ExtremeWireless™ Maintenance Guide

V10.51.01

9036082-00

Published February 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Table of Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Safety Information

Dangers

- Replace the power cable immediately if it shows any sign of damage.
- Replace any damaged safety equipment (covers, labels and protective cables) immediately.

- Use only original accessories or components approved for the system. Failure to observe these instructions may damage the equipment or even violate safety and EMC regulations.
- Only authorized Extreme Networks service personnel are permitted to service the system.

Warnings

- This device must not be connected to a LAN segment with outdoor wiring.
- Ensure that all cables are run correctly to avoid strain.
- Replace the power supply adapter immediately if it shows any sign of damage.
- Disconnect all power before working near power supplies unless otherwise instructed by a maintenance procedure.
- Exercise caution when servicing hot swappable components: power supplies or fans. Rotating fans can cause serious personal injury.
- This unit may have more than one power supply cord. To avoid electrical shock, disconnect all power supply cords before servicing. In the case of unit failure of one of the power supply modules, the module can be replaced without interruption of power to the ExtremeWireless Appliance. However, this procedure must be carried out with caution. Wear gloves to avoid contact with the module, which will be extremely hot.
- There is a risk of explosion if a lithium battery is not correctly replaced. The lithium battery must be replaced only by an identical battery or one recommended by the manufacturer.
- Always dispose of lithium batteries properly.
- Do not attempt to lift objects that you think are too heavy for you.

Cautions

- Check the nominal voltage set for the equipment (operating instructions and type plate). High voltages capable of causing shock are used in this equipment. Exercise caution when measuring high voltages and when servicing cards, panels, and boards while the system is powered on.
- Only use tools and equipment that are in perfect condition. Do not use equipment with visible damage.
- To protect electrostatic sensitive devices (ESD), wear a wristband before carrying out any work on hardware.
- Lay cables so as to prevent any risk of them being damaged or causing accidents, such as tripping.

Sicherheitshinweise

Gefahrenhinweise

- Sollte das Netzkabel Anzeichen von Beschädigungen aufweisen, tauschen Sie es sofort aus.
- Tauschen Sie beschädigte Sicherheitsausrüstungen (Abdeckungen, Typenschilder und Schutzkabel) sofort aus.
- Verwenden Sie ausschließlich Originalzubehör oder systemspezifisch zugelassene Komponenten. Die Nichtbeachtung dieser Hinweise kann zur Beschädigung der Ausrüstung oder zur Verletzung von Sicherheits- und EMV-Vorschriften führen.
- Das System darf nur von autorisiertem Extreme Networks-Servicepersonal gewartet werden.

Warnhinweise

- Dieses Gerät darf nicht über Außenverdrahtung an ein LAN-Segment angeschlossen werden.
- Stellen Sie sicher, dass alle Kabel korrekt geführt werden, um Zugbelastung zu vermeiden.
- Sollte das Netzteil Anzeichen von Beschädigung aufweisen, tauschen Sie es sofort aus.
- Trennen Sie alle Stromverbindungen, bevor Sie Arbeiten im Bereich der Stromversorgung vornehmen, sofern dies nicht für eine Wartungsprozedur anders verlangt wird.
- Gehen Sie vorsichtig vor, wenn Sie an Hotswap-fähigen Wireless Controller-Komponenten (Stromversorgungen oder Lüftern) Servicearbeiten durchführen. Rotierende Lüfter können ernsthafte Verletzungen verursachen.
- Dieses Gerät ist möglicherweise über mehr als ein Netzkabel angeschlossen. Um die Gefahr eines elektrischen Schlages zu vermeiden, sollten Sie vor Durchführung von Servicearbeiten alle Netzkabel trennen. Falls eines der Stromversorgungsmodule ausfällt, kann es ausgetauscht werden, ohne die Stromversorgung zum Wireless Controller zu unterbrechen. Bei dieser Prozedur ist jedoch mit Vorsicht vorzugehen. Das Modul kann extrem heiß sein. Tragen Sie Handschuhe, um Verbrennungen zu vermeiden.
- Bei unsachgemäßem Austausch der Lithium-Batterie besteht Explosionsgefahr. Die Lithium-Batterie darf nur durch identische oder vom Händler empfohlene Typen ersetzt werden.
- Achten Sie bei Lithium-Batterien auf die ordnungsgemäße Entsorgung.
- Versuchen Sie niemals, ohne Hilfe schwere Gegenstände zu heben.

Vorsichtshinweise

- Überprüfen Sie die für die Ausrüstung festgelegte Nennspannung (Bedienungsanleitung und Typenschild). Diese Ausrüstung arbeitet mit Hochspannung, die mit der Gefahr eines elektrischen Schlages verbunden ist. Gehen Sie mit großer Vorsicht vor, wenn Sie bei eingeschaltetem System Hochspannungen messen oder Karten, Schalttafeln und Baugruppen warten.
- Verwenden Sie nur Werkzeuge und Ausrüstung in einwandfreiem Zustand. Verwenden Sie keine Ausrüstung mit sichtbaren Beschädigungen.
- Tragen Sie bei Arbeiten an Hardwarekomponenten ein Armband, um elektrostatisch gefährdete Bauelemente (EGB) vor Beschädigungen zu schützen.
- Verlegen Sie Leitungen so, dass sie keine Unfallquelle (Stolpergefahr) bilden und nicht beschädigt werden.

Consignes De Sécurité

Dangers

- Si le cordon de raccordement au secteur est endommagé, remplacez-le immédiatement.
- Remplacez sans délai les équipements de sécurité endommagés (caches, étiquettes et conducteurs de protection).
- Utilisez uniquement les accessoires d'origine ou les modules agréés spécifiques au système. Dans le cas contraire, vous risquez d'endommager l'installation ou d'enfreindre les consignes en matière de sécurité et de compatibilité électromagnétique.
- Seul le personnel de service Extreme Networks est autorisé à maintenir/réparer le système.

Avertissements

- Cet appareil ne doit pas être connecté à un segment de LAN à l'aide d'un câblage extérieur.
- Vérifiez que tous les câbles fonctionnent correctement pour éviter une contrainte excessive.
- Si l'adaptateur d'alimentation présente des dommages, remplacez-le immédiatement.
- Coupez toujours l'alimentation avant de travailler sur les alimentations électriques, sauf si la procédure de maintenance mentionne le contraire.
- Prenez toutes les précautions nécessaires lors de l'entretien/réparations des modules du Wireless Controller pouvant être branchés à chaud : alimentations électriques ou ventilateurs.Les ventilateurs rotatifs peuvent provoquer des blessures graves.
- Cette unité peut avoir plusieurs cordons d'alimentation.Pour éviter tout choc électrique, débranchez tous les cordons d'alimentation avant de procéder à la maintenance.En cas de panne d'un des modules d'alimentation, le module défectueux peut être changé sans éteindre le Wireless Controller. Toutefois, ce remplacement doit être effectué avec précautions. Portez des gants pour éviter de toucher le module qui peut être très chaud.
- Le remplacement non conforme de la batterie au lithium peut provoquer une explosion. Remplacez la batterie au lithium par un modèle identique ou par un modèle recommandé par le revendeur.
- Sa mise au rebut doit être conforme aux prescriptions en vigueur.
- N'essayez jamais de soulever des objets qui risquent d'être trop lourds pour vous.

Précautions

- Contrôlez la tension nominale paramétrée sur l'installation (voir le mode d'emploi et la plaque signalétique). Des tensions élevées pouvant entraîner des chocs électriques sont utilisées dans cet équipement. Lorsque le système est sous tension, prenez toutes les précautions nécessaires lors de la mesure des hautes tensions et de l'entretien/réparation des cartes, des panneaux, des plaques.
- N'utilisez que des appareils et des outils en parfait état. Ne mettez jamais en service des appareils présentant des dommages visibles.
- Pour protéger les dispositifs sensibles à l'électricité statique, portez un bracelet antistatique lors du travail sur le matériel.
- Acheminez les câbles de manière à ce qu'ils ne puissent pas être endommagés et qu'ils ne constituent pas une source de danger (par exemple, en provoquant la chute de personnes).

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.

- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).
3 Select the products for which you would like to receive notifications.

Note
You can modify your product selections or unsubscribe at any time.

4 Click **Submit**.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/

Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

1 About This Guide

Who Should Use This Guide
How to Use This Guide

The purpose of this guide is to assist you in performing the maintenance of the following hardware and software components of the ExtremeCloud™ Solution:

HARDWARE

- ExtremeWireless Appliances
- ExtremeWireless APs

This guide covers the following ExtremeWireless Appliance models:

- ExtremeWireless Appliance C5210
- ExtremeWireless Appliance C5215
- ExtremeWireless Appliance C35
- Virtual Wireless Appliance V2110 (VMWare and MS Hyper-V platforms)

SOFTWARE

- ExtremeCloud™ Software

Who Should Use This Guide

This guide is intended for network administrators who are responsible for maintaining the ExtremeWireless Solution.

Electrical Hazard: Only qualified personnel should install or service this unit.

Riesgo Electrico: Nada mas personal capacitado debe de instalar o darle servicio a esta unida.

Elektrischer Gefahrenhinweis: Installationen oder Servicearbeiten sollten nur durch ausgebildetes und qualifiziertes Personal vorgenommen werden.

How to Use This Guide

Read through this guide completely to familiarize yourself with its contents and to gain an understanding of the features and capabilities of the ExtremeCloud™ software. A general working knowledge of data communications networks is helpful when setting up these modules.

This section provides an overview of this guide and a brief summary of each chapter; defines the conventions used in this document; and instructs how to obtain technical support from Extreme Networks. To locate information about various subjects in this guide, refer to the following table.

For...	Refer to...
Information on how to back up the existing software image before performing the upgrades.	Backing Up and Restoring the Image on page 13
Information on how to restore the previously backed up configuration on various platforms.	Backing Up and Restoring the Configuration on page 29
Information on various upgrade paths to upgrade the ExtremeWireless Convergence Software.	Upgrading the Wireless Convergence Software on page 38
Information on how to work with ExtremeWireless external storage devices.	Working with External Storage Devices on page 52
Information on how to connect to the ExtremeWireless console port to access the Rescue mode.	Using the Console Port on page 58
Information on how to perform the following system maintenance tasks: Changing the log level, setting a poll interval for checking the status of the Wireless APs (Health Checking), enabling and defining parameters for Syslog event reporting, forcing an immediate system shutdown with, or without reboot, and resetting the ExtremeWireless to its factory defaults.	Performing System Maintenance on page 60
Information on how to configure the ExtremeWireless utilities.	Using Controller Utilities on page 78
Information on how to recover the ExtremeWireless lost login password via the Rescue mode.	Recovering the Wireless Controller on page 92
Information on how to maintain various platforms.	Maintaining the Wireless Controller on page 95
Information on how to perform Wireless AP software maintenance.	Maintaining the Wireless AP Software on page 105
Information about performing wireless AP diagnostics using SSH.	Performing Wireless AP Diagnostics on page 110

2 Backing Up and Restoring the Image

Creating a Backup Image

When creating the image backup, the wireless controller makes an exact copy (snapshot) of the running image and saves it as a tgz file. Restoring the controller with a backup image restores the appliance to the exact state at the time backup was created.

A backup image can be created in two ways:

1. During upgrade of the image. Before installing the new image version, the upgrade process takes the backup of the running image. The backup image can be stored locally, on a flash drive (if present), or remotely on an FTP server.
2. From rescue mode using the menu driven commands. To do this, you have to enter rescue mode on startup. No service to clients is provided while you are in rescue mode. Again, the backup image can be stored on the local, flash (if flash is present) or an FTP server.

The only way to create a backup image independently of an upgrade is to run it from the rescue mode.

Backing Up and Restoring Characteristics by Controller Models

The following table describes the backup and restore capabilities and characteristics for all wireless controllers.

Table 3: Controller Backup and Restore Capabilities and Characteristics

FTP	Local	Flash
Requires management port connectivity	Administrator can upload/download local backup images provided they end in `'-rescue-user.tgz'`	USB device

Note
Backup file names must end in '`-rescue-user.tgz`'.

Note
Before you proceed with an FTP backup, ensure that the management port is configured correctly and connected to the network. To enter **Rescue** mode, you must connect to the serial console. The V2110 (MS Hyper-V platform) does not support flash functionality.

Backing Up Image File Name

The default file name used for backup image is: `<hostname/domain>-<platform>-<version>-rescue-user.tgz`

In order to distinguish multiple backup images, rename the file when saving to flash or FTP. If modification is required, you should prepend the custom text to the default image name.

Backing Up the Current Image During the Upgrade Process from the Wireless Assistant GUI

You must follow the procedures detailed in this section if you want to backup the current image via the Wireless Assistant GUI while upgrading the image. For more information on how to upgrade the image, see Upgrading Using the GUI on page 39.

Note
When you backup the current image, the license activation key and option keys are also backed up.

External Storage

The wireless controller models C35, C5210, C5215 and V2110. support only the USB storage device. If you select the Flash option to backup the existing image in these models, the image will be backed up on the USB device. You must ensure that the USB device is installed and mounted on the wireless controller. For more information, see Working with an External Storage Device on page 52.

To back up the existing software:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **Software Maintenance**. The EWC Software tab displays.

3 Select the **Backup system image to:** check box and choose the appropriate backup option.

To save the existing software image in local storage, select the **Local** option. The upgrade process will delete the previous backup image stored in local storage (if one exists).

To save the existing software image on the flash device, select the **Flash** option, and then type a file name for the backup image in the **Filename** box.

Note

The backup image file name is self generated when saved for both local or remote options (for example, EWC-<platform>10.01.0001-rescue-user.tgz). It is recommended that you maintain this format for the backup image file name. If you must customize the file name, prepend the customized file name to the original generated file name of the backup image.

To save the existing software image on a remote FTP server, select the **Remote** option, and then type the following:

FTP Server – The IP address of the FTP server that stores the image file.

User ID – The user ID used to log on to the FTP server.

Password – The corresponding password for the user ID.

Confirm – The corresponding password for the user ID to confirm the password was typed correctly.

Directory – The directory on the server in which the image file is stored.

Filename – The image file name, which must end with -rescue-user.tgz.

Backing Up the Current Image During Upgrade from the CLI

A backup image can be created during an upgrade from the CLI.

1 Check the backups present on the controller by running the **show upgrade** command.

```
EWC.extremenetworks.com# show upgrade
1: AC-MV-09.01.01.0123-1.rue
2: rue-08.31.01.0192-rescue-user.tgz
```

If you want a local backup file to be created, the upgrade process removes any previous *-rescue-user.tgz file. Optionally, you can remove any existing local backup file by running the no upgrade <filename> command.

```
EWC.extremenetworks.com# no upgrade 2
```

The command deletes the image with index 2, which, in this example, is vps-08.31.01.0192-rescue-user.tgz. You can also specify the full image name.

2 Upgrade the software with a backup image to local storage using the `upgrade ac new-image-name` **`bckto local`** command. During the upgrade process, a backup image with the default backup image name is created on the local storage:

```
upgrade ac AC-MV-09.01.01.0123-1.rue
 bckto local
```

3 Upgrade the software with a backup image to flash using the `upgrade ac new-image-name` **`bckto flash [filename]`** command.

```
upgrade ac AC-MV-09.01.01.0123-1.rue
 bckto flash
```

The command will upgrade and create a backup image with the default name on the flash drive.

You can also specify the custom name for the backup image.

```
upgrade ac AC-MV-09.01.01.0123-1.rue bckto flash backup-rescue-user.tgz
```

Note
To backup to flash, you must insert a flash drive before running the command.

4 If backing up the software to FTP, set up the FTP server credentials before running the upgrade by running the `upgrade_backup_dest ftp server ip user password dir file` command.

```
upgrade_backup_dest 192.168.4.10 test abc123 system/backups backup-rescue-user.tgz
```

The name specified for “upgrade_backup_dest” is used as the backup file name.

5 Start the upgrade by running the `upgrade ac new-image-name` **`bckto ftp`** command.

```
upgrade ac AC-MV-09.01.01.0123-1.rue bckto ftp
```

The command first makes a backup image of the running system preserved on the FTP server, then installs the selected upgrade image.

Backing Up the Current Image from Rescue Mode

You must follow the procedures in this section if you are backing up the current image.

You can also backup the current image via the Wireless Assistant GUI. For more information, see Backing Up the Current Image During the Upgrade Process from the Wireless Assistant GUI on page 14.

Note
When you backup the current image, the license activation key and option keys are also backed up.

To back up the existing current image:

1 Connect to the console port. Do not use the ESA ports or the Admin management port. For more information, see Using the Console Port on page 58.

2 Reboot the system.The following menu appears during the reboot process.

```
------------------------------------------------------------
Controller
Controller Rescue
------------------------------------------------------------
```

3 Select **Controller Rescue**, and then press **Enter**. The first repairFS script runs after the OS initialization.

Note
The above process may take several minutes. You must not reboot the system. After the filesystem check is completed, the main rescue menu is displayed.

```
Rescue Start-up Menu. Use with extreme caution.
1) Force System Recovery
2) Create System Backup Image
3) Display Backup Images
4) FTP Menu
5) Network Interface Menu
6) Manually run File System Check Utility (fsck)
7) Restore Backup Image directly from the FTP server
8) Authentication Service Management Menu
9) Flash Menu
R) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the selected
image (either backup or factory).
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice:
```

Note
If you want to create a backup image either on the wireless controller local drive or the USB device, follow Step 4 and skip the remaining steps. If you want to upload the backup image, follow steps 6 to 12.

4 Type 2 in the **Rescue** menu to create a backup image.

```
Your choice: 2
mounting rest of normal mode partitions...done
Do you want to create a system backup image to USB key? (Y/N)
```

5 Type Y to backup the image to a USB device or N to backup the image to the controller's local drive.

Note
Creating a system backup image to the controller's local drive will overwrite the existing backup image.

If you type Y, the following screen is displayed:

```
Please enter a backup filename:
```

a Enter the backup image filename ending in -rescue-user.tgz and press Enter.

The following screen is displayed.

```
Proceed with backup (Y/N):
```

b Type Y. The system backs up the image to the USB device.

```
Creating a Backup image is Complete!
 << Press any key to continue >>
```

If you type N, the following message is displayed:

```
Proceed with backup (Y/N):
```

Type Y. The system backs up the image.

```
--------------- Creating 'Normal' mode backup ------------
Please be patient. It may take a while. Do not reboot the machine
```

```
Mount the normal mode partitions:
mounting root partition...done.
mounting rest of normal mode partitions...done.
Creating a backup, please wait
Creating a Backup image is Complete!
Unmounting partitions...
done.
<< Press any key to continue >>
```

Note

You can also upload the backed up image to the FTP server. To upload the image to the FTP server, continue with the following procedures.

6 Enter Rescue mode.

a Type 5 in Rescue menu to enter the Network Interface menu.

b Type 2 in the Network Interface menu. The following screen is displayed.

```
Your choice: 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.210:255.255.255.0 192.168.1.1
```

Note

You can use the Network Interface menu options from 3 to 5 (IP, Netmask, and default gateway) one at a time.

7 Press **[Enter]**. The following screen is displayed.

```
ip is 192.168.1.210 netmask is 255.255.255.0
Configuring interface …
Setting up network interface … Done!
<< Press any key to continue >>
```

8 Test the interface.

a Type 6 in the Network Interface menu.

```
PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84)
bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=63 time=2.49 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=63 time=0.881 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=63 time=0.706 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=63 time=0.738 ms
64 bytes from 192.168.3.10: icmp_seq=5 ttl=63 time=0.707 ms
--- 192.168.3.10 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4031ms
rtt min/avg/max/mdev = 0.706/1.106/2.498/0.698 ms
<< Press any key to continue >>
```

Note

If the Network Interface is not configured properly, the following screen is displayed.

```
PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84) bytes of data.
--- 192.168.3.10 ping statistics ---
9 packets transmitted, 0 received, 100% loss, time 9038ms
 << Press any key to continue >>
```

9 Type B to return to the top menu. The following screen is displayed.

```
Your choice: B
Going back to the top menu...
```

10 Configure the FTP Settings.

a Type 4 in the Rescue menu to configure the FTP Settings. The following screen is displayed:

```
FTP MENU
--------------
1) Enter FTP Settings
2) Change FTP server IP address
3) Change FTP port
4) Change user name
5) Change password
6) Change FTP directory
7) Change file name
8) Display current FTP Settings
9) Display locally stored images
10) Download Image from FTP server
11) Upload Image onto the FTP server
12) Remove locally stored images
B) Return back to the top menu
Your choice:
```

b Type 1 to enter the FTP settings.

c Type 1 in the FTP menu. The following screen is displayed.

```
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&filename>
~port information is optional: the default value is 21~
Please enter ftp info:
```

d Type the name of the image to be uploaded, as part of the FTP settings. For example:

Please enter FTP info:

```
ftp://tester:123456@192.168.10.10:21/backup_dir/rue-rescue-user.tgz
```

Note

When you are uploading the backup image, the filename in the command syntax corresponds to the image that is being uploaded to the FTP server (filenames can be displayed by typing 9 in the FTP menu). When you are downloading the backup image, the filename in the command syntax corresponds to a file that is being downloaded from the FTP server.

11 Check the FTP settings.

a Type 8 in the FTP menu. The following screen is displayed.

```
Your choice: 8
Current Settings:
-----------------
FTP IP address: 192.168.10.10 port: 21
user name: tester
password: 123456
FTP directory: "backup_dir"
FTP file: "rue-rescue-user.tgzz"
<< Press any key to continue >>
```

b Confirm that the name of the file to be uploaded to the FTP server is correct.

12 If applicable, modify the FTP settings.

In the FTP menu, choose options from 2 to 7 to individually configure the FTP settings:

- FTP server's IP address
- FTP port
- User name
- Password
- FTP directory
- File Name

13 Upload the image on the FTP server:

a Type `11` in the FTP menu. The following screen is displayed:

```
Your choice: 11
Attempting to upload an image to the ftp server. Please be patient
Please verify at the ftp server that image has successfully been uploaded
<< Press any key to continue >>
```

Note

The minimum backup image size is approximately 250 MB.

You must have write permission for the FTP server and the specified FTP directory.

14 Confirm that the image is backed up.

```
Type 9 in the FTP menu. The following screen is displayed:
Your choice: 9
Currently Locally Stored Images:
--------------------------------
1 ) rue-rescue-user.tgz
2 ) AC-MV-09.01.01.0163-1.rue
<< Press any key to continue >>
```

Restoring the Backup Image from the GUI

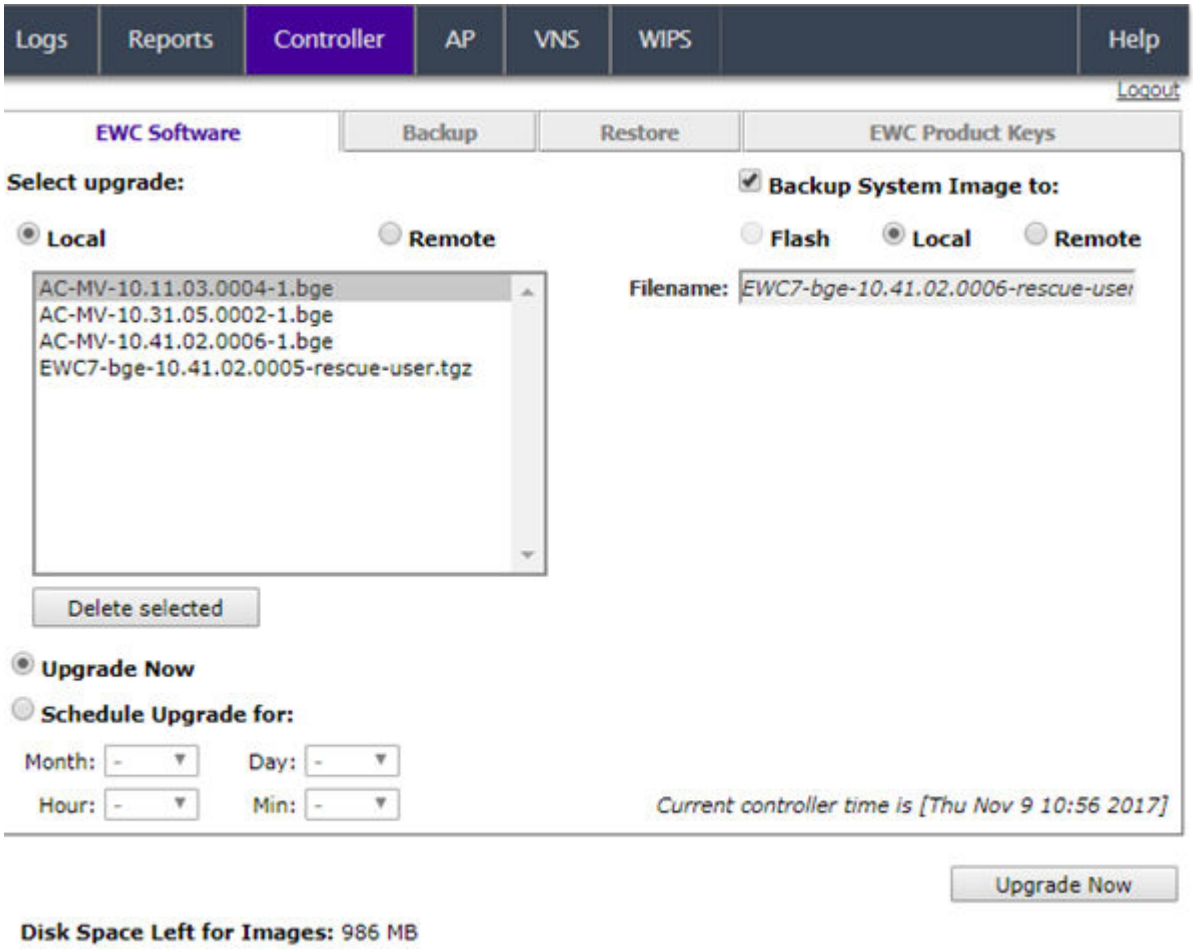
The following section describes how to restore the backup image using the GUI.

To restore the Wireless Controller Software:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **Software Maintenance**.

The **EWC Software** tab is displayed.



The list displays items that are available.

3 In the list, click the backup image you want to restore. The list displays all images available on the local disk or the flash card, if the flash card is mounted. Backup images have names ending in -rescue-user.tgz (see Backing Up Image File Name on page 14).

Note
The Local option must be cleared in the **Backup system image** to section.

4 To restore the image, click **Upgrade now**. A dialog is displayed informing you that the restore process requires rebooting the wireless controller.

Note
The Upgrade now parameter does not support IPv6 FTP.

5 Click **OK** to confirm the restore.

The Software Maintenance window is displayed.

The wireless controller reboots automatically.

Downloading a Backup Image from an FTP or SCP Server

You can choose to download a backup image from an FTP or SCP server for a restore. After it is downloaded, the system is restored in the same way as restoring from the local storage.

To download a backup image from an FTP or SCP Server for a restore:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 Select the **Remote option**, and then type the following:
   - **Protocol** – FTP or SCP.
   - **Server** – The server to retrieve the backup file from.

     Note
     The Server parameter supports both IPv4 and IPv6 addresses.

   - **User ID** – The user ID used to log into the server.
   - **Password** – The corresponding password for the user ID.
   - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
   - **Directory** – The directory on the server in which the backup file that is to be retrieved is stored.
   - **Filename** – The name of the image file to retrieve.
4 Click **Get Image now**. The image is downloaded and added to the list.

Note
SCP can only be used to download an image and cannot be used to start remote upgrade. The Upgrade now button is disabled when SCP is selected from the drop-down list.

Deleting a Backup Image That Is Available for Restore

To delete a backup image that is available for restore:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 To delete a backup image from the list, click the image in the list that you want to delete.
4 Click **Delete selected**.

   A dialog box is displayed. If correct, click **OK** to confirm the deletion.

Restoring Characteristics by Controller Models

Refer to Table 3 on page 14 for details on the backup and restoration capabilities and characteristics for each wireless controller.

Note
Before you proceed with an FTP restoration, ensure that the Management Port is configured correctly and connected to the network. You cannot enter Rescue mode without the management port's connectivity to the network.

Restoring the Backup Image from the CLI

The backup image can be restored using the CLI from local storage, flash and FTP server.

To restore the backup image from local storage and flash:

1 Locate the backup image from local storage and flash (if a flash device is inserted) using the `show upgrade` command. This command lists all upgrade files and backup image files.

```
EWC.extremenetworks.com# show upgrade
1: AC-MV-09.01.01.0123-1.rue
2: rue-08.31.01.0192-rescue-user.tgz
```

Note
Backup image files are identified based on the file name format.

2 Restore the backup image from the local storage or flash device using the `upgrade ac` *`backup-image-name`* command. Make sure that you do not specify a **`bckto local`** option.

```
EWC.extremenetworks.com# upgrade ac rue-08.31.01.0192-rescue-user.tgz
This command restores the system to the backup image selected.
```

To avoid typing the full image name, you can specify the image using the index returned by the show upgrade command.

For example, the command below will install the image with index 2 which, in this case, is

rue-08.31.01.0192-rescue-user.tgz.

```
EWC.extremenetworks.com# upgrade ac 2
```

To Restore the Local Image from the FTP or SCP Server:

3 Download the backup image from the FTP or SCP server by using the `copy upgrade` *`server | user | dir | backup-file-name`* [**`scp`** *`scp password`*] command.

In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the Wireless Appliance local drive:

```
EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-
MV-08.21.01.2222-1.rue scp TestPassword
```

4 Restore the backup image by using the `upgrade ac` *`new-image-name`* command.

```
EWC.extremenetworks.com# upgrade ac rue-08.31.01.0192-rescue-user.tgz
```

Restoring the Backup Image from Rescue Mode

To restore the backup image from rescue mode:

1 Connect to the console port. Do not use the ESA ports or the Admin management port. For more information, see Using the Console Port on page 58.

2 Reboot the system. The following menu is displayed during the reboot process:

```
------------------------------------------------------------
Controller
Controller rescue
------------------------------------------------------------
```

3 Use your cursor to highlight **Controller rescue**, and then press **[Enter]** to enter Rescue mode.

The following menu is displayed.

```
1) Force System Recovery
2) Create System Backup Image
3) Display Backup Images
4) FTP Menu
5) Network Interface Menu
6) Manually run File System Check Utility (fsck)
7) Restore Backup Image directly from the FTP server
8) Authentication Service Management Menu
9) Flash Menu
R) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the selected
image (either backup or factory).
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice:
```

4 Do one of the following:

- If the backup image was backed up to the local drive of the ExtremeWireless Appliance, restore from the local drive.
- If the backup image was backed up to a remote FTP server, restore from a remote FTP server.
- If a USB device with the backup image on it is mounted on the ExtremeWireless Appliance, restore from the USB device.

Restoring from the Local Drive

To restore from the local drive:

1 On the **Rescue** menu, type `1`.

The list of backup images on the local drive of the wireless controller are displayed.

```
Currently Stored Images
-----------------------
1) AC-MV-09.01.01.0123-1.ruevps
2) rue-08.31.01.0192-rescue-user.tgz
B) Abort and go back to previous Menu
Please select which image to use for restoring:
```

Backup image names end in `-rescue-user.tgz` (see Backing Up Image File Name on page 14). Be careful not to select the upgrade image (AC-MV-09.01.01.0123-1.rue) when the backup image is needed.

Restoring to the upgrade image will restore the system to factory defaults and lose all of the configuration (see Restoring to Factory Default on page 27).

2 Type the sequence number of the backup image that you want to restore.

The following message is displayed:

```
Selected Restore Image is: rue-08.31.01.0192-rescue-user.tgz
This procedure is irreversible, do you wish to continue (Y/N)?
```

3 Type `Y`.

The wireless controller initiates the recovery process.

```
Performing System recovery, this may take a while...
Cleaning out normal mode partitions...
Cleaning Completed.
Mount normal mode main partition
Mounting rest of normal mode partitions...done.
Restoring from the backup image...
Restoration Completed!
Unmount normal mode partitions
System Recovery Complete!
Reboot the system for changes to take effect.
Proceed with reboot (y/n):
```

4 Type `y`.

The wireless controller will reboot. After the reboot, the wireless controller restores the backed up image with its original configuration.

