Managing the Mobility Express Network

Under the Management tab on the navigation pane, an admin users can do the following:

1. Configure access to the Mobility Express controller
2. Manage Admin Accounts
3. Configure Time
4. Perform a Software Update

Configuring Management Access

The Management Access Interface on the Mobility Express controller is the default interface for in-band management of the controller and connectivity to enterprise services. It is also used for communications between the controller and access points.

There are four types of Management Access supported on the Mobility Express controller.

1. HTTP Access-To enable HTTP access mode, which allows you to access the controller GUI using http://<ip-address> through a web browser, choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled.

   The default value is Disabled. HTTP access mode is not a secure connection.

2. HTTPS Access-To enable HTTPS access mode, which allows you to access the controller GUI using http://ip-address through a web browser, choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled.

   The default value is Enabled. HTTPS access mode is a secure connection.

3. Telnet Access-To enable Telnet access mode, which allows remote access to the controller's CLI using your laptop's command prompt, choose Enabled from the Telnet Access drop-down list. Otherwise, choose Disabled.

The default value is Disabled. The Telnet access mode is not a secure connection.

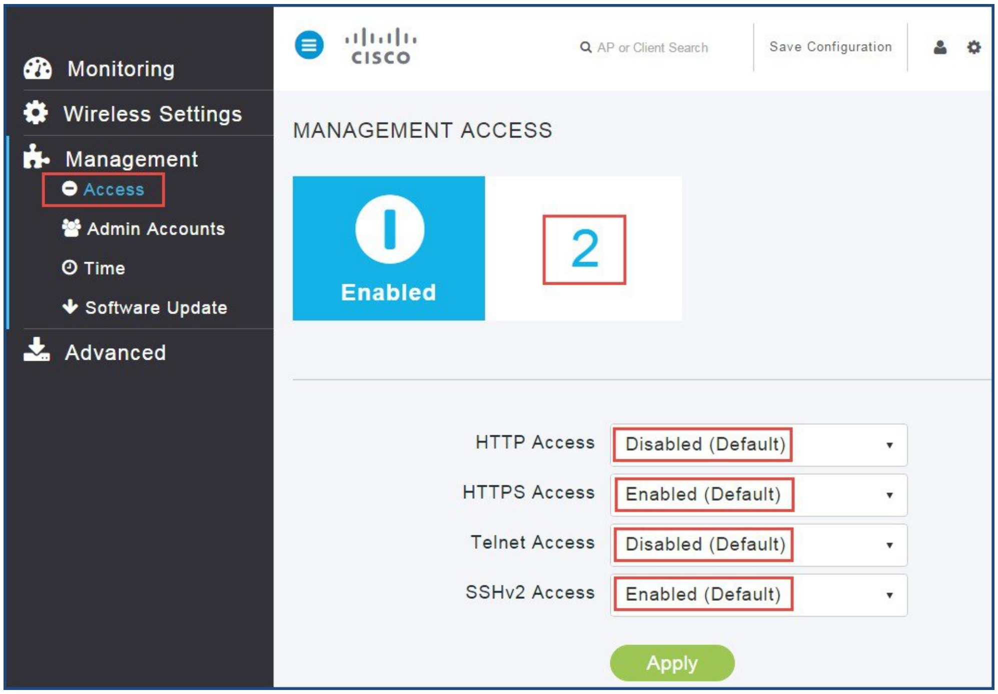
4. SSHv2 Access-To enable Secure Shell Version 2 (SSHv2) access mode, which is a more secure version of Telnet that uses data encryption and a secure channel for data transfer, choose Enabled from the SSHv2 Access drop-down list. Otherwise, choose Disabled.

   The default value is Enabled. The SSHv2 access mode is a secure connection.

To enable or disable the different types of management access to the controller, do the following:

Procedure

Step 1 Navigate to **Management** > **Access**. The Management Access page is shown displaying the count of the access type which are enabled.



MANAGEMENT ACCESS

Enabled: 2

HTTP Access: Disabled (Default)

HTTPS Access: Enabled (Default)

Telnet Access: Disabled (Default)

SSHv2 Access: Enabled (Default)

Step 2 For the various Access Types, select either Enabled or Disabled.

Note There must be at least one access enabled else admin user will locked out of Mobility Express Controller and will have to use console to make changes to provide access again.

Step 3 Click the Apply button to submit the changes.

Managing Admin Accounts

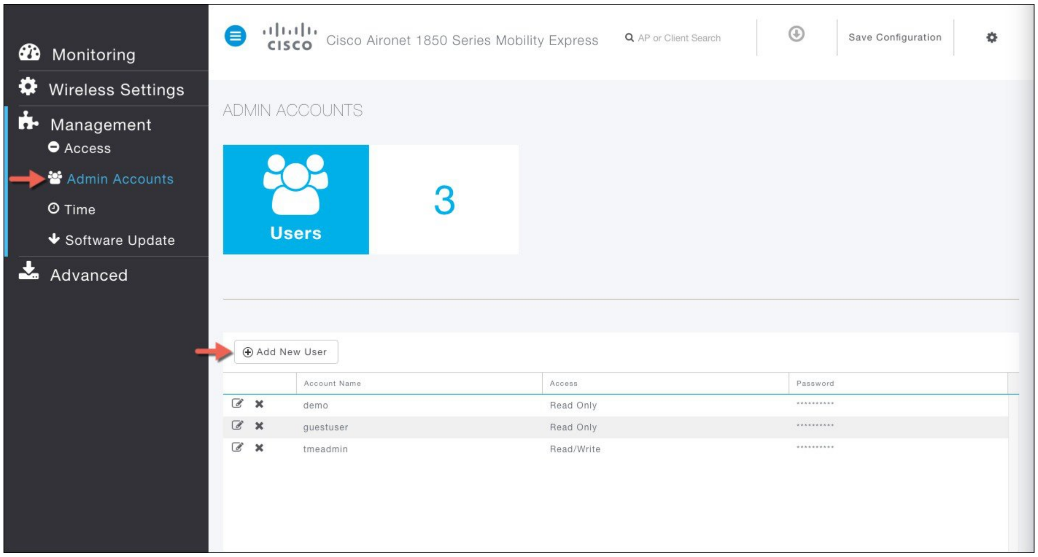
Cisco Mobility Express supports creation of admin usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

Admin user accounts are required for logging into Mobility Express controller to monitor and configure the wireless network. Admin accounts can be configured with Read/Write or Read only privileges.

