



Media Flow Devices



Published: 2013-06-20

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Media Flow Devices

Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	vii
	Documentation and Release Notes	vii
	Documentation Conventions	vii
	Documentation Feedback	ix
	Requesting Technical Support	ix
	Self-Help Online Tools and Resources	x
	Opening a Case with JTAC	x
Part 1	Overview	
Chapter 1	Understanding Media Flow Controllers with Media Flow Activate	3
	Media Flow Activate Overview	4
	Understanding Media Flow Controller Management with Media Flow Activate	6
	BGP Traffic Steering Overview	8
	Resource Pools Overview	9
	Configuration Templates Overview	10
Part 2	Administration	
Chapter 2	Managing and Monitoring Media Flow Controllers with Media Flow Activate	19
	Monitoring a Media Flow Controller Dashboard from MFA	19
	Launching the Media Flow Controller Secure Console from MFA	20
	Upgrading or Rolling Back the Media Flow Controller Software Image	22
	Restoring Media Flow Controller Device Configuration	24
	Replicating Media Flow Controller Device Configuration	26
	Restarting Media Flow Controller Devices or Services	27
	Tagging Media Flow Controller Objects	28
	Provisioning Resource Pools to MFC Devices	29
	Managing Resource Pool Associations	30
	Actions on Resource Pools	32
	Fault Monitoring with SNMP	33
	Audit Logs Workspace Overview	39
	Job Management Workspace Overview	42
Part 3	Configuration	
Chapter 3	Configuring Media Flow Controllers with Media Flow Activate	47
	Configuring MFC Device Interfaces	47
	Configuring Bonded Interfaces	49

Configuring Devices	51
Configuring BGP-Based Traffic Steering	53
Creating Resource Pools	55

Part 4

Index

Index	59
-------------	----

List of Tables

	About the Documentation	vii
	Table 1: Notice Icons	viii
	Table 2: Text and Syntax Conventions	viii
Part 1	Overview	
Chapter 1	Understanding Media Flow Controllers with Media Flow Activate	3
	Table 3: MFC CLI Commands Supported Through Junos Space Configuration Templates	14
Part 2	Administration	
Chapter 2	Managing and Monitoring Media Flow Controllers with Media Flow Activate	19
	Table 4: SNMP Alarm Events	35
	Table 5: SNMP Clear Alarm Events	37

About the Documentation

- Documentation and Release Notes on page vii
- Documentation Conventions on page vii
- Documentation Feedback on page ix
- Requesting Technical Support on page ix

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

Table 1 on page viii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page viii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: <code>user@host> configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: <code>[edit]</code> <code>root@# set system domain-name <i>domain-name</i></code>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub <default-metric <i>metric</i>>;</code>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [Understanding Media Flow Controllers with Media Flow Activate on page 3](#)

CHAPTER 1

Understanding Media Flow Controllers with Media Flow Activate

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- [BGP Traffic Steering Overview on page 8](#)
- [Resource Pools Overview on page 9](#)
- [Configuration Templates Overview on page 10](#)

Media Flow Activate Overview

Media Flow Activate (MFA) is a Junos Space–based management application that helps you to simplify the configuration and deployment of Juniper Networks Media Flow Controller devices. With Media Flow Activate, network administrators can centrally configure their content delivery nodes and rapidly provision new content delivery services.



NOTE:

- Use Media Flow Activate to manage Media Flow Controllers that you have discovered with the Junos Space Network Platform application. For information about discovering Media Flow Controllers, see the “Discovering Media Flow Controllers” section in the *Media Flow Activate Installation Guide*. At this time, you cannot use the SNMP method to discover Media Flow Controllers via the Junos Space Network Platform application; you must use the Ping method.
- Media Flow Activate version 3.3 can manage Media Flow Controller devices installed with a Media Flow Controller version 12.2.4 image.

Refer to the “Version Compatibility Matrix” table in the *Media Flow Activate Installation Guide*, for more information.

If you are an Internet service provider, you can create a **Network Optimization Service** to transparently cache a popular website, thereby saving bandwidth and optimizing Internet content delivery.

If you are a content provider or a Content Delivery Network (CDN) service provider who owns or manages any content, you can create an **HTTP Reverse Proxy Service** to efficiently deliver that content.