Restoring from a Remote FTP Server

To restore from a remote FTP server:

1 On the **Rescue** menu, type `5`.

The following menu is displayed:

```
1) Display Current Rescue Interface Info
2) Enter Interface Information
3) Change default gateway
4) Test interface by ICMP (ping)
B) Return back to the top menu
```

2 Configure the Network Interface. Type in the Network Interface menu, and then type the following:

- IP address of your wireless controller management port
- IP mask
- IP address of Gateway

```
Your choice> 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.201:255.255.255.0 192.168.1.1
Configuring interface ...
Setting up network interface ...Done!
```

3 Type `B` to return to the top menu.

4 Type `4` in the top menu to configure the FTP settings.

The **FTP** menu is displayed.

```
1) Enter FTP Settings
2) Change FTP server IP address
3) Change FTP port
4) Change user name
5) Change password
6) Change FTP directory
7) Change file name
8) Display current FTP settings
9) Display locally stored images
10) Download image from FTP server
```

```
11) Upload image onto the FTP server
12) Remove locally stored images
B) Return back to the top menu
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&file>
~port information is optional: the default value is 21~
Please enter ftp info:
```

5 Type the FTP information.

```
ftp://administrator:abc123@192.168.4.181/tester/v6/backup-rescue-user.tgz
```

6 Type `B` to return to the top menu.

```
1) Force system recovery
2) Create System Backup Image
3) Display Backup Images
4) FTP Menu
5) Network Interface Menu
6) Manually run File System Check Utility (fsck)
7) Restore Backup Image Directly From The FTP Server
8) Authentication Service Management Menu
9) Flash Menu
R) Reboot
Your choice:
```

7 Type `7`.

The following message is displayed:

```
Your choice: 7
Make sure correct information is entered for Interface and FTP settings.
IP: 192.168.4.191 netmask 255.255.255.0 gateway:
FTP Settings: IP 192.168.4.181, port 21, user: administrator, password: abc123,
directory: /tester/v6/, file backup-rescue-user.tgz
This procedure is irreversible, do you wish to continue (Y/N)?
```

8 Type `Y`.

The wireless controller initiates the recovery process.

9 Reboot the wireless controller.

After the reboot, the wireless controller restores the backed up image with its original configuration.

Restoring the Rescue Image

The rescue image resides on the wireless controller's hard disk in a separate partition called the rescue partition; the running software image is stored in the normal mode partition.

You can restore the rescue partition in the rare event that it becomes unavailable or corrupted (for example, because of a hardware disk hardware error or a power failure during upgrade). To restore the rescue partition, you must obtain a healthy rescue image and install it on the wireless controller.

A healthy rescue image is available from one of the following locations:

- The normal mode partition. A locally saved rescue image is delivered as part of the upgrade image and saved on the normal mode partition during the upgrade process.
- The Extreme Networks repository site. On the Extreme Networks repository site, one rescue image exists for each controller platform. The following table lists the file extension associated with each of the controller platforms. The file extension for the rescue image begins with the letter r to identify the file as a rescue image.

Table 4: Rescue Image File Naming Conventions

Wireless Appliance Model	Rescue File Extension
C5210	.rrue
C5215	.rice
C35	.rcwe
V2110 (VmWare platform)	.rbge
V2110 (MS Hyper-V platform)	.rize

Note

Use the restore procedure in an emergency only when the rescue partition is not accessible. Restore commands are available in the CLI to administrators only; these commands are not listed when you enter the help command.

To restore the rescue image:

1 Log into the CLI as administrator from the console or by using SSH.

2 List the locally saved rescue images by entering the command:

```
EWC.extremenetworks.com# show restore-rescue
1: rescue.rrue
```

If a rescue image exists, go to step 3; if no rescue images exist, skip to step 5.

3 To restore the rescue partition using the locally saved rescue image, enter the command: `restore-rescue local` *`imagefilename`*

For example, to restore from the locally saved rescue image, rescue.rrue, enter the command:

```
EWC.extremenetworks.com# restore-rescue local rescue.rrue
```

4 To restore the rescue partition from any repository site:

a Download the appropriate rescue image to the locally accessible FTP server. Make sure that the rescue image you download matches the main image (platform and version). Table 4 on page 27 lists the platforms and the corresponding rescue image file extensions.

b Download the rescue image from the FTP server and install it into the controller by entering the following command:

`restore-rescue ftp` *`serverip`* `|` *`user`* `|` *`password`* `|` *`dir`* `|` *`imagefilename`*

For example, to download the rescue image for the C5210 model controller from the FTP site and, as the user admin with the password abc123, install the rescue image, AC-MV-09.01.01.0183-1.rrue, into the store directory, enter the following command:

```
EWC.extremenetworks.com# restore-rescue ftp 1.1.1.1 admin abc123 store/ AC-
MV-09.01.01.0183-1.rrue
```

Restoring to Factory Default

To restore the system to a particular image with factory defaults, restore the system from rescue mode with the upgrade image as the restore image.

For example, if the system needs to be restored to factory default image V10.01, enter the rescue mode, follow the procedure to restore the backup image (as explained in Restoring the Backup Image from

Rescue Mode on page 24) and, instead of selecting the backup image, provide the upgrade image V10.01 (local, flash or download from FTP), and perform the restore. The system is restored to the V10.01 with factory default values.

Caution

Be aware that restoring a system to factory defaults means that the configuration is lost including the IP connectivity, certificates, and licenses. Restoring to factory default is possible only from rescue mode.

3 Backing Up and Restoring the Configuration

Backing Up the Wireless Controller Configuration

Backing up the wireless controller database and creating a software package backup are two different processes. Backing up the wireless database only involves creating a backup of specific content in the wireless database. For example, you can choose to backup configuration, logs, or audit information. To create a backup image of your operating system, use the backup and restore functionality of the system.

Note
Configuration data for the wireless controller is saved in NVRAM (non-volatile memory).

When you backup the wireless database, you can choose to do the following:

- Back up the wireless database now
- Upload a backup to an FTP or SCP server or flash
- Schedule when a backup occurs
- Schedule a backup and copy it to an FTP or SCP server or flash

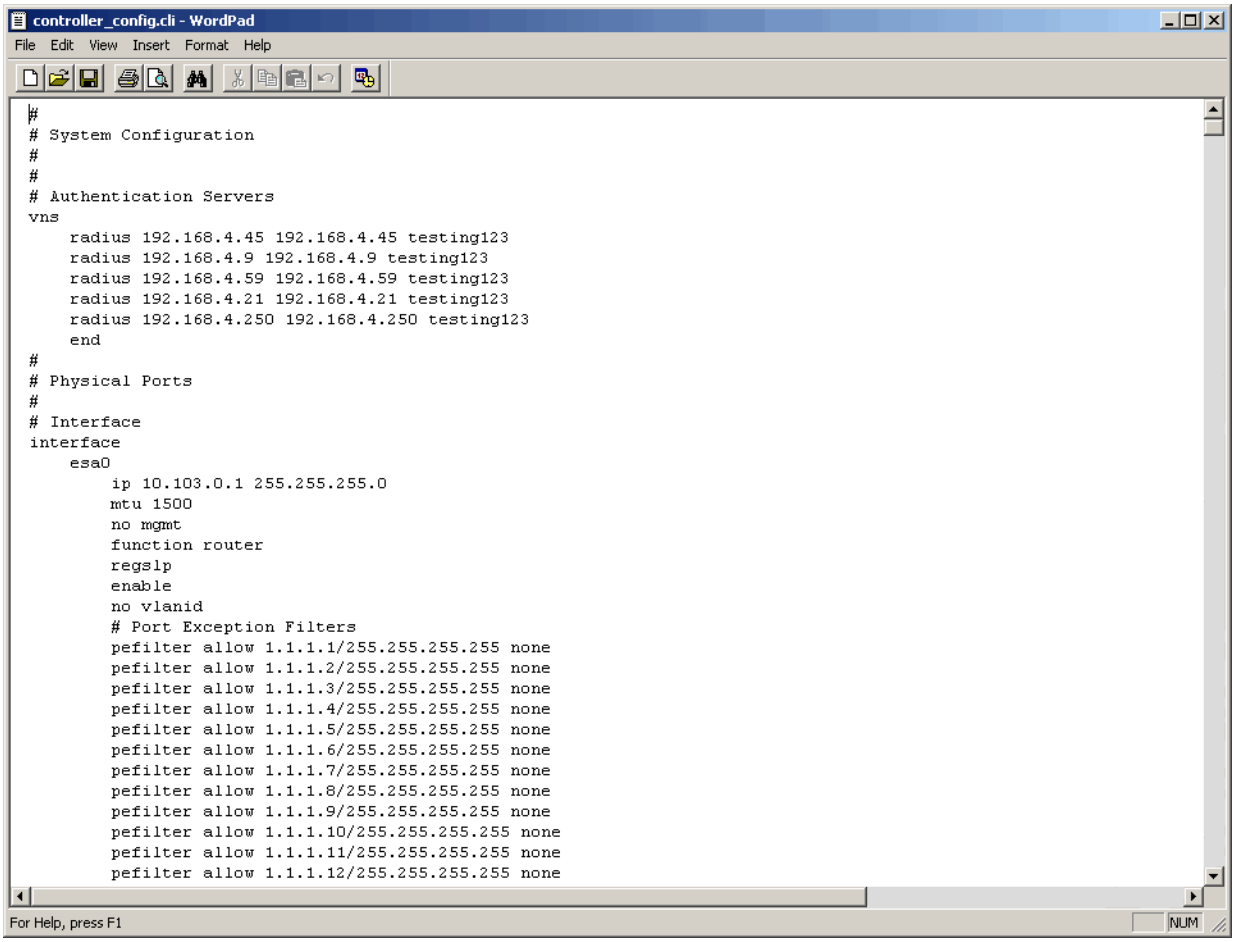
Note
V2110 (MS Hyper-V platform) does not support flash functionality.

Working with a Portable and Text Editable Backup

When the controller database backup is processed, a .zip file is created. The contents of the .zip file will vary depending on what type of database backup you process.

If you process a configuration information backup, one of the files included in the .zip file is a .cli file. When the .zip file is stored on a server or flash, the .zip file contents can be extracted and the .cli file can be edited.

This editable .cli file when imported to the controller will reproduce the identical configuration from which the original configuration was generated. This editable .cli file provides an easy method for replicating identical configurations on multiple controllers. Below is a sample .cli file. The .cli file contains CLI commands, which will replicate the configuration that the backup was based on when the file is imported.



For information on how to import a backup onto the controller, see Restoring the Wireless Controller Configuration on page 34.

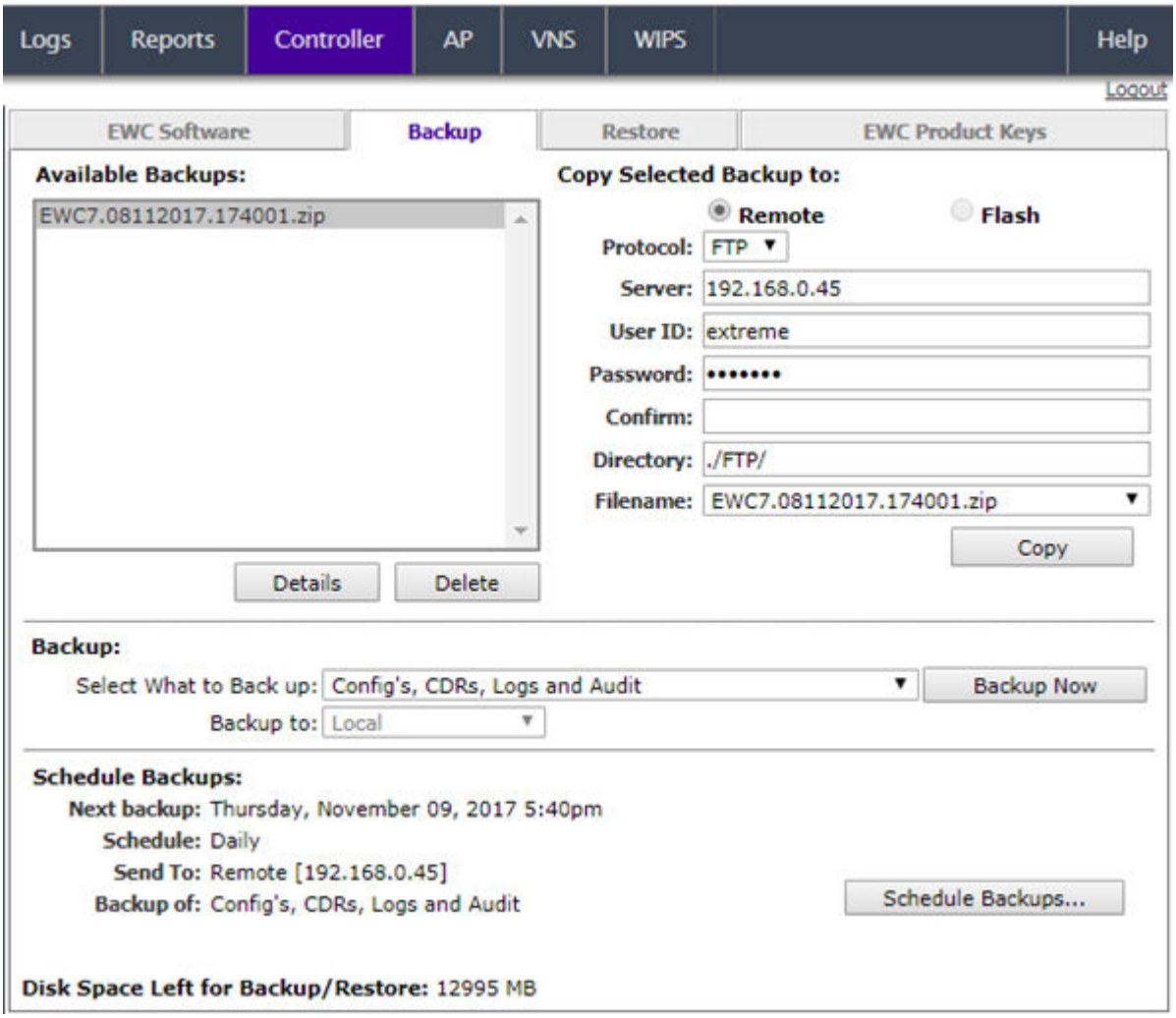
Note

Backup configurations saved in local storage are deleted during the upgrade. To preserve your backed up configurations, upload them to an external FTP or SCP server, or flash before performing the upgrade.

To back up the wireless database using the GUI:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.

3 Click the **Backup** tab.



The **Available Backups** list displays items that have already been backed up and are available.

4 In the **Backup** section:

- click an item from the **Select what to backup** drop-down list.
- select Local or Flash from the **Backup to** drop-down list.

5 To launch the backup of the selected items, click **Backup Now**.

The Software Maintenance window is displayed, providing the status and results of the backup.

Uploading a Backup to a Server

You can upload an existing backup file to a server using FTP (file transfer protocol) or SCP (secure copy protocol).

To upload an existing backup to a server using the GUI:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **Software Maintenance**.

3 Click the **Backup** tab.
4 Select **Remote** in **Copy Selected Backup to**.
5 To upload a backup, do the following:
   - **Protocol** – Click the file transfer protocol you want to use to upload the backup file, SCP or FTP.
   - **Server** – Type the IP address of the server where the backup will be uploaded.
   - **User ID** – Type the user ID used to log into the server.
   - **Password** – Type the corresponding password for the user ID.
   - **Confirm** – Type the corresponding password for the user ID to confirm it was typed correctly.
   - **Directory** – Type the directory on the server where the backup file will be stored.
6 In the **Filename** drop-down list, click the backup you want to upload.
7 Click **Copy**.
   The Software Maintenance window is displayed, providing the status and results of the operation.

Copying a Local Backup to Flash

You can copy an existing local backup file to a flash drive.

To copy an existing local backup to a flash using the GUI:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 Click the Backup tab.
4 Select **Flash** in **Copy Selected Backup to**. Flash has to be mounted for this.
5 In the Filename drop-down list, select the local backup you want to copy.
6 Click **Copy**. The Software Maintenance window is displayed, providing the status and results of the operation.
7 The backup copy located on flash is going to be displayed in Available Backups list as well.
   To copy an existing local backup to a flash using the CLI:
8 Log into the system using SSH or console.
9 Transfer the backup file from the local storage to a flash using the following command:
   `copy configuration (to-local | to-flash | to-remote server user dir [ftp password | scp password]) (from-local filename |number | from-flash filename|number | from-remote server user dir file [ftp password | scp password])`

   For example, to transfer the backup file BAK.03122009.071327.zip from local storage to a flash:

```
EWC.extremenetworks.com#copy configuration to-flash from-local BAK.03122009.071327.zip
```

   To see all backup files stored locally and on flash, use the show export command.

```
EWC.extremenetworks.com#show export
1: BAK.03122009.071327.zip
2: BAK.03122009.071327.zip(flash)
```

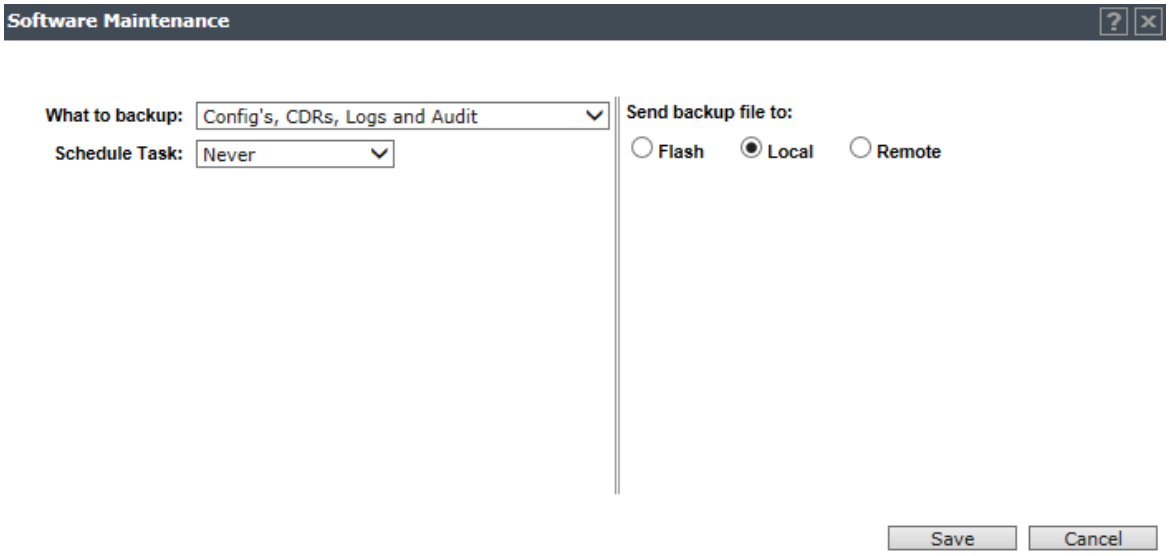
Scheduling a Backup

When you schedule a backup, you can choose to upload the backup to a server, have the scheduled backup saved on your system or flash drive.

To schedule a backup:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 Click the **Backup** tab.
4 Click **Schedule Backups**.

The **Software Maintenance** screen is displayed.



5 In the **What to backup** drop-down list, click what you want to backup:

- Configs, CDRs, Logs and Audit
- Configurations only
- CDRs only
- Logs only
- Audit only

6 In the **Schedule task** drop-down list, click the frequency of the backup:

- **Daily** – Click the **Start Time** and Recurrence for the backup.
- **Weekly** – Click the **Start Time** and Recurrence for the backup.
- **Monthly** – Click the **Start Time** and Recurrence for the backup.
- **Never** – Click to disable schedule backup.

7 Under **Send backup file to**, select Flash, Local, or Remote.

8 If you select **Remote** (scheduling a backup to a remote server), specify a server to where the scheduled backup will be copied to. Do the following:

- **Protocol** – Click the file transfer protocol you want to use to upload the backup file, SCP or FTP.
- **Server** – Type the IP address of the server to where the scheduled backup will be copied to.

Note
The Server parameter supports both IPv4 and IPv6 addresses.

- **User ID** – Type the user ID used to log into the server.
- **Password** – Type the corresponding password for the user ID.
- **Confirm** – Type the corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – Type the directory on the server where the image file will be stored.

9 To save your changes, click **Save**.

Deleting a Backup

You can delete a backup if it is no longer needed on your system or flash drive.

To delete a backup using the GUI:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 Click the **Backup** tab.
4 In the **Available Backups** list, click the backup you want to delete.
5 Click **Delete**.
6 In the dialog box that is displayed, click **OK** to confirm the deletion.

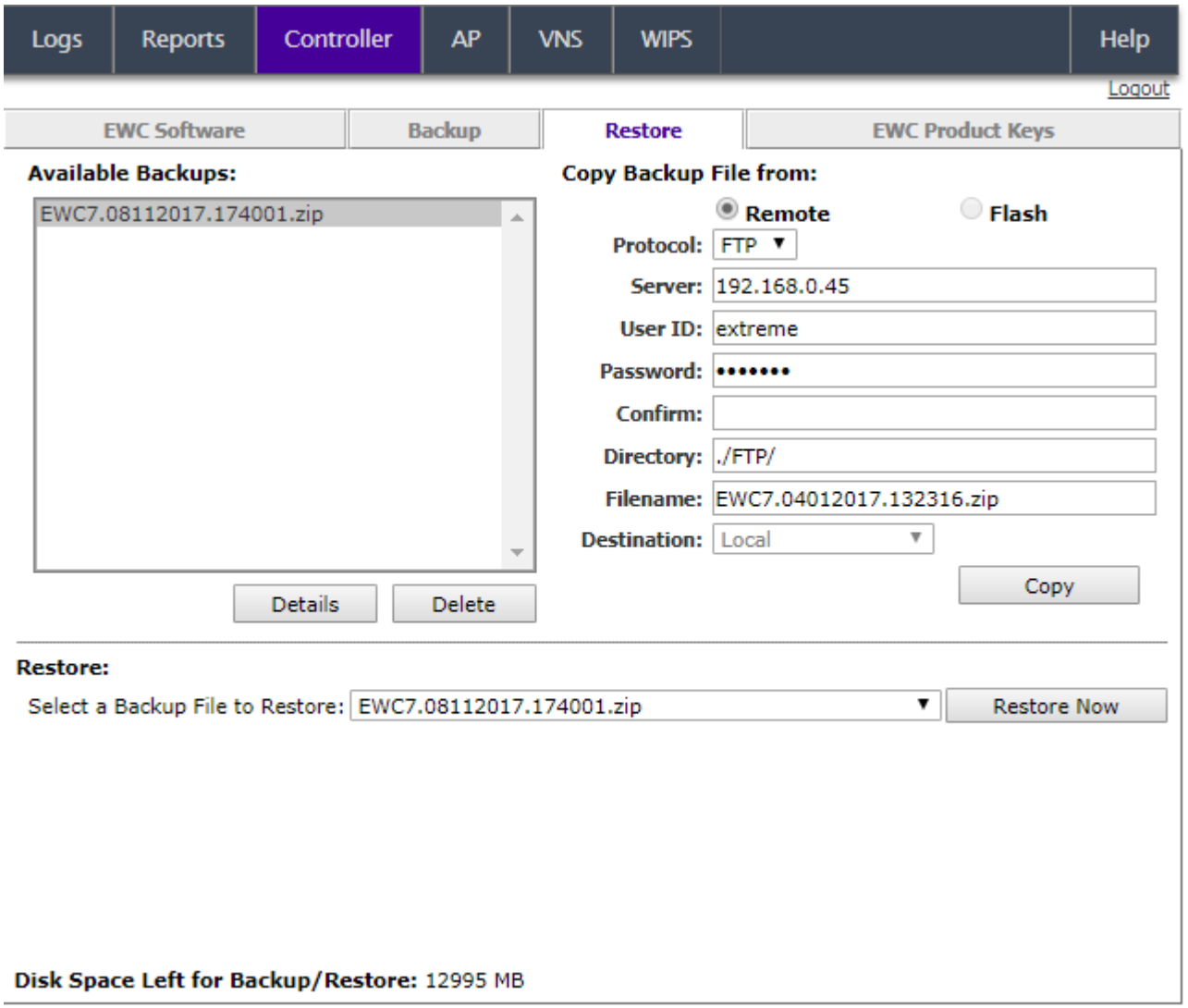
The Software Maintenance window is displayed, providing the status and results of the deletion.

Restoring the Wireless Controller Configuration

To restore the configuration using the GUI:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 Click the **Restore** tab.
4 The **Available Backups** list displays available backup files for restore.
5 In the **Restore** section, select a backup to restore.
6 To launch the restore of the selected item, click **Restore Now**.

7 The Software Maintenance window is displayed, providing the status and results of the restore.



To restore the configuration using the CLI:

8 Log into the CLI using SSH or console.

9 View all backup files in local storage by using the `show import` command.

```
EWC.extremenetworks.com#show import
1: EWC.03122009.071327.zip
```

10 Restore the configuration by using the `import` *`filename|number`* command.

For example, to restore the backup file shown in the example under step 1:

```
EWC.extremenetworks.com#import EWC.03122009.071327.zip
```

To avoid typing the full name of the backup file, you can use the index number returned by the show import command.

The restore can be run directly from an imported file stored on flash. In this case, the string "(flash)" must be suffixed to the end of the specified file name.

```
EWC.extremenetworks.com#import 1
```

The command will restore the controller configuration to the configuration in the backup file.

Downloading a Backup File

You can download an existing backup file from a server using FTP (file transfer protocol) or SCP (secure copy protocol), or from flash to local storage.

To download an existing backup from a server using the GUI:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 Click the **Restore** tab.
4 Select a Remote under **Copy Backup File From**.
5 Enter values for the following:
- Protocol — Select the file transfer protocol you want to use to download the backup file (SCP or FTP).
- Server — Type the IP address of the server from which the backup will be downloaded.

Note
The Server parameter supports both IPv4 and IPv6 addresses.

- **User ID** — Type the user ID used to log into the server.
- **Password** — Type the corresponding password for the user ID.
- **Confirm** — Type the corresponding password for the user ID to confirm it was typed correctly.
- **Directory** — Type the directory on the server where the backup file is stored.
- **Filename** — Enter the name of the backup file you want to download.
- **Destination** — Define whether a file is transferred to local or flash from a remote server.

6 Click **Copy**.

The Software Maintenance window is displayed, providing the status and results of the download.

To download an existing backup from a server using the CLI:

7 Log into the system using SSH or console.
8 Download the backup file from the FTP or SCP server using the following command:
`EWC.extremenetworks.com#copy configuration (to-local | to-flash | to-remote serveruser dir [ftp password | scp password]) (from-local filename|number | from-flash filename|number | from-remote server user dir file [ftp password | scp password])`

For example, to download the backup file EWC.03122009.071327.zip locally from an SCP server:

```
EWC.extremenetworks.com#copy configuration to-local from-remote 192.168.3.10 test
conf_bak_dir
EWC.03122009.071327.zip scp abc123
```

The command will download the file and store in the local storage.

To see all backup files stored in the local storage, use the show import command.

```
EWC.extremenetworks.com#show import
1: EWC.03122009.071327.zip
```

To copy an existing backup from a flash to local storage using the GUI:

9 From the top menu, click **Controller**.

The Wireless Controller Configuration screen is displayed.

10 From the left pane, click **Administration** > **Software Maintenance**.

The EWC Software tab is displayed.

11 Click the **Restore** tab.

12 Select a source Flash under **Copy Backup File From**. Flash has to be mounted for this.

13 In the **Filename** drop-down list, click the backup you want to transfer.

14 Click **Copy**.

The Software Maintenance window is displayed, providing the status and results of the operation. The local backup copy is going to be displayed in Available Backups list as well.

To copy an existing backup from a flash to local storage using the CLI:

15 Log into the system using SSH or console.

16 Copy the backup file from the local storage to flash using the following command:
`EWC.extremenetworks.com#copy configuration (to-local | to-flash | to-remote serveruser dir [ftp password | scp password]) (from-local filename|number | from-flash filename|number | from-remote server user dir file [ftp password | scp password])`

For example, to copy the backup file BAK.03122009.071327.zip locally from a flash:

```
EWC.extremenetworks.com#copy configuration to-local from-flash BAK.03122009.071327.zip
```

To see all backup files stored locally and on flash, use the show import command.

```
EWC.extremenetworks.com#show import
1: BAK.03122009.071327.zip
2: BAK.03122009.071327.zip(flash)
```

4 Upgrading the Wireless Convergence Software

Upgrading Process

During the upgrade process, the upgrade program does the following:

- Uninstalls the old version
- Installs the new version
- Preserves and migrates the configuration to the new version

Note
V2110 (MS Hyper-V platform) does not support flash functionality.

Note
When you upgrade the Wireless Controller Software, the previous SSL Configuration file is replaced by a new one. Consequently, the manual edits that were made in the previous SSL Configuration file are lost. If you have done manual edits to the SSL configuration file to install certificates for Captive Portal on the virtual interfaces, it is suggested to use EWC Captive Portal Certificate Configuration instead.

Upgrading to V10

If you are running a software version earlier than V9.01, you must first upgrade to V9 before upgrading to V10.

Upgrade Path Matrix to V9

Use the following matrix to determine the upgrade path to required version V9 that is appropriate for your wireless controller and the software running on it.

Table 5: Upgrade Matrix

Platform	From	To
V2110	V8.01, V8.11, V8.21, V8.31, V8.32, V9.01, V9.12, V9.15	V9.21
C5210	V8.21, V8.31, V8.32, V9.01, V9.12, V9.15	V9.21

For information about migrating from one platform to another, see Migrating the Platform Configuration on page 47.

For information about upgrading controllers operating in "availability" mode, see Upgrading Two Controllers in Availability Mode on page 49.

Upgrading the Image File Name

The format of the upgrade image file name is: `AC-MV-<version>-<revision>.<platf>`

- version — version number (for example 08.00.00.0174)
- revision — software release number
- platf — is one of the values from the table below

Table 6: Upgrade File Name Extensions

Wireless Appliance models	Platform
ExtremeWireless Appliance C5210	.rue
ExtremeWireless Appliance C5215	.ice
ExtremeWireless Appliance C35	.cwe
ExtremeWireless Virtual Appliance V2110 (VmWare platform)	.bge
ExtremeWireless Virtual Appliance V2110 (MS Hyper-V platform)	.ize

Upgrading Using the GUI

Use the following procedure if you are upgrading using the GUI.

Note

You should always backup the existing software image during the upgrade process. Backing up provides you the option of restoring your wireless controller to its previous configuration. For more information, see Restoring the Backup Image from the GUI on page 20.

The wireless software provides two upgrade options:

- **Local** – Upgrades the wireless software by using the image file that is located either on the local drive or USB device. This is the preferred method of upgrade.

Note

Before starting the local upgrade, the image file needs to be downloaded to the local drive or a flash device has to be provided with the image file.

- **Remote** – Upgrades the wireless software by using an image file that is located on an external FTP server. The upgrade program downloads the image file from the FTP server, unpacks it and installs it directly on the system without retaining a local copy of the image file.