To create these users, follow the steps below.

Procedure

Step 1 Navigate to **Management Admin Accounts** and click on the **Add New User** button.



	Account Name	Access	Password
✎ ✖	demo	Read Only	**********
✎ ✖	guestuser	Read Only	**********
✎ ✖	tmeadmin	Read/Write	**********

Step 2 Enter the following to configure the admin user account.

a) **Account Name** - Enter the admin user name. Usernames are case-sensitive and can contain up to 24 ASCII characters. Usernames cannot contain spaces

Note Admin account name must be unique

b) **Access -** Select Read/Write or Read Only access for the admin account

- Read Only - This option creates an administrative account with read-only privileges. The admin user can only view the controller configuration but cannot make any changes to the configuration.

- Read/Write - This option creates an administrative account with read and writes privileges. The admin user can view and make changes to the controller configuration.

c) **New Password & Confirm Password -** Enter a password for the admin user account, in-keeping with the following rules:

- Passwords are case sensitive and cannot contain spaces

- The password should contain a minimum of 8 characters from ALL of the following classes:

  Lowercase letters

  Uppercase letters

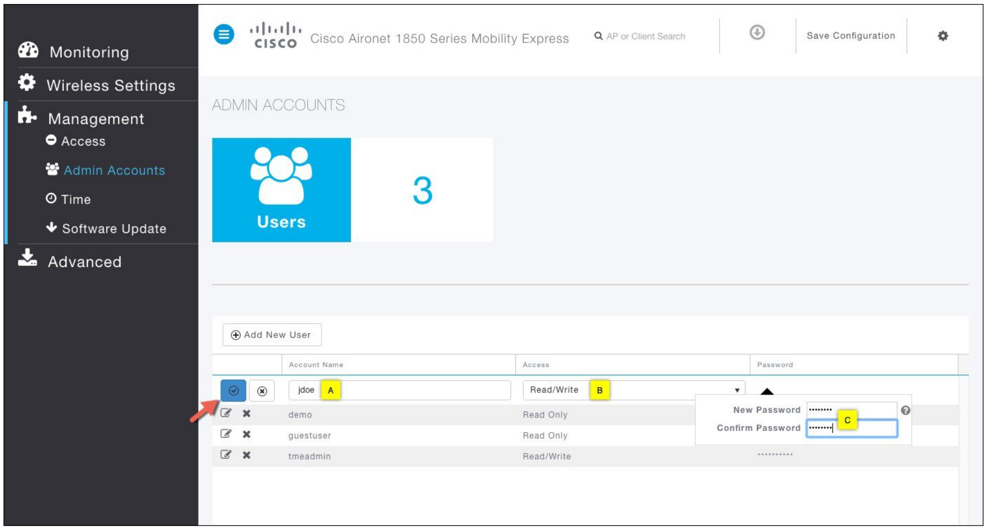
  Digits

  Special characters

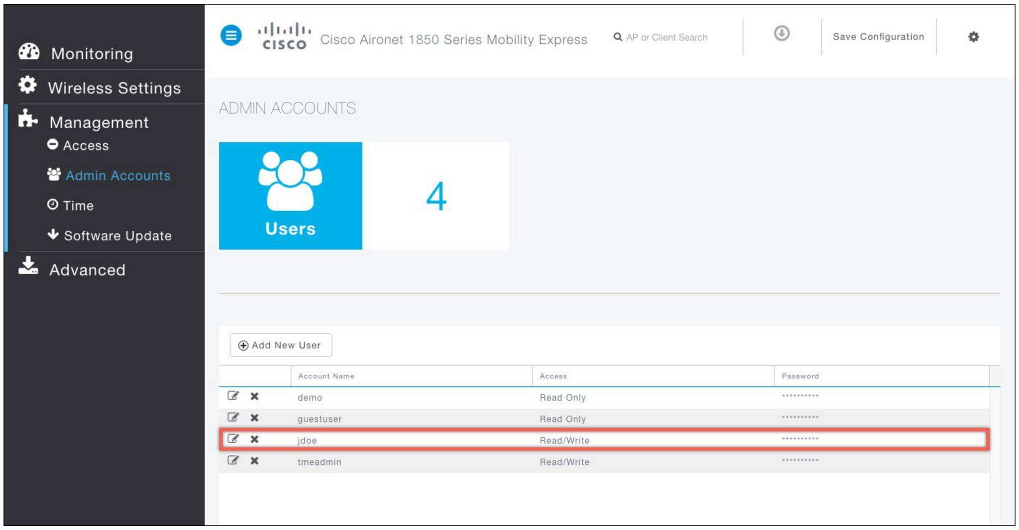
- No character in the password can be repeated more than three times consecutively.

- The password should not contain the word Cisco or a management username. The password should also not be any variant of these words, obtained by reversing the letters of these words, or by changing the capitalization of letters, or by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

d) Click on the icon pointed by the Red arrow to create the account.



Account Name	Access	Password
jdoe	Read/Write	New Password ········· Confirm Password ·········
demo	Read Only	
guestuser	Read Only	
tmeadmin	Read/Write	··········



Account Name	Access	Password
demo	Read Only	··········
guestuser	Read Only	··········
jdoe	Read/Write	··········
tmeadmin	Read/Write	··········

Managing TIME on Mobility Express Controller

The system date and time on the Cisco Mobility Express controller is first configured when running the initial Wireless Express setup wizard.

