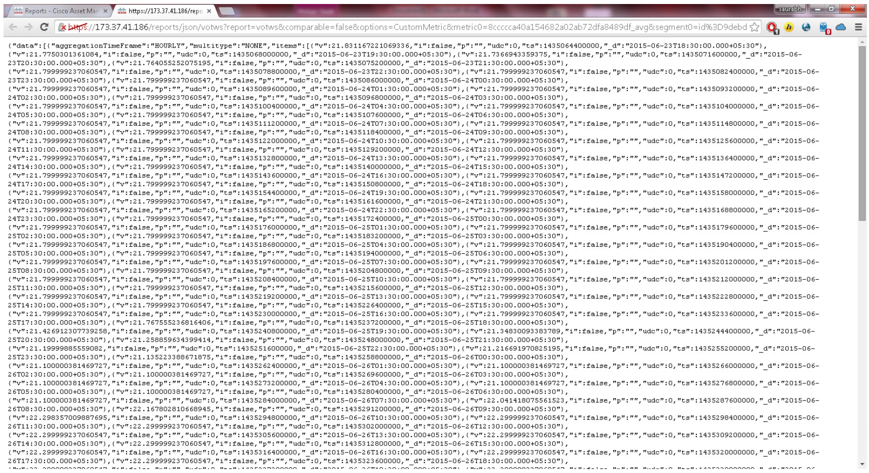


Figure 4-22 Custom Report in JSON Format


Reports - Cisco Asset Man
https://173.37.41.186/repo
saurabh
https://173.37.41.186/reports/json/votws?report=votws&comparable=false&options=CustomMetric&metric0=8ccccca40a154682a02ab72dfa8489df_avg&segment0=id%3D9debd
375176

```
{"data":[{"aggregationTimeFrame":"HOURLY","multitype":"NONE","items":[{"v":21.831167221069336,"i":false,"p":"","udc":0,"ts":1435064400000,"_d":"2015-06-23T18:30:00.000+05:30"},
{"v":21.7750301361084,"i":false,"p":"","udc":0,"ts":1435068000000,"_d":"2015-06-23T19:30:00.000+05:30"},{"v":21.7366943359375,"i":false,"p":"","udc":0,"ts":1435071600000,"_d":"2015-06-
23T20:30:00.000+05:30"},{"v":21.764055252075195,"i":false,"p":"","udc":0,"ts":1435075200000,"_d":"2015-06-23T21:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435078800000,"_d":"2015-06-23T22:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435082400000,"_d":"2015-06-
23T23:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435086000000,"_d":"2015-06-24T00:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435089600000,"_d":"2015-06-24T01:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435093200000,"_d":"2015-06-
24T02:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435096800000,"_d":"2015-06-24T03:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435100400000,"_d":"2015-06-24T04:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435104000000,"_d":"2015-06-
24T05:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435107600000,"_d":"2015-06-24T06:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435111200000,"_d":"2015-06-24T07:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435114800000,"_d":"2015-06-
24T08:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435118400000,"_d":"2015-06-24T09:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435122000000,"_d":"2015-06-24T10:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435125600000,"_d":"2015-06-
24T11:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435129200000,"_d":"2015-06-24T12:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435132800000,"_d":"2015-06-24T13:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435136400000,"_d":"2015-06-
24T14:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435140000000,"_d":"2015-06-24T15:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435143600000,"_d":"2015-06-24T16:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435147200000,"_d":"2015-06-
24T17:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435150800000,"_d":"2015-06-24T18:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435154400000,"_d":"2015-06-24T19:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435158000000,"_d":"2015-06-
24T20:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435161600000,"_d":"2015-06-24T21:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435165200000,"_d":"2015-06-24T22:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435168800000,"_d":"2015-06-
24T23:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435172400000,"_d":"2015-06-25T00:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435176000000,"_d":"2015-06-25T01:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435179600000,"_d":"2015-06-
25T02:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435183200000,"_d":"2015-06-25T03:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435186800000,"_d":"2015-06-25T04:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435190400000,"_d":"2015-06-
25T05:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435194000000,"_d":"2015-06-25T06:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435197600000,"_d":"2015-06-25T07:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435201200000,"_d":"2015-06-
25T08:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435204800000,"_d":"2015-06-25T09:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435208400000,"_d":"2015-06-25T10:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435212000000,"_d":"2015-06-
25T11:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435215600000,"_d":"2015-06-25T12:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435219200000,"_d":"2015-06-25T13:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435222800000,"_d":"2015-06-
25T14:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435226400000,"_d":"2015-06-25T15:30:00.000+05:30"},
{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435230000000,"_d":"2015-06-25T16:30:00.000+05:30"},{"v":21.799999237060547,"i":false,"p":"","udc":0,"ts":1435233600000,"_d":"2015-06-
25T17:30:00.000+05:30"},{"v":21.767555236816406,"i":false,"p":"","udc":0,"ts":1435237200000,"_d":"2015-06-25T18:30:00.000+05:30"},
{"v":21.426912307739258,"i":false,"p":"","udc":0,"ts":1435240800000,"_d":"2015-06-25T19:30:00.000+05:30"},{"v":21.34830093383789,"i":false,"p":"","udc":0,"ts":1435244400000,"_d":"2015-06-
25T20:30:00.000+05:30"},{"v":21.258859634399414,"i":false,"p":"","udc":0,"ts":1435248000000,"_d":"2015-06-25T21:30:00.000+05:30"},
{"v":21.19999885559082,"i":false,"p":"","udc":0,"ts":1435251600000,"_d":"2015-06-25T22:30:00.000+05:30"},{"v":21.216691970825195,"i":false,"p":"","udc":0,"ts":1435255200000,"_d":"2015-06-
25T23:30:00.000+05:30"},{"v":21.135223388671875,"i":false,"p":"","udc":0,"ts":1435258800000,"_d":"2015-06-26T00:30:00.000+05:30"},
{"v":21.10000381469727,"i":false,"p":"","udc":0,"ts":1435262400000,"_d":"2015-06-26T01:30:00.000+05:30"},{"v":21.10000381469727,"i":false,"p":"","udc":0,"ts":1435266000000,"_d":"2015-06-
26T02:30:00.000+05:30"},{"v":21.10000381469727,"i":false,"p":"","udc":0,"ts":1435269600000,"_d":"2015-06-26T03:30:00.000+05:30"},
{"v":21.10000381469727,"i":false,"p":"","udc":0,"ts":1435273200000,"_d":"2015-06-26T04:30:00.000+05:30"},{"v":21.10000381469727,"i":false,"p":"","udc":0,"ts":1435276800000,"_d":"2015-06-
26T05:30:00.000+05:30"},{"v":21.10000381469727,"i":false,"p":"","udc":0,"ts":1435280400000,"_d":"2015-06-26T06:30:00.000+05:30"},
{"v":21.10000381469727,"i":false,"p":"","udc":0,"ts":1435284000000,"_d":"2015-06-26T07:30:00.000+05:30"},{"v":22.041418075561523,"i":false,"p":"","udc":0,"ts":1435287600000,"_d":"2015-06-
26T08:30:00.000+05:30"},{"v":22.167802810668945,"i":false,"p":"","udc":0,"ts":1435291200000,"_d":"2015-06-26T09:30:00.000+05:30"},
{"v":22.298357009887695,"i":false,"p":"","udc":0,"ts":1435294800000,"_d":"2015-06-26T10:30:00.000+05:30"},{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435298400000,"_d":"2015-06-
26T11:30:00.000+05:30"},{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435302000000,"_d":"2015-06-26T12:30:00.000+05:30"},
{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435305600000,"_d":"2015-06-26T13:30:00.000+05:30"},{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435309200000,"_d":"2015-06-
26T14:30:00.000+05:30"},{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435312800000,"_d":"2015-06-26T15:30:00.000+05:30"},
{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435316400000,"_d":"2015-06-26T16:30:00.000+05:30"},{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435320000000,"_d":"2015-06-
26T17:30:00.000+05:30"},{"v":22.299999237060547,"i":false,"p":"","udc":0,"ts":1435323600000,"_d":"2015-06-26T18:30:00.000+05:30"},
```

Step 4 We can directly get this data, using the URL link of this window. In this example URL link is as shown below:

https://173.37.41.186/reports/json/votws?report=votws&comparable=false&options=CustomMetric&metric0=8ccccca40a154682a02ab72dfa8489df_avg&segment0=id%3D9debdbc63e4848fd9656afdd0ed79970%20dqllabel%3D%22Temperature%20Inside%22&dtype=last7days&ds=&de=&hrsconsiderdaterange=0&granularity=&export=json&limit=undefined&offset=undefined&orgfolder=6d3bb2795b944616a46e977ea178cc5c&locale=en&tz=330&ts=eb83453adbb785adfac896b6cb3224f2

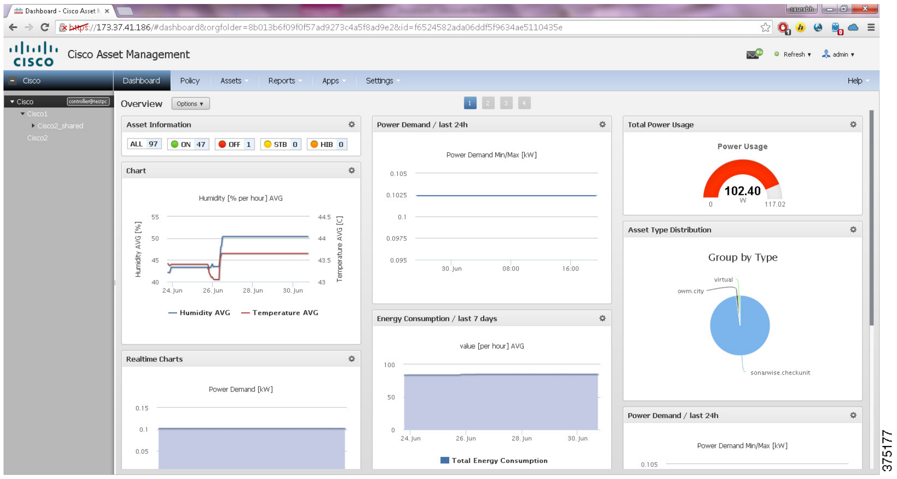
If we want to get the data from this link in the script, we can use the api_get() function, as shown below:

```
var res  =
api_get("/reports/json/votws?report=votws&comparable=false&options=CustomMetric&metric0=c2
b675a30f19401394722c4d82b9ec39_avg&segment0=id%3D09344b950ea8436aa285e0c52439152b
dqllabel%3D\"Humidity
Inside\"&dtype=last7days&ds=&de=&hrsconsiderdaterange=0&granularity=&export=json&limit=und
efined&offset=undefined&orgfolder=8b013b6f09f0f57ad9273c4a5f8ad9e2&locale=en&tz=330&ts=e7b
d61d2b3fd9f9f41d6f9de238085be");
```

Dashboard

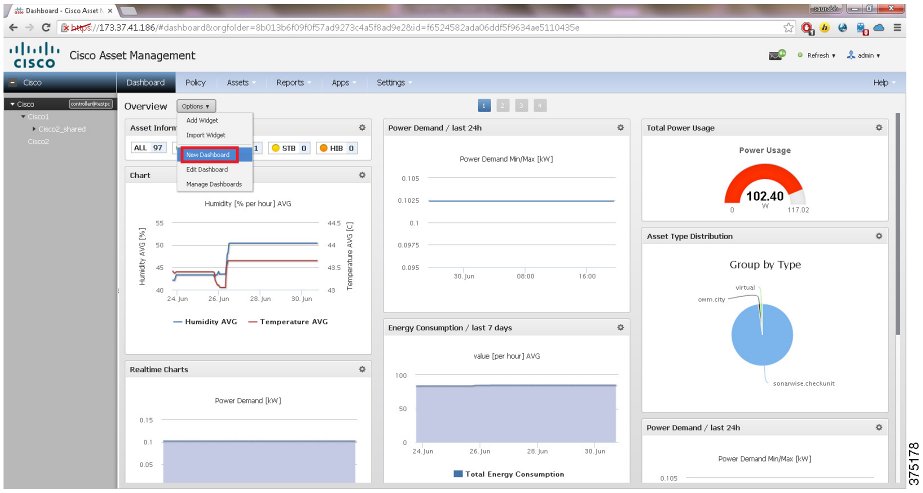
The Dashboard is the default view in the CAM application (see Figure 4-23). It can be customized according to the user needs. When Auto-Refresh is activated, the CAM application updates the dashboard every 15 seconds.

Figure 4-23 Cisco Asset Management Web Page



Users can create new dashboard, edit available dashboard and add widget in the available dashboard, as shown in Figure 4-24.

Figure 4-24 Selection of New Dashboard



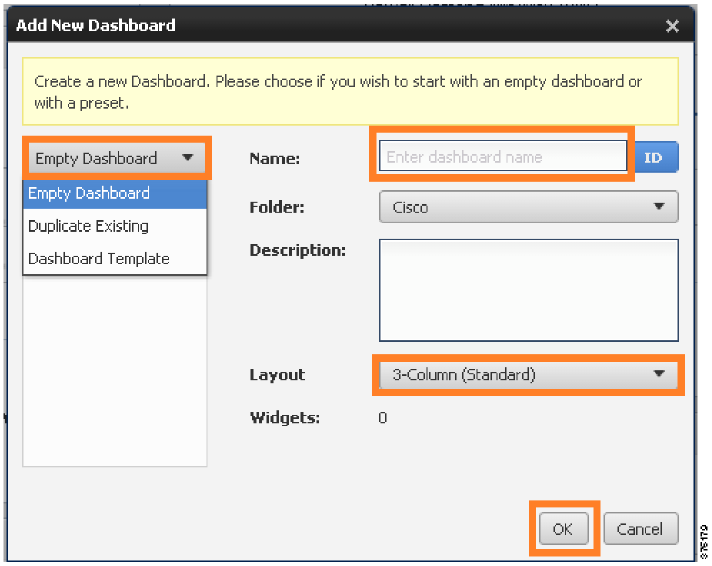
Create New Dashboard

You can create a dashboard from a predefined template or copy an existing dashboard.

To create a new dashboard, complete the following steps:

Step 1 On the dashboard page, select **New Dashboard** from **Options**. The Add New Dashboard window appears (see Figure 4-25).

Figure 4-25 Add New Dashboard



Add New Dashboard

Create a new Dashboard. Please choose if you wish to start with an empty dashboard or with a preset.

Empty Dashboard
- Empty Dashboard
- Duplicate Existing
- Dashboard Template

Name: Enter dashboard name ID

Folder: Cisco

Description:

Layout 3-Column (Standard)

Widgets: 0

OK Cancel

Step 2 Select one of the following three options in the **Add New Dashboard** window based on requirements:

- Empty Dashboards
- Duplicate Dashboards
- Dashboard Template (The Dashboard Template option has three choices: Asset Overview, Overview and Energy Saving.)

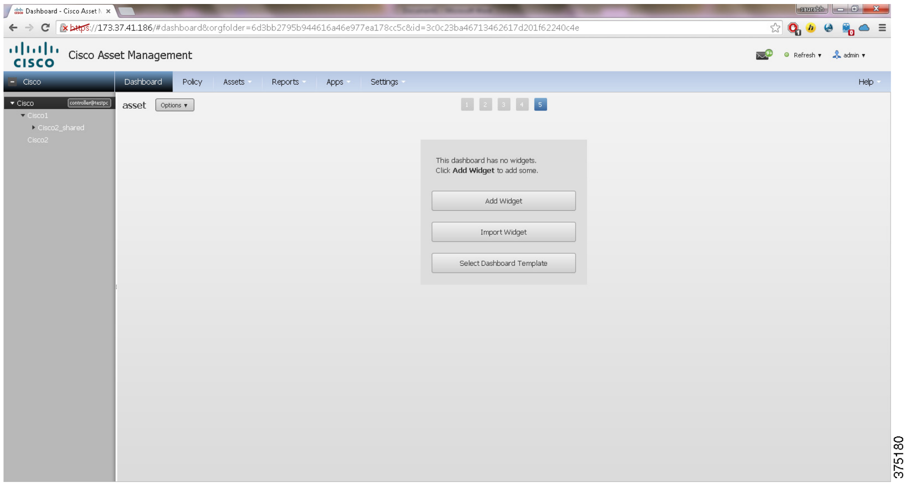
Step 3 Choose a name for the dashboard and folder where the dashboard should be saved.

Step 4 Select a layout based on requirements.

Step 5 Select **OK**.

For example, we select Empty Dashboard, asset as Name and cisco as folder, and select the OK button. The new dashboard will appear, as shown in Figure 4-26.

Figure 4-26 New Dashboard



This dashboard has no widgets.
Click **Add Widget** to add some.

Add Widget

Adding a widget allows the user to use predefined widgets or create new widgets by using the scripts. Select **Add Widget** from **Option** (see Figure 4-27). The Add New Dashboard window appears (see Figure 4-28). There are the following two types of widgets:

- Pre-defined widget
- User-defined widget

Figure 4-27 Selection of Add Widget

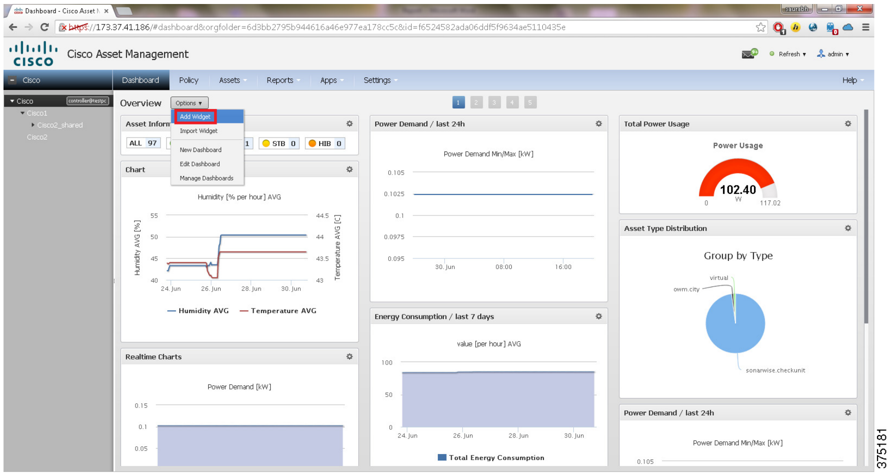
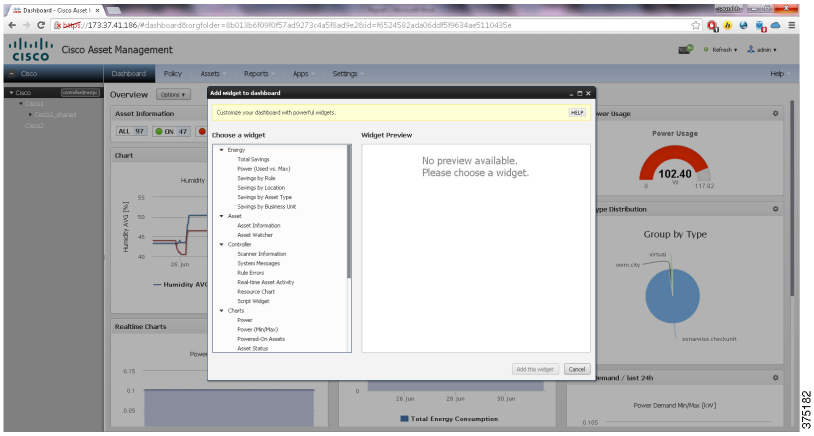


Figure 4-28 Customization of Dashboard with Powerful Widget



Add widget to dashboard

Customize your dashboard with powerful widgets. HELP

Choose a widget

- Energy
  - Total Savings
  - Power (Used vs. Max)
  - Savings by Rule
  - Savings by Location
  - Savings by Asset Type
  - Savings by Business Unit
- Asset
  - Asset Information
  - Asset Watcher
- Controller
  - Scanner Information
  - System Messages
  - Rule Errors
  - Real-time Asset Activity
  - Resource Chart
  - Script Widget
- Charts
  - Power
  - Power (Min/Max)
  - Powered-On Assets
  - Asset Status

Widget Preview

No preview available.
Please choose a widget.

