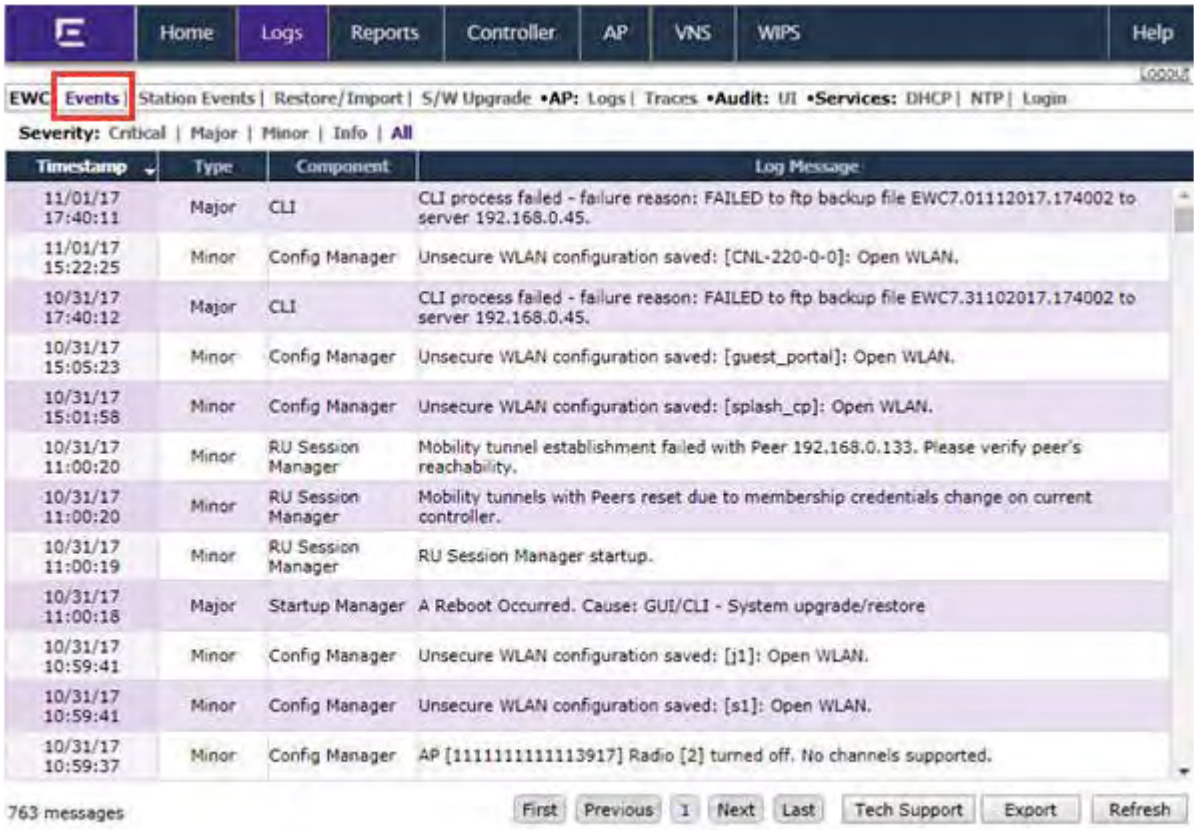
2 Click **EWC Events** and the severity level. The log screen displays and the events are displayed in chronological order.



3 To sort the events by Timestamp, Type, or Component, click the appropriate column heading.

4 To filter the events by severity, Critical, Major, Minor, Info, and All, click the appropriate log severity.

5 To refresh the log screen, click **Refresh**.

6 To export the log screen, click **Export**. The File Download dialog is displayed.

7 Do one of the following:

- To open the log file, click **Open**.
- To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

> **Note**
> The component 'Langley' is the term for the inter-process messaging infrastructure on the wireless controller.

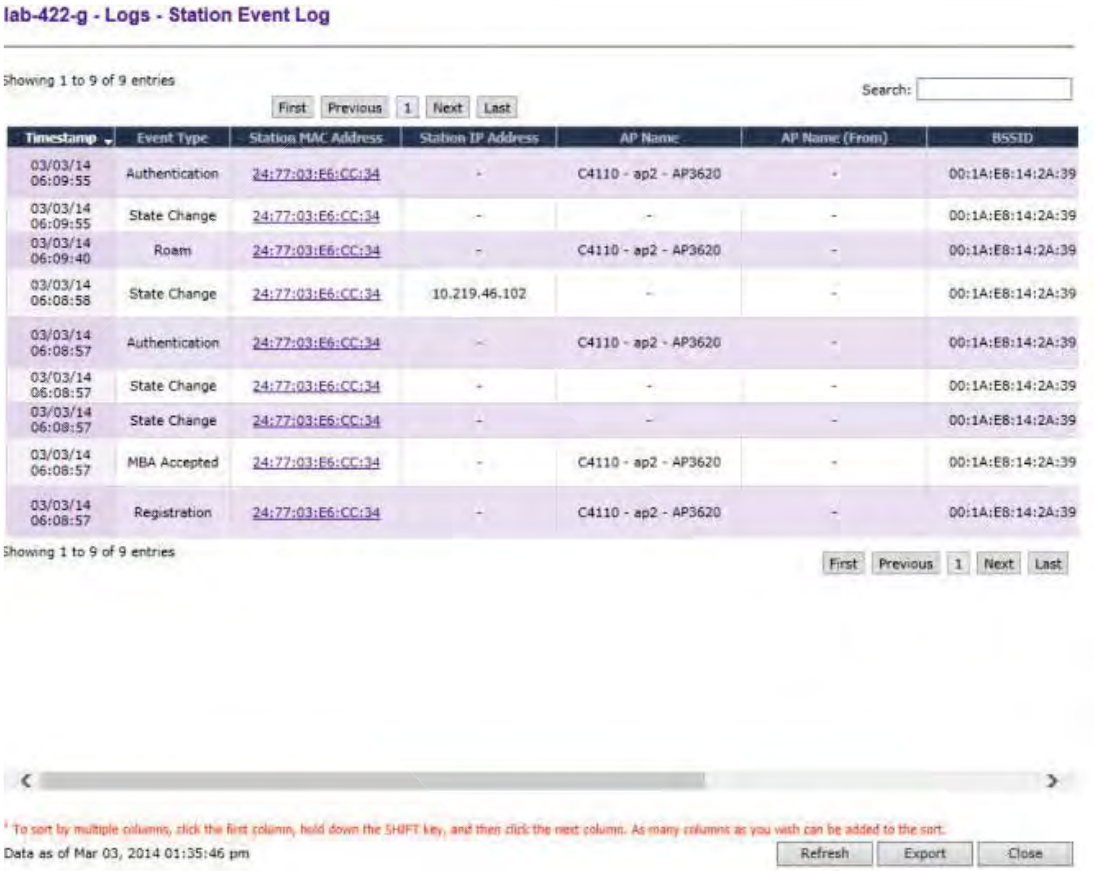
Viewing Wireless Controller Station Logs

To view wireless controller station logs:

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

2 Click EWC: **Station Events**. The Station Events screen displays and the events are displayed in chronological order.

Note
Station log generation is controlled by the "Report station events on controller" check box on the wireless **Controller** > **Logs** > **Logs Configuration** page.



The table is sortable on all column (ascending and descending), if you close this log window and open it again within the same GUI session, it remembers you previous column sorting option, plus it has multi-column sorting.

3 To sort by multiple columns, click the first column, hold down the **[Shift]** key, and then click the next column. As many columns as you wish can be added to the sort.

4 Click on MAC addresses in Station MAC Address column to see up-to-date details about the particular station.

5 Click the **Search** box and enter text. The information is filtered automatically as you type and only lines which match this text in any column (on all pages) are displayed.

6 Click **Refresh** to refresh the log. This log doesn't refresh automatically (the same as other logs).

7 To export the Station log screen, click **Export**. The File Download dialog is displayed. Do one of the following:

- To open the log file, click **Open**.
- To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

