
Release Notes for Foundry IronPoint™ 200 Access Point

Release 02.02.04



Release Date: June 9, 2008

Publication date: June 9, 2008

4980 Great America Parkway
Santa Clara, CA 95054
Tel 408.207.1700
www.foundrynetworks.com

Copyright © 2008 Foundry Networks, Inc. All rights reserved.

No part of this work may be reproduced in any form or by any means – graphic, electronic or mechanical, including photocopying, recording, taping or storage in an information retrieval system – without prior written permission of the copyright owner.

The trademarks, logos and service marks ("Marks") displayed herein are the property of Foundry or other third parties. You are not permitted to use these Marks without the prior written consent of Foundry or such appropriate third party.

Foundry Networks, BigIron, FastIron, IronView, *JetCore*, NetIron, ServerIron, *TurboIron*, *IronWare*, *EdgeIron*, *IronPoint*, the Iron family of marks and the Foundry Logo are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries.

All other trademarks mentioned in this document are the property of their respective owners.

These release notes describe the IronPoint 200 Access Point 02.02.04 software release.

ABOUT RELEASE 02.02.04	1
SUMMARY OF ENHANCEMENTS	1
MIXED IRONPOINT 200 AND IRONPOINT 250 ENVIRONMENT	2
SYSTEM REQUIREMENTS	2
SOFTWARE IMAGES	2
INSTALLING THE ACCESS POINT	2
UPGRADING TO RELEASE 02.02.04	3
BEFORE UPGRADING	3
UPGRADING TO RELEASE 02.02.04	3
SUPPORTED FEATURES	5
SOFTWARE FIXES	9
KNOWN LIMITATIONS AND ISSUES	9
WHERE TO GET MORE INFORMATION	15
UPDATES TO MANUALS AND RELEASE NOTES	15
HOW TO GET HELP OR REPORT ERRORS	15
WEB ACCESS	15
E-MAIL ACCESS	15
TELEPHONE ACCESS	15

These release notes describe Release 02.02.04 of the Foundry IronPoint™ 200 access point software. They contain the following sections:

- “Summary of Enhancements”
- “Mixed IronPoint 200 and IronPoint 250 Environment” on page 2
- “System Requirements” on page 2
- “Software Images” on page 2
- “Installing the Access Point” on page 2
- “Upgrading to Release 02.02.04” on page 3
- “Supported Features” on page 5
- “Software Fixes” on page 9
- “Known Limitations and Issues” on page 9
- “Where to Get More Information” on page 15
- “Updates to Manuals and Release Notes” on page 15
- “How to Get Help or Report Errors” on page 15

About Release 02.02.04

IronPoint software release 02.02.04 can be installed only on IronPoint 200 Access Points running software release 02.02.00, 02.02.01, 02.02.02, and 02.02.03.

You cannot install this release on an IronPoint 250 Access Point.

Summary of Enhancements

The following enhancement is in this release:

Enhancement	Description	See ...
Data rate based access and RSSI rate based access	The datarate-based-access and the rssi-based-access CLI commands are introduced in this release. The datarate-based-access command prevents clients from transmitting data frames to the access point with low data rates, while the rssi-based-access command prevents clients with low RSSI values from connecting to an access point.	Book: <i>Foundry IronPoint 200 Access Point User Guide</i> Chapter: Radio Interface Configuration Sections: datarate-based-access and rssi-based-access

Also, Release 02.02.04 contains software fixes as listed in Table 1 on page 9.

Mixed IronPoint 200 and IronPoint 250 Environment

If you have both IronPoint 200 and IronPoint 250 Access Points on your network, note the following:

- You can copy configuration files from an IronPoint 200 running release 02.02.04 to an IronPoint 250 running software release 03.02.01.
- Inter Access Point Protocol (IAPP) is supported between IronPoint 200 and IronPoint 250 for Layer 2 Roaming.
- You can have IronPoint 250 in RF sensor mode, IronPoint 250 in IronPoint 200 compatible RF sensors mode, and IP 200 in RF sensor mode on the same network. However, it is recommended that you use IP 200 running software release 02.02.03 or later if the IP 200 will be running in RF sensor mode. Also, IronView Network Manager software 03.0.00 and earlier cannot be used to manage IronPoint 250 in RF sensor mode.

