



BlackBerry AtHoc

Indoor Fire Panel Installation and Configuration Guide

Last Published: May 2020

Contents

- Overview..... 4**

- Configure the centralized integration with the 16-channel indoor fire panel..... 5**
 - Prerequisites..... 5
 - Hardware requirements..... 5
 - Software requirements..... 6
 - Additional requirements..... 6
 - Configure the 16-Channel IIM..... 6
 - Configure the Indoor Fire Panel IIM CapCon and IIM agent..... 6
 - (Optional) Configure the IIM agent..... 7
 - INFP IIM variable parameters..... 7
 - INFP Activation Modes..... 10
 - Configure the INFP device on the BlackBerry AtHoc management system..... 11
 - Enable the INFP device on the BlackBerry AtHoc application server..... 11
 - Configure the indoor fire panel delivery gateway..... 11
 - Enable the indoor fire panel device..... 12
 - Configure a mass device for each INFP IIM..... 12
 - Verify the INFP configuration..... 13

- Configure a distributed integration with the 8-channel IIM..... 15**
 - Prerequisites..... 15
 - Software requirements..... 15
 - Hardware requirements..... 16
 - Configure the 8-channel IIM..... 16
 - Configure the IIM..... 16
 - (Optional) Configure the IIM agent..... 17
 - Configure the INFP device on the BlackBerry AtHoc management system..... 18
 - Enable the INFP device on the BlackBerry AtHoc application server..... 18
 - Configure the indoor fire panel delivery gateway..... 18
 - Enable the indoor fire panel device..... 18
 - Configure a mass device for each INFP IIM..... 19
 - Verify the INFP configuration..... 20

- BlackBerry AtHoc Customer Support Portal..... 22**

- Legal notice..... 23**

Overview

Indoor fire panels alert end-users that there is a fire. You can send alerts from BlackBerry AtHoc to the fire panel.

This document describes the steps needed to set up and integrate the fire panel with BlackBerry AtHoc and with the IP Integration Module (IIM) manager (used to integrate the fire panel with the alerting system using a Web interface). This guide describes the setup and configuration for a 16 or an 8-channel Indoor Fire Panel IP Integration Module (IIM). Your configuration determines which type of INFP IIM to use.

The 16-channel IIM enables you to send alerts to one or more fire panels, using one IIM to activate up to 16 fire panels. This is a centralized configuration.

For a distributed configuration, in which each fire panel has its own IIM, use the 8-channel INFP IIM.

The indoor fire panel connects with notification devices using the following two networks:

- Control network, token ring loop (sustaining single break)
- Audio network, typically digital audio with 8 channels (over twisted pair or fiber)

A single indoor fire panel can control a standard size building, where larger buildings (high rise or very large buildings) might have more indoor fire panels. In a campus configuration, it is typical to have multiple indoor fire panels ride the same control and audio networks. In that case, a single indoor fire panel can trigger alarms in remote locations with the same control and audio networks, with override provisions (as programmed in the fire panels).

The audio and control networks connect to amplifiers (Flex-50) which drive the speakers mounted in the buildings.

The fire panel is equipped with an RS232 computer port that can be used for control.

Additionally, an Auxiliary Audio Input Module provides line level audio input. The audio input can be programmed to relay input audio to one of the 8 channels.

Configure the centralized integration with the 16-channel indoor fire panel

The BlackBerry AtHoc 16-channel IIM provides IP access for your fire panels to the BlackBerry AtHoc Management System. If you have a central fire alarm panel that can activate other buildings through dry contacts, you can use the 16-channel INFP IIM for that panel.

The 16-channel IIM can activate multiple building fire panels in several modes: sequentially, simultaneously, or simultaneously with a delay. The IIM with 16 channels provides the 16 relay card, where each relay that closes activates a particular building; it is programmed to activate building X when relay X is closed. All advanced audio functions are available, including pre-tone, post tone, repeats, text to speech and stored audio.

Example: Company XYZ decides to use a centralized configuration for their campus that has five buildings. They put a fire panel in each building, connected to the BlackBerry AtHoc management system with the 16-channel IIM.

In a centralized configuration, one IIM manages alerting for up to 16 endpoints. There are no groups. The targets in the alert tell the IIM which contact to close, which activates the correct building fire panel.