8 Click **Close** to close this log window.

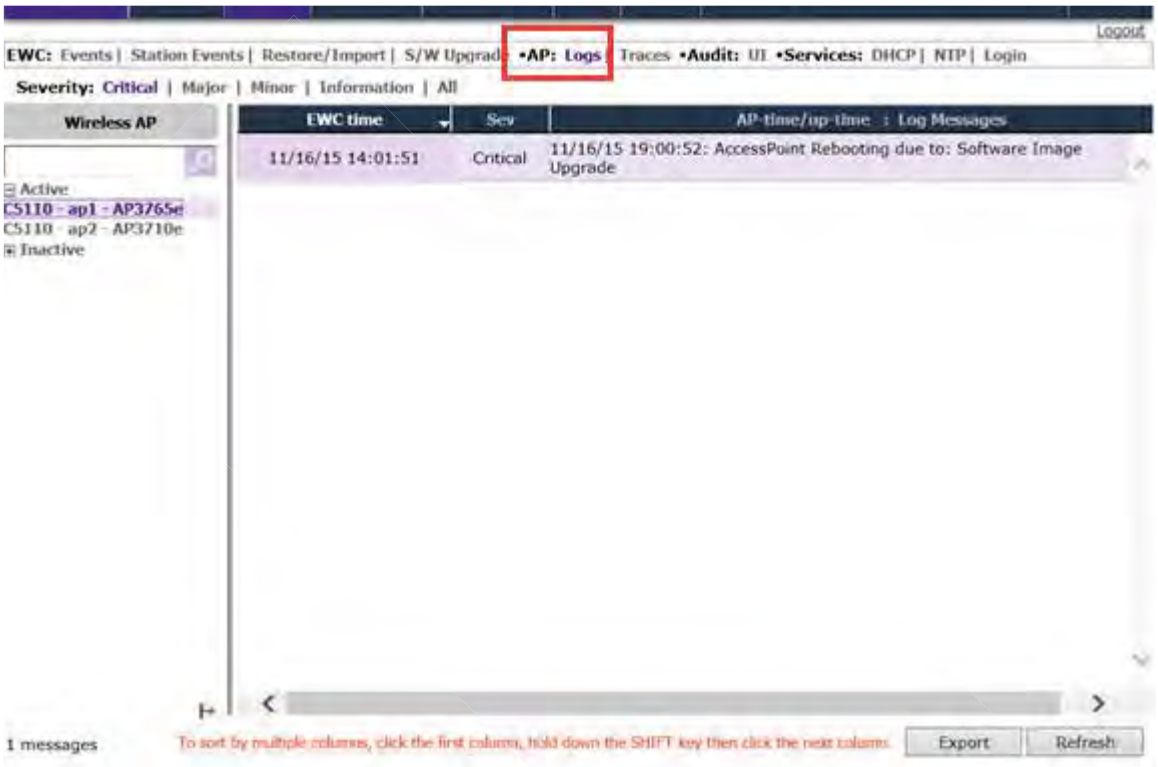
Viewing Wireless AP Logs

To view wireless AP logs:

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

2 Click **AP: Logs**.

The Wireless AP Log screen displays and the events are displayed in chronological order.



3 In the **Wireless AP** list, click a Wireless AP to view the log events for that particular Wireless AP.

4 To sort the events by **EWC time** or **Sev** (Severity), click the appropriate column heading.

5 To filter the events by severity, **Critical**, **Major**, **Minor**, **Information**, and **All**, click the appropriate log severity.

6 To refresh the log screen, click **Refresh**.

7 To export the logs, click **Export**. The File Download dialog is displayed.

8 Do one of the following:

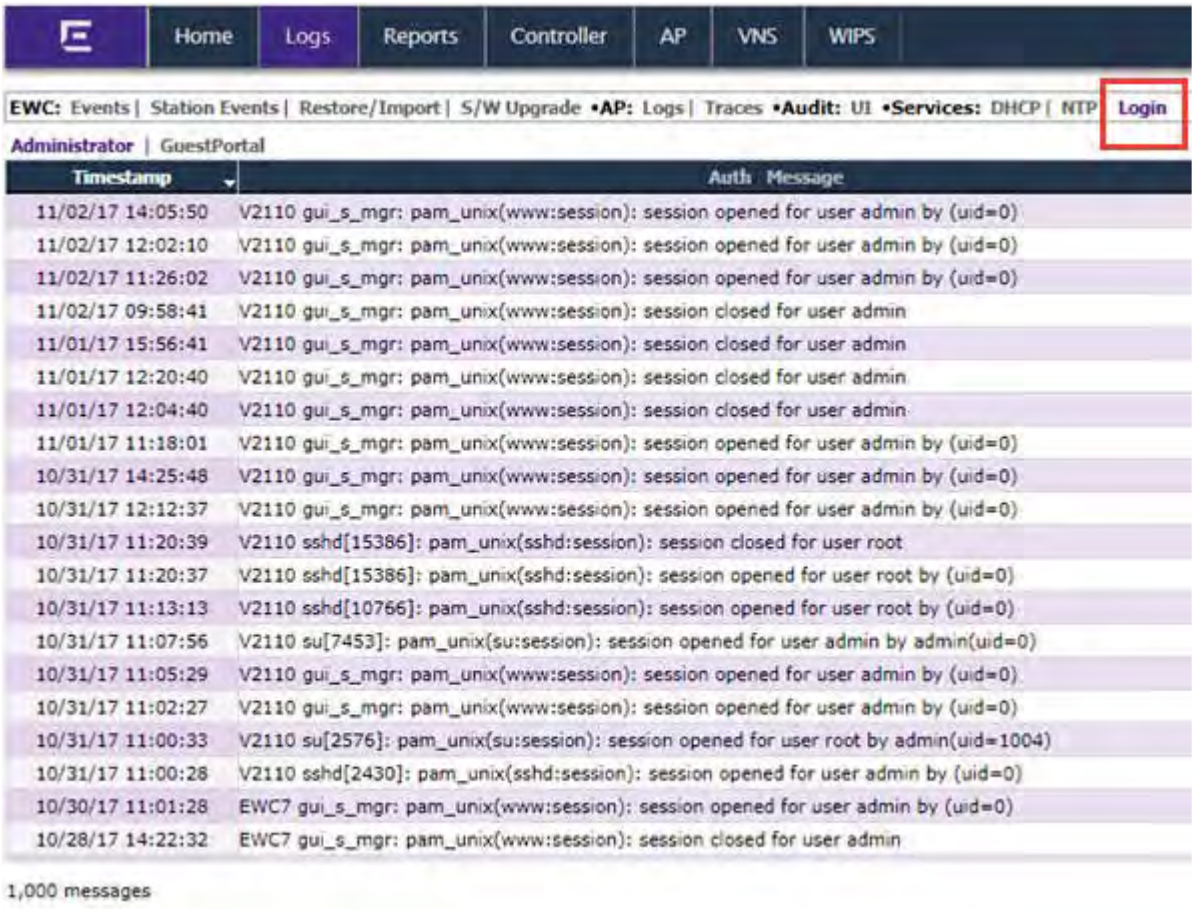
- To open the log file, click **Open**.
- To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Viewing Login Logs

To view administrator login logs:

1 From the top menu, click **Logs**.
2 Click **Login** .

The Login screen displays and the login events are displayed in chronological order.



3 To refresh the Login screen, click **Refresh**.

Working with GuestPortal Login Logs

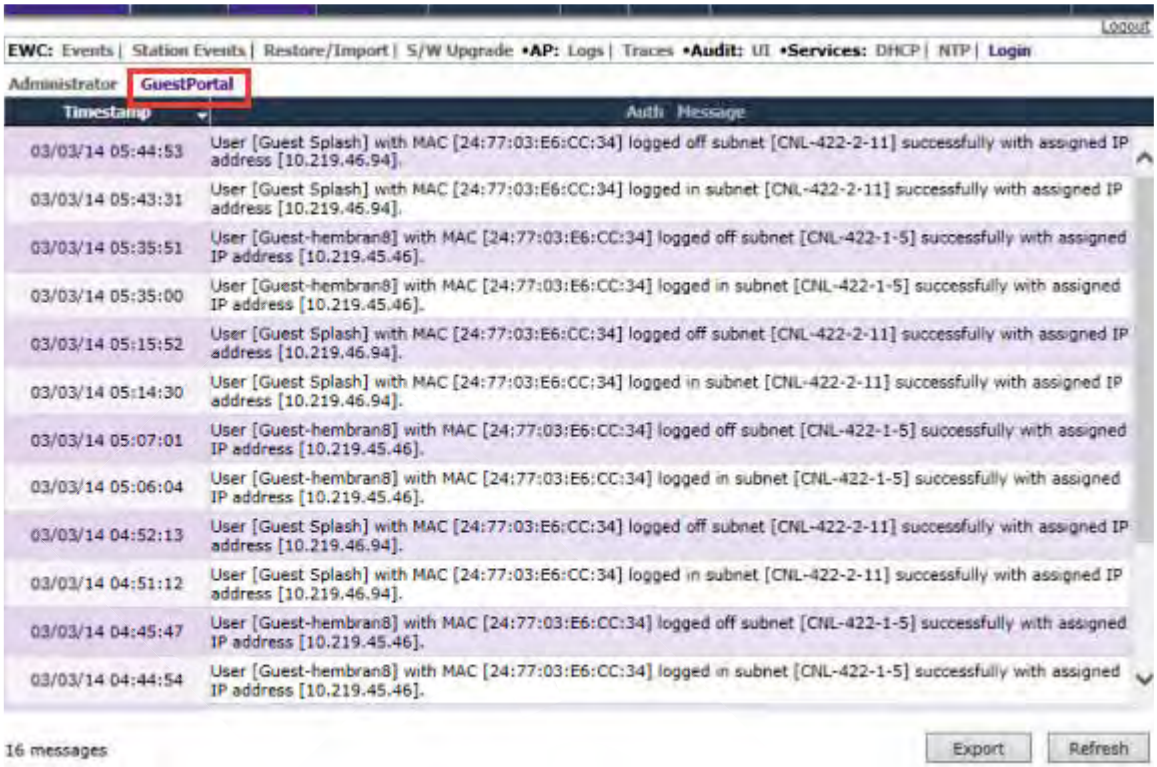
To view GuestPortal login logs:

1 From the top menu, click **Logs**.
2 Click **Login** .

The Login screen displays and the login events are displayed in chronological order.

3 Click **GuestPortal**.

The GuestPortal login events are displayed in chronological order.



