SOFTWARE INSTALLATION GUIDE

RUCKUS IoT Insights Software Installation Guide, 2.0.0

Supporting IoT Insights Release 2.0.0

Part Number: 800-73159-001 Rev A
Publication Date: March 2022

Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **5**
Contacting RUCKUS Customer Services and Support 5
What Support Do I Need? 5
Open a Case 5
Self-Service Resources 6
Document Feedback 6
RUCKUS Product Documentation Resources 6
Online Training Resources 6
Document Conventions 7
Notes, Cautions, and Safety Warnings 7
Command Syntax Conventions 7

About This Guide **9**
Introduction to RUCKUS IoT Insights 9

Installing IoT Insights on a VMWare ESXi **11**

Installing RUCKUS IoT Insights on Amazon Web Service **31**
Setting up an AWS Account 31
Configuring the AWS Command Line Interface 33
Installing Insights 34

Installing RUCKUS IoT Insights on Linux KVM Machine **45**

Preface

- Contacting RUCKUS Customer Services and Support 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Document Conventions 7
- Command Syntax Conventions 7

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Guide

- Introduction to RUCKUS IoT Insights..... 9

Introduction to RUCKUS IoT Insights

The RUCKUS IoT Insights is a RUCKUS CommScope application that provides an OT overview of the RUCKUS IoT Controller network and its associated data. The RUCKUS IoT Insights provides a full northbound API that allows for integration into 3rd party building management eco-systems, development or customization of front end dashboard solutions, this API allows for the re-skinning and development of custom IOT- OT solutions, integration into existing dashboards or the data push to external Service Data Analytics platforms from existing Cloud Service Providers such as Amazon, Google or Microsoft without the need for lengthy integration or Software development efforts.

This guide provides information about how to install the RUCKUS IoT Insights on a supported hypervisor. Topics include the installation instructions using the .OVA or .qcow2 file.

NOTE
If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

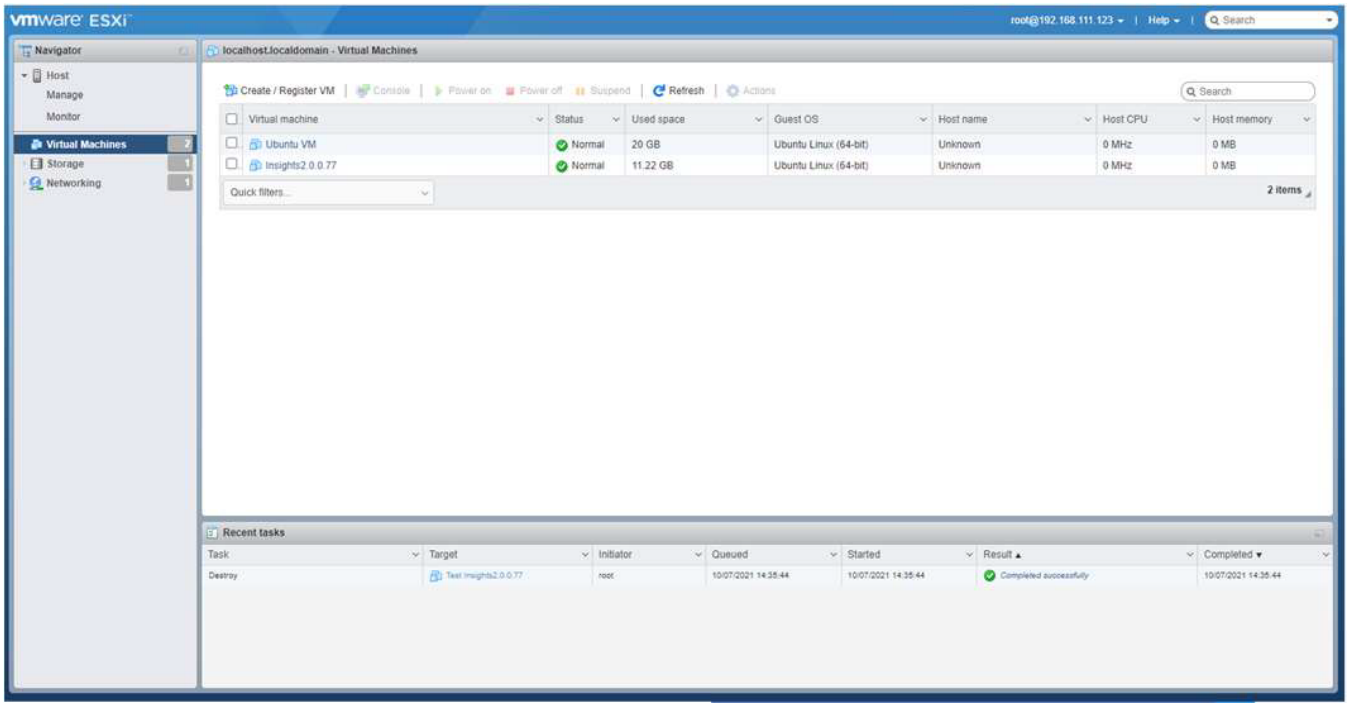
This guide is intended for use by those responsible for installing and setting up network equipment. It assumes a basic working knowledge of local area networking, wireless networking, and wireless devices.

Installing IoT Insights on a VMWare ESXi

The RUCKUS IoT Insights can be installed on a VMware ESXi hypervisor using an .OVA file.

1. Download the distribution package in the .OVA file format from the RUCKUS Support website at https://support.ruckuswireless.com.
2. Open VMware ESXi and select **Virtual Machines** from the **Navigator** pane.

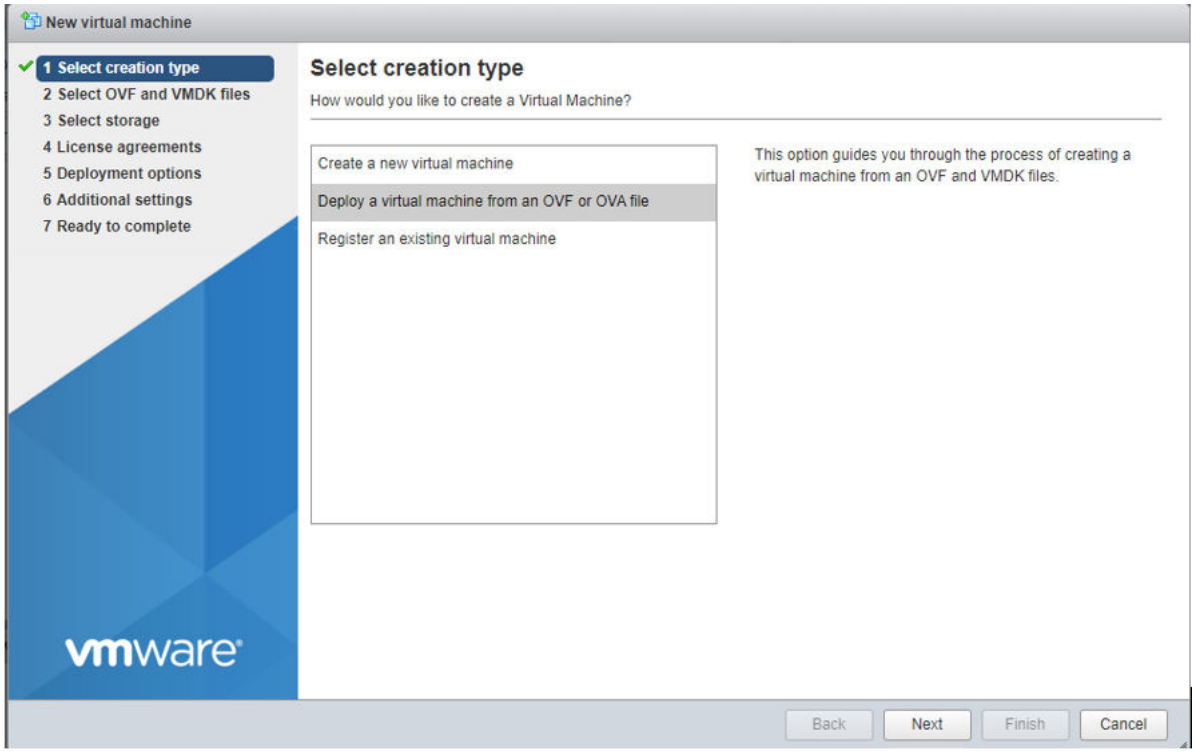
FIGURE 1 Selecting Virtual Machine



3. Click **Create/Register VM**.

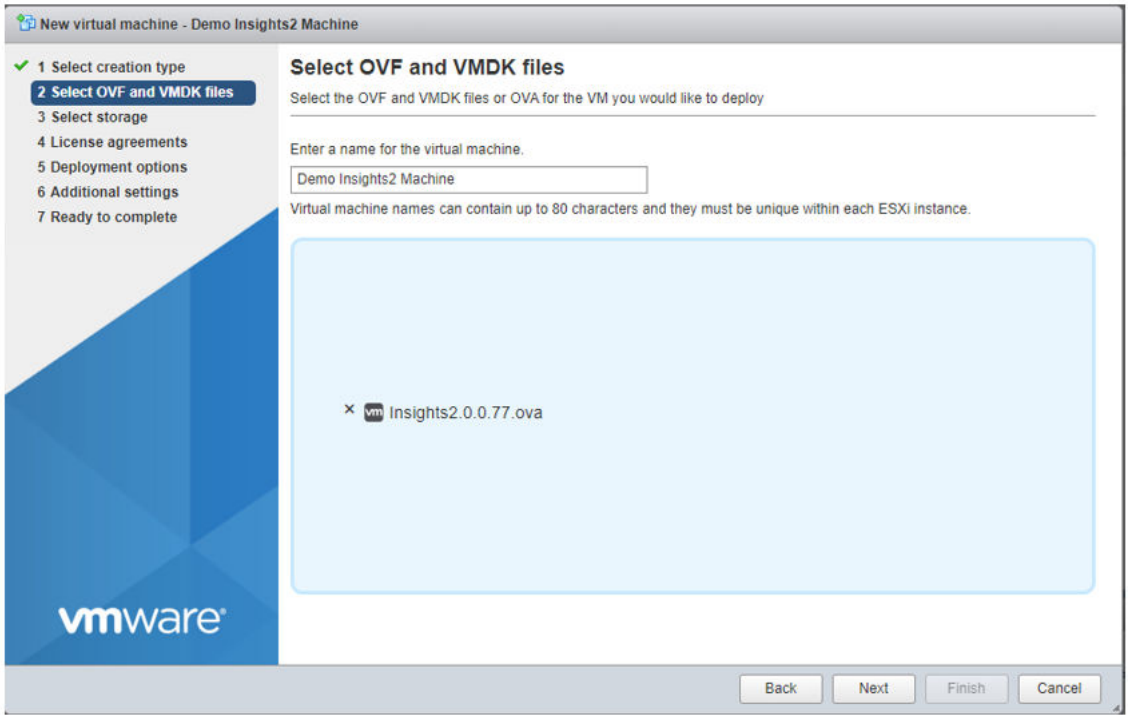
4. On the **New virtual machine** page, click **Select creation type**, and select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.

FIGURE 2 Creating New Virtual Machine



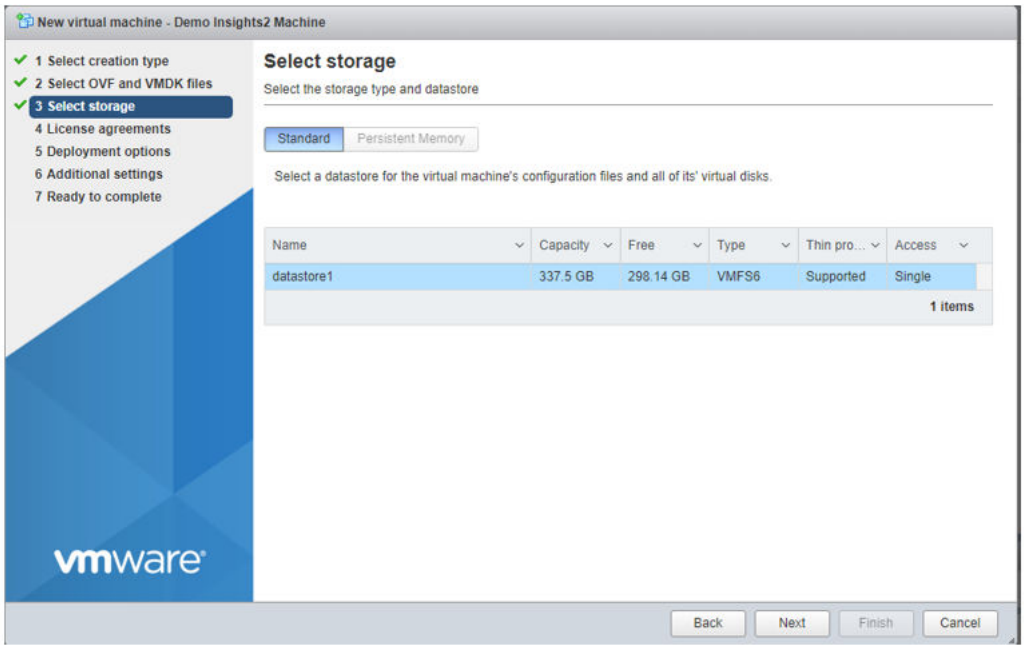
5. Click **Select OVF and VMDK files**, enter a name for the virtual machine, and select the OVF file. Click **Next**.

FIGURE 3 Importing OVA File



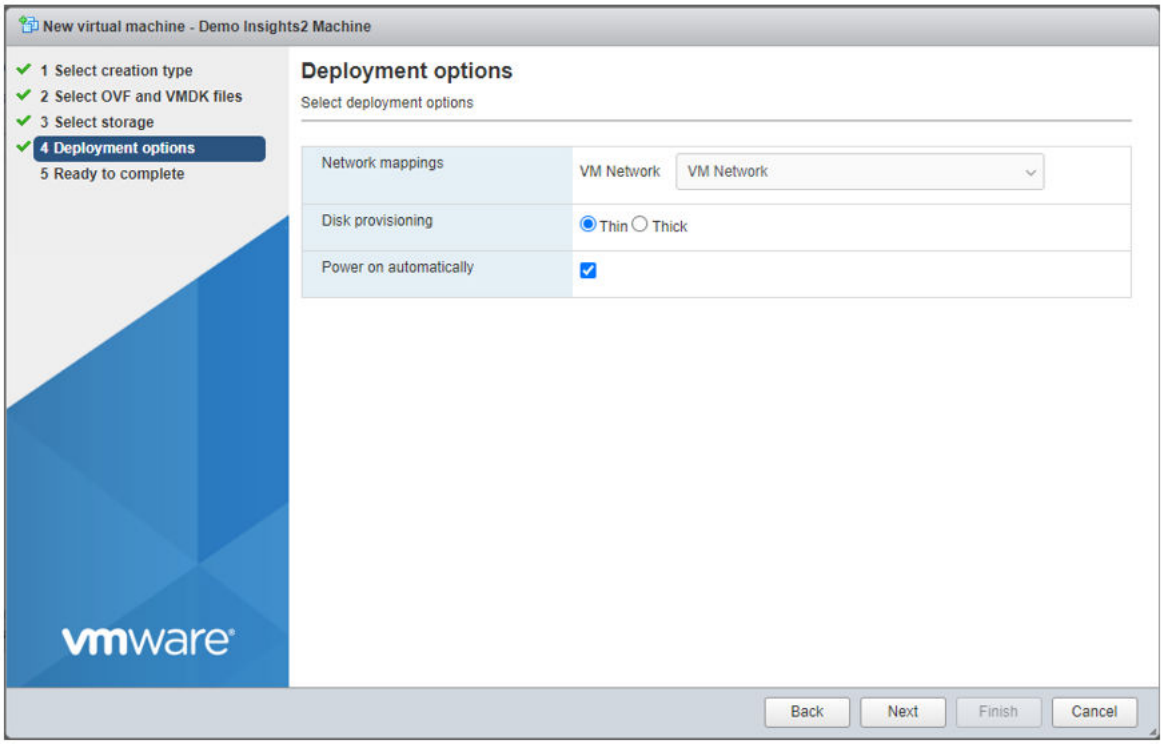
6. Click **Select storage**, and select the datastore in which you want to save the configuration and disk files. Click **Next**.

FIGURE 4 Selecting Storage



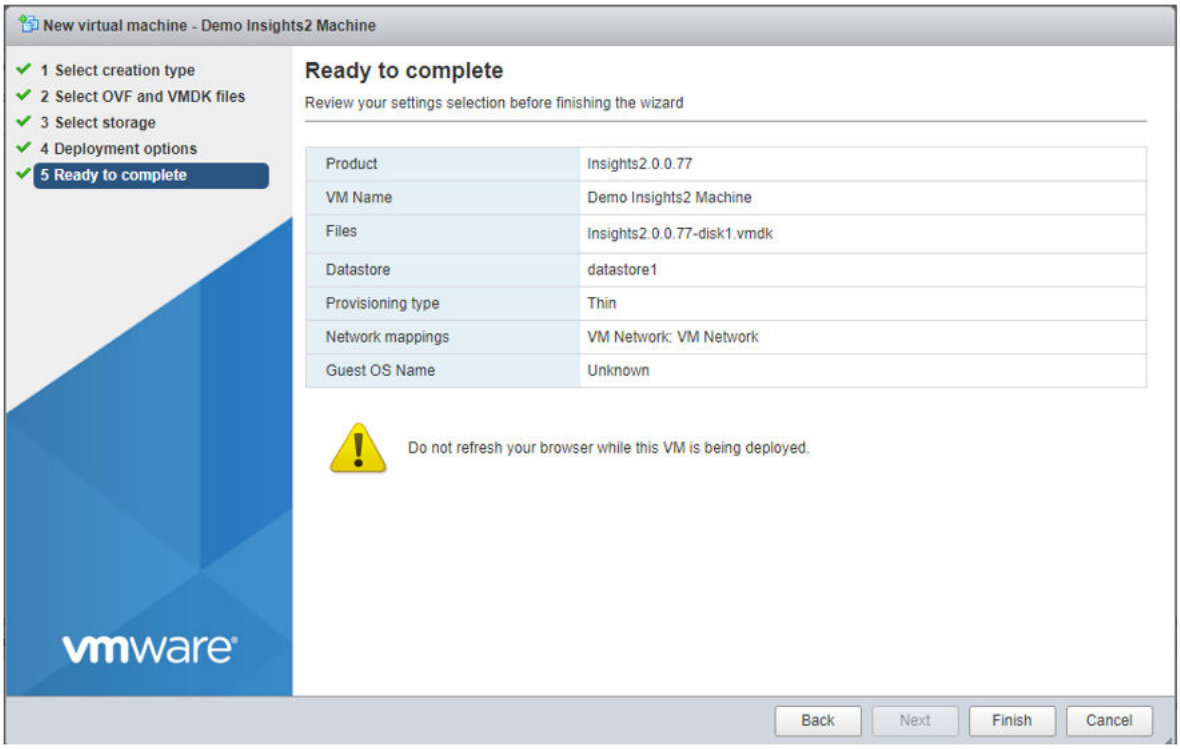
7. Click **Deployment options**, and select the **Network mappings** and **Disk provisioning**. Click **Next**.