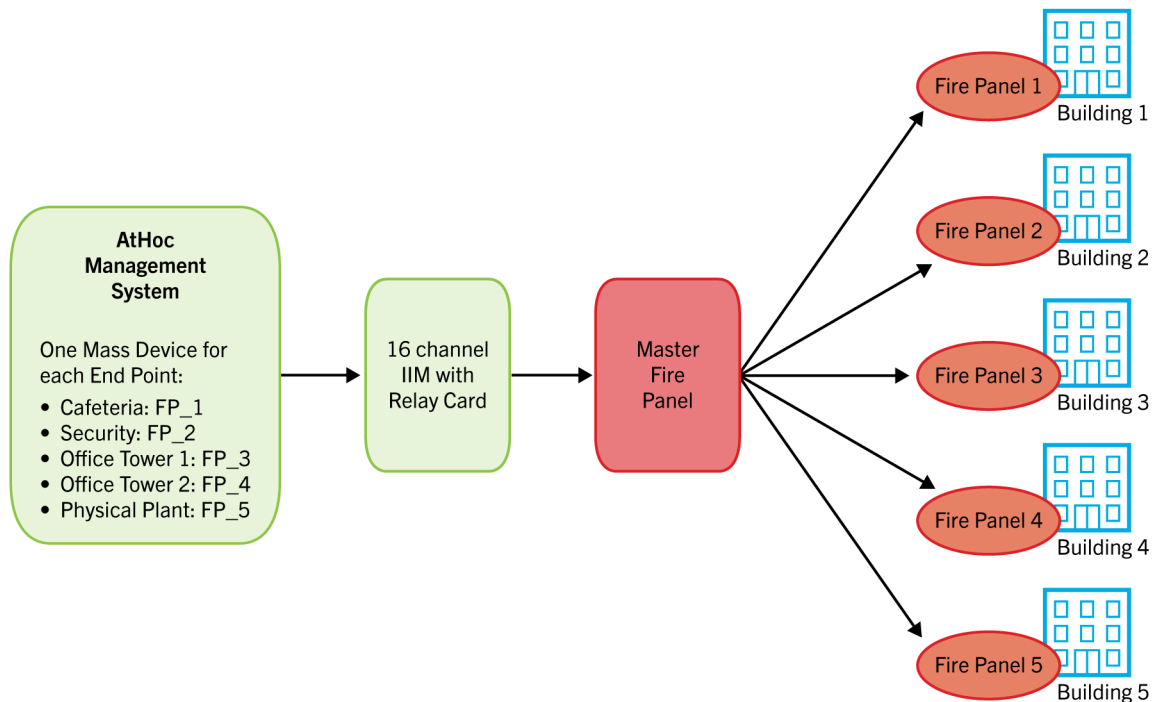


Figure 1: 16-channel fire panel IIM configuration

Prerequisites

The following sections describe hardware and software requirements that are necessary for configuring the 16-channel INFP.

Hardware requirements

- BlackBerry AtHoc 16 channel INFP IIM.
Contact the IIM team in Martinez, California to get the hardware.

- A line level input into an auxiliary audio input module

Software requirements

BlackBerry AtHoc management system release 6.1.8.85 CP9 and higher with the INFP Installation Package

Additional requirements

Determine relay assignments for each fire panel. Contact the fire panel vendor to determine what relay to close for each fire panel.

Configure the 16-Channel IIM

For each building fire panel, configure an INFP IIM.

Prerequisite: Ensure that the following packages are installed and configured before starting these steps:

- Latest Indoor Fire Panel package
- Latest Capnode package on the IIM

Configure the Indoor Fire Panel IIM CapCon and IIM agent

1. Log in to the INFP IIM as an administrator.
2. Modify the CapCon services (and optionally the IIM Agent) to poll and post to the BlackBerry AtHoc management system URL:
 - a. From the INFP IIM server, open the following file: `..\ProgramFiles\capnode\system_private.config`
 - b. Change the `indexURL` value using the following format: `indexURL=http://IWSAlertsServerURL/Syndication/CAP_INFP/VPSPProvider_ID/Capindex?ast=MAC_Address`
3. Optionally, for the IIM Agent, make sure following values have the identical ID:
 - The `myid.txt` file
 - The database record in the `AST_ASSET_TAB`
 - The Inbound CAP Event Agent `<EventMapping>` node
 - The value of the `<sender>` node in the IIM originates from the `myid.txt` file in the following location `..\programfiles\capnode\myid.txt` and should match the `ASSET_NAME` field in the `AST_ASSET_TAB` database table.

`..\Program Files\capnode\.` The value of the `myid.txt` file is the MAC address of the IIM that manages the INFP.
4. In the `system_private.config` file, modify the `CapPostingTarget.capurl` value. Enter the BlackBerry AtHoc server URL in the highlighted attribute value:


```
CapPostingTarget=True
CapPostingTarget.capurl=https://IWSAlertsURL/Syndication/PostCap
```
5. Optionally, configure the proxy server and port settings in the same file:
 - a. Add the values for the proxy port and server parameters.
 - b. Save the file.
6. In the `system_private.config` file, configure parameters with the values as described in [INFP IIM variable parameters](#).
7. Save your changes.
8. Restart the CapCon service.

(Optional) Configure the IIM agent

1. Edit the following file: `..\programfiles\capnode\iimm\IIMAgent.exe.config`.
2. Modify the `<add>` node with the following BlackBerry AtHoc application server information: `<add key = "ServerURL" value="https://IWSAlertServerURL".../>`
3. Save your changes.
4. Restart the IIM Agent service.
 - a. Navigate to the following directory: `../AtHocENS/DeliveryServer/Installations`
 - b. Run `Start Services`.