4 To export the GuestPortal log information, click **Export**. The File Download dialog is displayed.

5 Do one of the following:

- To open the log file, click **Open**.
- To save the log file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Working with a Tech Support File

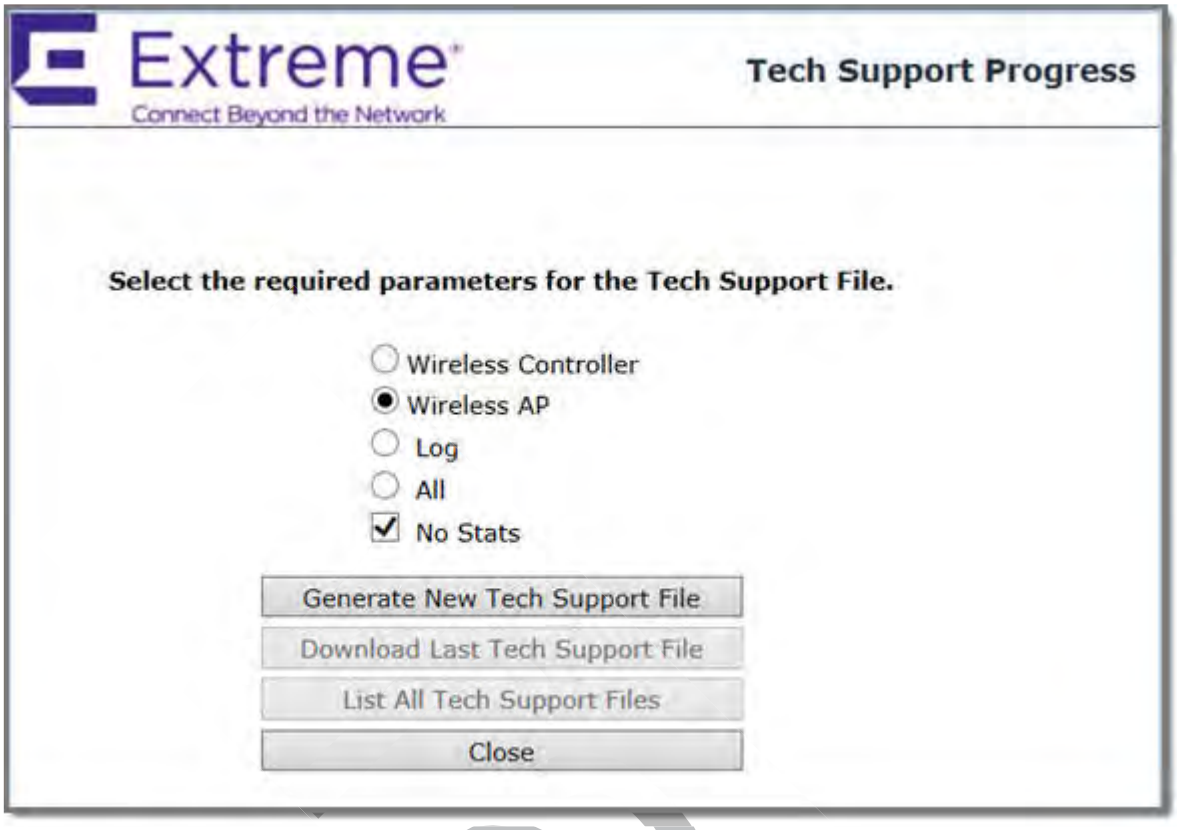
1 To generate a Tech Support file, click **Logs** from the top menu.

The Logs & Traces screen displays.

2 Ensure that **EWC:Events** is selected.

3 Click the **Tech Support** button at the bottom of the page.

The Generate Tech Support File screen displays.



4 Select the parameters for the tech support file:

- **Wireless Controller**
- **Wireless AP**
- **Logs**
- **All**
- **No Stats** – If **Wireless AP** is selected, select this check box to include or exclude Wireless AP statistics in the tech support file.

5 Click **Generate New Tech Support File**.

A warning message is displayed informing you that this operation may temporarily affect system performance.

6 Click **OK** to continue.

The tech support file generation status is displayed.

7 When the file generation has completed, click **Close**.

8 To download the last generated Tech Support file, click **Logs** from the top menu.

The Logs & Traces screen displays.

9 Ensure that the EWC tab is selected.

10 Click the **Tech Support** button at the bottom of the page.

The Generate Tech Support File screen displays.

11 Click **Download Last Tech Support File**.

The File Download dialog is displayed.

12 Click **Save**.

The Save as window is displayed.

13 Navigate to the location you want to save the generated tech support file, and then click **Save**.

14 To delete a Tech Support file, click **Logs** from the to pmenu.

The Logs & Traces screen displays.

15 Ensure that the EWC tab is selected.

16 Click the **Tech Support** button at the bottom of the page.

The Generate Tech Support File screen displays.

17 Click **List All Tech Support Files**.

18 In the drop-down list, click the tech support file you want to delete.

The tech support file is deleted.

19 Click **Close**.

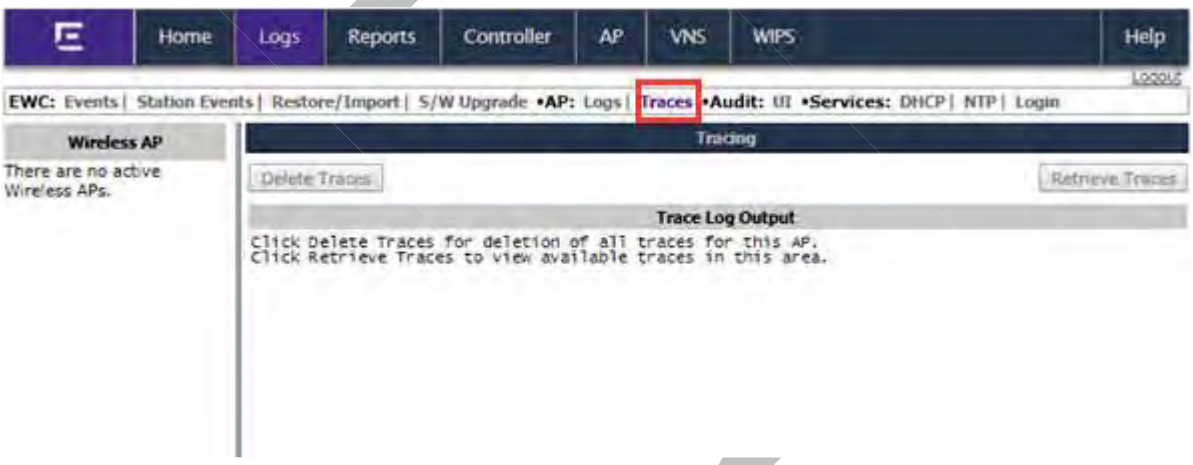
Viewing Wireless AP Traces

To view wireless AP traces:

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

2 Click **AP: Traces**.

The Wireless AP trace screen displays.



3 In the **Wireless AP** list, click the Wireless AP whose trace messages you want to view.

4 Click **Retrieve Traces**. Depending on the browser, the File Download dialog appears.

5 Click **Save** and navigate to the location on your computer that you want to save the Wireless AP trace report.

The file is saved as a .tar file.

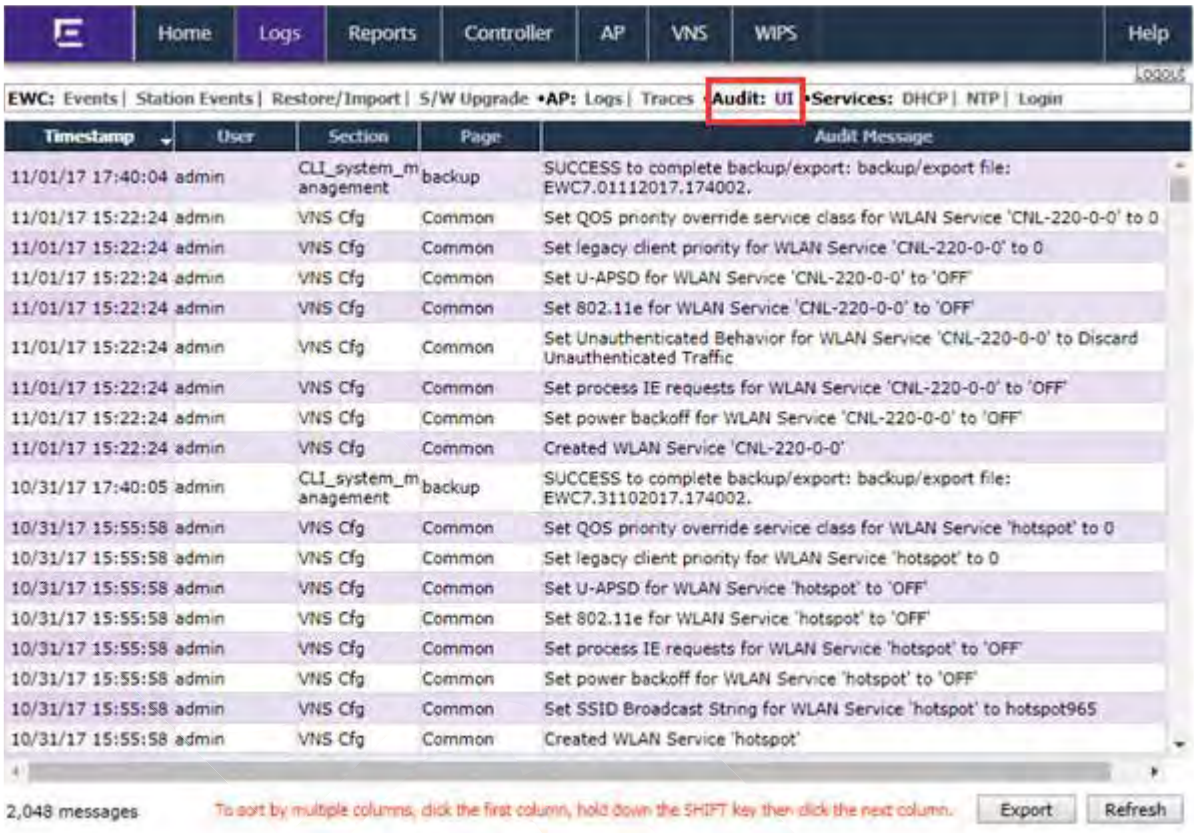
6 To view the file, unpack the .tar file.