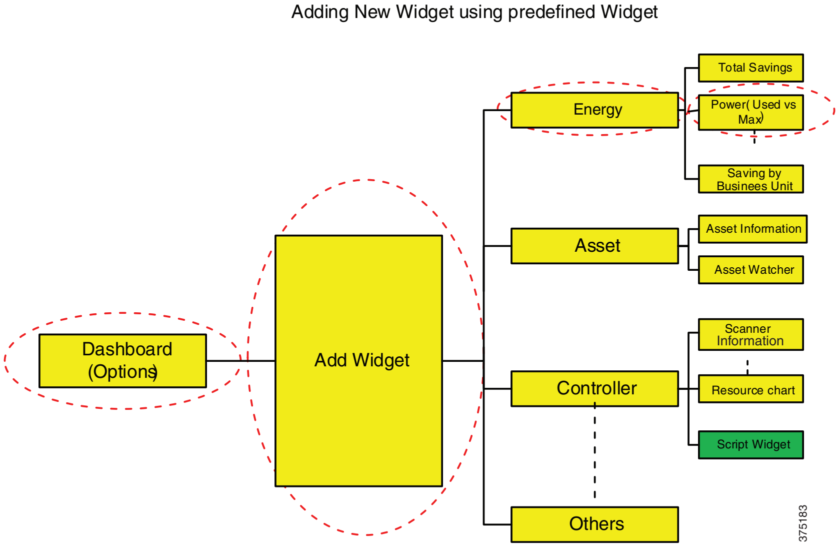
Add this widget | Cancel

Pre-Defined Widget

A pre-defined widget allows the user to create a widget based on the pre-defined layout and scripts. If a widget is selected from the Choose a Widget option, under the Widget Preview option, a custom title and select assets will appear. Enter a title for the widget and use the DQL ID to determine for which asset, the information should be displayed.

Figure 4-29 shows the flow diagram of adding a new widget using a pre-defined widget.

Figure 4-29 Flow Diagram of Adding New Widget using Pre-Defined Widget



For example, to know the power uses for a particular device, complete the following steps (see Figure 4-30):

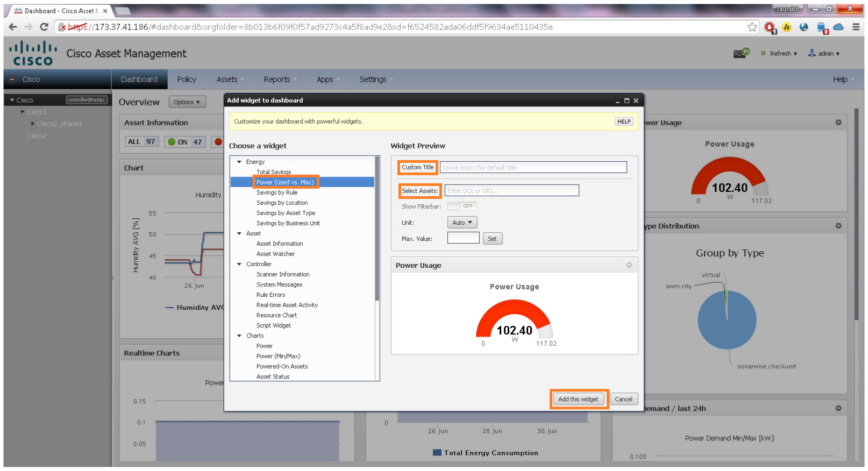
Step 1 Select **Power (Used vs. Max)** from the **Energy** option.

Step 2 Enter **Title** (for example Power) in the **Custom Title** option.

Step 3 Enter the **DQL ID** of the device in the **Select Assets** option.

Step 4 Select **Add this Widget**.

Figure 4-30 Selection of Pre-Defined Widget



User-Defined Widget

This option allows the user to create a widget based on the personal requirements by using scripts. In this case, perform the following actions:

Step 1 Select **Script Widget** from the **Controller** option.

Step 2 Enter the title in the **Custom Title** option.

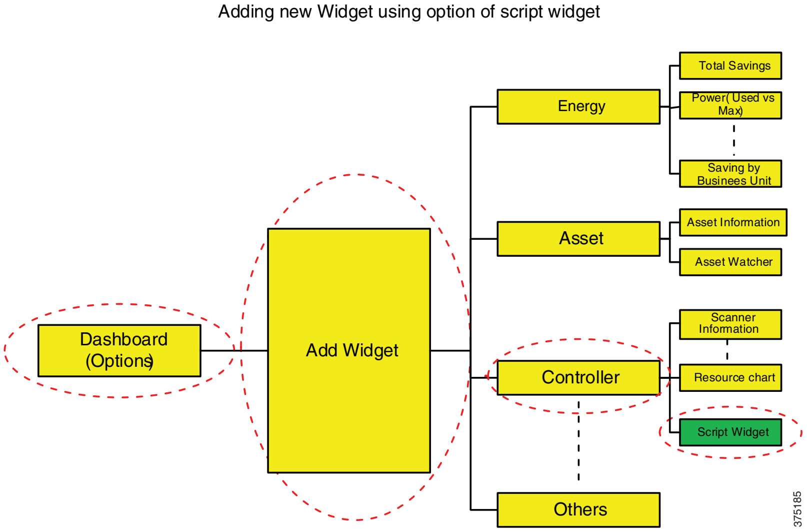
Step 3 Enter the script in the **Edit the Script** option based on required results.

Step 4 Enter html code to display the result in the **Layout** option.

Step 5 Select the place where the script should run (controller or server).

Figure 4-31 shows the flow diagram of adding new widget using the option of a script widget.

Figure 4-31 Flow Diagram of Adding New Widget using Option of Script Widget

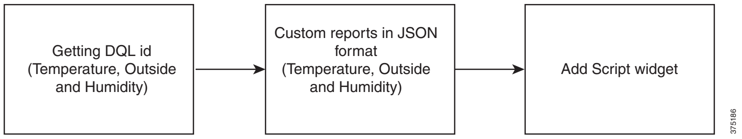


Example for User-Defined Widget

Assume we want to know the inside and outside temperature of a cell tower and the humidity inside the cell tower for 7 days. Figure 4-32 shows the flow for the use case for widget of temperature inside/outside and humidity.

Figure 4-32 Use Case for Widget of Temperature Inside/Outside and Humidity

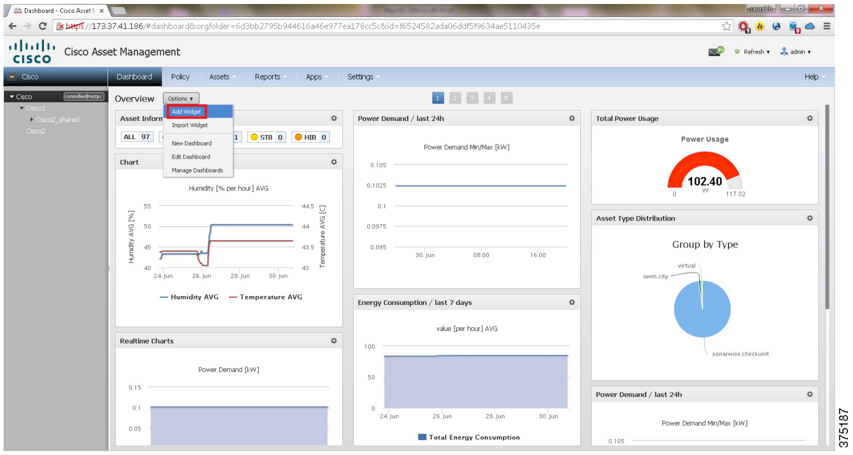
Usecase for Widget of Temperature Inside/outside /Humidity


Getting DQL id (Temperature, Outside and Humidity)
Custom reports in JSON format (Temperature, Outside and Humidity)
Add Script widget
375186

Complete the following steps:

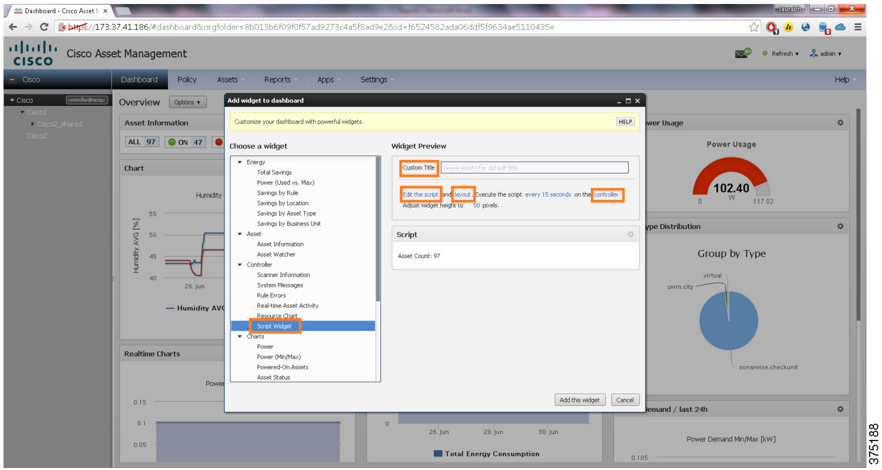
Step 1 Go to main window and select **Add widget** from **Options**, as shown in Figure 4-33. The **Add Widget to Dashboard** window opens.

Figure 4-33 Selection of Add Widget in Dashboard



Step 2 Select **Script Widget** from **Controller,** as shown in . The Widget Preview option will appear. Put a title, for example, Temperature (Inside, Outside) and Humidity Trend, in the **Custom Title** option. Refer to

Figure 4-34 Selection of Script Widget



Add widget to dashboard

Customize your dashboard with powerful widgets. HELP

Choose a widget

- Energy
  - Total Savings
  - Power (Used vs. Max)
  - Savings by Rule
  - Savings by Location
  - Savings by Asset Type
  - Savings by Business Unit
- Asset
  - Asset Information
  - Asset Watcher
- Controller
  - Scanner Information
  - System Messages
  - Rule Errors
  - Real-time Asset Activity
  - Resource Chart
  - Script Widget
- Charts
  - Power
  - Power (Min/Max)
  - Powered-On Assets
  - Asset Status

Widget Preview

Custom Title: Leave empty for default title

Edit the script and layout. Execute the script every 15 seconds on the controller

Adjust widget height to 50 pixels.

Script

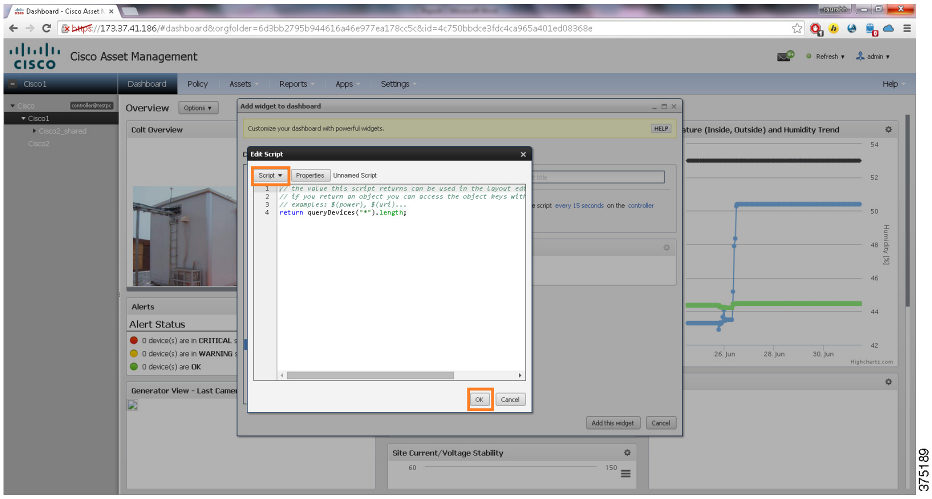
Asset Count: 97

Add this widget | Cancel

Step 3 Get the JSON data link for the inside temperature, outside temperature and the inside humidity of the cell tower for 7 days, using the steps explained in Creation of Custom Report. This JSON data link will be used in the option **Edit Script** with the function of api_get().

Step 4 Select **Edit the Script** from **Widget Preview** and write the script according to the requirements and select **OK**. The result will display based on HTML code in the **Layout** option, as shown in Figure 4-35.

Figure 4-35 Edit Script Window



Add widget to dashboard

Customize your dashboard with powerful widgets.

Edit Script

Script ▾ | Properties | Unnamed Script

```
// the value this script returns can be used in the layout edi
// if you return an object you can access the object keys with
// examples: $(power), $(uri)...
return queryDevices("*").length;
```

OK | Cancel

Alert Status

0 device(s) are in CRITICAL

0 device(s) are in WARNING

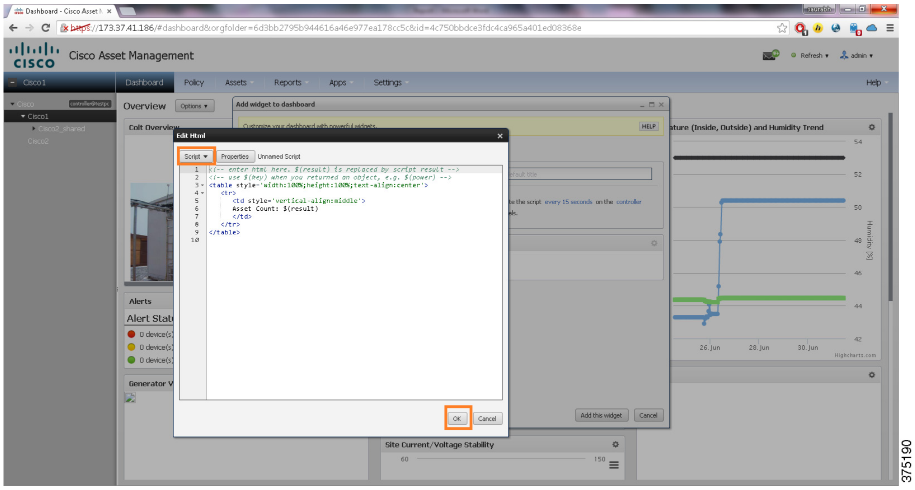
0 device(s) are OK

For this example, our script is as shown below:

```
function getdata(result) {
    var mydata=[];
    var test = result.result.data[0].items;
    for (var i=0; i<test.length; i++)
    {
        if (test[i].v!==0) {
           mydata.push([test[i].ts,parseFloat(test[i].v.toFixed(2))]);
                                 }
                 }
               return mydata;
  }

var result = [];
var res = api_get("/reports/json/votws?report=votws&comparable=false&options=Custom
Metric&metric0=c2b675a30f19401394722c4d82b9ec39_avg&segment0=id%3D09344b950ea8436aa285e0c5
2439152b dqllabel%3D\"Humidity
Inside\"&dtype=last7days&ds=&de=&hrsconsiderdaterange=0&granularity=&export=json&limit=und
efined&offset=undefined&orgfolder=8b013b6f09f0f57ad9273c4a5f8ad9e2&locale=en&tz=330&ts=e7b
d61d2b3fd9f9f41d6f9de238085be");
result.push({name: 'Humidity', data: getdata(res)});
res=api_get("/reports/json/votws?report=votws&comparable=false&options=CustomMetric&metric
0=8ccccca40a154682a02ab72dfa8489df_avg&segment0=type%3D\"owm.city\"dqllabel%3D\"Temp
Outside\"&dtype=last7days&ds=&de=&hrsconsiderdaterange=0&granularity=&export=json&limit=un
defined&offset=undefined&orgfolder=6d3bb2795b944616a46e977ea178cc5c&locale=en&tz=330&ts=27
3c5d5edd2ffde1d987a7daf784a0e5");
result.push({name: 'Temperature Outside', data: getdata(res)});
varres = api_get("/reports/json/votws?report=votws&comparable=false&options=
CustomMetric&metric0=8ccccca40a154682a02ab72dfa8489df_avg&segment0=id%3D9debdbc63e4848fd96
56afdd0ed79970%20dqllabel%3D\"Temperature
Inside\"&dtype=last7days&ds=&de=&hrsconsiderdaterange=0&granularity=&export=json&limit=und
efined&offset=undefined&orgfolder=6d3bb2795b944616a46e977ea178cc5c&locale=en&tz=330&ts=ad8
0c8a2b1573494406284933ae0b0b9");
result.push({name: 'Temperature Inside', data: getdata(res)});
return (JSON.stringify(result));
```

Step 5 Select **Layout** from **Widget Preview** (see Figure 4-36). Write html code in the layout window to create the layout (that is, how data looks on the dashboard) and click **OK**.

Figure 4-36 Edit html Window for Layout



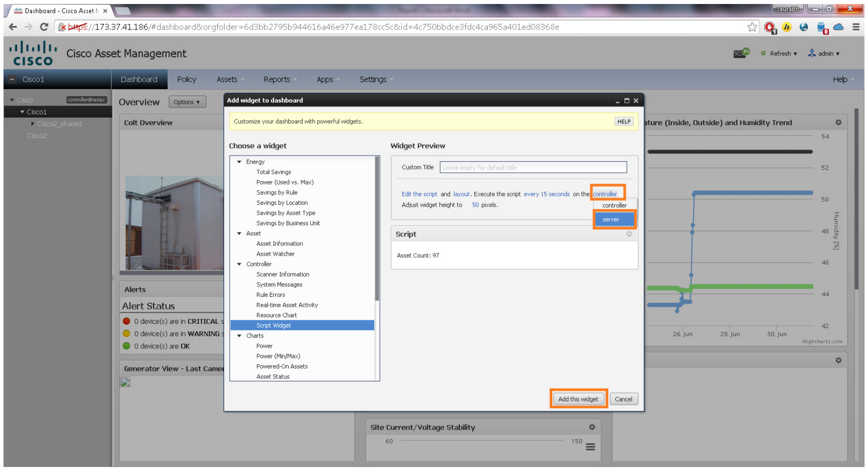
```
<!-- enter html here. $(result) is replaced by script result -->
<!-- use $(key) when you returned an object, e.g. $(power) -->
<table style='width:100%;height:100%;text-align:center'>
    <tr>
        <td style='vertical-align:middle'>
        Asset Count: $(result)
        </td>
    </tr>
</table>
```

For this example, the following is our html code for the layout:

```
<myscript4 style="display:none;">
var result = $(result);
var chart = new Highcharts.Chart({
       chart: {
           zoomType: 'x',
         renderTo : 'myHighChart4'
     },
     title: {
         text: ''
     },
    xAxis: {
    type: 'datetime',
    <!--minRange: 1 * 24 * 3600000 // fourteen days-->
  },
    yAxis: [{
        title: {
           text: 'Temperature [°F]'
        }
     },{
         title: {
              text: 'Humidity [%]'
         },
        opposite: true
     }],
    legend: {
        enabled: false
    },
  series: [
     {
        name: result[0].name,
       data: result[0].data,
        yAxis : 1
    },
     {
         name: result[1].name,
        data: result[1].data
     },
      {
        name: result[2].name,
       data: result[2].data
   }
    ]
  });
</myscript4>
<img src="/resource/pem/box_help.png" onload="eval($('myscript4').text());"
style="display:none">
<div id="myHighChart4"></div>
```

Step 6 Select **Server** from the **Write Preview** option and click the **Add Widget** button, as shown in Figure 4-37.