INFP IIM variable parameters

This section provides the INFP parameters, their values, and purpose.

Parameter Name: `encoders`

Value: `com.ha.capnode.drivers.sirencentral.SirenCentralEncoder`

Purpose: Tells IIM to use the siren central processing as we do for all BlackBerry AtHoc IIM Mass devices.

Parameter Name: `encoder.SirenCentralEncoder.SirenCentralDriver`

Value: `com.ha.capnode.drivers.sirencentral.firepanel.SirenCentralDriverFirePanel16`

Purpose: Tells IIM to use the fire panel with 16 channels.

Parameter Name: `indexURL`

Value: `https\://<IWS Root>/Syndication/CAP_INFP/<VPS>/capindex?ast=<MAC address>`

Purpose: Tells IIM where to look for the CAP feed from BlackBerry AtHoc.

Parameter Name: `delayBetweenRXPolls`

Value: `7`

Purpose: Indicates how long to wait between each poll to the BlackBerry AtHoc server. This is the minimum time it takes for an alert to play.

Parameter Name: `encoder.SirenCentralDriverFirePanel16.activationMode`

Value: `simultaneous | simultaneousDelayed sequential`

Purpose: Tells the IIM which of three modes to active the relays. See [INFP activation modes](#).

Parameter Name: `encoder.SirenCentralDriverFirePanel16.pauseBetweenSequentialSites`

Value: `5000`

Purpose: Sets the number of milliseconds to wait between each site activation. Only applies for when `activationMode` is "sequential."

Parameter Name: `encoder.SirenCentralDriverFirePanel16.pauseAfterPlayingAudio`

Value: `10000`

Purpose: Sets the number of milliseconds to wait between when the audio completed and the relays are opened.

Parameter Name: `encoder.SirenCentralDriverFirePanel16.pauseBeforeContactClosure`

Value: `2000`

Purpose: Sets the number of milliseconds to wait once the alert is accepted to processing by the IIM and the first relay is closed (in any mode.)

Parameter

Name: `encoder.SirenCentralDriverFirePanel16.pauseBetweenSimultaneousSitesDeActivate`

Value: 5000

Purpose: Sets the number of milliseconds between simultaneous site relay openings.

Parameter

Name: `encoder.SirenCentralDriverFirePanel16.pauseBetweenSimultaneousSitesActivate`

Value: 3000

Purpose: Sets the number of milliseconds between simultaneous site relay closing.

Parameter Name: `encoder.SirenCentralEncoder.pauseBeforePlayingAudio`

Value: 3500

Purpose: Sets the number of milliseconds to wait between when the relays are closed and the audio playing starts.

Parameter Name: `encoder.SirenCentralEncoder.SupportPrimarySecondaryIIM`

Value: No

Purpose: Unsupported for this IIM. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.Primary`

Value: Yes

Purpose: Unsupported for this IIM. Do not modify.

Parameter

Name: `encoder.SirenCentralEncoder.TimeToWaitBeforeFirstPrimaryStatusCheckInSec`

Value: 45

Purpose: Unsupported for this IIM. Do not modify.

Parameter

Name: `encoder.SirenCentralEncoder.TimeToWaitBeforeSecondPrimaryStatusCheckInSec`

Value: 900

Purpose: Unsupported for this IIM. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.PrimaryStatusFilePath`

Value: `C:\ProgramFiles\capnode\Primary`

Purpose: Unsupported for this IIM. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.SecondaryStatusFilePath`

Value: `\\C237089\Secondary`

Purpose: Unsupported for this IIM. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.TTS_Volume`

Value: 50

Purpose: Volume of the spoken text-to-speech portion of the alert.

Parameter Name: `encoder.SirenCentralEncoder.TTS_Speed`

Value: 110

Purpose: Speed of the spoken text-to-speech portion of the alert.

Parameter Name: `encoder.SirenCentralEncoder.TTS_Pitch`

Value: 70

Purpose: Pitch of the spoken text-to-speech portion of the alert.

Parameter Name: `encoder.SirenCentralEncoder.TTS_Range`

Value: 7

Purpose: System value. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.TTSType`

Value: 1

Purpose: System value. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.TTS_SynthesizerIndex`

Value: 1

Purpose: System value. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.TTS_VoiceIndex`

Value: 1

Purpose: System value. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.TTS_InputFile`

Value: `TTSTemplate.txt`

Purpose: System value. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.TTS_Engines`

Value: 1

Purpose: System value. Do not modify.

Parameter Name: `encoder.SirenCentralEncoder.DelayBeforePreTone`

Value: 5

Purpose: Indicates how long to wait to before playing a pretone in the alert, if a pre-tone is requested.

Parameter Name: `encoder.SirenCentralEncoder.DelayAfterPreTone`

Value: 5

Purpose: Indicates how long to wait to after playing a pretone in the alert, if a pre-tone is requested.