Viewing Audit Messages

To view Audit messages:

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

2 Click **Audit: UI** . The Audit screen displays and the events are displayed in chronological order.



3 To sort the events by **Timestamp, User, Section, or Page**, click the appropriate column heading.

4 To refresh the audit screen, click **Refresh**.

5 To export the audit screen, click **Export**. The File Download dialog is displayed.

6 Do one of the following:

- To open the audit file, click **Open**.
- To save the audit file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

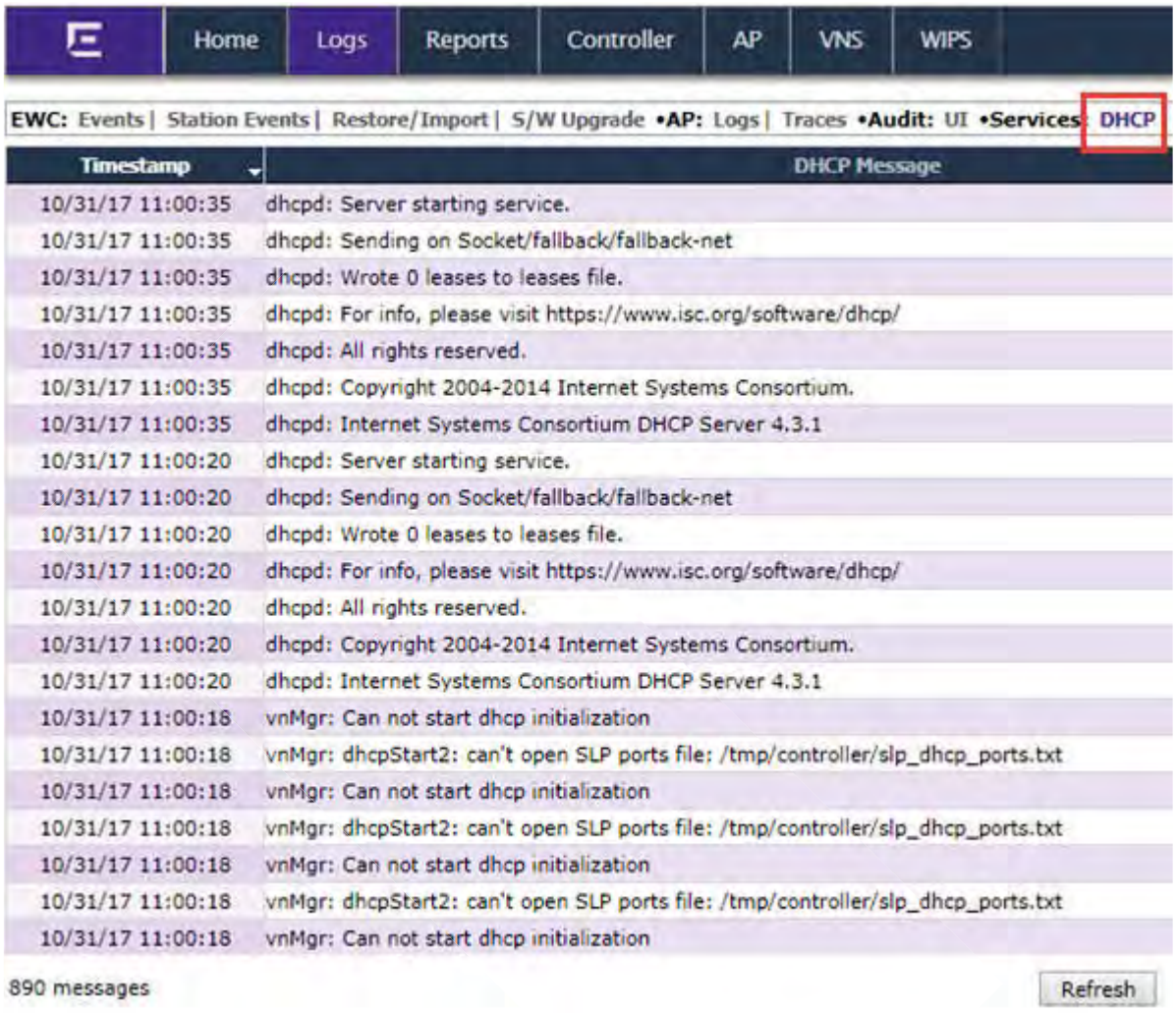
Viewing the DHCP Messages

To view DHCP messages:

1 From the top menu, click **Logs**. The Logs & Traces screen displays.

2 Click **Service: DHCP**.

The DHCP Message screen displays and the events are displayed in chronological order.



3 To sort the events by **timestamp,** click **Timestamp**.

4 To refresh the DHCP message screen, click **Refresh**.

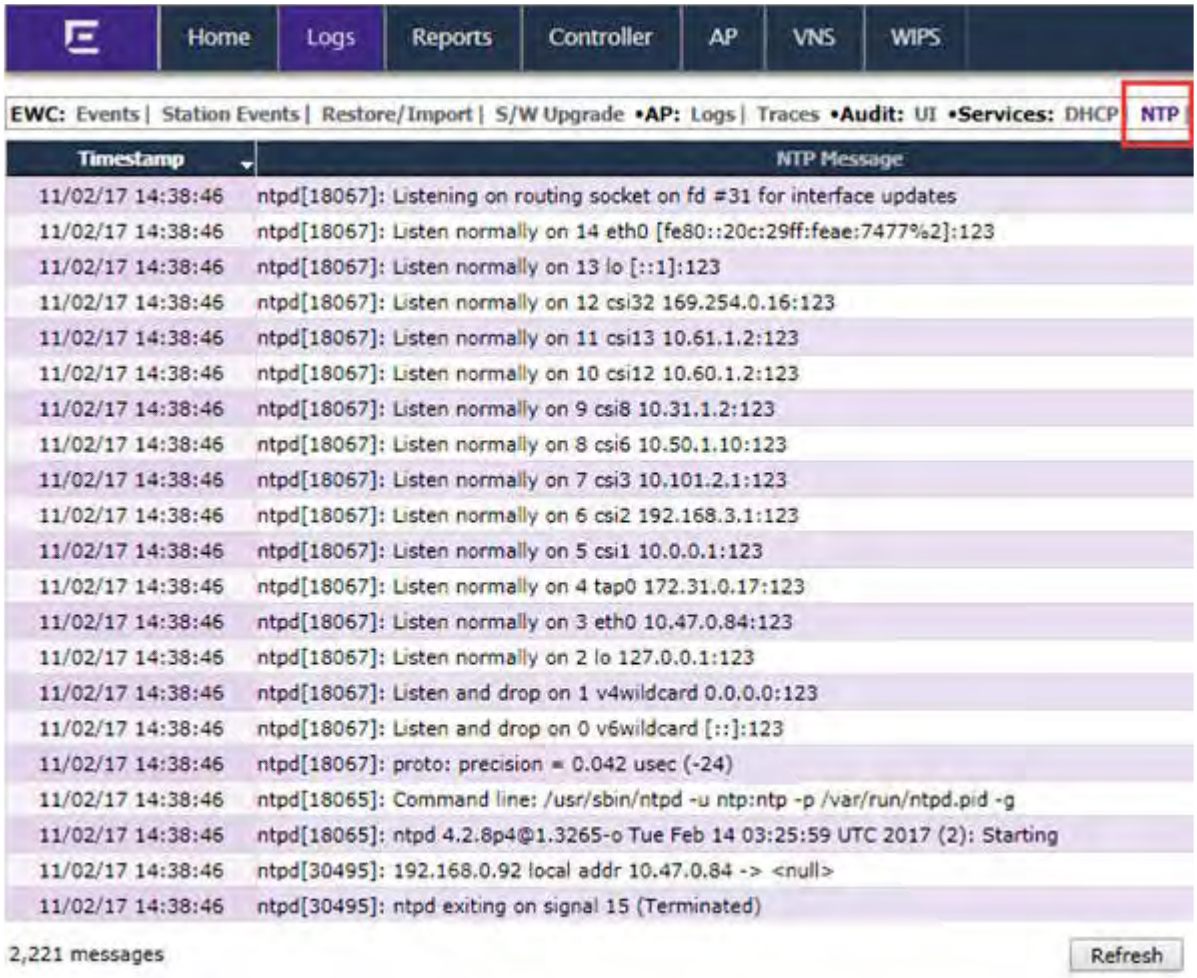
Viewing the NTP Messages

To view NTP messages:

1 From the top menu, click **Logs**. The Logs & Traces screen displays.

2 Click Service: NTP.

The NTP Message screen displays and the events are displayed in chronological order.