FIGURE 5 Viewing Deployment Options



8. Click **Ready to complete** and review the settings. Click **Finish**.

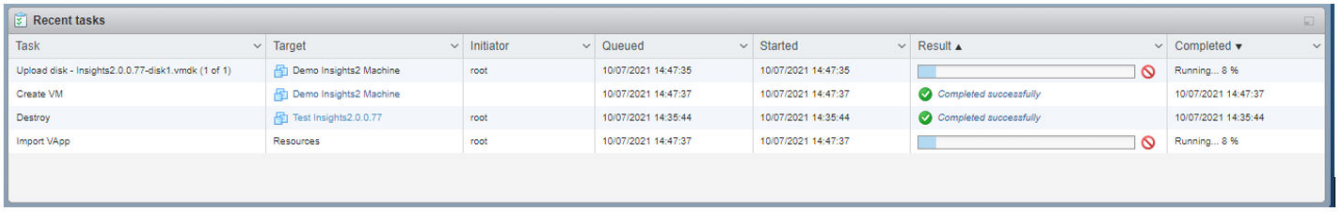
FIGURE 6 Confirming the Settings



NOTE
The OVA file upload can take some time, so it is important not to refresh or navigate away from the VMware dashboard during this VM creation phase.

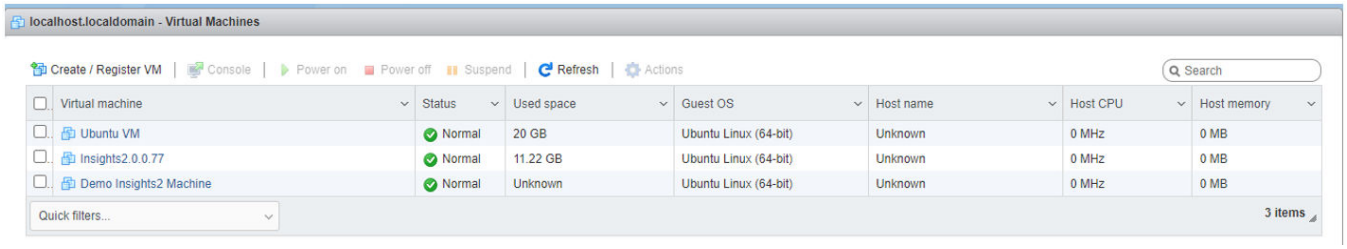
You can monitor the VM status and System status in the Recent Tasks Window.

FIGURE 7 Viewing ESXI Upload Image



After installing the VM, if the VM is not set to auto power on then the Installer can start the VM and initiate the Insights System Startup.

FIGURE 8 Confirming the Upload

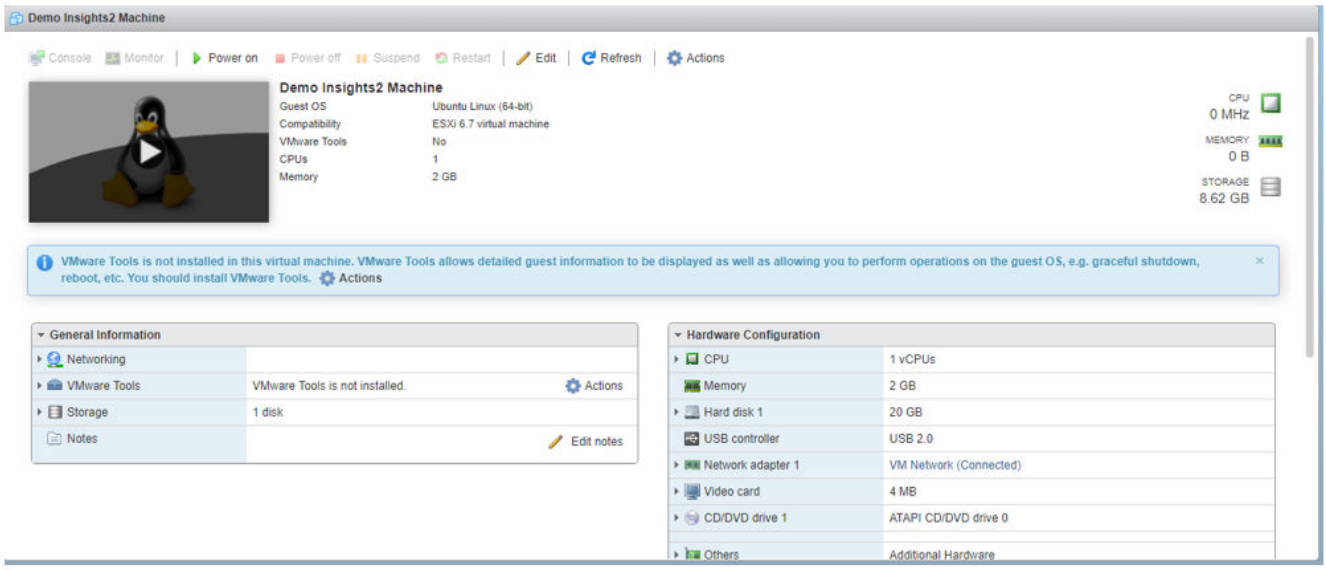


9. Click on the VM name **Demo Insights2 Machine**.

   NOTE
   The **Demo Insights2 Machine** VM is an example here.

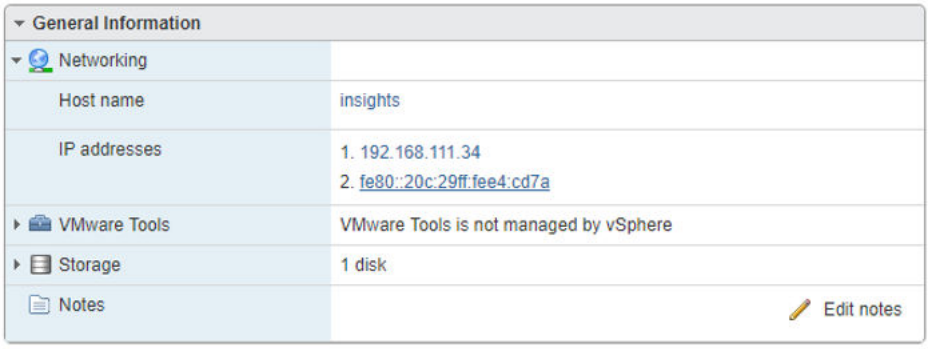
10. From the main menu, click the **Power on** to start the VM.

FIGURE 9 ESXI Startup Page



11. Under the **General Information** tab, you can view the name of the host, IP address of the VM, storage capacity etc .

FIGURE 10 ESXI Network Address

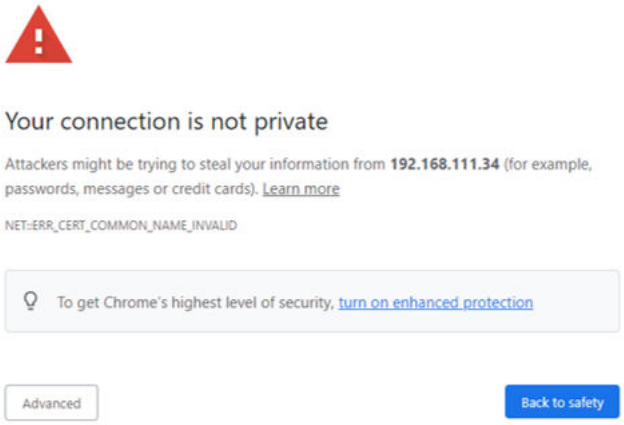


12. Open a web browser on your host machine and enter the IP address of the VM in the address bar. A warning sign with the message `Your connection is not Private` is displayed.

    In the example here, the IP address is 192.168.111.34.

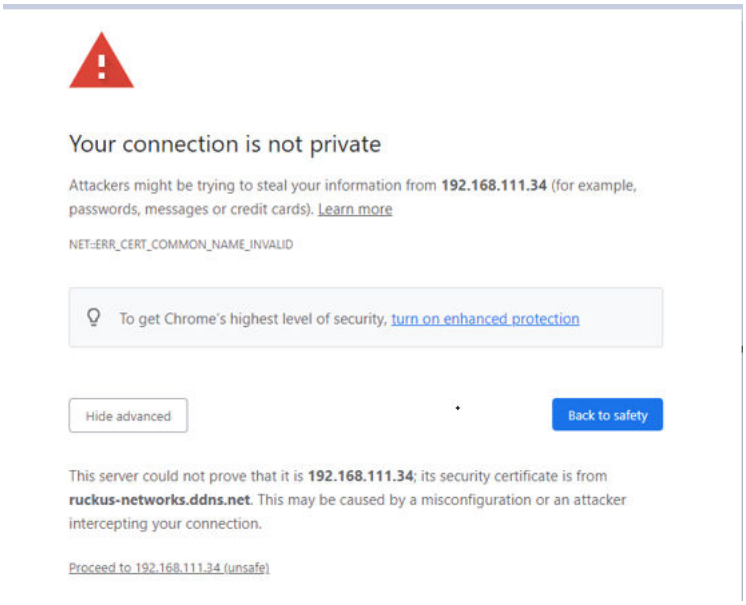
13. Click **Advanced** tab.

FIGURE 11 Clicking on Advanced Tab



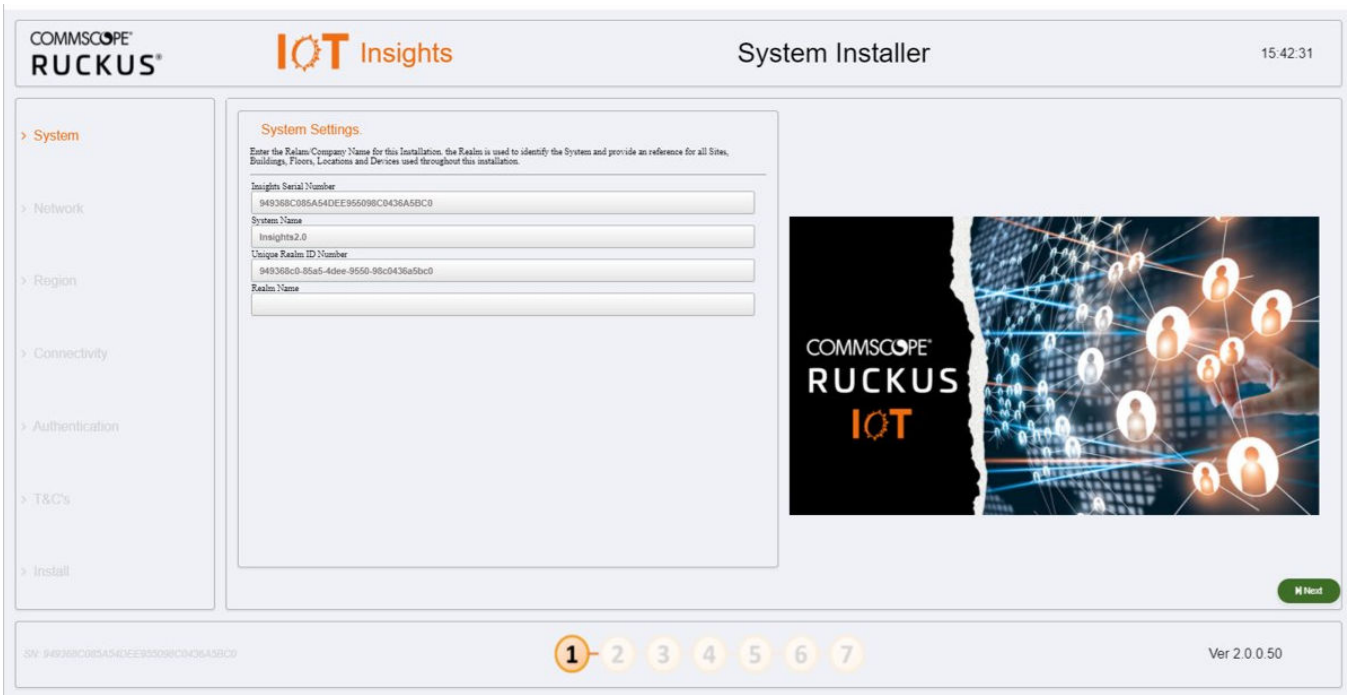
14. Click the link **Proceed to 192.168.111.34(unsafe)** to open the **IoT Insights System Installer** page.

FIGURE 12 Browser Security Accept



15. In the left navigation pane of System Installer, click **System**. The **System Settings** page is displayed. Complete the following configuration. Click **Next** after the configuration is complete.

FIGURE 13 Viewing System Settings



a) **Insights Serial Number** - The Insights serial number is unique and is auto generated during the system initalization.

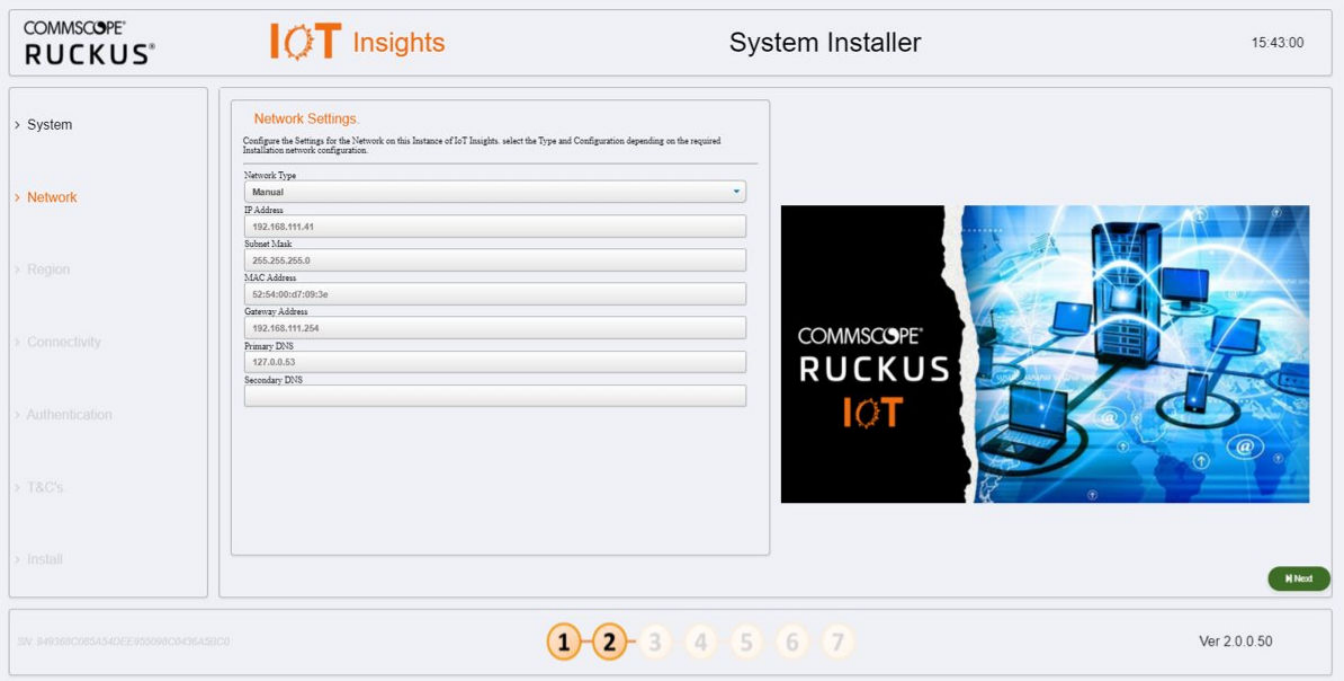
b) **System Name** - The system name is populated in this box.

c) **Unique Realm ID Number** - The Realm ID number is unique and is auto generated along with Insights Serial Number.

d) **Realm Name** - Enter the Realm Name. The Realm Name is referenced and used as part of the System Identification and Site Association process.

16. In the left navigation pane of System Installer, click **Network**. The **Network Settings** page is displayed. Complete the following configuration. Click **Next** after the configuration is completed.

FIGURE 14 Configuring Network Settings



a) **Network Type** - Select **Manual** or **DHCP** from the list. Depending upon the option selected the Dashboard page changes. In the above example, the **Network** Type is **Manual**.

b) **IP Address** - Enter the IP Address.

c) **Subnet Mask** - Enter the IP address of Subnet Mask.

d) **MAC Address** - Enter the MAC address of Machine

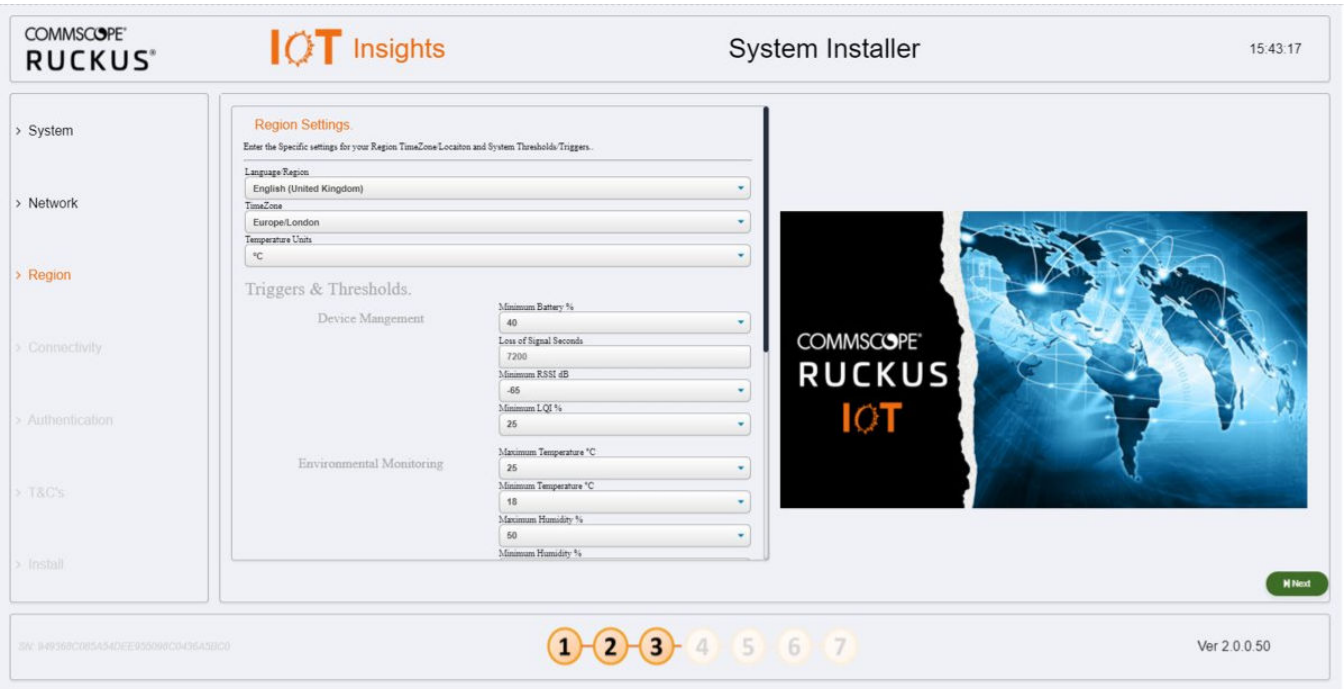
e) **Gateway Address** - Enter the IP address of Gateway.

f) **Primary DNS** - Enter the IP address of Primary DNS.

g) **Secondary DNS** - Enter the IP address of Secondary DNS.

17. In the left navigation pane of System Installer, click **Region**. The **Region Settings** page is displayed. Complete the following configuration. After selecting the regional values, click **Next**.

FIGURE 15 Configuring Region Settings



a) **Language Region** - Select the language from the list.

b) **TimeZone** - Selec the timezone from the list.

c) **Temperature Units** - Select the temperature unit from the list.

In addition to the units, the Installer can also modify any system level **Triggers** or alarm **Thresholds**. These are the values that will be used to set maximum and minimum tolerances for basic operation and alarm generation. In a lot of cases the default value will be suitable, but you can change these depending on the requirements.