Parameter Name: `encoder.SirenCentralEncoder.DelayBeforePosttone`

Value: 5

Purpose: Indicates how long to wait to before playing a post-tone in the alert, if a post-tone is requested.

Parameter Name: `encoder.SirenCentralEncoder.DelayAfterPosttone`

Value: 5

Purpose: Indicates how long to wait to after playing a post-tone in the alert, if a post-tone is requested.

Parameter Name: `proxyServer`

Value: <name of proxy server>

Purpose: The address of the proxy, if a proxy is used in your network for HTTPS.

Parameter Name: proxyPort

Value: <port number>

Purpose: The port of the proxy, if a proxy is used in your network for HTTPS.

Parameter Name: AckPostingTarget

Value: False

Purpose: If False, the IIM does not post an Ack to Server when it downloads an alert and it passes the filter. If set to True, the IIM posts an Ack CAP message to the server when an alert is downloaded and passes the filter.

Parameter Name: ackuser

Value: —

Purpose: This parameter is no longer used and can be disregarded.

Parameter Name: ackpassword

Value: —

Purpose: This parameter is no longer used and can be disregarded.

Parameter Name: ackaccount

Value: —

Purpose: This parameter is no longer used and can be disregarded.

Parameter Name: CapPostingTarget

Value: True

Purpose: If set to True, IIM posts progress messages in CAP format to the server as it activates the end-point device. If set to false, IIM does not post progress messages.

Parameter Name: CapPostingTarget.capURL

Value: https\:\/\/<IWS Root>/Syndication/postCap

Purpose: The URL to which to post progress messages.

Parameter Name: CapPostingTarget.user

Value: —

Purpose: This parameter is no longer used and can be disregarded.

Parameter Name: CapPostingTarget.password

Value :—

Purpose: This parameter is no longer used and can be disregarded.

Parameter Name: CapPostingTarget.account

Value: —

Purpose: This parameter is no longer used and can be disregarded.

INFP Activation Modes

The following list describes the three activation modes for the INFP.

- Simultaneous
 1. Closes all relays at the same time.

2. Waits for "pauseBeforePlayingAudio" milliseconds.
 3. Plays audio.
 4. Waits for "pauseAfterPlayingAudio" milliseconds.
 5. Opens all relays at the same time.
- SimultaneousDelayed
 1. Closes all relays for every chosen site, one after the other, with a delay of "pauseBetweenSimultaneousSitesActivate" ms between each relay.
 2. Waits for "pauseBeforePlayingAudio" milliseconds.
 3. Plays audio Wait for "pauseAfterPlayingAudio" milliseconds.
 4. Opens all relays for every chosen site, one after the other, with a delay of "pauseBetweenSimultaneousSitesDeActivate" milliseconds between each relay.
 - Sequential
 1. Closes a relay for first site.
 2. Waits for "pauseBeforePlayingAudio" milliseconds.
 3. Plays audio Wait for "pauseAfterPlayingAudio" milliseconds.
 4. Opens relay.
 5. Waits for "pauseBetweenSequentialSites" milliseconds and then repeats the process for each site.

Configure the INFP device on the BlackBerry AtHoc management system

This section describes the steps to configure an INFP on the BlackBerry AtHoc management system to make it available as a target in an alert. Before starting these steps, ensure that you meet the requirements in the Prerequisites section for this device.


Enable the INFP device on the BlackBerry AtHoc application server

Enable the INFP device on the BlackBerry AtHoc application server to make it available for the AtHoc organizations in the system. Depending on the version of BlackBerry AtHoc, the device is either included in the installation of BlackBerry AtHoc, or available from your account representative.

1. Log in to the BlackBerry AtHoc server as a system administrator.
2. Navigate to the following directory: `\AtHocENS\ServerObjects\tools`.
3. Run the following file: `AtHoc.Applications.Tools.InstallPackage.exe`.
4. On the **Configure Device Support** screen, select **Indoor Fire Panel**.


Note: If the device does not appear in the list, contact BlackBerry AtHoc Technical Support to get the installation package for the device.
5. Click **Enable** to install and enable the devices.
6. Close the **Installation Complete** screen.
7. Close the **Device Support** Dialog.

Configure the indoor fire panel delivery gateway

1. Log into the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click .
3. In the **Devices** section, open the **Indoor Fire Panel** gateway.
4. On the **gateway** screen, click **Copy default settings**.
5. Click **Save**.

Enable the indoor fire panel device

After you have configured the Indoor Fire Panel gateway, configure the associated device.