3 To sort the events by timestamp, click **Timestamp**.

4 To refresh the NTP message screen, click **Refresh**.

Viewing Software Upgrade Messages

The S/W Upgrade tab displays the most recent upgrade actions, either success or failure, and the operating system patch history. Some examples of the upgrade actions that can be displayed are:

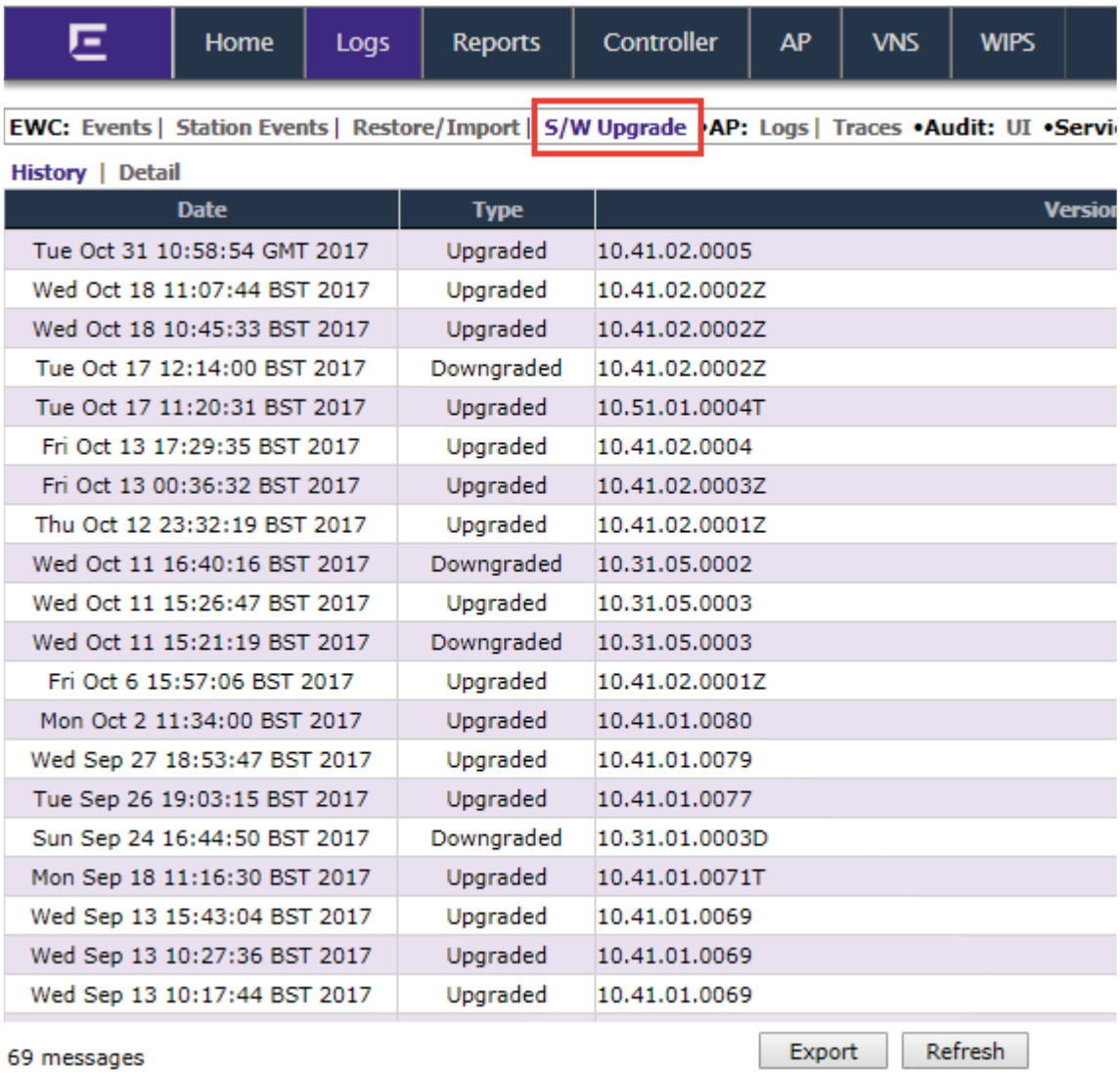
- FTP failure during backup of system image
- Configuration reset failure
- Configuration export failure
- Configuration import details

To view software upgrade messages:

1 From the top menu, click **Logs**. The Logs & Traces screen displays.

2 Click the S/W Upgrade tab.

The S/W Upgrade message screen displays.



3 Do the following:

- To view software upgrade messages, click **Detail**.
- To view the operating system history, click **History**.

4 To refresh the screen, click **Refresh**.

5 To export the software upgrade messages or operating system history, click **Export**. The File Download dialog is displayed.

6 Do one of the following:

- To open the file, click **Open**.
- To save the file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

Viewing Configuration Restore/Import Messages

The Restore/Import tab displays the most recent configuration restore/import results.

To view Restore/Import messages:

1 From the top menu, click **Logs**. The Logs & Traces screen displays.
2 Click the Restore/Import tab.
The restore/import message screen displays.

3 To refresh the restore/import message screen, click **Refresh**.
4 To export the restore/import message screen, click **Export**. The File Download dialog is displayed.
5 Do one of the following:
- To open the file, click **Open**.
- To save the file, click **Save**, and then navigate to the directory location you want to save the file. Click **Save**.

21 Working with GuestPortal Administration

About GuestPortals

A GuestPortal provides wireless device users with temporary guest network services. A GuestPortal is serviced by a GuestPortal-dedicated VNS. The GuestPortal-dedicated VNS is configured by an administrator with full administrator access rights. For more information, see Creating a GuestPortal VNS on page 477.

A GuestPortal administrator is assigned to the GuestPortal Manager login group and can only create and manage guest user accounts — a GuestPortal administrator cannot access any other area of the Wireless Assistant. For more information, see Defining Wireless Assistant Administrators and Login Groups on page 673.

From the **GuestPortal Guest Administration** page of the Wireless Assistant, you can add, edit, configure, and import and export guest accounts.

Adding New Guest Accounts

To add a new guest account:

1 Do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
  - From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
  - In the left pane, expand the **WLAN Services** pane, click the dedicated *WLAN (Wireless Local Area Network)* Service that provides the temporary guest network services. The WLAN Services configuration window for that service displays.
  - Click the **Auth & Acct** tab.
  - Make sure the Mode is set to Guest Splash and then click **Configure**. The Configuration page displays.
  - In the **Guest Splash** section, click **Manage Guest Users**.
  - The **Guest Splash Administration** screen displays.

Note
You have three minutes to add new guest user accounts. If that time expires, close the Guest Splash Administration screen and click **Manage Guest Users** again. You can also increase the **Start date** time to be within three minutes of the current network time.

2 In the **Account Management** section, click **Add Guest Account**.

The Add Guest User screen displays.

3 To enable the new guest account, select the **Enabled** check box. For more information, see Enabling or Disabling Guest Accounts on page 693.

4 In the **Credentials** section, do the following:

- **User Name** — Type a user name for the person who will use this guest account.
- **User ID** — Type a user ID for the person who will use this guest account. The default user ID can be edited.
- **Password** — Type a password for the person who will use this guest account. The default password can be edited.

  Toggle between **Mask/Unmask** to hide or see the password.
- **Description** — Type a brief description for the new guest account.

5 In the **Account Settings** section, do the following:

- **Start date** — Specify the start date and time for the new guest account.
- **Account lifetime** — Specify the account lifetime, in days, for the new guest account. The default **0** value specifies no limit to the account lifetime. Only a user with administrative privileges can change the value of the Account lifetime.

6 In the **Session Settings** section, do the following:

- **Session lifetime** — Specify a session lifetime, in hours, for the new guest account. The default **0** value specifies no limit to the session lifetime. The session lifetime is the allowed cumulative total in hours spent on the network during the account lifetime.
- **Start Time** — Specify a start time for the session for the new guest account.
- **End Time** — Specify an end time for the session for the new guest account.

7 To save your changes, click **OK**.

Enabling or Disabling Guest Accounts

A guest account must be enabled in order for a wireless device user to use the guest account to obtain guest network services.

When a guest account is disabled, it remains in the database. A disabled guest account cannot provide access to the network.

To enable or disable guest accounts:

1 Do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
  - From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
  - In the left pane, expand the WLAN Services pane, click the dedicated *WLAN* Service that provides the temporary guest network services. The WLAN Services configuration window for that service displays.
  - Click the Auth & Acct tab, and then click **Configure**. The Settings screen displays.
  - In the **Guest Splash** section, click **Manage Guest Users**.
  - The Guest Splash Administration screen displays.

2 In the guest account list, select the check box next to the user name of the guest account that you want to enable or disable.

3 In the **Account Enable/Disable** section, click **Enable Selected Accounts** or **Disable Selected Accounts** accordingly. A dialog is displayed requesting you to confirm your selection.