18. In the left navigation pane of System Installer, click **Connectivity**. The **IoT Connectivity** page is displayed. The Insights Installer will try to auto discover the local IoT controller on the network. During this scan process, the scan window or the progress bar will increment showing that the scan is underway. After the scan is completed, you can select the IoT controller server from the **Discovered Servers** list. You can bypass this scan and enter the address of the IoT controller manaully in the field **Selected Server**. Type username in the field **Server Username**, and password in the field **Server Password**, and click **Connect**.

FIGURE 16 Scanning for the IoT Controoler

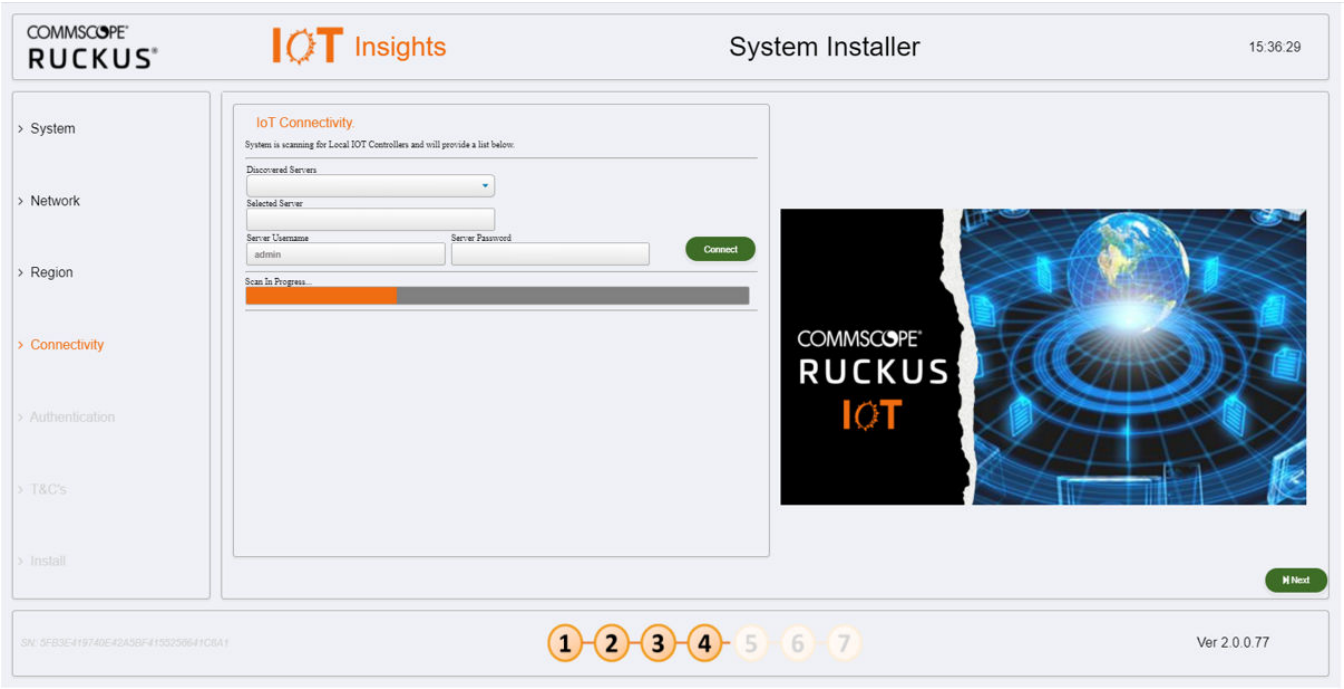


FIGURE 17 Completing the Scan

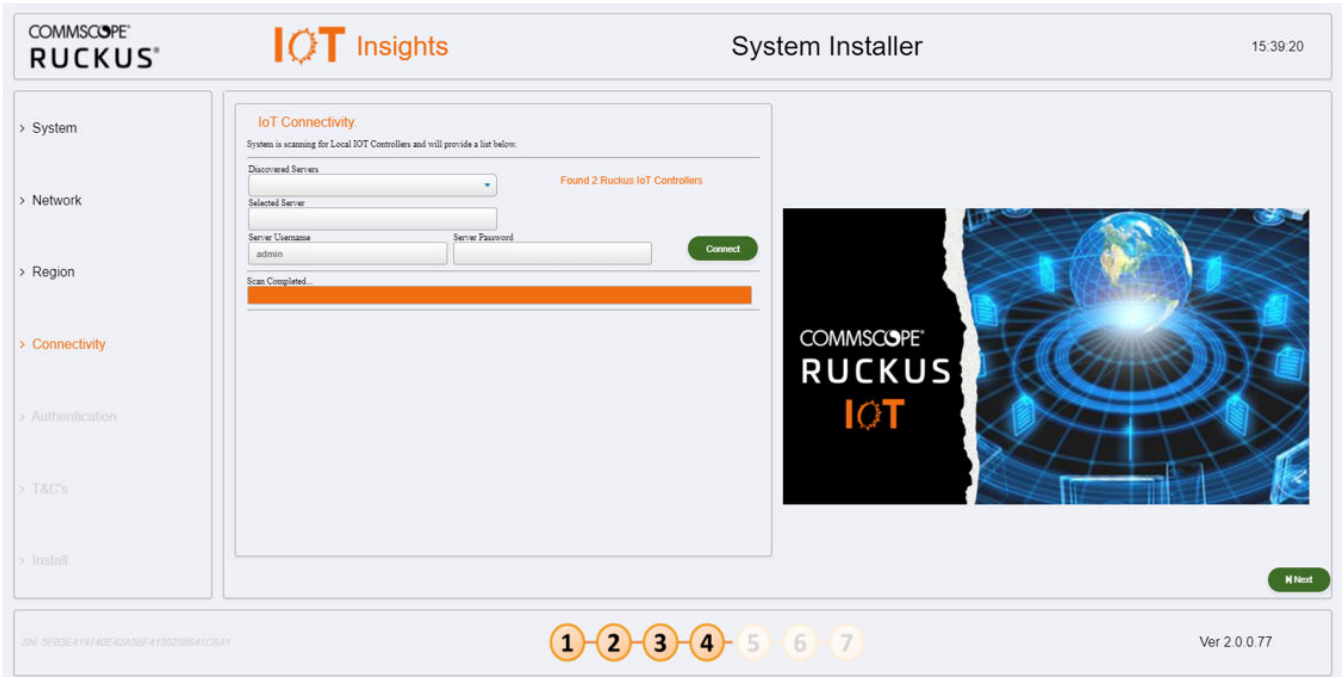
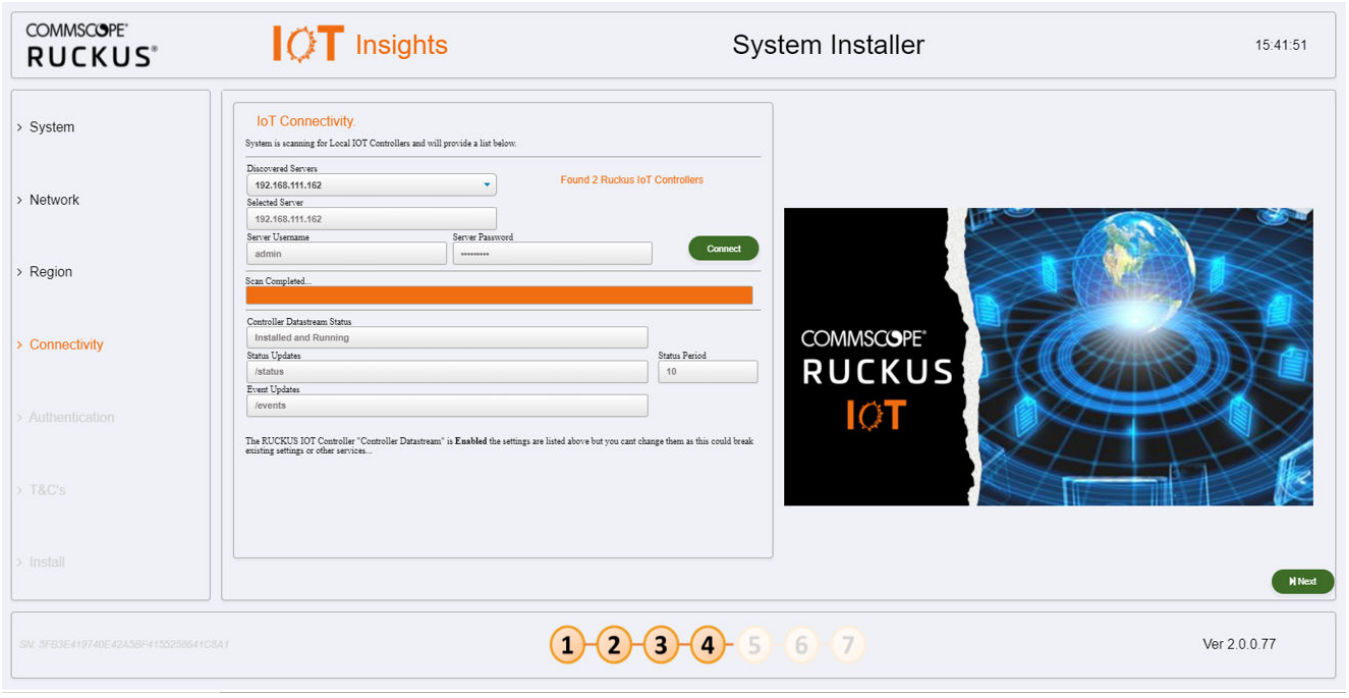


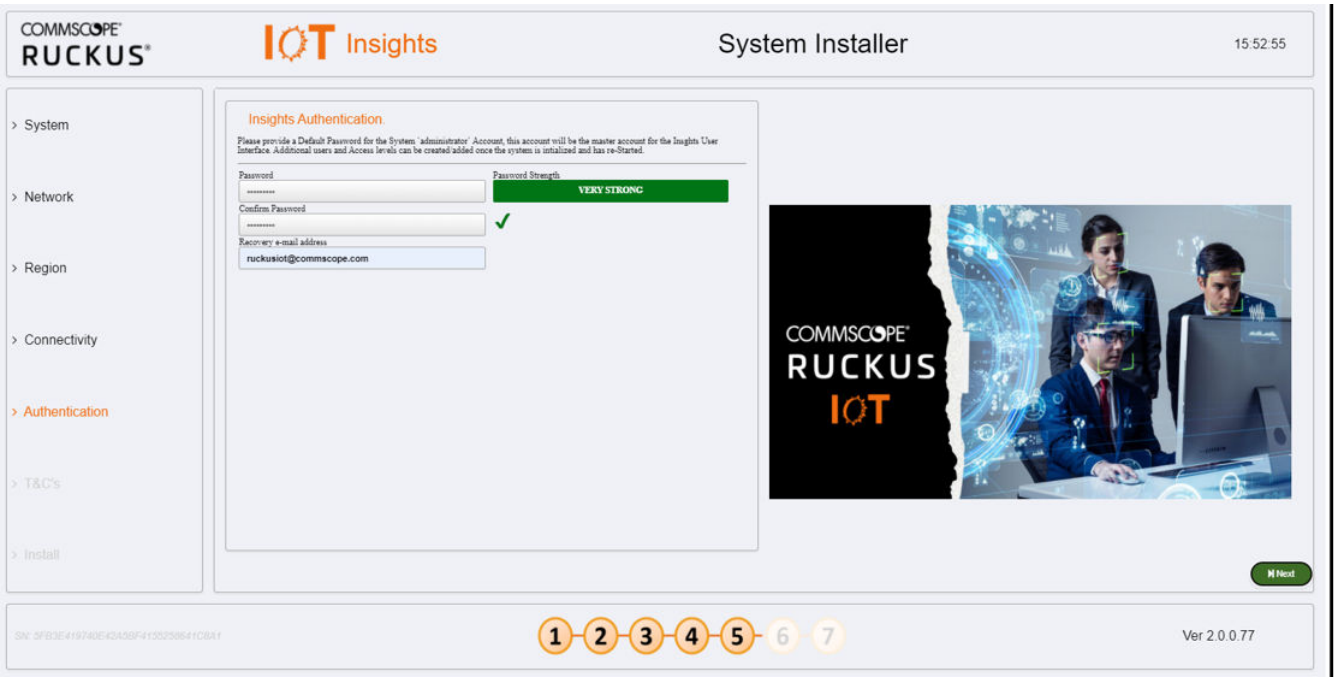
FIGURE 18 Configuring Controller Datastream Plugin



If the Controller Datastream Plugin is already configured on the controller then the status of **Controller Datastream Plugin**, **Status Update** and **Event Update** is displayed on the Installer. If it is not configured, then the system can be configured from the Installer and provisioned in the IoT controller as part of the setup process. Click **Next**.

19. In the left navigation pane of System Installer, click **Authentication**. The **Insights Connectivity** page is displayed. Complete the following configuration. Click **Next** after the configuration is completed.

FIGURE 19 Configuring the Insights Authentication



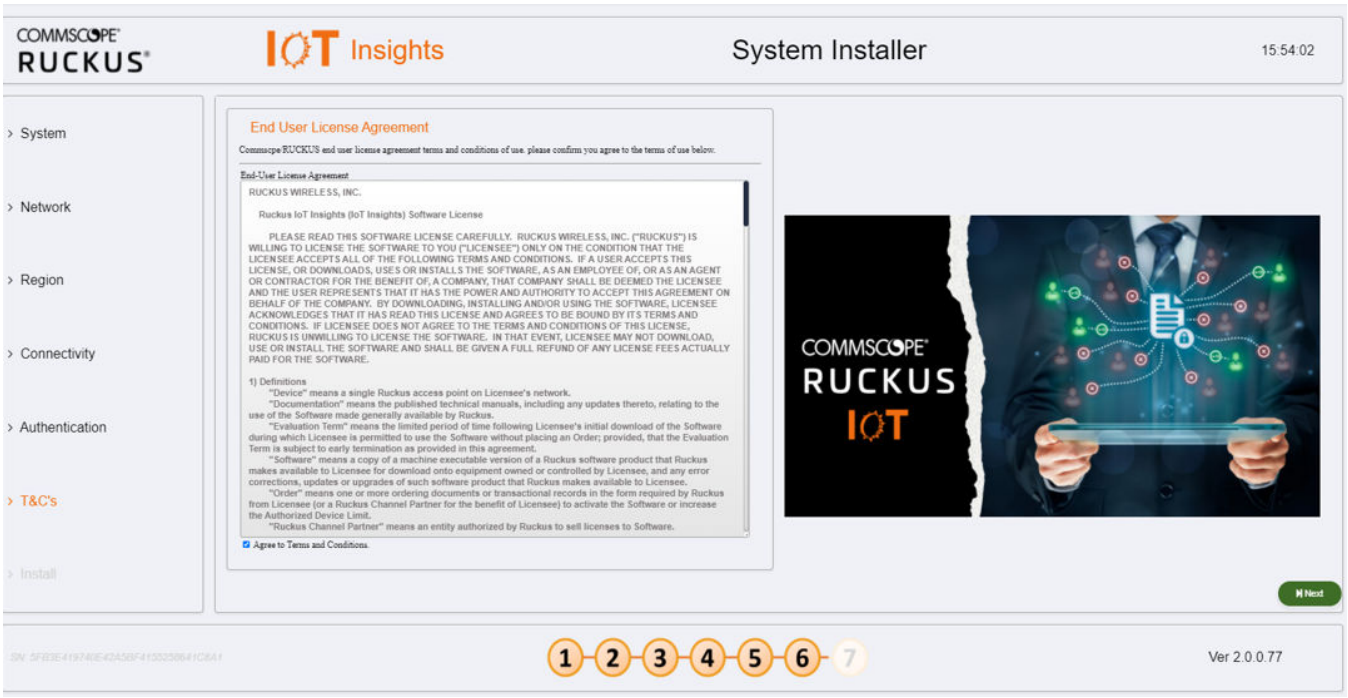
a) **Password** - Enter the Administration password. To have a strong password, confirm the following criteria are met.
   - The length of the password must be 8 characters long.
   - The password must have both upper and lower case letters.
   - It must have minimum one number.
   - It must have one special character.

b) **Confirm Password** - Type the password again in this field.

c) **Recovery email address** - Type the recovery email address.

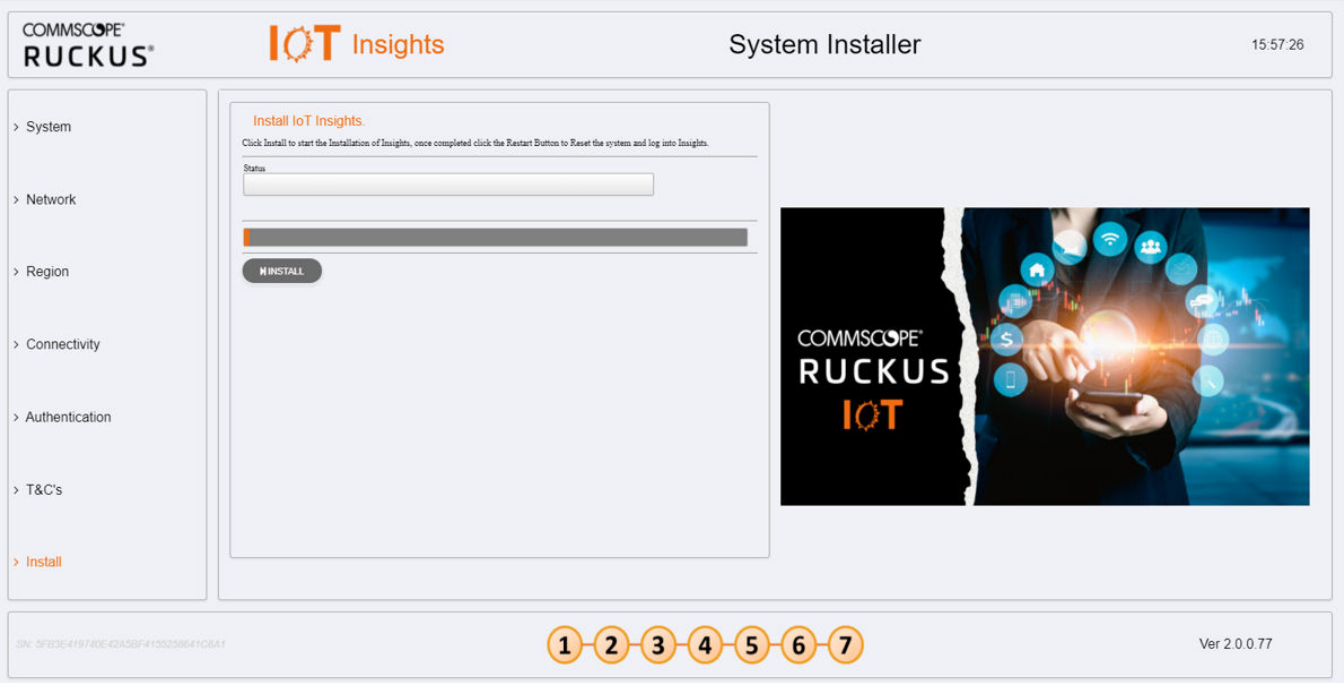
20. In the left navigation pane of System Installer, click **Terms and Conditions**.The **End User License Agreement** page is displayed. Click the **Agree to Terms and Conditions** checkbox, click the **Next** tab to perform the final installation step.

