# **MeshCentral<sup>2</sup>** Installer's Guide





# **Table of Contents**

1.	Abs	tract	1
2.	Qui	ck Start	1
3.	Win	dows Installation	2
	3.1	Windows Installation Tool	2
	3.2	NPM Installation for Advanced Users	3
	3.3	Windows Defender Firewall Settings	5
	3.3.	1 Editing the existing rules	6
	3.3.	2 Add new firewall rules	7
4.	Ama	azon Linux 2	8
	4.1	Getting the AWS instance setup	8
	4.2	Installing NodeJS	9
	4.3	Installing MongoDB	9
	4.4	Port permissions	10
	4.5	Installing MeshCentral	10
	4.6	Configuring for MongoDB	11
	4.7	Manually starting the server	12
	4.8	Automatically starting the server	13
5.	Ras	pberry Pi	14
	5.1	Installing NodeJS	14
	5.2	Port permissions	14
	5.3	Installing MeshCentral	15
	5.4	Configuring for LAN-only mode	16
	5.5	Manually starting the server	17
	5.6	Automatically starting the server	17
6.	Ubu	intu 18.04	18
	6.1	Installing NodeJS	18
	6.2	Installing MongoDB	19
	6.3	Port permissions	19
	6.4	Installing MeshCentral	19
	6.5	Configuring for MongoDB	21
	6.6	Manually starting the server	22
	6.7	Automatically starting the server	22
	6.8	Increased Security Installation	23
7.	Mici	rosoft Azure	24
8.	Goo	gle Cloud	27
9.	Ubu	intu 16.04	30
	9.1	Installing NodeJS	30
10	). O	penBSD 6.4	31
	10.1	Installing MongoDB	31
	10.2	Installing NodeJS	31
	10.3	Installing MeshCentral	31

# **Document Changes**

- July 20, 2018 0.0.1 Initial version with Amazon Linux 2, Raspberry Pi and Ubuntu 18.04.
- July 21, 2018 0.0.2 Added Microsoft Azure using Ubuntu.
- July 23, 2018 0.0.3 Added Google Cloud.
- July 31, 2018 0.0.4 Added a section on a better and more secure way to install on Ubuntu.
- December 7, 2018 0.0.5 Many fixes to Ubuntu installation.
- February 21, 2019 0.0.6 Moved Windows installation to this document. Made some fixes.
- May 7, 2019 0.0.7 More fixes and added OpenBSD section.
- August 2<sup>nd</sup>, 2019 0.0.8 Fixed how node port permissions are set.
- August 23<sup>rd</sup>, 2019 0.0.9 Added Windows Defender Firewall instructions.
- November 28, 2020 0.1.0 Corrections to how Windows installation is done.

## 1. Abstract

This guide is specifically intended to help users install MeshCentral from start to finish. Once installed, you can take a look at the MeshCentral user's guide for information on how to configure MeshCentral for your specific use. In this document, we will look at installing MeshCentral on AWS Linux, Raspberry Pi and Ubuntu.

## 2. Quick Start

For some who want to skip this document entirely, there are quick install scripts that will get a MeshCentral2 instance up and running on Linux in a few minutes. These scripts will pretty much do what this document explains very rapidly. Right now, there are two such scripts available:

#### Amazon Linux 2

For Amazon EC2 users, that want to manage 100 devices or less. Launch a t3.nano or t3.micro EC2 instance with Amazon Linux 2 with TCP ports 22 (SSH), 80 (HTTP), 443 (HTTPS) and 4433 (CIRA) open. Then login as "ec2-user" and enter the following commands:

```
wget <u>http://info.meshcentral.com/scripts/mc-aws-linux2.sh</u>
chmod 755 mc-aws-linux2.sh
./mc-aws-linux2.sh
```

This will download the fast install script and once run, will install nodejs, meshcentral, setup systemd and start the server. For a larger instance like a t3.small, t3.medium or larger you can run the following that does the same but also installs MongoDB.

```
wget <u>http://info.meshcentral.com/scripts/mc-aws-linux2-mongo.sh</u>
chmod 755 mc-aws-linux2-mongo.sh
./mc-aws-linux2-mongo.sh
```

After these scripts are run, try accessing the server using a browser. MeshCentral will take a minute or two to create certificates after that, the server will be up. The first account to be created will be the site administrator – so don't delay and create an account right away. Once running, move on to the MeshCentral's user's guide to configure your new server.

#### Microsoft Azure

For 100 devices or less, launch an instance of Ubuntu 18.04 using a small B1s instance. Set the username to "default" in all lower case and open ports 22, 80, 443 and 3389 using the basic network profile. Then start the instance and run the following lines.

```
wget <u>http://info.meshcentral.com/scripts/mc-azure-ubuntu1804.sh</u>
chmod 755 mc-azure-ubuntu1804.sh
./mc-azure-ubuntu1804.sh
```

In this situation, port 3389 will be used to receive Intel AMT CIRA connections instead of port 4433. After these scripts are run, try accessing the server using a browser. MeshCentral will take a minute or two to create certificates after that, the server will be up. The first account to be created will be the site administrator – so don't delay and create an account right away. Once running, move on to the MeshCentral's user's guide to configure your new server.

# 3. Windows Installation

MeshCentral is constructed entirely with NodeJS, an asynchronous event driven JavaScript runtime (<u>https://nodejs.org/</u>). A basic understanding on NodeJS may be preferable but not compulsory. MeshCentral server which heavily relies on NodeJS runtime will be able run on almost any computing platform with contemporary operating systems including Windows\*, Linux\* and macOS\*.

There are two ways to get MeshCentral setup.

- For Linux\*, macOS\*, or advanced users can use CLI based NPM tool.
- For Windows users, you can use the MeshCentral installation tool.

#### 3.1 Windows Installation Tool

The MeshCentral installer tool for Microsoft Windows can be downloaded at <u>www.meshcommander.com/meshcentral2</u> or by clicking this <u>link</u>. This tool will automatically detect and install NodeJS if needed. NodeJS will be downloaded from <u>https://nodejs.org</u> checked and installed. We recommend the installer be run on a modern version of Windows (.e.g. Win8.1, Win10, Win Server 2012\* or better)



During installation, the installation tool will prompt for the following settings:

• **Multi-user Server**: By enabling this option, the server will be open to any user with a web browser app. Users will be able to create accounts and start managing computers associated in their respective accounts.

**Note:** If this option is disabled (unchecked), the server will run as a single-user server, no login screen will be presented and MeshCentral application will be limited to the server host machine only.

• Auto-update Server: By enabling this option, the server will check new version releases daily and perform automatic update.

**Note:** Update check occurs at 0000 between 0100 hours (local time). During update, the server will not be accessible until update is completed.

• Server Modes, LAN, WAN or Hybrid:

**LAN mode**: Recommended for small installation within a local network. Server host does not need a fixed IP address or DNS record to operate.

**WAN or Hybrid modes**: Server host will require a fixed IP address or DNS record to function correctly. If selected, user will need to enter server's DNS name or static IP address in the "Server Name" field. This name or IP address will be used by browsers and agents to connect back to the server, this name MUST be correct or the server will not work. If you do not have a fixed name, select LAN mode to get started.

Acquiring a static IP or DNS record is beyond the scope of this document. Please seek advice or consult your network administrator if unsure. If unsure, leave the settings as default (as-is) and proceed setup in LAN mode to manage computers that reside within the same network.

Once installed MeshCentral will run as a background Windows Service and can be accessed using a web browser with the link provided by the installer.

The installation tool can be run again to perform server update, re-installation or un-installation. When performing an update check, the tool will look at the currently installed version and compare it to the one present on NPM.



By default, MeshCentral will use TCP ports 80 (HTTP), 443 (HTTPS) and 4433 (Intel® AMT CIRA). The installer will add Windows Defender Firewall rules to allow incoming connections on these ports. In addition, if the server is in LAN or Hybrid mode, an addition rule on UDP port 16990 is added to allow for server discovery.

#### 3.2 NPM Installation for Advanced Users

For advanced users or administrators, MeshCentral can be installed with NPM, a NodeJS package manager that can be accessed via web browser (<u>https://www.npmjs.com/</u>) or command line tool, "npm".



**Note**: As a prerequisite, NodeJS and NPM must be installed on host OS and HTTP/HTTPS proxy settings maybe required if server host resides behind a HTTP proxy server.

- To begin, start a command line terminal (Windows Command Prompt or Linux Terminal) and type the following to verify if nodeJS and npm has been installed correctly as shown below
  - a. To check on nodeJS installed version, type "node -v" and hit "enter" key
  - b. To check on npm installed version, type "npm -v" and hit "enter" key
- 2. If MeshCentral installation is performed on a server host that resides behind a HTTP proxy, NPM's proxy settings must be updated with respective proxy settings associated with the network environment. Skip this step if not applicable.

```
.e.g. for http proxy "npm config set proxy http://proxy.com:88"
.e.g. for https proxy "npm config set https-proxy http://proxy.com:88"
```

Create a new directory "MeshCentral" and run the NPM install command as shown below:

```
mkdir meshcentral
cd meshcentral
npm install meshcentral
```

Do not use "sudo" in front of "npm install meshcentral".

4. Upon download completion, the server can be started with the commands below:

node node\_modules/meshcentral [arguments]

Do not run MeshCentral by going into the "node\_modules/meshcentral" folder as this may cause auto-install and self-update features to fail. Instead, go into the directory above "node\_modules" and run "node node\_modules/meshcentral".