Figure 4-37 Selection of Server for Script Execution



Add widget to dashboard

Customize your dashboard with powerful widgets.

Widget Preview

Custom Title: Leave empty for default title

Edit the script and layout. Execute the script every 15 seconds on the controller

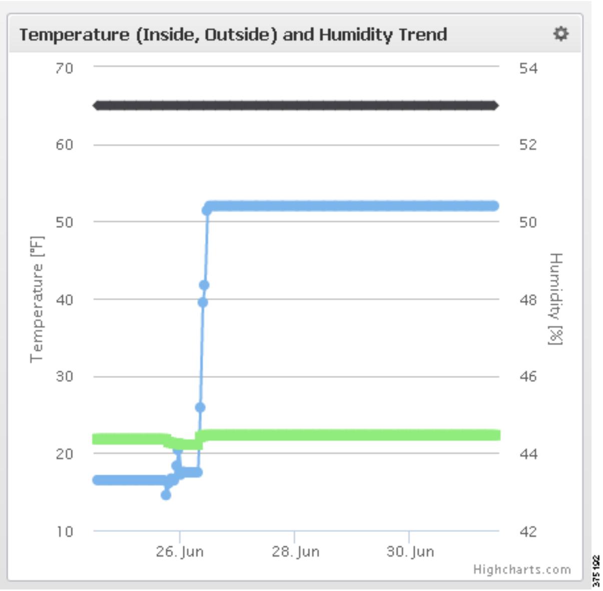
Adjust widget height to 50 pixels.

Script

Asset Count: 97

Figure 4-38 shows the widget.

Figure 4-38 Widget Output



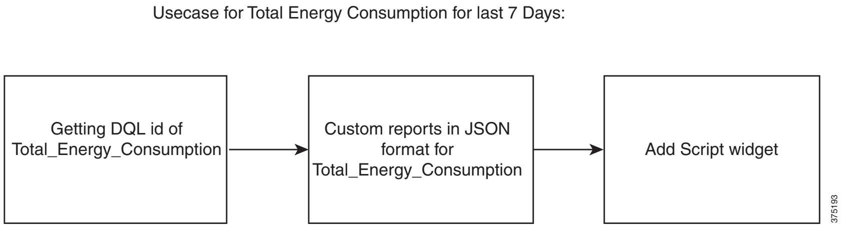
Dashboard Customization

This section covers some use cases of the dashboard.

Creating Total Energy Consumption

Figure 4-39 shows the flow for the use case for total energy consumption for the last seven days.

Figure 4-39 Use Case for Total Energy Consumption for Last 7 Days


Usecase for Total Energy Consumption for last 7 Days:
Getting DQL id of Total_Energy_Consumption
Custom reports in JSON format for Total_Energy_Consumption
Add Script widget
375193

Complete the following steps to create total energy consumptions for the last seven days:

Step 1 Create and save a custom report in JSON format for Total Energy Consumption for the last 7 days and create a user-defined widget. (For details, refer to "Prerequisite for creating Dashboard Use Cases" section).

Step 2 The following is the same script used in "Script" in "User-defined widget":

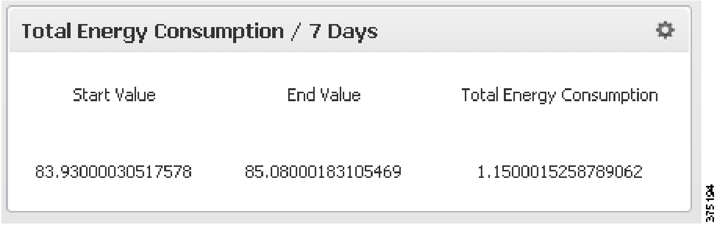
```
function getdata(res) {
              var test = res.result.data[0].items;
    var len = test.length;
    var minimum = test[0].v;
    var maximum = test[len-1].v;
    var data = '';
    var Diff = maximum - minimum;
    data = data+'<tr><td>'+minimum+'</td><td>'+maximum+'</td><td>'+ Diff +
'</td></tr>';
    return data;
}
var res =
api_get("/reports/json/votws?report=votws&comparable=false&options=CustomMetric&metric0=da
04469f3fd7490c9d4e0c16ce23375e_avg&segment0=id%3D609ebbbde68f4f618e4dfb9087543f85
dqllabel%3D\"Total Energy
Consumption\"&dtype=last7days&ds=&de=&hrsconsiderdaterange=0&granularity=&export=json&limi
t=undefined&offset=undefined&orgfolder=6d3bb2795b944616a46e977ea178cc5c&locale=en&tz=330&t
s=76421d403209fdea244f79cd6e139fac");
return getdata(res);
```

Step 3 The following html code is the same as that in the "Layout" section:

```
<table style='width:100%;height:100%;text-align:center'>
<tr>
        <td style='vertical-align:middle'>
        Start Value
        </td>
        <td style='vertical-align:middle'>
        End Value
        </td>
        </td>
        <td style='vertical-align:middle'>
        Total Energy Consumption
        </td>
    </tr>
$(result)
</table>
```

Step 4 Select **Server** for execution. shows the widget output.

Figure 4-40 Widget Output



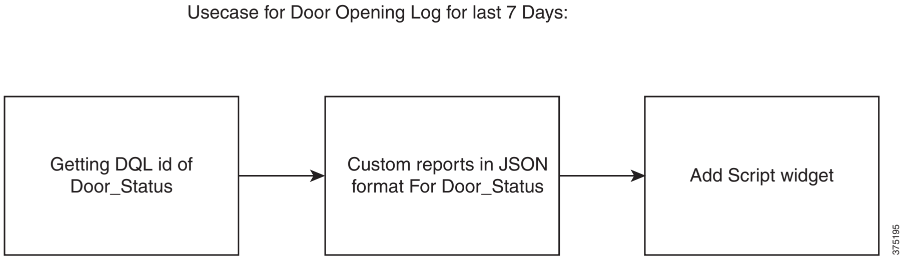
Total Energy Consumption / 7 Days

Start Value	End Value	Total Energy Consumption
83.93000030517578	85.08000183105469	1.1500015258789062

Door Opening Log for the Last Seven Days

Figure 4-41 shows the flow of the use case for door opening log for the last seven days.

Figure 4-41 Use Case for Door Opening Log for Last 7 Days


Usecase for Door Opening Log for last 7 Days:
Getting DQL id of Door_Status
Custom reports in JSON format For Door_Status
Add Script widget
375195

Complete the following steps to create a door opening log for last 7 days:

Step 1 Create and save a custom report in the JSON format for the door opening log for the last 7 days and create a user-defined widget. (For detail, refer to "Prerequisite for creating Dashboard use cases".)

Step 2 The following is the same script as that used in “Script" in "User-defined widget":

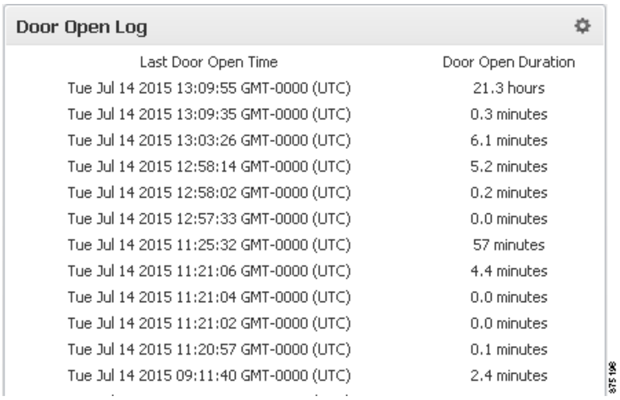
```
var dev1={ "id":"6f750e670f224d6083a728eae82e5d66","property":"value"}
var result = [];
var mystr = '';
function getdata(device) {
    var resp =
api_get("/objectstore/items/"+device.id+"/history?property="+device.property+"&deviceid="+
device.id+"&limit=1000");
    var data = '';
    var endtime = 0;
    var starttime = 0;
    var trigger = 0;
    for (i=resp.result.length-1; i>-1; i--) {
       if (resp.result[i].json[device.property]!=='') {
                    var state=resp.result[i].json[device.property];
          //1-closed, 0-open 1 1 1 0
          var time=resp.result[i].d;
           if (state == 1 && trigger === 0) {
                 endtime = time;
                     }
           if (state === 0){
                 starttime = time;
                 trigger = 1;
           }
           if (trigger == 1 && state ==1) {
                 trigger = 0;
                 var timediff = endtime-starttime;
                 timediff=timediff/(1000*60);
                 if (timediff < 10) {
                    timediff = timediff.toFixed(1)+' minutes';
                 } else if (timediff < 60) {
                    timediff  = timediff.toFixed(0)+' minutes';
                 } else {
                    timediff = timediff/60;
                    timediff = timediff.toFixed(1)+' hours';
                 }
                 data=data+'<tr><td>'+Date(starttime)+'</td><td>'+
            +timediff+'</td></tr>';
                 endtime = time;
           }
       }
    }
    return data;
}
return getdata(dev1);
```

Step 3 The following code is the same html code used in the "Layout" section:

```
<table style='width:100%;height:100%;text-align:center'>
<tr>
        <td style='vertical-align:middle'>
        Last Door Open Time
        </td>
        <td style='vertical-align:middle'>
        Door Open Duration
        </td>
    </tr>
$(result)
</table>
```

Step 4 Select Server for execution. Figure 4-42 shows the widget output.

Figure 4-42 Widget Output



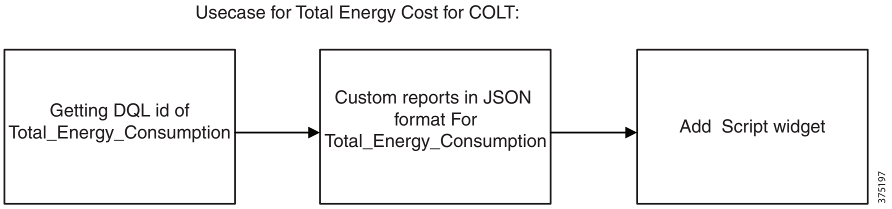
Door Open Log

Last Door Open Time	Door Open Duration
Tue Jul 14 2015 13:09:55 GMT-0000 (UTC)	21.3 hours
Tue Jul 14 2015 13:09:35 GMT-0000 (UTC)	0.3 minutes
Tue Jul 14 2015 13:03:26 GMT-0000 (UTC)	6.1 minutes
Tue Jul 14 2015 12:58:14 GMT-0000 (UTC)	5.2 minutes
Tue Jul 14 2015 12:58:02 GMT-0000 (UTC)	0.2 minutes
Tue Jul 14 2015 12:57:33 GMT-0000 (UTC)	0.0 minutes
Tue Jul 14 2015 11:25:32 GMT-0000 (UTC)	57 minutes
Tue Jul 14 2015 11:21:06 GMT-0000 (UTC)	4.4 minutes
Tue Jul 14 2015 11:21:04 GMT-0000 (UTC)	0.0 minutes
Tue Jul 14 2015 11:21:02 GMT-0000 (UTC)	0.0 minutes
Tue Jul 14 2015 11:20:57 GMT-0000 (UTC)	0.1 minutes
Tue Jul 14 2015 09:11:40 GMT-0000 (UTC)	2.4 minutes

Total Energy Cost for COLT

Figure 4-43 shows the flow of the use case for the total energy cost for COLT.

Figure 4-43 Use Case for Total Energy Cost for COLT


Usecase for Total Energy Cost for COLT:
Getting DQL id of Total_Energy_Consumption
Custom reports in JSON format For Total_Energy_Consumption
Add Script widget
375197

Complete the following steps to create the total energy cost for COLT:

Step 1 Create and save a custom report in JSON format for the total energy consumption for the last 30 days and create a user-defined widget. (For details, refer to "Prerequisite for creating Dashboard use cases".)

Step 2 The following is the same script as the one used in "Script" in "User-defined widget":

```
Var
res=api_get("/reports/json/votws?report=votws&comparable=false&options=CustomMetric&metric
0=da04469f3fd7490c9d4e0c16ce23375e_avg&segment0=id%3D609ebbbde68f4f618e4dfb9087543f85%20dq
llabel%3D\"Total%20Energy%20Consumption\"&dtype=last30days&ds=&de=&hrsconsiderdaterange=0&
granularity=&export=json&limit=undefined&offset=undefined&orgfolder=8b013b6f09f0f57ad9273c
4a5f8ad9e2&locale=en&tz=330&ts=500e55c9e8644a91f03dfcb96f95f58d");
var test = res.result.data[0].items;
var len = test.length;
var minimum = test[0].v;
var maximum = test[len-1].v;
var kwh=maximum - minimum;
var monthly =kwh*0.25;
monthly = parseFloat(monthly).toFixed(2);
var daily = monthly/30;
daily = parseFloat(daily).toFixed(2);
var weekly = daily * 7;
return "Long Beach Total Cost For 30 Days: $ "+ monthly +" <br /> weekly estimated Cost: $
"+weekly+" <br /> Daily estimated Cost: k$ "+daily;
```

Step 3 The following is the same html code as the code used in "Layout":

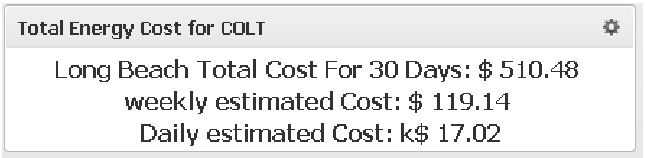
```
<table style='width:100%;height:100%;text-align:center'>
    <tr>
```

```
        <td style='vertical-align:middle'>
        <div style='font-size:16px;font-weight:bold'>$(result)</div>
        </td>
    </tr>
</table>
```

Step 4 Select **Server** for execution.

Figure 4-44 shows the widget output.

Figure 4-44 Widget Output



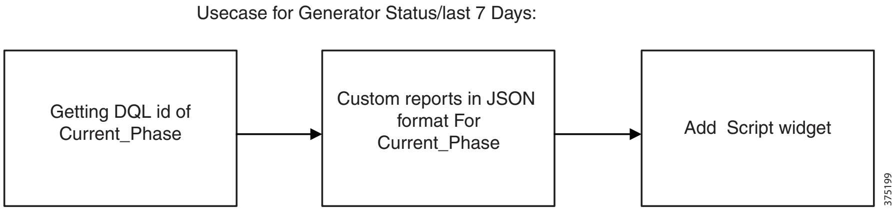
Total Energy Cost for COLT

Long Beach Total Cost For 30 Days: $ 510.48
weekly estimated Cost: $ 119.14
Daily estimated Cost: k$ 17.02

Generator Status for the Last Seven Days

Figure 4-45 shows the flow of the use case for the generator status for the last seven days.

Figure 4-45 Use Case for Generator Status for the Last Seven Days


Usecase for Generator Status/last 7 Days:
Getting DQL id of Current_Phase
Custom reports in JSON format For Current_Phase
Add Script widget
375199

Complete the following steps for the generator status for the last seven days:

Step 1 Create and save a custom report in JSON format for the total energy consumption for the last 30 days and create a user-defined widget. (For details, refer to "Prerequisite for creating Dashboard use cases" section.)

Step 2 The following script is the same that is used in "Script" section in "User-defined widget":

```
function getdata(result){
              var data = '';
    var onStartTime = 0;
               var onEndTime = 0;
    var offStartTime = 0;
    var offEndTime = 0;
    var timeDiff = 0;
    var trigger = 0;
    // TRIGER .... 1 for ON, 2 for OFF
    var test = result.result.data[0].items;
    for (i=0; i<test.length; i++)
    {
        if(test[i].v !== 0 && trigger === 0){
           onStartTime = test[i].ts;
           trigger = 1;
        }
        if(test[i].v === 0 && trigger === 0){
           offStartTime = test[i].ts;
                     trigger = 2;
        }
```

```
           if(test[i].v === 0 && trigger === 1){
           onEndTime = test[i].ts;
           timeDiff = (onEndTime - onStartTime)/(1000*60);
           if (timeDiff < 10) {
                    timeDiff = timeDiff.toFixed(1)+' minutes';
                 }
           else if (timeDiff < 60) {
                    timeDiff  = timeDiff.toFixed(0)+' minutes';
                 }
           else {
                    timeDiff = timeDiff/60;
                    timeDiff = timeDiff.toFixed(1)+' hours';
                 }
         data = data+'<tr><td>'+"ON"
+'</td><td>'+Date(onStartTime)+'</td><td>'+Date(onEndTime)+ '</td><td>'+
timeDiff+'</td></tr>';
        offStartTime = onEndTime;
        trigger = 2;
        }
         if(test[i].v !== 0 && trigger === 2){
           offEndTime = test[i].ts;
           timeDiff = (offEndTime - offStartTime)/(1000*60);
           if (timeDiff < 10) {
                    timeDiff = timeDiff.toFixed(1)+' minutes';
                 }
         else if (timeDiff < 60) {
                    timeDiff  = timeDiff.toFixed(0)+' minutes';
                 }
        else {
                    timeDiff = timeDiff/60;
                    timeDiff = timeDiff.toFixed(1)+' hours';
                 }
        data = data+'<tr><td>'+"OFF"
+'</td><td>'+Date(offStartTime)+'</td><td>'+Date(offEndTime)+'</td><td>'+
timeDiff+'</td></tr>';
        onStartTime = offEndTime;
            trigger = 1;
        }
    if(i === test.length-1){
            if(test[i].v === 0){
                data = data+'<tr><td>'+"OFF" +'</td><td>'+ Date(offStartTime) +'
</td></tr>';
            }
            if(test[i].v !== 0){
                data = data+'<tr><td>'+"ON" +'</td><td>' +Date(onStartTime) +
'</td></tr>';
            }
        }
    }
    return data;
}
var
res=api_get("/reports/json/votws?report=votws&comparable=false&options=CustomMetric&metric
0=da04469f3fd7490c9d4e0c16ce23375e_avg&segment0=id%3Db90fc0f7dfa347a08cc8e6a5d90059b7
dqllabel%3D\"current
phase\"&dtype=last7days&ds=&de=&hrsconsiderdaterange=0&granularity=&export=json&limit=unde
fined&offset=undefined&orgfolder=6d3bb2795b944616a46e977ea178cc5c&locale=en&tz=330&ts=ae4b
9b6e0d37e265e9088fb8512c1072");
return getdata(res);
```

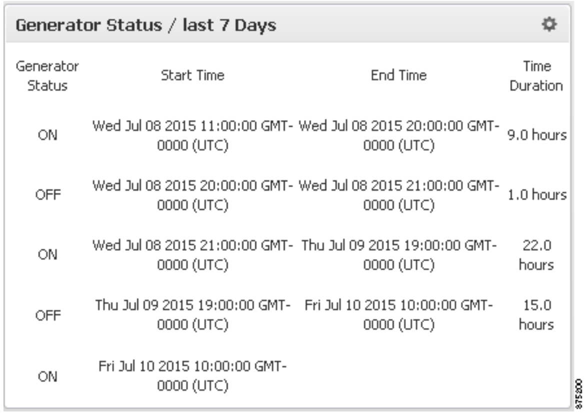
Step 3 The following html code is the same code used in "Layout":

```
<table style='width:100%;height:100%;text-align:center'>
<tr>
        <td style='vertical-align:middle'>
        Generator Status
        </td>
        <td style='vertical-align:middle'>
        Start Time
        </td>
        <td style='vertical-align:middle'>
        End Time
        </td>
        </td>
        <td style='vertical-align:middle'>
        Time Duration
        </td>
    </tr>
$(result)
</table>
```

Step 4 Select **Server** for execution.