1. In the navigation bar, click .
2. In the **Devices** section, click **Devices**.
3. Select **Indoor Fire Panel**.
4. On the **device settings** page, click **Edit**.
5. Click **Add a Delivery Gateway** and select the gateway.
6. Click **Save**.
7. Click **Configure** to verify that the configuration information is populated.
8. Check for XML code in the text field. If the XML statements are not provided, cut and paste the following code into the text field:

```
<Configuration>
  <CapParams>
    <GVSystemType>INFP</GVSystemType>
    <AllMode>0</AllMode>
    <ZoneMode>0</ZoneMode>
    <PoleMode>0</PoleMode>
    <UnusedMode>0</UnusedMode>
    <DefaultAllCall>0</DefaultAllCall>
    <DefaultKeyActivationCode>0</DefaultKeyActivationCode>
    <NoPARequired>0</NoPARequired>
    <PARequired>1</PARequired>
    <IsCancelable>>false</IsCancelable>
    <ContentSource>Indoor-Fire-Panel</ContentSource>
  </CapParams>
</Configuration>
```

9. Click **Enable**.

The status line at the top of the screen updates and indicates that the device is enabled.

Configure a mass device for each INFP IIM

Each fire panel is an endpoint of an alerting system. In this case, the fire panel is also considered a mass communication device because it alerts an unknown number of recipients—whichever is in the vicinity of the device. In the BlackBerry AtHoc management system, an object called a mass device is configured for each mass communication endpoint. For each building fire panel, you will configure a mass device.

Before you begin, plan how many mass devices to create based on the number of building fire panels. First, determine how many fire panels you have. You create a mass device for each fire panel. Next, map the mass device to the relay that closes for a particular fire panel.

Example:

Company, XYZ Corp., has five buildings. Each building has a fire panel, for a total of five fire panels. Each of these fire panels are controlled by a master fire panel, to which the 16- channel IIM is connected. For this configuration, you will create five mass device endpoints. Enter the device addresses shown in the highlighted column in the Configuration section of the New Mass Device Endpoint screen. The address range is from 0-15.


Note: The second number in the endpoint address corresponds to the relay number on the IIM relay card.

Building	Mass Device Endpoint	Endpoint Address	Relay Card Dry Contact
Cafeteria	Cafeteria	INFP,0,1	D1

Building	Mass Device Endpoint	Endpoint Address	Relay Card Dry Contact
Security	Security	INFP,0,2	D2
Office Tower 1	Office Tower 1	INFP,0,3	D3
Office Tower 2	Office T ower 2	INFP,0,4	D4
Physical Plant	Physical Plant	INFP,0,5	D5


If the device name for the Cafeteria is "Cafeteria", and the device address is INFP,0,1, then an operator can target "Cafeteria" in an alert. When the alert is sent, the dry contact D1 on the relay card is closed. Closing the dry contact activates the relay for the fire panel in the Cafeteria.

To configure mass device accounts, complete the following steps for each fire panel:




1. Log in to the BlackBerry AtHoc management system with operator privileges.
2. In the navigation bar, click .
3. In the **Devices** section, click **Mass Device Endpoints**.
4. On the **Mass Device Endpoints**, click **New**, and then select the fire panel.
5. On the **New Mass Device Endpoint** screen, in the **General** section, enter the **Endpoint Name** and **Common Name** for the device. For example: *Cafeteria*.
6. In the **Configuration** section, enter the device address. For example: *INFP , 0 , 1*
7. Click **Save**.

Verify the INFP configuration

You can verify that the configuration of the INFP by sending an alert and checking the logs. To verify that the INFP plug-in has been correctly installed, complete the following steps:

1. Log in to the BlackBerry AtHoc Management System as an operator and create an alert.
2. Fill in the **Content** section.
3. In the navigation bar, click .
4. In the **Targeting** section, select the **Indoor Fire Panel device** under **Mass Devices**.
5. Select the mass device account for the INFP to be activated.
6. Click **Options**.

The options for playing the audio message appear.

7. Select **Pre Tone** and choose a tone that announces a message.
8. Click  to listen to the selected tone.
9. Specify the audio message that will be played:
 - Select **Audio Message** to choose an audio message (pre-recorded) that plays an announcement.
 - Click  to listen to the selected message.
 - Select **Text to Speech** to convert the alert content, or custom text, to a spoken announcement.
10. Enter numerical value for the number of times the audio message will be played. One time is the default.
11. Select **Post Tone** and choose a tone to play after the message completes.
12. Click  to listen to the selected tone.
13. Click **Apply**.
14. Complete the alert content and settings.
15. Click **Review and Publish**.

16.Review the alert content and settings.

17.Click **Publish**.

18.Check the device to determine whether the INFP relay has been activated and if the tones and alert audio content are heard.

19.Check the logs for any errors.

Configure a distributed integration with the 8-channel IIM

The BlackBerry AtHoc 8-channel INFP IIM provides IP access for your fire panel to the BlackBerry AtHoc Management System. If you want BlackBerry AtHoc to send alerts directly to each fire panel (as opposed to a central fire panel that controls the other fire panels) you connect an 8-channel INFP IIM to each fire panel.

Example: Company XYZ decides to use a distributed configuration for their campus that has five buildings. They put a fire panel and IIM in each building; each IIM connects the fire panel to the BlackBerry AtHoc management system. Additionally, they decide they need several groups so that certain fire panels can be activated together, or all together at once.