FIGURE 20 Configuring the End License Agreement



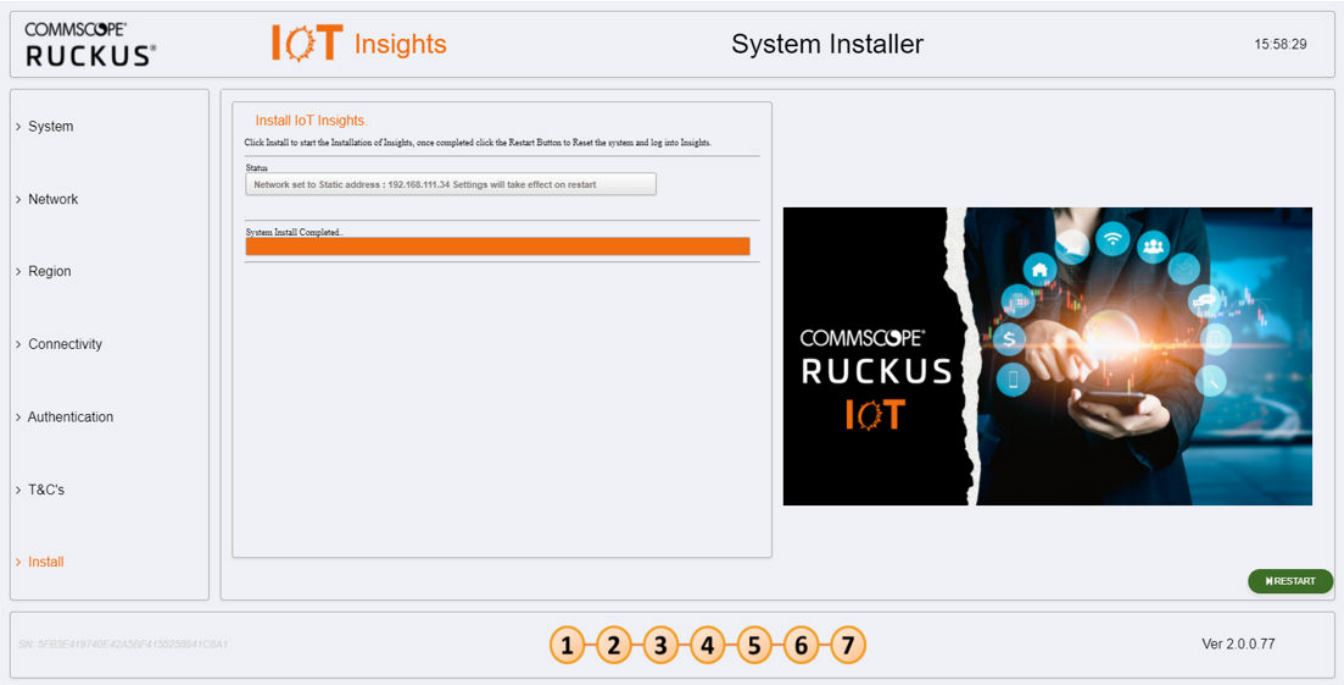
21. In the left navigation pane of System Installer, click **Install** to start the installation process. The **Install IoT Insights** page is displayed. The system will update the Installer with the current status, and the progress bar will show the total progress of the installation.

FIGURE 21 Configuring the IoT Install Insights



After the installation has completed, click **Restart**.

FIGURE 22 Restarting the IoT Insights

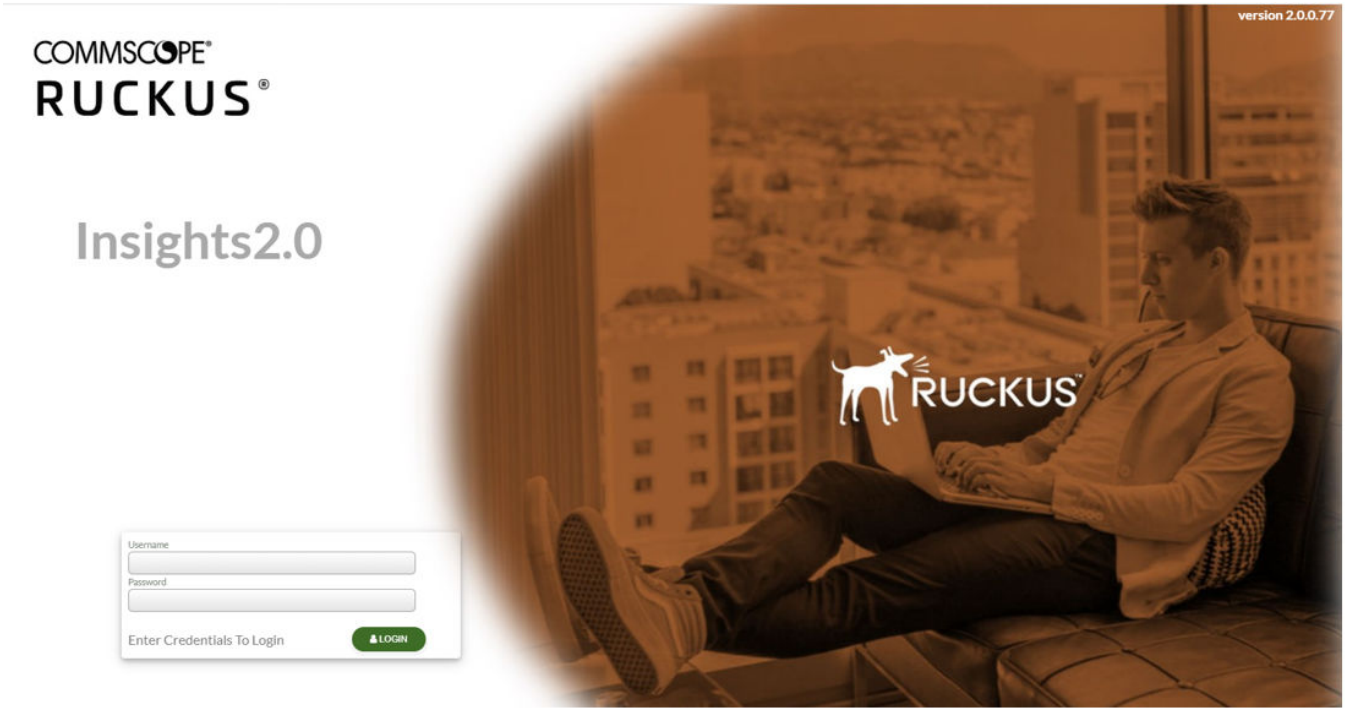


The following page appears showing the progress bar indicating the status of the restarting process.

FIGURE 23 Rebooting the IoT Insights

22. After the restart is completed, a login screen is displyed. The Administration can now enter the username and password and click **Login**.

FIGURE 24 Logging into IoT Insights



Installing RUCKUS IoT Insights on Amazon Web Service

- Setting up an AWS Account..... 31
- Configuring the AWS Command Line Interface..... 33
- Installing Insights..... 34

Installing Insights under Amazon Web Service (AWS) requires the set-up of two parts. The first part includes setting up an AWS account. The second part includes obtaining and configuring the AWS Command Line Interface (CLI).

Setting up an AWS Account

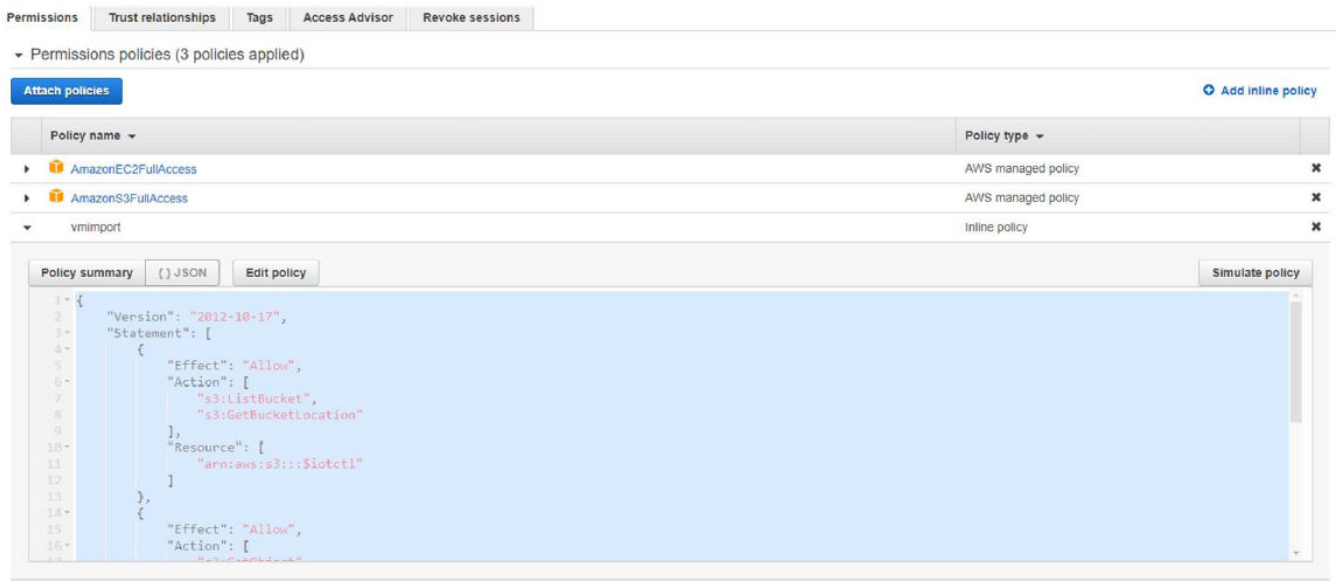
Perform the following steps to set-up an AWS account.

1. Login into the AWS console using the url `https://aws.amazon.com/console/`
2. Select **Services** > **Security** > **Identity and Compliance** > **IAM**.
3. Click **Users** in the left pane.
   a) Under the column **User name**, select a user from the group of users .
   b) Click **Security Credentials** tab.
   c) In the **Access Key** section, click **Create Access Key**.
   d) Click **Download .CSV file**.
4. Select **Roles** in the left pane and create a new role called **vmimport**.
5. Select the **vmimport** role and attach the following policies:

6. Edit the vmimport policy JSON file {} as per the following code.
7. Download the access keys (excel file).

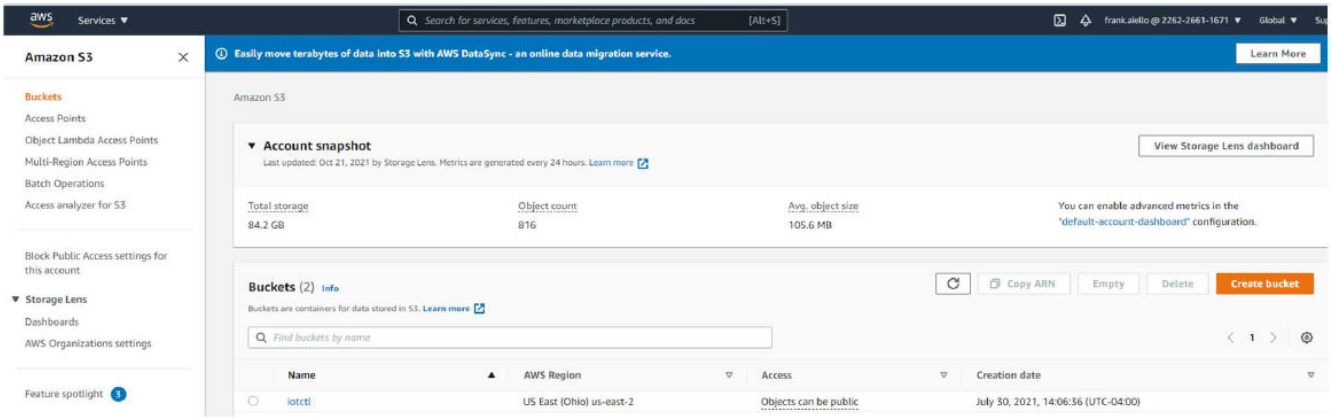
8. Select **Roles** in the left pane, and create a new role called “vmimport”