4 Click **Ok**. A confirmation message is displayed in the Guest Splash Administration screen footer.

Editing Guest Accounts

An already existing guest account can be edited.

To edit a guest account:

1 Do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
  - From the top menu, click **VNS**.
  - In the left pane, expand the **WLAN Services** pane, click the dedicated *WLAN* Service that provides the temporary guest network services. The **WLAN Services configuration** window for that service displays.
  - Click the **Auth & Acct** tab, and then click **Configure**. The **Settings** screen displays.
  - In the **Guest Splash** section, click **Manage Guest Users**.
  - The **Guest Splash Administration** screen displays.

2 In the guest account list, select the check box next to the user name of the guest account that you want to edit.

3 In the **Account Management** section, click **Edit Selected Accounts**.

4 Edit the guest account accordingly. For more information on guest account properties, see Adding New Guest Accounts on page 690.

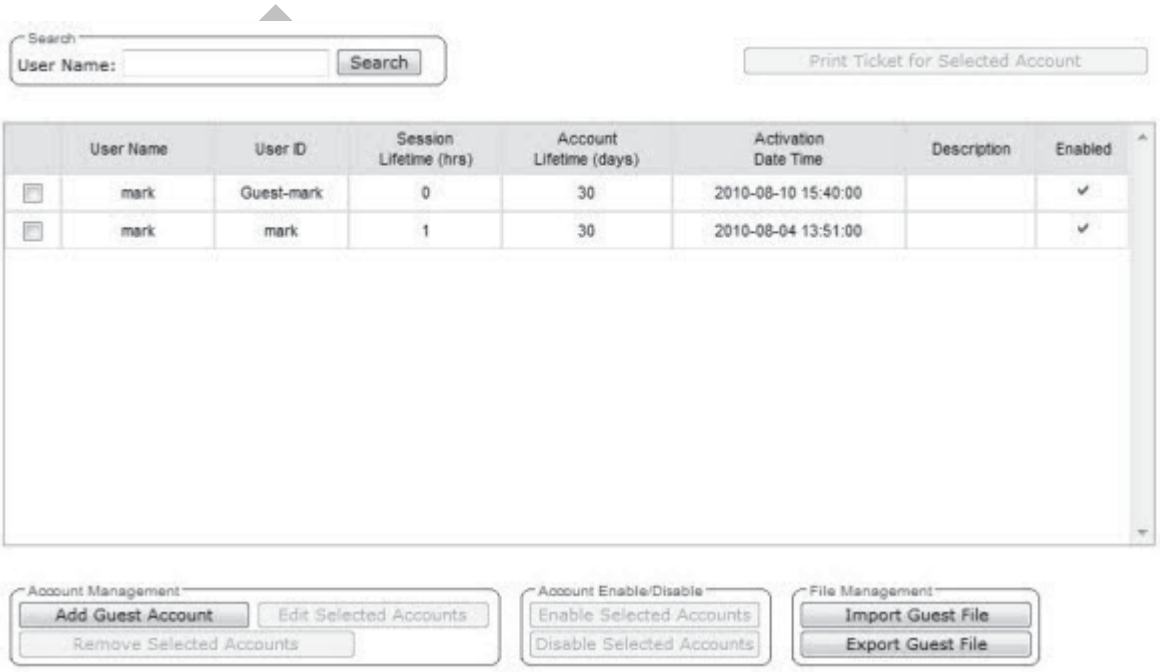
5 To save your changes, click **OK**. A confirmation message is displayed in the **Guest Splash Administration** screen footer.

Removing Guest Accounts

An already existing guest account can be removed from the database.

1 To remove a guest account, do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
  - From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
  - In the left pane, expand the WLAN Services pane, click the dedicated *WLAN* Service that provides the temporary guest network services. The WLAN Services configuration window for that service displays.
  - Click the Auth & Acct tab, and then click **Configure**. The Settings screen displays.
  - In the Guest Splash section, click **Manage Guest Users**. The Guest Splash Administration screen displays.



2 In the guest account list, select the check box next to the user name of the guest account that you want to remove.

3 In the Account Management section, click **Remove Selected Accounts**.

A dialog is displayed requesting you to confirm your removal.

4 Click **OK**.

A confirmation message is displayed in the Guest Splash Administration screen footer.

Importing and Exporting a Guest File

To help administrators manage large numbers of guest accounts, you can import and export .csv (comma separated value) guest files for the controller.

The following describes the column values of the .csv guest file.

Table 133: Guest Account Import and Export .csv File Values

Column	Value
A	User ID
B	User name
C	Password
D	Description
E	Account activation date
F	Account lifetime, measured in days
G	Session lifetime, measured in hours
H	Is the account enabled (1) or disabled (0)
I	Time of day, start time
J	Time of day, duration
K	Total session used time, measured in seconds. A user session starts when the guest user is authenticated, and ends when the guest user is disassociated.
L	Is the guest user account synchronized on a secondary controller in an availability pair, yes (1) no (0)

1 To export a guest file, do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
  - From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
  - In the left pane, expand the WLAN Services pane, click the dedicated *WLAN* Service that provides the temporary guest network services. The WLAN Services configuration window for that service displays.
  - Click the Auth & Acct tab, and then click **Configure**. The Settings screen displays.
  - In the **Guest Splash** section, click **Manage Guest Users**.

The Guest Splash Administration screen displays.

2 In the **File Management** section, click **Export Guest File**.

A File Download dialog is displayed.

3 Click **Save**.

The Save As dialog is displayed.

4 Name the guest file, and then navigate to the location where you want to save the file.

By default, the exported guest file is named `exportguest.csv`.

5 Click **Save**.

The File Download dialog is displayed as the file is exported.

6 Click **Close**.

A confirmation message is displayed in the Guest Splash Administration screen footer.

7 To import a guest file, do one of the following:

- If you have Guest Splash Manager rights, log onto the controller.
- If you have full administrator rights:
  - From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
  - In the left pane, expand the WLAN Services pane, click the dedicated WLAN Service that provides the temporary guest network services. The WLAN Services configuration window for that service displays.
  - Click the Auth & Acct tab, and then click **Configure**. The Settings screen displays.
  - In the Guest Splash section, click **Manage Guest Users**.
  - The GuestPortal Guest Administration screen displays.

8 In the **File Management** section, click **Import Guest File**.

The Import Guest File dialog is displayed.

9 Click **Browse** to navigate to the location of the .csv guest file that you want to import, and then click **Open**.

10 Click **Import**.

The file is imported and a confirmation message is displayed in the Import Guest File dialog.

11 Click **Close**.

Viewing and Printing a GuestPortal Account Ticket

You can view and print a GuestPortal account ticket from the GuestPortal Guest Administration screen. A GuestPortal account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account.

The controller is shipped with a default template for the GuestPortal account ticket. The template is an html page that is augmented with system placeholders that display information about the user.

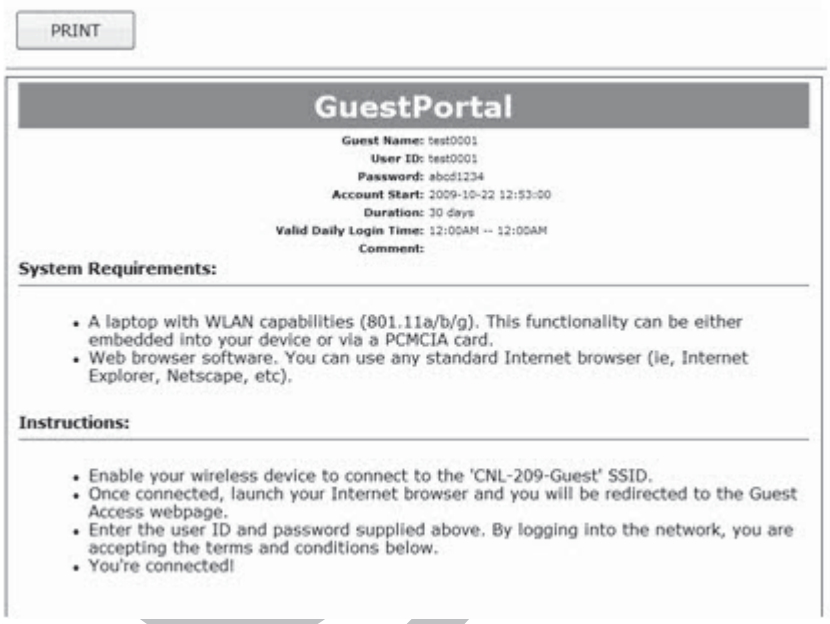
You can also upload a custom GuestPortal ticket template for the controller. To upload a custom GuestPortal ticket template you need full administrator access rights on the controller. The filename of a custom GuestPortal ticket template must be .html. For more information, see Working with the Guest Portal Ticket Page on page 700.

To view and print a GuestPortal account ticket:

1 Do one of the following:

- If you have GuestPortal Manager rights, log onto the controller.
- If you have full administrator rights:
  - From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
  - In the left pane, expand the **WLAN Services** pane, click the dedicated *WLAN* Service that provides the temporary guest network services. The **WLAN Services** configuration window for that service displays.
  - Click the **Auth & Acct** tab, and then click **Configure**. The Settings screen displays.
  - In the **GuestPortal** section, click **Manage Guest Users**.
  - The GuestPortal Guest Administration screen displays.