A distributed configuration places an IIM at each end point. This type of configuration uses the same feed for all end points, so you must assign addresses in the filter.options file that match the address for a mass device for each IIM/fire panel. The alert targets the addresses for the mass devices to be activated.

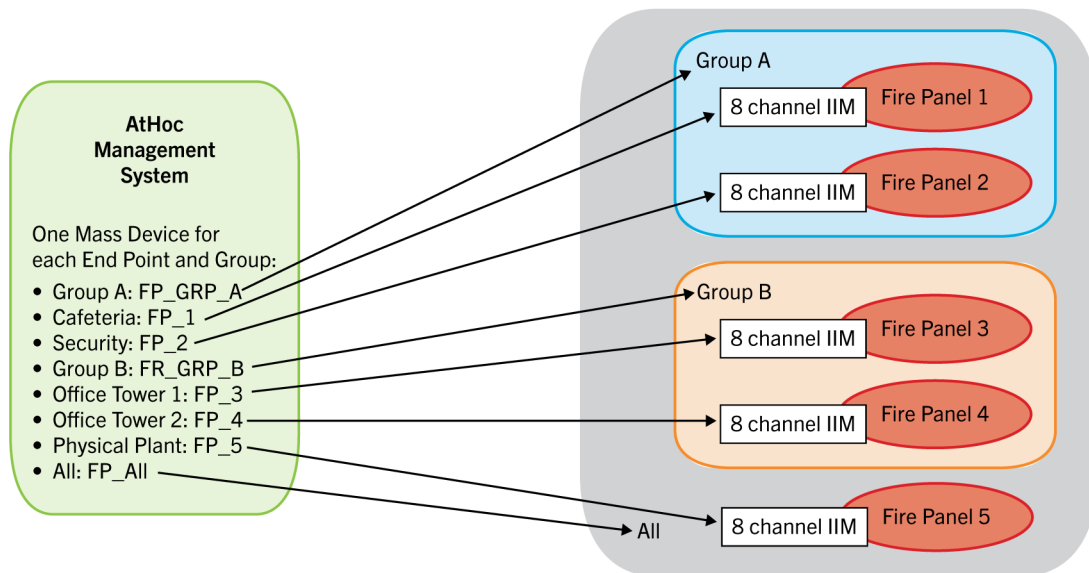


Figure 2: 8-channel fire panel IIM configuration

Prerequisites

The following sections describe hardware and software requirements that are necessary for configuring INFP.

Software requirements

- BlackBerry AtHoc Management System, Version 6.1.8.85 CP9 and higher.
- The following packages must be installed and configured:
 - Latest IIM Agent 1.1.0 package
 - Latest INFP package
 - Latest CapNode package on each IIM

Hardware requirements

For each connected INFP, you must have an A-line level input into an auxiliary audio input module.

Configure the 8-channel IIM

For each building fire panel, configure an INFP IIM.

Prerequisite: Ensure that the following packages are installed and configured before starting these steps:

- Latest Indoor Fire Panel package
- Latest Capnode package on the IIM

Configure the IIM

1. Attach a keyboard and mouse to the IIM device.
2. Log in to the IIM as an administrator.
3. Edit the `filter.configure` file to configure the addresses of the INFP IIM that is targeted by BlackBerry AtHoc alerts.

Assign an individual address to each INFP IIM device and also each INFP group. If the IIM is in a group, assign a group address to it, as well. If you target a group, all IIMs in that group will activate. The address range is 0-7.

The address has the following syntax: `INFP, x, n`:

Where:

`x` specifies the type of address.

- 0 - all IIMs
- 1 - a group of fire panels
- 2 - an individual fire panel

`n` identifies a single IIM, or a group of IIMs.

Examples:

- `INFP,0,0` is all connected fire panels.
- `INFP,1,1` is group 1
- `INFP,2,1` is the first individual fire panel

A typical INFP IIM will have filter entries of `INFP,0,0` `INFP,1,x` and `INFP,2,y` where `x` is the group (zone) it belongs to and `y` is the identifier number (such as a building number). There may be multiple `INFP,1,x` settings if an individual is part of multiple groups.

Example: Company XYZ Corp. has five buildings. Each building has a fire panel, for a total of five fire panels. Additionally, you want to group buildings that are next to each other, in case a fire has spread to the next building. You decide to use two groups (A, B). You would assign an address for each INFP and for each group.

INFP IIM	Building	Addresses in filter.config	Group Name	Device Name
1	Cafeteria	INFP,2,1 INFP,1,6 INFP,0,0	INFP_A	Cafeteria
2	Security	INFP,2,2 INFP,1,6 INFP,0,0	INFP_A	Security
3	Office Tower 1	INFP,2,3 INFP,1,7 INFP,0,0	INFP_B	Office Tower 1

INFP IIM	Building	Addresses in filter.config	Group Name	Device Name
4	Office Tower 2	INFP,2,4 INFP,1,7 INFP,0,0	INFP_B	Office Tower 2
5	Physical Plant	INFP,2,5 INFP,0,0	None	Physical Plant
None	Group A	INFP,1,6	None	Group A
None	Group B	INFP,1,7	None	Group B
None	ALL	INFP,0,0	INFP_ALL	All

This configuration will allow you to target each INFP IIM, either of the groups, or all of the INFP devices.