**Note**: If MeshCentral is started <u>without</u> any arguments, default settings in LAN-only mode will be in effect and user/administrator will only be able to manage computers that reside within the local network.

5. To manage computers over the internet, the server needs to have static IP settings or a DNS record that resolves back to the right server. The mesh agents will be using the mechanism to call home to MeshCentral server. For WAN or Hybrid mode, run one of the commands below

```
node node_modules/meshcentral --cert servername.domain.com
node node_modules/meshcentral --cert hostname.domain.com
node node modules/meshcentral --cert 1.2.3.4
```

Note: On first attempt running on WAN or Hybrid Mode,

• Certificates will be generated for the first time and this may take a few minutes to complete.

At this point, no user account will be created or available for the user hence 1<sup>st</sup> user account will be the most privileged user with Administrator rights

 User is advised to create an "admin" account <u>immediately</u> by navigating to https://127.0.0.1 with a web browser.

**Note**: To run MeshCentral as a service, run it using "--install" argument. Once running, start a web browser and access MeshCentral application with respective URL.

#### 3.3 Windows Defender Firewall Settings

On Windows, the built-in firewall will need to be configured to allow TCP ports 80, 443 and 4433 and sometimes UDP port 16990. The MeshCentral Windows Installer will add incoming rules for these ports automatically. If using the advanced NPM installation or when changing the default ports, it may be needed to add or edit these firewall rules. In this section we look at how to do this.

To get started, we need to go in the control panel, click "System and Security" then "Windows Defender Firewall" and "Advanced Settings" on the left side then click on "Inbound rules". This will get us on the right place to add or edit firewall rules.

All and a state of the state of			- 0	x
T 🛄 > Control Par	nel	~ Õ		4
Adjust your compu	ter's settings		View by: Category -	
System and Series pour, Serie Boday, Beckgrand B Wetworks Hardware Hardware Hardware Wetworks Hardware Programs Uninstal a pri	d Security computer's states pages of your files with File actore (Windows 7) and Internet status and tasks and Sound and printers ogram	User Accounts Charge accounts Appearance and Clock and Regio Charge data time, o Ease of Access Let Windows upget Optimize visual depl	System and Security Control Panel Home System and Security Network and Internet Hardware and Sound Programs User Accounts Appearance and Personalization Clock and Brayion Ease of Access	Comparing the Maintenance     Security and Maintenance     Security a
Windows Defender Firewall     → → ↑	J Security > Windows Defende Help protect your PC Windows Defender Firewall your PC through the Interne Private network	Firewall v 0 with Windows Defender Fire can help prevent hackers or malicious or a network. rrks where you know and trut the secole	-      Search Control Panel  wall  software from gaining access to  Connected  and devices on the network	X BitLocker Drive Encryption P Storage Spaces Manage Storage Spaces
Firmual on or off	Windows 🔐 Windows E	efender Firewall with Advanced Secu View Help	arity	- 0
Restore defaults Advanced settings	The Honor	and the second se		

If the MeshCentral Windows Installer was used, the "MeshCentral Server TCP ports" and optionally "MeshCentral Server UDP ports" rules should already be present.

#### 3.3.1 Editing the existing rules

To edit an existing rule, simply double click on it. To change the allowed inbound ports, go to the "Protocols and Ports" tab and change the local ports.

		MeshCentr	al Server TC	P ports Pro	perties			
		Gener Protocols	al and Ports	Programs a Scope	nd Services Advanced	Ren Local Principal	note Compu s Remo	ters te User
Indows Defender Firewall with Advanced Security Action Yeew Help Monor Defender Firewall with Inbound Rules Connection Security Rules Media Center Etenders - qWave (ICP-In) Media Center Etenders - gWave (ICP-In) Media Center Etenders - StSP (ICP-In) Media Center Etenders - SSP (ICP-In) Media Center Etenders - SSP (ICP-In) Media Center Etenders - WAVEN-NDR-MEDIA Center Etenders - SSP (ICP-In) Media Center Etenders - WAVEN-NDR-MEDIA Media Center Etenders - SSP (ICP-In) Media Center Etenders - SSP (ICP-I	Acti Inb V V V V Acti Inb Acti	Protocols 4	and Ports Is and ports Protocol ty Protocol n Local port Bernote por Internet Co (ICMP) set	Scope //	Advanced TCP Specific Pr 80, 443, 44 Example: 8 All Ports Example: 8 pe Protocol	Local Principal	s Remo ~ 010 010 010 010	te User

#### 3.3.2 Add new firewall rules

To add a new firewall rule, click on the "New Rule..." then select "Port" and ok. TCP or UDP and enter the specific local ports needed and ok. Then click ok twice, enter the rule name and ok again.