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"s3:ListBucket",
"s3:GetBucketLocation"
],
"Resource": [
"arn:aws:s3:::$iotctl"
]
},
{
"Effect": "Allow",
"Action": [
"s3:GetObject"
],
"Resource": [
"arn:aws:s3:::$iotctl/*"
]
},
{
"Effect": "Allow",
"Action": [
"ec2:ModifySnapshotAttribute",
"ec2:CopySnapshot",
"ec2:RegisterImage",
"ec2:Describe*"
],
"Resource": "*"
}
]
}
```



9. Select **System** > **S3**.

10. Create S3 bucket **iotcl**.



11. Download the IoT Insights2 .ova file from the Ruckus support site or `https://ruckus-networkssoleng.s3.eu-west-2.amazonaws.com/Insights2/Insights2.0.0.93.ova`.
12. Upload the Insights2 .ova file to the **iotctl** s3 bucket.

Configuring the AWS Command Line Interface

Before completing the Command Line Interface (CLI) steps ensure you have the log-in details for the AWS account and access keys.

1. Open the command prompt, and enter the below commands.
   - sudo apt-get update
   - sudo apt-get install awscli
   - aws --version

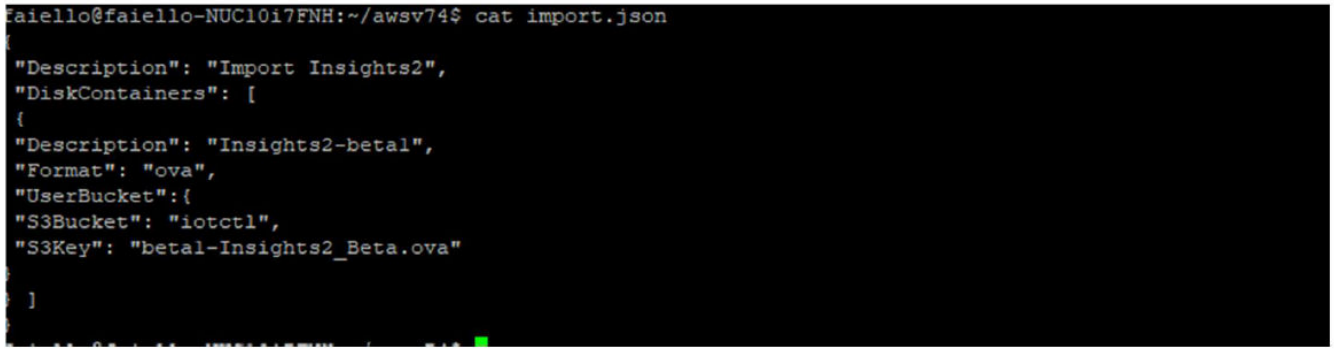
```
faiello@faiello-NUC10i7FNH:~/awsv74$ aws --version
aws-cli/1.20.10 Python/3.7.5 Linux/5.3.0-64-generic botocore/1.21.10
faiello@faiello-NUC10i7FNH:~/awsv74$
```

2. Configure the AWS CLI using the access keys as below.

   NOTE
   Ensure the region name that is entered is the same as in AWS account set-up.

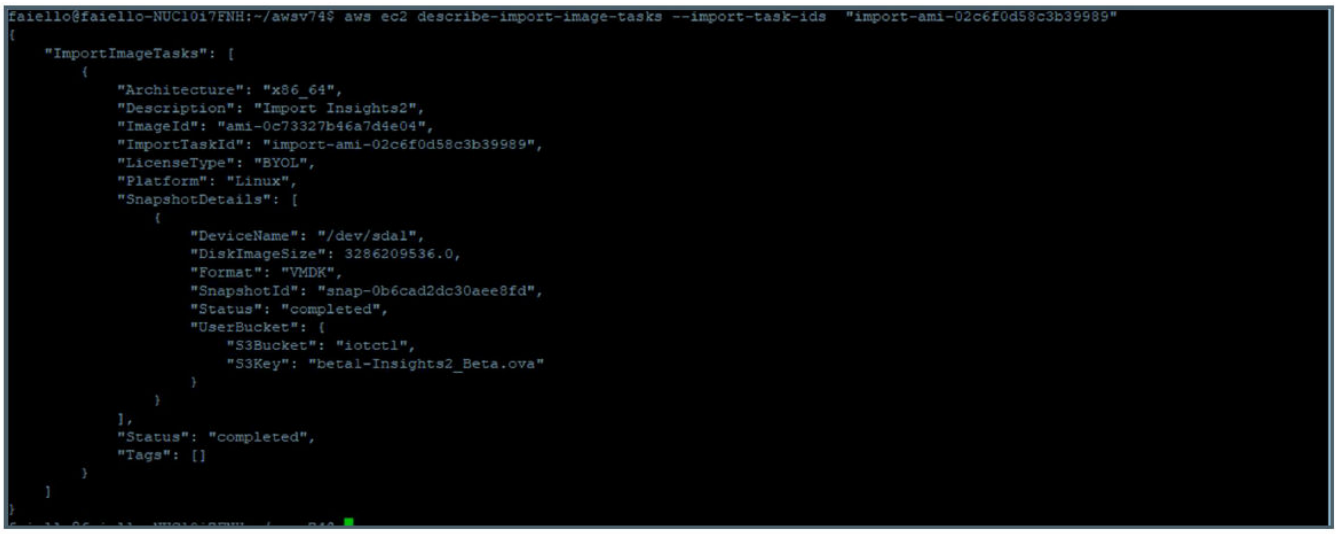
```
faiello@faiello-NUC10i7FNH:~/awsv74$ aws configure
AWS Access Key ID [****************I2UH]:
AWS Secret Access Key [****************6dSf]:
Default region name [us-east-2]:
Default output format [json]:
faiello@faiello-NUC10i7FNH:~/awsv74$
```

3. Create a JSON file called “import.json” The file should contain the following:



NOTE
Replace the "S3Key" with the correct file name of the Insights2 .ova file.

4. Enter the command **aws ec2 import-image --cli-input-json file://import.json** to attach the policy to the role previously created.
5. Use the command **aws ec2 describe-import-image-tasks –import-task-ids “import-ami-of662ebae1a3c5ed4"** to monitor the status of the imported Insights ova image.



6. When the status shows “completed”, the Insights2 instance is installed in your AWS account, refer **Services** > **EC2** > **Instances**.

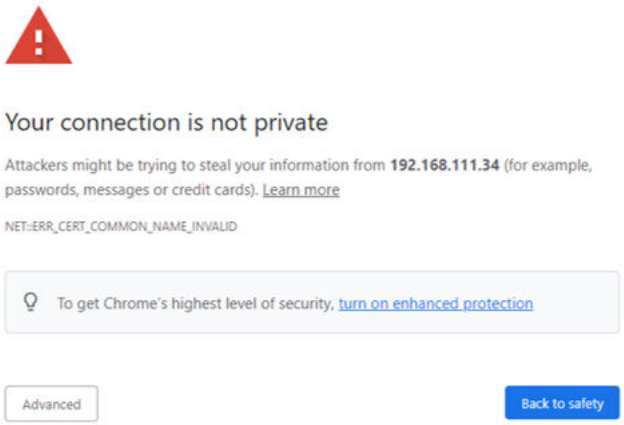
Installing Insights

1. Open a web browser on your host machine and enter the IP address of the VM in the address bar. A warning sign with the message `Your connection is not Private` is displayed.

   In the example here, the IP address is 192.168.111.34.

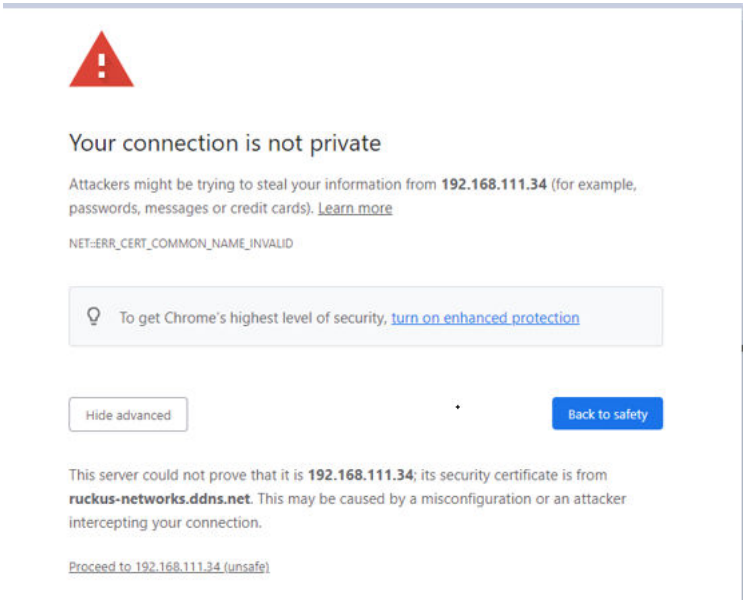
2. Click **Advanced** tab.

FIGURE 25 Clicking on Advanced Tab



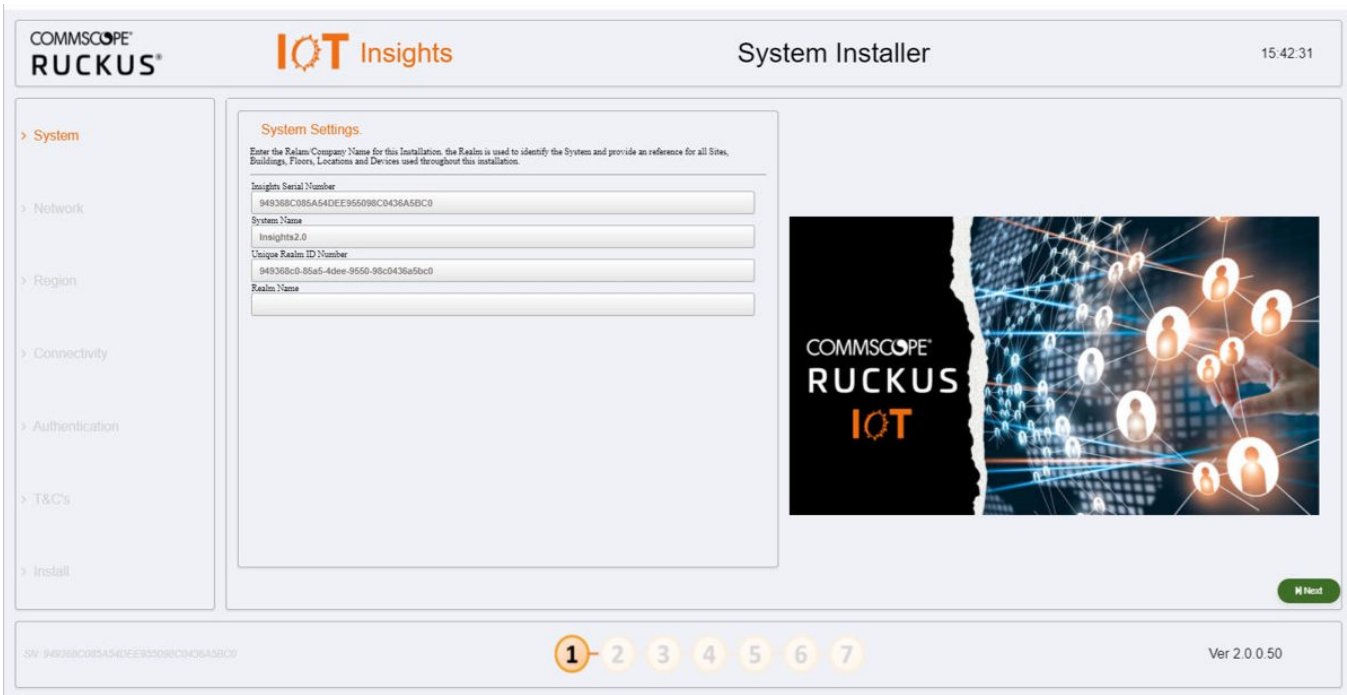
3. Click the link **Proceed to 192.168.111.34(unsafe)** to open the **IoT Insights System Installer** page.

FIGURE 26 Browser Security Accept



4. In the left navigation pane of System Installer, click **System**. The **System Settings** page is displayed. Complete the following configuration. Click **Next** after the configuration is complete.

FIGURE 27 Viewing System Settings



a) **Insights Serial Number** - The Insights serial number is unique and is auto generated during the system initalization.

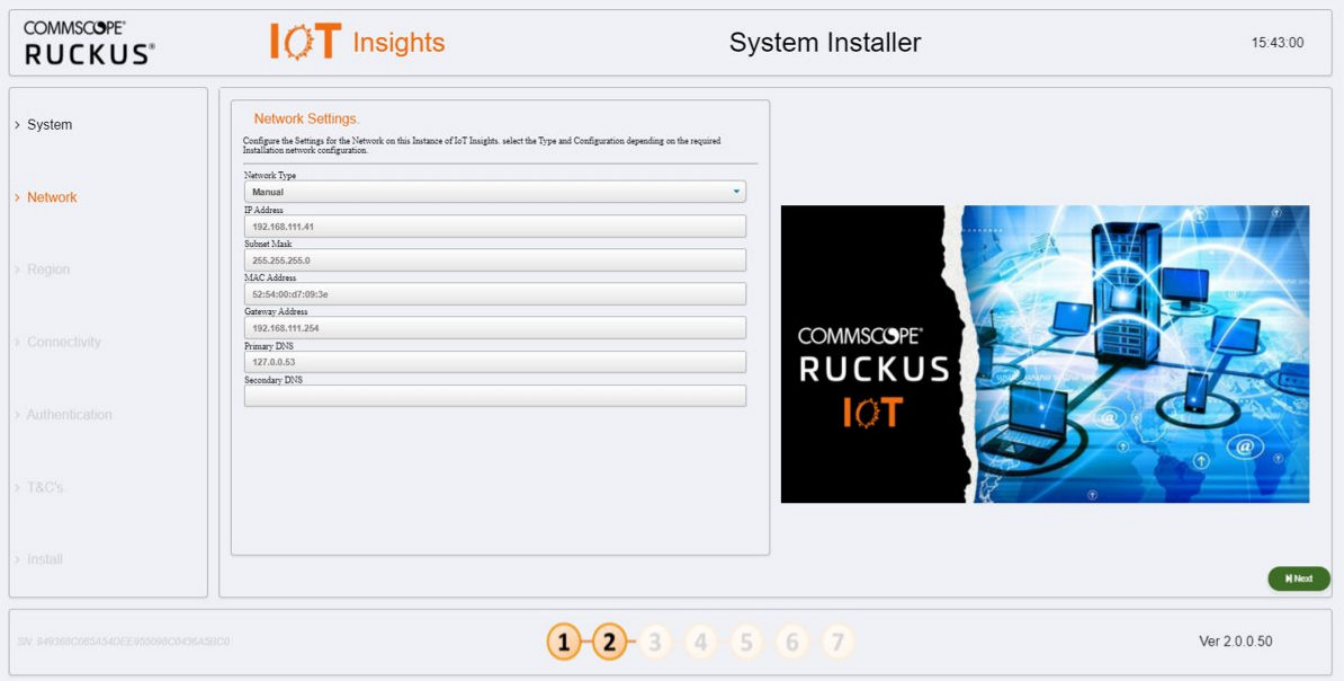
b) **System Name** - The system name is populated in this box.

c) **Unique Realm ID Number** - The Realm ID number is unique and is auto generated along with Insights Serial Number.

d) **Realm Name** - Enter the Realm Name. The Realm Name is referenced and used as part of the System Identification and Site Association process.

5. In the left navigation pane of System Installer, click **Network**. The **Network Settings** page is displayed. Complete the following configuration. Click **Next** after the configuration is completed.

FIGURE 28 Configuring Network Settings



a) **Network Type** - Select **Manual** or **DHCP** from the list. Depending upon the option selected the Dashboard page changes. In the above example the**Network Type** is **Manual**.

b) **IP Address** - Enter the IP Address.

c) **Subnet Mask** - Enter the IP address of Subnet Mask.