To configure the address for an INFP IIM, complete the following steps:

1. Navigate to the following directory: `C:\program files\capnode`.
2. Edit the `filter.config` file to add an address for the current INFP IIM.
3. Add the address values: `addresses=<INFPaddress1 INFPaddress2 INFPaddressn>`

In the example, the address values for the first INFP IIM include the address for the cafeteria INFP IIM the address for the Group A,, and the address for ALL, as shown in the following example: `address=INFP,1,1 INFP,1,6 INFP,0,0`.

4. Save the file.

Modify the IIM Agent and Capcon services to poll and post to the BlackBerry AtHoc URL:

1. From the IIM server, open the following file: `..\ProgramFiles\capnode\system_private.config`.
2. Change the `indexURL` value using the following format: `indexURL=http\://IWSAlertsServerURL/Syndication/CAP_INFP/VPSProvider_ID/Capindex?ast=MAC_Address`.

Make sure following values have the identical ID:

- The `myid.txt` file
- The database record in the `AST_ASSET_TAB`
- The Inbound CAP Event Agent `<EventMapping>` node
- The value of the `<sender>` node in the IIM originates from the `myid.txt` file in the following location `..programfiles\capnode\myid.txt` and should match the `ASSET_NAME` field in the `AST_ASSET_TAB` database table...`\Program Files\capnode\`. The value of the `myid.txt` file is the MAC address of the IIM that manages the INFP.

In the same file, modify the `CapPostingTarget.capurl` value. Enter the BlackBerry AtHoc server URL in the highlighted attribute value:

```
CapPostingTarget=True
CapPostingTarget.capurl=https\://IWSAlertsURL/syndication/PostCap
```

Optionally, configure the proxy server and port settings in the same file:

1. Add the values for the proxy port and server parameters.
2. Save the file.

Restart the CapCon service.

(Optional) Configure the IIM agent

1. Edit the following file: `..\programfiles\capnode\iimm\IIMAgent.exe.config`.
2. Modify the `<add>` node. `<add key = "ServerURL" value="https://IWSAlertServerURL".../>`

3. Save your changes.
4. Restart the IIM Agent service.
 - a. Navigate to the following directory: `../AtHocENS/DeliveryServer/Installations`.
 - b. Run `Start Services`.

Configure the INFP device on the BlackBerry AtHoc management system

This section describes the steps to configure an INFP on the BlackBerry AtHoc management system to make it available as a target in an alert. Before starting these steps, ensure that you meet the requirements in the Prerequisites section for this device.

Enable the INFP device on the BlackBerry AtHoc application server


Enable the INFP device on the BlackBerry AtHoc application server to make it available for the AtHoc organizations in the system. Depending on the version of BlackBerry AtHoc, the device is either included in the installation of BlackBerry AtHoc, or available from your account representative.

1. Log in to the BlackBerry AtHoc server as a system administrator.
2. Navigate to the following directory: `\AtHocENS\ServerObjects\tools`.
3. Run the following file: `AtHoc.Applications.Tools.InstallPackage.exe`.
4. On the **Configure Device Support** screen, select **Indoor Fire Panel**.

Note: If the device does not appear in the list, contact BlackBerry AtHoc Technical Support to get the installation package for the device.


5. Click **Enable** to install and enable the devices.
6. Close the **Installation Complete** screen.
7. Close the **Device Support** Dialog.

Configure the indoor fire panel delivery gateway

1. Log into the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click .
3. In the **Devices** section, open the **Indoor Fire Panel** gateway.
4. On the **gateway** screen, click **Copy default settings**.
5. Click **Save**.

Enable the indoor fire panel device

After you have configured the Indoor Fire Panel gateway, configure the associated device.

1. In the navigation bar, click .
2. In the **Devices** section, click **Devices**.
3. Select **Indoor Fire Panel**.
4. On the **device settings** page, click **Edit**.
5. Click **Add a Delivery Gateway** and select the gateway.
6. Click **Save**.
7. Click **Configure** to verify that the configuration information is populated.

- Check for XML code in the text field. If the XML statements are not provided, cut and paste the following code into the text field:

```
<Configuration>
  <CapParams>
    <GVSystemType>INFP</GVSystemType>
    <AllMode>0</AllMode>
    <ZoneMode>0</ZoneMode>
    <PoleMode>0</PoleMode>
    <UnusedMode>0</UnusedMode>
    <DefaultAllCall>0</DefaultAllCall>
    <DefaultKeyActivationCode>0</DefaultKeyActivationCode>
    <NoPARequired>0</NoPARequired>
    <PARequired>1</PARequired>
    <IsCancelable>>false</IsCancelable>
    <ContentSource>Indoor-Fire-Panel</ContentSource>
  </CapParams>
</Configuration>
```

- Click **Enable**.