	File Action View Hele				
	The Works Tien Tien				
		Jahaward Datas			
	Inbound Rules	Inbound Rules	1049000	Actions	
	Connection Security Rules	Name Media Center Extenders - RI Media Center Extenders - SS Media Center Extenders - W	Group TSP (TCP-In) Media Center Ext SDP (UDP-In) Media Center Ext /MDRM-ND/R Media Center Ext	te Rule te ⊽ Filter by Profile	•
		Madia Center Extenders - X	SP (TCP-In) Media Center Ext	te 🛛 🖓 Filter by State	•
New Inbound Rule Wiz	zard		×	Filter by Group	•
le Type			ana Ousuin	View	•
ct the type of firewall rule t	to create.		age Queuin	g Refresh	
<b>5</b> .			age Queuin	ig 🖉 🗟 Export List	
ule Type	What type of rule would you like to on	sate?	PNew Inbound Rule Wit	zard	
rotocol and Ports	0.8		Protocol and Ports		
ction Imfile	Rule that controls connections for	a program.	Specify the protocols and port	ts to which this rule applies.	
lame	Pgrt		Steps:		
	Rule that controls connections for	a TCP or UDP port.	<ul> <li>Rule Type</li> </ul>	Does this rule apply to TCP or UDP?	
	O Predefined:		Protocol and Ports	• ICP	
	AliJoyn Router		<ul> <li>Action</li> </ul>	O UDP	
	Hule that controls connections for	a Windows experience.	<ul> <li>Profile</li> </ul>		
	Custom rule.		Name	Does this rule apply to all local ports or specific local	l ports?
				All local ports	
				Specific local ports: 80.443,4433	
Specify the act Steps: Plute Type Protocol an	tion to be taken when a connection matches the o What action should be d Pots () Allow the connec	onditions specified in the rule. taken when a connection matches the sp ction	pecified conditions?		
Specify the act Steps: Picto Content Action Profile Name	d Pots What action should be <b>e</b> Allow the conner This includes com <b>Niow the conner</b> This includes com <b>With the conner</b> <b>With the conner</b>	anditions specified in the rule. taken when a connection matches the sp ction ections that are protected with iPsec as w ction <i>if</i> is secure connections that have connections that have p the settings in iPsec propeties and rule	ecified conditions? ell a	apples.	×
Specify the act Steps: Pute Type Protocol an Acton Protile Name Name	ton to be taken when a connection matches the co What action should be (a) Pots (b) Allow the common This includes com (c) Allow the gomen This includes com Rule node. It with a connection of the connection (c) Allow the gomen This includes com Rule node.	unditions specified in the rule. taken when a connection matches the sp cition extens that are protected with Pisec as w cition <b>#</b> at as excute promedions that have been authenticated g the settings in Piece properties and rule	eeched conditions? eef a Profile s int Specify the profiles for which this rule i	apples. When does this rule apply?	×
Specify the act Steps: Pictor an Action Pictor an Pictor Name Name Name	ton to be taken when a connection matches the or what action should be what action should be what action should be what action should be will be secured using the Wizard le Wizard escription of the nule.	unditions specified in the rule. taken when a connection matches the sp ction ections that are protected with iPsec as w ciclion <b>if</b> is secure prometions that have been authenticated grite settings in iPsec properties and rule	eecified conditions? eel a Profile Specify the profiles for which this rule a X	apples. When does this rule apply?	×
Specify the act Steps: Pactors and Protoce and Protoc	ton to be taken when a connection matches the o What action should be	unditions specified in the rule. taken when a connection matches the sp <b>ction</b> and the are protected with lPace as w diction <b>if</b> at a socure connections that have been authenticated g the settings in lPace properties and rule	ee offed conditions? ee a Profile s and Specify the profiles for which this rule i X	applies. When does this rule apply? Domain Apples when a computer is connected to its corporate of	koman.
Specify the act Steps: Profece a Profece Profece Name New Inbound Rul Name Specify the name and de Steps: Data Steps: Profece	ton to be taken when a connection matches the or d Ports What action should be (e) Allow the corner This includes conn (i) Allow the corner mit be secured use Rule node. Its witzard secription of this rule.	onditions specified in the rule. taken when a connection matches the sp <b>ction</b> extra that are protected with IPsec as w <b>ction if it is secure</b> connections that have been authenticated is the wettings in IPsec properties and rule	ectifed conditions ? et a Profile Specify the profiles for which this rule : X	apples. When does this rule apply? Domain Apples when a computer is connected to its corporate o Divide	oman.
Specify the act Steps: Protoce an Protoce an Protoce an Protoce Protoce an Protoce an Protoce an Protoce and Protoce and Protoce Protoce and Protoce	ton to be taken when a connection matches the of d Pots d	onditions specified in the rule. taken when a connection matches the sp ction tections that are protected with iPisce as w ction <b>if</b> is as second or relations that have been authenticated by the settings in IPisce properties and rule	eedfed conditions? eed a Profile Specify the profiles for which this rule . X	applies. When does this rule apply? Demain Applies when a computer is connected to its corporate of Disples when a computer is connected to a private networe work place.	tomain. vork location, such as a home
Specify the act Steps:	Ion to be taken when a connection matches the or What action should be	onditions specified in the rule. taken when a connection matches the sp ction ections that are protected with IPsec as w cotion if it is secure connections that have been authenticated g the settings in IPsec properties and rule	eedfed conditions?	apples. When does this rule apply? Domain Apples when a computer is connected to its corporate of Private Apples when a computer is connected to a private netw or work place. Private Private	toman. vok location, such as a home
Specify the act Steps: a Rule Type Protocal and Protocal and Protoc	ton to be taken when a connection matches the of What action should be	unditions specified in the rule. taken when a connection matches the sp ction extens that are protected with Pisec as w cition <b>if</b> is assecute prometions that have been authenticated g the settings in IPiec properties and rule	eecified conditions? eel a Profile Specify the profiles for which this rule a	apples. When does this rule apply? Demain Apples when a computer is connected to its corporate of When does this a computer is connected to a private network place. Publics Apples when a computer is connected to a public network	toman. vok location, such as a home ok location.
Specify the act Steps: Pactors and Protocal and Protocal and Protocal and Protocal Protocal and Protocal Pr	ton to be taken when a connection matches the o d Ports	unditions specified in the rule. taken when a connection matches the sp ction and methods with Parce as we defined if a secure promotions that have been authenticated grite settings in IParc properties and rule and the settings in IParc properties and rule	eedfed conditions? eed a Profile Specify the profiles for which this rule it X	apples. When does this rule apply?  Domain Apples when a computer is connected to its corporate of Private Apples when a computer is connected to a private netw or work place. Phylice Apples when a computer is connected to a public netw	domain. volk location, such as a home ook location.
Specify the act Steps: Pactor and Protoce and Protoce and Protoce and Protoce and Protoce and Protoce Protoce and Protoce Prot	ton to be taken when a connection matches the of d Ports	onditions specified in the rule. taken when a connection matches the sp ction taken when a connection matches the sp ction if it is secure connections that are protected with lPace as w connections that have been authenticated gifte settings in lPace properties and rule ntel	ectifed conditions ? et a ref New Inbound Rule Wizard Profile Specify the profiles for which this rule i X	apples. When does this rule apply?  Domain Apples when a computer is connected to its coporate of Private Apples when a computer is connected to a private netw or work place.  Phylice Apples when a computer is connected to a public netw	doman. wolk location, auch as a home
Specify the act Steps: Protocal and Protocal and Proto	ton to be taken when a connection matches the of d Ports	enditions specified in the rule. taken when a connection matches the sp ction extra are protected with Place as w chain <i>if</i> is accure connections that have been authenticated grite settings in iPlace properties and rule ntel	ectied conditions ? et a  Profile Specify the profiles for which this rule a	apples. When does this rule apply?  Domain Apples when a computer is connected to its corporate of Private Apples when a computer is connected to a private network Probles Probles Apples when a computer is connected to a public network Probles Pr	doman. work location, such as a home
Specify the act Steps: Pictor	ton to be taken when a connection matches the of d Pots	onditions specified in the rule. taken when a connection matches the sp ction taken when a protected with iPisc as w ction <b>f</b> is assectively a setting an iPisc properties and rule the settings in iPisc properties and rule and	ectied conditions?	apples. When does this rule apply?  Demain Apples when a computer is connected to its corporate of Private Apples when a computer is connected to a private network place.  Private Apples when a computer is connected to a public network	toman. rok location, such as a home of location.
Specify the act Steps: Protocian Protocia	ton to be taken when a connection matches the d of Pots   What action should be Potential of the come The includes com Potential of the come Potential of the come Pot	enditions specified in the rule. taken when a connection matches the sp ction ction and are protected with Pasc as w ction if it is secure connections that have been authenticated y the settings in Piece properties and rule ntal	eecified conditions?	apples. When does this rule apply?  Demain Apples when a computer is connected to its corporate of work place.  Public Public Apples when a computer is connected to a private network place.  Public Apples when a computer is connected to a public network	doman. vok location, such as a home ork location.
Specify the act Steps:	ton to be taken when a connection matches the d d Ports	endions specified in the rule. taken when a connection matches the sp ction ection if an expected with iPsec as w ciclion if an execute connections that have been authenticated pite settings in iPsec properties and rule end	eecfied conditions? et a Profile Specify the profiles for which this rule a X	apples. When does this rule apply?  Demain Apples when a computer is connected to its corporate of work place.  Public. Public. Apples when a computer is connected to a private netw or work place.  Public. Apples when a computer is connected to a public netw	tomain. work location, such as a home ork location.
Specify the act Steps:	ton to be taken when a connection matches the of d Ports	enditions specified in the rule.  Itaken when a connection matches the sp ction connection that are protected with lPace as w connections that have been authenticated protections in the have been authenticated state the settings in lPace properties and rule	eedfed conditions? ef a Profile Specify the profiles for which this rule i	apples. When does this rule apply?  Domain Apples when a computer is connected to its corporate of Private Apples when a computer is connected to a private netw or work place. Phylice Apples when a computer is connected to a public netw	domain. work location, such as a home ook location.
Specify the act Steps: Pactor an Protoce an Protoce an Protoce and Protoce and Protoce and Posts Protoce and Posts Pro	ton to be taken when a connection matches the of d Ports	enditions specified in the rule. taken when a connection matches the sp ction taken when a connection matches the sp ction that are protected with Place as w choin if is a secure connections that have been authenticated gifte settings in iPlace properties and use ntel	ectied conditions ? et a  New Inbound Rule Wizard Profile Specify the profiles for which this rule i	apples. When does this rule apply?  Domain Apples when a computer is connected to its coporate of Private Apples when a computer is connected to a private netw or work place.  Phylice Apples when a computer is connected to a public netw	domain. volk location, auch as a home
Specify the act Steps: Picto Pi	to to be taken when a connection matches the of d Ports	endions specified in the rule.  Isken when a connection matches the sp cion extra are protected with Pisec as w clock of # is ascent connections that have been authenticated grite settings in iPisec properties and rule ntel	ected conditions? et a Profile Specify the profiles for which this rule a	apples. When does this rule apply?  Define the acceptor is connected to its corporate of the index when a computer is connected to a private meter in origh place.  Define when a computer is connected to a public network place.  Define when a computer is connected to a public network place.  Define when a computer is connected to a public network place.  Define when a computer is connected to a public network place.	toman. nok location, such as a home ork location.
Specify the act Steps: Profile Profile Name Secoly the name and de Steps: Profile Prof	ton to be taken when a connection matches the d of Pots  What action should be  Rife which action which a connection  Note the conner  Note th	enditions specified in the rule. taken when a connection matches the sp ction tion that are protected with Pisec as w citorin <b># a</b> in secure connections that have been authenticated yite settings in IPiec properties and rule ntia	eedled conditions?	apples. When does this rule apply?  Define the a computer is connected to its corporate of the across place.  Define when a computer is connected to a private metric across place.  Define when a computer is connected to a public network place.  Define the across place is connected to a public network place.  Define the across place is connected to a public network place.  Define the across place is connected to a public network place.	doman. work location, such as a home ork location.
Specify the act Steps: Pictocal and Pictocal and Pictoc	to to be taken when a connection matches the d of Ports What action should be Bior the corner This includes corn O Allow the corner This includes corn O Allow the corner Rule node.  It Wizard Exception of this rule.  Exception of this rule.  Exception (optional):	endions specified in the nule. taken when a connection matches the sp ction ection that are protected with iPsec as w cition if it is accure connections that have been authenticated pite settings in iPsec properties and nule end	eedfed conditions?	apples. When does this rule apply?  Demain Apples when a computer is connected to its corporate of Protec Prote Apples when a computer is connected to a private network place. Protec Apples when a computer is connected to a public network Protec Apples when a computer is connected to a public network Protec Apples when a computer is connected to a public network Protec	toman. wok location, such as a home ok location.
Specify the act Steps: Pictocal and Pictocal and Pictocal and Pictocal Pictocal and Pic	ton to be taken when a connection matches the d  of Ports  what action should be  file Microse come To includes come To includes come To includes come Rule node.  It witzard  escription of this rule.  Name: Mathies Server TCP po Description (optional):	endions specified in the rule.  Isken when a connection matches the sp ction control that are protected with Parce as w connections that have been authenticated protection if an is accure	eedled conditions? eed a Profile Specify the profiles for which this rule a	apples. When does this rule apply?  Domain Apples when a computer is connected to its corporate of Provide Apples when a computer is connected to a private netw or work place.  Phylic Apples when a computer is connected to a public netw	domain. work location, such as a home ook location.
Specify the act Steps: Protocol and Protocol and Protocol and Protocol and Protocol Protocol and Protocol P	to to be taken when a connection matches the d  of Ports  what action should be  file Must action should be  file	Inditions specified in the rule.	Peofied conditions ? et a Profile Specify the profiles for which this rule a	apples.  When does this rule apply?  Domain  Apples when a computer is connected to its coporate of  Private  Apples when a computer is connected to a pruste netw  or work place.  Paples  Apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apples when a computer is connected to a public netw  I apple apples when a computer is connected to a public netw  I apple apples when a computer is connected to a public netw  I apple apples when a computer is connected to a public netw  I apple apple apples when a computer is connected to a public netw  I apple apple apple apples appl	doman. nok location, such as a home onk location.