d) **MAC Address** - Enter the MAC address of Machine

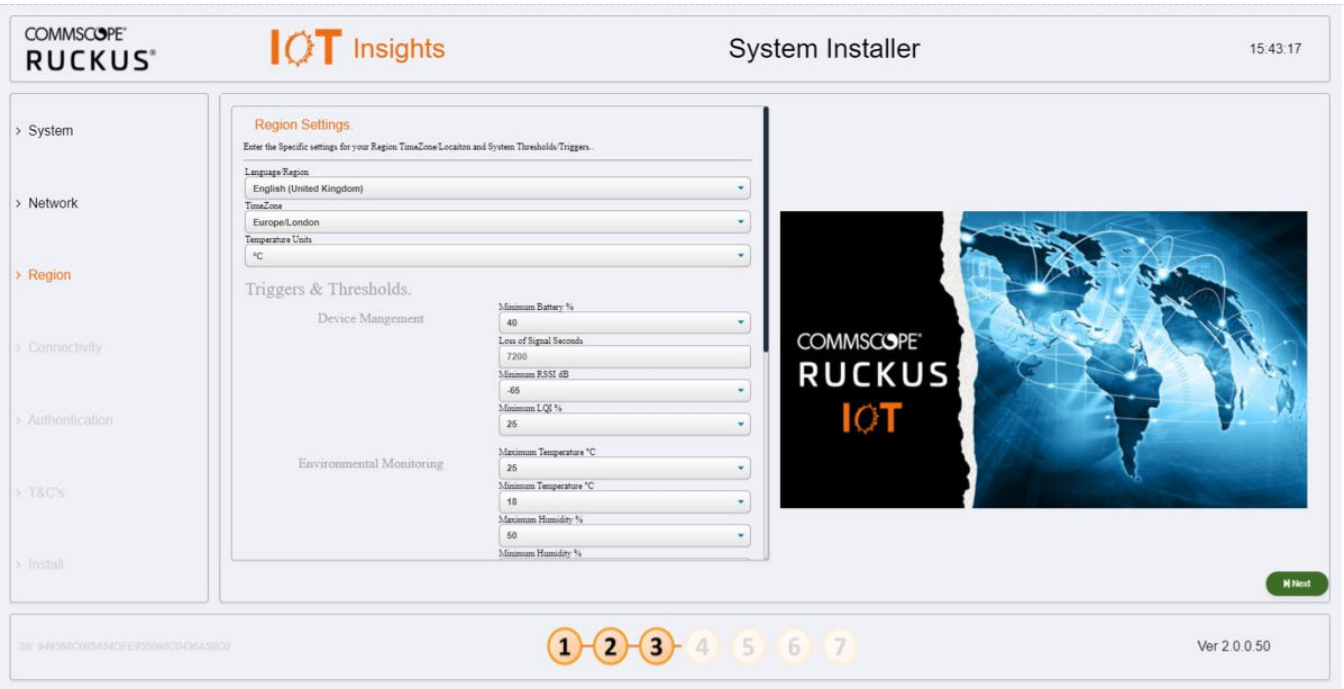
e) **Gateway Address** - Enter the IP address of Gateway.

f) **Primary DNS** - Enter the IP address of Primary DNS.

g) **Secondary DNS** - Enter the IP address of Secondary DNS.

6. In the left navigation pane of System Installer, click **Region**. The **Region Settings** page is displayed. Complete the following configuration. After selecting the regional values, click **Next**.

FIGURE 29 Configuring Region Settings



a) **Language Region** - Select the language from the list.

b) **TimeZone** - Selec the timezone from the list.

c) **Temperature Units** - Select the temperature unit from the list.

In addition to the units, the Installer can also modify any system level **Triggers** or alarm**Thresholds**. These are the values that will be used to set maximum and minimum tolerances for basic operation and alarm generation. In a lot of cases the default value will be suitable, but you can change these depending on the requirements.

7. In the left navigation pane of System Installer, click **Connectivity**. The **IoT Connectivity** page is displayed. The Insights Installer will try to auto discover the local IoT controller on the network. During this scan process the scan window or the progress bar will increment showing that the scan is underway. After the scan is completed, you can select the IoT controller server from the **Discovered Servers** list. You can bypass this scan and enter the address of the IoT controller manaully in the field **Selected Server**. Type username in the field **Server Username**, and password in the field **Server Password** and click **Connect**.

FIGURE 30 Scanning for the IoT Controoler

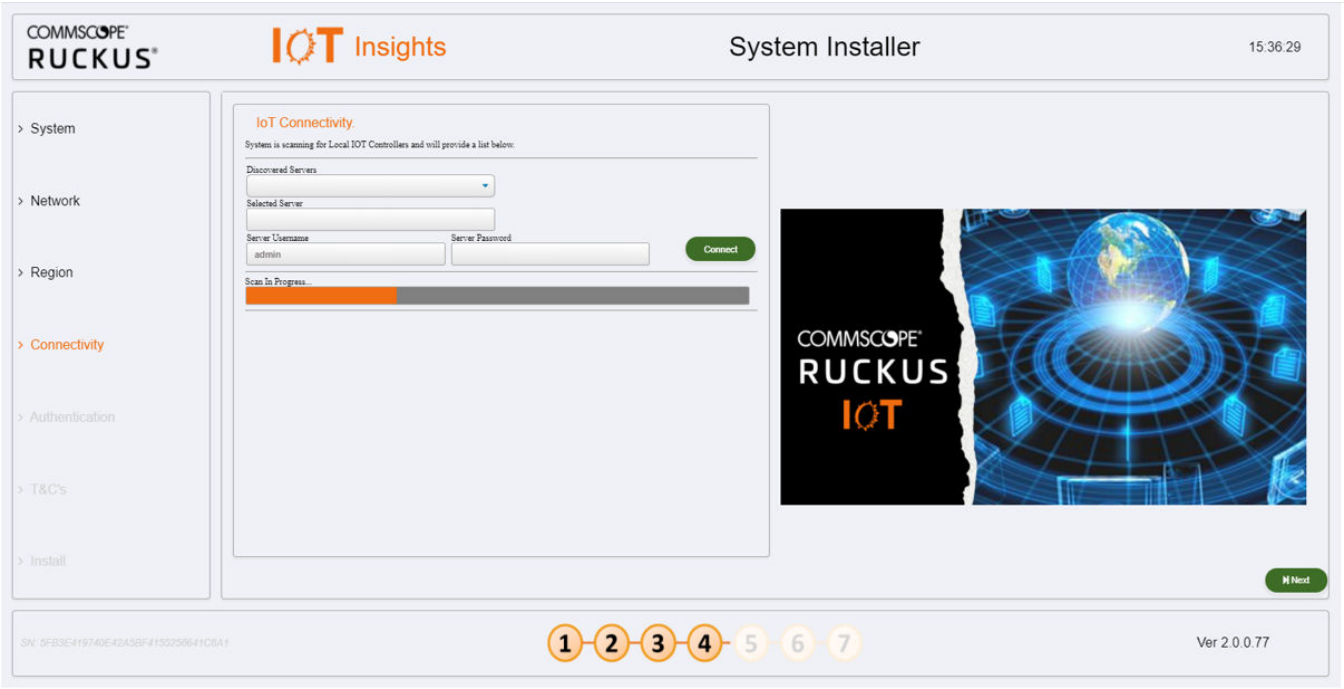


FIGURE 31 Completing the Scan

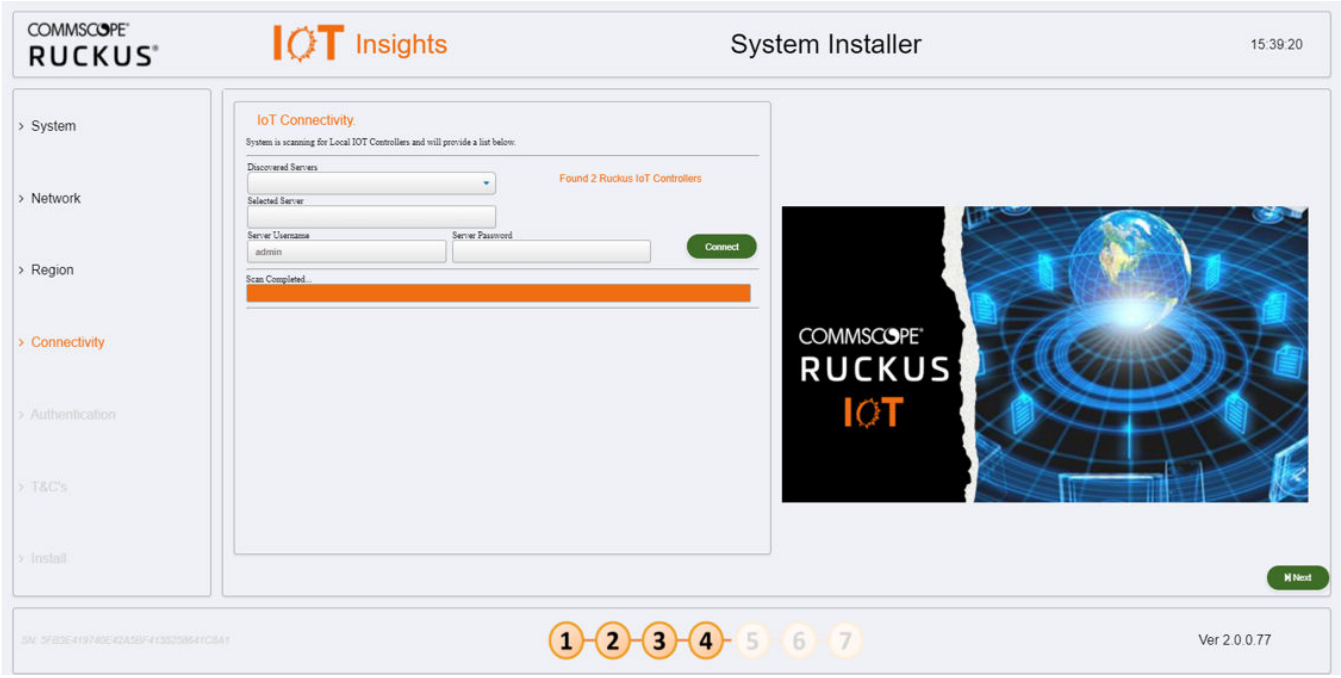
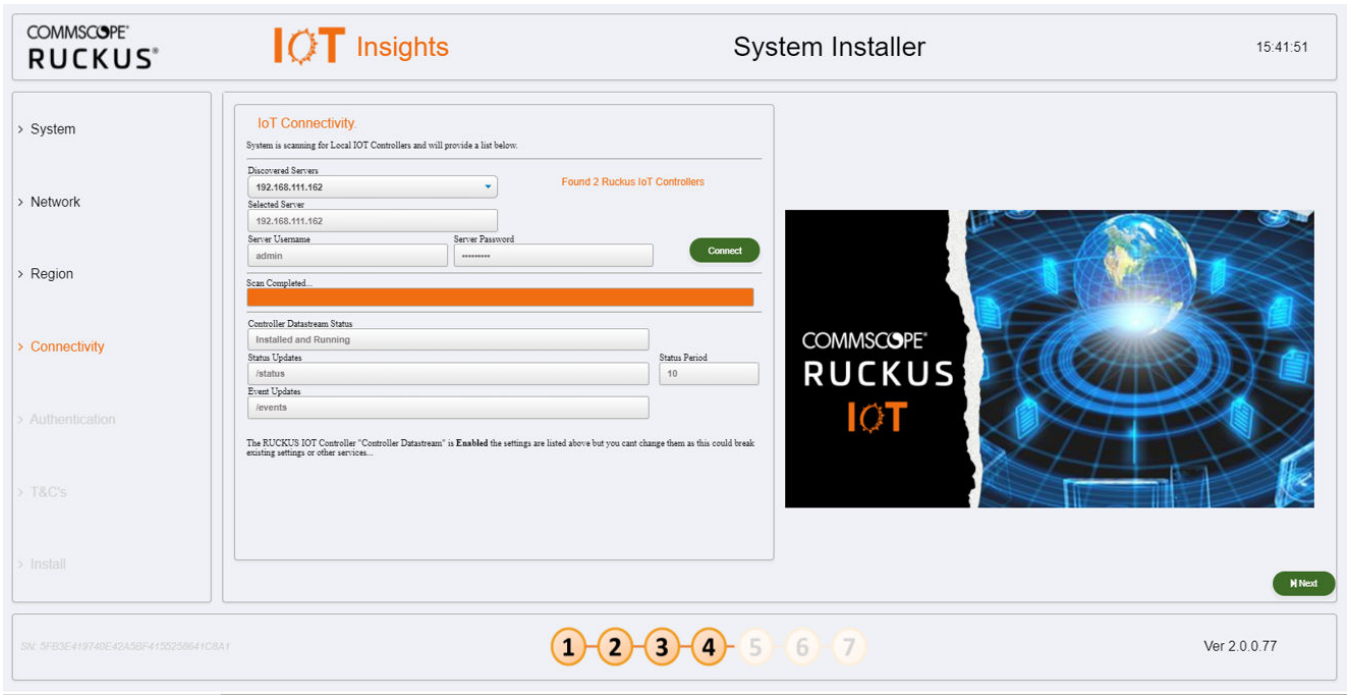


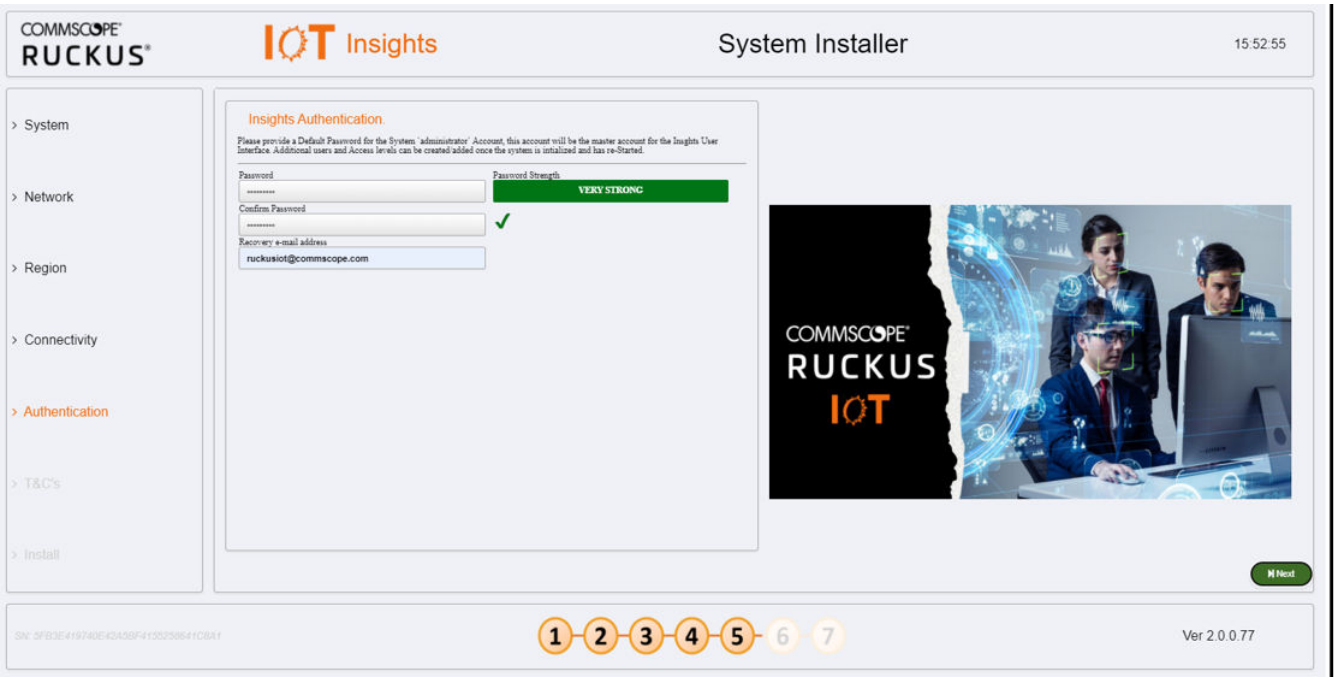
FIGURE 32 Configuring Controller Datastream Plugin



If the Controller Datastream Plugin is already configured on the controller then the status of **Controller Datastream Plugin**, **Status Update** and **Event Update** is displayed on the Installer. If it is not configured, then the System can be configured from the Installer and provisioned in the IoT controller as part of the setup process. Click **Next**.

8. In the left navigation pane of System Installer, click **Authentication**. The **Insights Connectivity** page is displayed. Complete the following configuration. Click **Next**. Click **Next** after the configuration is completed.

FIGURE 33 Configuring the Insights Authentication



a) **Password** - Enter the Administration password. Ensure that the strength of the password is strong.

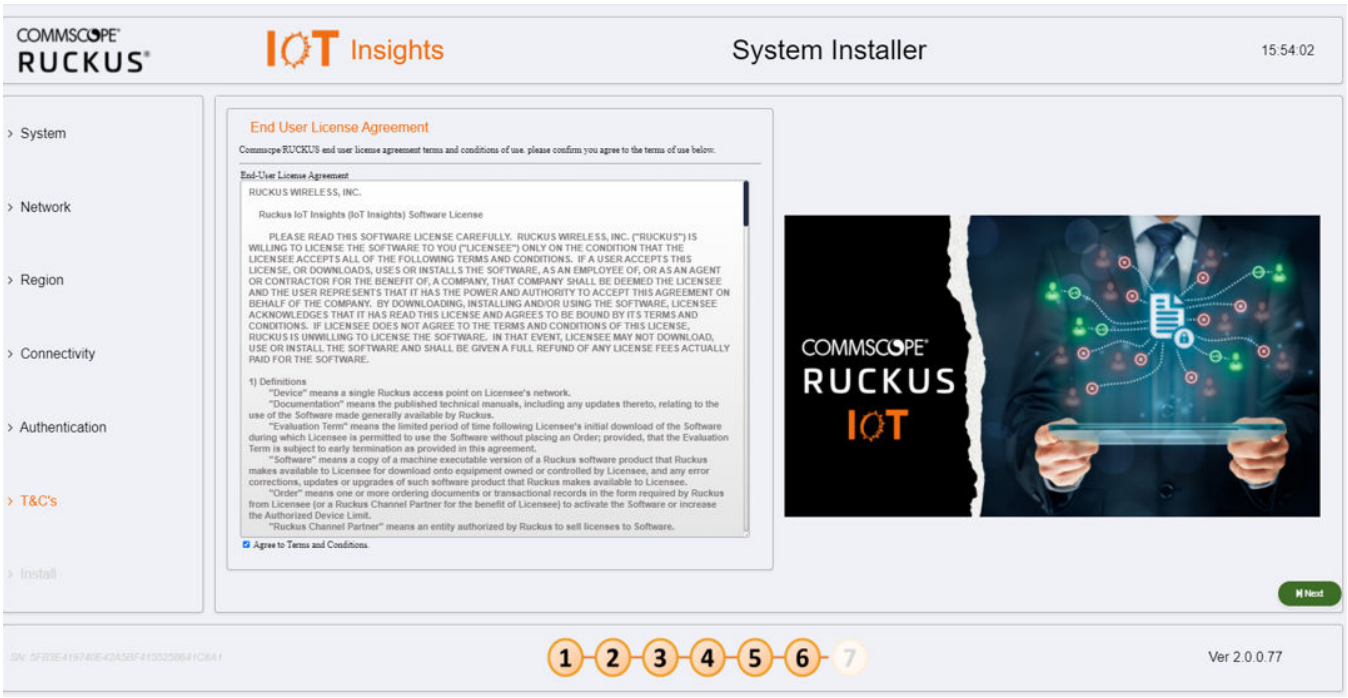
- The length of the password must be 8 characters long.
- The password must have both upper and lower case letters.
- It must have minimum one number.
- It must have one special character.

a) **Confirm Password** - Type the password again in this field.

b) **Recovery email address** - Type the recovery email address.

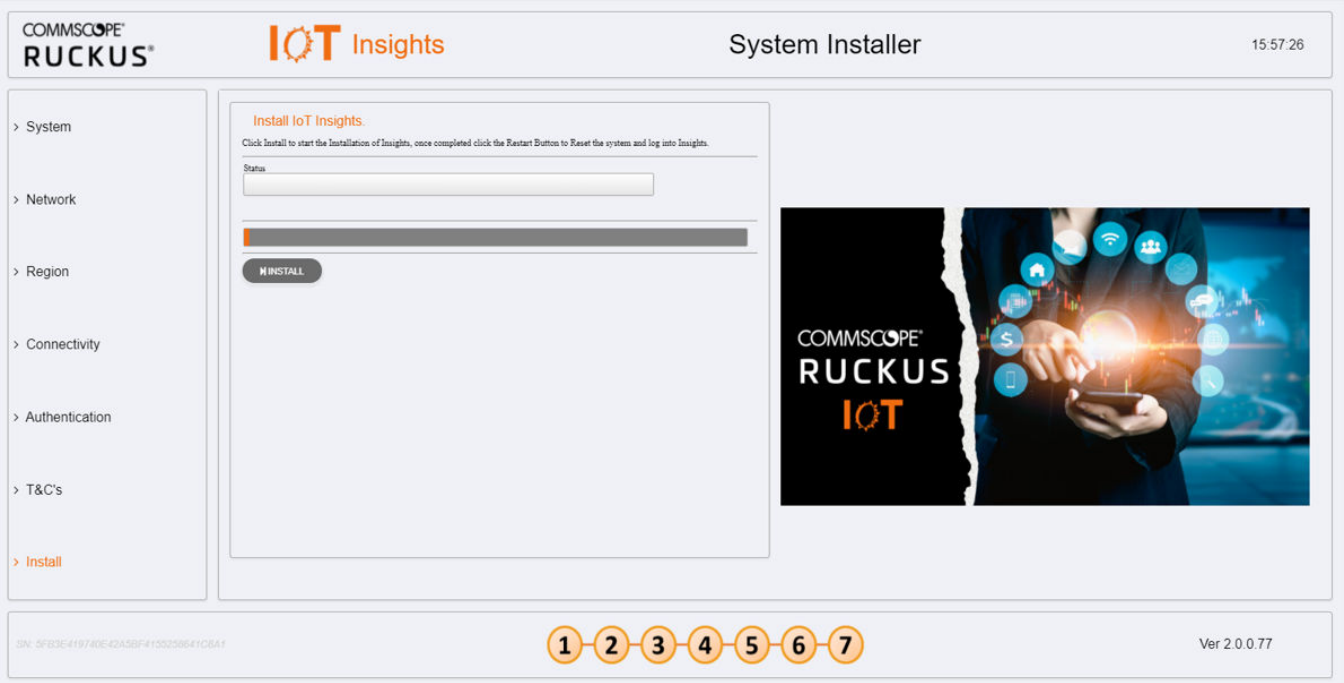
9. In the left navigation pane of System Installer, click **Terms and Conditions**.The **End User License Agreement** page is displayed. Click the **Agree to Terms and Conditions** checkbox, click the **Next** tab to perform the final installation step.

FIGURE 34 Configuring the End License Agreement



10. In the left navigation pane of System Installer, click **Install** to start the installation process. . The **Install IoT Insights** page is displayed. Click **Install**. The system will update the Installer with the current status, and the progress bar will show the total progress of the installation.

FIGURE 35 Configuring the IoT Install Insights

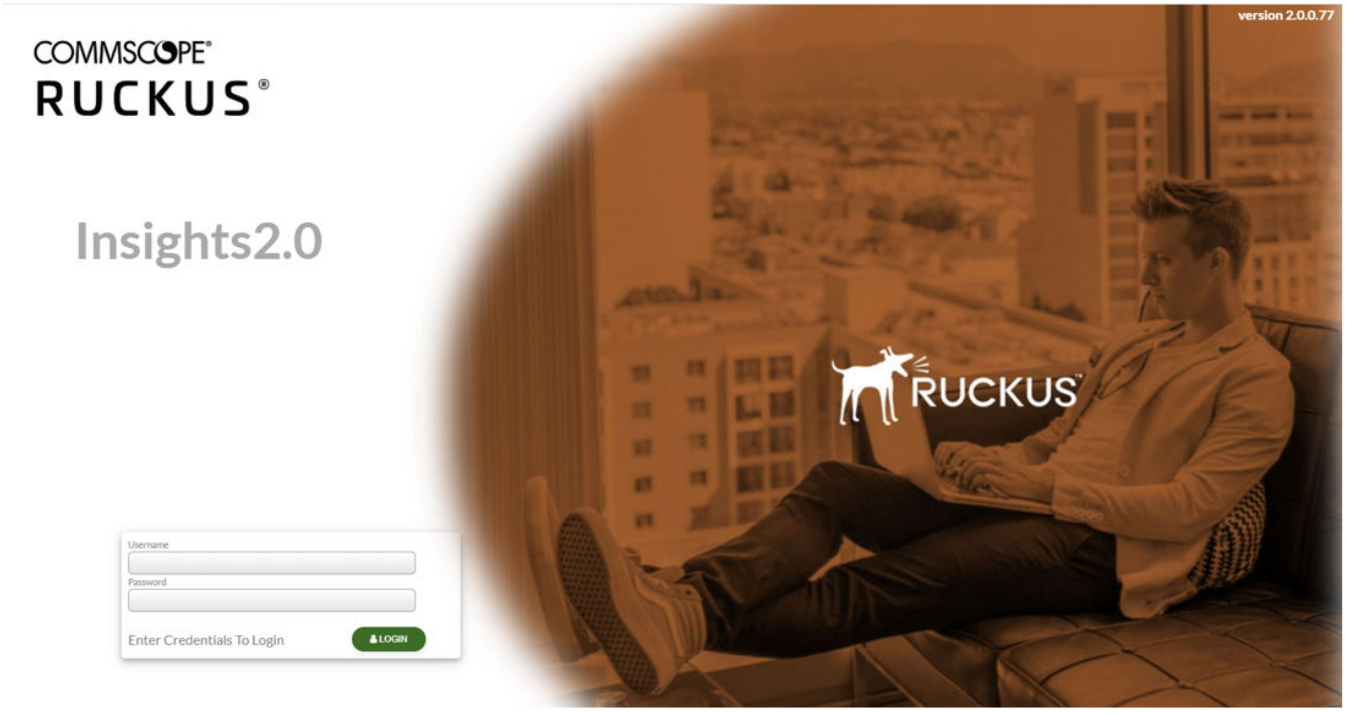


The following page appears showing the progress bar indicating the status of the restarting process.

FIGURE 36 Rebooting the IoT Insights

11. After the restart is completed, a login screen is displyed. The Administration can now enter the username and password and click **Login**.