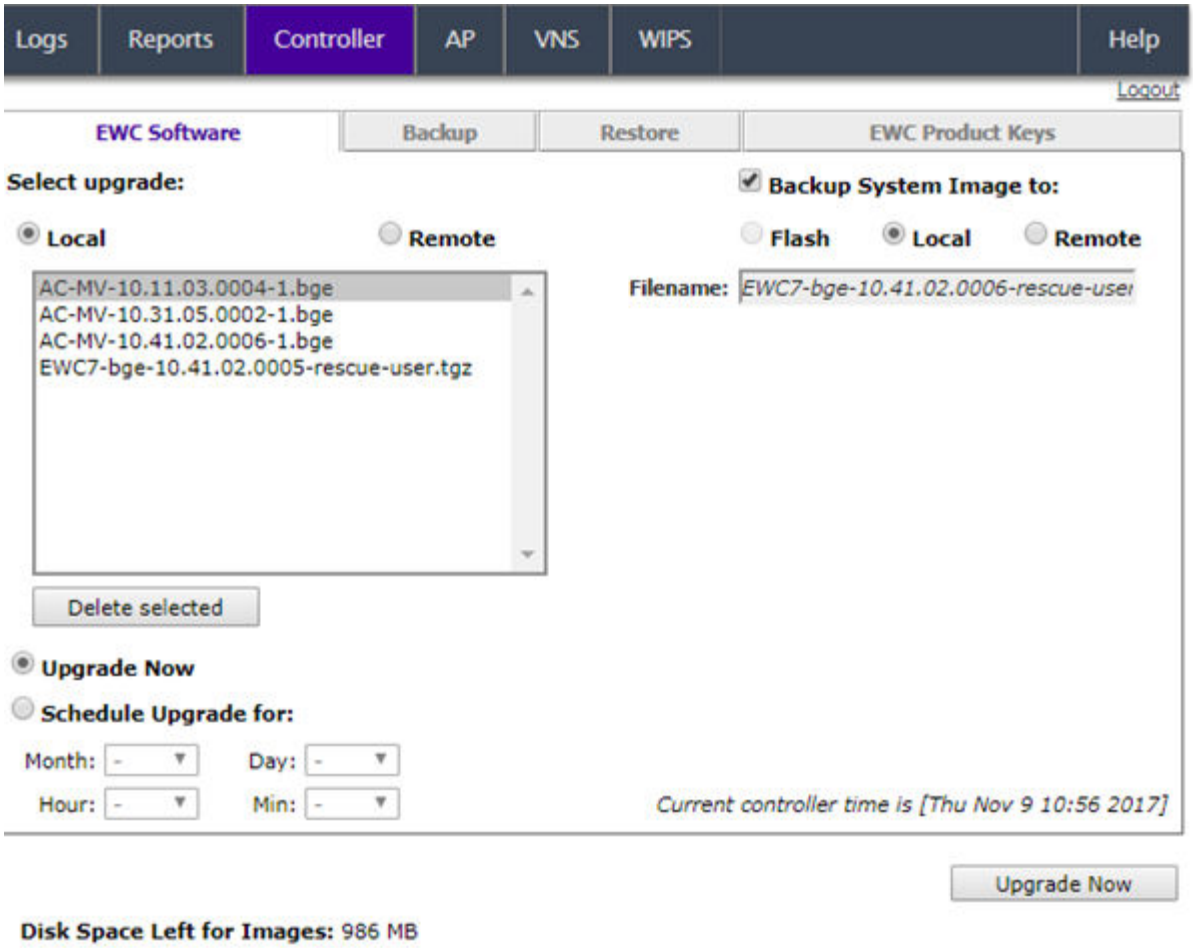
Note
The Wireless Assistant GUI displays Remote as the upgrade option for upgrade from a remote FTP server.

Upgrading Locally

When you upgrade locally, the upgrade program upgrades the wireless software by using the image file that is located either on the local drive or USB device.

To perform a local upgrade of the wireless software:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.



3 Select **Local**, and then click the image file you want to use from the list of upgrade files.

Note
Multiple images may be listed: image files on the local drive, image files on the flash device (if a flash device is inserted), and image backup files (end with -rescue-user.tgz) if they exist on the local drive or flash device. Select the desired image. Image files use the AC-MV-<version>-<revision>.<platf> name format, as explained in Upgrading the Image File Name on page 39.

Note
Regardless of whether the upgrade image file is on the local drive or flash device, the wireless controller displays it in the list of upgrade files.

Caution
You should always backup the existing software image during the upgrade process. Backing up provides you the option of restoring your wireless controller to its previous configuration if needed. For more information, see Restoring the Backup Image from the GUI on page 20.

4 Select one of the following upgrade options:

- To schedule a software upgrade, select the Schedule upgrade for option. The earliest you can schedule an upgrade is 5 minutes into the future.

  Use the Month, Day, Hour, and Minute drop-down lists to schedule the upgrade and then click **Schedule upgrade**.

  Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. The **EWC Software** tab fields gray out.

  Note
  A scheduled upgrade is not a recurring event. The wireless controller allows only one **Scheduled upgrade** to be configured at a time.

- To upgrade the software immediately, select the **Upgrade now** option.

  Click the **Upgrade now** button.

  Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. A window displays the upgrade status.

  The wireless controller reboots after the upgrade process is completed.

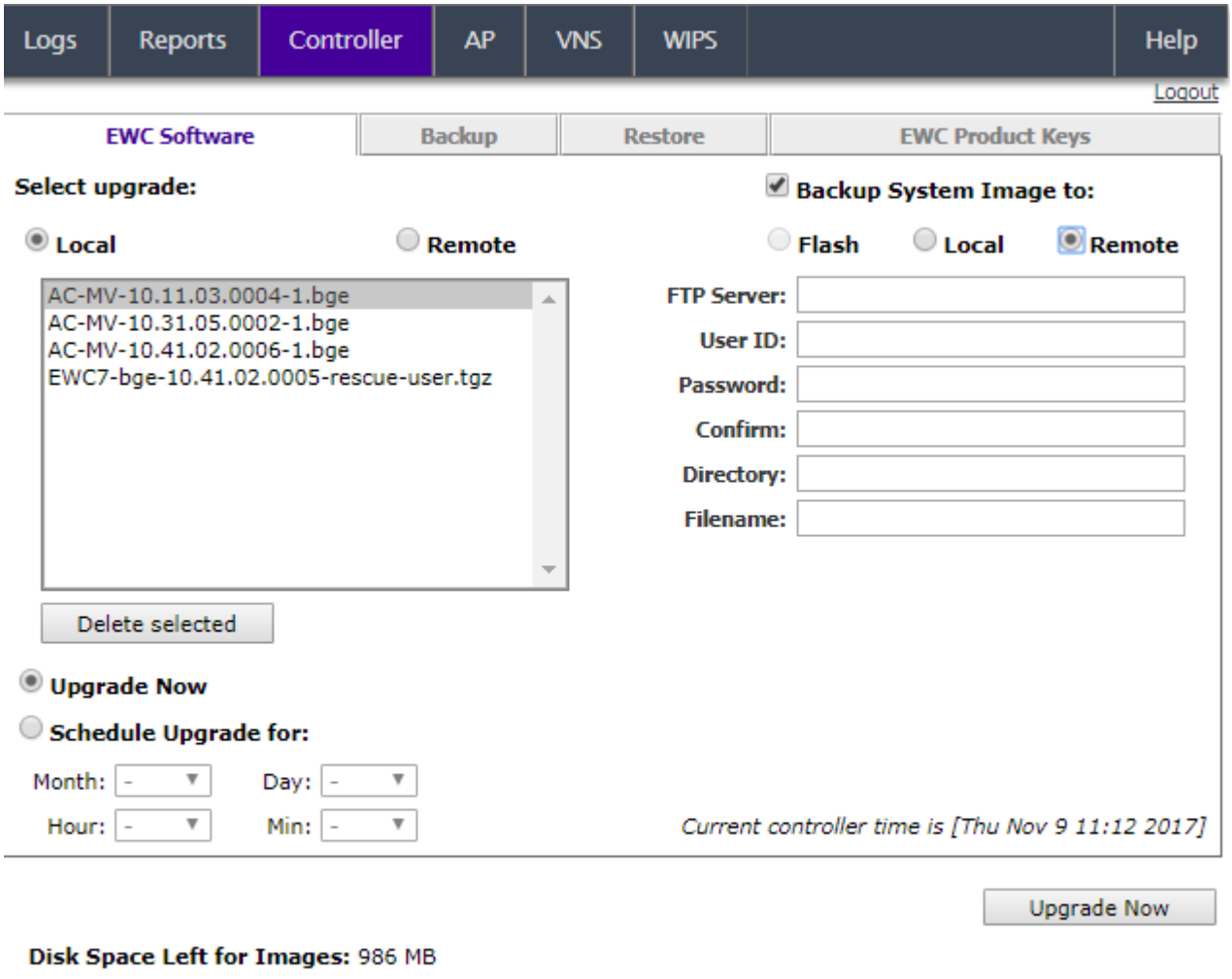
Downloading the Remote Image File to the Local Drive or USB Device

To download the Remote Image File to the local drive or USB device:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.

3 Select **Remote**.

The FTP/SCP server boxes are displayed.



4 Type the following:

- **Protocol** – FTP or SCP.
- **Server** – The IP address of the server to retrieve the image file from.
- **User ID** – The user ID used to log into the server.
- **Password** – The password for the user ID.
- **Confirm** – The password to log on to the server. This field is to confirm you have typed the correct password.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.

5 In the **Destination** drop-down list, click **Local** or **Flash** to specify where the image is downloaded to.

6 Click **Get Image now**.

The **Download Image** window is displayed, providing the status and results of the download. The image is downloaded onto your system and added to the **Select upgrade** list.

Note
SCP can only be used to download an image and cannot be used to start remote upgrade. The Upgrade now button is disabled when SCP is selected from the drop-down list.

Upgrading Remotely

When you upgrade the wireless software remotely, the upgrade program upgrades the software image by using the image file that is located on an external FTP server. The upgrade program downloads the image file from the FTP server, unpacks it and installs it directly on the system without retaining a local copy of the image file. The Wireless Assistant GUI displays Remote as the upgrade option for upgrade from a remote FTP server with FTP selected as the protocol.

Note
SCP can only be used to download an image and cannot be used to start remote upgrade. The Upgrade now button is disabled when SCP is selected from the drop-down list.

Caution
You should always backup the existing software image during the upgrade process. Backing up provides you the option of restoring your controller to its previous configuration if needed. For more information, see Restoring the Backup Image from the GUI on page 20.

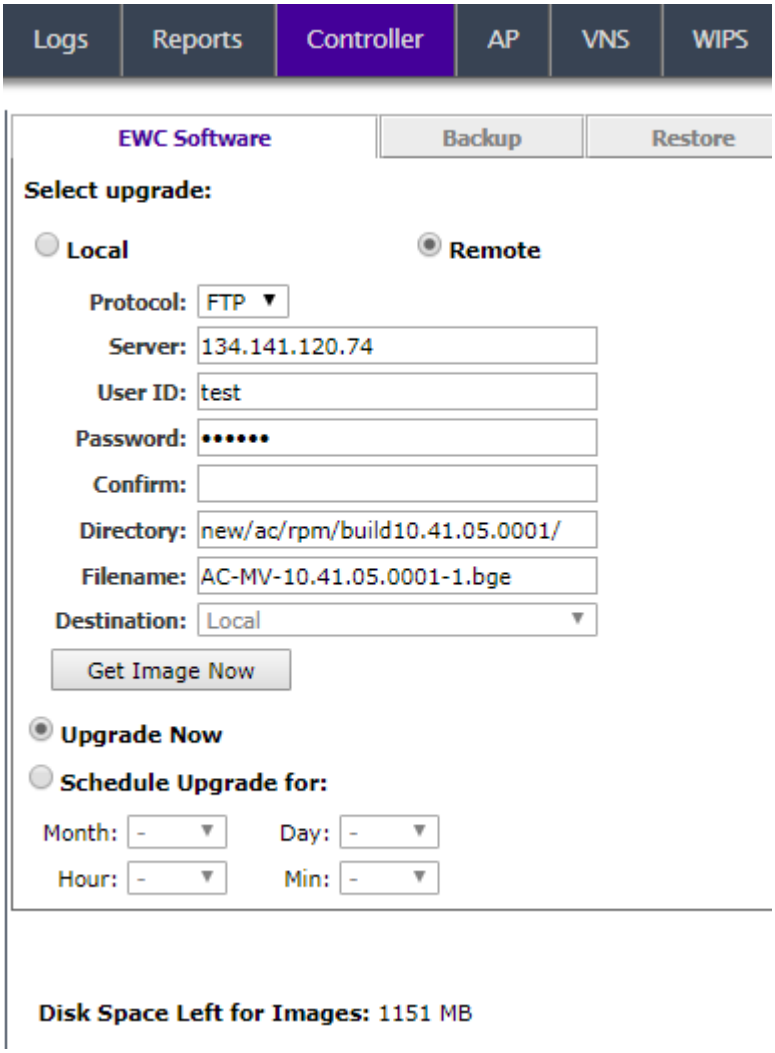
Running the Upgrade from the FTP Server

To run the upgrade from the FTP Server via the Wireless Assistant GUI:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.

3 Select **Remote**.

The FTP server boxes are displayed.



4 Type the following:

- **Protocol** – FTP.
- **Server** – The IP address of the FTP server to retrieve the image file from.
- **User ID** – The user ID used to log into the FTP server.
- **Password** – The password for the user ID.
- **Confirm** – The password to log on to the FTP server. This field is to confirm you have typed the correct password.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.

5 To schedule a software upgrade, select the **Schedule upgrade for** option. The earliest you can schedule an upgrade is five minutes into the future.

   a Use the Month, Day, Hour, and Minute drop-down lists to schedule the upgrade.

   b Click **Schedule upgrade**.

   c Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. The **EWC Software** tab fields gray out.

Note
A scheduled upgrade is not a recurring event. The wireless controller only allows one scheduled upgrade to be configured at a time.

6 To upgrade the software immediately, select the **Upgrade now** option.

   a Click the **Upgrade now** button.

   b Review the upgrade settings in the dialog box, and then click **OK** to confirm the upgrade settings. A window displays the upgrade status.

The wireless controller reboots after the upgrade process is completed.

Modifying a Scheduled Software Upgrade

To modify a scheduled software upgrade, first cancel the existing scheduled upgrade, then reschedule a new upgrade.

To modify a scheduled software upgrade:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 Click **Cancel upgrade**.
4 In the dialog box that is displayed, click **OK** to confirm the cancellation of the upgrade. The scheduled software upgrade is cancelled and the **EWC Software** tab fields become available for scheduling a new software upgrade.

Deleting a Software Image

It is OK to delete a software image if it is no longer needed on your system.

To delete a software upgrade:

1 From the top menu, click **Controller**.
2 From the left pane, click **Administration** > **Software Maintenance**.
3 In the **Select upgrade** list, click the software upgrade you want to delete.
4 Click **Delete selected**.
5 In the dialog box that is displayed, click **OK** to confirm the deletion of the upgrade. The Software Maintenance window is displayed, providing the status and results of the deletion.

Upgrading Using the CLI

Note
The first step to upgrade the software is to backup the image of the existing software release. For more information, see Backing Up and Restoring the Image on page 13.

To upgrade the wireless software locally:

1 Use the `copy upgrade` *`server | user | dir | file`* [**`dest`**] [**`scp`** *`scp password`*] command to download the software upgrade bundle from the remote FTP or SCP server.

- If you want to download the file on the controller flash device, type flash for **`dest`** option in the copy upgrade *`server`* | *`user`* | *`dir`* | *`file`* [**`dest`**] syntax.
- If you want to download the file on the controller local drive, leave out the [dest] option in the copy upgrade *`server`* | *`user`* | *`dir`* | *`file`* [**`dest`**] syntax.
- If you want to download the file from the SCP server, provide the corresponding SCP server, user, dir and file appended with **`scp`** *`scp password`*.
- If you want to download the file from the FTP server do not specify **`scp`** *`scp password`* at the end, where server, user, dir and file will specify FTP server parameters.

  Example 1 – In the following example, the CLI command states that the upgrade file will be downloaded from the FTP server to the flash card.

  ```
  EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images/ AC-
  MV-08.00.01.0003-1.pfe flash
  ```

  Example 2 – In the following example, the CLI command states that the upgrade file will be downloaded from the FTP server to the controller local drive.

  ```
  EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images/ AC-
  MV-08.00.00.0123-1.pfe
  ```

  Example 3 – In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the flash card.

  ```
  EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-
  MV-08.31.01.0200-1.rue flash scp TestPassword
  ```

  Example 4 – In the following example, the CLI command states that the upgrade file will be downloaded from the SCP server to the controller local drive.

  ```
  EWC.extremenetworks.com# copy upgrade 192.168.4.10 test system/images AC-
  MV-08.31.01.0200-1.rue scp TestPassword
  ```

2 Use the `show upgrade` command to confirm the upgrade file was downloaded successfully.

```
EWC.extremenetworks.com# show upgrade
1: AC-MV-08.00.00.0123-1.pfe
```

3 Upgrade the software by running `upgrade ac` *`file name`* command. Type `Yes` to the `Do you wish to continue?` prompt.

```
EWC.extremenetworks.com# upgrade ac AC-MV-08.00.00.0123-1.pfe bckto local
```

This command makes a local backup image of the running system and installs the selected upgrade image.

To avoid typing the image name, you can specify the image using the index returned by the show upgrade command.

For example, the command below will install the image with index 1 which, in this case, is AC-MV-08.00.00.0123-1.pfe: upgrade ac 1 bckto local

To upgrade the wireless software remotely:

4 Set up the FTP server from which you are downloading the file.

```
upgrade_image_src 192.168.4.10 test abc123 system/images AC-MV-08.00.00.0123-1.pfe
```

5 Start the upgrade with `upgrade ac ftp bckto local` command.

This command first makes a local backup image of the running system, downloads the upgrade image in temporary directory, and installs the image. No local copy of the image exists after the upgrade.

Migrating the Platform Configuration

You can migrate a configuration from one model of wireless controller to another model. Table 7 provides information on the pairs of wireless controller models that support configuration migration from one another. Figure 1 on page 48, displays the steps to migrate a configuration between platforms.

Table 7: Configuration Migration Table

From	To
V2110, running V9.01/V9.12/9.15/V9.21/V10.01/V10.11/V10.21/V10.31/V10.41	C5210, C5215 running V10.51
C35, running V9.21/V10.01/V10.11/V10.21/V10.31/V10.41	C5210, C5215, running V10.51
C5210, running V9.01/V9.12/V9.15/V9.21/V10.01/V10.11/V10.21/V10.31/V10.41	C5215, running V10.51

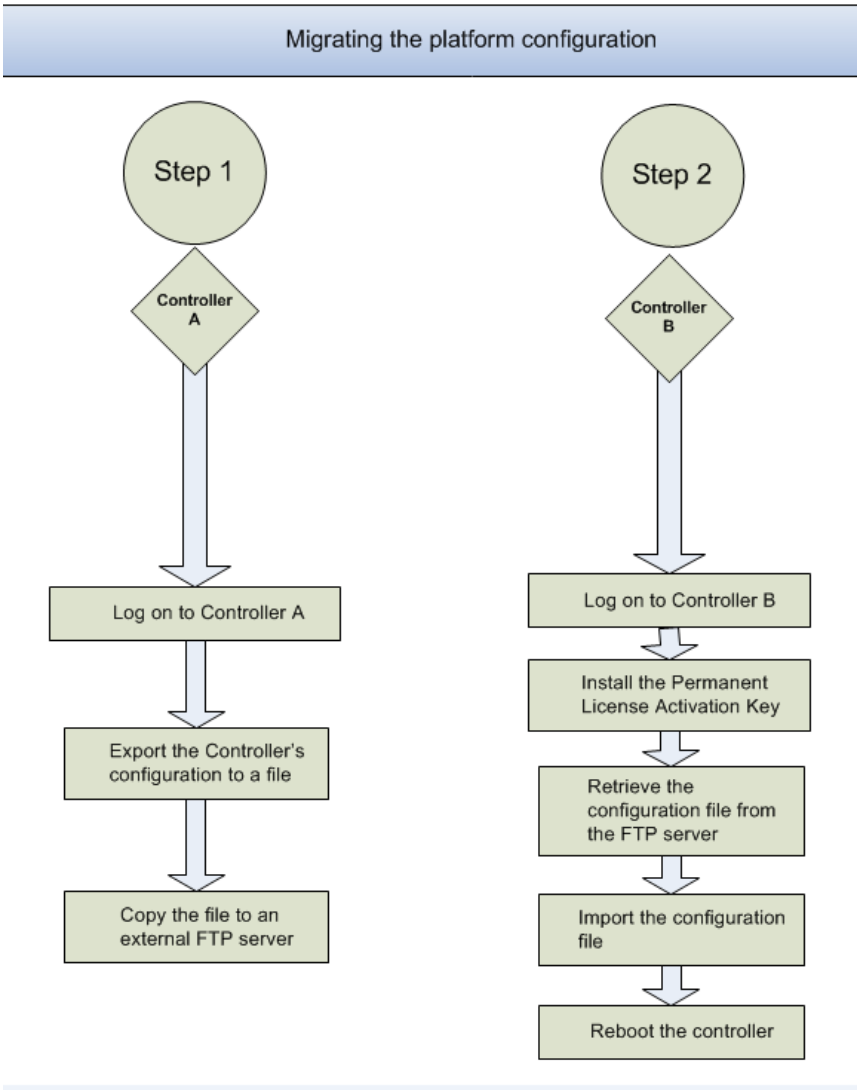


Figure 1: Sequential Steps for Migrating a Configuration

To Migrate a Platform Configuration

To migrate a platform configuration, both the Source controller model and software and the Destination controller model and software must support the migration as described in Table 7 on page 47.

1 Log on to the Source controller.

2 Export the controller configuration to a file by running the following CLI command.

```
EWC.extremenetworks.com# export configuration
Filename (EWC.extremenetworks.com.13062007.132046):
Comment: <enter a comment here - optional>
Please wait...
Creating EWC.extremenetworks.com.13062007.132046...
Backup/Export complete.
```

3 Use the `show export` command to list the current set of backup files.

4 Copy the file to an external FTP or SCP server by running the `copy configuration` command.

```
EWC.extremenetworks.com#copy configuration to-remote server IP
username destination directory [ftp password
| scp password] from-local filename
```

5 Log on to the Destination controller.

6 Install the Permanent License Activation key.

7 Retrieve the configuration file from the external FTP or SCP server by running the `copy configuration` command.

```
EWC.extremenetworks.com#copy configuration to-remote server IP
username destination directory [ftp
password | scp password]
from-local filename
```

8 Type the password.

9 Use the `show import` command to list the current set of backup files, which will include the retrieved configuration file.

10 Import the configuration by running the `import filename` command.

After the import process is completed, the wireless controller will reboot.

Note
The Management IP address will be identical to that of the controller from where the configuration is migrated.

Upgrading Two Controllers in Availability Mode

This section, which describes how to upgrade the software version on two controllers in availability mode, is applicable if the availability pair is made of one of the following combinations:

Table 8: Availability Pairs

Controller 1	Controller 2
C35	C35
C5210	C5210
C5215	C5215
V2110	V2110

Note
The two wireless controllers in an ‘availability’ pair must be running the identical version of the software.

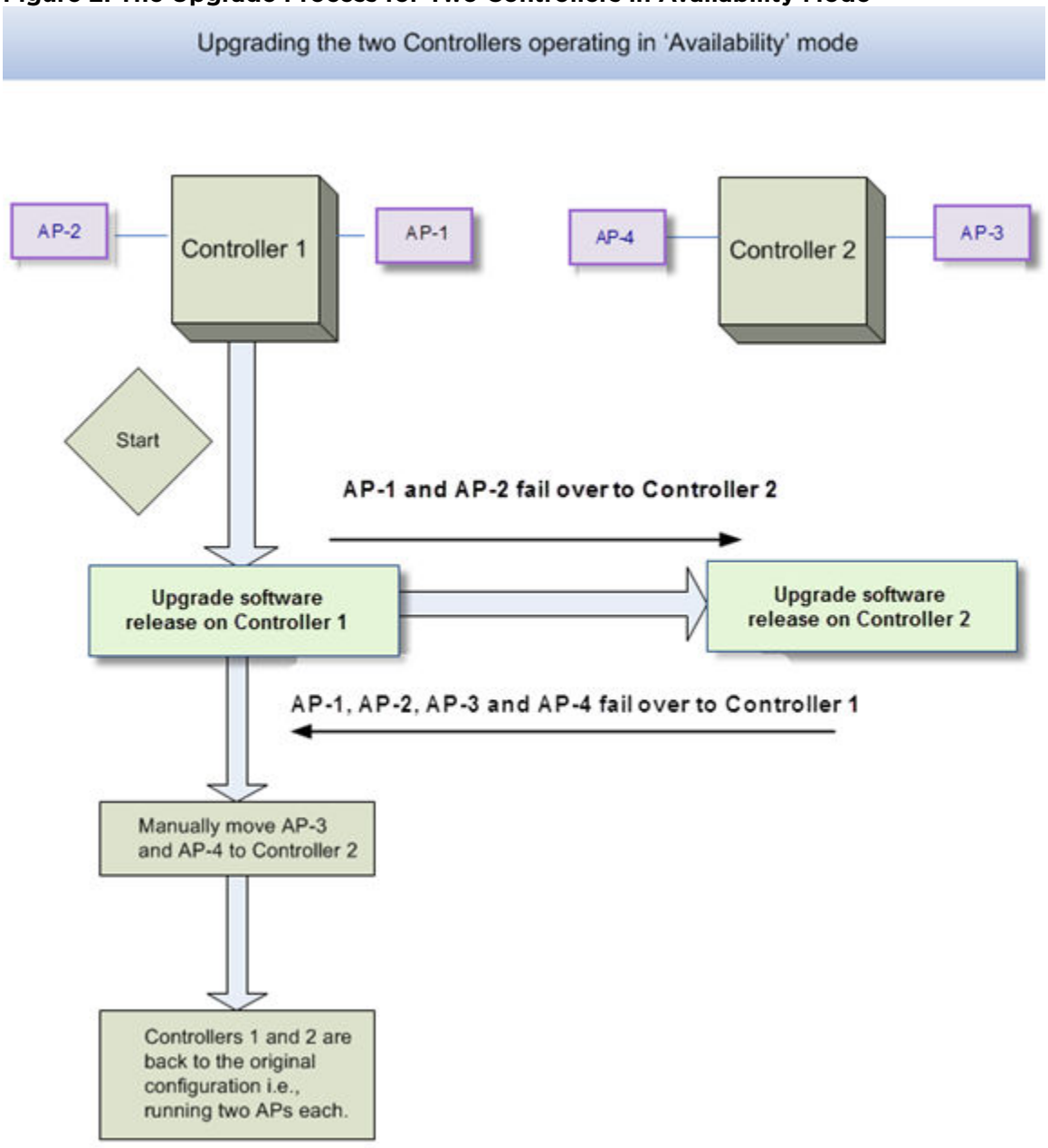
For the ease of understanding, this section is explained with the help of the following hypothetical scenario:

- The upgrade is to be carried out on the two controllers — EWC-1 and EWC-2.
- Both the controllers are operating in ‘availability’ mode.
- Both controllers are running the previous software release, and they need to be upgraded to the next software release.

- Each controller has two APs. EWC-1 has AP-1 and AP2, whereas EWC-2 has AP-3 and AP-4.
- AP-1 and AP-2 are configured as 'Local' on EWC-1 and 'Foreign' on EWC-2.
- AP-3 and AP-4 are configured as 'Local' on EWC-2 and 'Foreign' on EWC-1.

The following figure depicts the hypothetical upgrade process:

Figure 2: The Upgrade Process for Two Controllers in Availability Mode



Upgrading Software on Controller 1

Note

If you upgraded the software on the two controllers in session availability mode, you must perform a controlled upgrade on the wireless APs. For more information, see Maintaining the Wireless AP Software on page 105.

Use the standard procedures via the Wireless Assistant GUI or CLI commands to upgrade the software.

When you upgrade the software version on Controller 1, it will reboot. Consequently, the 'availability' feature automatically moves both AP-1 and AP-2 from Controller 1 to Controller 2. All clients registered with these two APs get disconnected. They re-connect automatically (if configured to do so) either to a different AP or to the same one after the service is restored.

After Controller 1 reboots, all 4 APs connect to Controller 2, which is still running the older software. Controller 1 is now upgraded to the new software release and has the same prior configuration. All 4 APs are running the older software.

Upgrading Software on Controller 2

Use the standard procedures via the Wireless Assistant GUI or CLI commands to upgrade the software.

When you upgrade the software version on Controller 2, it will reboot. Consequently, the "Availability" feature will automatically move all 4 APs from Controller 2 to Controller 1. Because Controller 1 was upgraded to the newer software version, all the 4 APs are upgraded as well. This causes a short disruption of service.

All clients on all the four APs get disconnected. They re-connect automatically (if configured to do so) after the service is restored.

After Controller 2 reboots, all the four APs are associated with Controller 1. Both controllers are now upgraded to the new software release and have the same prior configuration. All the four APs are also upgraded to the new software release.

Manually Moving APs Back to Local Controller

Manually move AP-3 and AP-4 from Controller 1 to Controller 2, where they were configured as 'Local' APs. After you manually move the APs, the network is back to its original configuration with each controller running two APs.

Upgrading Two Controllers in Session Availability Mode

The process for upgrading two wireless controllers in session availability mode is identical to upgrading two controllers in availability mode. For more information, see Upgrading Two Controllers in Availability Mode on page 49.

5 Working with External Storage Devices

Note
In this section, the term “flash device” applies to all external storage devices that can be used with the controllers.

Working with an External Storage Device

Note
V2110 (MS Hyper-V platform) does not support flash functionality (upgrade, backup, restore, storage, etc.).

You can use a USB device to do the following maintenance tasks:

- **Installing and upgrading the software**: You can install or upgrade the wireless software from a USB device.
- **Backing up the system**: You can store the existing image of the wireless software on a USB device as a backup while upgrading the software.
- **Restoring the software**: You can restore the backed up wireless software from a USB device.
- **Storing configuration backup files**: You can export and import configuration backup to/from flash, as well as transfer configuration backup file between flash, local storage and remote servers.
- **Storing exception traffic files**: You can store captured exception traffic on the USB device. For example, *DHCP (Dynamic Host Configuration Protocol)*, *OSPF (Open Shortest Path First)*, TFTP traffic.

The USB device is automatically made available to the GUI/CLI (mounted) by the controller when inserted in the device slot. After the flash device is mounted, the GUI/CLI shows the content of the flash device for the related operation, such as backup and upgrade. To manually unmount or remount an already inserted flash device, use the controller GUI:

- **Mount the flash device** – By mounting the flash device, you make the flash device that has been inserted into the controller available for use.

- **Unmount the flash device** – By unmounting the flash device, you make the flash device that has been inserted into the controller unavailable for use.

  Caution
  You must always unmount the flash device via the controller GUI before removing it from the controller. Failure to do so may corrupt the files on the flash device. Always wear an ESD wristband when inserting or removing a flash device.

- **Delete files stored on the flash device** – You can also delete files stored on a USB device. By deleting the files, you can create space on the USB device. For more information, see Deleting Files from a Flash Device on page 56.

Flash Device File System Format

All flash devices used with the controller must be formatted in FAT32. Only the first partition of the flash device is used by the controller.

Controller software can operate (backup, restore, delete, etc.) only with files located in the root directory on the flash drives. In other words, it cannot operate with files located under directories.

Wireles controllers equipped with multiple USB connectors support only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

Warning
Ensure all flash devices used with the controller are formatted to be non-bootable. Otherwise, the controller may experience difficulties when rebooting if connected to a bootable formatted flash device.

Mounting a Flash Device on the Wireless Controller

To mount a flash device on the controller:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **Flash**.