Typically, inbound TCP ports 80, 443 and 4433 are used, but the rule can be added with different ports as needed.

# 4. Amazon Linux 2

In this section, we will look at installing MeshCentral on Amazon AWS with "Amazon Linux 2". This is a low cost instance and a free tier is available so you can experiment or run a small instance of MeshCentral and it will work perfectly fine.

## 4.1 Getting the AWS instance setup

On AWS EC2, you can launch an instance and select "Amazon Linux 2". In this case, it's the first option available.

) → C û ()	A https://us-west	-2.console.aws.amazon.com/ec2/v2/h … 🏠 🔍 Search	III\ 🤨 🗉
aws Services	✓ Resource	Groups 🗸 🏠	
Choose AMI 2. Choose Ins	ance Type 3. Cont	figure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group	7. Review
tep 1 <sup>.</sup> Choose an	Amazon M	achine Image (AMI)	Cancel and Exit
AMI is a template that contai u can select an AMI provided	ns the software con by AWS, our user c	figuration (operating system, application server, and applications) required to ommunity, or the AWS Marketplace; or you can select one of your own AMIs.	launch your instance
Quick Start		< < 1 to	35 of 35 AMIs $\rightarrow$
My AMIs	Û	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-a9d09ed1	Select
AWS Marketplace	Amazon Linux Free tier eligible	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc	64-bit
Community AMIs		2.26, Binutils 2.29.1, and the latest software packages through extras. Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	
Free tier only (i)	Ũ	Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type -	Select
	Amazon Linux Free tier eligible	HTH-Vad99/72     The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.     Root device type: ebs Virtualization type: thrm ENA Enabled: Yes	64-bit
	Red Hat	Red Hat Enterprise Linux 7.5 (HVM), SSD Volume Type - ami-28e07e50	Select
	Free tier eligible	Red Hat Enterprise Linux version 7.5 (HVM), EBS General Purpose (SSD) Volume Type	64-bit

When launching a new instance, you are asked to use or create a security group with the allowed inbound TCP and UDP ports. The security group should look like this:

Туре	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere	SSH
HTTP	TCP	80	Anywhere	HTTP
HTTPS	TCP	443	Anywhere	HTTPS
Custom TCP Rule	TCP	4433	Anywhere	Intel AMT CIRA
Custom TCP Rule	TCP	8080	Anywhere	Swarm Server*

All security group rules should have a source of "0.0.0.0/0" and "::/0". The last rule for port 8080 is only needed if migrating from a MeshCentral1 server, most people don't need it and should not be added.

If you are not going to be managing Intel AMT computers, you can remove port 4433. One can also remove port 80, however it's needed to get a Let's Encrypt certificate and useful to route users from the HTTP to the HTTPS web page.

For all the following sections, we assume that we are in the "ec2-user" home path. You can do:

cd ~

This will change the current path to the home folder.

#### 4.2 Installing NodeJS

To get started, launch an instance and start a SSH session to it. You can use SSH on Linux or Putty on Windows to login to the AWS instance.

The first thing to do is get NodeJS installed on the instance. We will be installing a long term support (LTS) version of NodeJS. Additional information on how to do this <u>can be found here</u>. We first install the node version manager then activate it and install the NodeJS LTS. It's done with 3 commands:



We can test what version of NodeJS is installed using:

node -v

#### 4.3 Installing MongoDB

If we are going to run a large instance, it's best to use MongoDB as the database. If you are using a small instance, you can skip installing MongoDB and MeshCentral will use NeDB instead which is a light weight database that is probably great for managing less than 100 computers.



If you want to use MongoDB, we can install MongoDB Community Edition. More information on how to do this <u>can be found here</u>.

Using "nano" create the file "/etc/yum.repos.d/mongodb-org-4.0.repo":

sudo nano /etc/yum.repos.d/mongodb-org-4.0.repo

Then, put this in it:

```
[mongodb-org-4.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/amazon/2/mongodb-org/4.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc
```

This file will setup the repository that we will be using to bet MongoDB. Once done, you can install the package using yum and get it started like this:

sudo yum install -y mongodb-org
sudo service mongod start

To verify that MongoDB is running, you can enter the MongoDB shell like this:

mongo --host 127.0.0.1:27017

You can leave the shell using Ctrl-C. The database and log files will be create at these locations:

/var/log/mongodb /var/lib/mongo

This is useful to know if you want to make a backup of the database file.

#### 4.4 Port permissions

On Linux, ports below 1024 are reserved for the "root" user. This is a security feature. In our case MeshCentral will need to listen to ports 80 and 443. To allow this, we need to allow node to listen to ports below 1024 like this:

whereis node node: /home/ec2-user/.nvm/versions/node/v8.11.3/bin/node sudo setcap cap net bind service=+ep /home/ec2-user/.nvm/versions/node/v8.11.3/bin/node

We first locate the node binary, using "whereis node", we then use the "setcap" command to add permissions to node. Note that we take the path given by whereis and place it in the setcap command. The "setcap" command will set permissions allowing node to use ports 1024 and below. This permission may be lost when updating the Linux kernel, so this command may need to be applied again in some case.

#### 4.5 Installing MeshCentral

It's almost time to install MeshCentral but first, we need to know the public name of our AWS instance, you can run the following command:

curl http://169.254.169.254/latest/meta-data/public-hostname

It will return the public name of the AWS instance, for example:

ec2-1-2-3-4.us-west-2.compute.amazonaws.com

You can use this name, or if you have another registered DNS name pointing to the server instance, you can also use that now. Note that you must setup any alternative name on your own, MeshCentral will not do this for you. This name must be correct and must resolve to this AWS instance as all mesh agents will use this name to connect back to this server.

Now, we can use the node package manager (NPM) to install MeshCentral.

npm install meshcentral

```
Do not use "sudo" in front of "npm install meshcentral".
```

After that, we can run MeshCentral for the first time. We want to run in WAN-only mode since we will not be managing any computers on the same local network at this server. We also want to

create a server with a certificate name that is the same at the AWS instance name. So, we will use "--wanonly" and "--cert [name]" arguments to get the server started. For example:

```
node ./node_modules/meshcentral --wanonly --cert ec2-1-2-3-4.us-west-2.compute.amazonaws.com
```

At this point, the server will create its certificates and start running.

```
MeshCentral HTTP redirection web server running on port 80.
Generating certificates, may take a few minutes...
Generating root certificate...
Generating HTTPS certificate...
Generating Intel AMT MFS certificate...
Generating Intel AMT console certificate...
MeshCentral Intel(R) AMT server running on ec2-54-245-141-130.us-west-2.compute.amazonaws.com:4433.
MeshCentral HTTPS web server running on ec2-54-245-141-130.us-west-2.compute.amazonaws.com:443.
Server has no users, next new account will be site administrator.
```

You can now open a browser to the name of the server, for example:

https://ec2-1-2-3-4.us-west-2.compute.amazonaws.com

You will see the server working as expected. You will get a certificate error since the server is used an untrusted certificate for now. Just ignore the error and see the MeshCentral User's Guide to fix this.



At this point, the server is usable but, there are two things that may still need to be done. First, if we opted to use MongoDB, we have to configure MeshCentral to use a MongoDB database. By default, NeDB will be used which should only be used for small deployments managing less than 100 computers. We also need to automatically start the server when the AWS instance starts.

To continue, stop the MeshCentral server with CTRL-C.

#### 4.6 Configuring for MongoDB

By default, MeshCentral uses NeDB with a database file located in ~/meshcentraldata/meshcentral.db. This is great for small servers, but if we opted to install MongoDB, let's make use of it. We need to edit the config.json file located in the meshcentral-data folder.

```
nano ~/meshcentral-data/config.json
```

Then, make the start of the file look like this:

```
{
   "settings": {
    "MongoDb": "mongodb://127.0.0.1:27017/meshcentral",
    "WANonly": true,
    "_Port": 443,
    "_RedirPort": 80,
    "_AllowLoginToken": true,
    "_AllowFraming": true,
    "_WebRTC": false,
    "_ClickOnce": false,
    "_UserAllowedIP" : "127.0.0.1,::1,192.168.0.100"
    },
...
}
```

If you start with the default config.json created by MeshCentral, you will need to remove some "\_" characters in front of settings, mongodb and wanonly. You can also add a "\_" to other values.

You can then same the same and run MeshCentral again. This time, you don't need to specify the certificate name or --wanonly. You just need to run it like this:

node ./node modules/meshcentral

The server should now run correctly and use MongoDB. You can even delete the file ~/meshcentral-data/meshcentral.db as it's not going to be used anymore. You can check that it runs correctly by browsing to the server's address again and creating a new account. The first account that is created will be administrator for the server, so don't delay and create the first account right away.

Once you are done, we can stop the server again using CTRL-C and in the next sections, we will look at starting the server in the background.