FIGURE 37 Logging into IoT Insights



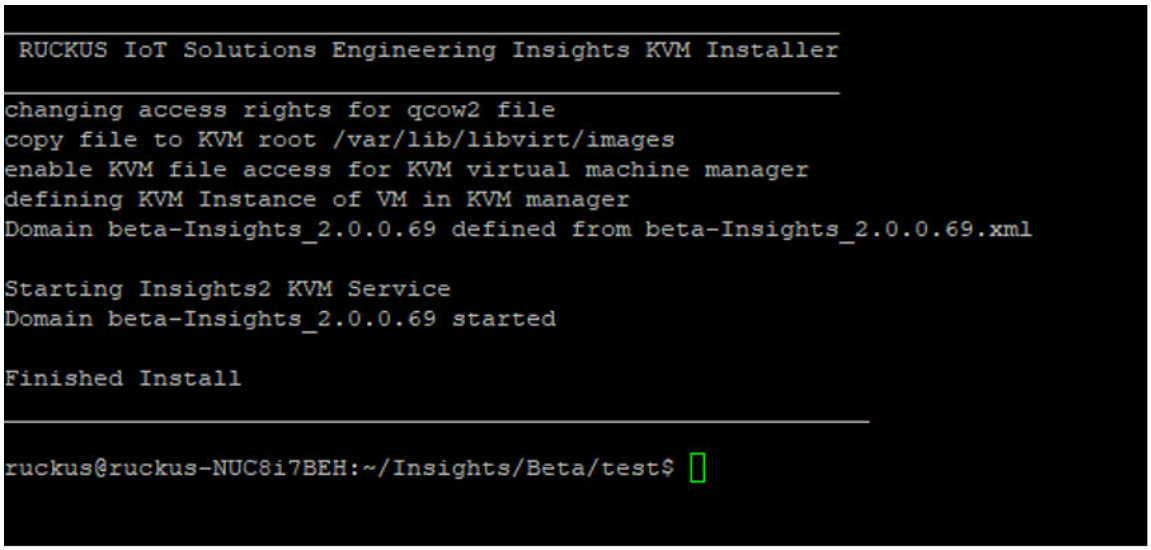
Installing RUCKUS IoT Insights on Linux KVM Machine

The RUCKUS IoT Insights software is provided in a compressed zip file containing all of the basic functions needed to setup install and provission the Insights platform on your own Virtual Machine (VM).

1. Downlaod the Beta file beta-Insights-qcow2_2.0.0.69.tar from the repository.
2. Use the **tar xvf beta-Insights-qcow2_2.0.0.69.tar** command to unzip the file.This will then provide the following 4 files.
   - ruckus@ruckus-NUC8i7BEH:~/Insights/Beta/test$ tar xvf beta-Insights-qcow2_2.0.0.69.tar
   - beta-Insights-qcow2_2.0.0.69.qcow2
   - beta-Insights_2.0.0.69.xml
   - install.sh
   - un-install.sh
   - ruckus@ruckus-NUC8i7BEH:~/Insights/Beta/test$

   To ease the setup, the system provides pre-configured xml, and scripts to install and configure the system. This script and xml file assumes certain file locations for KVM and Bridge configuration for Linux, if these are different the system wil not work and will need to be changed for correct operation.
3. Run the Installer to install the `ruckus@ruckus-NUC8i7BEH:~/Insights/Beta/test$ ./install.sh`, VM and start the system.

FIGURE 38 Viewing Insights KVM Installer



4. After the installation is completed, the system will start automatically and Insights 2 image will boot. You can verify this by using the command **virsh list –all**.

FIGURE 39 Viewing the Beta Insights Image Using the Virsh Command

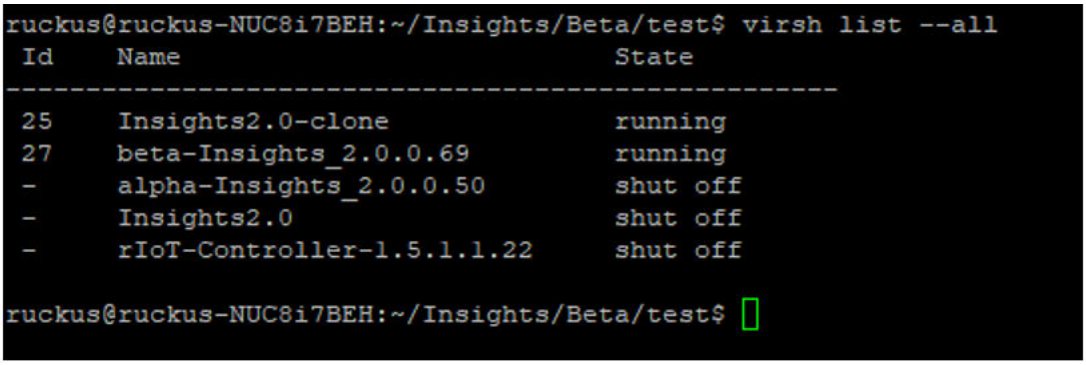
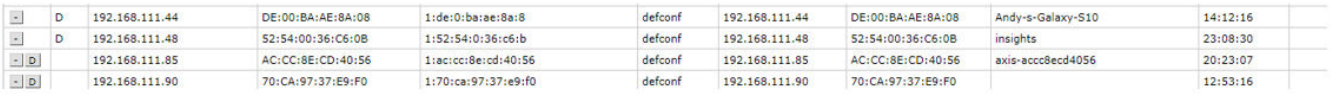


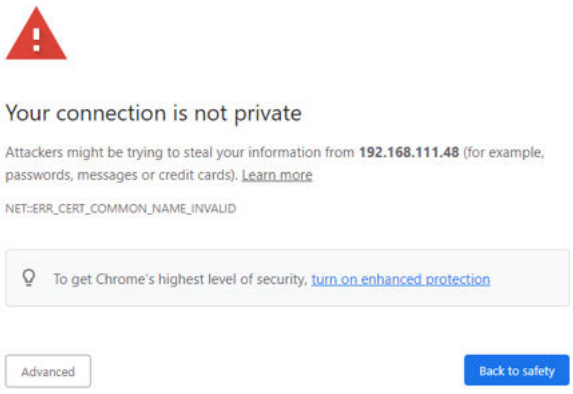
FIGURE 40 Viewing the IP address of Insights Server



-	D	192.168.111.44	DE:00:BA:AE:8A:08	1:de:0:ba:ae:8a:8	defconf	192.168.111.44	DE:00:BA:AE:8A:08	Andy-s-Galaxy-S10	14:12:16	
-	D	192.168.111.48	52:54:00:36:C6:0B	1:52:54:0:36:c6:b	defconf	192.168.111.48	52:54:00:36:C6:0B	insights	23:08:30	
- D		192.168.111.85	AC:CC:8E:CD:40:56	1:ac:cc:8e:cd:40:56	defconf	192.168.111.85	AC:CC:8E:CD:40:56	axis-accc8ecd4056	20:23:07	
- D		192.168.111.90	70:CA:97:37:E9:F0	1:70:ca:97:37:e9:f0	defconf	192.168.111.90	70:CA:97:37:E9:F0		12:53:16	

5. You must connect to the Host Insight web server using the web browser https://192.168.88.48.

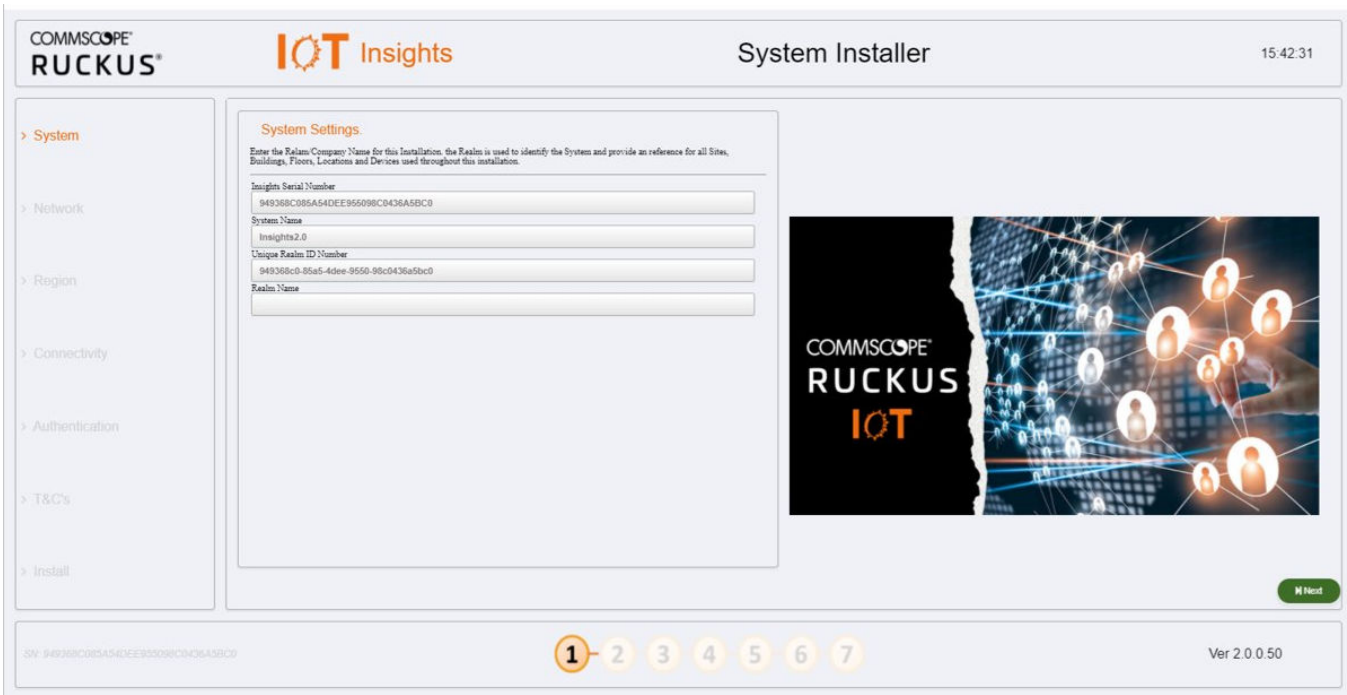
FIGURE 41 Connecting to the IP address of Installer



6. Click **Advanced** tab.
7. Click the link **Proceed to 192.168.111.48(unsafe)** to open the **IoT Insights System Installer** page.

8. In the left navigation pane of System Installer, click **System**. The **System Settings** page is displayed. Complete the following configuration. Click **Next** after the configuration is complete.

FIGURE 42 Viewing System Settings



a) **Insights Serial Number** - The Insights serial number is unique and is auto generated during the system initalization.

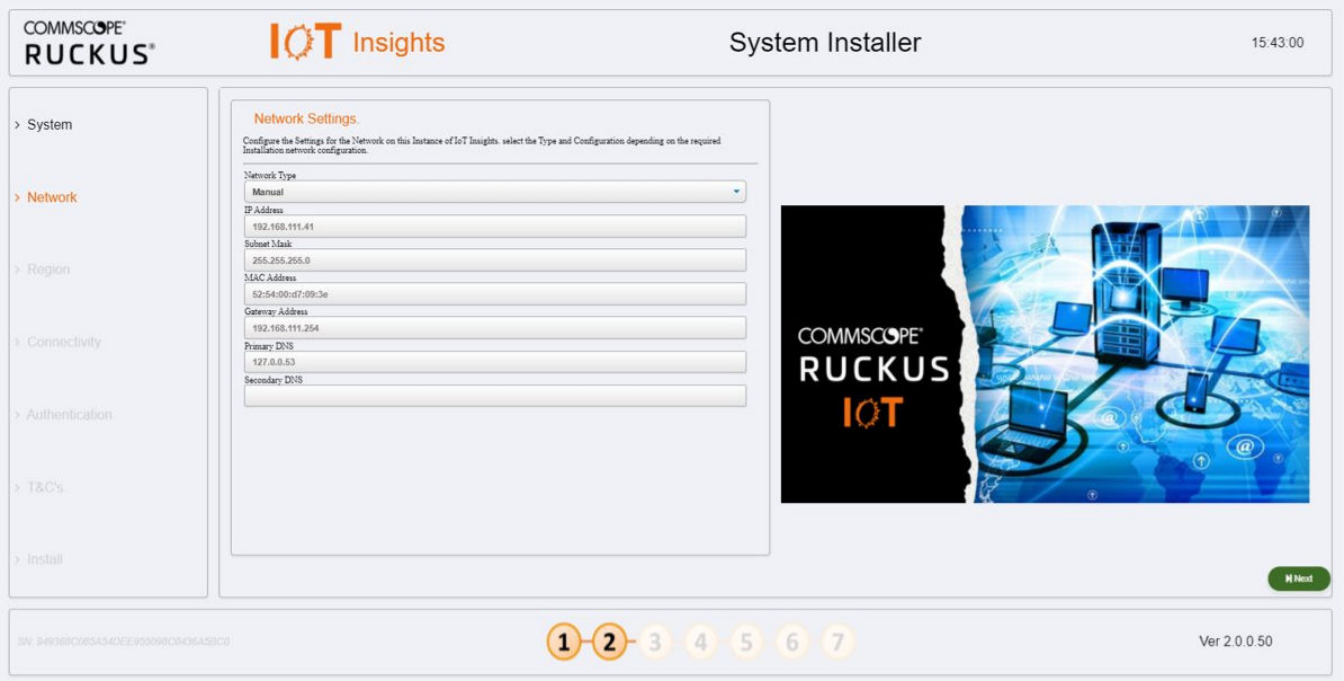
b) **System Name** - The system name is populated in this box.

c) **Unique Realm ID Number** - The Realm ID number is unique and is auto generated along with Insights Serial Number.

d) **Realm Name** - Enter the Realm Name. The Realm Name is referenced and used as part of the System Identification and Site Association process.

9. In the left navigation pane of System Installer, click **Network**. The **Network Settings** page is displayed. Complete the following configuration. Click **Next** after the configuration is completed.

FIGURE 43 Configuring Network Settings



a) **Network Type** - Select **Manual** or **DHCP** from the list. Depending upon the option selected the Dashboard page changes. In the above example, the **Network** Type is **Manual**.

b) **IP Address** - Enter the IP Address.

c) **Subnet Mask** - Enter the IP address of Subnet Mask.

d) **MAC Address** - Enter the MAC address of Machine

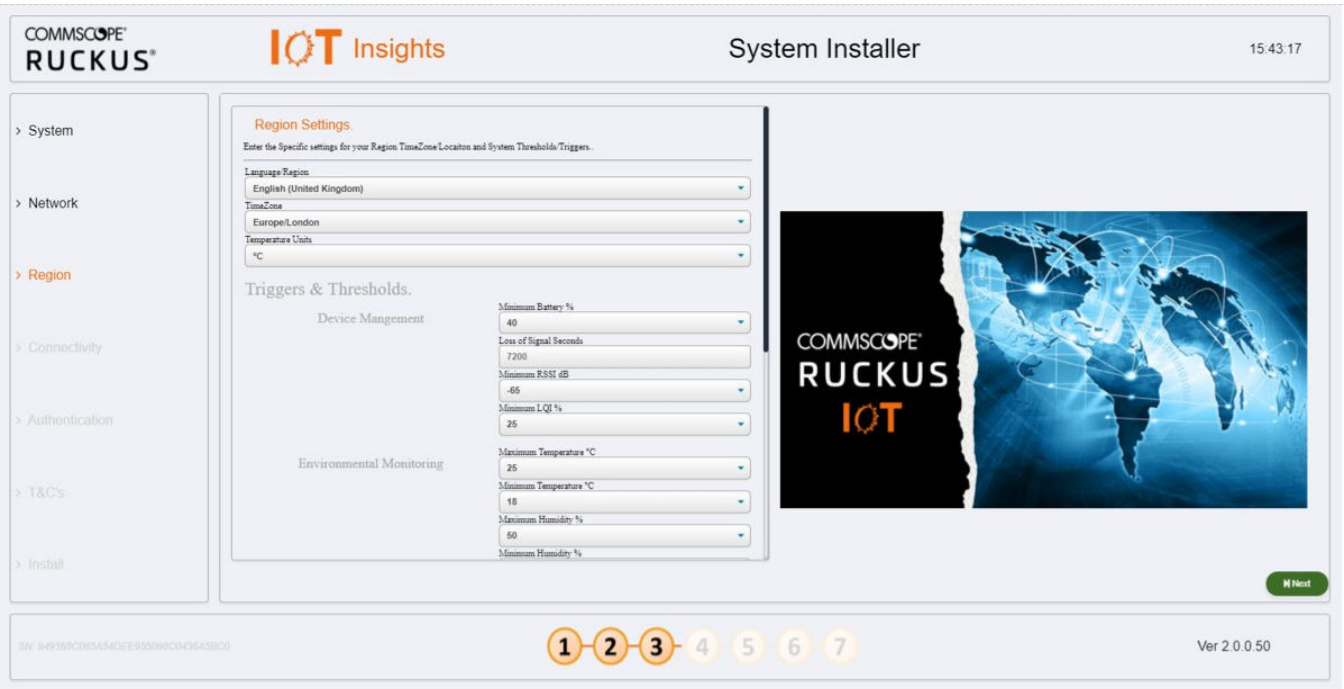
e) **Gateway Address** - Enter the IP address of Gateway.

f) **Primary DNS** - Enter the IP address of Primary DNS.

g) **Secondary DNS** - Enter the IP address of Secondary DNS.