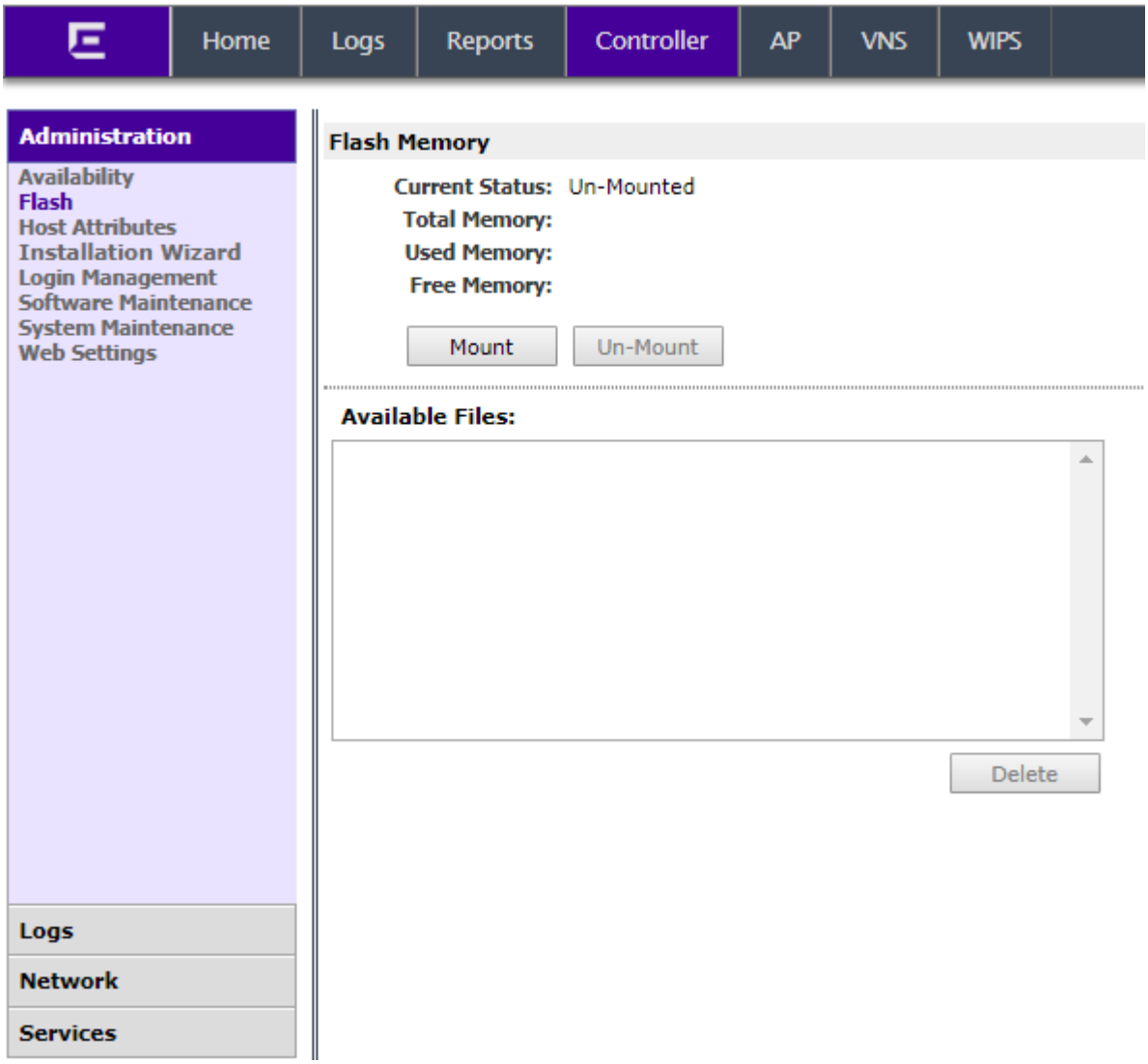


Figure 3: Flash Memory Screen

3 Click **Mount**, and then click **OK** to confirm the flash device mount. Once the mounting process is complete, the flash memory space is displayed and the files contained on the flash device are listed in the **Available Files** box.

When you mount the flash device, the F icon in the footer changes from red to green.

Note
If a flash device was already mounted (previously inserted), the screen shows the status as Mounted as well as all available files on the flash device.

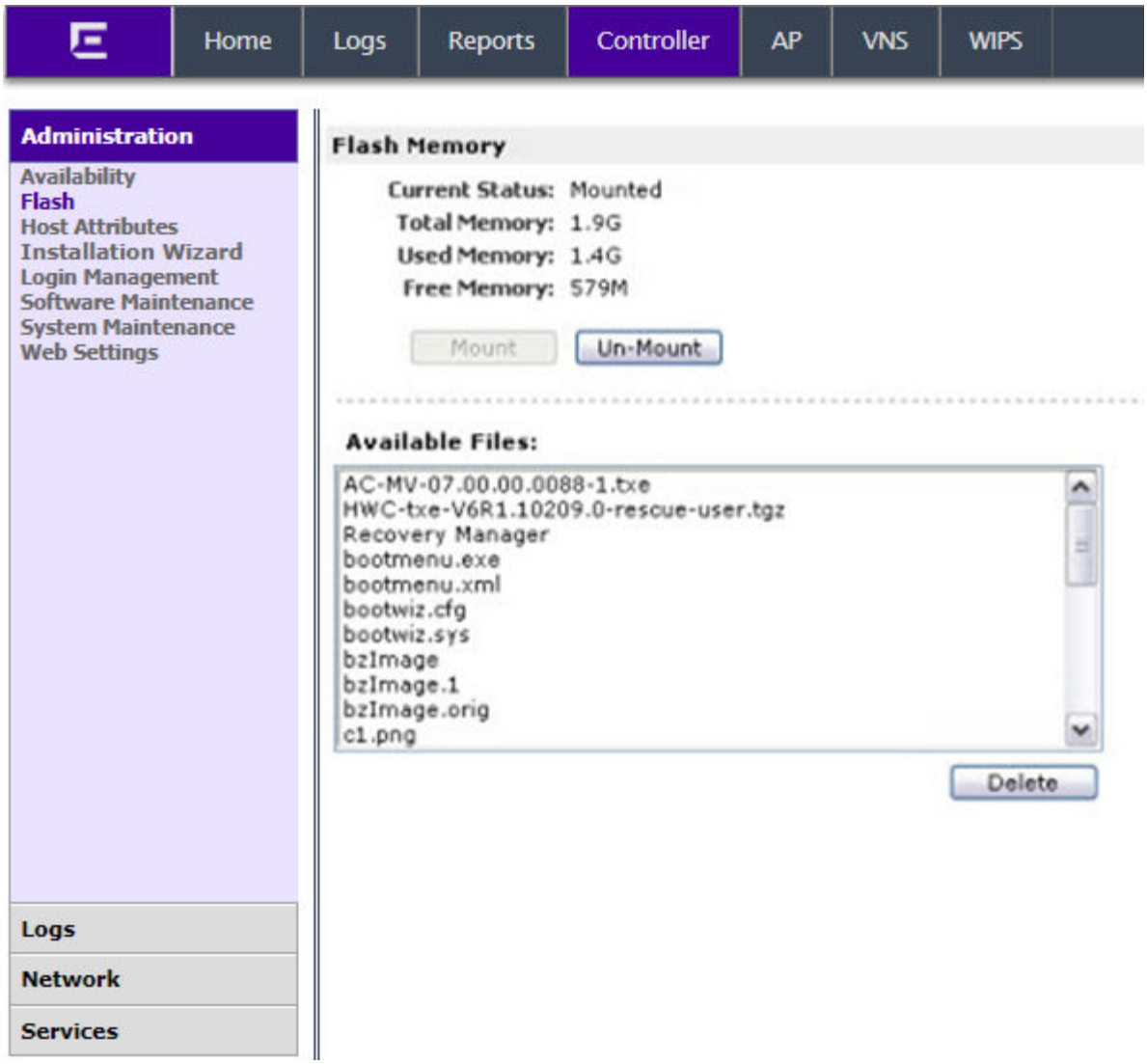


Figure 4: Available Files

Un-mounting a Flash Device from the Controller

To un-mount a flash device from the controller:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **Flash**.

The mounted flash memory space is displayed and the Available Files box displays any files located on the flash device.

3 Click **Un-Mount**, and then click **OK** to confirm the flash device unmount.

Once the un-mounting process is complete, the Flash Memory screen is refreshed and no longer displays any of the flash memory information. When you un-mount the flash device, the F icon in the footer changes from green to red.

Deleting Files from a Flash Device

To delete files from a flash device:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **Flash**.

The Flash Memory screen is displayed. The mounted flash memory space is displayed and the **Available Files** box displays any files located on the flash device.

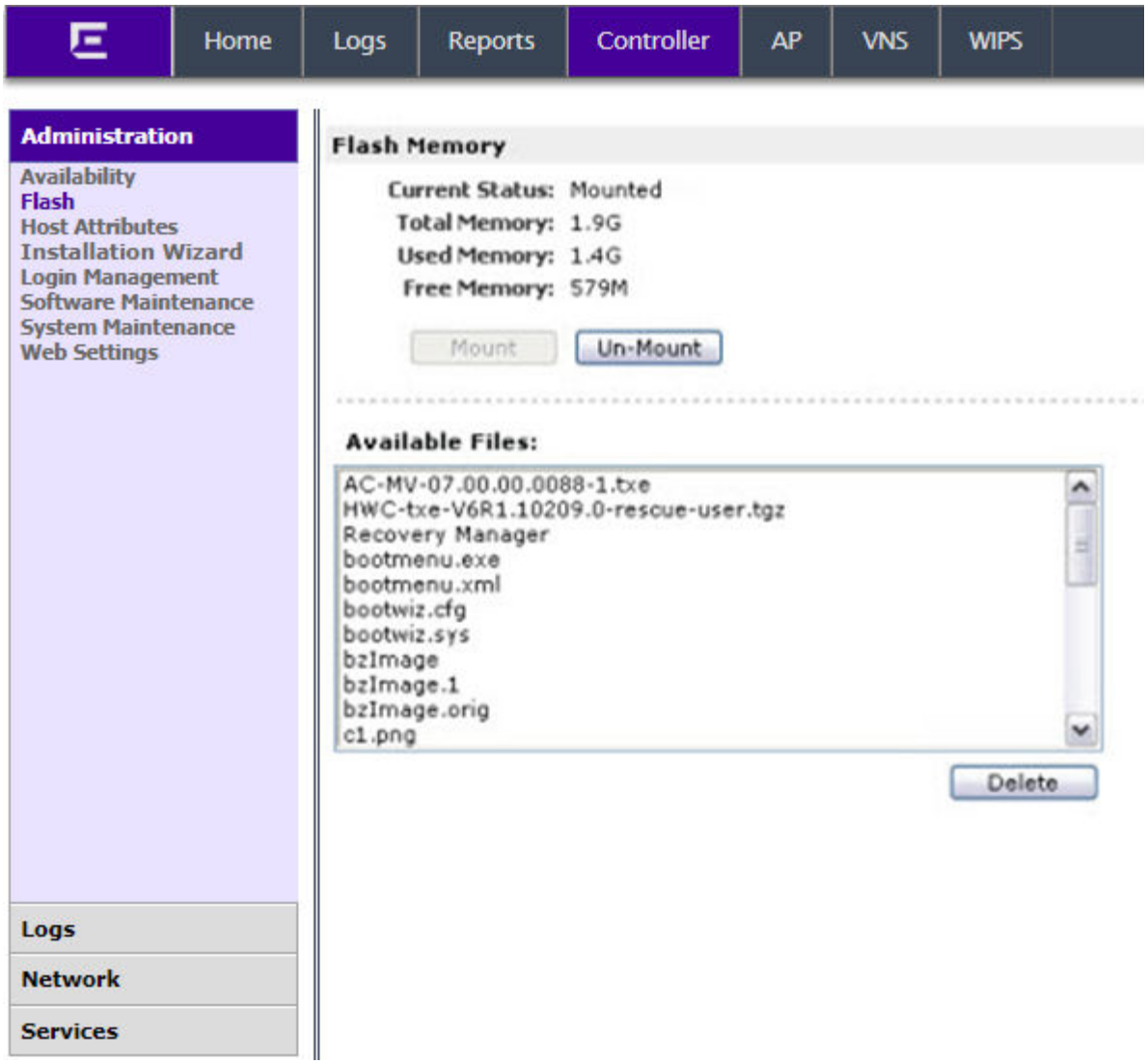


Figure 5: Deleting Files

3 In the **Available Files** box, click the file you want to delete, and then click **Delete**.

4 To confirm the file deletion from the flash device, click **OK**. The file is deleted.

6 Using the Console Port

Using the Console Port in the Wireless Controller

The following controller models are supported by ExtremeWireless:

- C35
- C5210
- C5215

Entering Rescue Mode on the Wireless Controller C35, C5210, and C5215

To get into Rescue mode, you must connect your laptop to the controller's console port using a Serial RJ45 to DB9 Female cable.

- Speed — 115200
- Databits — 8
- Parity — None
- Stop Bits — 1
- Flow Control — None

If your laptop has a USB port instead of a serial port, you must use the USB 2.0 to RS232 Serial Adapter to connect the RJ45 to DB9 cable to the laptop.

Related Links

Maintaining the C35 Controller on page 95

Maintaining the C5210 Controller on page 97

Maintaining the C5215 Controller on page 100

Using the Console Port for the V2110

To get into Rescue mode in the V2110 Virtual Wireless Appliance, you must connect your laptop to the VMware server's serial port via the Null Modem DB9 F- F (Female to Female) cable.

The serial port settings on the laptop should be the following:

- Speed — 115200
- Databits — 8
- Parity — None

- Stop Bits — 1
- Flow Control — None

7 Performing System Maintenance

Note

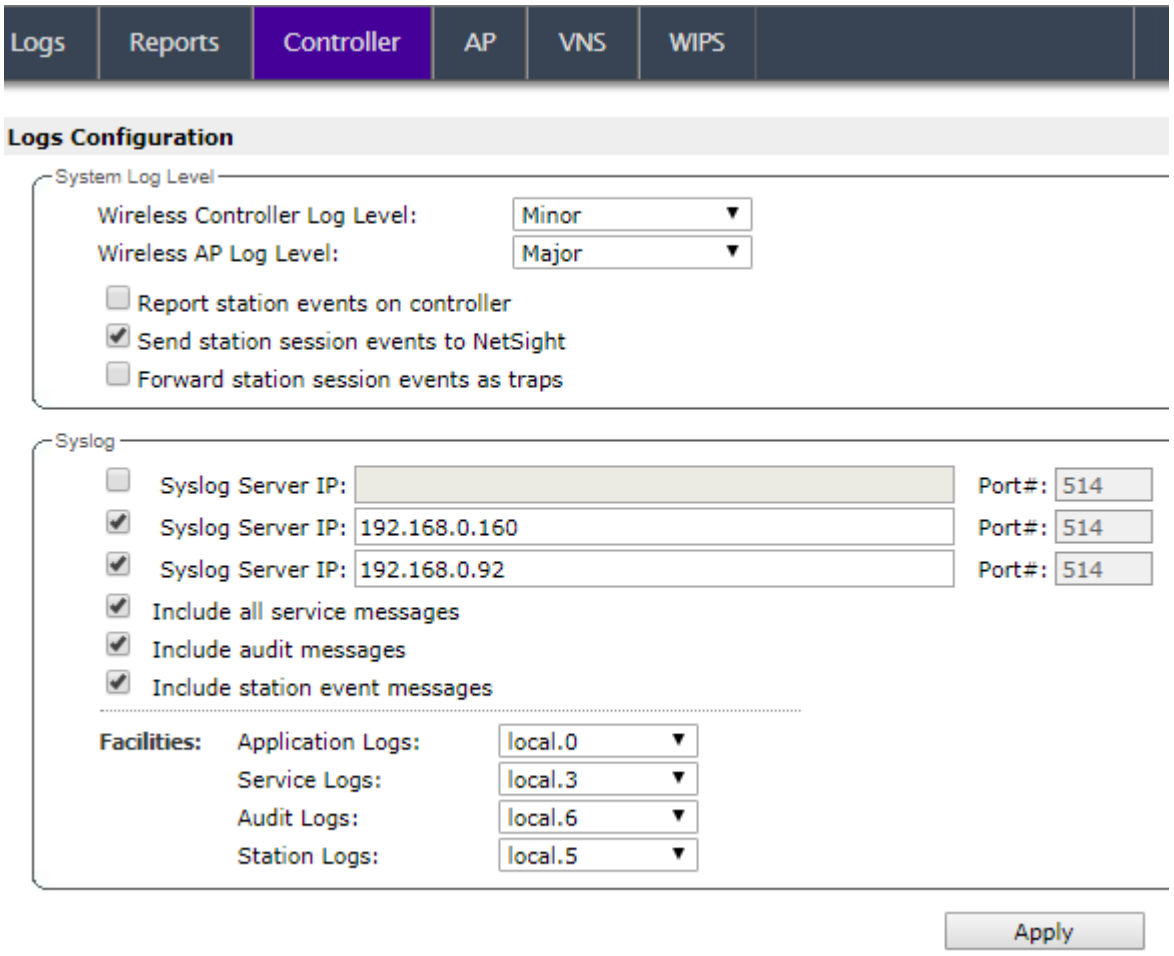
Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

Changing Log Levels, Syslog Event Reporting, and AP Log Management

This section provides procedural information related to log management and event reporting.

Changing Log Levels

1 From the top menu, click **Controller**. From the left pane, click **Logs**. The Logs Configuration screen is displayed.



Note

Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

Note

The log statements **Low water mark level was reached** and **Incoming message dropped, because of the rate limiting mechanism** indicate that there is a burst of log messages coming to the event server and the processing speed is slower than the incoming rate of log messages. These messages do not indicate that the system is impaired in any way.

2 In the **System Log Level** section:

- From the **Wireless Controller Log Level** drop-down list, select the least severe log level for the controller that you want to receive: Information, Minor, Major, Critical.

  For example, if you select **Minor**, you receive all Minor, Major and Critical messages. If you select **Major** you receive all Major and Critical messages. The default is Minor.
- From the **Wireless AP Log Level** drop-down list, select the least severe log level for the AP that you want to receive: Information, Minor, Major, Critical.

  For example, if you select **Major** you receive all Major and Critical messages. The default is Major.
- Click Report station events on controller to collect and display station session events on the controller station events log.
- Click **Send station session events to NetSight** to forward station session events to NetSight for monitoring. Event information will not be sent to NetSight unless this check box is selected.
- Click **Forward station session events as traps** to forward station events as *SNMP (Simple Network Management Protocol)* traps.

3 Click **Apply**.

Enabling and Defining Parameters for Syslog

To enable and define parameters for Syslog:

1 From the top menu, click **Controller**.
2 From the left pane, click **Logs.**
3 In the **Syslog** section, to enable the **Syslog** function for up to three syslog servers, select the appropriate check boxes.
4 For each enabled syslog server, in the **IP** box, type a valid IP address for the server on the network.

  In the **Port #** box, the default port for syslog (514) is displayed.
5 To include all system messages, select the **Include all service messages** check box. If the box is not selected, only component messages (logs and traces) are relayed. This setting applies to all three servers. The additional service message is: **DHCP messages reporting users receiving IP addresses**.
6 To include audit messages, select the **Include audit messages** check box.
7 To include station session event messages, select the **Include station event messages** check box.
8 In the **Application Logs** drop-down list, click the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.
9 If the **Include all service messages** check box is selected, the **Service Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.
10 If you select the **Include audit messages** check box, the **Audit Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.
11 If you select the **Include station event messages** check box, the **Station Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies to all three servers.

12 To apply your changes, click **Apply**.

Note

The syslog daemon must be running on both the controller and on the remote syslog server before the logs can be synchronized. If you change the log level on the controller, you must also modify the appropriate setting in the syslog configuration on remote syslog server.

Table 9: Syslog and Controller Event Log Mapping

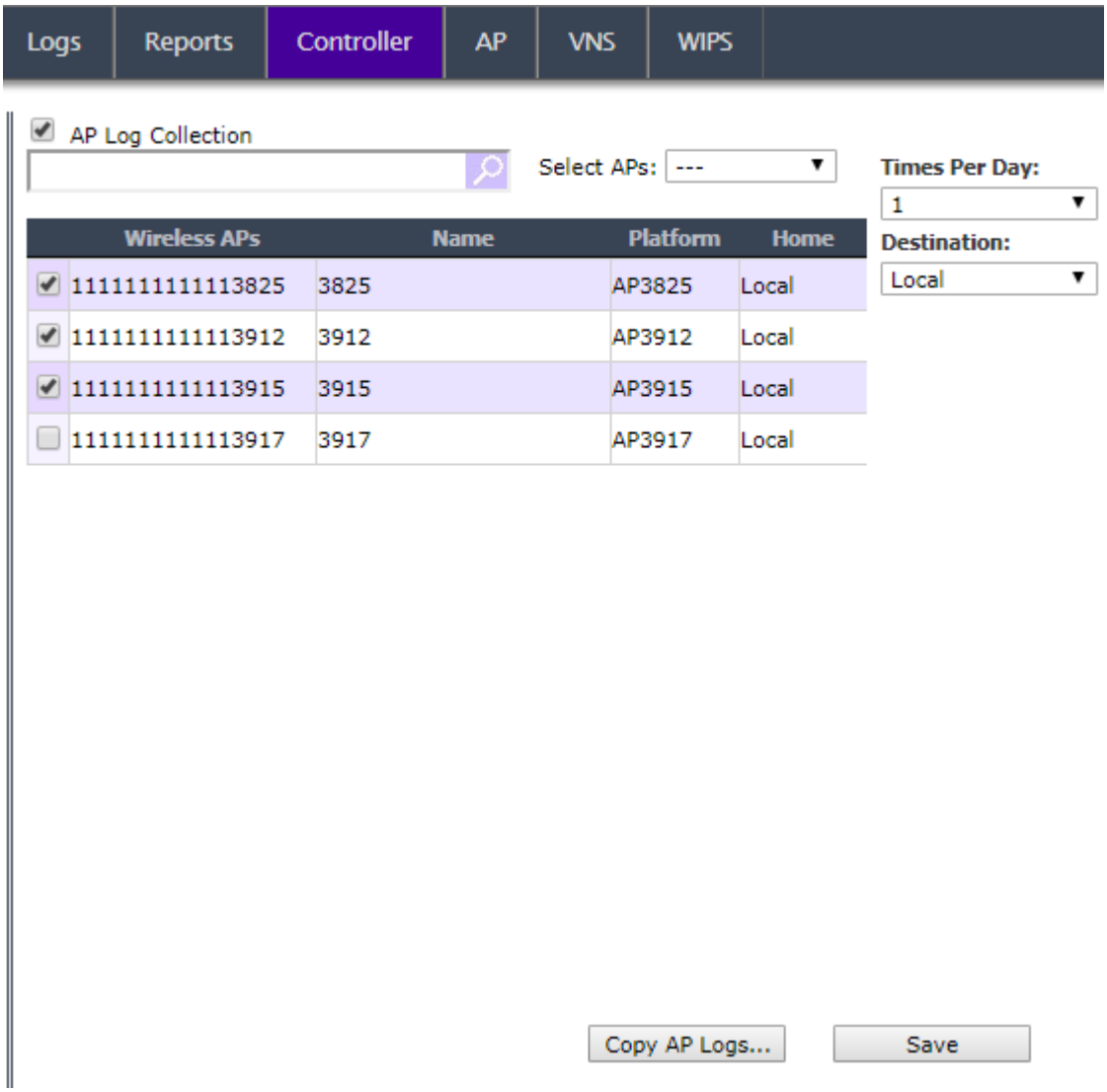
Syslog Event	Controller Event
LOG_CRIT	Critical
LOG_ERR	Major
LOG_WARNING	Minor
LOG_INFO	Information

Enabling AP Log Management

To enable AP Log Management:

1 From the top menu, click **Controller**.

2 From the left pane, click **Logs** > **AP Log Management** > **AP Log Collection** .



3 To specify which APs will be included, do one of the following:

- Search for a specific AP by entering the AP in the search bar and clicking ( ).
- For a specific AP, select the corresponding check box.
- For APs by category, click one of the **Select APs** options:
  - "---" option - Selected APs will be cleared from the AP Logs search.
  - Local APs - Select active or inactive local configured APs.
  - Foreign APs - Select active or inactive foreign configured APs.

4 To clear your AP selections, click **Deselect All**.

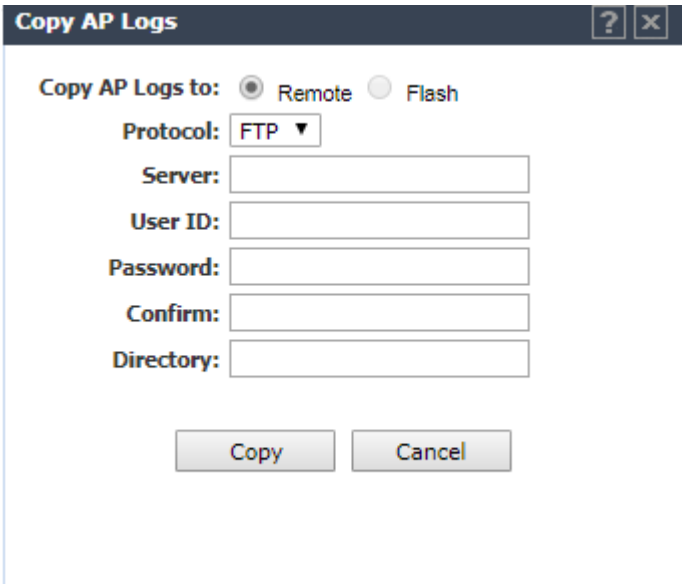
5 To set the frequency of the collection, under **Times Per Day**, select 1 (default), 2, 4, or 6 times per day.

6 To set the destination of the AP logs, under **Destination**, select **Local**, **Flash**, or **Remote**.

7 Click **Save**.

Copying AP Logs

1 From the AP Log Management dialog, click **Copy AP Logs** to transfer locally collected logs. The Copy AP Logs dialog is displayed.



2 Set the location of the AP Logs by selecting either **Remote** or **Flash**. The Flash button is disabled when flash is not mounted.

3 When Remote is selected, do the following:

- Under Protocol, select SCP or FTP to select the file transfer protocol you want to use to upload the AP Log file.
- Under Server, type the IP address of the server where the AP Logs will be uploaded.
- Under User ID, enter the user ID used to log into the server.
- Under Password, enter the corresponding password for the user ID.
- Under Confirm, enter the corresponding password for the user ID to confirm it was typed correctly.
- Under Directory, enter the directory on the server where the AP Log file will be stored.

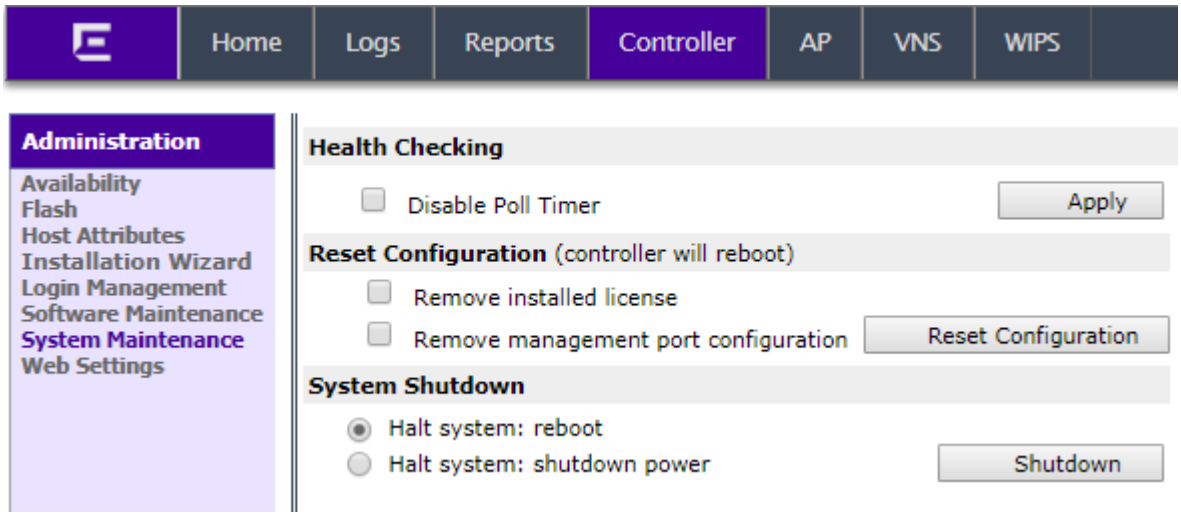
4 Click **Copy** to copy the logs.

Enabling or Disabling the Poll Timer

To enable or disable the Poll Timer:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **System Maintenance**.



3 Do one of the following:

- To disable the poll timer, select the **Disable Poll Timer** check box in the **Health Checking** section.
- To enable the poll timer, clear the **Disable Poll Timer** check box in the **Health Checking** section.

4 Click **Apply**.

Related Links

#unique_85

Shutting Down the System on page 66

Shutting Down the System

An alternative method of stopping the software operation is to use CLI commands. For more information, see the *CLI Reference Guide*.

Warning

Do not power off the controller by using the power switches only. Instead, carry out the entire procedure as described in this section. Failure to do so may corrupt the data on the hard disk drive.

To shut down the system:

1 From the top menu, click **Controller**.

2 From the left pane, click **Administration** > **System Maintenance**.

3 In the **System Shutdown** section, select the appropriate shut down option:

- Halt system: reboot – The system shuts down, then reboots.
- Halt system: Shutdown power – The system enters the halted state, which stops all functional services and the application. To restart the system, the power to the system must be reset.

4 To shut down the system including associated wireless APs, click **Shutdown**.

A warning message is displayed, asking you to confirm your shutdown selection.

5 Click **Yes** to continue. Your system shuts down.

Resetting Wireless APs to Factory Default Settings

The AP boot-up sequence includes a random delay interval, followed by a vulnerable time interval. During the vulnerable time interval (2 seconds), the LEDs flash in a particular sequence to indicate that the controller is in the vulnerable time interval. For more information, see the *User Guide*.

If you power up the AP and interrupt the power during the vulnerable time interval three consecutive times, the next time the AP reboots, it will restore its factory defaults including the user password and the default IP settings.

Caution
The restoration of factory default settings does not erase the non-volatile log.

Resetting APs to Factory Defaults

1 Switch off, and then switch on the wireless AP. The wireless AP reboots.
2 Switch off, and then switch on the wireless AP during the vulnerable time interval.

   Refer to the wireless AP's LED pattern to determine the vulnerable period. For more information, see the *User Guide*.
3 Repeat Step 2 two more times.

   When the wireless AP reboots for the fourth time, after having its power supply interrupted three consecutive times, it restores its factory default settings. The wireless AP then reboots again to put the default settings into effect.

   Refer to the wireless AP's LED pattern to confirm that the wireless AP is set to its factory defaults. For more information, see the *User Guide*.

Using the Reset Button (Hardware)

All wireless APs have a reset button, but they are located in different places on the AP chassis. Use it to reset the AP to its factory default settings by pressing and holding the reset button for at least six seconds.

Note
If you press the reset button and do not hold it longer than six seconds, the wireless AP simply reboots, and does not reset to its factory defaults.

The AP installation documentation is available at: https://extranet.extremenetworks.com/downloads

AP37xx Series Reset

Figure 6 illustrates the location of the reset button on the WS-AP3705i.