#### 4.7 Manually starting the server

We can manually start and stop the MeshCentral server in the background in different ways. In this section, we are going to create two commands "mcstart" and "mcstop" to take care of this. Type this to create the two commands:

```
echo "node ./node_modules/meshcentral > stdout.txt 2> stderr.txt &" > mcstart
chmod 755 mcstart
echo "pkill -f node_modules/meshcentral" > mcstop
chmod 755 mcstop
```

You can now run the "./mcstart" command to launch the server in the background and stop it using the "./mcstop" to stop it. This should work pretty well, but if the AWS instance is ever stopped and started again, the server will not automatically launch.

#### 4.8 Automatically starting the server

Since Amazon Linux 2 supports systemd, we are going to use that to auto-start MeshCentral in the background. First, we need to know our own username and group. If we do "Is -I" in our home folder we get for example:

```
drwxr-xr-x 2 default default 4096 Jul 20 00:03 Desktop
drwxr-xr-x 2 default default 4096 Jul 20 00:03 Documents
drwxr-xr-x 2 default default 4096 Jul 20 00:03 Downloads
...
```

Note the username and group name, in this example it's "default" for both. We need this information to create the system service description file. To create this file type:

sudo pico /etc/systemd/system/meshcentral.service

Then enter the following lines:

[Unit] Description=MeshCentral Server

```
[Service]
Type=simple
LimitNOFILE=1000000
ExecStart=/usr/bin/node /home/default/node_modules/meshcentral
WorkingDirectory=/home/default
Environment=NODE_ENV=production
User=default
Group=default
Restart=always
# Restart service after 10 seconds if node service crashes
RestartSec=10
# Set port permissions capability
AmbientCapabilities=cap_net_bind_service
[Install]
WantedBy=multi-user.target
```

Note that the user and group values have to be set correctly for your specific situation. Also, the ExecStart and WorkingDirectory lines includes the path to the user's home folder which includes the username in it. Make sure that is set correctly.

Once this is done, you can now start, enable, stop and disable using the following commands:

sudo systemctl enable meshcentral.service sudo systemctl start meshcentral.service sudo systemctl stop meshcentral.service sudo systemctl disable meshcentral.service

Type in the first two commands to start and enable the service. Enabling the service will make it automatically start when the computer restarts.

Once the server is launched, you can access it using a web browser as before. From this point on, refer to the MeshCentral User's Guide for information on how to configure and use MeshCentral.

## 5. Raspberry Pi

In this section, we will look at installing MeshCentral on the famous Raspberry Pi. This computer's low price makes it a perfect always-on system for managing computers on a home or small business network. This installation will work on any version of the Raspberry Pi, but version 3 certainly much faster.



For this installation, we are going to use the Raspbian operating system. You can use the NOOBS version to install this operating system on your Raspberry Pi and install Raspbian. For best performance you can use the "Raspbian Stretch Lite" image which is much smaller and does not have the X desktop interface. To keep things even smaller, we are not going to be installing MongoDB, instead we are just going to be using NeBD as a database that comes by default with MeshCentral.

## 5.1 Installing NodeJS

Start by opening a terminal. For all of the installation, we will assume we are the default "pi" user and we are in the home ( $\sim$ ) folder. Let's get started by installing NodeJS.

```
sudo apt-get update
sudo apt-get dist-upgrade
curl -sL https://deb.nodesource.com/setup_8.x | sudo -E bash
sudo apt-get -y install nodejs
```

We can now check what version of Node was installed by typing:

node -v

If all goes well, we can now move on to port permissions and installing MeshCentral itself.

#### 5.2 Port permissions

On Linux, ports below 1024 are reserved for the "root" user. This is a security feature. In our case MeshCentral will need to listen to ports 80 and 443. To allow this, we need to allow node to listen to ports below 1024 like this:

```
whereis node
node: /usr/bin/node /usr/include/node /usr/share/man/man1/node.1.gz
sudo setcap cap_net_bind_service=+ep /usr/bin/node
```

We first locate the node binary, using "whereis node", we then use the "setcap" command to add permissions to node. Note that we take the path given by whereis and place it in the setcap command. The "setcap" command will set permissions allowing node to use ports 1024 and below. This permission may be lost when updating the Linux kernel, so this command may need to be applied again in some case.

#### 5.3 Installing MeshCentral

Now, we can use the Node Package Manager (NPM) to install MeshCentral.

```
npm install meshcentral
```

Do not use "sudo" in front of "npm install meshcentral".

After that, we can run MeshCentral for the first time. We want to run in WAN-only mode since we will not be managing any computers on the same local network at this server. We also want to create a server with a certificate name that is the same at the AWS instance name. So, we will use "--wanonly" and "--cert [name]" arguments to get the server started. For example:

node node\_modules/meshcentral --lanonly --fastcert

At this point, the server will create its certificates and start running.

MeshCentral HTTP redirection web server running on port 80. Generating cortificates, may take a few minutes... Generating root certificate... Generating METPS certificate... Generating Intel AMT MPS certificate... Generating Intel AMT console certificate... Server name not configured, running in LAN-only mode. MeshCentral HTTPS web server running on port 443. Server has no users, next new account will be site administrator.

The next step is to get the IP address of the Raspberry Pi. Use "ipconfig":

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.2.162 netmask 255.255.255.0 broadcast 192.168.2.255 inet6 fe80::8841:34b7:685:14a7 prefixlen 64 scopeid 0x20<link> ether b8:27:eb:01:13:3f txqueuelen 1000 (Ethernet) RX packets 58325 bytes 72302196 (68.9 MiB) RX errors 0 dropped 271 overruns 0 frame 0 TX packets 28457 bytes 3576126 (3.4 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

You can now open a browser to the name of the server, for example:

https://192.168.2.162

You will see the server working as expected. You will get a certificate error since the server is used an untrusted certificate for now. Just ignore the error and see the MeshCentral User's Guide to fix this.



#### 5.4 Configuring for LAN-only mode

By default, MeshCentral will assume that you are managing devices both on a local network and on the internet. In the case of this Raspberry Pi installation, we only want to manage device on the local network and so, we can configure MeshCentral to do this. It will adapt the server for this usages. To do this, edit the config.json file:

```
pico ~/meshcentral-data/config.json
```

Then, make the start of the file look like this:

```
{
   "settings": {
    "LANonly": true,
    "FastCert": true,
    "_Port": 443,
    "_RedirPort": 80,
    "_AllowLoginToken": true,
    "_AllowFraming": true,
    "_AllowFraming": true,
    "_WebRTC": false,
    "_ClickOnce": false,
    "_UserAllowedIP" : "127.0.0.1,::1,192.168.0.100"
    },
...
}
```

While we are at it, we can put "FastCert" to true so that RSA2048 certificates are created instead of RSA3072. This is less secure but runs much faster on small processors like the Raspberry Pi. This is the same as specifying "--fastcert" in the prior section.

#### 5.5 Manually starting the server

We can manually start and stop the MeshCentral server in the background in different ways. In this section, we are going to create two commands "mcstart" and "mcstop" to take care of this. Type this to create the two commands:

```
echo "node ./node_modules/meshcentral > stdout.txt 2> stderr.txt &" > mcstart
chmod 755 mcstart
echo "pkill -f node_modules/meshcentral" > mcstop
chmod 755 mcstop
```

You can now run the "./mcstart" command to launch the server in the background and stop it using the "./mcstop" to stop it. This should work pretty well, but if the AWS instance is ever stopped and started again, the server will not automatically launch.

#### 5.6 Automatically starting the server

Since Raspbian OS supports systemd, we are going to use that to auto-start MeshCentral in the background. First, we need to know our own username and group. If we do "Is -I" in our home folder we

drwxr-xr-x 2 pi pi 4096 Jul 19 21:23 Desktop drwxr-xr-x 2 pi pi 4096 Jun 26 18:23 Documents drwxr-xr-x 2 pi pi 4096 Jun 26 18:23 Downloads ...

Note the username and group name, in this example it's "pi" for both. We need this information to create the system service description file. To create this file type:

```
sudo nano /etc/systemd/system/meshcentral.service
```

Then enter the following lines:

```
[Unit]
Description=MeshCentral Server
[Service]
Type=simple
LimitNOFILE=1000000
ExecStart=/usr/bin/node /home/pi/node_modules/meshcentral
WorkingDirectory=/home/pi
Environment=NODE_ENV=production
User=pi
Group=pi
Restart=always
# Restart service after 10 seconds if node service crashes
RestartSec=10
# Set port permissions capability
AmbientCapabilities=cap net bind service
```

```
[Install]
WantedBy=multi-user.target
```

Note that the user and group values have to be set correctly for your specific situation. Also, the ExecStart and WorkingDirectory lines includes the path to the user's home folder which includes the username in it. Make sure that is set correctly.

Once this is done, you can now enable, start, stop and disable using the following commands:

```
sudo systemctl enable meshcentral.service
sudo systemctl start meshcentral.service
sudo systemctl stop meshcentral.service
sudo systemctl disable meshcentral.service
```

Type in the first two commands to start and enable the service. Enabling the service will make it automatically start when the computer restarts.

Once the server is launched, you can access it using a web browser as before. From this point on, refer to the MeshCentral User's Guide for information on how to configure and use MeshCentral.

#### 6. Ubuntu 18.04

In this section, we will look at installing MeshCentral on Ubuntu 18.04 LTS. This is a long term support of Ubuntu freely available for download at <u>https://www.ubuntu.com</u>. Both the desktop and server versions of Ubuntu will work. If this is a remote server and the desktop will not be needed, the server version of Ubuntu can be used. This section will describe a way to install MeshCentral in a user's home folder, however there is a more secure way to do it, see "Increased Security Installation" at the end of this section.



In all cases, MeshCentral <u>must not be installed as root user</u>. It's not secure and the instructions below will not work correctly.

#### 6.1 Installing NodeJS

The first thing to do is get NodeJS installed on the computer. We first install the node version manager then activate it and install the NodeJS LTS. It's done with 4 commands:

```
sudo add-apt-repository universe
sudo apt update
sudo apt install nodejs -y
sudo apt install npm -y
```

We can test what version of Node and NPM are installed using:

```
node -v
npm -v
```

#### 6.2 Installing MongoDB

If we are going to run a large instance, it's best to use MongoDB as the database. If you are using a small instance, you can skip installing MongoDB and MeshCentral will use NeDB instead which is a light weight database that is probably great for managing less than 100 computers.



If you want to use MongoDB, we can install MongoDB Community Edition. More information on how to do this for Ubuntu can be found here.

You can install the package using apt and get it started like this:

```
sudo apt install mongodb -y
```

Then start the Mongodb service in the background and enable it for auto-restart.

sudo systemctl start mongodb
sudo systemctl enable mongodb

To verify that MongoDB is running, you can enter the MongoDB shell like this:

mongo --host 127.0.0.1:27017

You can leave the shell using Ctrl-C. The database and log files will be create at these locations:

/var/log/mongodb /var/lib/mongo

This is useful to know if you want to make a backup of the database file.

#### 6.3 Port permissions

On Linux, ports below 1024 are reserved for the "root" user. This is a security feature. In our case MeshCentral will need to listen to ports 80 and 443. To allow this, we need to allow node to listen to ports below 1024 like this:

whereis node node: /usr/bin/node /usr/include/node /usr/share/man/man1/node.1.gz sudo setcap cap net bind service=+ep /usr/bin/node

We first locate the node binary, using "whereis node", we then use the "setcap" command to add permissions to node. Note that we take the path given by whereis and place it in the setcap command. The "setcap" command will set permissions allowing node to use ports 1024 and below. This permission may be lost when updating the Linux kernel, so this command may need to be applied again in some case.

#### 6.4 Installing MeshCentral

Now, we can use the node package manager (NPM) to install MeshCentral.

```
npm install meshcentral
```

Do not use "sudo" in front of "npm install meshcentral".

After that, we can run MeshCentral for the first time. For example:

node ./node modules/meshcentral

If the computer has a well-known DNS name that users and agents will use to connect to this server, run MeshCentral like this:

node ./node\_modules/meshcentral --cert example.servername.com

At this point, the server will create its certificates and start running.

```
MeshCentral HTTP redirection web server running on port 80.
Generating certificates, may take a few minutes...
Generating root certificate...
Generating HTTPS certificate...
Generating Intel AMT MPS certificate...
Generating Intel AMT console certificate...
MeshCentral Intel(R) AMT server running on ec2-54-245-141-130.us-west-2.compute.amazonaws.com:4433.
MeshCentral HTTPS web server running on ec2-54-245-141-130.us-west-2.compute.amazonaws.com:443.
Server has no users, next new account will be site administrator.
```

You can now open a browser and try the server. If you can on the same computer, you navigate to this URL:

http://localhost

If installing on a server that does not have a desktop GUI, use a different computer and enter http:// followed by the IP address or name of the server you installed.

You should see the server working as expected. You will get a certificate error since the server is used an untrusted certificate for now. Just ignore the error and see the MeshCentral User's Guide to fix this.



At this point, the server is usable but, there are two things that may still need to be done. First, if we opted to use MongoDB, we have to configure MeshCentral to use a MongoDB database. By default, NeDB will be used which should only be used for small deployments managing less than 100 computers. We also need to automatically start the server when the computer starts.

To continue, stop the MeshCentral server with CTRL-C.

#### 6.5 Configuring for MongoDB

By default, MeshCentral uses NeDB with a database file located in ~/meshcentraldata/meshcentral.db. This is great for small servers, but if we opted to install MongoDB, let's make use of it. We need to edit the config.json file located in the meshcentral-data folder.

pico ~/meshcentral-data/config.json

Then, make the start of the file look like this:

```
{
   "settings": {
    "MongoDb": "mongodb://127.0.0.1:27017/meshcentral",
    "WANonly": true,
    "_Port": 443,
    "_RedirPort": 80,
    "_AllowLoginToken": true,
    "_AllowFraming": true,
    "_MebRTC": false,
    "_ClickOnce": false,
    "_UserAllowedIP" : "127.0.0.1,::1,192.168.0.100"
    },
...
}
```

If you start with the default config.json created by MeshCentral, you will need to remove some "\_" characters in front of settings, mongodb and wanonly. You can also add a "\_" to other values. For details on all of the config.json options, including the "WANonly" option, refer to the **MeshCentral User's Guide**.

You can then save the config.json file and run MeshCentral again. This time, you don't need to specify the certificate name. You just need to run it like this:

```
node ./node modules/meshcentral
```

The server should now run correctly and use MongoDB. You can even delete the file ~/meshcentral-data/meshcentral.db as it's not going to be used anymore. You can check that it runs correctly by browsing to the server's address again and creating a new account. The first account that is created will be administrator for the server, so don't delay and create the first account right away.

Once you are done, we can stop the server again using CTRL-C and in the next sections, we will look at starting the server in the background.

#### 6.6 Manually starting the server

We can manually start and stop the MeshCentral server in the background in different ways. In this section, we are going to create two commands "mcstart" and "mcstop" to take care of this. Type this to create the two commands:

```
echo "node ./node_modules/meshcentral > stdout.txt 2> stderr.txt &" > mcstart
chmod 755 mcstart
echo "pkill -f node_modules/meshcentral" > mcstop
chmod 755 mcstop
```

You can now run the "./mcstart" command to launch the server in the background and stop it using the "./mcstop" to stop it. This should work pretty well, but if the AWS instance is ever stopped and started again, the server will not automatically launch.

#### 6.7 Automatically starting the server

Since Ubuntu 18.04 supports systemd, we are going to use that to auto-start MeshCentral in the background. First, we need to know our own username and group. If we do "Is -I" in our home folder we get for example:

```
drwxr-xr-x2defaultdefault4096Jul2000:03Desktopdrwxr-xr-x2defaultdefault4096Jul2000:03Documentsdrwxr-xr-x2defaultdefault4096Jul2000:03Downloads
```

Note the username and group name, in this example it's "default" for both. We need this information to create the system service description file. To create this file type:

sudo pico /etc/systemd/system/meshcentral.service

Then enter the following lines:

```
[Unit]
Description=MeshCentral Server
[Service]
Type=simple
LimitNOFILE=1000000
ExecStart=/usr/bin/node /home/default/node modules/meshcentral
WorkingDirectory=/home/default
Environment=NODE ENV=production
User=<mark>default</mark>
Group=default
Restart=always
# Restart service after 10 seconds if node service crashes
RestartSec=10
# Set port permissions capability
AmbientCapabilities=cap net bind service
[Install]
WantedBy=multi-user.target
```

Note that the user and group values have to be set correctly for your specific situation. Also, the ExecStart and WorkingDirectory lines includes the path to the user's home folder which includes the username in it. Make sure that is set correctly. Lastly the path to node may need to be changed. Type "whereis node" to find the correct path.

Once this is done, you can now start, enable, stop and disable using the following commands:

sudo systemctl enable meshcentral.service sudo systemctl start meshcentral.service sudo systemctl stop meshcentral.service sudo systemctl disable meshcentral.service

Type in the first two commands to start and enable the service. Enabling the service will make it automatically start when the computer restarts.

Once the server is launched, you can access it using a web browser as before. From this point on, refer to the MeshCentral User's Guide for information on how to configure and use MeshCentral.

#### 6.8 Increased Security Installation

On Debian based Linux distributions like Ubuntu, a better and more secure way to install MeshCentral is to have it run within a user account this restricted privileges. When installed like this, the self-update capability of MeshCentral will not work. Instead of installing MeshCentral in the user's home folder, we install it in /opt/meshcentral and we create a meshcentral user that does not have rights to login or change any of the MeshCentral files. To do this, start by creating a new user called "meshcentral"

sudo useradd -r -d /opt/meshcentral -s /sbin/nologin meshcentral

We can then create the installation folder, install and change permissions of the files so that the "meshcentral" account gets read-only access to the files.

```
sudo mkdir /opt/meshcentral
cd /opt/meshcentral
sudo npm install meshcentral
sudo -u meshcentral node ./node modules/meshcentral
```

The last line will run MeshCentral manually and allow it to install any missing modules and create the MeshCentral data folders. Once it's running, press CTRL-C and continue. The following two lines will change the ownership of files to the meshcentral user and restrict access to the files.

```
sudo chown -R meshcentral:meshcentral /opt/meshcentral
sudo chmod 755 -R /opt/meshcentral/meshcentral-*
```

To make this work, you will need to make MeshCentral work with MongoDB because the /meshcentral-data folder will be read-only. In addition, MeshCentral will not be able to update itself since the account does not have write access to the /node\_modules files, so the update will have to be manual. First used systemctl to stop the MeshCentral server process, than use this:

```
cd /opt/meshcentral
sudo npm install meshcentral
sudo -u meshcentral node ./node modules/meshcentral
```

sudo chown -R meshcentral:meshcentral /opt/meshcentral

This will perform the update to the latest server on NPM and re-set the permissions so that the meshcentral user account has read-only access again. You can then use systemctl to make the server run again.