A Network Time Protocol (NTP) server can be configured to sync date and time if one was not configured during the Wireless Express setup. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

Configuring NTP Server on Mobility Express Controller from GUI

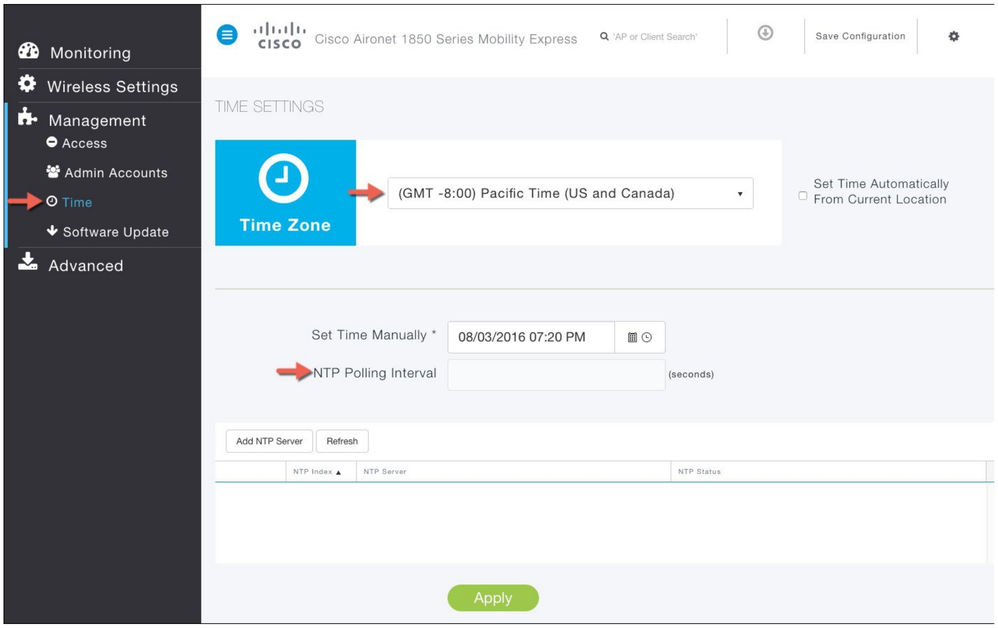
To configure an NTP server, perform the following steps:

Procedure

Step 1 Navigate to **Management > Time** from the left pane.

Step 2 Choose the desired **Time Zone** from the **Time Zone** drop down list.

Step 3 Enter the **NTP Polling Interval**. The polling interval ranges from 3600 to 604800 seconds.



TIME SETTINGS

Time Zone: (GMT -8:00) Pacific Time (US and Canada)

□ Set Time Automatically From Current Location

Set Time Manually * 08/03/2016 07:20 PM

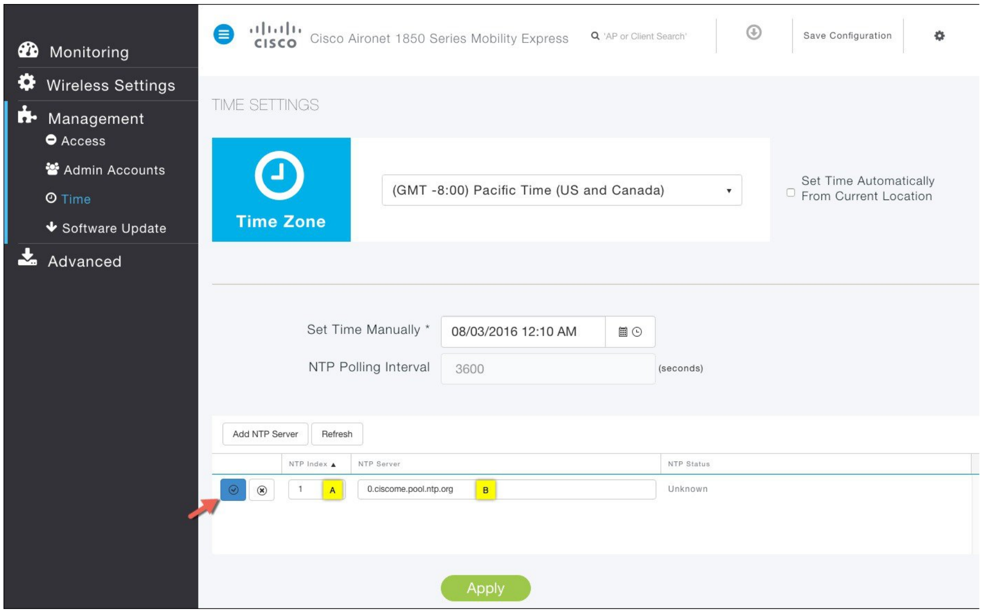
NTP Polling Interval (seconds)

Step 4 To add an NTP server, click **Add NTP Server** button and configure the following:

- NTP Index
- NTP Server - This can be the NTP Server IP address, NTP Server Name or pool. A maximum of three NTP Servers are supported.

Step 5 Click on the icon pointed by the Red arrow to add the NTP Server.

Note Synchronization of the date and time with the NTP Server occurs each time the controller reboots and at each user-defined polling interval.



(GMT -8:00) Pacific Time (US and Canada)

□ Set Time Automatically From Current Location

Set Time Manually * 08/03/2016 12:10 AM

NTP Polling Interval 3600 (seconds)

	NTP Index ▲	NTP Server	NTP Status
	1 A	0.ciscome.pool.ntp.org B	Unknown

Step 6 Click on the **Apply** Button.

Configuring Date and Time manually on Mobility Express Controller from GUI

To configure Date and Time manually, follow the steps below.