Figure 4-46 shows the widget output.

Figure 4-46 Widget Output



Generator Status / last 7 Days

Generator Status	Start Time	End Time	Time Duration
ON	Wed Jul 08 2015 11:00:00 GMT-0000 (UTC)	Wed Jul 08 2015 20:00:00 GMT-0000 (UTC)	9.0 hours
OFF	Wed Jul 08 2015 20:00:00 GMT-0000 (UTC)	Wed Jul 08 2015 21:00:00 GMT-0000 (UTC)	1.0 hours
ON	Wed Jul 08 2015 21:00:00 GMT-0000 (UTC)	Thu Jul 09 2015 19:00:00 GMT-0000 (UTC)	22.0 hours
OFF	Thu Jul 09 2015 19:00:00 GMT-0000 (UTC)	Fri Jul 10 2015 10:00:00 GMT-0000 (UTC)	15.0 hours
ON	Fri Jul 10 2015 10:00:00 GMT-0000 (UTC)		

Camera View - Generator

Complete the following steps to create a camera view-generator widget:

Step 1 Get DQL id of "Camera View - Generator" and create a "User-defined widget", for details, refer "Prerequisite for creating dashboard use case" section. In this case, no need of "custom report".

Step 2 Step 2Script used for "Script" section in "User-defined widget:

```
return sysget("image_52bdbaafdb0148cc96c968484c782aac");
// "52bdbaafdb0148cc96c968484c782aac" is DQL ID.
```

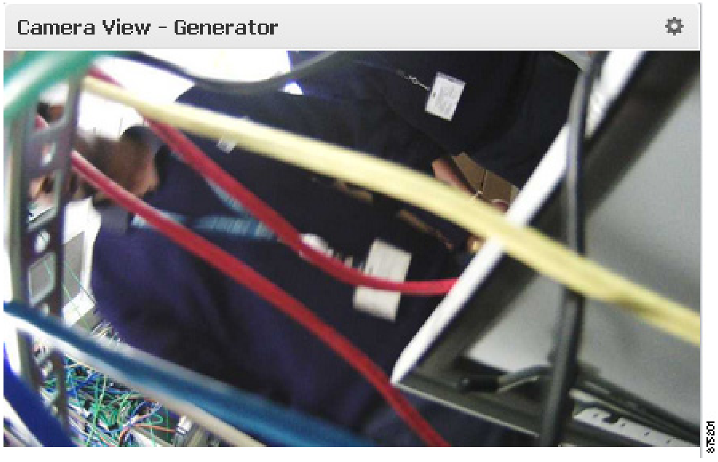
Step 3 Step 3Html code used for "Layout" section:

```
<img src="data:image/jpeg;base64,$(result)" style="width:100%">
```

Step 4 Select **Controller** for execution.

Figure 4-47 shows the widget output.

Figure 4-47 Widget Output



Camera View - Alley 1

Complete the following steps to create a camera view-alley 1 widget:

Step 1 Get the DQL ID of Camera View - Alley 1 and create a User-defined widget. For details, refer to "Prerequisite for creating dashboard use case".

Step 2 The following script is the script that was used in "Script" in "User-defined widget":

```
return sysget("image_261d75326d424e0db64b7890d2ea98ff");
// "261d75326d424e0db64b7890d2ea98ff" is DQL ID.
```

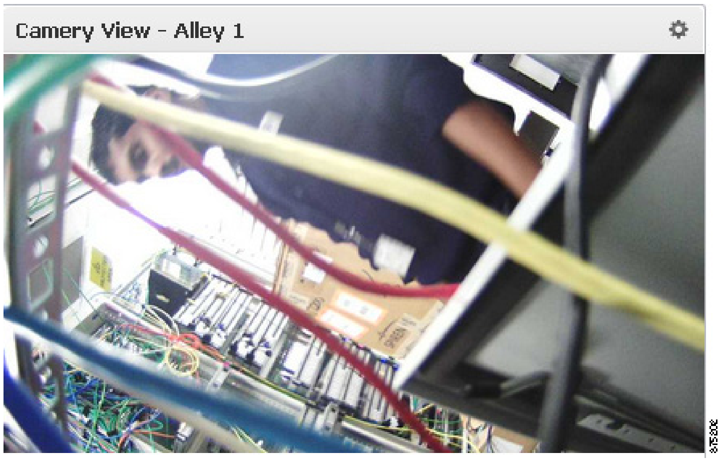
Step 3 The following script is the script that was used in "Layout":

```
<img src="data:image/jpeg;base64,$(result)" style="width:100%">
```

Step 4 Select **Controller** for execution.

Figure 4-48 shows the widget output.

Figure 4-48 Widget Output

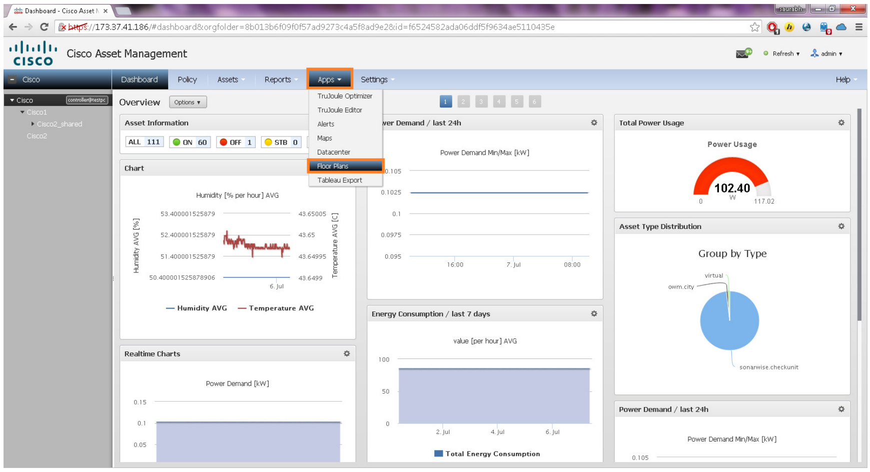


Floor Plan

Complete the following steps to add the temperature outside, temperature inside, and humidity to the floor plan:

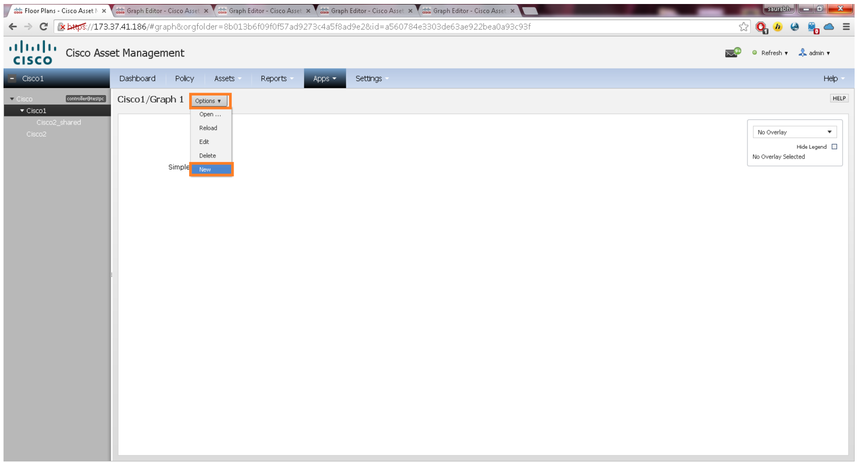
Step 1 Select **Floor Plans** from the **Apps** menu, as shown Figure 4-49.

Figure 4-49 Selection of Floor Plans



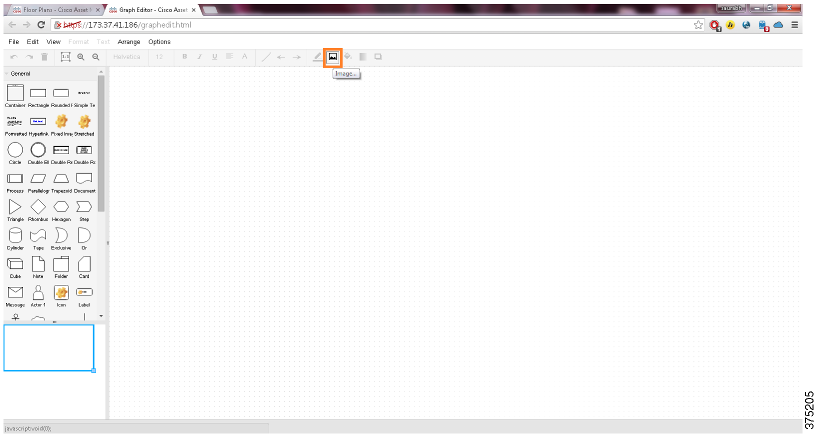
Step 2 Select **New** from **Options**. The graph edit section appears in a new tab window, as shown in .

Figure 4-50 Addition of New Graph



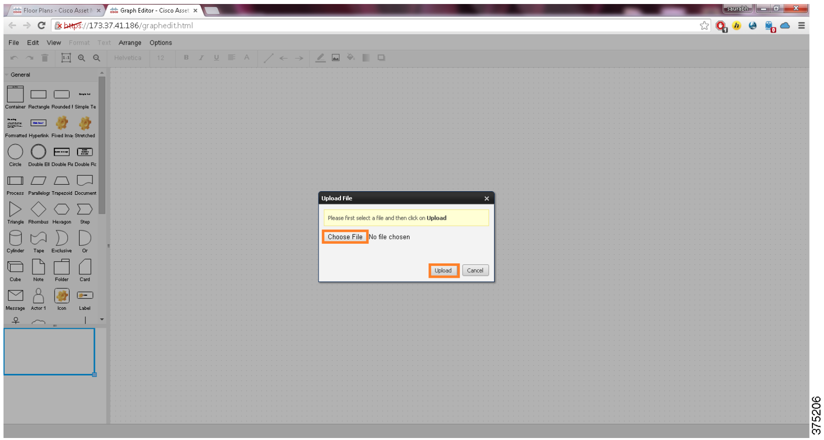
Step 3 Select **Image** upload an image, as shown in Figure 4-51.

Figure 4-51 Selection of Images


Floor Plans - Cisco Asset
Graph Editor - Cisco Asset
https://173.37.41.186/graphedit.html
File Edit View Format Text Arrange Options
Helvetica
12
Image...
General
Container Rectangle Rounded Simple Te
Formatted Hyperlink Fixed Ima Stretched
Circle Double Ell Double Re Double Re
Process Parallelogr Trapezoid Document
Triangle Rhombus Hexagon Step
Cylinder Tape Exclusive Or
Cube Note Folder Card
Message Actor 1 Icon Label
javascript:void(0);
375205

Step 4 Select **Choose File** and upload image, as shown in Figure 4-52.

Figure 4-52 Selection of Images from Stored Database

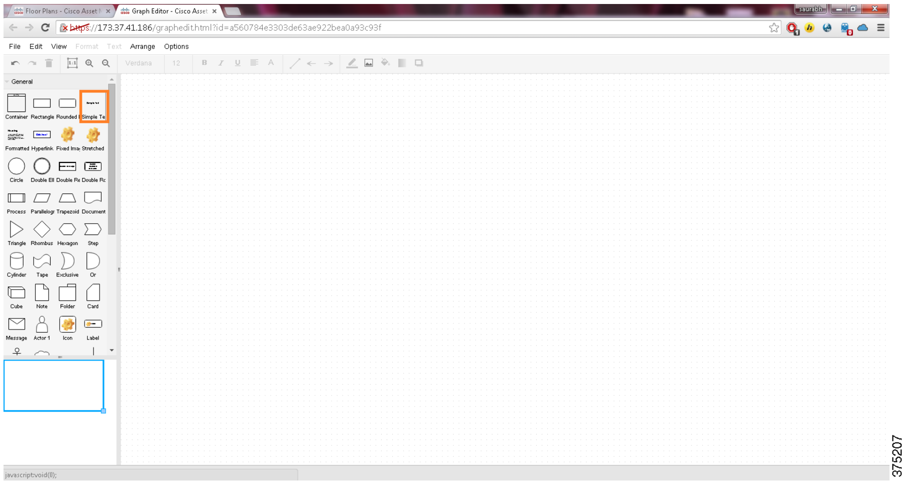

Floor Plans - Cisco Asset
Graph Editor - Cisco Asset
https://173.37.41.186/graphedit.html
File Edit View Format Text Arrange Options
General
Upload File
Choose File
Upload
Cancel
375206

Please first select a file and then click on **Upload**

No file chosen

Step 5 Drag **Simple Text** and drop it in the graph area, as shown in Figure 4-53. We can write texts or get the asset values by dragging and dropping Simple Text.

Figure 4-53 Selection of Simple Text


Floor Plans - Cisco Asset
Graph Editor - Cisco Asset
https://173.37.41.186/graphedit.html?id=a560784e9303de63ae922bea0a93c93f
File Edit View Format Text Arrange Options
Verdana
12
General
Container Rectangle Rounded Simple Te
Formatted Hyperlink Fixed Ima Stretched
Circle Double Ell Double Re Double Re
Process Parallelogr Trapezoid Document
Triangle Rhombus Hexagon Step
Cylinder Tape Exclusive Or
Cube Note Folder Card
Message Actor 1 Icon Label
javascript:void(0);
375207

Step 6 Right-click on **Simple text** and select **Properties,** as shown in Figure 4-54. The Edit Properties window appears, as shown in Figure 4-55.

Figure 4-54 Selection of Properties of Simple Text

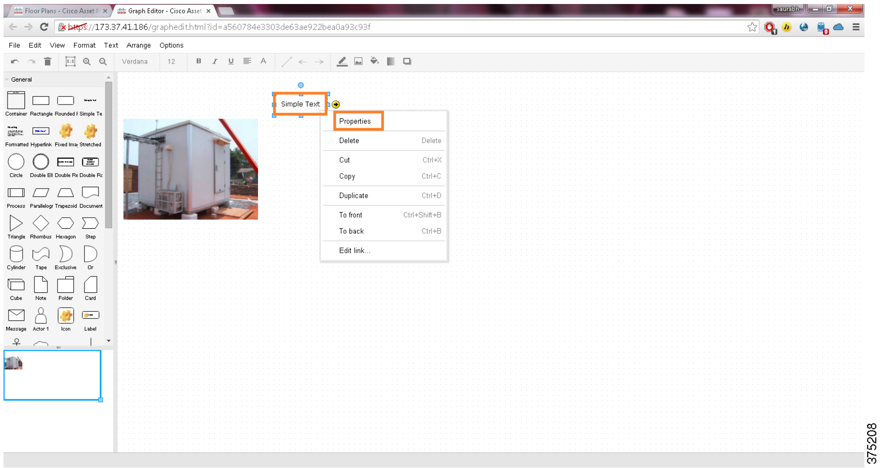
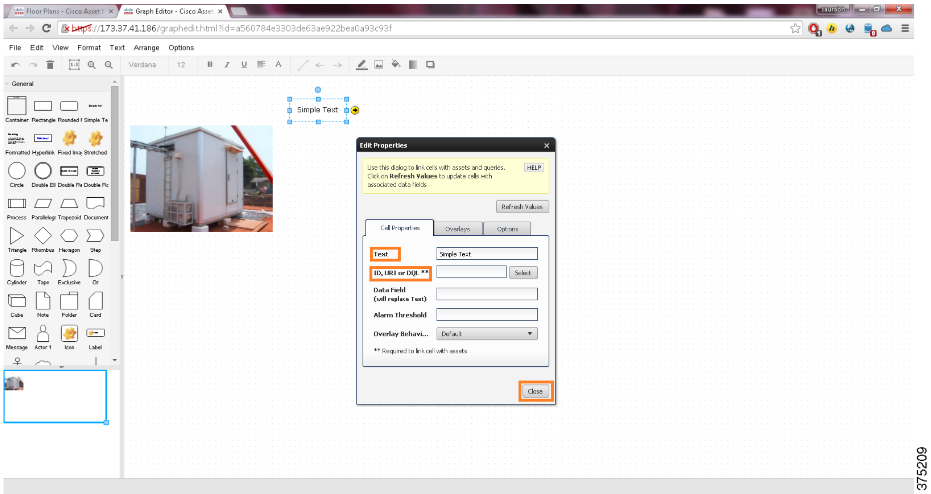

Floor Plans - Cisco Asset
Graph Editor - Cisco Asset
https://173.37.41.186/graphedit.html?id=a560784e3303de63ae922bea0a93c93f
File Edit View Format Text Arrange Options
Verdana 12
General
Simple Text
Properties
Delete Delete
Cut Ctrl+X
Copy Ctrl+C
Duplicate Ctrl+D
To front Ctrl+Shift+B
To back Ctrl+B
Edit link...
375208

Figure 4-55 Create Properties Based on Text or DQL ID


Floor Plans - Cisco Asset
Graph Editor - Cisco Asset
https://173.37.41.186/graphedit.html?id=a560784e3303de63ae922bea0a93c93f
File Edit View Format Text Arrange Options
Simple Text
Edit Properties
HELP
Refresh Values
Cell Properties
Overlays
Options
Select
Close
375209

Use this dialog to link cells with assets and queries. Click on **Refresh Values** to update cells with associated data fields

Text: Simple Text
ID, URI or DQL **:
Data Field (will replace Text):
Alarm Threshold:
Overlay Behavi...: Default

** Required to link cell with assets

Step 7 Type **text** in the **Text** section based requirements. To get the Asset Value, type the DQL ID of the asset in the **ID, URI or DQL**** section. (For the DQL ID, refer to the get DQL ID of Asset section).

In this example, we need to get three asset values. We select the **Text** section to enter the asset name and unit, and select the **ID** section to choose an asset.

Step 8 Select **Save** from the **File** menu and save the floor plan, as shown in Figure 4-56. The Graph Settings window appears. Enter the floor plan name in the **Name** section, select a folder from the **Folder** section and click **Save** to save this floor plan, as shown in Figure 4-57.

Figure 4-56 Save the Graph

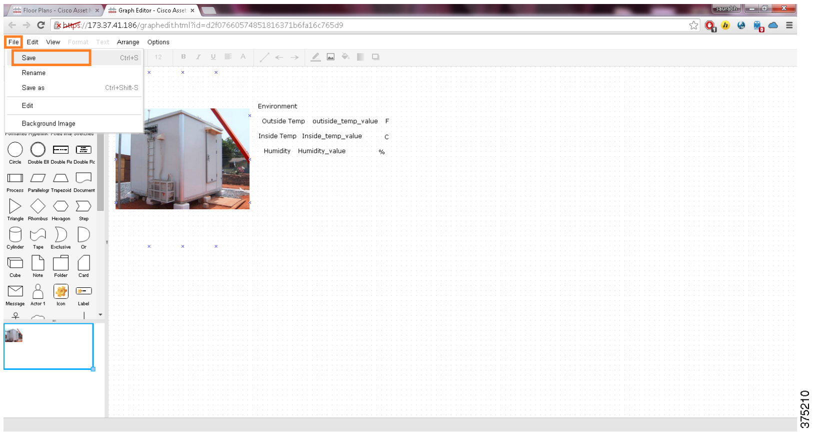
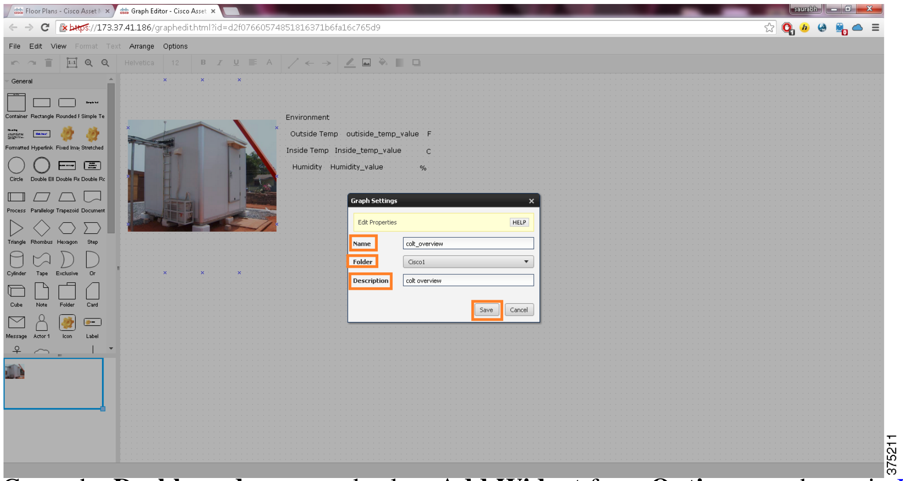


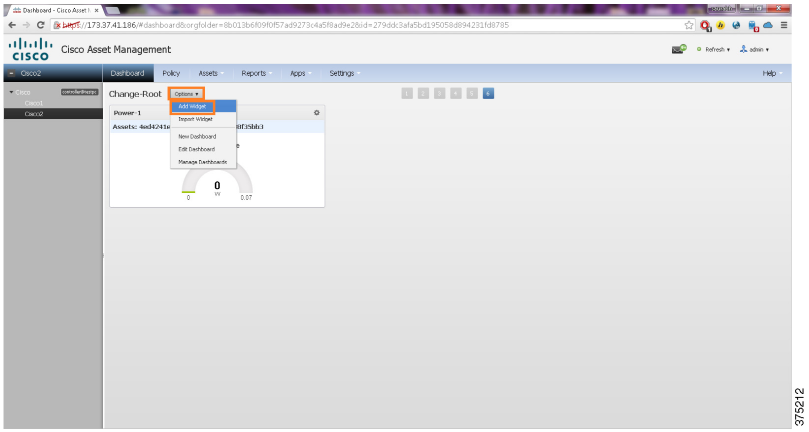
Figure 4-57 Save the Graph in a Specific Folder



Name: colt_overview
Folder: Cisco1
Description: colt overview

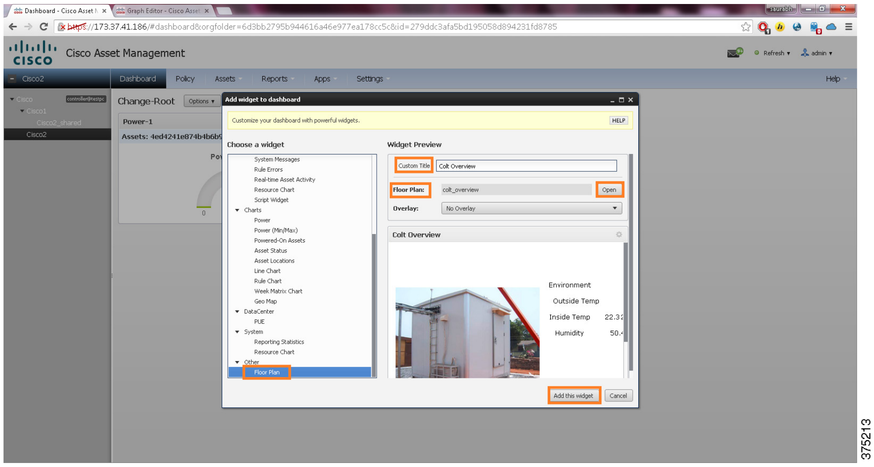
Step 9 Go to the **Dashboard** menu and select **Add Widget** from **Options**, as shown in Figure 4-58.

Figure 4-58 Selection of Add Widget in the Dashboard



Step 10 Select **Floor Plan** from the **Choose a Widget** section. In **Widget Preview**, enter a custom title, select a floor plan and choose **Add this widget** in the Dashboard, as shown in .

Figure 4-59 Selection of Floor Plan



Custom Title: Colt Overview

Floor Plan: colt_overview

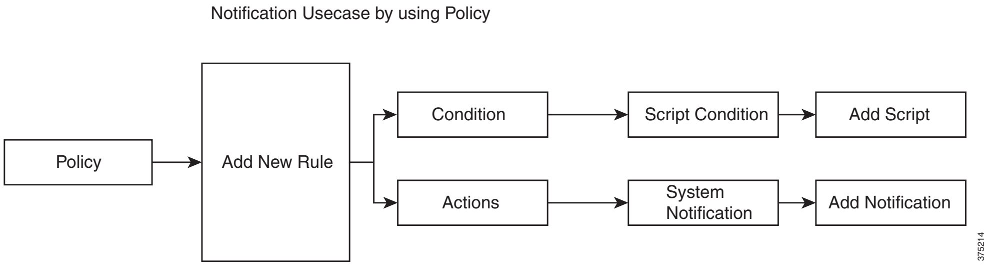
Overlay: No Overlay

Reports Customization

In this section, policy and send notifications are created based on requirements.

Figure 4-60 shows the notification use case by clicking the Policy menu.

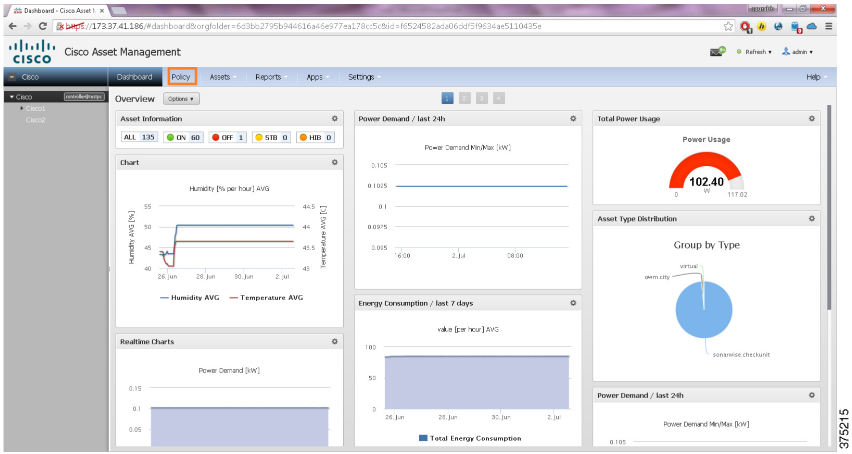
Figure 4-60 Notification Use Case by using Policy



Complete the following steps to create a notification through the Policy menu:

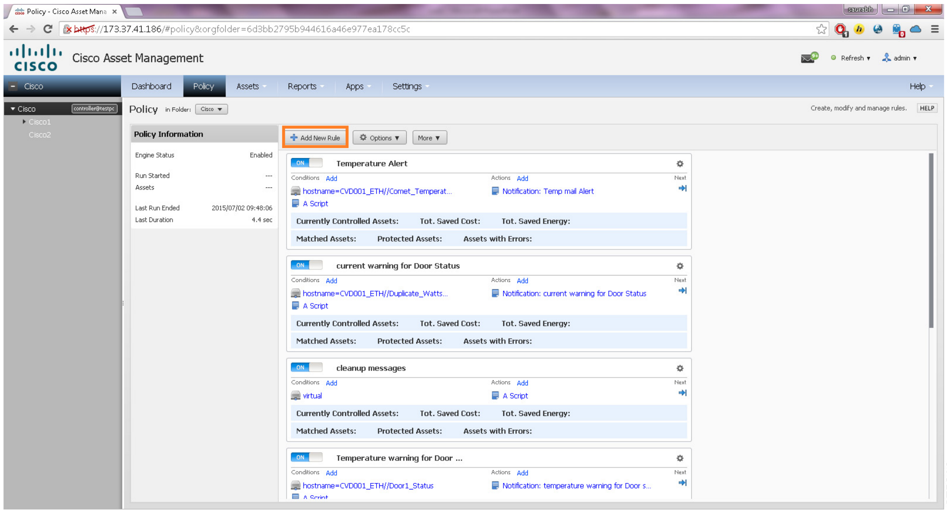
Step 1 Click on the **Policy** menu, as shown in Figure 4-61.

Figure 4-61 Selection of Policy



Step 2 Click on **Add New Rule**, as shown in Figure 4-62.

Figure 4-62 Selection of Add New Rule



Policy Information

Engine Status Enabled

Run Started ---

Assets ---

Last Run Ended 2015/07/02 09:48:06

Last Duration 4.4 sec

Temperature Alert
- hostname=CVD001_ETH//Comet_Temperat...
- A Script
- Notification: Temp mail Alert

Currently Controlled Assets: Tot. Saved Cost: Tot. Saved Energy:
Matched Assets: Protected Assets: Assets with Errors:

current warning for Door Status
- hostname=CVD001_ETH//Duplicate_Watts...
- A Script
- Notification: current warning for Door Status

Currently Controlled Assets: Tot. Saved Cost: Tot. Saved Energy:
Matched Assets: Protected Assets: Assets with Errors:

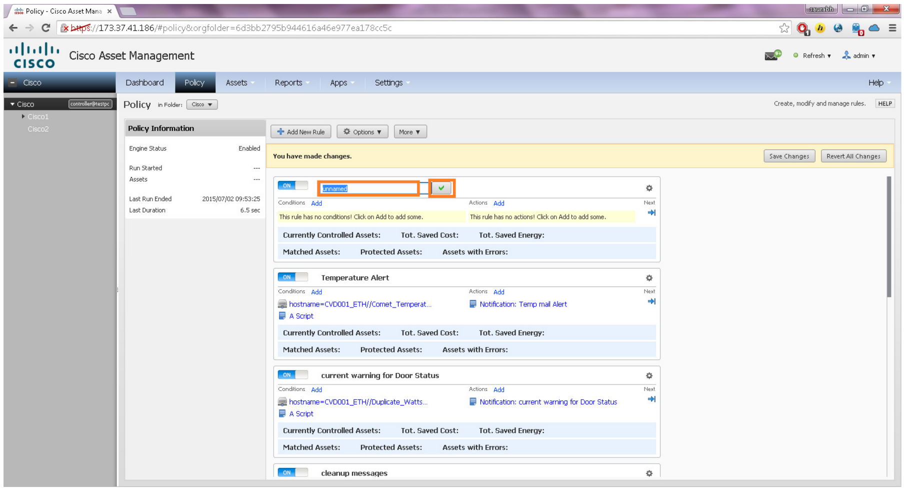
cleanup messages
- virtual
- A Script

Currently Controlled Assets: Tot. Saved Cost: Tot. Saved Energy:
Matched Assets: Protected Assets: Assets with Errors:

Temperature warning for Door ...
- hostname=CVD001_ETH//Door1_Status
- A Script
- Notification: temperature warning for Door s...

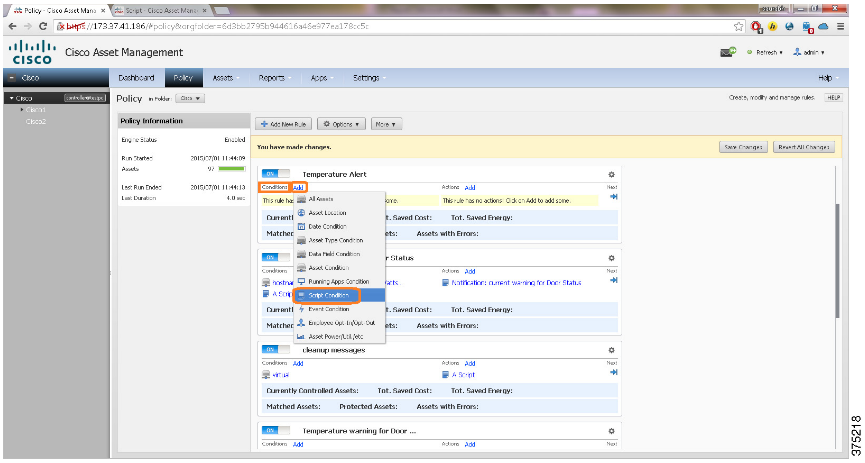
Step 3 Enter the policy name in the given area (for example Temperature Alert), as shown in Figure 4-63.

Figure 4-63 Define New Policy Name


Policy - Cisco Asset Mana
https://173.37.41.186/#policy&orgfolder=6d3bb2795b944616a46e977ea178cc5c
Cisco Asset Management
Refresh
admin
Cisco
Dashboard
Policy
Assets
Reports
Apps
Settings
Help
Policy in Folder: Cisco
Create, modify and manage rules.
HELP
Policy Information
Engine Status Enabled
Run Started ---
Assets ---
Last Run Ended 2015/07/02 09:53:25
Last Duration 6.5 sec
Add New Rule
Options
More
You have made changes.
Save Changes
Revert All Changes
ON
unnamed
Conditions Add
Actions Add
Next
This rule has no conditions! Click on Add to add some.
This rule has no actions! Click on Add to add some.
Currently Controlled Assets:
Tot. Saved Cost:
Tot. Saved Energy:
Matched Assets:
Protected Assets:
Assets with Errors:
Temperature Alert
hostname=CVD001_ETH//Comet_Temperat...
A Script
Notification: Temp mail Alert
current warning for Door Status
hostname=CVD001_ETH//Duplicate_Watts...
Notification: current warning for Door Status
cleanup messages
375217

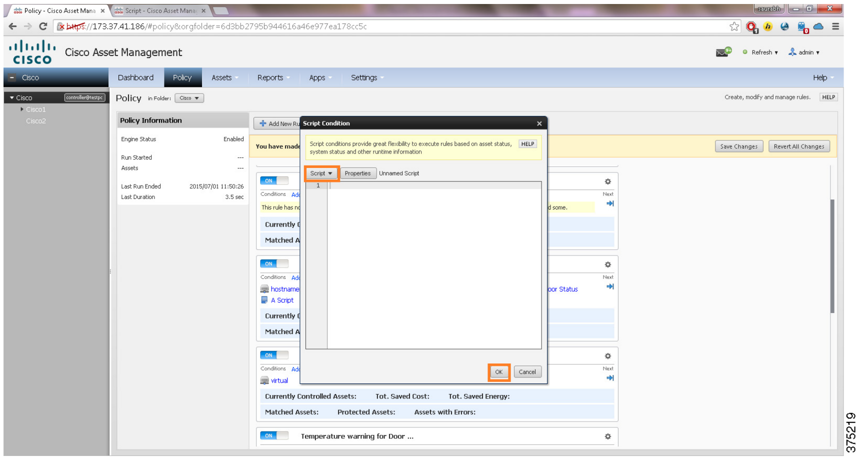
Step 4 Add conditions in the policy. In the **Condition** option, select **Script Condition** from the **Add** drop-down list. The Script Condition appears, as shown in Figure 4-64.

Figure 4-64 Selection of Script Condition



Step 5 Enter **script** in the **Script** section and select **OK**, as shown in Figure 4-65.

Figure 4-65 Script Condition Window

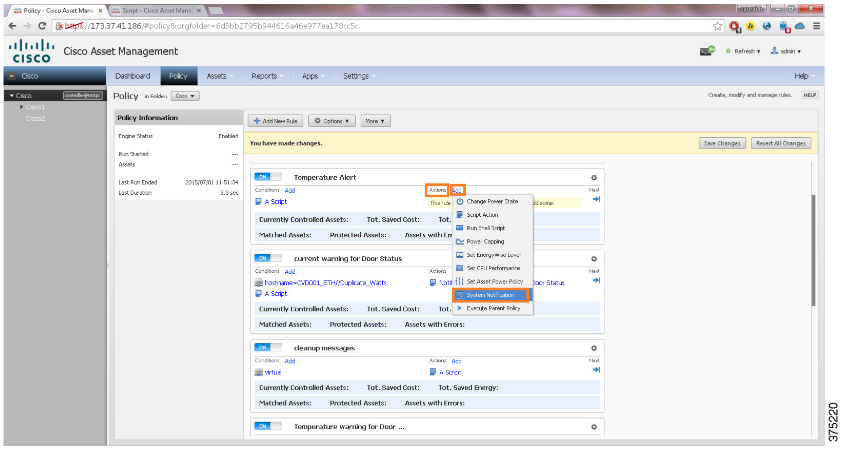


For example, the following script configures the temperature alert to be sent out with condition of temperature value is either less than 10 or greater than 50:

```
// id is DQL ID of Temperature Asset sensor.
var id="9debdbc63e4848fd9656afdd0ed79970";
// fetching the current value of the asset.
var res = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id") +
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
res1=JSON.parse(res);
temperature = res1.result.state.value;
// Condition defined
if (temperature < 10 || temperature >50){
   return true;
}
else{
   return false;
}
```

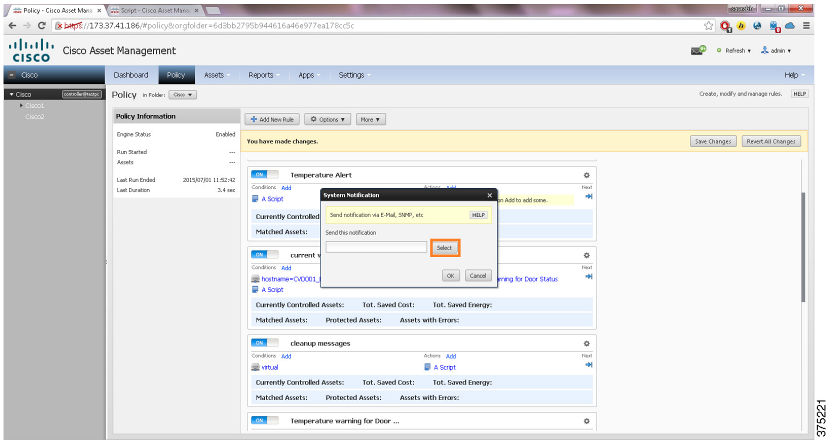
Step 6 Add an action for your policy by selecting **Actions** and **System Notification** from the **Add** drop-down option, as shown in Figure 4-66. The System Notification window appears.