The status line at the top of the screen updates and indicates that the device is enabled.

Configure a mass device for each INFP IIM

Each fire panel is an endpoint of an alerting system. In this case, the fire panel is also considered a mass communication device because it alerts an unknown number of recipients—whichever is in the vicinity of the device. In the BlackBerry AtHoc management system, an object called a mass device is configured for each mass communication endpoint. For each building fire panel, you will configure a mass device.

Before you begin, plan how many mass devices to create based on the number of building fire panels. First, determine how many fire panels you have. You define a mass device endpoint for each INFP. You create the endpoint and use the addresses that you entered in the `filter.options` file.

Example

XYZ Corp. has five buildings. Each building has a fire panel, for a total of five fire panels. Additionally, you want to group buildings that are next to each other, so you decide that you are going to use two groups (A, B). You would also like one mass device that activates all building fire panels. You would create eight mass device accounts and in the Configuration section of the New Device Endpoint screen, enter the device addresses

Building	Mass Device Endpoint	Mass Device Endpoint Display Name	Endpoint Address
Cafeteria	FP_1	Cafeteria	INFP,2,1
Security	FP_2	Security	INFP,2,2
Office Tower 1	FP_3	Office Tower 1	INFP,2,3
Office Tower 2	FP_4	Office Tower 2	INFP,2,4
Physical Plant	FP_5	Physical Plant	INFP,2,5
Group A (Cafeteria and Security)	FP_GRP_A	Group A	INFP,1,6

Building	Mass Device Endpoint	Mass Device Endpoint Display Name	Endpoint Address
Group B (Office Towers 1 and 2)	FP_GRP_B	Group B	INFP,1,7
All Buildings	FP_ALL	All Buildings	INFP,0,0

If the device name for the Cafeteria is FP_1, and the device address is INFP,2,1, then an operator can target FP_1 in an alert. When the alert is sent, the dry contact on the Cafeteria IIM is closed. Closing the dry contact activates the relay for the fire panel in the Cafeteria.

The address has the following syntax: `INFP , x , n`

Where:

x specifies the type of address.

- 0—all IIMs
- 1—a group of fire panels
- 2—an individual fire panel


n identifies a single IIM, or a group of IIMs.

Examples:

- INFP,0,0 is all connected fire panels
- INFP,1,1 is group 1
- INFP,2,1 is the first individual fire panel


Each of these mass devices represents an INFP IIM and the address information must be configured manually. This includes creating hierarchies, distribution lists, and other grouping mechanisms.

To create a mass device endpoint for an INFP IIM, complete the following steps:

1. Log in to the BlackBerry AtHoc management system with operator privileges.
2. Click .
3. In the **Devices** section, click **Mass Device Endpoints**.
4. On the **Mass Device Endpoints** page, click **New**, and then select the fire panel.
5. On the **New Mass Device Endpoints** screen, in the **General** section, enter the **Endpoint Name** and **Common Name** for the device. For example: `FP_1`.
6. In the **Configuration** section, enter the device address. For example: `INFP , 2 , 1`.
7. Click **Save**.

Verify the INFP configuration


You can verify that the configuration of the INFP by sending an alert and checking the logs. To verify that the INFP plug-in has been correctly installed, complete the following steps:

1. Log in to the BlackBerry AtHoc Management System as an operator and create an alert.
2. Fill in the **Content** section.
3. In the navigation bar, click .
4. In the **Targeting** section, select the **Indoor Fire Panel device** under **Mass Devices**.
5. Select the mass device account for the INFP to be activated.


6. Click Options.

The options for playing the audio message appear.

7. Select Pre Tone and choose a tone that announces a message.


8. Click  **to listen to the selected tone.**

9. Specify the audio message that will be played:

- Select **Audio Message** to choose an audio message (pre-recorded) that plays an announcement.
- Click  to listen to the selected message.
- Select **Text to Speech** to convert the alert content, or custom text, to a spoken announcement.

10. Enter numerical value for the number of times the audio message will be played. One time is the default.

11. Select Post Tone and choose a tone to play after the message completes.

12. Click  **to listen to the selected tone.**

13. Click Apply.

14. Complete the alert content and settings.

15. Click Review and Publish.

16. Review the alert content and settings.

17. Click Publish.

18. Check the device to determine whether the INFP relay has been activated and if the tones and alert audio content are heard.

19. Check the logs for any errors.

BlackBerry AtHoc Customer Support Portal

BlackBerry AtHoc customers can obtain more information about BlackBerry AtHoc products or get answers to questions about their BlackBerry AtHoc systems through the Customer Support Portal:

<https://support.athoc.com/customer-support-portal.html>

The BlackBerry AtHoc Customer Support Portal also provides support via computer-based training, operator checklists, best practice resources, reference manuals, and user guides.

Legal notice

©2020 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at <http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp>.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada