Table of Contents

Introduction
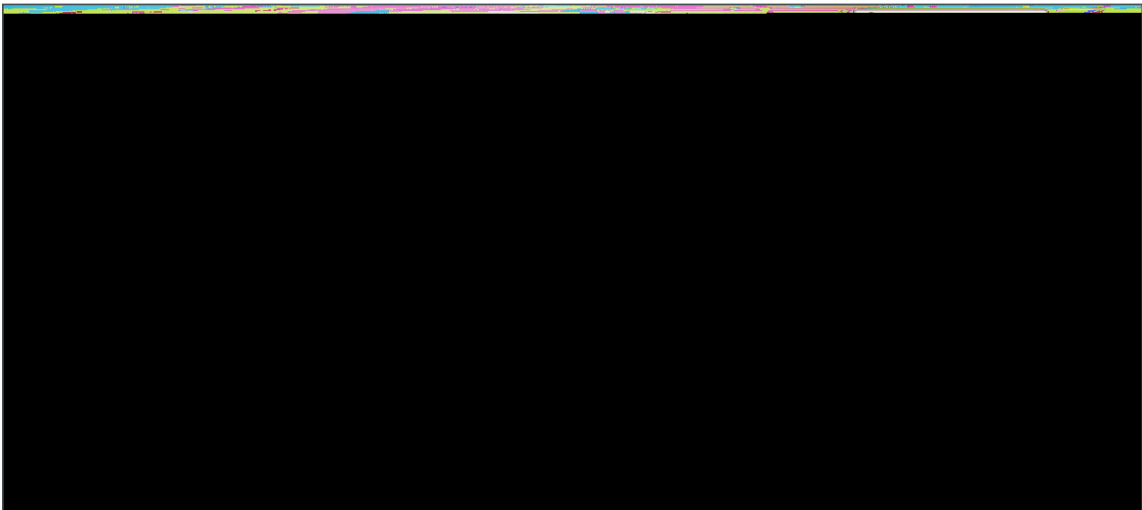
Technology Use Cases

Step 1:

Step 6:

Step 4: On the 802.11a/n tab, ensure that both **CleanAir** and **Enable** are selected.

Step 5: On the 802.11b/g/n tab, ensure that both **CleanAir** and **Enable** are selected.

Step 6: On the Apply/Schedule tab, click **Save**.

Step 3: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the

Step 5:

Step 2: At the **mse login** prompt, enter the default username and password: **root/password**

Step 5: Type **Y** for Yes, and then configure the domain name. (Example: cisco.local)

```
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Yes]:<ENTER>

Enter a domain name for the network domain to which this device belongs. It must
```

```
0) LOCAL0 (16)
1) LOCAL1 (17)
2) LOCAL2 (18)
3) LOCAL3 (19)
4) LOCAL4 (20)
5) LOCAL5 (21)
6) LOCAL6 (22)
7) LOCAL7 (23)
Enter a facility(0-7) :4 <ENTER>
```

Step 13: Type **S** for Skip. This skips the next step, which is used for modifying the iptables for the Cisco MSE.

```
Enter whether or not you would like to change the iptables for this machine
(giving access to certain host).

Configure Host access control settings ?(Y)es/(S)kip [Skip]: <ENTER>
```

Step 14: Configure Network Time Protocol (NTP), as shown below.

```
Network Time Protocol (NTP) Setup.
If you choose to enable NTP, the system time will be configured from NTP servers
that you select. Otherwise, you will be prompted to enter the current date and
time.
NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Yes] Yes
Enter whether or not you would like to set up the Network Time Protocol(NTP) for
this machine.
If you choose to enable NTP, the system time will be configured from NTP servers
that you select. Otherwise, you will be prompted to enter the correct date and
time.
Enable NTP (yes/no) [no]: Yes
Enter NTP server name or address: 10.4.48.17
Enter another NTP server IP address (or none) [none]: <ENTER>
Configure NTP Authentication ? (Y)es/(S)kip/(U)se default [Yes]: Skip
```

Step 15: Type **S** for Skip. This skips the configuration of the Cisco MSE audit rules, login banner, and console access.

```
Audit rules Setup.
Configure audit rules and enable Audit daemon? (Y)es/(S)kip/(U)se default [Yes]:
Skip <ENTER>
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [yes]: Skip <ENTER>
System console is not restricted.
Configure system console restrictions (Y)es/(S)kip(U)se default value [Yes] :
Skip <ENTER>
```

Step 16: Type **Yes**. This enables SSH root access.
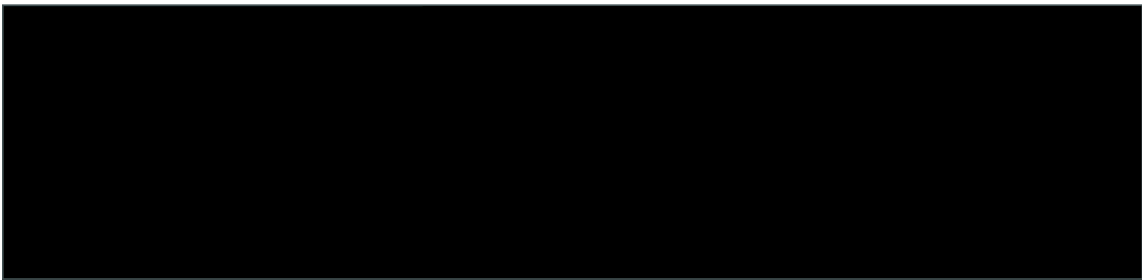
Step 2:

Step 3:

The Status changes to bi-directional as shown by the green arrows in the status column.

Step 8: Click **Next** to continue.

Step 9: On the Mobile App Enablement page, do not enable Mobile App Integration, click **Done**, and then on the "Your MSE Settings have been saved" message, click **OK**.

Step 1: Navigate to **Design > Mobility Services Engines**, and then verify that the configured IP address of the

Cat8SMSE154(es876pank+ActualText<FEFF2002>»»i2)(M)NavigateTU04385402(i)req och oigem5(c)5.6(ch o)6221.uGS1 gs

Step 5: At the **cmd>** prompt, issue the **show server-a3**çntvto]TJ0.264 0.319 0.327 rg/GS0 gs/T1o 1 Tf-.004 Tc 0-.00

Step 9: Verify that the Cisco MSE has been authorized on the wireless LAN controller.

```
(Cisco Controller) >show auth-list
Authorize MIC APs against Auth-list or AAA ...... disabled
Authorize LSC APs against Auth-List ............ disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate............... no
  AP with Locally Significant Certificate....... no

Mac Addr          Cert Type   Key Hash
----------------- ---------   --------------------------------------
00:50:56:a2:78:88 SSC         1f80d6662f2e42f9bf53f16671838193c3d751f1
(Cisco Controller) >
```

Step 10: Repeat Step 7 through Step 9 for each of the wireless LAN controllers that do not have an established
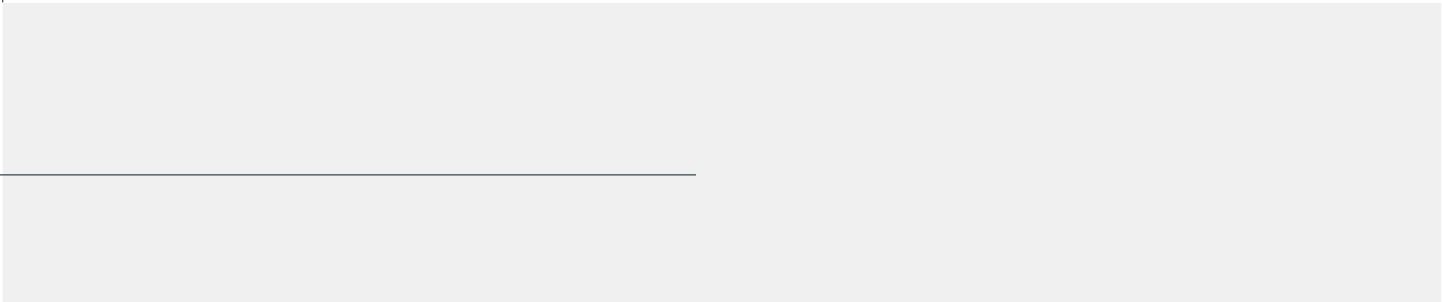
Step 8: In the Interferer Filter pane, in the

Appendix A: Product List

Wireless LAN ControllersFunctional Area

Please use the feedback form to send comments and suggestions about this guide.