Figure 4-66 Selection of Script Notification



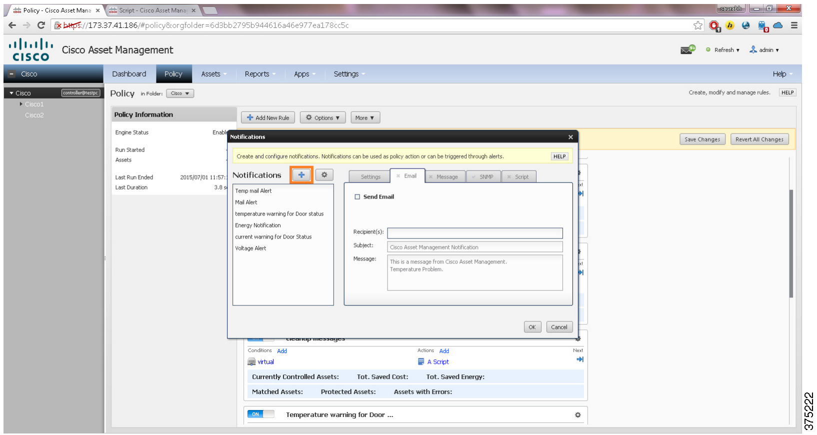
Step 7 Click on the **Select** button in the System Notification window shown in Figure 4-67. The Notification window appears.

Figure 4-67 System Notification Window



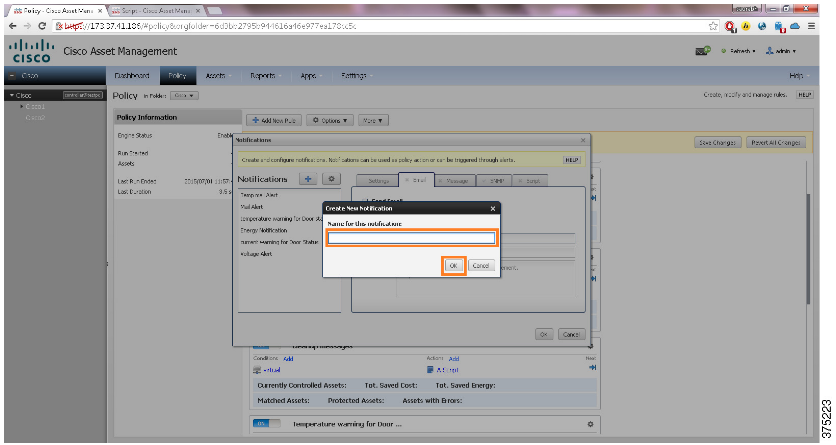
Step 8 Select the + button, as shown in Figure 4-68. The Create New Notification window appears.

Figure 4-68 Creation of New Notification


Cisco Asset Management
Notifications
Create and configure notifications. Notifications can be used as policy action or can be triggered through alerts.
HELP
Notifications
Settings
Email
Message
SNMP
Script
Temp mail Alert
Mail Alert
temperature warning for Door status
Energy Notification
current warning for Door Status
Voltage Alert
Send Email
Recipient(s):
Subject:
Cisco Asset Management Notification
Message:
This is a message from Cisco Asset Management. Temperature Problem.
OK
Cancel
375222

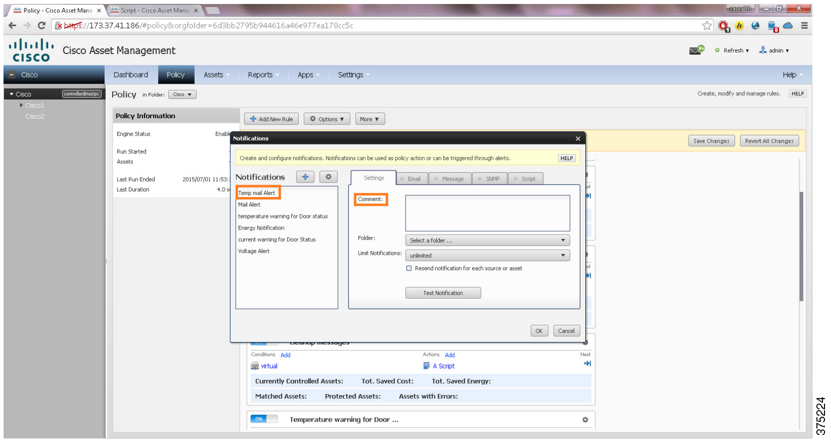
Step 9 Enter the condition name in the **Name for this Notification** area, for example, Temperature Alert, and select **OK**, as shown in Figure 4-69.

Figure 4-69 Creation of the Name of the Notification



Step 10 Select **Notification Name** from the **Notification** option. Put comments in the **Comment** area under the **Setting** option, as shown in Figure 4-70.

Figure 4-70 Creation of Comment for Notification



Notifications

Create and configure notifications. Notifications can be used as policy action or can be triggered through alerts. HELP

Notifications

Temp mail Alert
Mail Alert
temperature warning for Door status
Energy Notification
current warning for Door Status
Voltage Alert

Settings | Email | Message | SNMP | Script

Comment:

Folder: Select a folder ...

Limit Notifications: unlimited

□ Resend notification for each source or asset

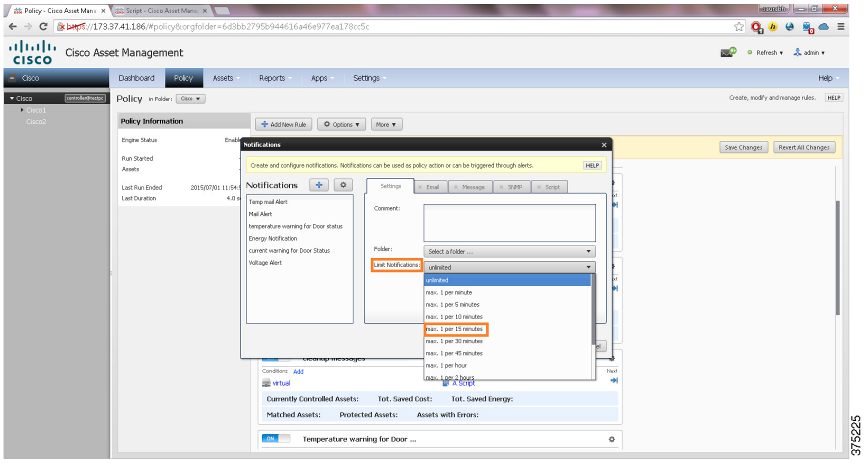
Test Notification

OK Cancel

Cisco Asset Management
Dashboard
Policy
Assets
Reports
Apps
Settings
Help
Policy Information
Add New Rule
Options
More
Save Changes
Revert All Changes
Currently Controlled Assets: Tot. Saved Cost: Tot. Saved Energy:
Matched Assets: Protected Assets: Assets with Errors:
Temperature warning for Door ...
375224

Step 11 Select the maximum number of notifications required in a fixed time from the **Limit Notification** option, as shown in Figure 4-71.

Figure 4-71 Selection of Limit Notification



Notifications

Create and configure notifications. Notifications can be used as policy action or can be triggered through alerts. HELP

Notifications

Temp mail Alert
Mail Alert
temperature warning for Door status
Energy Notification
current warning for Door Status
Voltage Alert

Settings | Email | Message | SNMP | Script

Comment:

Folder: Select a folder ...

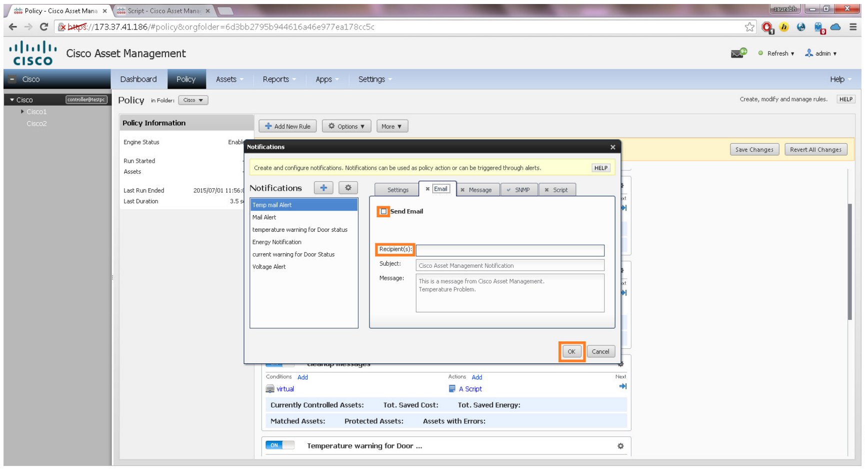
Limit Notifications: unlimited

unlimited
max. 1 per minute
max. 1 per 5 minutes
max. 1 per 10 minutes
max. 1 per 15 minutes
max. 1 per 30 minutes
max. 1 per 45 minutes
max. 1 per hour
max. 1 per 2 hours

Cisco Asset Management
Dashboard
Policy
Assets
Reports
Apps
Settings
Help
Policy Information
Add New Rule
Options
More
Save Changes
Revert All Changes
Currently Controlled Assets: Tot. Saved Cost: Tot. Saved Energy:
Matched Assets: Protected Assets: Assets with Errors:
Temperature warning for Door ...
375225

Step 12 Go to the **Email** option and put email IDs in the recipient area, as shown in Figure 4-72. Select **Send Email** and click **OK**.

Figure 4-72 Configure Recipients Email ID



Notifications

Create and configure notifications. Notifications can be used as policy action or can be triggered through alerts.

□ Send Email

Recipient(s):

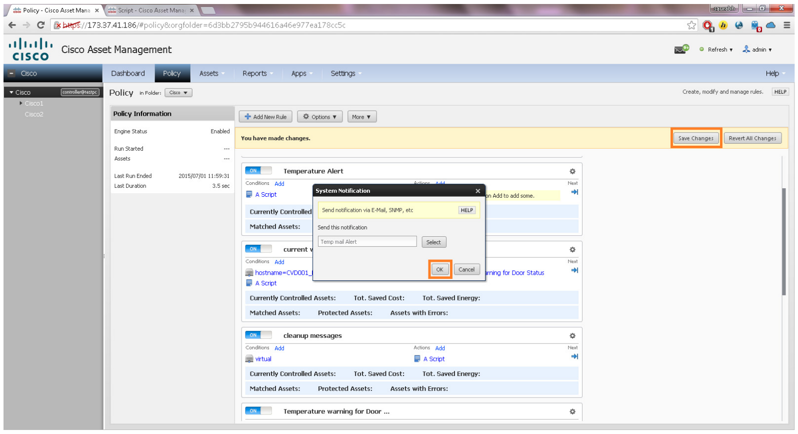
Subject: Cisco Asset Management Notification

Message: This is a message from Cisco Asset Management. Temperature Problem.

Step 13 Click on the **OK** button in the System Notification window.

Step 14 Click on **Save Changes** in the Policy option, as shown in Figure 4-73.

Figure 4-73 Save New Policy



You have made changes.

System Notification

Send notification via E-Mail, SNMP, etc

Send this notification: Temp mail Alert

Use Cases for Notification using Policy

Energy Consumption

The following script is used for the notification for energy consumption. For details, refer to "Steps for creating Notification using Policy" section.

```
var res =
httpGet("https://173.39.211.85/reports/json/votws?report=votws&comparable=false&options=Cu
stomMetric&metric0=da04469f3fd7490c9d4e0c16ce23375e_avg&segment0=id%3D609ebbbde68f4f618e4d
fb9087543f85%20dqllabel%3D%22Total%20Energy%20Consumption%22&dtype=last7days&ds=&de=&hrsco
nsiderdaterange=0&granularity=&export=json&limit=undefined&offset=undefined&orgfolder=6d3b
b2795b944616a46e977ea178cc5c&locale=en&tz=330&ts=7180ffe5b19f12b88bee396ace0b9a85&auth=6e7
34ae05c144c799253e034696ace51@6f7e907176c449aea2091d841f310096");
res1=JSON.parse(res);
var test = res1.data[0].items;
var len = test.length;
```

```
// minimum is starting value and maximum is last value.
var minimum = test[0].v;
var maximum = test[len-1].v;
var Diff = maximum - minimum;
// var "th" is consumption value for energy notification.
var th = 2;
if(Diff >  th){
   return true;
}
else{
   return false;
}
```

Generator Startup Problem

The following script is used for notification of generator startup problems. For details, refer to "Steps for creating Notification using Policy" section.

```
// id id DQL ID of voltage for Generator.
var id="2429669b837c42e589560467d7a77900";
var res = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id") +
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
res1=JSON.parse(res);
voltage = res1.result.state.value;
// var "th" is consumption value for energy notification.
var th = 10;
if (voltage > 10){
   return true;
}
else{
   return false;
}
```

Temperature Warning for Door Status

The following script is used for notification of the temperature warning for door status. For details, refer to "Steps for creating Notification using Policy" section.

```
var id1 = "6f750e670f224d6083a728eae82e5d66";
var id2 = "9debdbc63e4848fd9656afdd0ed79970";
// id1 is id of doorStatus and id2 is id of temperature.
var door = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id1") +
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
door=JSON.parse(door);
var doorStatus = door.result.state.value;
// doorStatus...... 0 for open and ......1 for close
if (doorStatus === 0){
    var temp = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id2") +
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
           temperature = JSON.parse(temp);
     var temperature1 = temperature.result.state.value;
    // wait till door is open.
     while(doorStatus === 0){
        door = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id1") +
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
              door=JSON.parse(door);
              doorStatus = door.result.state.value;
```

```
               sleep(120);
    }
    temp = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id2") + 
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
           temperature = JSON.parse(temp);
    var temperature2 = temperature.result.state.value;
            // If temperature difference is greater than 1, send notification.
    if ((temperature2 - temperature1) > 1 || (temperature2 - temperature1) < -1) {
        return true;
    }
    else {
        return false;
    }
}
else {
    return false;
}
```

Current Warning for Door Status

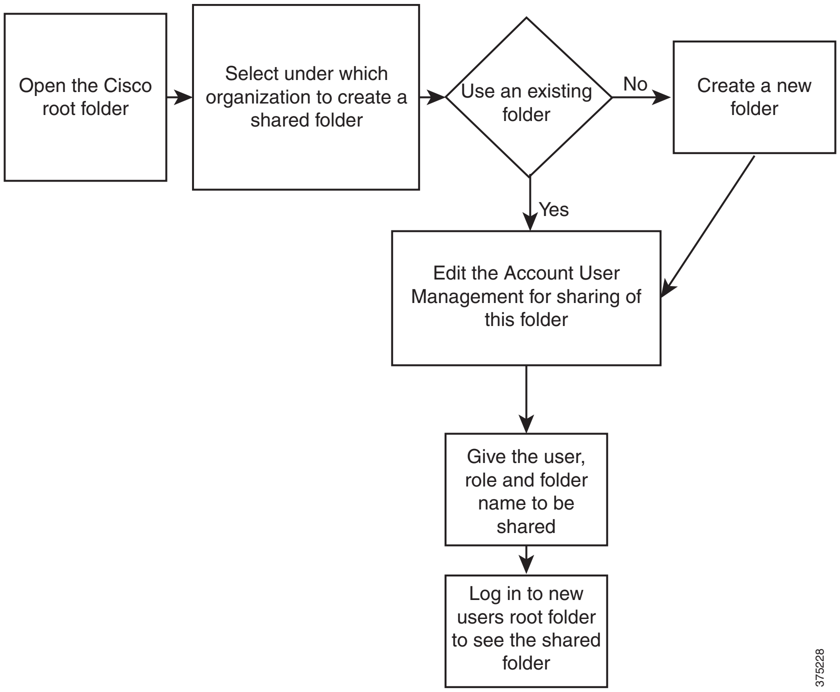
The following script is used for notification of the current warning for door status. For details, refer to "Steps for creating Notification using Policy" section.

```
var id1 = "6f750e670f224d6083a728eae82e5d66";
var id2 = "b90fc0f7dfa347a08cc8e6a5d90059b7";
// id1 is id of doorStatus and id2 is id of current.
var door = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id1") + 
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
door = JSON.parse(door);
var doorStatus  =  door.result.state.value;
// doorStatus...... 0 for open and ......1 for close
if (doorStatus === 0) {
    var current = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id2") + 
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
       current = JSON.parse(current);
    var current1 = current.result.state.value;
    // wait till door is open.
    while(doorStatus === 0){
        door = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id1") + 
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
           door=JSON.parse(door);
           doorStatus = door.result.state.value;
           sleep(120);
    }
    current = httpGet("https://localhost/api/1.0/objectstore/device/" + dget("id2") + 
"/history/?property=value&limit=1&auth=6e734ae05c144c799253e034696ace51@6f7e907176c449aea2
091d841f310096");
        current = JSON.parse(current);
    var current2 = current.result.state.value;
     // If current difference is more than 1, send notification.
    if ((current2 - current1) > 1 || (current2 - current1) < -1) {
        return true;
    }
    else {
        return false;
    }
}
else {
    return false;
}
```

Multi-Tenant Setup

Multi-tenant site operations means that different Telco operators using one tower site, pay only for the energy they consume. The below example considers two Telcos, named Cisco1 and Cisco2. The energy consumed by Cisco2 Telco is shared from the Cisco1 organization. Figure 4-74 shows the configuration flow for multi-tenant power monitoring.

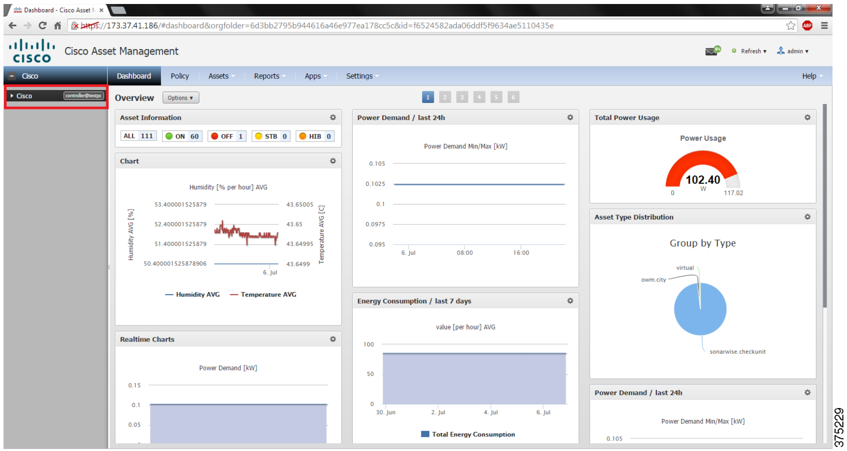
Figure 4-74 Configuration Flow of Multi-Tenant Power Monitoring


Open the Cisco root folder
Select under which organization to create a shared folder
Use an existing folder
No
Create a new folder
Yes
Edit the Account User Management for sharing of this folder
Give the user, role and folder name to be shared
Log in to new users root folder to see the shared folder
375228

Complete the following steps to share services:

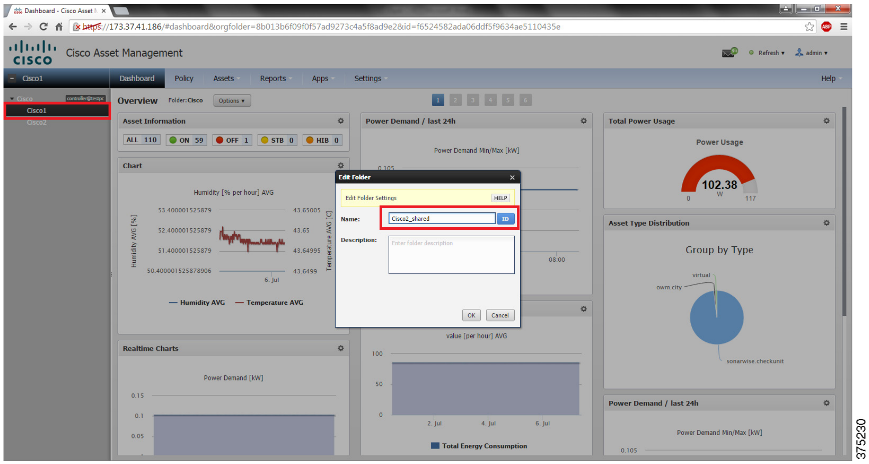
Step 1 Figure 4-75 shows the root folder **Cisco**, under which organizations can be created.

Figure 4-75 Selection of Cisco Root Folder



Step 2 Right-click on **Cisco1** and select **Create Folder**. Name the new folder, as shown in Figure 4-76.

Figure 4-76 Creation of New Folder

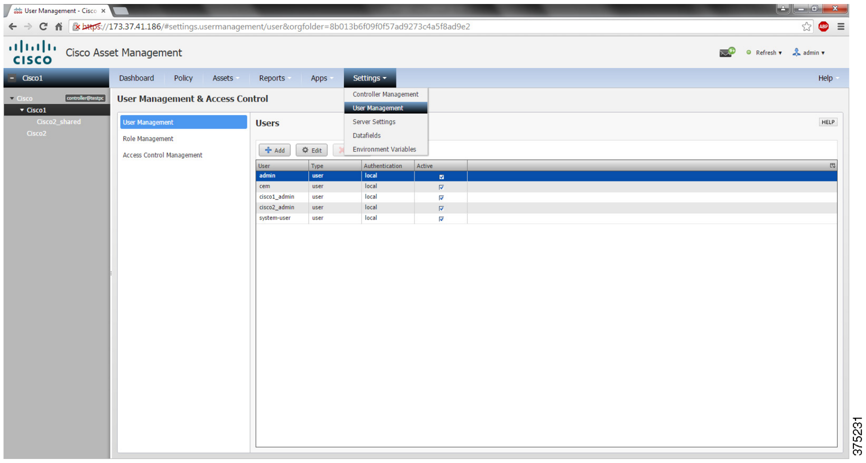


Name: Cisco2_shared

Description: Enter folder description

Step 3 Select the **User Management** option under **Settings** to add or edit users, as shown in Figure 4-77.

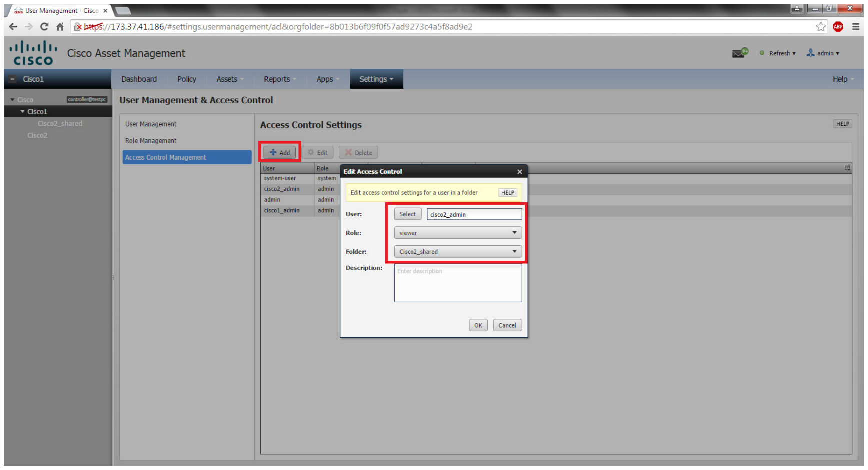
Figure 4-77 Selection of User Management



User	Type	Authentication	Active
admin	user	local	☑
cem	user	local	☑
cisco1_admin	user	local	☑
cisco2_admin	user	local	☑
system-user	user	local	☑

Step 4 Create a new user by selecting **Add** under **Access Control Management**. Name the user, role and the folder that has to be shared and select **OK**, as shown in Figure 4-78.

Figure 4-78 Creation of New User



https://173.37.41.186/#settings.usermanagement/acl&orgfolder=8b013b6f09f0f57ad9273c4a5f8ad9e2

User Management & Access Control

Access Control Settings

User	Role
system-user	system
cisco2_admin	admin
admin	admin
cisco1_admin	admin

Edit Access Control

Edit access control settings for a user in a folder

User: Select cisco2_admin

Role: viewer

Folder: Cisco2_shared

Description: Enter description

Step 5 To check if the folder got shared, log in to the CAM again with the user name **cisco2_admin** and password **admin**.

APPENDIX A

Troubleshooting

This section describes how to troubleshoot if the cloud does not show service. To troubleshoot the issues, understanding the information flow from the sensor to the cloud is required. This section covers the information flow and troubleshooting scenario.

Information Flow

This section describes how the information flows from the sensors to the site controller, and eventually to our cloud server. This will be illustrated with examples and diagrams that will help you understand how the events and results are flowing in the system. The diagrams illustrate a concrete flow of information and hence, in each of them, we draw and describe the main modules and topics involved, outlining their role in the information flow.

Flow of Information When the System Starts

The starting script runs all of the processes simultaneously. Therefore, you may expect a load peak when you start. All modules subscribe to their corresponding configuration topics in the mosquitto broker, and wait to receive their configuration.

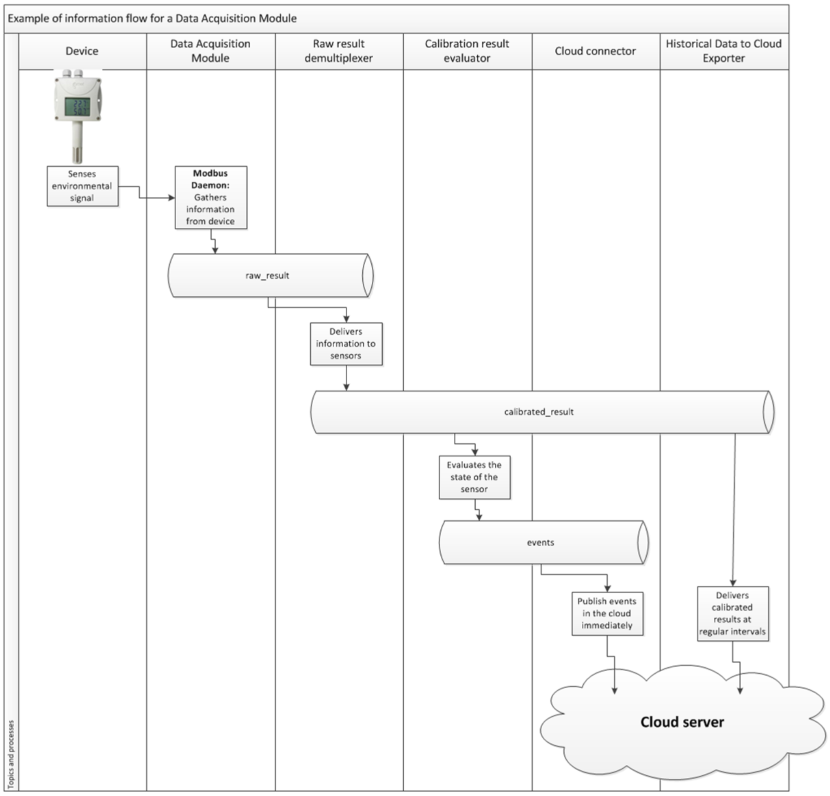
In the case of the mosquitto broker not being stopped, it will have the latest valid configuration for the modules, so it will get distributed to the modules immediately.

In case there is no configuration (or the configuration file has changed), the module Configuration Provider will parse the configuration and distribute the configuration to all the modules using the topic /config/module/%NameOfModule. Once a module receives its configuration, it is ready to start performing its function.

Information Flow for a Data Acquisition Module

Figure A-1 shows how the information flows across the system, from a sensing device to the cloud server.

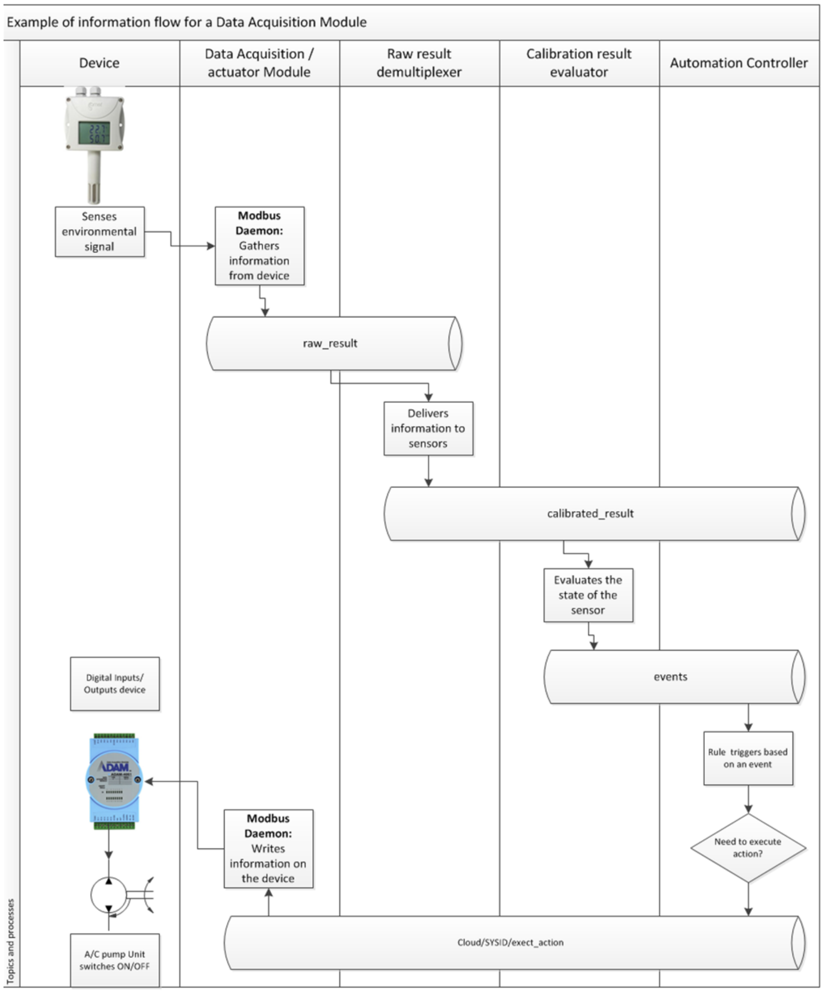
Figure A-1 Information Flow for Data Acquisition Module


Example of information flow for a Data Acquisition Module
Device
Data Acquisition Module
Raw result demultiplexer
Calibration result evaluator
Cloud connector
Historical Data to Cloud Exporter
Senses environmental signal
Modbus Daemon: Gathers information from device
raw_result
Delivers information to sensors
calibrated_result
Evaluates the state of the sensor
events
Publish events in the cloud immediately
Delivers calibrated results at regular intervals
Cloud server
Topics and processes

Information Flow for Automatic Control-Based on Parameters

Figure A-2 is an example of the information flow of a system configured to perform as a closed loop in temperature regulation. The system senses the temperature and based on its readings, activates a pump for an air conditioning device.

Figure A-2 Automatic Control-Based on Parameters Information Flow


Example of information flow for a Data Acquisition Module
Device
Data Acquisition / actuator Module
Raw result demultiplexer
Calibration result evaluator
Automation Controller
Senses environmental signal
Modbus Daemon: Gathers information from device
raw_result
Delivers information to sensors
calibrated_result
Evaluates the state of the sensor
events
Digital Inputs/ Outputs device
Rule triggers based on an event
ADAM
Need to execute action?
Modbus Daemon: Writes information on the device
Cloud/SYSID/exect_action
A/C pump Unit switches ON/OFF
Topics and processes

Troubleshooting Scenario

Services Show Timed Out in Cloud

The CAM shows a value for a service as TimeOut. Complete the following steps to rectify the problem:

Step 1 Log in to IR910 using ssh with the username **system**.

Step 2 Go to the log folder **cd /mnt/data/azeti/SiteController/log.**

Step 3 All raw information received from any sensor is kept in the log file **ModbusMaster.log**.

Step 4 Tail -f ModbusMaster.log and collect logs. For example, the output is shown below:

```
" Reply Time-out
```

```
08:33:25,585:3240:[ModbusSensor.py:212]:DEBUG:CE_ADB11# Comet_Temperature_Humidity_Sensor:
Reply time-out
```

Step 5 It indicates a problem in the sensor or connectivity to IR910

Step 6 It can be caused for the following reasons:

- **a.** Wrong sensor ID configured.
- **b.** There is power problem on the sensor.
- **c.** Problem in wiring.

Step 7 Once resolved the results are as shown below:

```
2015-08-26
08:33:22,649:3240:[ModbusSensor.py:212]:DEBUG:Comet_Temperature_Humidity_Sensor#Comet_Temp
erature_Humidity_Sensor: [49]: 228, [50]: 422
```

Services Show Wrong Value in Cloud

The CAM may show a wrong value to a service. For example, the humidity service shows that the value is 417 but it is actually 41.7, which means the form factor is not configured correctly. This can be checked by completing the following steps:

Step 1 Log in to IR910 using ssh with the username **system**.

Step 2 Go to the log folder **cd /mnt/data/azeti/SiteController/log**.

Step 3 All raw information received from any sensor is kept in the log file **Raw_resultdemux.log**.

Step 4 Tail -f Raw_resultdemux.log and collect logs:

```
015-08-04 04:12:22,664:2888:[RawResultsDeMux.py:265]:DEBUG:INT:
raw_result/Comet_Temperature_Humidity_Sensor : {"timestamp":
"2015-08-04T04:12:22.581Z+0530", "sensor_gateway_id": "Comet_Temperature_Humidity_Sensor",
"error_code": 0, "result_dict": {"50": {"changed": true, "value": 417}, "49": {"changed":
false, "value": 225}}}
2015-08-04 04:12:22,666:2888:[RawResultsDeMux.py:300]:DEBUG:processResult()
2015-08-04 04:12:22,699:2888:[RawResultsDeMux.py:312]:DEBUG:sensor_gateway_id:
Comet_Temperature_Humidity_Sensor errorcode: 0 timestamp: 2015-08-04T04:12:22.581Z+0530
result_dict: {u'50': {u'changed': True, u'value': 417}, u'49': {u'changed': False,
u'value': 225}}
2015-08-04 04:12:22,701:2888:[RawResultsDeMux.py:347]:DEBUG:DEMUX keylist: [u'49']
2015-08-04 04:12:22,702:2888:[RawResultsDeMux.py:363]:DEBUG:No relevant change in the raw
result for sensor Comet_Temperature_Status, skip publishing
2015-08-04 04:12:22,704:2888:[RawResultsDeMux.py:347]:DEBUG:DEMUX keylist: [u'50']
2015-08-04 04:12:22,705:2888:[RawResultsDeMux.py:397]:INFO:Raw Result for sensor
Comet_Humidity_Status: 417
2015-08-04 04:12:22,733:2888:[RawResultsDeMux.py:402]:DEBUG:Sensor Comet_Humidity_Status
has a calibration rule
2015-08-04 04:12:22,738:2888:[RawResultsDeMux.py:403]:DEBUG:About to calibrate the raw
result
2015-08-04 04:12:22,740:2888:[RawResultsDeMux.py:422]:DEBUG:raw_result_factor: 0.100000
2015-08-04 04:12:22,741:2888:[RawResultsDeMux.py:423]:DEBUG:offset: 0.000000
2015-08-04 04:12:22,742:2888:[RawResultsDeMux.py:433]:DEBUG:rounding_precision: 2
2015-08-04 04:12:22,743:2888:[RawResultsDeMux.py:438]:DEBUG:result_calibrated: 41.7
2015-08-04 04:12:22,745:2888:[RawResultsDeMux.py:452]:DEBUG:About to publish
calibrated_result/Comet_Humidity_Status
```

Event Is Not Raised for Service

The following steps show whether an Event is raised or not, based on the configuration in the site controller for that service:

Step 1 Log in to IR910 using ssh with username **system**.

Step 2 Go to the log folder **cd /mnt/data/azeti/SiteController/log.**

Step 3 All raw information received from any sensor is kept in the log file **CalibResultsEvaluator.log aw_resultdemux.log**.

Step 4 Tail -f CalibResultsEvaluator.log and collect logs:

```
CalibResultsEvaluator.log ---- sends event based on OK, WARNING or any state change
2015-08-04 04:12:22,777:2934:[CalibResultsEvaluator.py:68]:DEBUG:INT:
calibrated_result/Comet_Humidity_Status : {"timestamp": "2015-08-04T04:12:22.581Z+0530",
"sensor_id": "Comet_Humidity_Status", "error_code": 0, "value": 91.7000000000000003}
2015-08-04 04:12:22,779:2934:[CalibResultsEvaluator.py:120]:DEBUG:Comet_Humidity_Status:
start sensor evaluation...
2015-08-04 04:12:22,781:2934:[CalibResultsEvaluator.py:184]:DEBUG:Comet_Humidity_Status:
value: 41.7 type(value): <type 'float'>
2015-08-04 04:12:22,782:2934:[CalibResultsEvaluator.py:188]:DEBUG:Comet_Humidity_Status:
rule: value > 90 value: 91.7
2015-08-04 04:12:22,784:2934:[CalibResultsEvaluator.py:223]:DEBUG:Comet_Humidity_Status:
expression: 91.7 > 90 -> True
2015-08-04 04:12:22,785:2934:[CalibResultsEvaluator.py:188]:DEBUG:Comet_Humidity_Status:
rule: value > 80 value: 91.7
2015-08-04 04:12:22,814:2934:[CalibResultsEvaluator.py:365]:INFO:Comet_Humidity_Status:
state: CRITICAL (value:91.7) -> change
```

Step 5 If an event is not raised, check the threshold value configured for this service.

CAM Shows Location Disconnected

The CAM shows the status of location as disconnected, which can be for the following reasons:

- Reachability issue
- Username/password wrong

This can be rectified by using the steps shown below:

Step 1 Log in to IR910 using ssh with username **system**.