MeshCentral allows users to upload and download files stores in the server's "meshcentral-files" folder. In an increased security setup, we still want the server to be able to read and write files to this folder and we can allow this with:

```
sudo chmod 755 -R /opt/meshcentral/meshcentral-files
```

If you plan on using the increased security installation along with MeshCentral built-in Let's Encrypt support you will need to type the following commands to make the "letsencrypt" folder in "meshcentral-data" writable.

```
sudo mkdir /opt/meshcentral/meshcentral-data
sudo mkdir /opt/meshcentral/meshcentral-data/letsencrypt
sudo chmod 755 -R /opt/meshcentral/meshcentral-data/letsencrypt
```

This will allow the server to get and periodically update its Let's Encrypt certificate. If this is not done, the server will generate an "ACCES: permission denied" exception.

## 7. Microsoft Azure

In this section, we will look installing MeshCentral on Microsoft Azure. Microsoft Azure offers many operating system options and we will be selecting "Ubuntu Server" as our choice. From the Azure portal, we select "Virtual machines" on the left and "Add".



Once you click on Ubuntu Server, you will see a list of available versions. In this example, we selected Ubuntu 18.04 LTS (Long Term Support). We then have to create an instance name and a way to authenticate to the instance.

A Basics - Microsoft Azure	× +				- 🗆 ×
← → ⊂ ŵ	(1) 🔒 https://portal.azure.com/#create/Canonic	al.UbuntuServer1804LTS-ARM ••••	🛡 🟠 🔍 Search		\ ≈ 💶 🛡 🗉 😑
Microsoft Azure		${\cal P}$ Search resources, services, and docs	× 🗘 >_ &	\$ © 0 F	
«	Home > Virtual machines > Compute > Ubuntu Serv	r > Ubuntu Server 18.04 LTS > Create virtual machine > Ba	isics		
	<b>1</b> Basics →	* Name MeshCentral			
— 🛧 FAVORITES ————	<ul> <li>Configure basic settings</li> </ul>	VM disk type 🛛			
📮 Dashboard	C Size	SSD V			
# All resources	Choose virtual machine size	* Username			
Resource groups		default 🗸			
🔇 App Services	3 Configure optional features	SSH public key Password			
Function Apps		* Password			
SOI databases	4 Summary > Ubuntu Server 18.04 LTS	•••••••••••••••••••••••••••••••••••••••			
		* Confirm password			
		Subscription			
Virtual machines		Visual Studio Enterprise $\checkmark$			
🍄 Load balancers		* Resource group  Create new			
Storage accounts		Mesh ~			
Virtual networks		* Location			
Azure Active Directory		East US 🗸 🗸			
😁 Monitor					
🔷 Advisor		ОК			
Security Center ¥	<				>

Next is the type of instance to launch. Any instance will do including the "B1s" which is the smallest possible instance. Of course, as you manage more computers, using an instance that is a bit more powerful is a good idea.

) → C' û	() 🔒 P	https://portal.az	ure.com/#ci	reate/Canonical.UI	ountuServer1804LTS-ARM		··· 🛡 🏠 🖸	C Search			I\ 🕫 🗳 🗊 🗊
licrosoft Azure				کر	O Search resources, service			< 🗘 >_	. 🏶 🙂	0 🗣	
Create a resource	Home >	Virtual machines Choose a Browse the ava	<ul> <li>Compute</li> <li>SiZE</li> <li>illable sizes and</li> </ul>	> Ubuntu Server >							
All services		Search			Compute type		Disk type			vCPUs	
	<b>~</b>				Show all compute types		<ul> <li>SSD only</li> </ul>		~		0 12
HAVORITES	0	RECOMME 🔧	SKU	TU TYPE TU	COMPUTE 斗 VCPUS	tu GB RAM	DATA DISKS	MAX IOPS	tocal SSD	°↓ PREMIUM °↓	ADDITION
Dashboard	>										
All resources		Available									
Resource groups			B1s	Standard	General purpose 1	1	2	800	4 GB	SSD	\$8.04
App Services	>		B1ms	Standard	General purpose 1	2	2	1600	4 GB	SSD	\$15.40
			B2s	Standard	General purpose 2	4	4	3200	8 GB	SSD	\$31.25
Function Apps	>		B2ms	Standard	General purpose 2	8	4	4800	16 GB	SSD	\$62.50
SQL databases			B4ms	Standard	General purpose 4	16	8	7200	32 GB	SSD	\$124.25
Azure Cosmos DB			B8ms	Standard	General purpose 8	32	16	10800	64 GB	SSD	\$249.24
Virtual machines		*	D2s_v3	Standard	General purpose 2	8	4	4000	16 GB	SSD	\$71.42
Load balancers		*	D4s_v3	Standard	General purpose 4	16	8	8000	32 GB	SSD	\$142.85
Storage accounts			D8s_v3	Standard	General purpose 8	32	16	16000	64 GB	SSD	\$285.70
Vistual astronom			D16s_v3	Standard	General purpose 16	64	32	32000	128 GB	SSD	\$571.39
Virtual networks		Dricos pro	od are estimat	tos in your local	anguthat include only A i	instructure contra	nd any discourt-f-	the subscription	and location. Th	e prices depit in -!!-	any applicable offerer
Azure Active Directory		Recommende	eu are estima ed sizes are de	termined by the pub	lisher of the selected image bas	ed on hardware an	d software requirem	ients.	r and location. Th	e prices don't include	any applicable software co
Monitor											
Advisor		Select									

After selecting the instance type, you can configure storage. 30 gigabytes is plenty. Then the Network Security Group. This is where it's important to open at least TCP ports 22, 80 and 443.

Туре	Protocol	Port Range	Description
SSH	ТСР	22	SSH
HTTP	ТСР	80	HTTP
HTTPS	TCP	443	HTTPS
Custom TCP Rule	TCP	4433	Intel AMT CIRA
Custom TCP Rule	TCP	8080	Swarm Server*

Optionally if you wish to use the instance with Intel AMT, open port 4433. In addition port 8080 must be open if you are migrating from MeshCentral1 (not typical).

Lastly we launch the instance, it will take a few minutes to setup.



You can then find the public IP address and use a SSH client like PUTTY on Windows to connect to the instance and start getting MeshCentral setup. From this point on, just use the Ubuntu section above to complete the installation.

# 8. Google Cloud

In this section, we will look installing MeshCentral on Google Cloud. You can sign up easily at <u>https://cloud.google.com/</u> and you can run a small instance for less than 5\$ a month.



Once you have create an account, you can go to the main console and on the left side, go to "Compute Engine" and create a new VM instance. For our demonstration, we are going to create the smallest instance possible which is a single shared CPU and only 0.6 gigs of RAM.

	😟 Compute Engine - MeshCentra 🗙	+						-		×	
¢	→ C' 🏠 (i) 🔒 htt	ps://console.cloud.google.com/compute/instan 🛛 💀 😒 🏠 🔍 Search	n			111	12	¢2	<b>v</b> (		
=	Google Cloud Platform	💲 MeshCentral 👻 🔍		Ĩ	>.	ø	?	۰	÷	0	
۲	Compute Engine	← Create an instance									
8	VM instances	Name 💿								^	
品	Instance groups	meshcentral									
	Instance templates	Region	\$4.28 per month estimated								
A	Sole tenant nodes	Machine type	Effective hourly rate \$0.006 (730 hours per month) Your first 744 hours of f1-micro instance usage are free thi								
	Disks	Customize to select cores, memory and GPUs.									
0	Snapshots	micro (1 shared • 0.6 GB memory Customize	↓ Deta	15							
[2]	Images	Upgrade your account to create instances with up to 96 cores									
~	TPUs	Container 🔞									
1%1	Committed use discounts	Deploy a container image to this VM instance. Learn more									
	Metadata	Boot disk 😡									
â	Health checks	New 10 GB standard persistent disk									
56	Zones	Ubuntu 18.04 LTS Minimal Change								- 1	
-											

We select the proper settings and select "Ubuntu 18.04 LTS Minimal" as the boot operating system. This is convenient as we already covered how to install MeshCentral on this operating system.

	Compute Engine - MeshCentra	× +		-	o ×
$\leftarrow$	→ C' û (i (i	https://console.cloud.google.com/compute/instant 🛛 🐨 😒 🏠 🔍 Search		II\ 🗠 🥵	♥ 🗊 😑
=	Google Cloud Platfo	m 🛟 MeshCentral 👻 🔍	ii 🛛 🤉	• • •	÷ 🗛
۲	Compute Engine	• VM instance details	STOP	T DELETE	
A	VM instances	Details Monitoring			^
晶	Instance groups	S meshcentral			
	Instance templates	Remote access			
8	Sole tenant nodes	SSH  Connect to serial console  Enable connecting to serial ports			
	Disks	Logs			
2	Snapshots	Stackdriver Logging Serial port 1 (console)			
[2]	Images				
×	TPUs	Machine type f1-micro (1 vCPU, 0.6 GB memory)			
1%)	Committed use discounts	CPU platform			
==	Metadata				
â	Health checks	us-east1-b			
56	Zones	Labels			
٩	Operations	Creation time			
	Quotas	Jul 22, 2018, 7:20:45 PM			
0	Security scans	Network interfaces Name Network Subnetwork Primary internal IP Alias IP ranges External IP	Network Tier 🔞	IP forwarding	Network deta
۰	Settings	nic0 default default 10.142.0.2 - 35.227.45.84 (ephemeral)	Premium	Off	View detail
		Public DNS PTR Record None Firewalls Allow HTTP traffic Allow HTTPS traffic			

Make sure to allow HTTP and HTTPS traffic. Setup like this, we will not be able to manage Intel AMT unless we also open TCP port 4433. Once done with all these options, we can launch the VM instance.