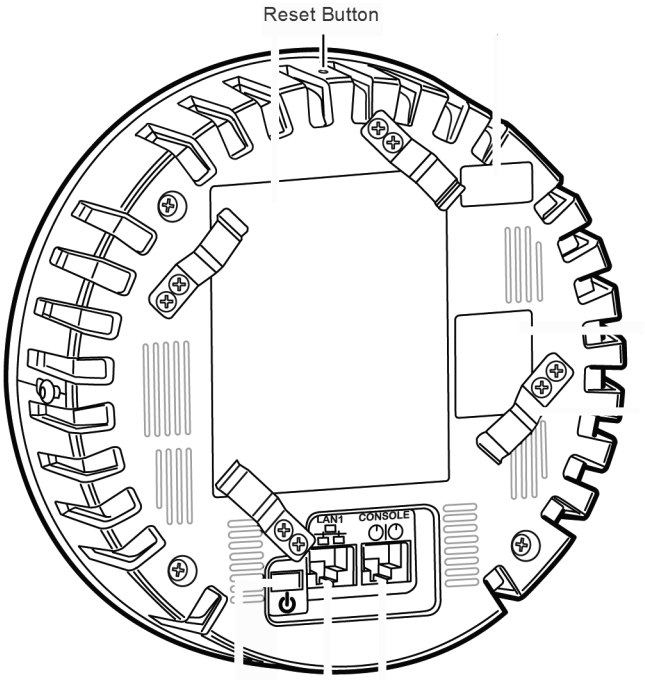


Figure 7 illustrates the location of the reset button on the WS-AP3710.

Figure 6: Position of the Reset Button on the AP3705i (rear view)

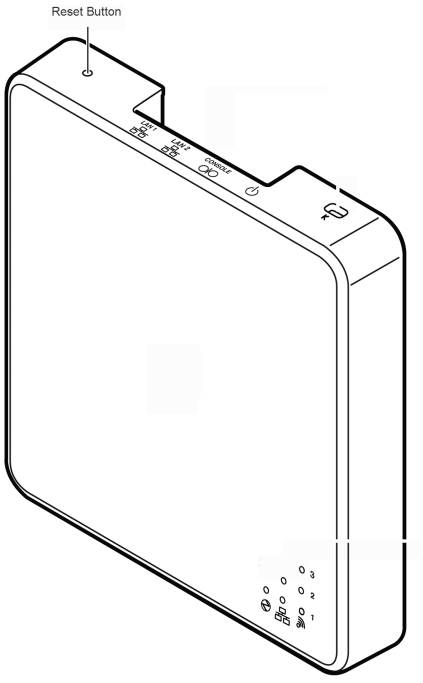


Figure 7: Position of the Reset Button on the AP3710

Figure 8 illustrates the location of the reset button on the WS-AP3765/3767.

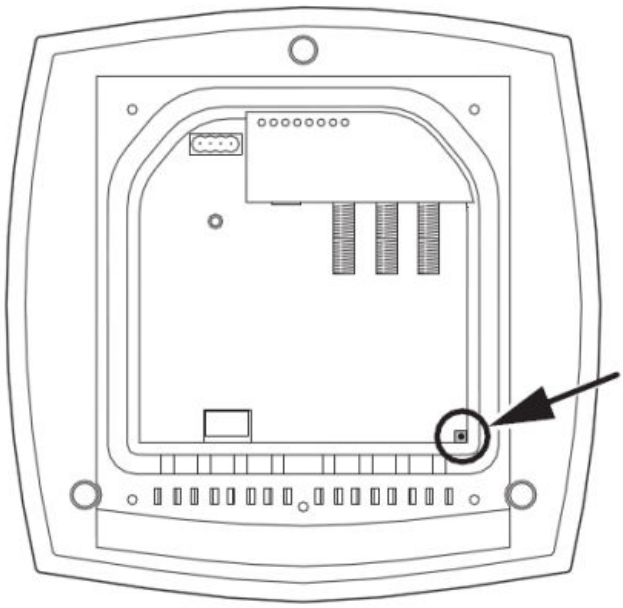


Figure 8: Position of the Reset Button on the AP3765/67 (rear view, with cover removed)

Figure 9 illustrates the location of the reset button on the WS-AP3715.

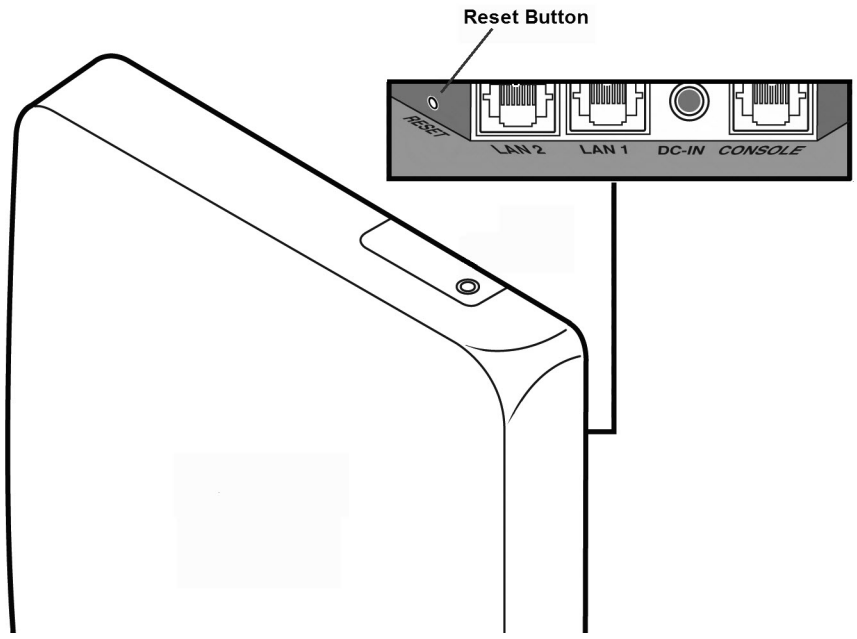


Figure 9: Position of the Reset Button on the AP3715

AP38XX Series Reset

Figure 10 illustrates the location of the reset button on the WS-AP3825i.

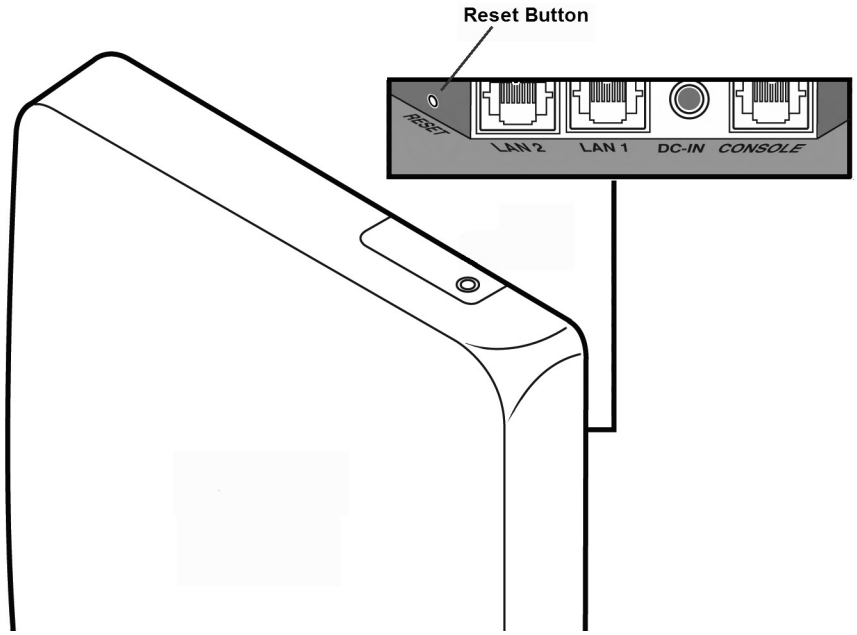


Figure 10: Position of the Reset Button on the AP3825

Figure 11 illustrates the location of the reset button on the WS-AP3805 and WSAP3801.

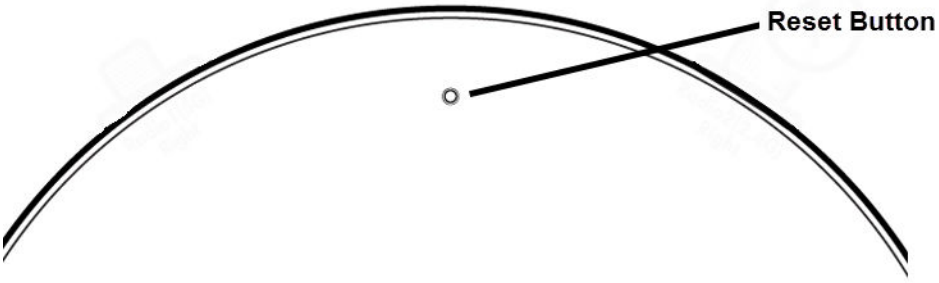


Figure 11: Position of the Reset Button on the AP3805 and AP3801

AP39xx Series Reset

The following AP39xx model access points are supported by ExtremeWireless:

- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

AP3917 Reset

Figure 12 illustrates the reset button on the AP3917 access points.

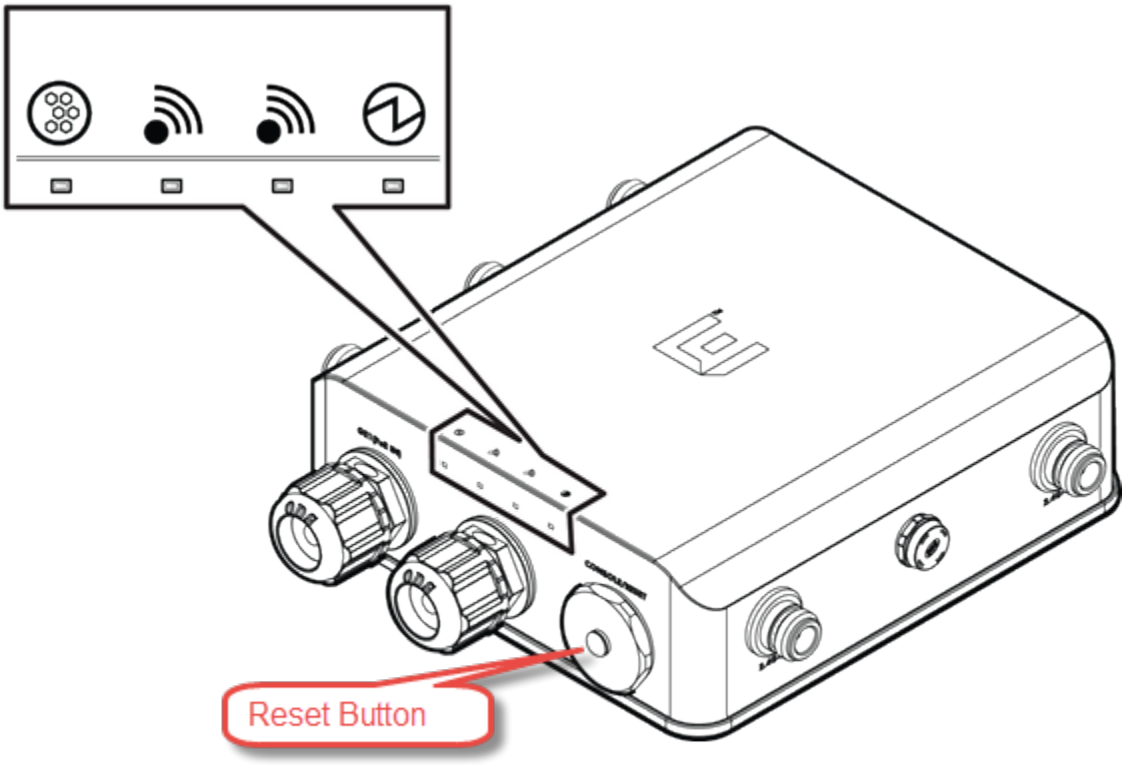


Figure 12: Position of the Reset Button on the AP3917

AP3916ic Reset

Figure 13 illustrates the reset button on the AP3916 access points.

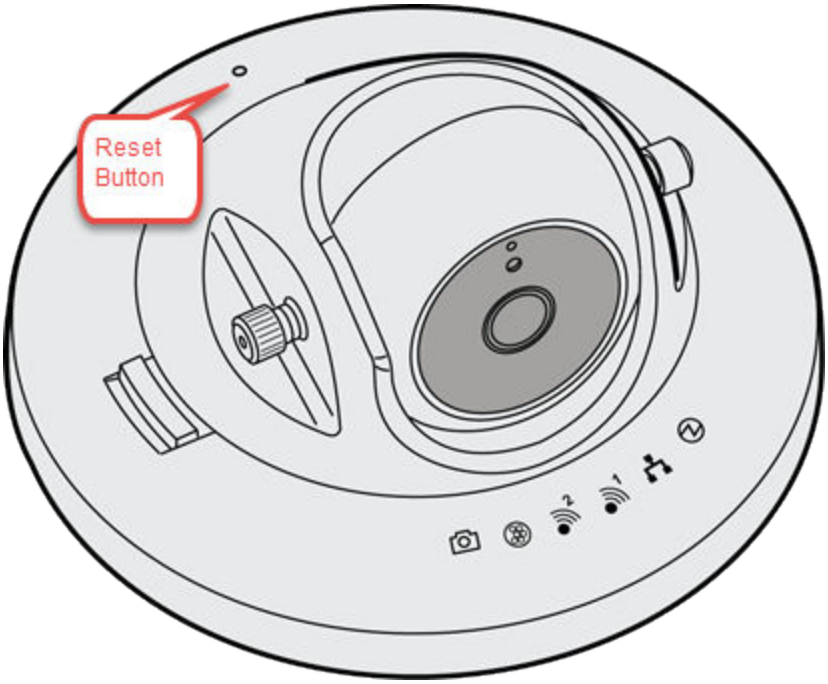


Figure 13: Position of the Reset Button on the AP3916ic

AP3915 Reset

The following figures illustrate the reset button on the AP3915i and AP3915e access points.

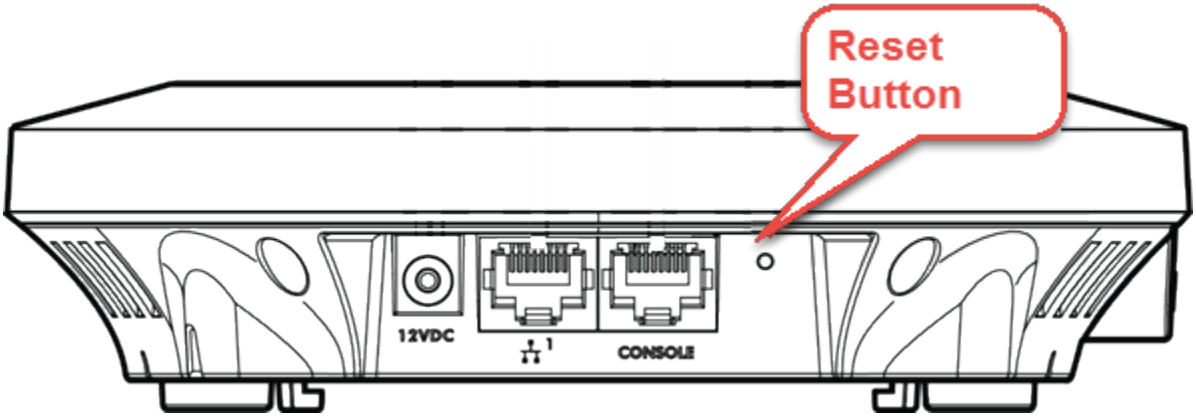


Figure 14: Position of the Reset Button on the AP3915i

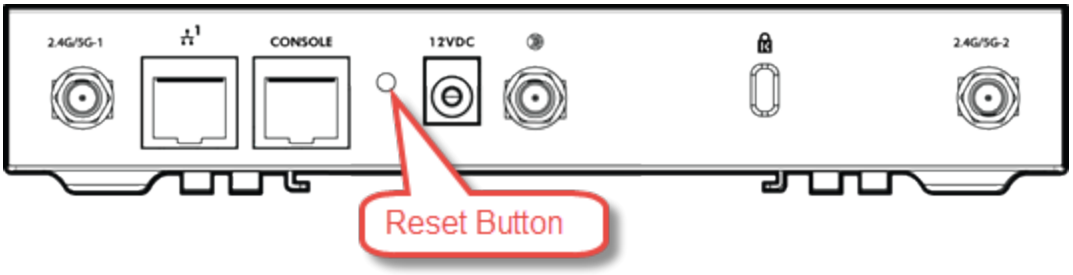


Figure 15: Position of the Reset Button on the AP3915e

AP3912 Reset

Figure 16 illustrates the reset button on the AP3912 access points.

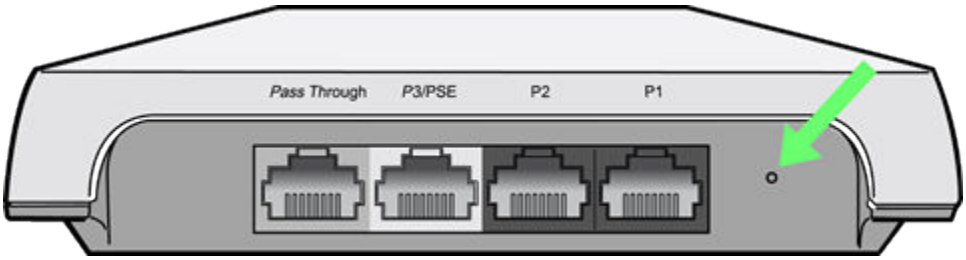


Figure 16: Position of the Reset Button on the AP3912

AP3935 Reset

Figure 17 illustrates the reset button on the AP3935 access points.

Figure 17: Position of the Reset Button on the AP3935

AP3965 Reset

Figure 18 illustrates the reset button on the AP3965 access points. Remove the console cap and use a non-corrosive probe to depress the black reset button.

Figure 18: AP3965 Reset Button

Replacing the CMOS Battery

Note
This procedure applies to the wireless controller model C5210 and C5215.

All wireless controllers contain a CMOS battery that retains BIOS information when the controller is powered off. The battery is located on the server board as shown in the figure below. See Table 10 for battery details.

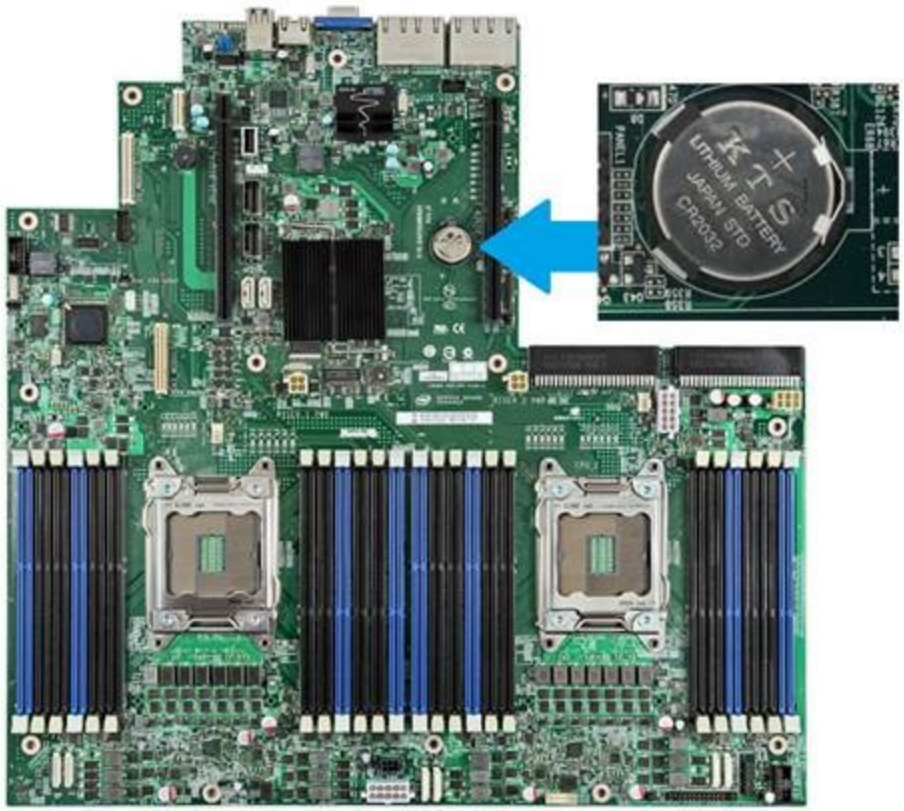


Figure 19: CMOS Battery Location

Table 10: Battery Details

Specification	Detail
Part Number	CR2032
Battery Type	Lithium
Voltage	3.3 Volts
Diameter	20 mm
Thickness	0.1 mm

Removing the Discharged Battery

1 Power off the controller.
2 Remove the power cables attached to the controller.
3 Remove the controller cover.

Warning
Make sure the controller is powered off and unplugged before removing the chassis cover.

4 Discharge the controller from static electricity by touching it with a metallic object and making sure all controller board LEDs are off.

5 Locate the battery as shown in Figure 19 on page 76. The positive pole of the battery should be visible.
6 Gently press the spring clip to eject the battery from the socket.
7 Remove the battery.

Installing the New Battery

1 Insert the new battery into the socket with the text on the battery facing up as shown in Figure 19 on page 76.

Note
Verify that the battery is placed correctly (firmly) in the slot location.

2 Replace the controller cover.
3 Install the power cable on the controller.
4 Power on the controller.

Verifying BIOS Data and Resetting the Controller Clock

Once the operation complete, it is important to re-configure the BIOS settings on the controller.

1 Connect a PC USB keyboard and VGA monitor to the controller.
2 Power up the controller and enter the BIOS by pressing **[F2]** during POST.
3 Modify the date and time as needed.
4 Press **[F9]** to load the Extreme Default settings
5 Press **[F10]** to Save and quit BIOS.

8 Using Controller Utilities

Using Controller Utilities

You can use wireless controller utilities to test a connection to the target IP address and record the route through the Internet between your computer and the target IP address. In addition, you can also use controller utilities to capture exception traffic, which can be useful for network administrators when debugging network problems.

To test or record IP address connections:

1 From the top menu, click **Controller**.

2 In the left pane, click **Network** > **Utilities**.

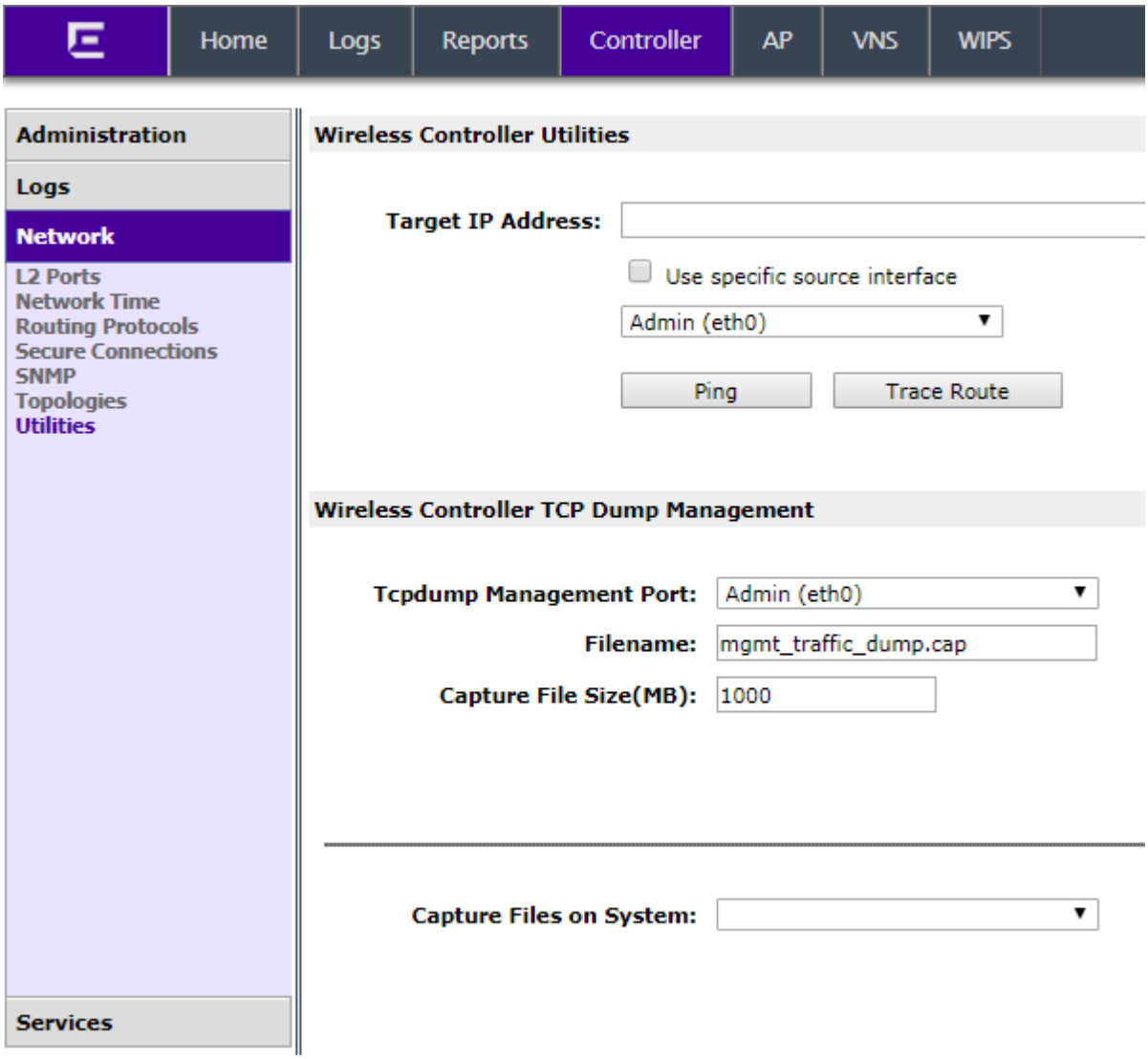


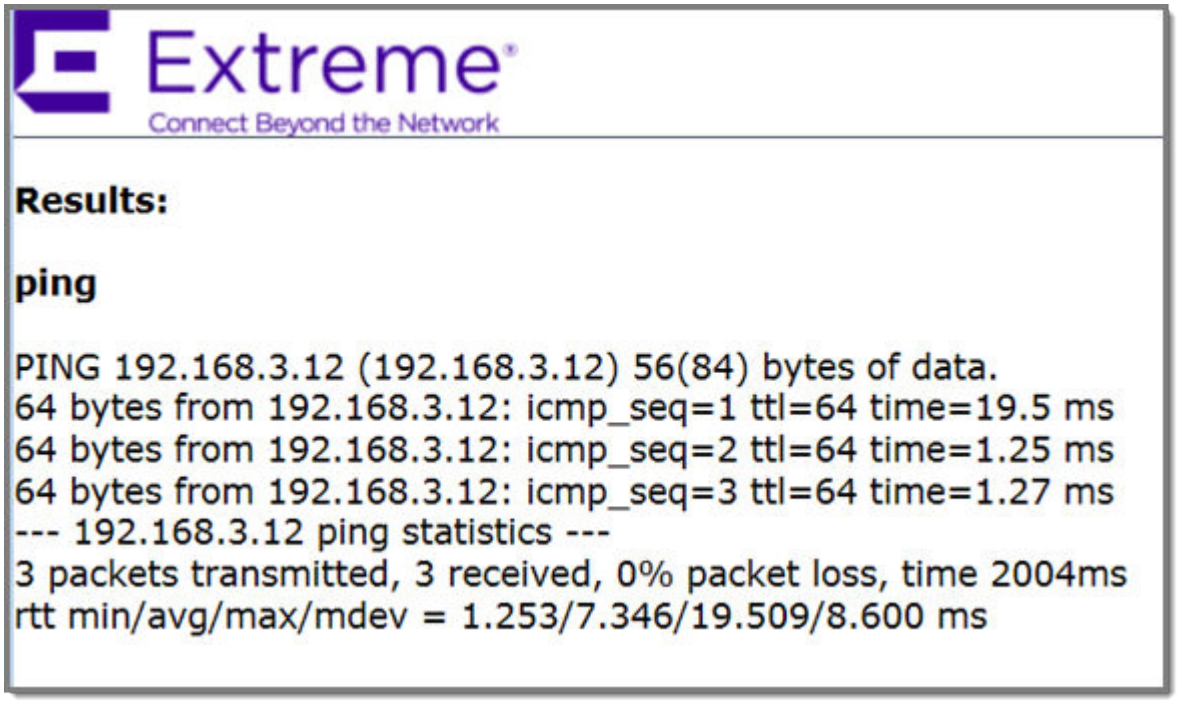
Figure 20: Wireless Controller Utilities Screen

3 In the **Target IP Address** box, type the IP address of the destination computer.

Note
The Target IP address supports both IPv4 and IPv6 addresses.

4 To test a connection to the target IP address, click **Ping**.

A window displays with the ping results. The following is an example:



5 To record the route through the Internet between your computer and the target IP address, click **Trace Route**.

The following is an example of trace results.

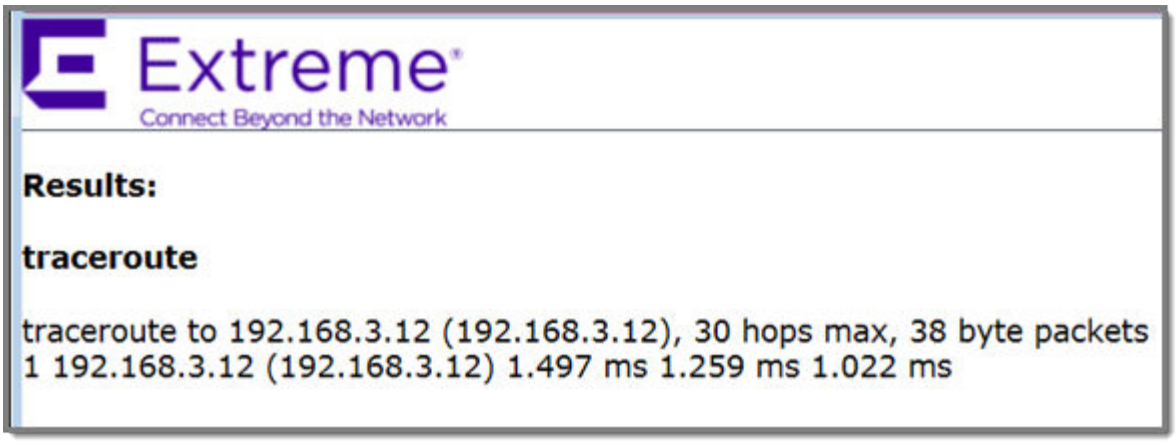


Figure 21: Wireless Controller TCP Dump Management

The wireless controller TCP dump management allows you to capture exception traffic that is sent to the management plane. Exception traffic is defined as traffic that is sent to the management plane from the data/control plane for special handling. For example, exception traffic can include *DHCP (Dynamic Host Configuration Protocol)*, *OSPF (Open Shortest Path First)*, and TFTP traffic.

When capturing exception traffic, you define the following:

- The physical or virtual *VNS (Virtual Networks Service)* port on which the captured exception traffic travels
- The name and size of the captured traffic file
  - When naming the file, the file name extension must be .cap.
  - 10 MB is the minimum and 1 GB is the maximum size of the captured traffic file.
- The location where the captured TCP dump file is saved

The captured traffic file is stored in a binary tcpdump-format file on the controller or flash card. The captured traffic file can then be exported to a local machine for packet analysis and opened with a traffic analysis tool. For example, Wireshark.

The controller can only store one captured traffic file locally. Alternately, if you choose to save the captured traffic file on a flash card, the available space on the flash card will dictate how many captured traffic files you can save.

Capturing Exception Traffic

1 From the top menu, click **Controller**.
2 In the left pane, click **Network** > **Utilities**.

The **Wireless Controller Utilities** screen is displayed.

3 In the **Tcpdump Management Port** drop-down list, click the port on which the exception traffic travels that you want to capture.

4 In the **Filename** box, type the name for the captured traffic file. The default name is **mgmt_traffic_dump.cap**.
5 In the **Capture File Size (MB)** box, type the maximum size for the captured traffic file. 10 MB is the minimum and 1 GB is the maximum size of the captured traffic file.
6 If applicable, in the **Destination** drop-down list, select one of the following:
   - Flash – Click to save the file on the flash card.
   - Local – Click to save the file locally on the controller.