System Requirements

Managing the access point using the Web interface requires Internet Explorer, version 6.0 and above, running on Windows platforms. Also, version 1.0 and above of the Firefox browser can be used to access the Web interface. Netscape browsers are not supported.

For Automatic Discovery and Configuration (ADC) enabled configurations, the following software releases must be used together to support all of the ADC enhancements in IronPoint-FES and IronView Network Manager:

- IronPoint 200 access points must be running software release 02.02.00 or later.
- IronPoint-FES must be running software release 02.02.00 or later.
- IronView Network Manager software release 02.0.00c or later (needed for automating VLAN deployment and deployment of a new boot image to the IronPoint 200).

Refer to the *Foundry IronPoint Wireless LAN Configuration Guide for the IronPoint - FastIron Edge Switch* and the IronView Network Manager user guide for details on the ADC feature.

Software Images

Release 02.02.04 requires the following images:

- Software image: IPFR02204.bin
- Boot Image: bootrom0400.bin

The IronPoint access point also contains a default (secondary) Image called dflt-img.bin. This image does not have to be upgraded.

Installing the Access Point

Refer to the *Foundry IronPoint 200 Installation Guide* for procedures on how to install the IronPoint 200 access point.

Upgrading to Release 02.02.04

-
- Notes:**
1. The access point configuration is reset to factory default if you downgrade the software version on an IronPoint access point.
 2. Foundry recommends that you use the same software release version on all IronPoint 200 access points on your network.
-

Read the following sections before you upgrade your access point:

- Before Upgrading on page 3
- Upgrading to Release 02.02.04 on page 3

Before Upgrading

Before you upgrade, make a backup copy of the access point configuration and determine what software version is currently installed on the access point.

Backup the Configuration

A backup is not required during the upgrade, but it is recommended that you backup the access point configuration in case you need to restore it. Backup your configuration file using the **copy config** command. For example,

```
Foundry AP#copy config tftp
TFTP Source file name:syscfg
TFTP Server IP:192.168.1.19
Foundry AP#
```

Check the Software Version on the Access Point

Determine what software release version is running in your access point by entering a **show version** command. For example,

```
Foundry AP#show version
Version Information
=====
Boot Rom Version : 04.0.00Tw5
Software Version : 02.02.03Tw8
Date : Sep 7 2007
Time : 10:55:10
=====
```

Your access point must have Release 02.02.00, 02.02.01, 02.02.02, or 02.02.03 installed. If it is a version earlier than Release 02.02.00, update it to Release 02.02.00. Go to the Foundry Knowledge Portal (kp.foundrynet.com) to obtain the software and release notes for Release 02.02.00. Follow the upgrade instructions described in the Release Notes for Release 02.02.00.

Upgrading to Release 02.02.04

You can upgrade the access points to Release 02.02.04 if your access point is running Release 02.02.00, 02.02.01, 02.02.02, or 02.02.04. Use any of the procedures described below.

Using IronView Network Manager

You can upgrade the access point using IronView Network Manager release 02.0.00c or later. Make sure the access point is connected to the network and IronView Network Manager has discovered the access point:

1. Deploy software image 02.02.04 (IPFR02204.bin) using the Software Image Upgrade payload.
2. Deploy a Reload APs payload.

Refer to the IronView Network Manager user guide for details.