Step 2 Go to the log folder **cd /mnt/data/azeti/SiteController/log.**

Step 3 The connection establishment from MQTT is in the log file **cloudConnector.log.**

Step 4 Tail -f cloudConnector.log and collect logs. The below log shows that the problem is due to reachability to the cloud:

```
"2015-08-23 00:37:23,087:2795:[cloudConnector.py:926]:DEBUG:ExternalCloudBroker: Using
user_id/password: broker.cisco@azeti.net/**********
2015-08-23 00:37:23,089:2795:[cloudConnector.py:931]:INFO:Using unencrypted connection to
the cloud.
2015-08-23 00:37:23,090:2795:[cloudConnector.py:946]:DEBUG:Trying to connect to
10.81.1.10:1883
2015-08-23 00:37:23,468:2795:[cloudConnector.py:764]:DEBUG:persist_outbox - persisted
msgs: [9866]
2015-08-23 00:37:25,707:2795:[cloudConnector.py:954]:ERROR:Exception while trying to
connect to 10.81.1.10:1883:
```

```
Traceback (most recent call last):
  File "/mnt/data/azeti/SiteController/src/cloudConnector.py", line 947, in
connect_to_broker
    mqttc.connect(host, port, 60)
  File
"/mnt/data/azeti/SiteController/lib/lib/python2.7/site-packages/paho_mqtt-1.1-py2.7.egg/pa
ho/mqtt/client.py", line 612, in connect
    return self.reconnect()
  File
"/mnt/data/azeti/SiteController/lib/lib/python2.7/site-packages/paho_mqtt-1.1-py2.7.egg/pa
ho/mqtt/client.py", line 734, in reconnect
    sock = socket.create_connection((self._host, self._port),
source_address=(self._bind_address, 0))
  File "/usr/lib/python2.7/socket.py", line 571, in create_connection
error: [Errno 113] No route to host"
```

Step 5 The log below shows that the problem is the username and password for the cloud:

```
[cloudConnector.py:408]:DEBUG: ExternalCloudBroker: Disconnected - rc: Connection Refused
```

APPENDIX B

Sensor - Data Sheets

Sensor - Data Sheets

Advantech Input/Output Modules

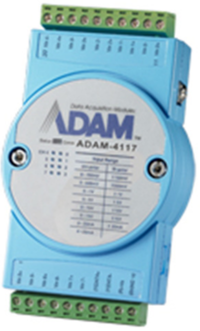
The Advantech I/O devices are a group of Modbus slave devices that allow us to receive input and create output using the RS-485 Modbus protocol. We can take measures in analogical (0-20mA, 0-5V) and dry contact way (0-1), as well as control outputs (dry contact 0-1, analog 0-10V).

Adam 4117

Figure B-1 shows the Adam 4117, which has the following characteristics:

- Analogue Input module
- Modbus RTU connectivity
- 3.8 analogue inputs: To change an input from current to voltage, the module has to be opened and a jumper changed. Can be configured connecting it to a PC (with a RS485 adapter).
- Voltage: 0~150 mV 0~500 mV 0~1V 0~5 V 0~10 V ±150 mV ±500 mV ±1 V ±5 V ±10 V ±15 V
- Current: ±20 mA 0~ 20 mA 4~20 mA

Figure B-1 Adam 4117



Adam 4150

Figure B-2 shows the Adam 4150, which has the following characteristics:

- Digital input/output module
- Modbus RTU connectivity
- 7 digital inputs
- Dry contact: Logic level 0: close to GND Logic level 1: open
- 8 digital outputs: Open collector to 40V, 1 A max. load Support
- Can be configured connecting it to a PC (with a RS485 adapter)

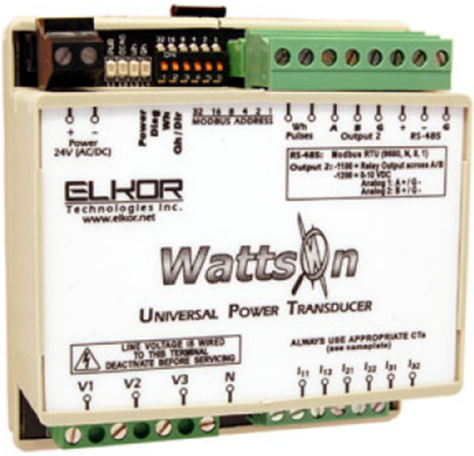
Figure B-2 Adam 4150

WattsOn-1100-MS360-500A and MSCT2

Figure B-3 shows the WattsOn AC Energy Meter, 3-phase AC voltage meter, up to 600A with the following characteristics:

- ANSI C12.20 Class 0,2 Accuracy compliant.
- Supports IEC 60687, IEC 61036, IEC 61268, IEC 62053-21, IEC 62053-22, and IEC 62053-23.
- Interfaces with almost ANY CT including: 5A, mA, 333mV, 500mV, 1000mV, Solid Core, Split Core, Rogowski Coil, and so on.
- Universal 24 VAC/VDC power supply
- DIN Mount
- High resolution (24-bit ADCs) with 16kHz sampling provide True RMS parameters per phase: voltage, current, power, energy (W, VA, VAR), frequency, and power factor.
- Standard RS-485 (Modbus) communications.
- Integer and floating point data transfer.
- Compatible with 3-Phase/3-wire, 3-Phase/4-wire, split and single phase configurations.
- Four-quadrant energy and demand calculations.
- Per phase import/export energy accumulation.
- Two pulse outputs: one for Wh, and the other configurable for VARh or direction of active power.

Figure B-3 WattsOn AC Energy Meter



Available output parameters via Modbus:

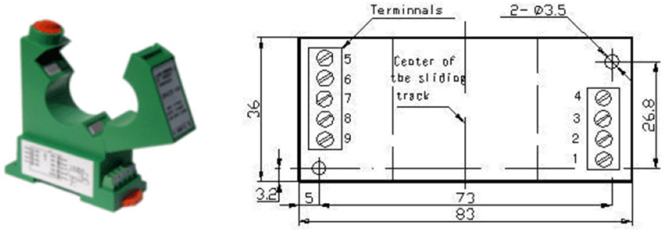
- 1.Voltage (A, B, C, Avg, AB, AC, BC, Avg)
- 2.Current (A, B, C, Avg)
- 3.Active Power (A, B, C, Total) - Bi-directional
- 4.Apparent Power (A, B, C, Total)
- 5.Reactive Power (A, B, C, Total) - Bi-directional
- 6.Power Factor (A, B, C, System) - Bi-directional
- 7.Frequency
- 8.Import/Export Energy (A, B, C, Total)
- 9.Inductive/Capacitive Energy(A, B, C, Total)
- 10.Apparent Energy (A, B, C, Total)
- 11.Total Demand Power (W)

DC Multiparameter CE AD11B-34GS4-1.0/0-250A*0-65V

The DC Multiparameter CE AD11B-34GS4-1.0/0-250A*0-65V (shown in Figure B-4) is a split core DC multi-parameter digital transducer, with the following features:

- DC multi-parameter monitoring, U, I, P, KWH
- Various measure range for option:
- Current: 0-250ADC
- Voltage: 0-65V
- 24V power source
- Bi-direction detect for U,I,P, KWH
- Energy data power failure protection
- High stability, 2KV surge protection on input, power supply and output interface

Figure B-4 DC Multi-Parameter

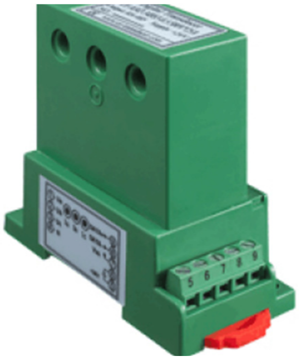


DC Voltage Meter CE-AU11-34MS3-0.2/0-65V

The DC Voltage Meter CE-AU11-34MS3-0.2/0-65V (shown in Figure B-5) is a single parameter DC voltage digital transducer with Modbus output, with the following specifications:

- Input (measuring range) - Voltage: 65V DC
- Data output - Voltage
- Output interface - RS-485: two-wire connection, communication distance: 1200m, ±15KV ESD protection
- Accuracy grade - 0.2%
- Baudrate - 1200, 2400, 4800, 9600, 19.2K bps
- Refreshing period - 100mS
- Isolation voltage - 2500V DC
- System power consumption - <200 mw (+12V)
- Power source +24V
- Operation temperature - 0°C ~50°C
- Storage condition - -20°C ~+80°C (RH: 5%~95% no dew)

Figure B-5 DC Voltage Meter

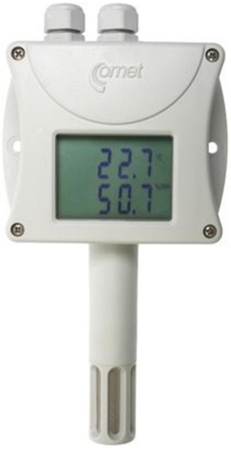


Comet T3411

The Comet T3411 (shown in Figure B-6) is relative humidity, temperature sensor. Measured values are also converted to other humidity interpretations: dew point temperature, absolute humidity, specific humidity, mixing ratio, specific enthalpy. Other characteristics are as follows:

- Modbus RTU (RS485) output
- Power: 9-30Vdc, current consumption approximately 0.5W
- Protection of the case with electronics: IP65 electronics, IP40 sensors

Figure B-6 Comet T3411



Analog Sensors

The analog sensors are discussed in the following sections.

Fuel Level Sensor: AST 4510 - 5PSI - Pressure Sensor

The Fuel Level Sensor: AST 4510 - 5PSI - Pressure Sensor (shown in) is a submersible pressure sensor up to 5 PSI (3,51 meters), with the following characteristics. For higher tanks, a different specification should be ordered.

- Performance @ 25°C (77°F)
- Accuracy1<±0.25% BFSL (<±0.5% BFSL for 0-1 PSI)
- Stability (1 Year)±0.25%FS, typ
- Proof Pressure2X Rated Pressure
- Burst Pressure5X or 1,250 psi (whichever is less)
- Pressure Cycles> 50 Million

Environmental data:

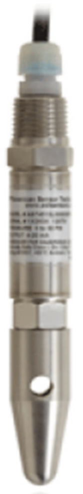
- Temperature
  - Operating -40 to 80°C (-40 to 176°F)
  - Storage -40 to 100°C (-40 to 212°F)

- Thermal Limits
  - Compensated Range 0 to 55°C (-32 to 131°F)
  - TC Zero <±1.5% of FS (<±2.5%, typ. for 1PSI)
  - TC Span <±1.5% of FS (<±2.5%, typ. for 1PSI)
- Other
  - Shock EN 60068-2-27
  - Vibration EN 60068-2-6, 60068-2-64, and IEC 68-2-32
  - EMI/RFI Protection Yes
  - Rating IP68

Electrical Data

- Output Signal4-20mA
- Excitation10-28VDC, Typ.
- Output Impedance>10k Ohms
- Current Consumption20mA, Max
- Bandwidth(-3dB): DC to 250 Hz
- Output Noise<2mV RMS
- Zero Offset<±1% of FS <±4%(1PSI)
- Span Tolerance<±1.5% of FS <±4%(1PSI)
- Output Load0-800 Ohms @10-28VDC
- Reverse Polarity Yes

Figure B-7 Pressure Sensor



AC On/Off Current Transducer i-Snail-S

The AC On/Off Current Transducer i-Snail-S (shown in Figure B-8) is a self-powered GO/NO-GO current status switch, with the following features:

- Low turn on (less than 0.150 A)

- Hysteresis and anti-transient circuitry eliminates chatter and false switching
- Easy Wiring
- Rugged enclosure

The i-Snail-S serves as an ultra-sensitive Go/No-Go load sensor. The dry contact relay (N.O.) closes when a minimum amount (150mA) of AC current is flowing through its monitored line. The device is ideal for monitoring the running state of fans, motors, pumps, heaters or any device that is AC powered, including large and small loads.

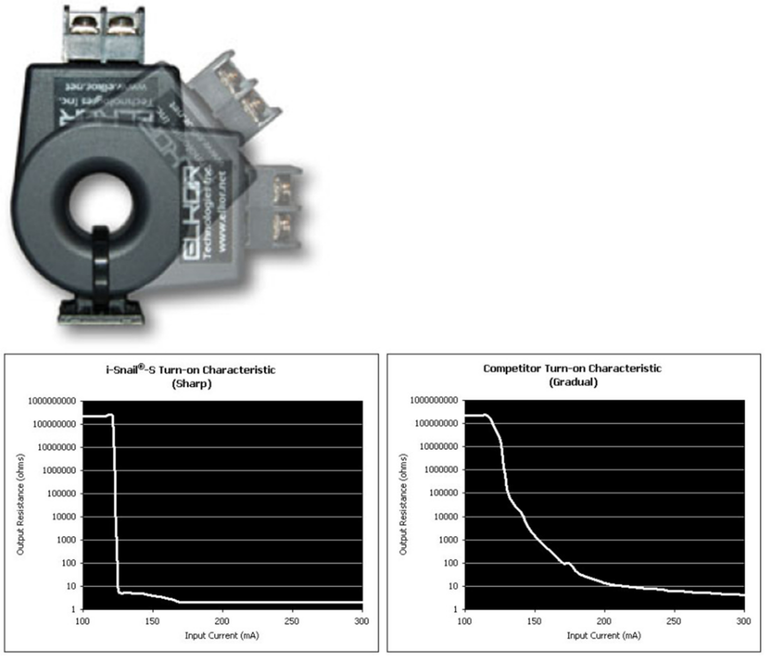
The output is a bi-directional solid state relay with a low turn on resistance of less than 4 ohms. The output may be interfaced to PLCs, DDC panels or other relays.

The advanced hysteresis and transient detection circuitry prevent chattering and false switching due to line spikes and transients.

The i-Snail-S features a rugged enclosure with integrated barrier strip terminal block or 6" leads for easy wiring in the field.

The i-Snail-S features advanced detection circuitry which enables an ideal switch characteristic. The output is turned on with a *brick wall* switching curve. Competitive products feature a gradual turn on with the resistance dropping gradually. In many applications, non-ideal switching may cause erroneous results.

Figure B-8 i-Snail-S



AC Current Transducer i-Snail-VC

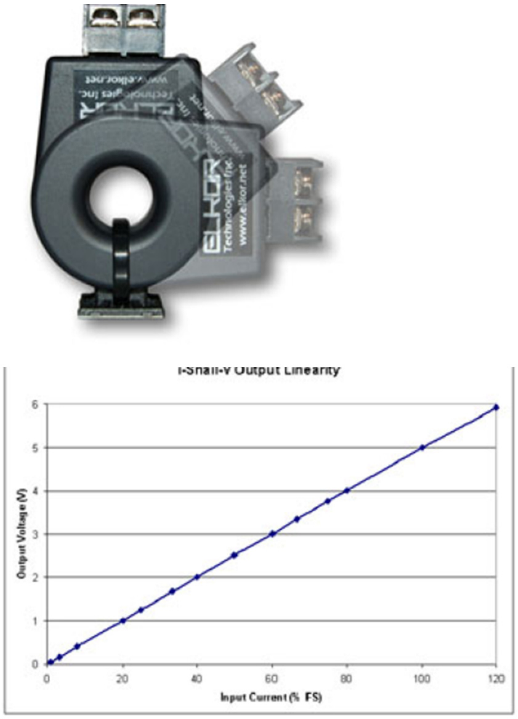
The i-Snail-VC (shown in Figure B-9) is a self-powered AC current transducer that provides a 0-5V dc analog signal proportional to the AC current flowing through the device wire window (sine wave RMS calibrated). This product is functionally identical to the i-Snail-V, but features a wire mount enclosure for smaller size and lower cost.

The i-Snail-VC is ideal for load monitoring without the need for an external power supply. Factory calibrated, fixed ranges ensure superior accuracy and eliminate configuration and adjustments in the field, saving time and avoiding confusion. Color coded labels allow for easy identification of full scale range.

The 14.5mm (0.570") wire window accommodates a conductor up to AWG #2. Multiple turns of the primary wire may be used to alter the input range. Output voltage is clamped at 6.5V, and the unit delivers a linear output up to 120% overload (6V).

- Power: Self powered by line current
- CT Wire Window: 13.7mm (0.54")
- Ranges: Fixed 10A, 25A, 50A or 100A (120% overload)
- Output: 0-5 VDC, proportional to RMS input current (sine wave)
- Clamped at approx 6.5V
- Linear to 120% overload (continuous)
- 200A overload (temporary)
- Accuracy: Better than 0.5% of full scale
- Ripple less than 0.1% of output
- Enclosure:L=2.5", W=1.6", H=0.9" (including terminal block)
- UL94V-0 ABS Plastic

Figure B-9 i-Snail-VC



Use Case: Complete Door Access

Configuration Detail

This section provides configuration detail of service BTS_arm_state and its corresponding, action and ACL rules of door access control. Table B-1 shows the list of services and the corresponding devices.

Table B-1 Door Access Control Configuration Detail

Service	Device	Purpose
Access_Control_Door1	VirtualSensorProvider	Validate PIN entered on Keypad. It can be either granted or denied or idle or brute force attack.
ADAM-4150-LED BLUE	ADAM-4150	Indicates armed (ON) or unarmed (OFF) on BLUE light.
ADAM-4150-LED GREEN	ADAM-4150	Indicates Deadman alert (Warning) Timer1.
ADAM-4150-LED RED	ADAM-4150	Indicates Deadman alert (Critical) Timer2 or Break-in.
BTS_arm_state	VirtualSensorProvider	Indicates ARMED or UNARMED in text.
Deadman-Button	ADAM-4150	Indicates status of physical button used for Deadman (button pressed or button released).
Door1_Movement	ADAM-4150	Indicates status of physical button used for Deadman (movement_detected or momenet_stopped).
Door1_Status	ADAM-4150	Indicates status of Door open or closed.
VS_break_in	VirtualSensorProvider	Indicates Door opened or movement detected in ARMED state.
VS_Brute_Force_Alert	VirtualSensorProvider	Indicates entering wrong PIN for more than three times.
VS_deadman_alert	VirtualSensorProvider	No Movement detected until T2 timer expired, it can be either DEADMAN ALERT ESCALATED or NO DEADMAN ALERT ESCALATION.
WTSC_Keypad_DO_1_red_LED	M2M_WTSC_Door_Controller	RED is initial state.

Table B-1 Door Access Control Configuration Detail

Service	Device	Purpose
WTSC_Keypad_DO_2_green_LED	M2M_WTSC_Door_Controller	Indicates right PIN entered.
WTSC_Keypad_DO_3_Buzzer	M2M_WTSC_Door_Controller	Buzzer indicates wrong or right PIN in audio.
WTSC_Keypad_Door_PIN_1	M2M_WTSC_Door_Controller	Entering PIN.
WTSC_Keypad_Relay	M2M_WTSC_Door_Controller	Door lock controlled using this relay.

Table B-2 shows a list of actions to be performed on the services.

Table B-2 List of Actions to be Performed on the Services

Action	Purpose
BruteForce_clear	Clear Brute force attack
ClearAlertsAndLights	Fire rule to clear alerts and lights
SiteArming	Changing ARM state
Switch_ARM_LED_0	Switch ON/OFF BLUE light
Switch_Break_in_LED	Switch ON/OFF RED light
Switch_Deadman_alert_LED_1	Switch ON/OFF GREEN light
Switch_Deadman_alert_LED_2	Switch ON/OFF RED light
Switch_M2M_WTSC_default	RESET keypad
Switch_M2M_WTSC_DO_1_red_LED	Switch to RED color
Switch_M2M_WTSC_DO_2_green_LED	Switch to GREEN color
Switch_M2M_WTSC_DO_3_Beep_short	Make beep short
Switch_M2M_WTSC_DO_3_Buzzer	Make buzzer
Switch_M2M_WTSC_orange_LED	Switch to ORANGE color
Switch_M2M_WTSC_Relay	Make relay ON /OFF

Table B-3 shows a list of ACLs.

Table B-3 List of ACLs

ACL Rule	Description
ArmState	Change the arm-state based on the result of Access_Control_Door1 sensor.
BreakIn	Check if there has been a break-in in the facility.
Brute_Force_Detection	Check if there has been a brute_Force in the facility.
ClearOutputs	When the clearoutputs action is fired, it will clear the VS_Brute_Force_Alert and VS_dead_man_warn.
DeadManControl	Publish result based on movement, Deadman button.
door1control	Fire actions to change LED colors based on Access_Control_Door1.