Procedure

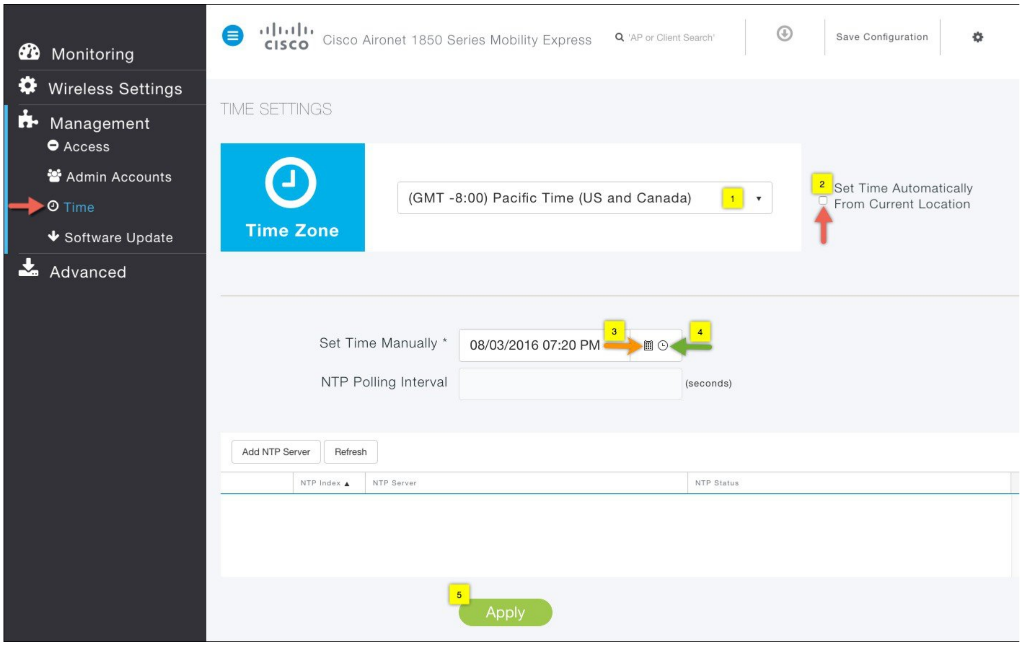
Step 1 Select the desired Time Zone from the drop down list.

Step 2 [Optional] Click the Set Time Automatically from Current Location check box, to adjust the time based on the Time Zone specified.

Step 3 Click on Date icon from Set Time Manually field and configure Date from the calendar.

Step 4 Click on Time icon from Set Time Manually field and configure time from the drop down list.

Step 5 Click the Apply button.



TIME SETTINGS

(GMT -8:00) Pacific Time (US and Canada)

□ Set Time Automatically From Current Location

Set Time Manually * 08/03/2016 07:20 PM

NTP Polling Interval (seconds)

NTP Index ▲	NTP Server	NTP Status

Updating Cisco Mobility Express Software

Cisco Mobility Express controller software update can be performed using the controller's web interface. Software update ensures that both the controller software and all the Access Points associated are updated. The Access Points that have older software are automatically upgraded to the Mobility Express software on joining the master AP. An AP joining the controller compares its software version with the master AP version and incase of mismatch, the new AP requests for a software upgrade. The master AP facilitates the transfer of the new software from the TFTP server to the new AP.

Software download on the Access Points is automatically sequenced to ensure that not more than 5 APs are downloading the software simultaneously and the queue refreshes till all the APs requiring upgrade have downloaded the new image.

Release 8.3.100.0 supports the following transfer modes for Software Update:

1. Cisco.com - Cisco.com transfer mode is introduced in 8.3.100.0. In this software update method, the software image can be directly streamed from cisco.com to the individual Access Points. Internet access required for this transfer mode and EULA and SMARTNet contract requirements have to be met for this transfer mode.
2. HTTP - HTTP transfer mode is supported if the Mobility Express Network has the same model of Access Points. Use HTTP as the transfer mode for Software Update using the AP file from a local machine.

Note If there is a mix of Access Points in the Mobility Express network, Software Update via cisco.com or TFTP must be used.

3. TFTP - TFTP transfer mode can be used to perform Software Update on a Mobility Express Network. Master AP facilitates transfer of image from the TFTP server to the Subordinate APs. The AP images are stored and served from the TFTP server upon request.

Note
- There is no service interruption during pre-image download. After pre-image download is complete on all APs, a Manual or scheduled reboot of Mobility Express network can be triggered.
- After the pre-image download is initiated, no new AP that has a different version than the running controller will be able to join until it is fully upgraded and is running the new image.

Software Update via cisco.com

Software Update via Cisco.com works on all APs supported in a Cisco Mobility Express Deployment. Below requirements must be met to initiate a Software Update from cisco.com.

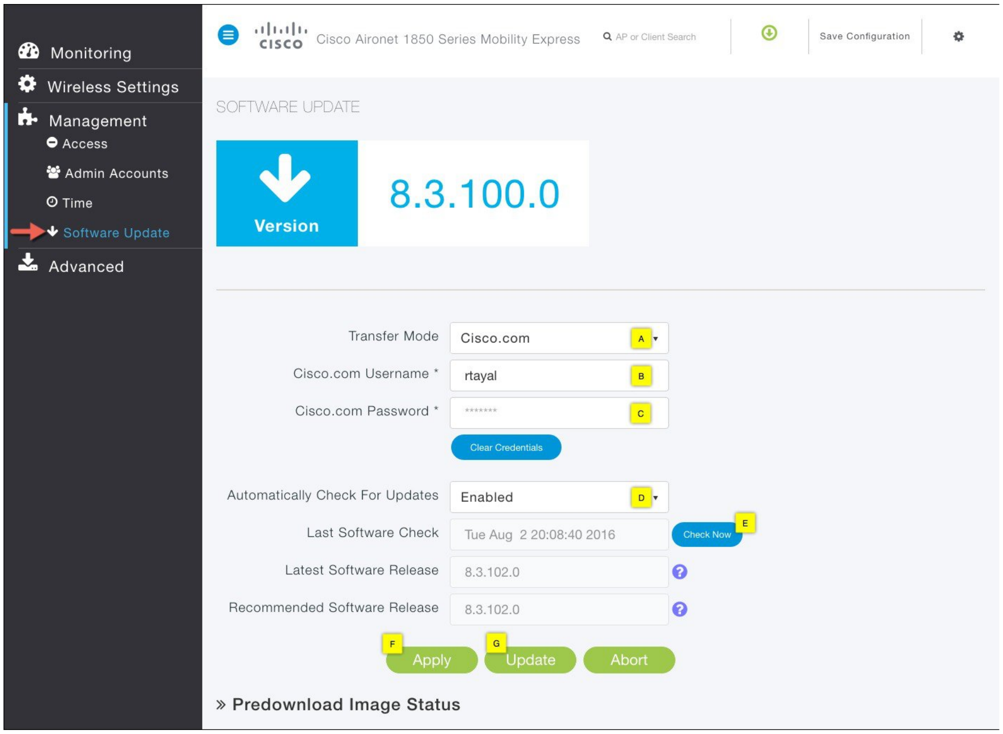
1. Internet access is required for software download from cisco.com to APs. However, no proxy is required.
2. A valid cisco.com (CCO) account with username & password required.
3. EULA Acceptance on a per user basis. Master AP (not all APs in the network) must have SMARTNet contract else Software Update will not start.

Note Software Update from cisco.com is supported via GUI only.

Procedure

Step 1 To perform Software Update via Cisco.com, navigate to **Management > Software Update** and perform the following:

a) For **Transfer Mode** select ***Cisco.com*** from the drop down list.
b) Enter Cisco.com Username.
c) Enter Cisco.com Password.
d) Enable **Automatically Check for Updates**. Check is done once in 30 days.
e) Click on the **Check Now** button to retrieve the Latest Software Release and the Recommended Software Release from Cisco.com.
f) Click on the **Apply** Button
g) Click on **Update** button to initiate software update



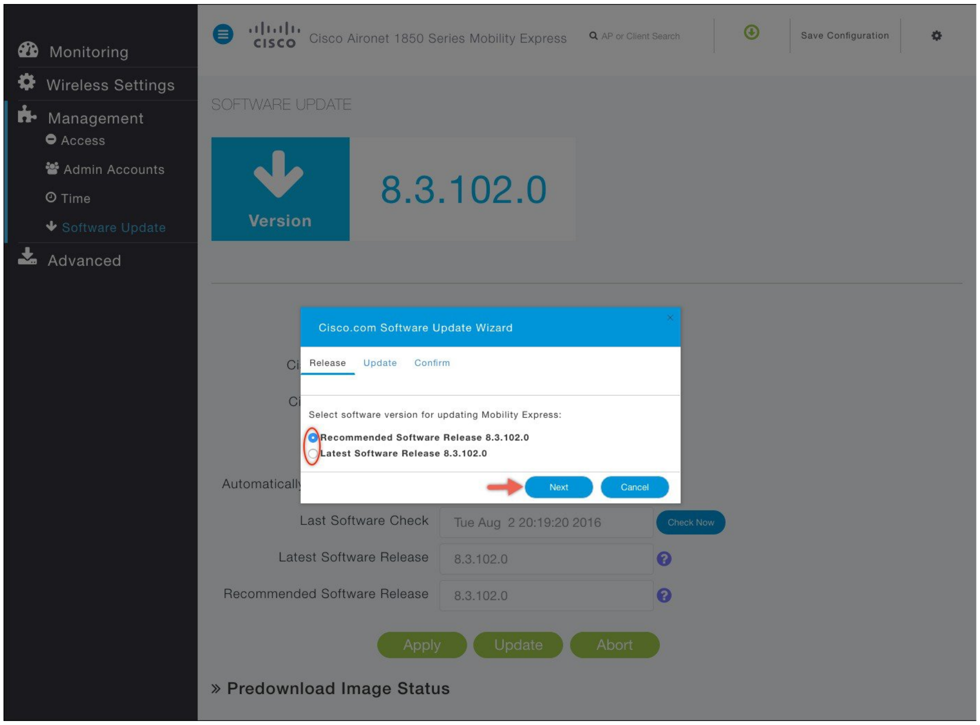
SOFTWARE UPDATE

Version 8.3.100.0

Transfer Mode: Cisco.com
Cisco.com Username *: rtayal
Cisco.com Password *: *******
Automatically Check For Updates: Enabled
Last Software Check: Tue Aug 2 20:08:40 2016
Latest Software Release: 8.3.102.0
Recommended Software Release: 8.3.102.0

» Predownload Image Status

h) In the Software Update Wizard, select the Recommended Software Release or Latest Software Release. Click on the **Next** Button.



SOFTWARE UPDATE

Version 8.3.102.0

Cisco.com Software Update Wizard

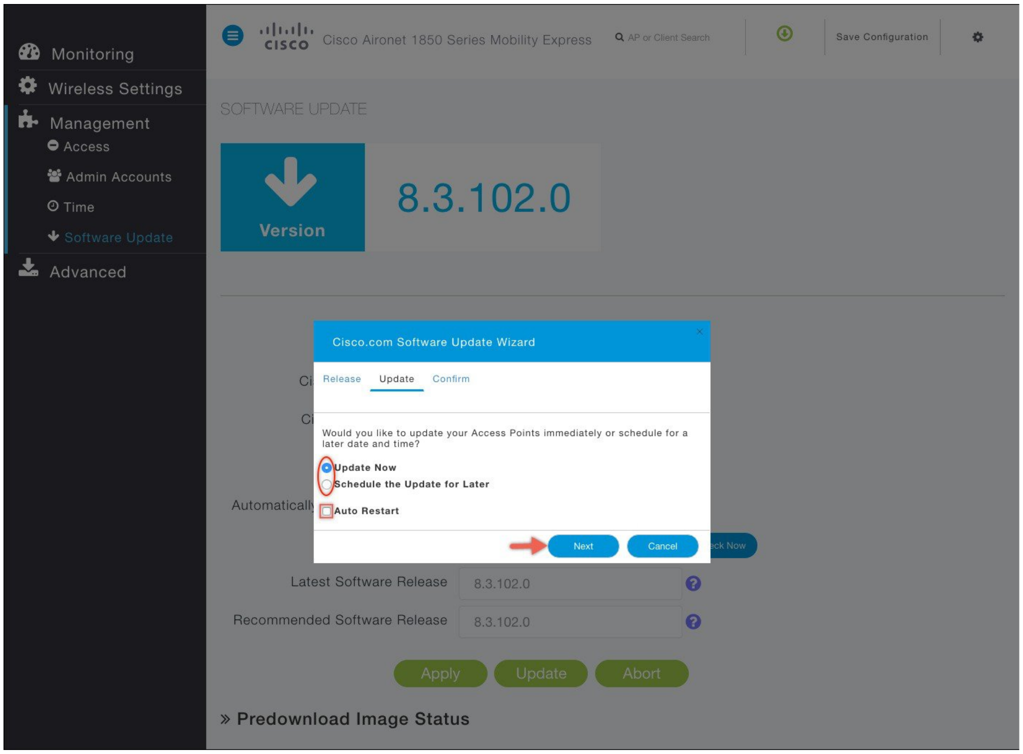
Select software version for updating Mobility Express:
● Recommended Software Release 8.3.102.0
○ Latest Software Release 8.3.102.0