Using the CLI

To upgrade the software image on the access point using the CLI, follow the steps below:

1. Make sure the access point is connected to the network.
2. At the CLI prompt, enter the following command:

```
Foundry AP# copy tftp file
```

3. Next, at the "Select the type of download <1, 2, 3>" prompt, enter 1 for Application Image. For example:

```
1. Application image
2. Config file
3. Boot block image
Select the type of download<1,2,3>: [1]:1
```

4. When prompted, enter the name of the source file. For example:

```
TFTP Source file name: IPFR02204.bin
```

5. Enter the IP address of the TFTP server. For example:

```
TFTP Server IP: 192.168.1.19
```

The download begins. Wait until you see the following messages:

```
Current firmware version is 02.02.03Tw8. Copying new firmware version Run-Time
code v02.02.04. Please wait ...
Firmware copy complete. Reboot access point to complete firmware upgrade.
Foundry AP#
```

6. Reboot the access point by entering the following command:

```
Foundry AP#reset board
Reboot system now? <y/n>: y
```

NOTE: The access point renames the file IPFR02204.bin file to foundry-img.bin after the update is complete.

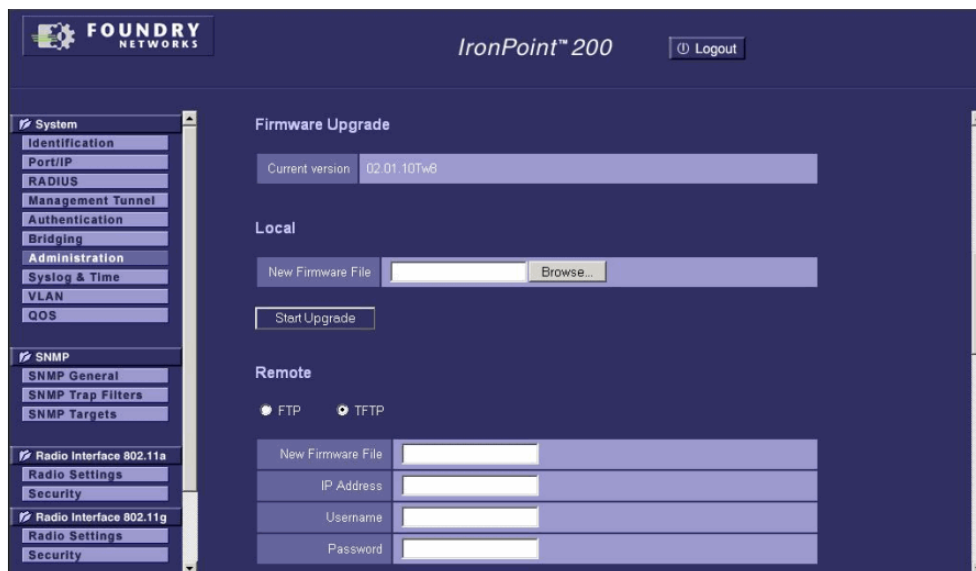
Once the access point reboots, upgrade is complete.

Using the Access Point Web Management Interface

You can upgrade an access point software image using the Web Management Interface. The procedure below steps you through the process.

1. Make sure the access point is connected to network.
2. Log into the Web Management Interface.

- From the System menu, click Administration and scroll down to the Firmware Upgrade section.



- Next, upgrade the software image by doing one of the following:
 - For a local upgrade, use the Browse button to find the IPFR02204.bin file on the local workstation before clicking Start Upgrade.
 - For a remote FTP/TFTP upgrade, specify the FTP/TFTP server details and software file name. Select IPFR02204.bin for the application image. Once downloaded, this file is renamed to foundry-img.bin
- Click Start Upgrade and wait for the message "Firmware copy complete. Reboot access point to complete firmware upgrade."
- Click OK to accept the message.
- When the Administration page is redisplayed, scroll to the bottom of the page and click the Reset Access Point button.

Once the access point reboots, upgrade is complete.

Supported Features

The following table lists the features supported on IronPoint 200 Release 02.02.04.