Note
The Destination drop-down list is only available if the controller has a mounted flash device. For more information, see Working with an External Storage Device on page 52.

7 Click **Start**. A dialog is displayed informing you the previously captured file will be removed.
8 To continue with the exception traffic capture, click **OK**. A dialog is displayed informing you the capture has started.

   If applicable, to stop the capture before it is completed, click Stop.

   To export an Exception Traffic Capture File:
9 From the top menu, click **Controller**.
10 In the left pane, click **Network** > **Utilities**.

   The **Wireless Controller Utilities** screen is displayed.
11 In the **Capture Files on System** drop-down list, click the capture file you want to export, and then click **Export**.

   A File Download dialog is displayed asking you where you want to save the file.
12 Click **Save**.
13 Navigate to the location on your network where you want to save the file, and then click **Save**.

Enabling SNMP

The Wireless Controller, Access Points and Convergence Software system supports *SNMP (Simple Network Management Protocol)*, Version 1 and 2c and Version 3.

Note
Due to the lack of a standard .11n MIB, the SNMP protocol does not provide full support for Wireless 802.11n AP attributes.

MIB Support

The wireless controller software accepts *SNMP* get commands and generates Trap messages for the following set of MIBs:

- SNMPv2-MIB
- IF-MIB
- IEEE802dot11-MIB
- RFC1213-MIB

The Siemens Enterprise MIB includes:

- HIPATH-WIRELESS-EWC-MIB
- HIPATH-WIRELESS-PRODUCTS-MIB
- HIPATH-WIRELESS-SMI.my
- HIPATH-WIRELESS-DOT11-EXTNS-MIB
- HIPATH-WIRELESS-BRANCH-OFFICE-MIB

The MIB is provided for compilation into an external NMS. No support has been provided for automatic device discovery by an external NMS.

The controller is the only point of SNMP access for the entire system. In effect, the controller proxies sets, gets, and alarms from the associated wireless APs.

NetSight Suite Integration

The Wireless Controller, Access Points and Convergence Software system now support get and set for a number of proprietary MIBs that are listed below. By using the Netsight Suite and the following MIBs, you can configure the controller to create and manage policy, *VNS*, *VLAN (Virtual LAN)*; backup and restore configurations.

- set support
  - EXTREME-CONFIGURATIONMANAGEMENT-MIB
  - EXTREME-RADIUS-ACCT-CLIENT-EXT-MIB ('set' supported for this MIB except scalar elements)
  - EXTREME-RADIUS-AUTH-CLIENT-MIB ('set' supported for this MIB except scalar elements)
  - EXTREME-POLICY-PROFILE-MIB (not all tables supported)
  - EXTREME-CLASS-OF-SERVICE-MIB (not all tables supported)
  - Q-BRIDGE-MIB (dot1qVlanStaticTable only)
- get support
  - BRIDGE-MIB (dot1dBasePortTable)

Use these MIBs to perform controller hardware and software resets, including backing up and restoring controller configurations via the NetSight Suite. *SNMP* must be enabled on the controller for NetSight Suite integration.

For more information on NetSight suite integration, see the *User Guide*.

Enabling SNMPv1/v2c on the Wireless Controller

You can enable SNMPv1/v2c or SNMPv3 on the wireless controller to retrieve statistics and configuration information.

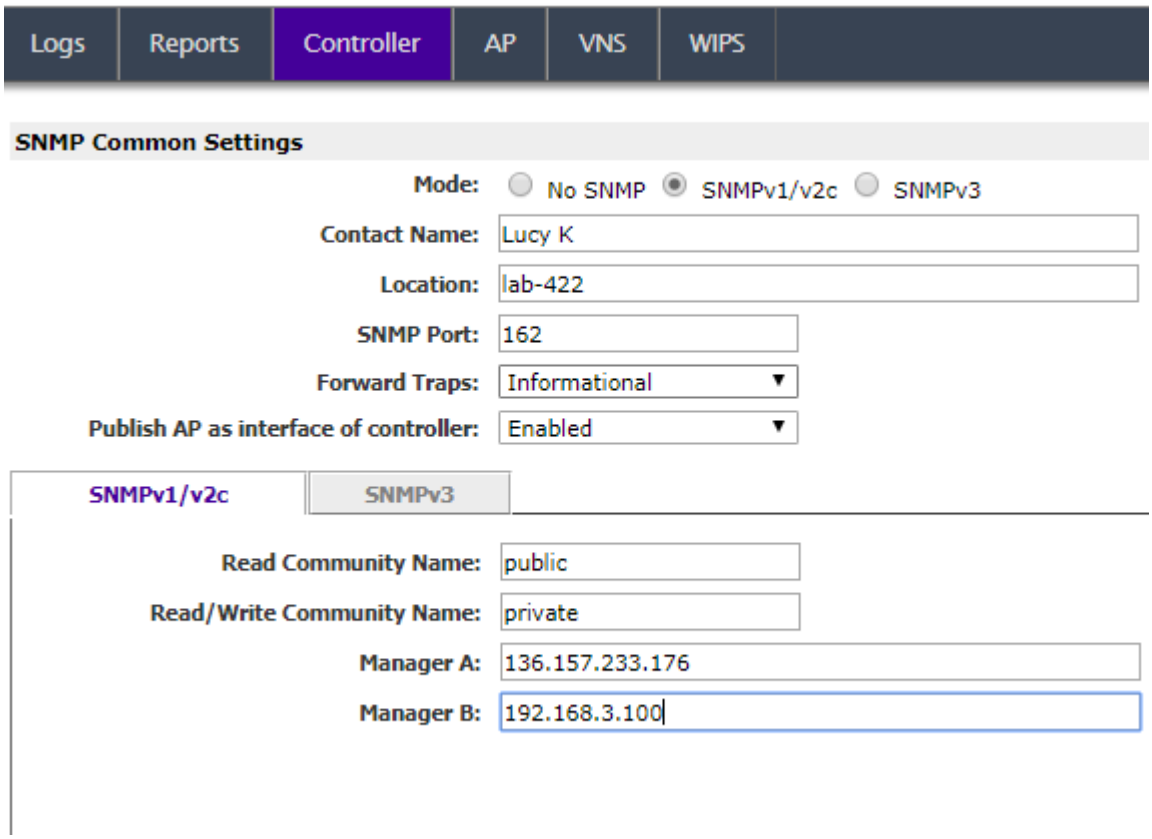
For information on editing or deleting SNMPv3 user accounts, see Editing SNMPv3 User Accounts on page 88 and Deleting SNMPv3 User Accounts on page 90.

To enable SNMPv1/v2c parameters:

1 From the top menu, click **Controller**.

2 In the left pane, click **Network** > **SNMP**.

The **SNMP Common Settings** screen is displayed.



3 To enable *SNMP*, select the **SNMPv1/v2c Mode** option.

4 Type the following information:

- **Contact Name** – Specifies the name of the SNMP administrator.
- **Location** – Specifies the location of the SNMP administration.
- **SNMP Trap Port** – Specifies the destination port for SNMP traps. The industry standard is 162. If left blank, no traps are generated.

5 In the **Forward Traps** drop-down list, click the security level of the traps to be forwarded: **Informational**, **Minor**, **Major**, or **Critical**.

6 In the **Publish AP as interface of controller** drop-down list, click to enable or disable publishing the wireless AP and their interfaces as interfaces of the controller. By default this option is enabled.

When this option is enabled, all wireless APs and their interfaces are published as interfaces of the controller when you retrieve topology statistics and configuration information using SNMP.

Topology statistics and configuration information on wireless APs are retrievable using both proprietary and standard MIBs. The Publish AP as interface of controller option only affects information retrieved through standard MIBs, i.e. IF-MIB, RFC1213. All information that is retrieved through proprietary MIBs is not affected. If the Publish AP as interface of controller option is disabled, the wireless APs' interfaces are not considered interfaces of the controller.

For example, if the Publish AP as interface of controller option is disabled, querying the ifTable would return information on the controller physical interfaces, plus all VNSs that are configured on that controller. If enabled, querying the same table would return the above information, in addition to information on each wireless APs' interfaces.

7 In the **SNMP v1/v2c** section, type the following:

- **Read Community Name** – Specifies the community name password for users with read privileges.
- **Read/Write Community Name** – Specifies the community name password for users with read and write privileges.
- **Manager A** – Specifies the IP address of the server on the network where the SNMP traps are monitored.
- **Manager B** – Specifies the IP address of a second server on the network where the SNMP traps are monitored.

Warning
For security purposes, it is recommended that you immediately change the Read Community Name (public) and the Read/Write Community Name (private) passwords to names that are less obvious and more secure.

8 To save your changes, click **Save**.

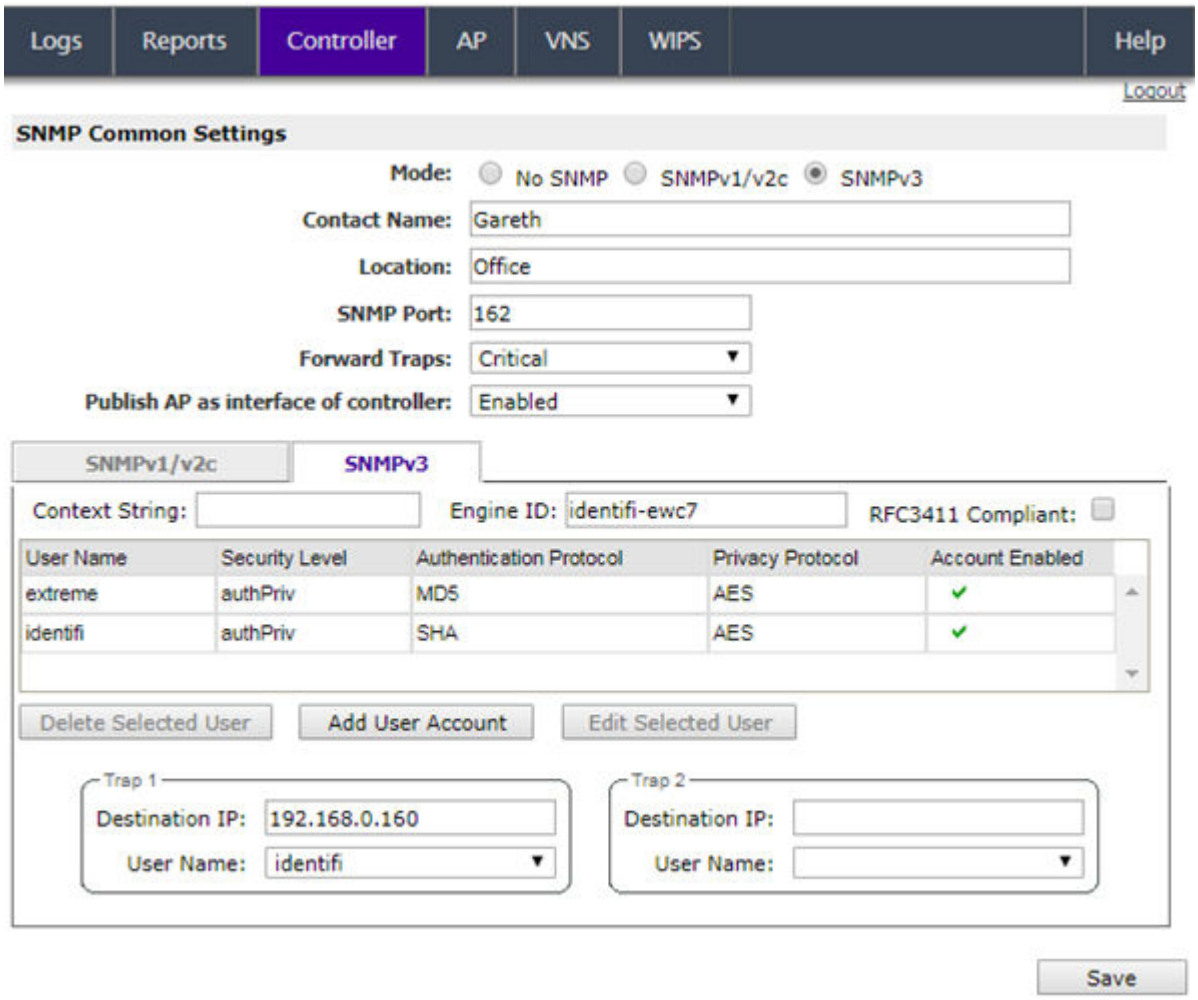
Enabling SNMPv3

To enable SNMPv3 parameters:

1 From the top menu, click **Controller**.

2 In the left pane, click **Network** > **SNMP**.

The **SNMP Common Settings** screen is displayed.



3 To enable *SNMP*, select the **SNMPv3 Mode** option.

4 Type the following information:

- **Contact Name** – Specifies the name of the SNMP administrator.
- **Location** – Specifies the location of the SNMP administration.
- **SNMP Trap Port** – Specifies the destination port for SNMP traps. The industry standard is 162. If left blank, no traps are generated.

5 In the **Forward Traps** drop-down list, click the security level of the traps to be forwarded: **Informational**, **Minor**, **Major**, or **Critical**.

6 In the **Publish AP as interface of controller** drop-down list, click to enable or disable publishing the wireless AP and their interfaces as interfaces of the controller. By default this option is enabled.

When this option is enabled, all wireless APs and their interfaces are published as interfaces of the controller when you retrieve topology statistics and configuration information using SNMP.

Topology statistics and configuration information on wireless APs are retrievable using both proprietary and standard MIBs. The Publish AP as interface of controller option only affects information retrieved through standard MIBs, i.e. IF-MIB, RFC1213. All information that is retrieved through proprietary MIBs is not affected. If the Publish AP as interface of controller option is disabled, the wireless APs' interfaces are not considered interfaces of the controller.

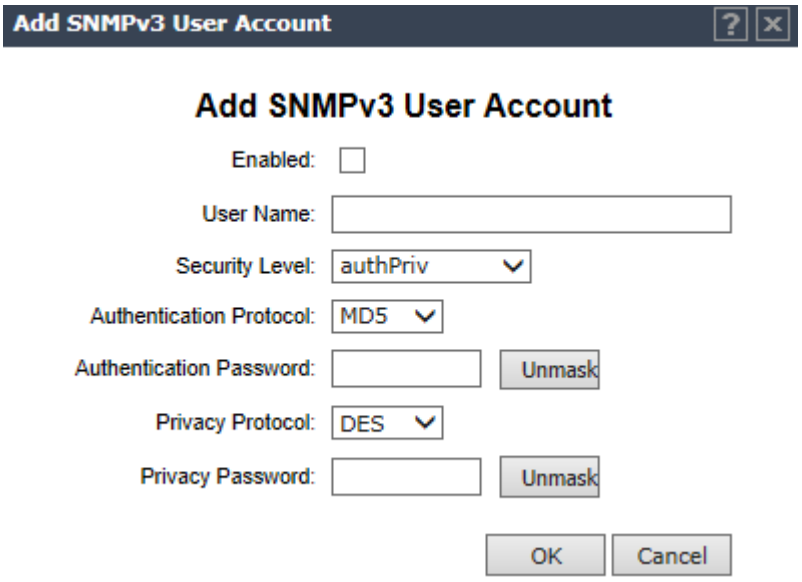
For example, if the Publish AP as interface of controller option is disabled, querying the ifTable would return information on the controller physical interfaces, plus all VNSs that are configured on that controller. If enabled, querying the same table would return the above information, in addition to information on each wireless APs' interfaces.

7 In the **SNMP v3** section, type the SNMP engine ID in **Engine ID**. The SNMP engine ID is a 5 – 32 character ID for the **EWC** SNMP agent. Do not use spaces, control characters, or tabs.

8 Add user accounts.

a Click **Add User Account**.

The Add SNMPv3 User Account screen is displayed.



b Select **Enabled** to enable the user.

c In User Name, type a user name.

d In the Security Level drop-down list, select the appropriate security level for the user: authPriv, authNoPriv, NoAuthNoPriv.

If NoAuthNoPriv is selected, click **OK** and go to the next step.

e In the Authentication Protocol drop-down list, select the authentication protocol: None, *MD5 (Message-Digest algorithm 5)*, SHA.

f In Authentication Password, type the password, which must be at least eight characters long. If desired, click Unmask to display the password in plain text.

If authNoPriv is the selected security level, click **OK** and go to the next step.

g In the Privacy Protocol drop-down list, select the encryption protocol: None, DES.

h In Privacy Password, type the password, which must be at least eight characters long. If desired, click Unmask to display the password in plain text.

i Click **OK** to save the user account information. The SNMP Common Settings screen is displayed.

9 In **Trap 1 Destination IP** and **Trap 2 Destination IP**, type the IP addresses of the servers on the network where the SNMP traps are monitored.

10 In the **Trap 1 User Name** and **Trap 2 User Name** drop-down lists, select the user name associated with the Trap 1 and Trap 2 destination servers. Only enabled users appear in these drop-down lists.

11 To save your changes, click **Save**.

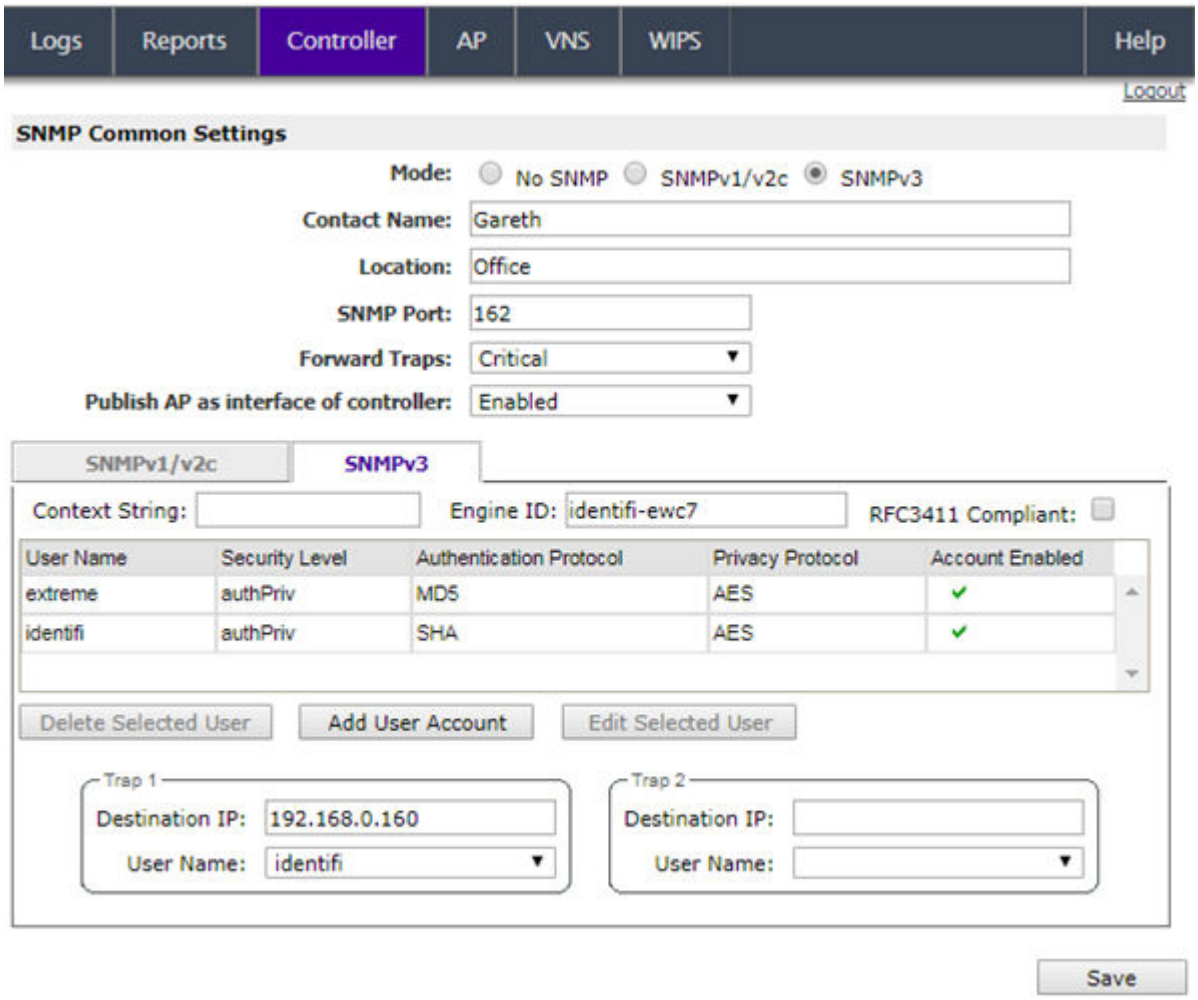
Editing SNMPv3 User Accounts

To edit SNMPv3 user accounts:

1 From the top menu, click **Controller**.

2 In the left pane, click **Network** > **SNMP**.

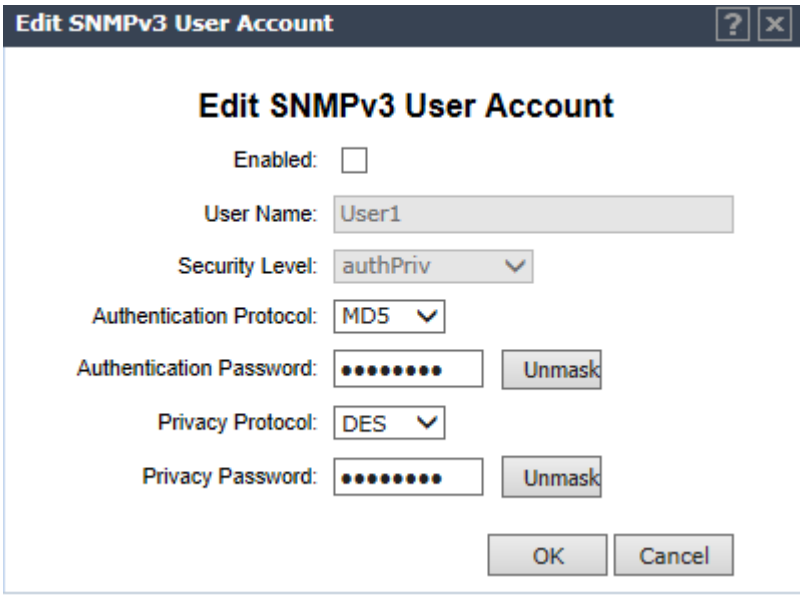
The **SNMP Common Settings** screen is displayed.



3 In the **SNMP v3** section, select a user account.

4 Click **Edit Selected User**.

The **Edit SNMPv3 User Account** screen is displayed.



You can change the setting of the Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password, depending upon how the user account's security level is set.

5 In the **Authentication Protocol** drop-down list, select the authentication protocol: **MD5**, **SHA**.

6 In **Authentication Password**, type the password, which must be at least eight characters long. If desired, click **Unmask** to display the password in plain text.

7 In the **Privacy Protocol** drop-down list, select the encryption protocol: **DES**.

8 In **Privacy Password**, type the password, which must be at least eight characters long. If desired, click **Unmask** to display the password in plain text.

9 Click **OK** to save the user account information.

10 To save your changes, click **Save**.

Deleting SNMPv3 User Accounts

To delete SNMPv3 user accounts:

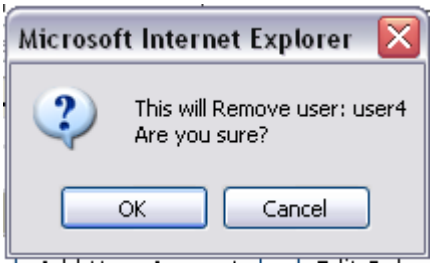
1 From the top menu, click **Controller**.

2 In the left pane, click **Network** > **SNMP**.

3 In the **SNMP v3** section, select a user account.

4 Click **Delete Selected User**.

A warning is displayed.



5 Click **OK** to delete the user account.
6 To save your changes, click **Save**.

9 Recovering the Wireless Controller

Rescue Mode Authentication Service Management Menu

Use Rescue mode's Authentication Service Management menu to do the following on the wireless controller:

- Set login mode to local
- Reset accounts and passwords to factory default
- Change administrator password

To use Rescue Mode's Authentication Service Management menu:

1 Connect to the console port. Do not use the ESA ports or the Admin management port. For more information, see Using the Console Port on page 58.

2 Reboot the system.

The following menu appears during the reboot process.

```
------------------------------------------------------------
Controller
Controller Rescue
------------------------------------------------------------
```

3 Select the **Rescue Mode**, and then press **[Enter]**.

The Rescue Start-up Menu appears.

```
Rescue Start-up Menu. Use with extreme caution.
1) Force System Recovery
2) Create System Backup Image
3) Display Backup Images
4) FTP Menu
5) Network Interface Menu
6) Manually run File System Check Utility (fsck)
7) Restore Backup Image directly from the FTP server
8) Authentication Service Management Menu
9) Flash Menu
R) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the selected
image (either backup or factory).
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice:
```

4 Type 8.

The Authentication Service Management menu displays.

```
Authentication Service Management Menu
======================================
1) Set Login Mode to Local
2) Reset Accounts and Passwords to Factory Default
3) Change administrator password
B) Return back to main menu
Please enter your choice:
```

5 Type the sequence number of the appropriate option, given in the **Authentication Service Management** menu.

- Set Login Mode to Local – Type 1 if the login authentication mode was set to *RADIUS (Remote Authentication Dial In User Service)*-based authentication, and you want to revert to the local login authentication mode.
- Reset Accounts and Passwords to Factory Default – Type 2 if you want to reset the login accounts and password to factory defaults.
- Change administrator password – Type 3 if you want to change the administrator's password.
- Return back to main menu – Type B if you want to return to the main menu.

6 After you have used any of the first three options in the **Authentication Service Management** menu, type B to return to the main menu.

```
Rescue Start-up Menu. Use with extreme caution.
1) Force System Recovery
2) Create System Backup Image
3) Display Backup Images
4) FTP Menu
5) Network Interface Menu
6) Manually run File System Check Utility (fsck)
7) Restore Backup Image directly from the FTP server
8) Authentication Service Management Menu
9) Flash Menu
R) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the selected
image (either backup or factory).
Reboot will restart the system back into Normal mode.
```

7 Type R. The system restarts into normal mode.

Recovering the Wireless Controller from File System Corruption

A power outage can, in rare cases cause file system corruption to the wireless controller. If file system corruption occurs, the controller might not be able to start up and provide service. This section describes how to recover the controller in such a situation.

To recover the controller from file system corruption:

1 Connect to the console port. Do not use the ESA ports or the Admin port. For more information, see Using the Console Port on page 58.

2 Monitor the console output of the system startup. In case there are file system corruptions, you will see similar output containing unexpected file system inconsistency with a request for the manual actions.

```
INIT: version 2.86 booting
Starting the hotplug events dispatcher: udevd.
Synthesizing the initial hotplug events...done.
Waiting for /dev to be fully populated...done.
Mounting readonly root filesystem...done.
Checking root file system...fsck 1.40 (29-Jun-2007)
/dev/hda2 has gone 14817 days without being checked, check forced.
Inodes that were part of a corrupted orphan linked list found.
/dev/hda2: UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.(i.e., without -a or -p options)
fsck failed (exit code 4). Please repair manually and reboot.
Please note that the root file system is currently mounted read-only.
To remount it read-write:
 # mount -n -o remount,rw /
CONTROL-D will exit from this shell and REBOOT the system.
```

```
Give root password for maintenance
(or type Control-D to continue):
```

3 Type the main admin password to log into the wireless controller.

The command prompt displays.

4 Use the `fsck.ext3` command to recover the file system partition, where `/dev/hda2` is a problematic partition name from the output above.

```
bash-3.00# fsck.ext3 -fycv /dev/hda2
```

5 After the recovery completes, use the `reboot` command to reboot the system.

```
e2fsck 1.40 (29-Jun-2007)
Checking for bad blocks (read-only test): done
Pass 1: Checking inodes, blocks, and sizes
Inodes that were part of a corrupted orphan linked list found. Fix? yes
Inode 17765 was part of the orphaned inode list. FIXED.
Inode 17786 was part of the orphaned inode list. FIXED.
Inode 64432 was part of the orphaned inode list. FIXED.
Inode 64433 was part of the orphaned inode list. FIXED.
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/hda2: ***** FILE SYSTEM WAS MODIFIED *****
/dev/hda2: ***** REBOOT LINUX *****
 12087 inodes used (15.61%)
 83 non-contiguous inodes (0.7%)
 # of inodes with ind/dind/tind blocks: 636/5/0
 83316 blocks used (53.88%)
 0 bad blocks
 0 large files
 10967 regular files
 742 directories
 2 character device files
 0 block device files
 6 fifos
 1418 links
 359 symbolic links (359 fast symbolic links)
 2 sockets
--------
13496 files
bash-3.00# reboot
```

Following the reboot, the wireless controller should proceed with the normal startup.

10 Maintaining the Wireless Controller

Maintaining the C35 Controller
Maintaining the C5210 Controller
Maintaining the C5215 Controller

Maintaining the C35 Controller

This topic outlines the features of the C35 controller.

Related Links

C35 Front Panel Features on page 95
C35 Back Panel Features on page 96

C35 Front Panel Features

The figure below depicts the chassis front panel of the C35. C35 System Status LEDs describes the C35 system status LED functions.

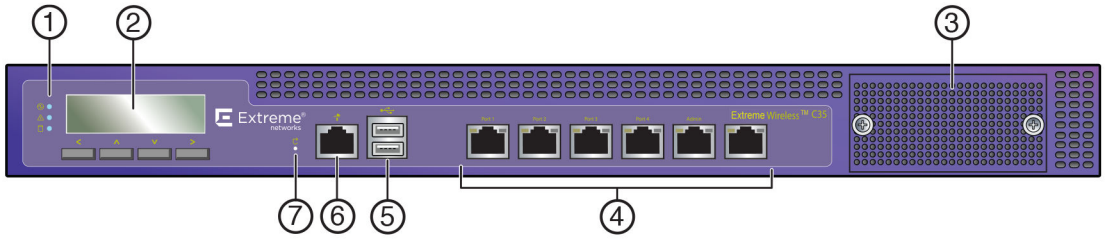


Figure 22: C35 Front Panel Features

1	System Status LEDs	5	USB Port
2	LCD Panel	6	Console Port
3	Not Used	7	Reset Switch
4	Ethernet Ports (see Figure 23)		

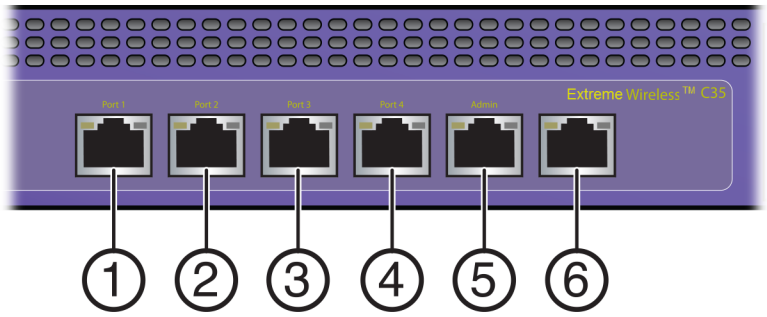


Figure 23: C35 Ethernet Ports

1	Data Port 1: 1GbE (esa0)	4	Data Port 4: 1GbE (esa3)
2	Data Port 2: 1GbE (esa1)	5	Mgmt Port: 1GbE (eth0)
3	Data Port 3: 1GbE (esa2)	6	Not used, plugged

Table 11: C35 System Status LEDs

LED	Function
	Power: When this LED is on, it indicates power is supplied to the WS-C35 power supply unit. This LED should be illuminated when the system is operating
	Status: When lit Green, it indicates operational state is normal. When lit Red, it indicates a system malfunction.
	Hardisk (HDD): When this LED flashes, it indicates hard drive activity. Otherwise, the LED remains off.

C35 Back Panel Features

The following figure depicts the C35 back panel. C35 Management and Data Port LEDs describes the management and data port LED functions.