The new instance will take a few minutes to start up. An interesting feature of Google Cloud is that you can access the VM instance shell directly from the web browser. No need for a separate SSH client. This is exactly what we need and we opt to go ahead and option the web console.



If will log you in automatically, no additional credentials needed. We can then follow the "Ubuntu 18.04 LTS" section above to complete the installation. If you opt for a very small instance, it's probably a good idea to skip installing MongoDB. Just to get started quickly, we can use the following commands:

```
sudo apt update
sudo apt install nodejs -y
sudo apt install npm -y
sudo setcap cap_net_bind_service=+ep /usr/bin/node
npm install meshcentral
```

node ./node modules/meshcentral --fastcert -wanonly --cert 35.227.45.84

#### Do not use "sudo" in front of "npm install meshcentral".

This will install node and npm. Will allow non-root access to ports 80 and 443 and install and start MeshCentral. Because this example uses a very small server instance, we opted to use the "fastcert" option to create RSA 2048 certificates (the default is RSA 3072 which is more secure).

We use the "wantonly" option because MeshCentral will not be managing computers on a local network, and for this demonstration just used the external IP address of the instance as the server name.

If you plan on using an instance without the Intel AMT CIRA port being open (TCP 4433), it's recommended to add "--mpsport 0" so to inform MeshCentral that this port is not open and to not offer Intel AMT CIRA features.

Of course, this set of commands is just to get the server started quickly. Follow the Ubuntu 18.04 instructions to setup the server to automatically start using system.

#### 9. Ubuntu 16.04

In this section, we will look at installing MeshCentral on Ubuntu 16.04 LTS. This is the same installation at Ubuntu 18.04 LTS, however you need to install NodeJS in a special way. If you use "apt install node", you will get an older version 4.x of NodeJS that will not work with MeshCentral.



#### 9.1 Installing NodeJS

The first thing to do is get NodeJS installed on the computer. We first install the node version manager then activate it and install the NodeJS LTS. It's done with 3 commands:

```
cd ~
wget https://deb.nodesource.com/setup_8.x
sudo bash setup_8.x
sudo apt-get -y install nodejs
```

We can test what version of Node and NPM are installed using:

node -v npm -v

You should see Node version 8 and NPM version 5. At this point, you can continue installing MeshCentral using the Ubuntu 18.04 installation instructions.

## 10. OpenBSD 6.4

In this section, we will look at installing MeshCentral on OpenBSD 6.4. This section was originally written by Daulton and placed here with this permission. The original instructions are located at: <a href="https://daulton.ca/meshcentral-server-on-openbsd/">https://daulton.ca/meshcentral-server-on-openbsd/</a>. The section will setup MeshCentral on non-standard ports HTTPS/3000 and HTTP/3001. Thank you to Daulton for his contribution.



#### 10.1 Installing MongoDB

Install the Mongodb package.

pkg\_add mongodb

Start and enable Mongodb at boot.

rcctl start mongod
rcctl enable mongod

Temporary remount /usr with wxallowed while we compile the port. For Cloud VPS they usually only have a root partition instead of how OpenBSD splits it up by default, you will need to edit /etc/fstab and add wxallowed to the options for the root partition and then reboot. Assure to remove this from the fstab options after you are done.

mount -r -o wxallowed /usr/

## 10.2 Installing NodeJS

Install NodeJS from ports as it is not available by a package.

```
$ cd /tmp
$ ftp https://cdn.openbsd.org/pub/OpenBSD/$(uname -r)/{ports.tar.gz,SHA256.sig}
# cd /usr
# tar xzf /tmp/ports.tar.gz
# cd /usr/ports/lang/node
# make install
# make clean
```

## **10.3 Installing MeshCentral**

Create the MeshCentral user. The parameters used here are important as we will not let this user login, it has no home directory, and its class is set to daemon. In line with the OpenBSD daemon user naming scheme, we preface the username with an underscore (\_) to make it easily identifiable as a daemon user.

useradd -s /sbin/nologin -d /nonexistent -L daemon -u 446 meshcentral

Let's install MeshCentral and adjust the permissions.

```
mkdir -p /usr/local/meshcentral
```

```
cd /usr/local/meshcentral
npm install meshcentral
chown -R meshcentral: meshcentral /usr/local/meshcentral
```

Configuring for MongoDB and adjusting some other settings such as the network port. Open up the following config in an editor then, make the start of the file look like below. If the setting does not exist yet, just add it below one of the ones we are adjusting in the main settings block.

If you start with the default config.json created by MeshCentral, you will need to remove some underscore character in front of settings to enable the setting, such as mongodb and wanonly. You can also add an underscore to other values. For details on all of the config.json options, including the "WANonly" option, refer to the MeshCentral User's Guide.

Before you can edit the configuration, start the Meshcentral briefly so it generates the default configurations and certificates. Once you see that it says "MeshCentral HTTPS server running...", Ctrl-C to exit then edit the configuration file next.

```
cd /usr/local/meshcentral/node_modules/meshcentral/ && doas -u _meshcentral
/usr/local/bin/node /usr/local/meshcentral/node_modules/meshcentral/meshcentral.js
--launch
```

Edit the MeshCentral config.json. For example using vi:

vi /usr/local/meshcentral/meshcentral-data/config.json

In the settings section, set the following key value pairs:

```
{
    "settings": {
        "Cert": "meshcentral.example.com",
        "MongoDb": "mongodb://127.0.0.1:27017/meshcentral",
        "WANonly": true,
        "Port": 3000,
        "ExactPorts": true,
        "RedirPort": 3001,
        "allowLoginToken": true,
        "allowFraming": true,
        "NewAccounts": 0,
    },
    ...
}
```

Add the following to the root crontab to start MeshCentral at boot. Edit the root crontab by doing the following command as root: crontab -e

```
@reboot cd /usr/local/meshcentral/node_modules/meshcentral/ && doas -u
_meshcentral /usr/local/bin/node
/usr/local/meshcentral/node_modules/meshcentral/meshcentral.js --launch
```

As root launch Meshcentral while it installs mongojs, once that finishes and Meshcentral launches close it by doing Ctrl-C. Adjust the permissions again as we ran Meshcentral and it generated new files we need to change the ownership of.

/usr/local/bin/node /usr/local/meshcentral/node\_modules/meshcentral chown -R meshcentral: meshcentral /usr/local/meshcentral

Warning: do not keep this running or use this command in the future to start the Meshcentral server as it starts the server as root!

This is a reference /etc/pf.conf for you to keep your server secure. Add any locally connected networks which should have access and any public IP address of a network which will have client

PCs connect from to target\_whitelist table. Add your own home and/or business IP to my\_own\_IPs table.

```
ext if = vio0
set reassemble yes
set block-policy return
set loginterface egress
set ruleset-optimization basic
set skip on lo
icmp types = "{ 0, 8, 3, 4, 11, 30 }"
table <target whitelist> const { 45.63.15.84, 10.18.5.0/24 }
table <my own IPs> const { 45.63.15.84 }
table <bruteforce>
match in all scrub (no-df max-mss 1440)
match out all scrub (no-df max-mss 1440)
block in quick log from urpf-failed label uRPF
block quick log from <fail2ban>
block in from no-route to any
block in from urpf-failed to any
block in quick on $ext if from any to 255.255.255.255
block in log quick on $ext_if from { 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16,
255.255.255.255/32 } to any antispoof for $ext if
block log all
pass in quick inet proto icmp icmp-type $icmp types
pass in quick inet6 proto icmp6
pass in quick proto tcp from <my own IPs> \
to (egress) port { 22 } \setminus
flags S/SA modulate state \
(max-src-conn 5, max-src-conn-rate 5/5, overload <bruteforce> flush global)
pass in quick inet proto tcp from <target whitelist> to port 3000
pass in quick inet6 proto tcp from <target whitelist> to port 3000
block in quick log on egress all
pass out quick on egress proto tcp from any to any modulate state
pass out quick on egress proto udp from any to any keep state
pass out quick on egress proto icmp from any to any keep state
pass out quick on egress proto icmp6 from any to any keep state
```

After saving the configuration in /etc/pf.conf, reload the pf rules with:

pfctl -f /etc/pf.conf

To save rebooting and have MeshCentral launch then, launch it so you can begin using it. This time it is running as \_meshcentral, now it is safe to keep running and you can use this command in the future.

```
cd /usr/local/meshcentral/node_modules/meshcentral/ && doas -u _meshcentral
/usr/local/bin/node /usr/local/meshcentral/node_modules/meshcentral/meshcentral.js
--launch
```

You can now access MeshCentral at https://your address:3000 or https://meshcentral.example.com:3000 if you named the machine meshcentral or create an A record named meshcentral. The first user you create will be the Administrator, there is no default user.