Category	Feature
IP Address Management	Automatic Discovery and Configuration (ADC)
	Static
	DHCP client
	DNS resolution

Category	Feature
VLAN	802.1Q tagging
	64 VLAN IDs
	Management VLAN ID
	Default VLAN ID per radio
	802.1X dynamic VLAN assignments
System Software	Dual firmware image
	TFTP upgrade
	FTP upgrade
	HTTP upgrade
SNMP	SNMP v1 and v2c
	SNMPv3 users
	SNMPv3 groups
	SNMPv3 trap targets
	SNMPv3 trap filters
Management Access	Console CLI
	HTTP
	HTTPS
	Telnet
	SSH v2.0
	PPPoE Management Tunnel
	ACLs to filter HTTP, HTTPS, Telnet, and SNMP access
	Banners
Logging	Event Logging
	Remote Syslog (4 servers)
	Console display and clear
	Web display and clear
System Clock	SNTP client
	Manual date and time setting
	Time zone
	Daylight saving
Bridge Filters	Wireless to wireless
	Ethernet protocols
	Management from wireless

Category	Feature
Authentication	Management user name & password
	802.1x supplicant
	RADIUS Accounting
	TACACS+ AAA
	Intrusion Detection and Lockout
Status Information	System configuration
	Wireless configuration
	Wireless client status
QoS	IEEE 802.1p
	Source/Destination MAC address
	Ethernet protocol type
	SpectraLink Voice Priority (SVP)
Rate Limiting	Rate limiting of incoming broadcast or multicast traffic on Ethernet interfaces
	Rate limiting of incoming wireless broadcast or multicast traffic on the IronPoint 200 (release 02.02.01 and later)
Radio Settings	Country Code setting
	External antenna
	Auto channel selection
	Selectable mode operation
	Selectable power setting
	Data rate setting
	Selectable beacon interval
	Selectable DTIM interval
	Adjustable RTS threshold
	Adjustable fragmentation threshold
	Maximum clients setting (64)
	802.11a Turbo mode
	IAPP support
	Load Balance
	SSID Prioritization
	Data rate based access control. Requires software release 02.02.04
	RSSI rate based access control. Requires software release 02.02.04

Category	Feature
Wireless Security	Virtual access points per radio (4)
	Hidden SSID
	RADIUS MAC authentication
	Local MAC authentication
	802.1x client authentication
	WEP authentication
	WEP encryption (64, 128, 152 bit)
	Dynamic WEP keys with 802.1x
	WPA and WPA2 over 802.1x
	WPA and WPA2 Pre-shared Key
	WPA-WPA2 Mixed Mode
	WPA2 Pre-authentication
	TKIP encryption
	AES-CCMP encryption
RF Monitoring	Supported on IronPoint 200

Software Fixes

The table below lists the software fixed in this release.

The **P** column indicates the priority of the known issue, as follows:

- 0 = Critical
- 1 = Major
- 2 = Medium
- 3 = Minor
- 4 = Enhancement

The table is sorted by category, then by priority.

Table 1: Software Fixed in Release 02.02.04

Category	P	Description	Bug ID #
Other	4	Symptom: You cannot configure the access point do the following: <ul style="list-style-type: none">• Allow only clients with 5.5 Mbps or higher data rates to connect with the access point.• Prevent clients with certain RSSI values from connecting with the access point. Resolution: Fixed in this release	82870
Syslog messages	2	Symptom: The access point does not report Syslog messages correctly. This issue causes IronView Network Manager to ignore syslog messages from the access point. Resolution: Fixed in this release.	84217

Known Limitations and Issues

The tables below list the known limitations and issues in this release.

The **P** column indicates the priority of the known issue, as follows:

- 0 = Critical
- 1 = Major
- 2 = Medium
- 3 = Minor

The table is sorted by category, then by priority.