10. In the left navigation pane of System Installer, click **Region**. The **Region Settings** page is displayed. Complete the following configuration. After selecting the regional values, click **Next**.

FIGURE 44 Configuring Region Settings



a) **Language Region** - Select the language from the list.

b) **TimeZone** - Selec the timezone from the list.

c) **Temperature Units** - Select the temperature unit from the list.

In addition to the units, the Installer can also modify any system level **Triggers** or alarm **Thresholds**. These are the values that will be used to set maximum and minimum tolerances for basic operation and alarm generation. In a lot of cases the default value will be suitable, but you can change these depending on the requirements.

11. In the left navigation pane of System Installer, click **Connectivity**. The **IoT Connectivity** page is displayed. The Insights Installer will try to auto discover the local IoT controller on the network. During this scan process, the scan window or the progress bar will increment showing that the scan is underway. After the scan is completed, you can select the IoT controller server from the **Discovered Servers** list. You can bypass this scan and enter the address of the IoT controller manaully in the field **Selected Server**. Type username in the field **Server Username**, and password in the field **Server Password**, and click **Connect**.

FIGURE 45 Scanning for the IoT Controoler

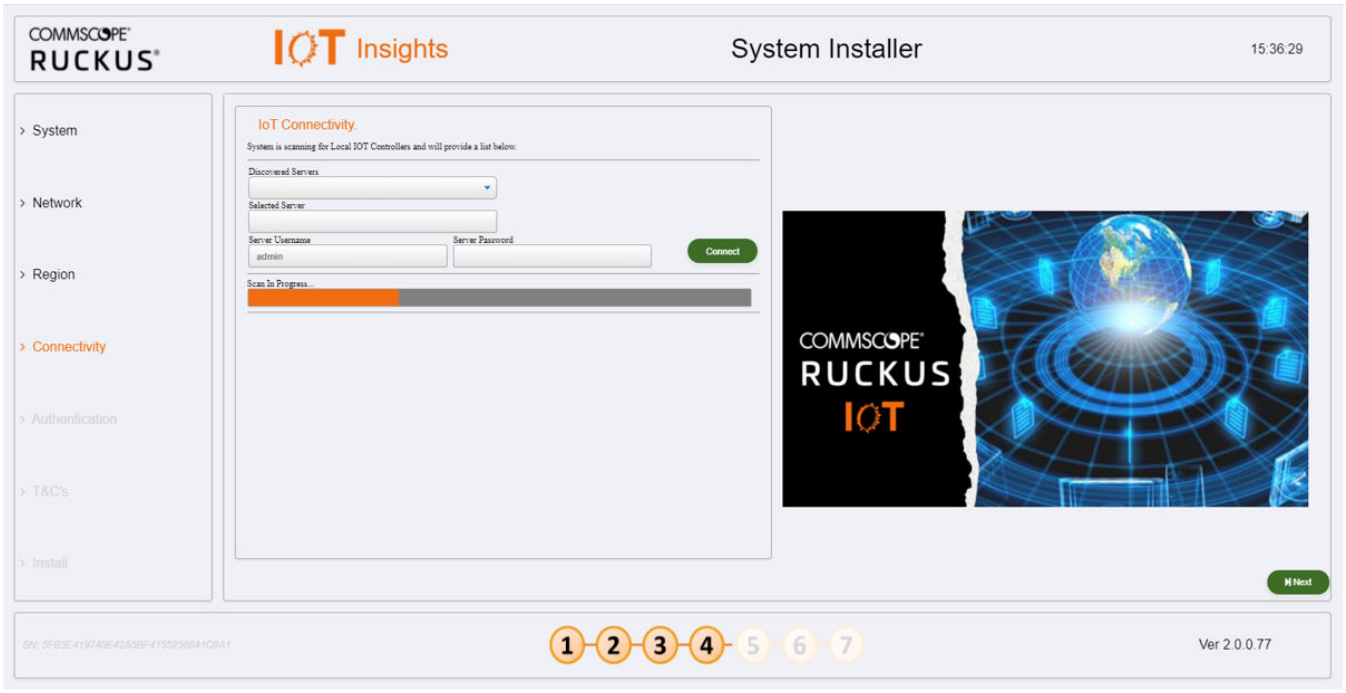


FIGURE 46 Completing the Scan

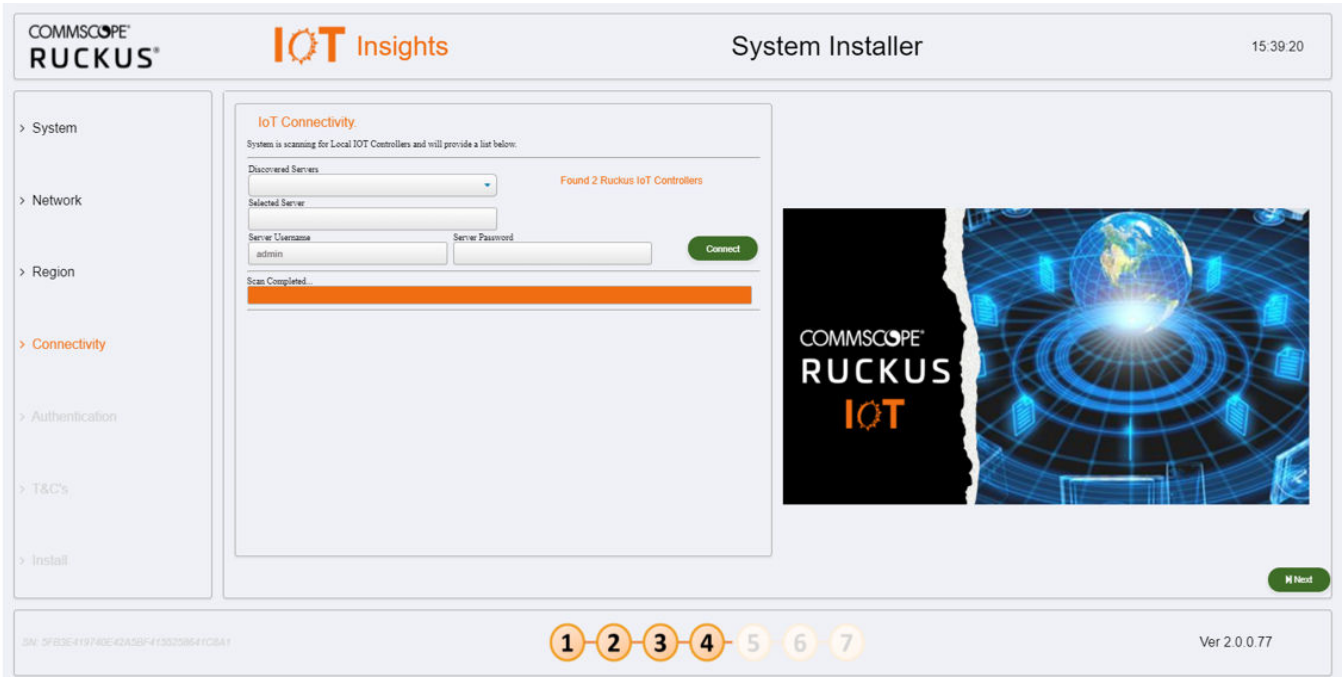
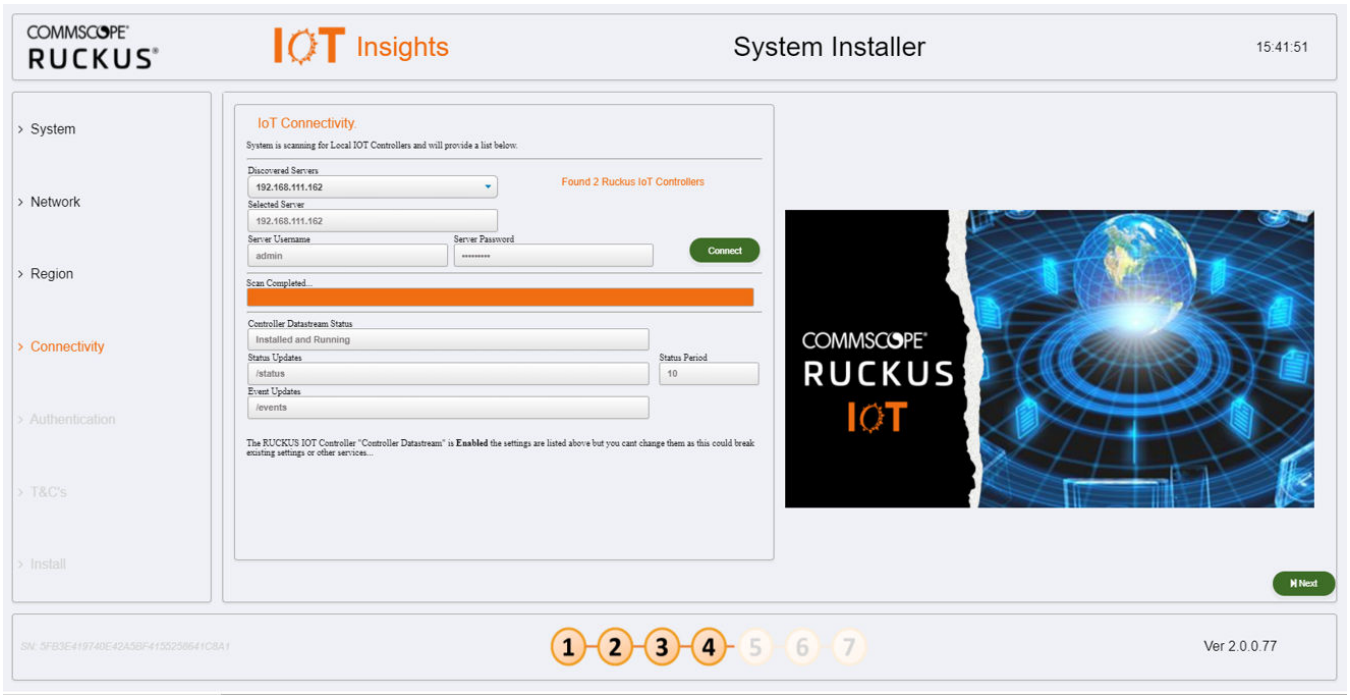


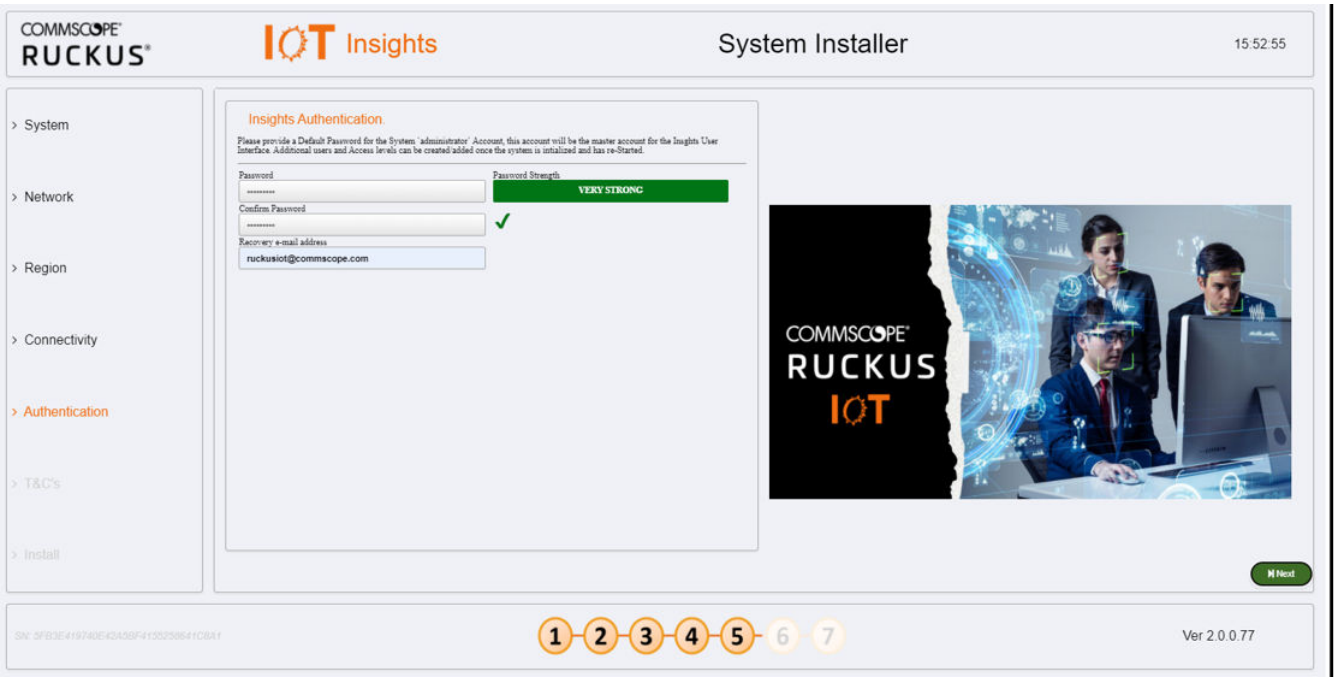
FIGURE 47 Configuring Controller Datastream Plugin



If the Controller Datastream Plugin is already configured on the controller then the status of **Controller Datastream Plugin**, **Status Update** and **Event Update** is displayed on the Installer. If it is not configured, then the system can be configured from the Installer and provisioned in the IoT controller as part of the setup process. Click **Next**.

12. In the left navigation pane of System Installer, click **Authentication**. The **Insights Connectivity** page is displayed. Complete the following configuration. Click **Next** after the configuration is completed.

FIGURE 48 Configuring the Insights Authentication



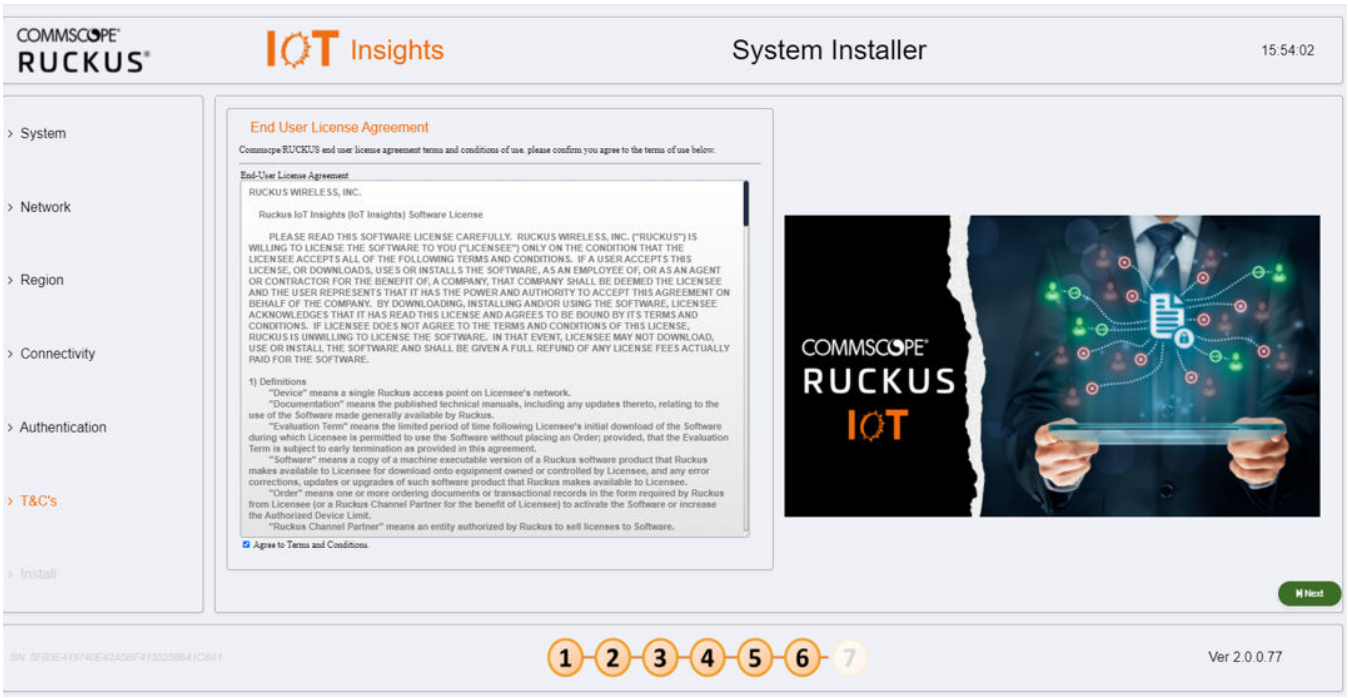
a) **Password** - Enter the Administration password. To have a strong password, confirm the following criteria are met.
   - The length of the password must be 8 characters long.
   - The password must have both upper and lower case letters.
   - It must have minimum one number.
   - It must have one special character.

b) **Confirm Password** - Type the password again in this field.

c) **Recovery email address** - Type the recovery email address.

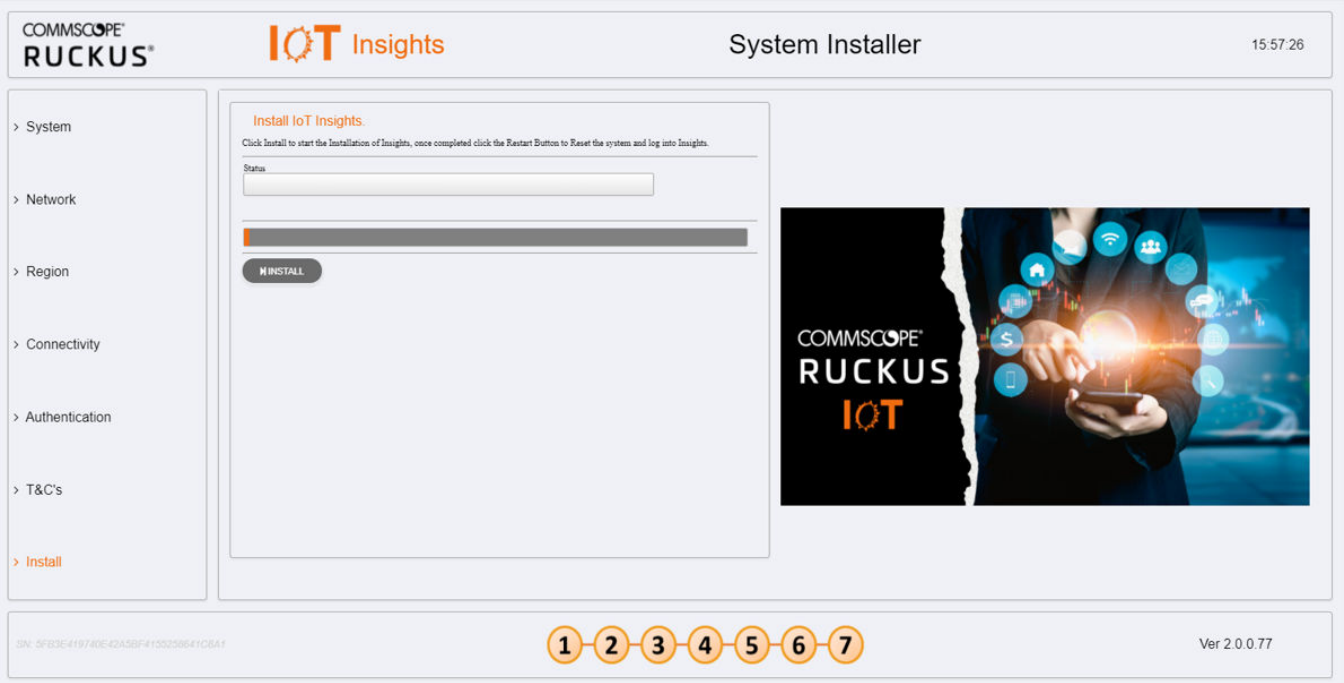
13. In the left navigation pane of System Installer, click **Terms and Conditions**.The **End User License Agreement** page is displayed. Click the **Agree to Terms and Conditions** checkbox, click the **Next** tab to perform the final installation step.

FIGURE 49 Configuring the End License Agreement



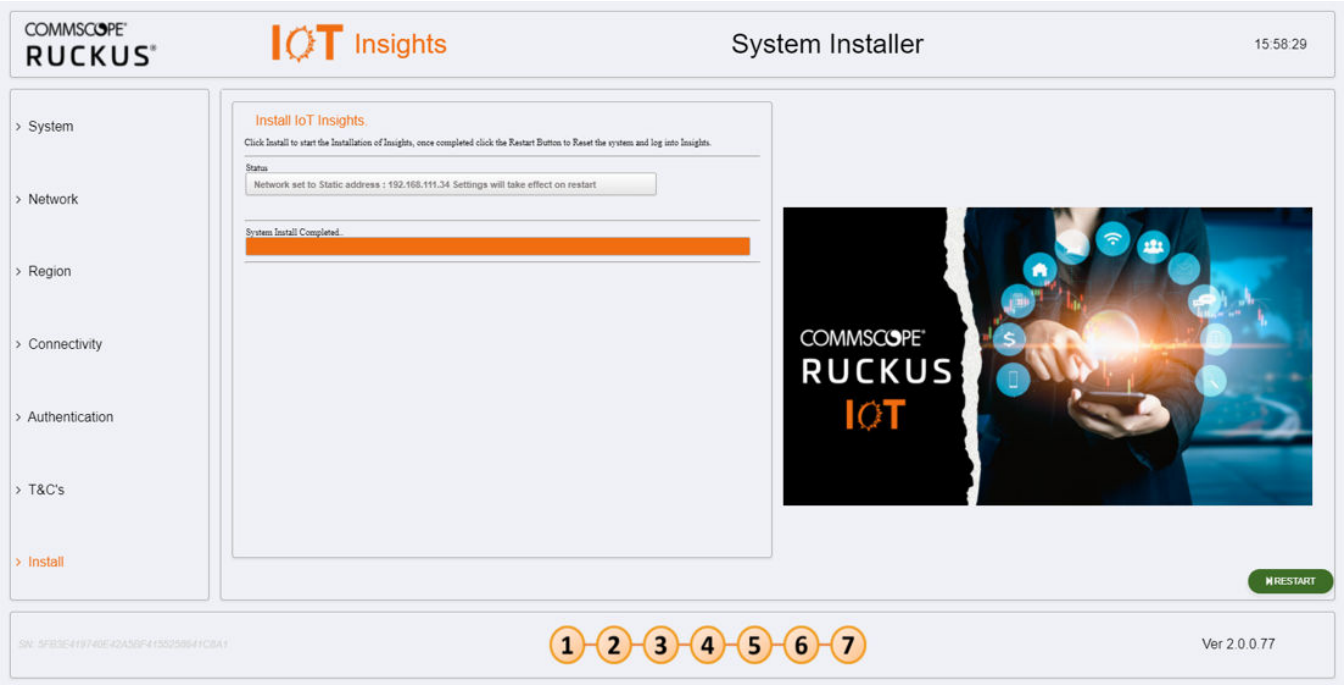
14. In the left navigation pane of System Installer, click **Install** to start the installation process. The **Install IoT Insights** page is displayed. The system will update the Installer with the current status, and the progress bar will show the total progress of the installation.

FIGURE 50 Configuring the IoT Install Insights



After the installation has completed, click **Restart**.

FIGURE 51 Restarting the IoT Insights

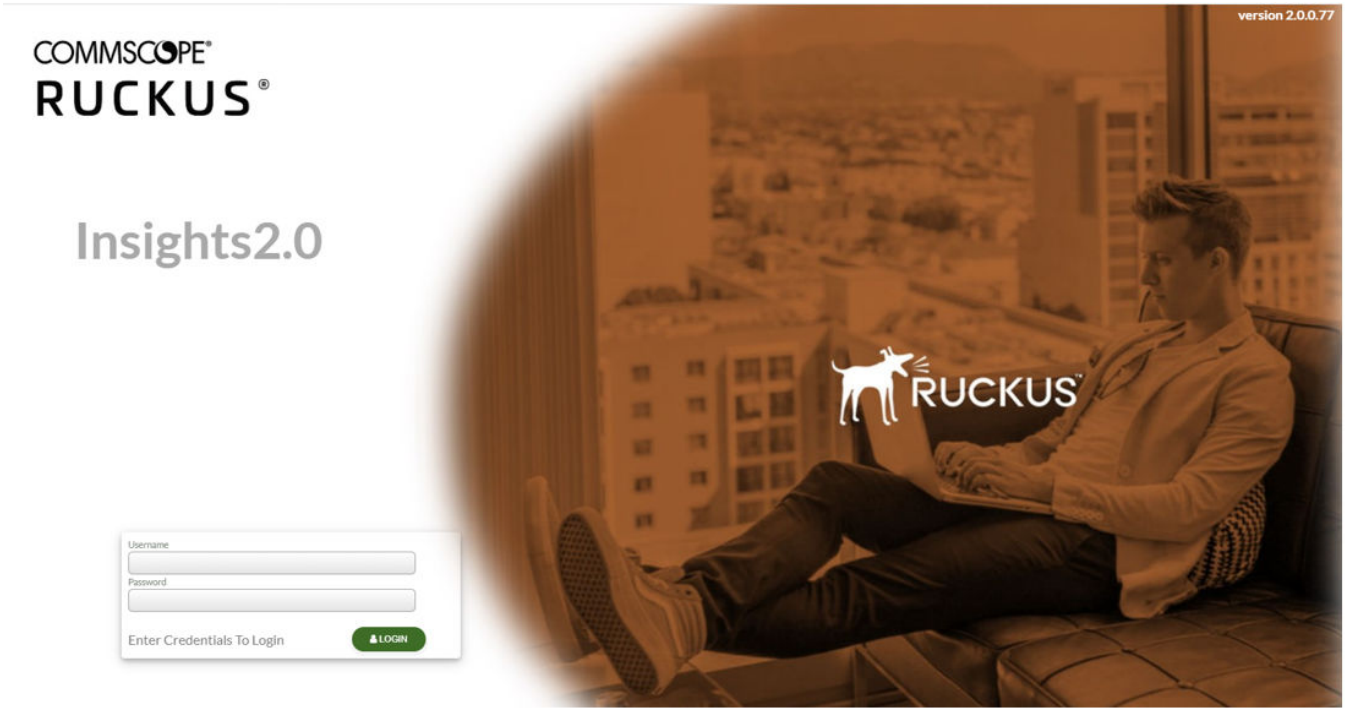


The following page appears showing the progress bar indicating the status of the restarting process.

FIGURE 52 Rebooting the IoT Insights

15. After the restart is completed, a login screen is displyed. The Administration can now enter the username and password and click **Login**.

FIGURE 53 Logging into IoT Insights



COMMSCOPE®
RUCKUS®

© 2022 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com