Last Software Check: Tue Aug 2 20:19:20 2016
Latest Software Release: 8.3.102.0
Recommended Software Release: 8.3.102.0

» Predownload Image Status

i) Select **Update Now** to initiate software update immediately or **Schedule the Update for Later**. If **Schedule the Update for Later** is selected, configure the **Set Update Time** field.

j) Click on the Auto Restart checkbox if automatic restart of all access points in the network is desired after the software update is finished. Click on the **Next** button.



Would you like to update your Access Points immediately or schedule for a later date and time?

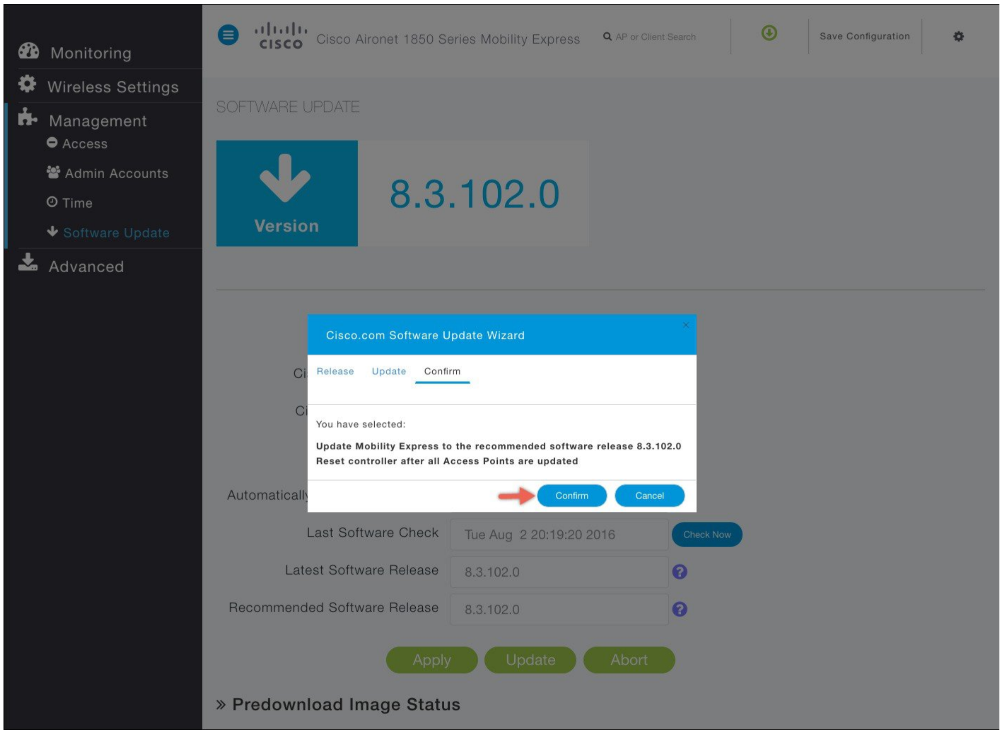
● Update Now
○ Schedule the Update for Later

□ Auto Restart

Latest Software Release: 8.3.102.0

Recommended Software Release: 8.3.102.0

k) Click on **Confirm** button to start the software update.

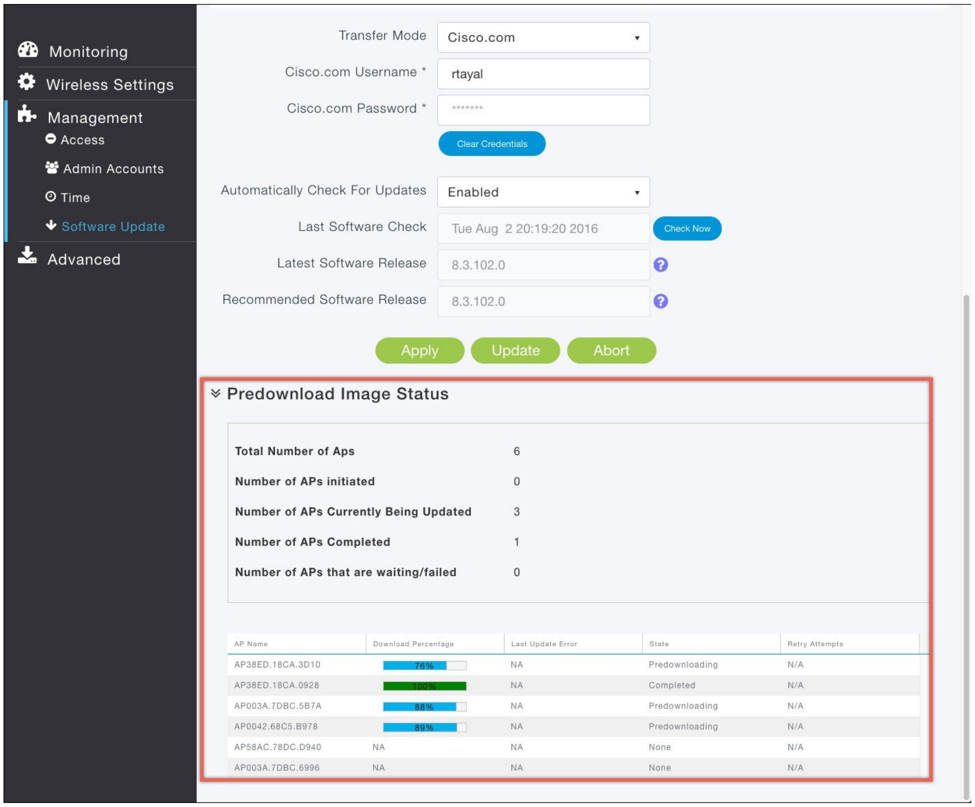


You have selected:

Update Mobility Express to the recommended software release 8.3.102.0
Reset controller after all Access Points are updated

Last Software Check	Tue Aug 2 20:19:20 2016
Latest Software Release	8.3.102.0
Recommended Software Release	8.3.102.0

Step 2 To view the download status, expand the Predownload image status.



Transfer Mode: Cisco.com

Cisco.com Username *: rtayal

Cisco.com Password *: *******

Automatically Check For Updates: Enabled

Last Software Check: Tue Aug 2 20:19:20 2016

Latest Software Release: 8.3.102.0

Recommended Software Release: 8.3.102.0

Predownload Image Status

Total Number of Aps	6
Number of APs initiated	0
Number of APs Currently Being Updated	3
Number of APs Completed	1
Number of APs that are waiting/failed	0

AP Name	Download Percentage	Last Update Error	State	Retry Attempts
AP38ED.18CA.3D10	76%	NA	Predownloading	N/A
AP38ED.18CA.0928	100%	NA	Completed	N/A
AP003A.7DBC.5B7A	88%	NA	Predownloading	N/A
AP0042.68C5.B978	89%	NA	Predownloading	N/A
AP58AC.78DC.D940	NA	NA	None	N/A
AP003A.7DBC.6996	NA	NA	None	N/A

Software Update via HTTP

Procedure

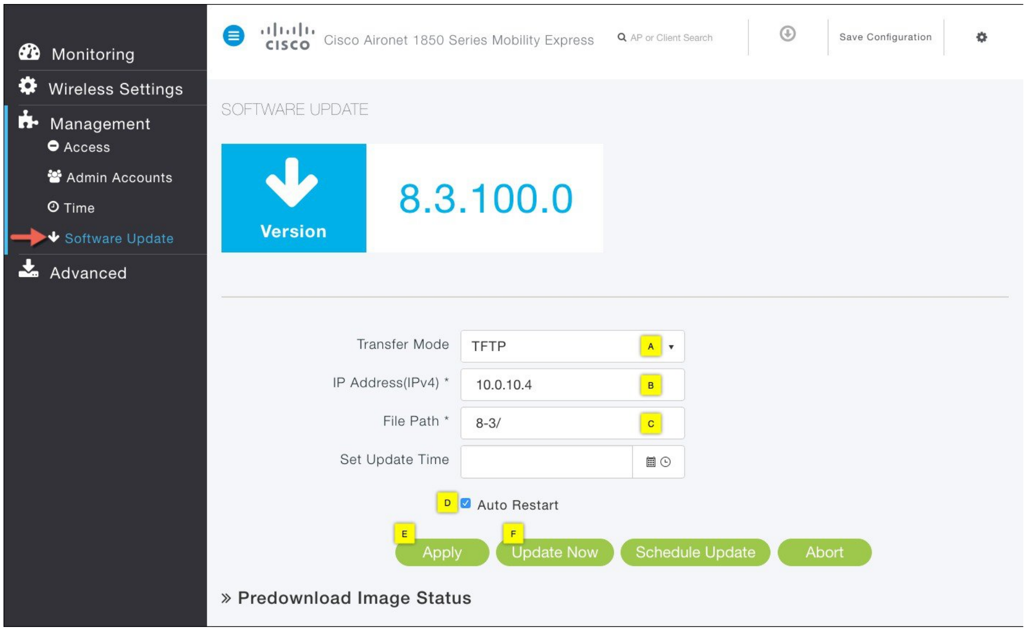
Step 1 Download the AP Image bundle from cisco.com to the local machine.

Step 2 Unzip the AP Image bundle to extract individual AP Images. Mapping of Access Points to their corresponding images is shown below.

AP Model	AP Image
AIR-AP1830	ap1g4
AIR-AP1850	ap1g4
AIR-AP2800	ap3g3
AIR-AP3800	ap3g3

Step 3 To perform Software Update via HTTP, navigate to **Management** > **Software Update** and perform the following:

a) For **Transfer Mode** select ***HTTP*** from the drop down list.
b) Browse to the local AP image, corresponding to the Access Point in your network.
c) Click on the Auto Restart checkbox if automatic restart of all access points in the network is desired after the software update is finished.
d) Click on the Apply Button.
e) Click on Update now to initiate software update.



8.3.100.0

Transfer Mode: TFTP
IP Address(IPv4) *: 10.0.10.4
File Path *: 8-3/
Set Update Time:
☑ Auto Restart

Step 4 To view the download status, expand the Predownload image status.

Software Update via TFTP

Procedure

Step 1 Download the AP Image bundle from cisco.com to the TFTP server.

Step 2 Unzip the AP Image bundle to extract individual AP Images.