Table 2: Known Issues in Release 02.02.04

Category	P	Description	Bug ID #
802.1X Clients	1	Symptom: When using WPA2 802.1x AES, clients that are using Microsoft WZC may become disconnected from the access point. Workaround: Users should disconnect and reconnect their clients to the access point.	54731
Authentication	1	Symptom: The access point fails to deauthenticate a client when SSID changes occur. If the client sends data after the SSID change, the client may receive an error. Workaround: Users should disconnect and reconnect their clients to the access point.	37513
Authentication	1	Symptom: RADIUS timeout value is always configured to 5 seconds internally. Workaround: None	40615
Authentication	1	Symptom: The access point ignores de-authentication messages sent from wireless 802.1x client; therefore, wireless clients may experience long authentication time. Workaround: Users should disconnect and reconnect their clients to the access point.	48696, 43448,4 4411
CLI	1	Symptom: Only data rates for Radio A can be configured using the CLI when the b/g radio mode is configured as G only. Workaround: Use the Web interface to configure a Radio's data rates.	40574 / 46959
CLI and SNMP	1	Symptom: When the access points are passing data at their maximum throughput, responses for CLI and SNMP requests may be slow. Workaround: Wait for a time when traffic throughput is reduced to use the CLI or SNMP.	35371, 35367
Event message	3	Symptom: Sometimes a show command creates the event message: INFO: all 11 display buffers are busy, please try later. Workaround: Wait and try the show command again. If the event message continues, enter the CLI command dm display-buffer reset .	40907
General	0	Symptom: After running for a few hours, the access point appears to hang. Telnet, Web interface, TFTP, and FTP processes are not available. Workaround: You must restart the access point.	43801
General	1	Symptom: If a wireless client that has performed a Layer 3 roam attempts to upgrade the access point image using the Web interface, the upgrade will fail. Workaround: Do not use a wireless client that has performed a Layer 3 roam to upgrade the access point's image from the Web interface.	34727
IDS	2	Symptom: IDS erroneously picks up "duplicate IP" errors as intruders from Windows operating systems. When a duplicate IP error is detected by the Windows operating system, Windows assigns the client a 0.0.0.0 IP address and blocks the client from accessing the network.	48674

Table 2: Known Issues in Release 02.02.04

Category	P	Description	Bug ID #
IDS	3	Symptom: The maximum number of invalid attempts allowed by the access point changed has been changed. If the IronPoint access point is running software release version 01.3.00 and IDS is configured for 65536 invalid attempts, you must change this value to 65535 if you upgrade to a version later than release 01.3.00.	41203
Layer 3 Roaming	0	Symptom: After a home agent switch reboots and the home agent and foreign agent switches fail to synchronized for Layer 3 roaming, wireless client cannot communicate with rest of network Workaround: Users should disconnect and reconnect their clients to the access point.	45649
NIC	0	Symptom: The IronPoint access point may not be able to authenticate a wireless client that has a Buffalo NIC when 802.1X authentication is enabled.	40608
NIC	1	Symptom: Some WPA clients cannot handle 802.1X re-authentication (during 802.1X session time-out) during client radio power save while connected to a mixed mode VAP (for example, WPA+WEP). This is because the client is failing to include the WPA IE in the associate request. The access point puts the client into forwarding state but sets the cipher to WEP instead of TKIP or AES. Workaround: None	59691
NIC	1	Symptom: Netgear NICs that support WPA2 may not connect properly to Channel 36 of the IronPoint access point's Radio A. Workaround: Use Radio B or do not use auto channel scan on Radio A and manually configure Channel 36.	59702
NIC	2	Symptom: The IronPoint access point cannot have the power save mode enabled if wireless clients are using Buffalo NICs. Workaround: None	56205
RADIUS	3	Symptom: Accounting stop requests may not be sent by the access point when a client disconnects from the network. Workaround: The access point will issue an event message when the client disconnects.	39566
Security	0	Symptom: Certain wireless clients may be intermittently disconnected from the network when they are using the 802.11 b/g radio, with 802.1X WPA security, and the access point is under a very heavy traffic load. Workaround: None	39529, 38342