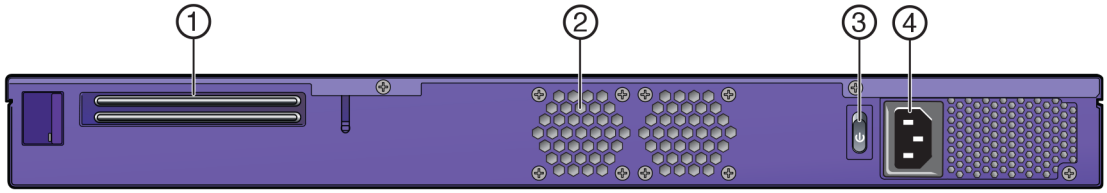


Figure 24: C35 Back Panel Features

1	Not Used	3	Power Switch
2	CPU-Fan	4	AC Power Socket

Table 12: C35 Management and Data Port LEDs

Port	LED	Function
Management	Network speed	Off = 10Mbs
		Green = 100Mbs
		Amber = 1000Mbs
Management	Activity/Link	Off = No Link
		Green = Active Link
		Blinking Amber = Network Activity

Maintaining the C5210 Controller

This topic outlines the features of the C5210 controller.

Related Links

C5210 Front Panel Features on page 97
C5210 Front Control Panel Features on page 98
C5210 Back Panel Features on page 99

C5210 Front Panel Features

Figure 25 depicts the front panel of the C5210. Table 13 depicts the features and functions of the C5210 front panel.

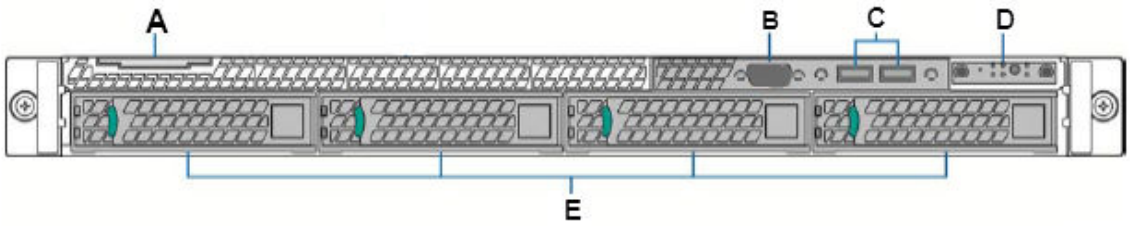


Figure 25: C5210 Front Panel Features

Table 13: C5210 Front Panel Features

Callout	Feature	Function
A	System Label Pull-out	
B	Not used	
C	USB Ports	Connects USB 2.0-compliant devices to the system. For more information, see the Note below.

Table 13: C5210 Front Panel Features (continued)

Callout	Feature	Function
D	Front Control Panel	For more information, see Figure 26 on page 98.
E	Hard Disk Drive Bays	Only left one used.

Note

The C5210 is equipped with 5 USB connectors—2 on the front panel and 3 on the back panel. However, the controller is capable of supporting only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

Related Links

C5210 Front Control Panel Features on page 98
C5210 Back Panel Features on page 99

C5210 Front Control Panel Features

This section highlights the control panel features on the front of the C5210. See callout D in Table 13 on page 97. See Table 14 for a description of each control.

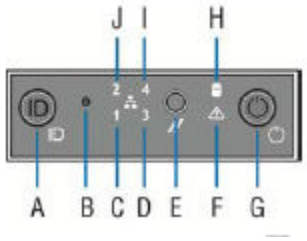


Figure 26: C5210 Front Control Panel Features

Table 14: C5210 Front Control Panel Features

Callout	Feature	Function
A	System ID Button w/Integrated LED	The identification buttons on the front panel can be used to locate a particular system within a rack. When one of the buttons is pushed, the blue system status indicator on the front and back blinks until one of the buttons is pushed again.
B	NMI Button	Not used
C	Mgmt Port Activity LED	For more information, see Table 15 on page 99.
D	Data Port 2 Activity LED	For more information, see Table 15 on page 99.
E	System Cold Reset Button	
F	System Status LED	The blue-colored system status indicator blinks to indicate the location of a particular system within a rack. The indicator continues to blink until one of the system identification button is pushed again.

Table 14: C5210 Front Control Panel Features (continued)

Callout	Feature	Function
G	Power Button w/Integrated LED	The power button controls the DC power supply output to the system.
H	Hard Drive Activity LED	LED Off - Power on and drive spinning up or spinning down/No access or no faults
		Blinking Green - Power on with drive activity
		Solid Amber - Hard drive fault has occurred
I	Data Port 4 Activity LED	Not used
J	Data Port 1 Activity LED	For more information, see the following table.

Table 15: RJ45 Port LEDs (Management Port, Data Port 1, Data Port 2)

LED Type	LED Pattern	Status Indication
Network Speed (Right)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Link Activity (Left)	Off	No link
	Solid Green	Active link
	Blinking Green	Data traffic activity
LED Type	LED Pattern	Status Indication

Related Links

C5210 Front Panel Features on page 97
C5210 Back Panel Features on page 99

C5210 Back Panel Features

Figure 27 displays back panel features of the C5210. Table 16 depicts the features and functions of the C5210 back panel.

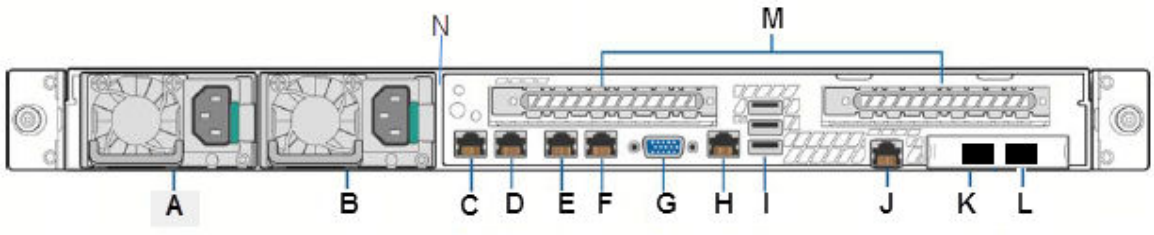


Figure 27: C5210 Back Panel Features

Table 16: C5210 Back Panel Features

Callout	Feature	Function
A	AC Power Supply 1	AC Power Supply 1 and 2 combine to make a redundant power supply.
B	AC Power Supply 2	
C	1GbE RJ45	Management port – eth0
D	1GbE RJ45	Data port 1 – esa0
E	1GbE RJ45	Data port 2 – esa1
F	Port 4	Not used
G	Video Connector	Used to see POST BIOS information during controller boot up
H	Serial-A Port RJ45	Console Port – Used to get into Rescue mode.
I	USB Ports	Connects USB 2.0-compliant devices to the system. For more information, see the Note below.
J	RMM4 NIC Port	Not used, plugged
K	1/10GbE SFP+	Data port 4 – esa3
L	1/10GbE SFP+	Data port 3 – esa2
M	Expansion slots.	Not used
N	Chassis tab	Used for optional cable bracket.

Note

The C5210 is equipped with 5 USB connectors — 2 on the front panel and 3 on the back panel. However, the controller is capable of supporting only one USB device at a time, regardless of what USB connector the device is connected to. If you connect a second USB device while the first is already connected, the system will return an error.

Related Links

C5210 Front Panel Features on page 97
C5210 Front Control Panel Features on page 98

Maintaining the C5215 Controller

This topic outlines the features of the C5215 controller.

Related Links

C5215 Front Panel Features on page 100
C5215 Front Control Panel Features on page 101
C5215 Back Panel Features on page 103

C5215 Front Panel Features

The following figure depicts the front panel of the C5215. Table 17 depicts the features and functions of the C5215 front panel.

Figure 28: C5215 Front Panel Features

Table 17: C5215 Front Panel Features

Callout	Feature	Function
1	Hard Disk Drive Bays	Holds hard disks.
2	Front Video Port	Connects VGA cable.
3	USB Ports	Connects USB 2.0 and 3.0 compliant devices to the system. For more information, see the Note below.

Note
Although the appliance has five USB connectors (two on the front panel and three on the back panel), only one USB connector can be used at a time.

Related Links

C5215 Front Control Panel Features on page 101
C5215 Back Panel Features on page 103

C5215 Front Control Panel Features

This section highlights the control panel features on the front of the C5215. See Table 18 for a description of each control.

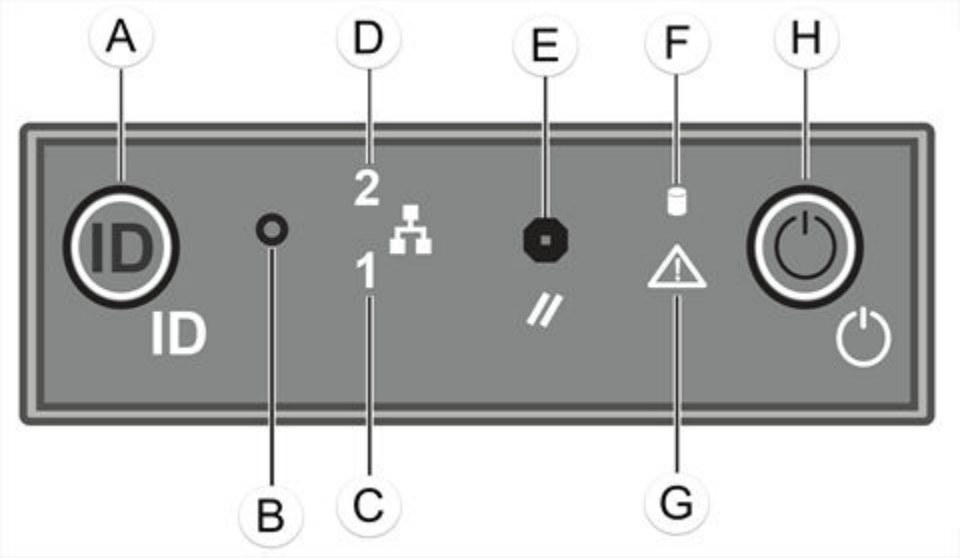


Figure 29: C5215 Front Control Panel Features

Table 18: C5215 Front Control Panel Features

Callout	Feature	Function
A	System ID Button w/Integrated LED	The identification buttons on the front panel can be used to locate a particular system within a rack. When one of the buttons is pushed, the blue system status indicator on the front and back blinks until one of the buttons is pushed again.
B	NMI Button	
C	Mgmt Port Activity LED	For more information, see Table 15 on page 99.
D	Data Port 2 Activity LED	For more information, see Table 15 on page 99.
E	System Cold Reset Button	
F	Drive Activity LED	The blue-colored system status indicator blinks to indicate the location of a particular system within a rack. The indicator continues to blink until one of the system identification button is pushed again.
G	System Status LED	The blue-colored system status indicator blinks to indicate the location of a particular system within a rack. The indicator continues to blink until one of the system identification button is pushed again.
H	Power Button w/Integrated LED	The power button controls the DC power supply output to the system.
		Blinking Green - Power on with drive activity
		Solid Amber - Hard drive fault has occurred

Table 19: RJ45 Port LEDs (Management Port, Data Port 1, Data Port 2, Data Port 3, Data Port 4)

LED Type	LED Pattern	Status Indication
RJ45 Port LEDs (Management Port)		
Network Speed (Right)	Off	10 Mbps
	Amber	100 Mbps
	Green	1000 Mbps
Link Activity (Left)	Off	No link
	Solid Green	Active link
	Blinking Green	Data traffic activity
Port LEDs (Data Ports 1 and 2)		
Network Speed (Right)	Off	10 Mbps
	Green	100 Mbps
	Amber	1000 Mbps
Link Activity (Left)	Off	No link
	Solid Green	Active link
	Blinking Green	Data traffic activity

Table 19: RJ45 Port LEDs (Management Port, Data Port 1, Data Port 2, Data Port 3, Data Port 4) (continued)

LED Type	LED Pattern	Status Indication
SFP+ Port LEDs (Data Ports 3 and 4)		
Network Speed (Right)	Off	Not used
	Amber	1 Gbps
	Green	10 Gbps
Link Activity (Left)	Off	No link
	Solid Green	Active link
	Blinking Green	Data traffic activity

Related Links

C5215 Front Panel Features on page 100
C5215 Back Panel Features on page 103

C5215 Back Panel Features

The following figure displays back panel features of the C5215. Table 20 depicts the features and functions of the C5215 back panel.

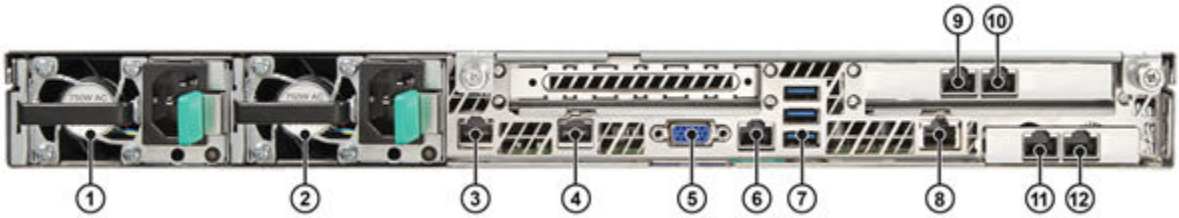


Figure 30: C5215 Back Panel Features

Table 20: C5215 Back Panel Features

Callout	Feature	Function
1	AC Power Supply 1	AC Power Supply 1 and 2 combine to make a redundant power supply.
2	AC Power Supply 2	
3	1GbE RJ45	Management port – eth0
4	Port 2	Not used, plugged
5	Video Connector	Used to see POST BIOS information during controller boot up
6	RJ45 Serial-A Port	Console Port – Used to get into Rescue mode.
7	USB Ports	Connects USB 2.0 and 3.0-compliant devices to the system. For more information, see the Note below.
8	RMM4 NIC Port	Not used, plugged
9	Data Port 1	1GbE RJ45(esa0)

Table 20: C5215 Back Panel Features (continued)

Callout	Feature	Function
10	Data Port 2	1GbE RJ45(esa1)
11	Data Port 3	1/10GbE SFP+(esa2)
12	Data Port 4	1/10GbE SFP+(esa3)

Related Links

C5215 Front Panel Features on page 100
C5215 Front Control Panel Features on page 101

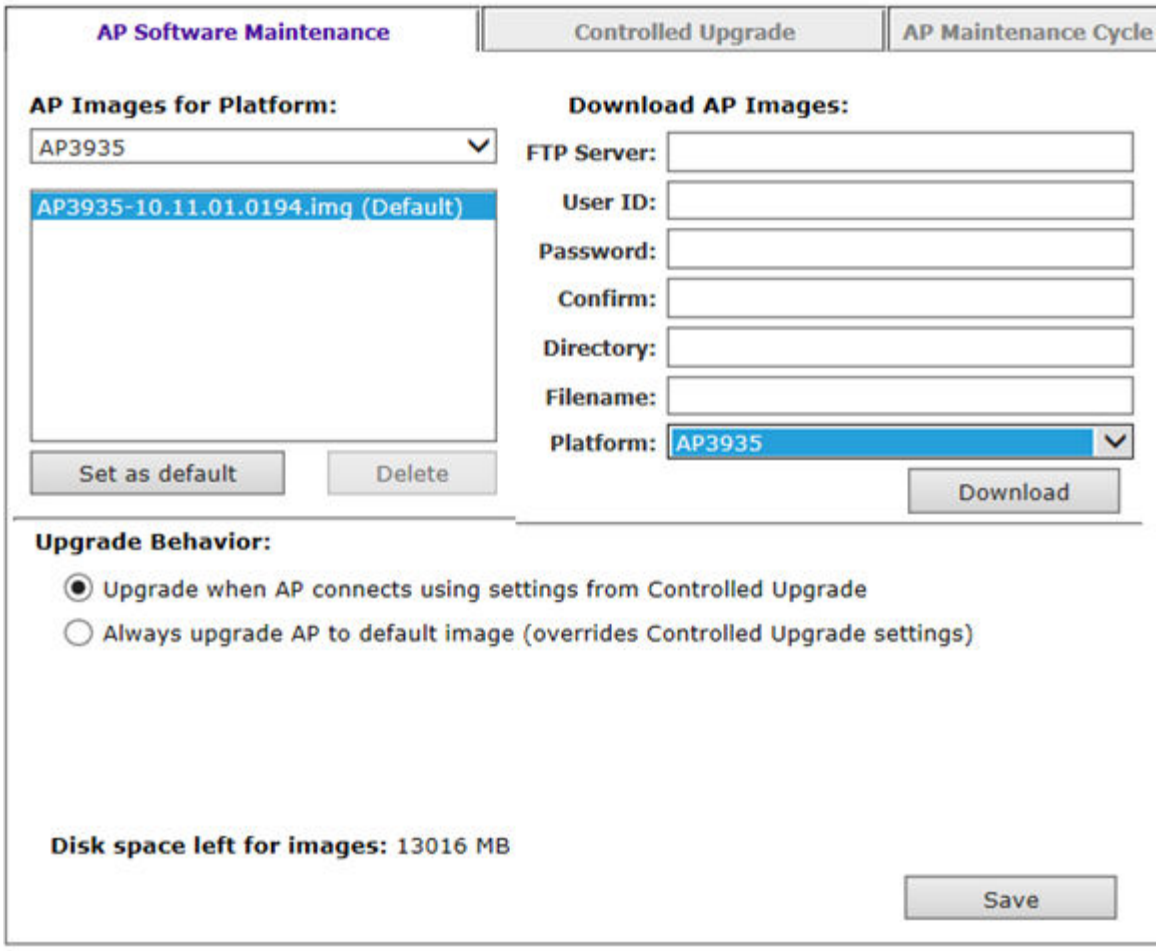
11 Maintaining the Wireless AP Software

Maintaining a List of Current Software Images

To maintain a list of current wireless AP software images:

1 From the top menu, click **AP**.

2 From the left pane, click **Global** > **Maintenance**.



3 In the **AP Images for Platform** drop-down list, click the appropriate platform.

4 To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.

5 In the **Upgrade Behavior** section, select one of the following:

- Upgrade when AP connects using settings from Controlled Upgrade – The **Controlled Upgrade** tab is displayed. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.
- Always upgrade AP to default image (overrides Controlled Upgrade settings) – Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.

6 To save your changes, click **Save**.

Deleting a Software Image

To delete a wireless AP software image:

1 From the top menu, click **AP**.
2 From the left pane, click **Global** > **Maintenance**.
3 In the **AP Images for Platform** drop-down list, click the appropriate platform.
4 In the **AP Images** list, click the image you want to delete.
5 Click **Delete**. The image is deleted.

Downloading a New Software Image

To download a new wireless AP software image:

1 From the top menu, click **AP**.
2 From the left pane, click **Global** > **Maintenance**.
3 In the **Download AP Images** list, type the following:
   - FTP Server – The IP address of the FTP server to retrieve the image file from.

     Note
     The FTP Server supports both IPv4 and IPv6 addresses.

   - User ID – The user ID that the controller should use when it attempts to log into the FTP server.
   - Password – The corresponding password for the user ID.
   - Confirm – The corresponding password for the user ID to confirm it was typed correctly.
   - Directory – The directory on the server in which the image file that is to be retrieved is stored.
   - Filename – The name of the image file to retrieve.
   - Platform – The AP hardware type to which the image applies. The are several types of APs and they require different images.
4 Click **Download**. The new software image is downloaded.

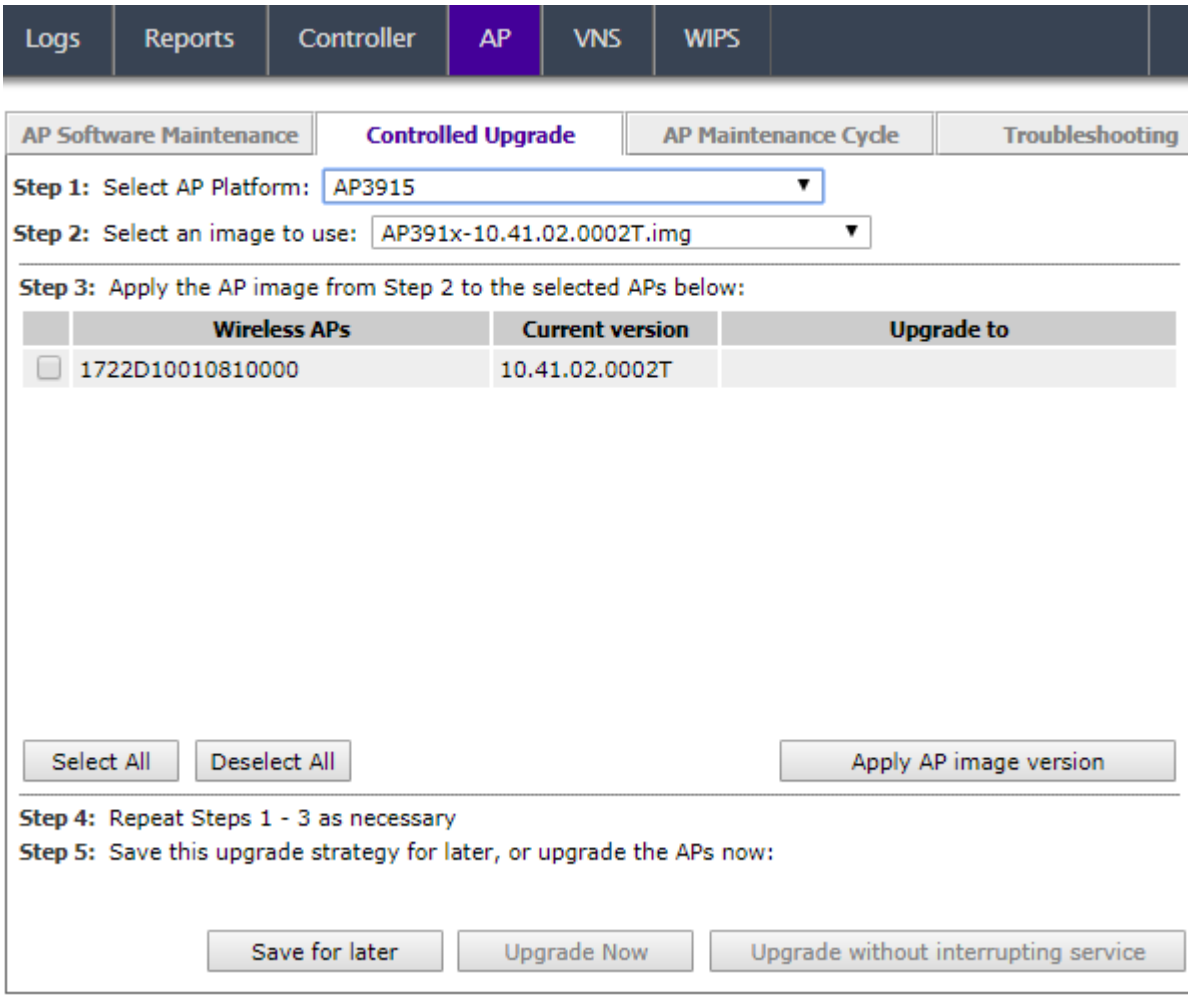
Defining Parameters for a Software Upgrade

To define parameters for a Wireless AP controlled software upgrade:

1 From the top menu, click **AP**.
2 In the left pane, click **Global** > **Maintenance**.
3 Under upgrade behavior, select **Upgrade when AP connects using settings from Controlled Upgrade**.

   The Controlled Upgrade tab displays.

4 Click the Controlled Upgrade tab.



Note
The Controlled Upgrade tab is displayed only when the Upgrade Behavior is set to **Upgrade when AP connects using settings from Controlled Upgrade** on the AP Software Maintenance tab.

5 In the **Select AP Platform** drop-down list, click the type of AP you want to upgrade.

6 In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.

7 In the list of registered **Wireless APs**, select the check box for each AP to be upgraded with the selected software image.

8 Click **Apply AP image version**. The selected software image is displayed in the **Upgrade To** column of the list.

9 To save the software upgrade strategy to be run later, click **Save for later**.

10 To run the software upgrade immediately, click **Upgrade Now**. The selected AP reboots, and the new software version is loaded.

Note
The Always upgrade AP to default image check box on the AP Software Maintenance tab overrides the Controlled Upgrade settings.

11 To upgrade without interrupting service, click **Upgrade without interrupting service**. If you click this option while the upgrade scheduler is running, the schedule is interrupted, and the current upgrade cycle calculates a new schedule that includes APs that weren't upgraded.

12 Performing Wireless AP Diagnostics

Use SSH and Remote Shell to perform diagnostics on traffic moving to and from APs in your network. You can also configure packet capture on selected APs.

Performing Wireless AP Diagnostics Using SSH

Caution
For security reasons, SSH is disabled by default. SSH should only be enabled to perform diagnostic sessions. When completed, SSH should always be disabled.

As a support tool to perform diagnostic debugging of the wireless AP, the capability to access the wireless AP by SSH has been provided. Normally, SSH are disabled and should be disabled again after diagnostics. This process should only be used by support services.

To configure the password for SSH access:

1 From the top menu, click **AP**.

2 From the left pane, click **Global** > **Registration**.

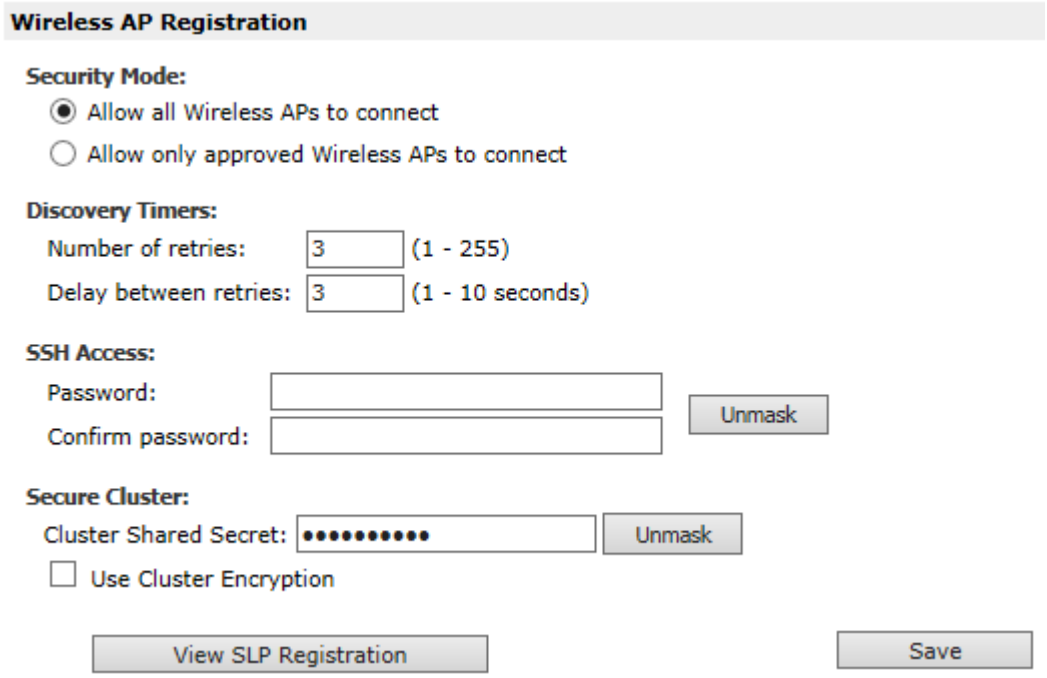


Figure 31: Wireless AP Registration Screen

3 If using SSH, in the **SSH Access** area, in the **Password** box, type the password for SSH access.

4 To confirm the password, in the **Confirm Password** box, re-type the password.

Note

When the controller ships from the factory it is configured with a default password to assign to the wireless APs that register with it. The default password is new2day. The password is sent to the wireless AP after it has registered. The administrator can override this password using the wireless AP Registration page in the user interface. For more information, see the *User Guide*.

5 To send the password information to all registered wireless APs, click **Save**.

Note

The admin password is modified in the wireless AP when a new password is saved for SSH access. SSH to wireless APs works via the console port only.

Enabling SSH on a Selected Wireless AP

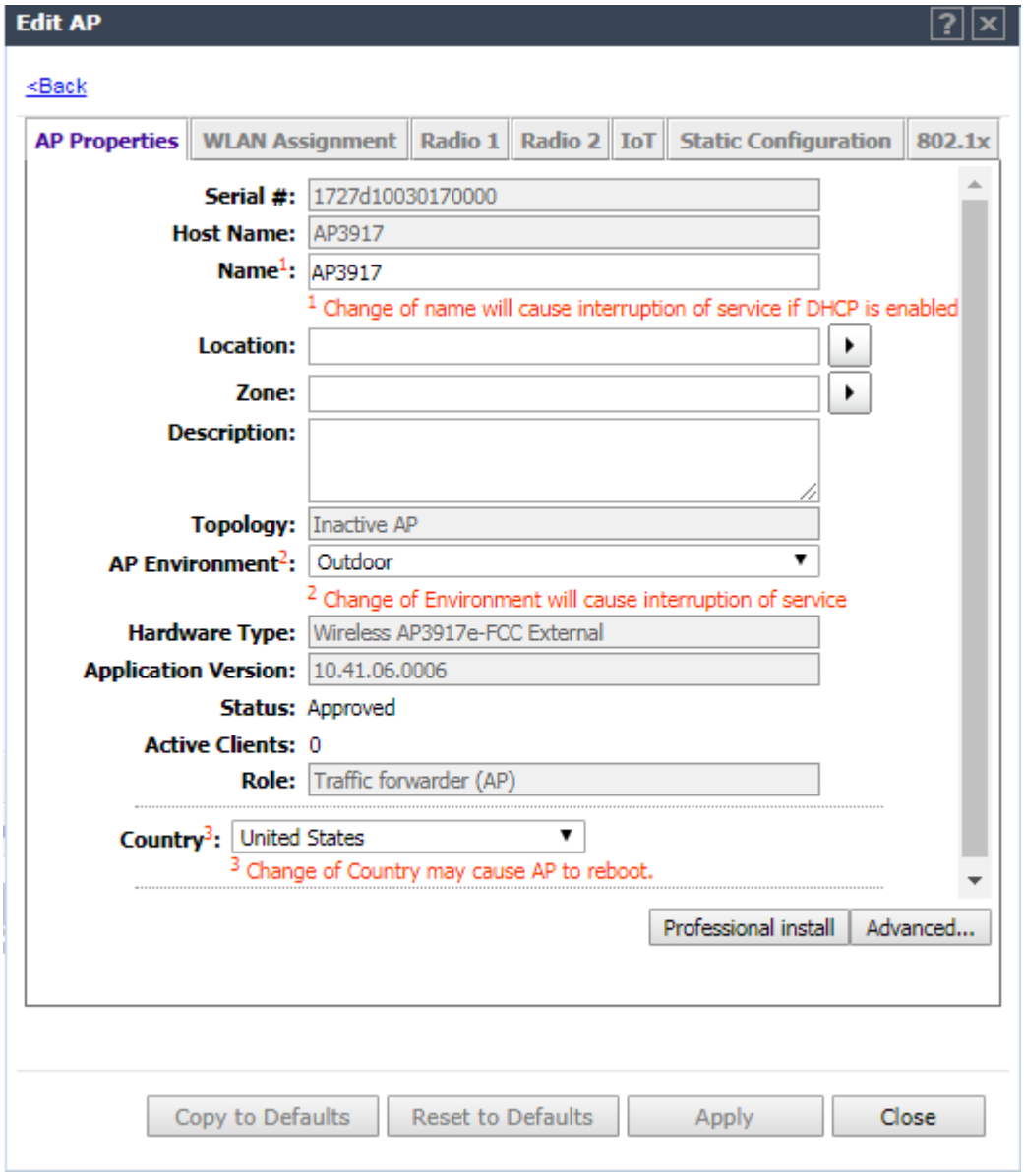
To enable SSH on a selected wireless AP:

1 From the top menu, click **AP**.

2 From the left pane, click **APs**.

3 Click the appropriate wireless AP in the list (not the check box). The AP dashboard displays.

4 Click **Configure**. The AP Properties tab displays.



5 Click **Advanced**.

6 Click the **Enable SSH Access** check box.

7 Click **Save**. This wireless AP is enabled for an SSH session.

Disabling SSH Access on a Selected AP

To disable SSH access:

1 From the top menu, click **AP**.

2 From the left pane, click **APs**.

3 Click the appropriate wireless AP in the list (not the check box). The AP dashboard displays.

4 Click **Configure**. The AP Properties tab displays.

5 Click **Advanced**, then clear the **Enable SSH Access** check box.
6 Click **Save**.

The wireless AP is disabled for the SSH sessions.

Opening Live SSH Console to a Selected AP

Note
By default, SSH is disabled for security reasons. However, to remotely access an AP's console, enable SSH on the AP. Ensure SSH is enabled before proceeding further.

ExtremeWireless provides a remote console to enable diagnostic debugging of wired and wireless APs. Use the remote console to open a live SSH console session to an AP and troubleshoot using the built-in commands, such as ping and traceroute. You can initiate remote console on both local and remote APs configured behind a firewall.

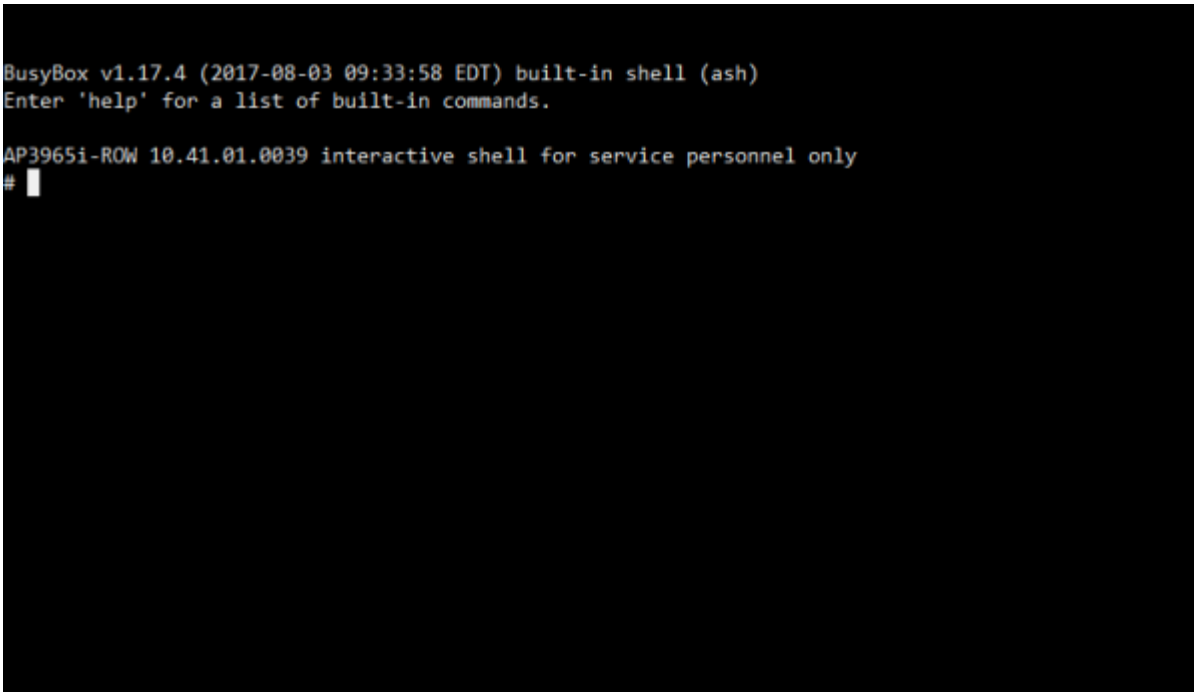
To open a remote console to an AP:

1 From the top menu, click **AP**.
2 From the left pane, click **Global** > **Maintenance**.

The AP Software Maintenance screen displays.

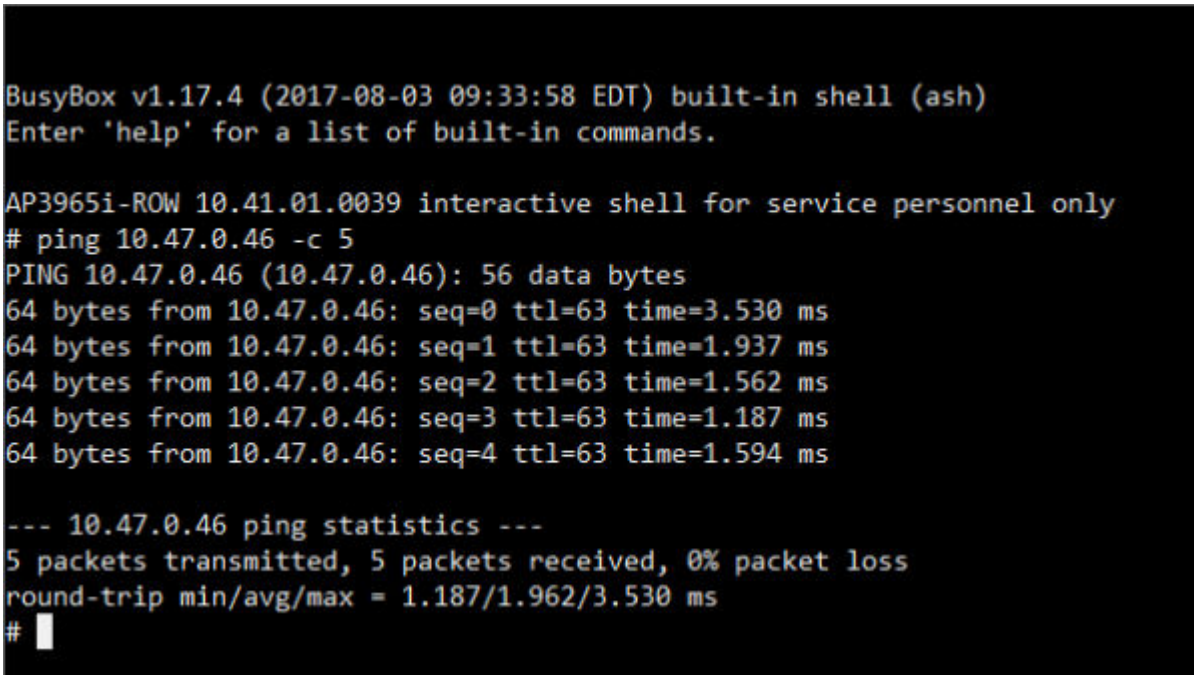
3 Select **Troubleshooting** > **Remote Console**.
4 In the **Search for AP name** field, enter the AP name, and select the appropriate AP from the list displayed.
5 Alternately, click the arrow icon and select the appropriate AP from the list displayed.
6 Click **Connect**.

The selected AP's SSH console appears.



7 Perform `ping` and `traceroute` at the SSH prompt.

See the following screen:



8 To terminate the SSH console session, click **Disconnect**.

Related Links

Performing Wireless AP Diagnostics Using SSH on page 110
Enabling SSH on a Selected Wireless AP on page 111
Disabling SSH Access on a Selected AP on page 112
Opening Remote Shell on page 114

Opening Remote Shell

Open a Remote Shell session to an AP:

1 From the top menu, click **AP** > **APs**.
2 Click an AP row in the list (not the check box).

3 Select the Remote Shell tab.

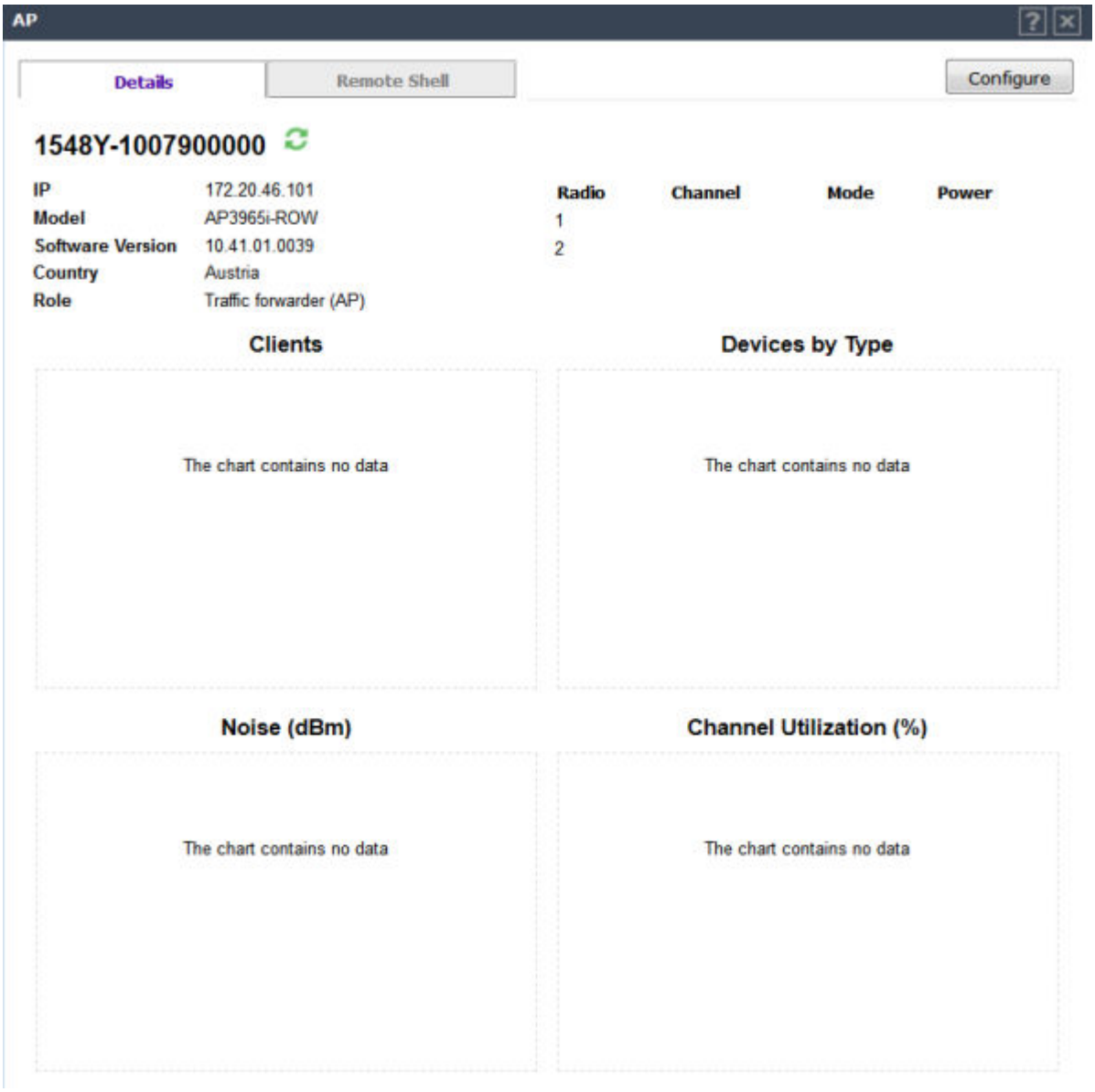


Figure 32: Remote Shell Tab for an AP

Related Links

Opening Live SSH Console to a Selected AP on page 113

Configuring Packet Capture on a Selected AP

Use Packet Capture to identify network inconsistencies by intercepting packets that travel from the APs to the controller. Packets are captured based on the parameter configurations that you specify.

The packets are logged in a PCAP file for each session. The PCAP file is temporarily stored on the controller that is associated with the AP. To view the PCAP file, export the file to a host running Wireshark.

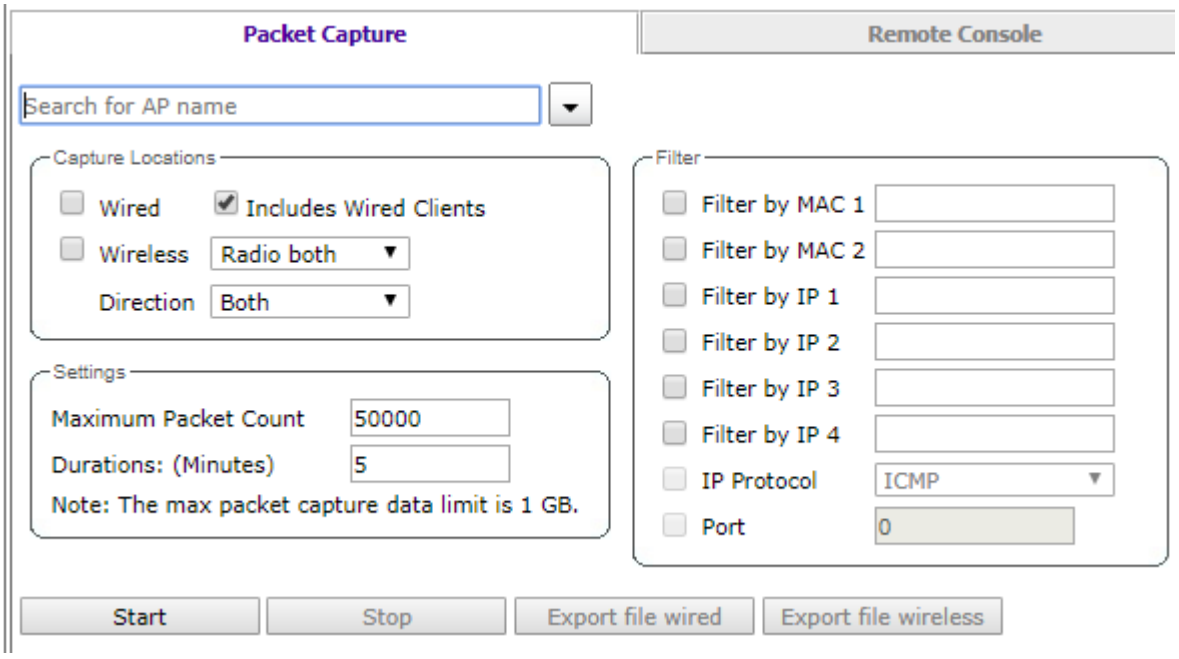
Note
Live Packet Capture is available in addition to the saved file option. After starting Packet Capture, start Wireshark and add the remote interface using the ExtremeWireless management IP address. See the Wireshark documentation for details.

Packets can be captured from APs associated with either controller in an Availability Pair. Packet capture will continue after failover displaying packet results in one file.

With AP39xx, once packet capture has started, you can change the capture parameters and refresh the capture, continuing to capture without interruption. This feature allows you to modify parameters as you monitor the capture process. All parameters are represented in a single file, except when the Capture Location is changed between wired and wireless. Wired and wireless packets are always represented in separate PCAP files.

To enable packet capture on an AP:

1 From the top menu, click **AP**.
2 From the left pane, click **Global** > **Maintenance**.
The **AP Software Maintenance** screen displays.
3 Click the **Troubleshooting** tab.
The **Packet Capture** screen displays.



4 In the **Search for AP name** field, enter the AP name, and select the appropriate AP from the list displayed.
5 Alternately, click the arrow icon and select the appropriate AP from the list displayed.
6 Configure the packet capture parameters.

7 Click **Start** to start the packet capture.

8 Click **Stop** to stop the packet capture.

Packet capture stops when capture file size reaches 1GB. If both wireless and wired capture is in progress, both captures stop if any file reaches the 1GB limit.

9 Click **Export** to export the generated PCAP file to a host running Wireshark.

Note

The controller can store only one PCAP file at a time. Therefore, export the file immediately upon completion of packet capture to avoid overwriting the file with the next capture file.

By default, captured packets are logged to the files *AP_traffic_dump_wired.pcap* for wired and *AP_traffic_dump_wireless.pcap* for wireless, and temporarily stored on the controller that is associated with the selected AP.

The PCAP file name can be changed through the CLI. In the CLI, move to the `ap-traffic-capture` context from the `root` context, and issue the `file *.pcap` command.

For more information about the CLI, see the *ExtremeWireless CLI Guide*.

Related Links

Packet Capture Parameters on page 117
Configuring Live Packet Capture on page 119
Wireshark Configuration on page 120

Packet Capture Parameters

Field Name	Field Description
In the **Capture Locations** pane, configure the following settings:	
Wired	Enables wired-packet capture on the selected AP. Filter packets on the basis of the direction of packet flow: • **In** — Capture packets received by the AP. • **Out** — Capture packets transmitted by the AP. • **Both** — Capture packets transmitted and received by the AP. This is the default value. Select **Includes Wired Clients** to include wired-packets received and transmitted to and from wired clients associated with the selected AP. This option is disabled by default.

Field Name	Field Description
Wireless	Enables wireless-packet capture on the selected AP. Filter packets on the basis of the direction of packet flow: • **In** — Capture packets received by the AP. • **Out** — Capture packets transmitted by the AP. • **Both** — Capture packets transmitted and received by the AP. This is the default value. Specify the radio interface on which to enable wireless-packet capture. • **Radio 1** — Enable packet capture on the AP's radio 1 interface. • **Radio 2** — Enable packet capture on the AP's radio 2 interface. • **Radio Both** — Enable packet capture on both radio 1 and radio 2 interfaces of the AP. This option is selected by default. Note: You have the option to capture wired and wireless packets simultaneously. The result is two PCAP files: one displays wired packet information, one displays wireless packet information.
In the **Settings** pane, specify how you want to determine the length of the packet capture. Options are: **Maximum Packet Count**, **Duration**, or manually end packet capture by clicking **Stop**.	
Maximum Packet Count	Specify the maximum number of packets captured and logged to the PACP file. The default value is 50000. Packet capture stops once the threshold specified here is reached, unless manually stopped beforehand. Note: Note: The default maximum packet capture data limit is 1 GB. Therefore, regardless of the Maximum Packet Capture Count specified, packet capture stops once the PCAP file size reaches 1 GB.
Duration	Packet transfer window. Default value is 5 minutes.
In the **Filter** pane, filter packets by MAC address, IP address, IP Protocol, or Port. The filters are mutually exclusive and are applied in the order in which they are listed. Enter at least one MAC address or IP address. Note: Excessive packet capture degrades network performance. If you are going to enable packet capture on all APs, specify at least one MAC address filter and one IP address filter to avoid performance degradation.	
Filter by MAC 1 and Filter by MAC 2	Specify one or two MAC addresses to filter packets for capture. When a MAC address is specified, only packets that move to and from the specified MAC addresses are captured.
Filter by IP 1 to Filter by IP 4	Specify one to four IP addresses to filter packets for capture. filters. When an IP address is specified, only packets that move to and from the specified IP addresses are captured. Both IPv4 and IPv6 address formats are supported.
IP Protocol	Specify the protocol to filter for packet capture. Packets matching the specified protocol are captured. Valid values are: • **ICMP** — Captures only ICMP packets. This is the default value. • **TCP** — Captures only TCP packets. • **UDP** — Captures only UDP packets • **GRE** — Captures only GRE packets • **IPsec - ESP** — Captures only IPsec - ESP packets • **IPsec - AH** — Captures only IPsec - AH packets

Field Name	Field Description
Port	Specify a TCP or UDP port number. Packets with the matching port number are captured. Use **Port** as an additional filter, or if you wish to specify a protocol that is not included in the **IP Protocol** menu.
Export	**Note:** You have the option to capture wired and wireless packets simultaneously. The result is two PCAP files: one displaying wired packet information, one displaying wireless packet information.

Related Links

Configuring Packet Capture on a Selected AP on page 115
Configuring Live Packet Capture on page 119

Configuring Live Packet Capture

Live Packet Capture is available during the creation of the saved packet file. After starting Packet Capture, start Wireshark and specify the Management Controller IP address. With Live Capture, use Wireshark to connect to a remote interface and view the packets live.

1 Go to **AP** > **Global** > **Maintenance** > **Troubleshooting**.
The **Packet Capture** screen displays.

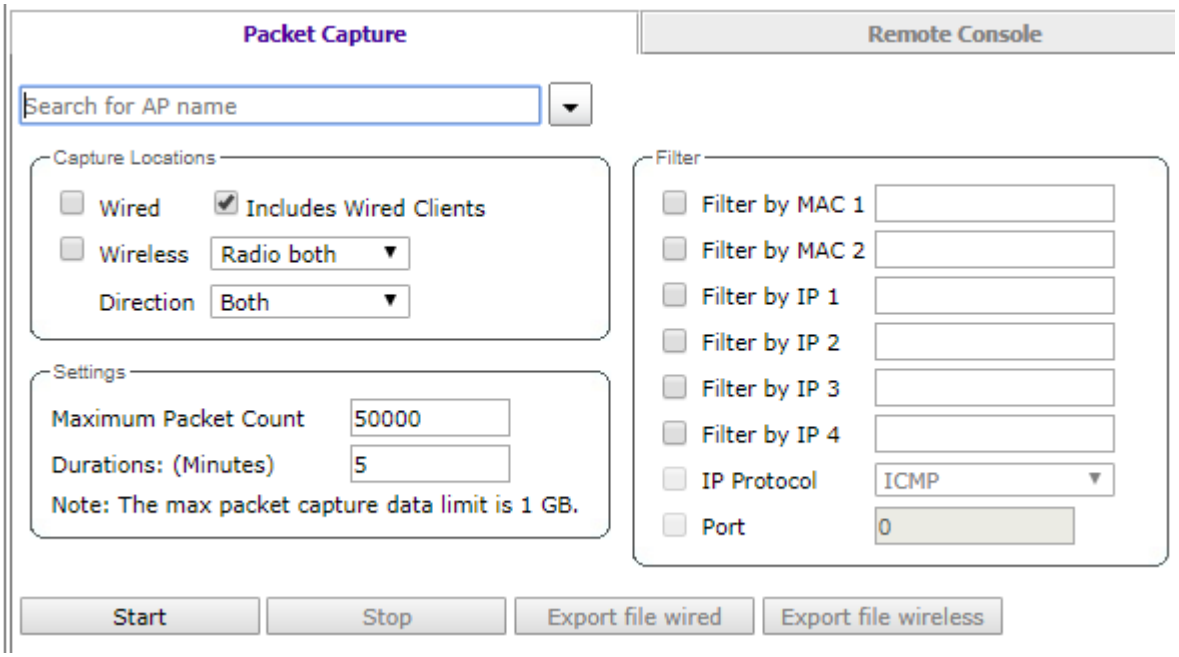


Figure 33: ExtremeWireless Packet Capture Parameters

2 Select an appropriate AP.
3 Configure the packet capture parameters.
4 Click **Start**.

Go to Wireshark Configuration on page 120.

Related Links

Packet Capture Parameters on page 117
Wireshark Configuration on page 120
Configuring Packet Capture on a Selected AP on page 115

Wireshark Configuration

For Live Packet Capture, configure packet capture parameters in ExtremeWireless, then configure the following parameters in Wireshark.

1 Open Wireshark and go to the Capture Options dialog.

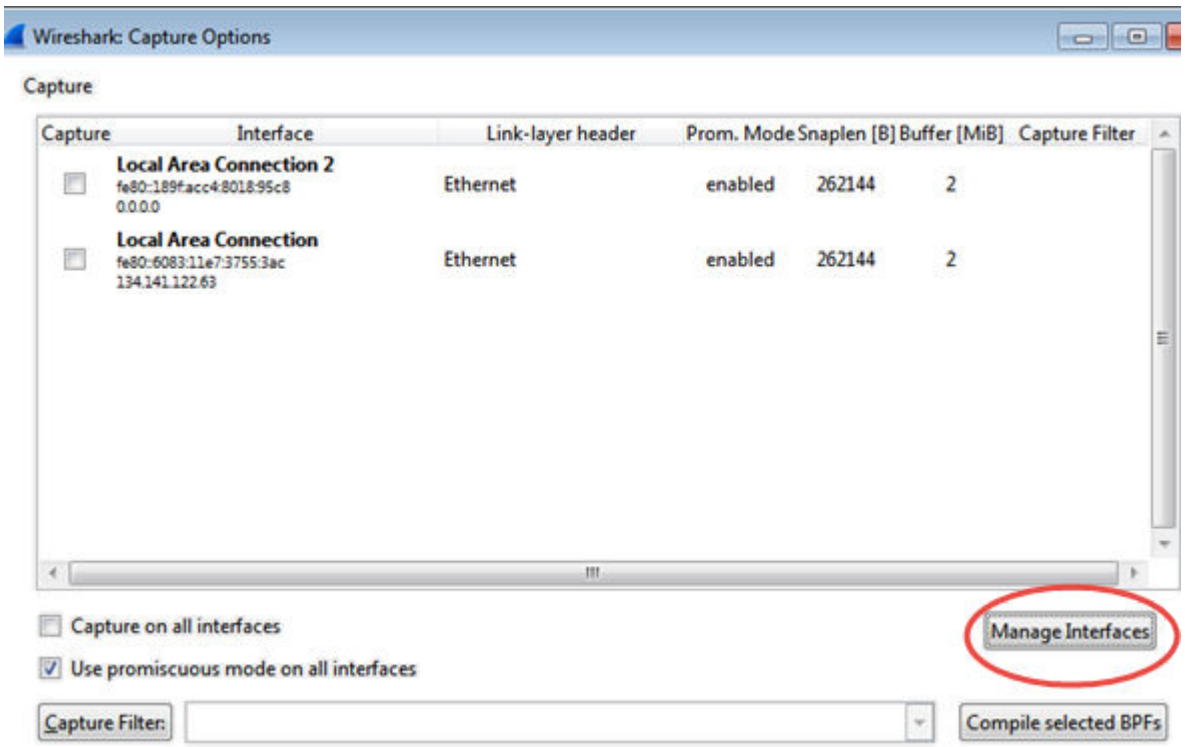


Figure 34: Wireshark Capture Options Dialog

2 Click **Manage Interfaces**
3 From the Remote Interfaces tab, select **Add**.
4 In the Host field, enter the controller Management IP address.

Note
Port 2002 is the default port for this Wireshark service.

5 Click **OK**.

The available interfaces for the controller are displayed.

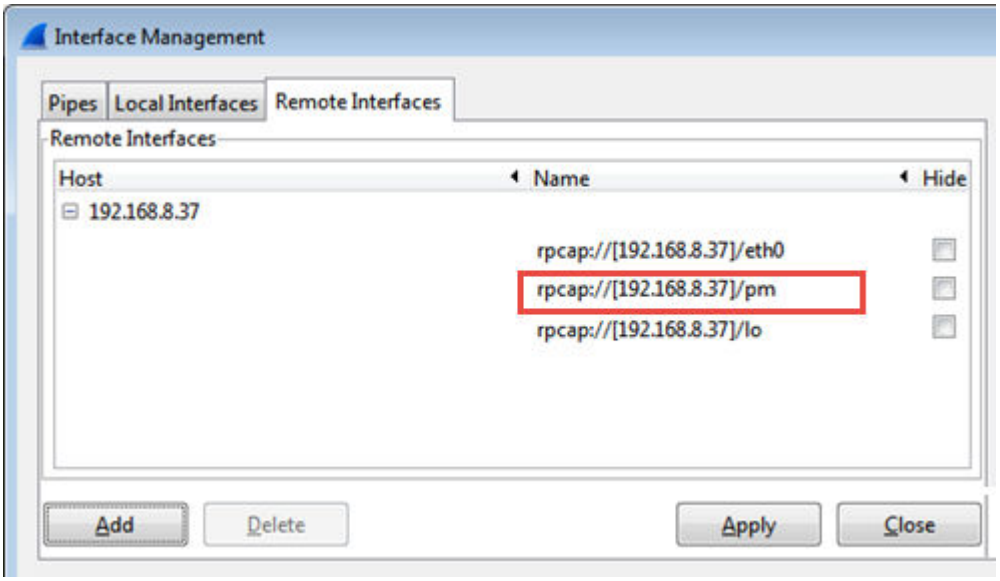


Figure 35: Remote Interfaces Tab with Wired and Wireless Interfaces Highlighted

Note

(Optional) To focus on the interface that you specified in ExtremeWireless Capture Location parameters, select the check box to hide the other interfaces.

6 Click **Add**.

The Capture Options dialog displays. All interfaces that are not hidden are selected. PM stands for packet mirror.

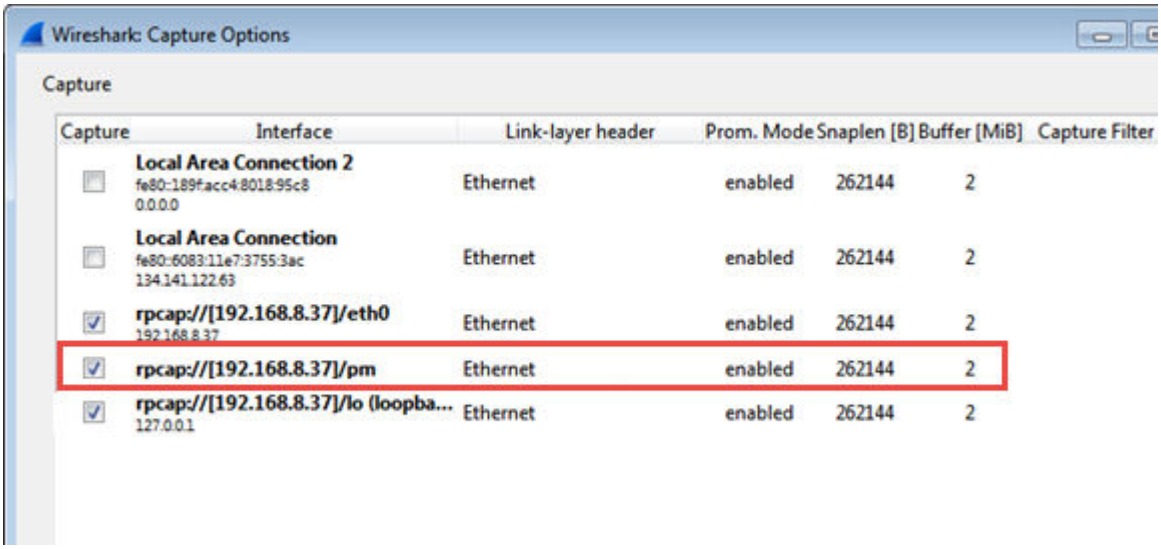


Figure 36: Wireshark Capture Options with Remote Interfaces

Note

The Wired and Wireless interfaces are highlighted.

7 Click **Start** to monitor the packet capture.

Glossary

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

DHCP

Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP

addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve

performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeCloud Appliance

The ExtremeCloud Appliance, the newest addition to the Smart OmniEdge portfolio, is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge. Learn more about ExtremeCloud Appliance at https://www.extremenetworks.com/product/extremecloud-appliance/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeControl

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at https://www.extremenetworks.com/product/extremecontrol/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: Modular (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); Stackable (X-series and A, B, C, and 7100 series switches); Standalone (SSA, X430, and D, 200, 800, and ISW series); and Mobile Backhaul (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

MD5

Message-Digest algorithm is a hash function that is commonly used to generate a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

OSPF

An interior gateway routing protocol for TCP/IP networks, Open Shortest Path First uses a link state routing algorithm that calculates routes for packets based on a number of factors, including least hops, speed of transmission lines, and congestion delays. You can also configure certain cost metrics for the algorithm. This protocol is more efficient and scalable than vector-distance routing protocols. OSPF features include least-cost routing, ECMP routing, and load balancing. Although OSPF requires CPU

power and memory space, it results in smaller, less frequent router table updates throughout the network. This protocol is more efficient and scalable than vector-distance routing protocols.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

RADIUS

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

SNMP

Simple Network Management Protocol is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

VLAN

The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.

VNS

A Virtual Networks Service is an Extreme Networks-specific technique that provides a means of mapping wireless networks to a wired topology.