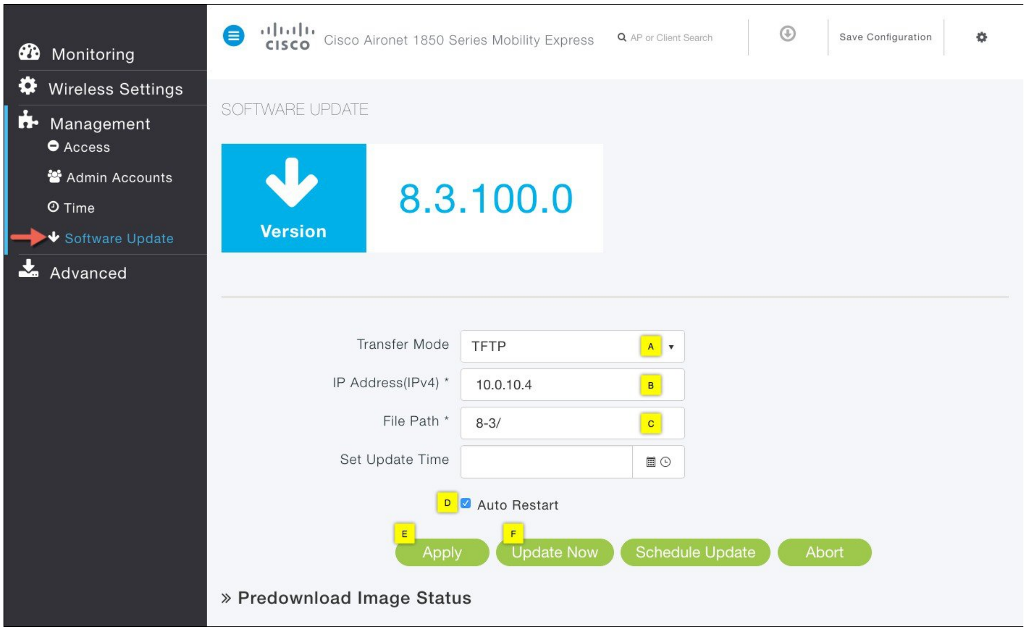
Step 3 To perform Software Update via TFTP, navigate to **Management** > **Software Update** and perform the following:

a) For **Transfer Mode** select ***TFTP*** from the drop down list.
b) Enter the IPv4 address of the TFTP server in the **IP Address (IPv4)** field.
c) Enter the **File Path** to the unzipped AP images on the TFTP Server.

d) Click on the Auto Restart checkbox if automatic restart of all access points in the network is desired after the software update is finished.

e) Click on the Apply Button.

f) Click on **Update Now** to initiate software update. To Schedule Update at a later time, configure the **Set Update Time** and click on the **Schedule Update** button.



8.3.100.0

Transfer Mode: TFTP

IP Address(IPv4) *: 10.0.10.4

File Path *: 8-3/

Set Update Time:

☑ Auto Restart

Note For schedule later, user must select a date and time in the future and then click on Schedule Later. Button. It is recommended that the Set Reboot Time should be at least 2 hours from the time pre-image download was initiated. This will ensure that pre-image download on all Access Points in the Mobility Express Network has completed.

Step 4 To view the download status, expand the Predownload image status.

Upgrading Cisco Mobility Express network via TFTP from the CLI

Procedure

Step 1 Login to AP running Mobility Express controller via Telnet or SSH.

Step 2 Specify the datatype.

```
 (Cisco Controller) >transfer download datatype ap-image
```

Step 3 Specify the transfer mode.

```
(Cisco Controller) >transfer download ap-images mode tftp
```

Step 4 Specify the IP address of the TFTP server.

```
(Cisco Controller) >transfer download ap-images serverIp <IP addr>
```

Step 5 Specify the path of the AP images on the TFTP server.

```
 (Cisco Controller) >transfer download ap-images imagePath <path to AP images>
```

Note For pre-image download to be successful make sure path to the AP images is correct

Step 6 Start pre-downloading of the image on the APs.

```
(Cisco Controller) > transfer download start
Mode........................................... TFTP
Data Type...................................... ap-image
TFTP Server IP................................. 10.1.1.77
TFTP Packet Timeout............................ 10
TFTP Max Retries............................... 10
TFTP Path...................................... ap_bundle_8.1.112.30/
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Code transfer starting.
Triggered APs to pre-download the image.
Reboot the controller once AP Image pre-download is complete
```

Step 7 Check the pre-download status by executing the CLI below.

```
(Cisco Controller) >show ap image all

Total number of APs.............. 3
Number of APs
       Initiated........................1
       Predownloading...................2
       Completed predownloading.........0
       Not Supported....................0
       Failed/BackedOff to Predownload...0

                   Primary    Backup  Predownload Predownload Next Retry  Retry Failure
AP Name              Image     Image     Status      Version    Time      Count Reason
____________   _________  ______-- _______    ________  ______  ___  ____

AP6412.256e.0e78 8.1.112.21  8.1.112.21 Predownloading   —       NA       NA
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Predownloading   —       NA       NA
3600-gemini   8.1.112.21  8.1.112.21 Predownloading   —          NA
```

Step 8 Wait for the pre-image download to complete on the APs.

```
(Cisco Controller) >show ap image all
Total number of APs.............. 3
Number of APs
       Initiated........................1
       Predownloading...................2
       Completed predownloading.........0
       Not Supported....................0
       Failed/BackedOff to Predownload...0

                    Primary    Backup  Predownload Predownload Next Retry Retry Failure
AP Name              Image     Image     Status      Version    Time      Count Reason
 ____________   _________  ______-- _______    ________  ______  ___  ____

AP6412.256e.0e78 8.1.112.21  8.1.112.21 Complete     —          NA        NA
```

```
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Complete     —          NA        NA
3600-gemini   8.1.112.21  8.1.112.21 Complete   —               NA
```

Step 9 After the pre-download is complete, issue a reset system as shown below. This will cause a reboot of the Cisco 1850 running Mobility Express followed by rest of the APs.

```
(Cisco Controller) > reset system
  The system has unsaved changes.
  Would you like to save them now? (y/n)y
  Configuration Saved!
  System will now restart!
```

Step 10 Log back in the Mobility Express and check the version under Primary Image. It will show the new version and the Backup Image will show the previous version.