Table 2: Known Issues in Release 02.02.04

Category	P	Description	Bug ID #
Security	N/A	<p>Symptom: Some WPA client may not support WEP Key #1 as the default transmit keys for WEP and WPA combination encryption schemes, because legacy hardware for wireless clients do not support WEP Key #1 for these schemes. In these schemes, Key #1 is reserved for internal WPA use; that is, dynamic key generation of both dynamic WEP and dynamic WPA keys use Key #1 for unicast traffic.</p> <p>Workaround: Although you can enter a value for WEP Key #1, that key may not be used as the default transmit key in the WEP and WPA encryption schemes. Select WEP Key #2, 3, or 4 as the default transmit key for these encryption schemes.</p> <p>NOTE: The limitation information can be found in the <i>Foundry IronPoint 200 User Guide</i>.</p>	N/A
Security: MAC Filtering	0	<p>Symptom: When RADIUS MAC Filtering is turned on, WPA is not allowed and clients cannot connect to the access points.</p> <p>Workaround: Do not use the RADIUS MAC and WPA encryption combination at this time.</p>	29169
SNMP	1	<p>Symptom: SNMP MIB walk using SNMP v2c on an access point loops on wpProducts branch.</p> <p>Workaround: None</p>	35167
SNMP and XML	1	<p>Symptom: When an access point's configuration is changed using SNMP and the syscfg.xml file is transferred as soon as the change is made, the changes are not included in the syscfg.xml.</p> <p>Workaround: None</p>	54489
SNMP Management	1	<p>Symptom: SNMP MIB reports InUcastPkts and OutUcastPkts for the loopback interface; however, loopback interface is not used by the access point.</p> <p>Workaround: None</p>	57817
System	0	<p>Symptom: The IP200 access point may experience a software reboot if it encounters very high noise floor and/or interference.</p> <p>Workaround: None. Normal operation should occur once the high noise floor/interference subsides.</p>	67205
TACACS+	1	<p>Symptom: If the access point's IP address is not in the list of AAA clients in the TACACS+ server, then authenticating users through the TACACS+ server will cause any current and future Telnet, console, and SSH session to hang. However, other functionalities on the access point are still available.</p> <p>Workaround: To recover, add the IP address of that IronPoint access point to the list of AAA clients in the TACACS+ server. Then reboot that IronPoint access point.</p>	66874
Time	1	<p>Symptom: The access point adds one hour to you enter time while daylight savings time is enabled.</p> <p>Workaround: Use SNTP to set date and time.</p>	35368

Table 2: Known Issues in Release 02.02.04

Category	P	Description	Bug ID #
Upgrade	2	Symptom: You may have to reconfigure your access point prompt when upgrading from release 2.0.02 to 2.0.04. However, once the prompt is reconfigured, it would persist across reboots. Workaround: None	56776
VAP	1	Symptom: A wireless client may not be able to reconnect to a VAP under the following conditions: <ul style="list-style-type: none"> Two wireless clients are connected to the same radio on the same access point that has four VAPs configured. Each of the four VAPs have a different authentication/encryption setting and one of the VAP is configured for 802.1x dynamic WEP. The two wireless clients change connections from one VAP to another VAP on the same access point. One of the of the wireless client tries to reconnect to the VAP to which he was originally connected, using 802.1X dynamic WEP. Workaround: None	37077
Windows Operating System	2	Symptom: The following are issues with the Microsoft Windows XP operating system: <ul style="list-style-type: none"> Two different IP addresses may be shown when using WZC supplicant. Error message for duplicate names or duplicate IP addresses are displayed even though there are no duplicates. This could interfere with the functionality of IDS and Wireless Mobility. Workaround: None	48846, 52144
Wireless Client	2	Symptom: Some wireless NICs when configured for PS polling and 802.1x authentication will take a long time to re-connect from one access point to another. Workaround: Configure the wireless NIC for Continuously Aware Mode instead of PS polling.	40916
Wireless Client	3	Symptom: Clients that use Funk Software Odyssey and have "connect to network" set to "any" and are using TKIP encryption cannot connect. Workaround: Configure the network to connect to instead of using "any".	38807
Wireless Client NIC drivers	NA	Symptom: Some NIC drivers may not be able to immediately recognize configuration changes to the multicast cipher parameter and prevent the wireless client to the access point after the configuration change. Workaround: If this happens, disconnect the wireless client from the network, for example by either removing the NIC card from the laptop, wait a few minutes, then reconnect the client.	NA
Wireless Clients	2	Symptom: Some wireless clients with Broadcom chipsets may not connect when using 802.1x authentication. Workaround: Check that your NIC's drivers are up to date.	40662, 40598
Wireless Clients	2	Symptom: An improperly configured wireless client may prevent other wireless clients from connecting on the same VAP when 802.1x authentication is enabled. Workaround: Enable Real-time IDS to block improperly configured clients.	40753

Table 2: Known Issues in Release 02.02.04

Category	P	Description	Bug ID #
Wireless Clients	3	Symptom: Some Pocket PC devices with NICs containing 802.11b the Intersil Prism chip set cannot connect to the access point when the access point is using Radio G in b+g mode. Workaround: Ensure that the devices has the newest drivers for the NIC. If the devices still does not connect, change Radio g to "b only" mode.	38995
Wireless Interface	3	Symptom: The Multicast Rate setting may also affect the data rate of management and control frames. Workaround: Use the default value for Multicast Rate	39936
WPA support	2	Symptom: WPA supported mode and WPA PSK Supported Mode do not work with the Intel 2200BG client and Intel 2915ABG clients. These modes are not supported by that client application. Workaround: None	57321
WPA support	2	Symptom: WPA-WPA2-Mixed Supported mode and WPA-WPA2-PSK-Mixed Supported Mode do not work with the Microsoft WZC Client Application. These modes are not supported by that client application. Workaround: None	57354
XML Export	N/A	Symptom: When you upgrade from software release 02.0.00 and earlier to release 02.1.01, XML configuration exports show null values for SNMPv3 credentials. This only applies to SNMPv3 user credentials for XML configuration export and does not affect the binary configuration export nor the SNMPv3 feature. Workaround: You must re-enter the SNMPv3 username and password for after an upgrade.	N/A

Where to Get More Information

Refer to the following manuals for information on how to install and configure the IronPoint Access Point:

- Foundry *IronPoint 200 Installation Guide* – Contains details on how to install the IronPoint Access Point, wireless network planning guidelines, troubleshooting guidelines, cabling, and general operating specifications
- Foundry *IronPoint 200 Access Point User Guide* – Contains procedures for configuring the IronPoint 200 Access Point using the command line interface and the Web interface.
- Foundry *IronView Network Manager User Guide*– Contains information on how to use IronView Network Manager to configure and manage the IronPoint 200 access point.
- *Foundry IronPoint Wireless LAN Configuration Guide* – Contains information on how to configure the IronPoint FastIron Edge switch for wireless features.

Updates to Manuals and Release Notes

Manuals and release notes for this product may be updated between releases. For the latest edition of manuals and release notes, check the Foundry Knowledge Portal at kp.foundrynet.com.

How to Get Help or Report Errors

Foundry Networks is committed to ensuring that your investment in our products remains cost-effective. If you need assistance or find errors in the manuals, contact Foundry Networks using one of the following options.

Web Access

Go to kp.foundrynet.com and log in to the Knowledge Portal (KP) to obtain more information about a product, or to report documentation errors. To report errors, click on Cases > Create a New Ticket.

E-mail Access

Send an e-mail to: support@foundrynet.com

Telephone Access

1.877.TURBOCALL (887.2622) United States

1.408.207.1600 Outside the United States