2 In the guest account list, select the check box next to the user name whose guest account ticket you want to print a ticket, and then click **Print Ticket for Selected Account**. The **GuestPortal** ticket is displayed.



3 Click **Print**. The Print dialog is displayed.

4 Click **Print**.

Note
The default GuestPortal ticket page uses placeholder tags. For more information, see Default GuestPortal Ticket Page on page 706.

Working with the Guest Portal Ticket Page

From the GuestPortal ticket page, you can activate a GuestPortal ticket page, upload a customized GuestPortal ticket page to the controller, and delete a customized GuestPortal ticket page.

Note
The default GuestPortal ticket page cannot be deleted.

To work with the GuestPortal account ticket page, you need full administrator rights. You can work with the guest account ticket page from the Settings screen. A guest account ticket is a print-ready form that displays the guest account information, system requirements, and instructions on how to log on to the guest account.

Related Links

Working with a Custom GuestPortal Ticket Page on page 701
Activating a GuestPortal Ticket Page on page 701
Uploading a Custom GuestPortal Ticket Page on page 701
Deleting a Custom GuestPortal Ticket Page on page 701
Example Ticket Page on page 706

Working with a Custom GuestPortal Ticket Page

A customized GuestPortal ticket page can be uploaded to the controller. When designing your customized GuestPortal ticket page, be sure to use the guest account information placeholder tags that are depicted in the default GuestPortal ticket page. For more information, see Default GuestPortal Ticket Page on page 706.

Activating a GuestPortal Ticket Page

To activate a GuestPortal ticket page:

1. From the top menu, click **VNS**.
2. In the left pane, expand the WLAN Services pane, click the dedicated *WLAN* Service that provides the temporary guest network services. The WLAN Services configuration window for that service displays.
3. Click the Auth & Acct tab, and then click **Configure**. The Settings screen displays.
4. In the **GuestPortal** section, click **Configure Ticket Page**. The Ticket Settings dialog is displayed.
5. In the **Active Template** list, click the GuestPortal ticket page you want to activate, and then click **Apply**.

   This list includes all GuestPortal ticket pages that have been uploaded to the controller.

Uploading a Custom GuestPortal Ticket Page

To upload a custom GuestPortal ticket page:

1. On the Ticket Settings dialog, click **Browse**. The Choose file dialog is displayed.
2. Navigate to the .html GuestPortal ticket page file that you want to upload to the controller, and then click **Open**. The file name is displayed in the **Upload Template** box.
3. Click **Apply**. The file is uploaded to the controller.

   The **Active Template** list includes all GuestPortal ticket pages that have been uploaded to the controller.

Deleting a Custom GuestPortal Ticket Page

To delete a custom GuestPortal ticket page:

1. On the **Ticket Settings** dialog, in the **Active Template** list, click the GuestPortal ticket page you want to delete, and then click **Delete**.

   A dialog prompts you to confirm you want to delete the GuestPortal ticket page.
2. To delete the file, click **OK**, and then click **Apply**.

Configuring Guest Password Patterns

This feature makes it easier for system administrators to create password patterns that the Wireless Assistant will use to auto generate guest passwords. You can specify a predefined pattern or you can

create a customized pattern. You must have full administrative rights to generate password patterns. Select from the following password patterns:

- Completely Random Sequence
- Two Words
- Phone number
- Postal Code
- Custom Pattern

The generator offers three character sets: Latin (ASCII), Cyrillic, and Greek.

Related Links

To Configure a Guest Password Pattern on page 702

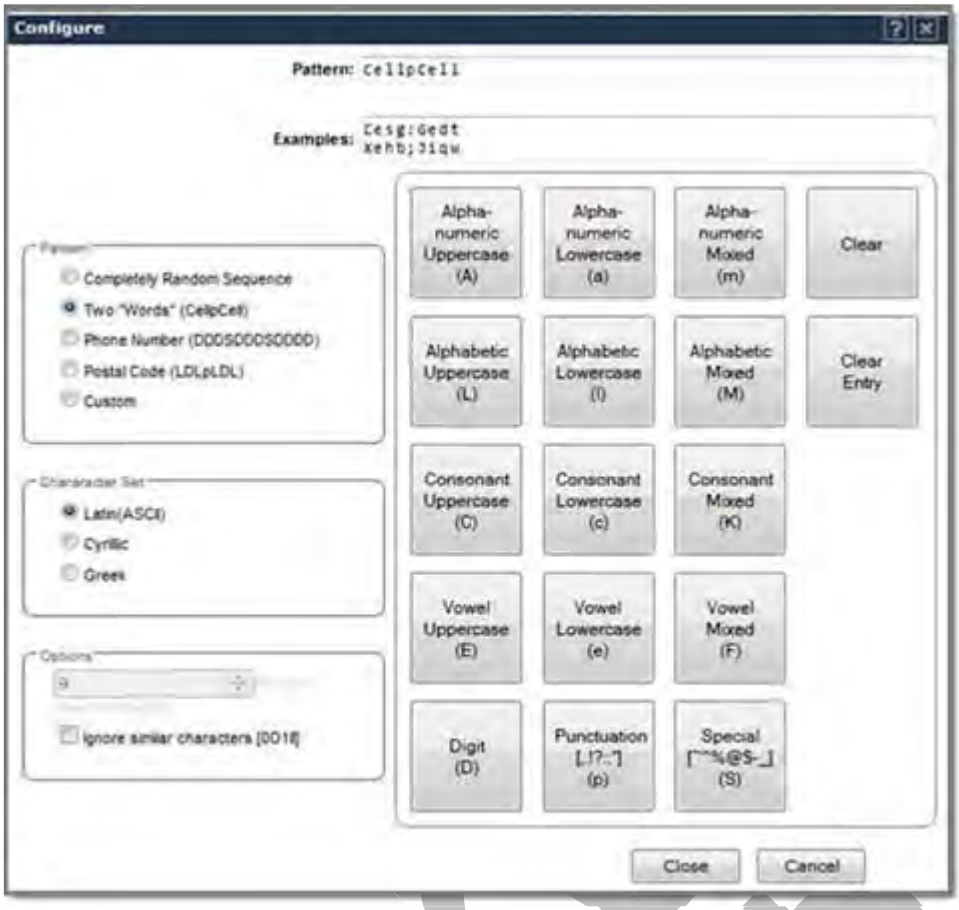
To Configure a Guest Password Pattern

To generate a password pattern:

1 From the top menu, click **VNS**. The Virtual Network Configuration screen displays.
2 In the left pane, expand the WLAN Services pane, click the dedicated *WLAN* Service that provides the temporary guest network services. The WLAN Services configuration window for that service displays.
3 Click the Auth & Acct tab, and then click **Configure**. The Settings screen displays.

4 In the GuestPortal section, click **Configure Password Generator**.

The Configure Password Generator screen displays.



To generate a custom password pattern:

1 From the Pattern pane, select **Custom**.

2 Select the character set and minimum password length.

3 Use the keypad to enter the pattern characters or type the pattern in the Pattern field.

> **Note**
> You can only type characters that are represented on the keypad. Entries in the **Pattern** field are editable.

The **Clear** key on the keypad clears the full pattern.

The **Clear Entry** key on the keypad clears the last entered character.

The password pattern displays in the **Pattern** field. Copy paste this pattern into the Add Guest User dialog. For more information, see Adding New Guest Accounts on page 690.

5 Click **Close** to close the dialog and save the password pattern.

6 Click **Cancel** to close the dialog without saving the password pattern.

Configuring Web Session Timeouts

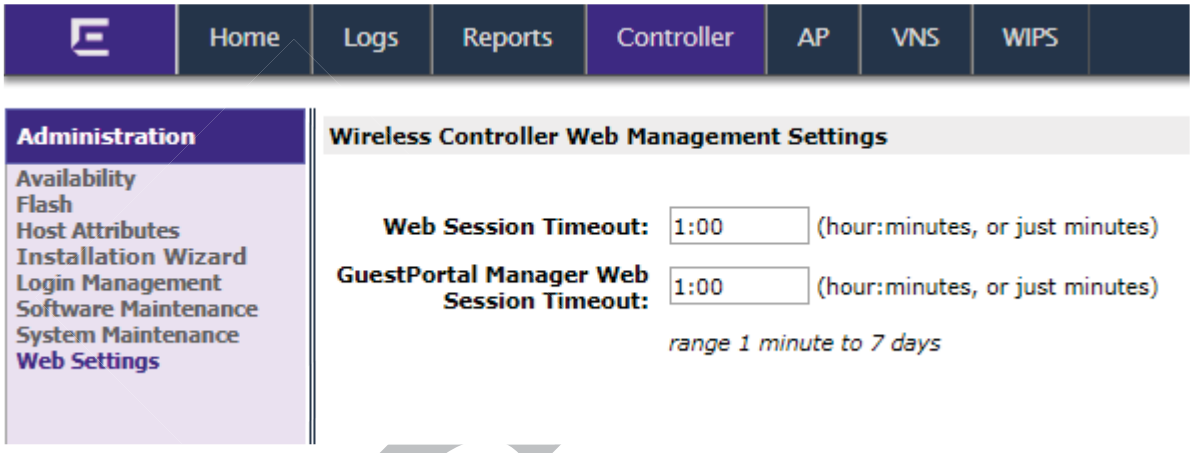
You can configure the time period to allow web sessions to remain inactive before timing out. To configure web session timeouts:

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

The Wireless Controller Configuration screen displays.

2 In the left pane, click **Administration** > **Web Settings**

The Wireless Controller Web Management Settings screen displays.



3 In the **Web Session Timeout** box, type the time period to allow the web session to remain inactive before it times out.

This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.

4 In the **GuestPortal Manager Web Session Timeout** box, type the time period to allow the GuestPortal web session to remain inactive before it times out.

This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.

5 To save your settings, click **Save**.

Note

Screens that auto-refresh will time-out unless a manual action takes place prior to the end of the timeout period.

A Regulatory Information

ExtremeWireless APs 37XX , 38XX, and 39XX

Warning
Warnings identify essential information. Ignoring a warning can lead to problems with the application.

Note
For technical specifications and certification information for a specific Outdoor AP refer to the appropriate AP Installation Guide.

Configuration of the ExtremeWireless AP frequencies and power output are controlled by the regional software license and proper selection of the country during initial installation and set-up. Customers are allowed to select only the proper country from their licensed regulatory domain related to that customer's geographic location, performing the set-up of access points in accordance with local laws and regulations. The ExtremeWireless AP must not be operated until configured with the correct country setting or it may be in violation of the local laws and regulations.

Warning
Changes or modifications made to the APs which are not expressly approved by Extreme Networks could void the user's authority to operate the equipment. Only authorized Extreme Networks service personnel are permitted to service the system. Procedures that must be performed only by Extreme Networks personnel are clearly identified in the respective AP guide.

Note
The APs are in compliance with the European Directive 2002/95/EC on the restriction of the use of certain hazardous substances (RoHS) in electrical and electronic equipment.

ExtremeWireless APs 37XX , 38XX, and 39XX

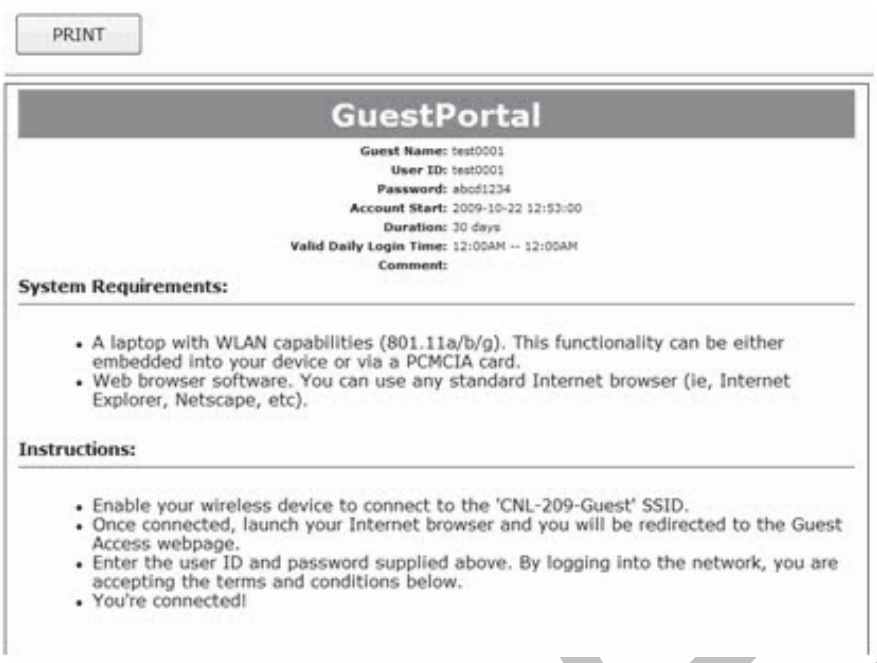
For regulatory information for the ExtremeWireless AP models 37xx, 38xx, and 39XX refer to the appropriate AP *Installation Guide*.

B Default GuestPortal Ticket Page

Example Ticket Page

This section provides an example ticket page with an explanation of each placeholder variable and example HTML source code.

Example Ticket Page



Placeholders Used in the Default GuestPortal Ticket Page

Table 134: Default GuestPortal Ticket Page Template Placeholders

Placeholder tag	Description
!GuestName	Guest Name
!GuestComment	Guest Comment
!TimeOfDayStart	Time-of-day start
!TimeOfDayDuration	Time-of-day session duration
!SessionLifeTime	Maximum session time
!UserID	User ID for the guest
!Password	Password for the guest

Table 134: Default GuestPortal Ticket Page Template Placeholders (continued)

Placeholder tag	Description
!SSID	SSID to connect to
!AccountActivationTime	Account available time
!AccountLifeTime	Account life time

Default GuestPortal Ticket Page Source Code

Note

The GuestPortal account information placeholders used in the html code are preceded by the ! character.

```
<HTML>
<HEAD>
        <title></title>
        <meta content="text/html;charset=utf-8" http-equiv="Content-Type"/>
</HEAD>
<body style="text-align:center">
        <table cellspacing="0" cellpadding="0" border="0" align="center" width="790">
        <tr>
                <td style="background-color:gray;color:white;font-weight:bold;font-size:
30;padding:5px"
align="center" width="790">GuestPortal</td>
        </tr>
        </table>
        <table cellspacing="5" cellpadding="0" border="0" style="margin:0 auto">
        <tr>
                <td align="right"><b>Guest Name:</b></td>
                <td align="left">!GuestName</td>
        </tr>
        <tr>
                <td align="right"><b>User ID:</b></td>
                <td align="left">!UserID</td>
        </tr>
        <tr>
                <td align="right"><b>Password:</b></td>
                <td align="left">!Password</td>
        </tr>
        <tr>
                <td align="right"><b>Account Start:</b></td>
                <td align="left">!AccountActivationTime</td>
        </tr>
        <tr>
                <td align="right"><b>Duration:</b></td>
                <td align="left">!AccountLifeTime</td>
        </tr>
        <tr>
                <td align="right"><b>Valid Daily Login Time:</b></td>
                <td align="left">!TimeOfDayStart -- !TimeOfDayDuration</td>
        </tr>
        <tr>
                <td align="right"><b>Comment:</b></td>
                <td align="left">!GuestComment</td>
        </tr>
        </table>
         <div style="width:790px;margin:0 auto;text-align:left">
```

```
                <b>System Requirements:</b>
                <hr width=790 size=2 noshade>
                <div style="padding-left:30px">
                        <ul>
                                <li>A laptop with WLAN capabilities (801.11a/b/g). This
functionality can be either embedded into your device or via a PCMCIA card.
                                <li>Web browser software. You can use any standard
Internet browser (ie, Internet Explorer, Netscape, etc).
                        </ul>
                </div>
        </div>
        <div style="width:790px;margin:10px auto;text-align:left">
                <b>Instructions:</b>
                <hr width=790 size=2 noshade>
                <div style="padding-left:30px;">
                        <ul>
                                <li>Enable your wireless device to connect to the '!SSID'
SSID.
                                <li>Once connected, launch your Internet browser and you
will be redirected to the Guest Access webpage.
                                <li>Enter the user ID and password supplied above. By
logging into the network, you are accepting the terms and conditions below.
                                <li>You're connected!
                        </ul>
                 </div>
         </div>
</div>
</body>
</HTML>
```

Glossary

ACL

An Access Control List is a mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP address, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

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.

CoS

Class of Service specifies the service level for the classified traffic type.

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 Access Control

EAC, formerly NAC™, featuring both physical and virtual appliances, is a pre- and post-connect solution for wired and wireless LAN and VPN users. Using Identity and Access appliances and/or Identity and Access Virtual Appliance with the *XMC (Extreme Management Center)* software, you can ensure only the right users have access to the right information from the right place at the right time. EAC is tightly integrated with the Intrusion Prevention System (IPS) and Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control. Learn more about EAC at http://www.extremenetworks.com/product/extreme-access-control/.

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 (Extreme Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Extreme 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, Extreme Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Extreme Management Center at http://www.extremenetworks.com/product/management-center/.

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/.

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*.

ICMP

Internet Control Message Protocol is the part of the TCP/IP protocol that allows generation of error messages, test packets, and operating messages. For example, the ping command allows you to send ICMP echo messages to a remote IP device to test for connectivity. ICMP also supports traceroute, which identifies intermediate hops between a given source and destination.

IGMP

Hosts use Internet Group Management Protocol to inform local routers of their membership in multicast groups. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. When all hosts leave a group, the router no longer forwards packets that arrive for the multicast group.

LAG

A Link Aggregation Group is the logical high-bandwidth link that results from grouping multiple network links in link aggregation (or load sharing). You can configure static LAGs or dynamic LAGs (using the LACP).

LLDP

Link Layer Discovery Protocol conforms to IEEE 802.1ab and is a neighbor discovery protocol. Each LLDP-enabled device transmits information to its neighbors, including chassis and port identification, system name and description, VLAN names, and other selected networking information. The protocol also specifies timing intervals in order to ensure current information is being transmitted and received.

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*.)

PoE

The Power over Ethernet standard (IEEE 802.3af) defines how power can be provided to network devices over existing Ethernet connections, eliminating the need for additional external power supplies.

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.

WLAN

Wireless Local Area Network.