To use Media Flow Activate to manage Media Flow Controllers, see the following topics:

- [“Understanding Media Flow Controller Management with Media Flow Activate” on page 6](#) for information about managing discovered devices, including software upgrades, device restarts, and service restarts, on selected Media Flow Controllers.
- [“Configuring Devices” on page 51](#) for information about configuring the interfaces to deliver media for transparent and reverse proxy services.
- [“Configuring BGP-Based Traffic Steering” on page 53](#) for information about redirecting traffic from a peering router to Media Flow Controller by advertising certain destination IP network addresses.
- [“Resource Pools Overview” on page 9](#) for information about configuring resource utilization limits for concurrent connections and bandwidth usage for multiple tenants that are hosted on Media Flow Controller.
- *Understanding Virtual Players* for information about setting media delivery options for video trick play (such as seek, fast start, and full download) and authentication. You configure a virtual player for each type of media that you deliver. A single virtual player

can be used in multiple configured services. See *Creating Virtual Players* for configuration details and for information about how to import a virtual player.

- *Understanding Cache-Tuning Policies* for information about setting cache-handling options, including how long objects can stay in the cache. A single cache-tuning policy can be used in multiple configured services. See *Creating Cache-Tuning Policies* for configuration details and for information about how to import a cache-tuning policy.
- *Understanding Origin Maps* for information about origin maps (consistent hash map and escalation map). You configure a consistent hash map when you want to create a cluster of nodes and distribute the incoming requests across these nodes, thereby increasing the cache storage capacity (see *Creating Consistent Hash Maps* for information about creating a consistent hash map). You configure an escalation map when you want to configure multiple redundant HTTP origin servers for failover protection (see *Creating Escalation Maps* for information about creating an escalation map).
- *Understanding Access Log Profiles* for information about configuring access log profiles. You configure an access log profile to tune the access log format and storage. Access logs are used to analyze the HTTP traffic handled by Media Flow Controller.
- *Understanding Policy Scripts* for information about configuring policy scripts. Using Media Flow Activate, you can bind a policy script to a service, which enables you to have a greater control over how Media Flow Controller caches and delivers objects when the service receives requests from clients.
- *Service Design Overview*, *Network Optimization Services Overview*, and *HTTP Reverse Proxy Services Overview* for information about configuring websites for media delivery, and *Content Ingest Services Overview* for information about preloading content from origin servers at predefined time intervals. See *Creating Network Optimization Services*, *Creating HTTP Reverse Proxy Services*, and *Creating Content Ingest Services* for configuring Network Optimization service, HTTP Reverse Proxy service, and Content Ingest service, respectively.
- *Provisioning Services Overview*, *Provisioning Services*, and *Managing Provisioned Services* for information about provisioning configured services to selected Media Flow Controllers.
- [“Configuration Templates Overview” on page 10](#) for information about managing Media Flow Controller specific device templates. Device templates provides a way to configure the CLI commands that are not supported through the Media Flow Activate GUI.

Though you can configure a Media Flow Controller device by using any of the following options—device templates, Media Flow Activate GUI, or console—the typical flow would be to use the device templates to perform the infrastructure provisioning before performing the service provisioning by using the Media Flow Activate GUI. Use the console to configure a feature that is not supported by Media Flow Activate either through the purpose built GUI or device configuration templates.
- [“Fault Monitoring with SNMP” on page 33](#) for information about monitoring the performance statistics of Media Flow Controller devices.

- [“Audit Logs Workspace Overview” on page 39](#) for information about monitoring the tasks initiated from the Media Flow Activate GUI.
- [“Job Management Workspace Overview” on page 42](#) for information about monitoring jobs, which represent user-initiated actions on selected Junos Space objects.



NOTE: See the *Juniper Networks Media Flow Controller Administrators Guide* for detailed information about configuring Media Flow Controllers. See *Quick Reference to Tasks in Media Flow Activate* for a list of tasks that you can perform in Media Flow Activate.

**Related
Documentation**

- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- *Quick Reference to Tasks in Media Flow Activate*

Understanding Media Flow Controller Management with Media Flow Activate

This topic describes the **Manage MFCs** page and the actions you can take on this page.

After you access the Media Flow Activate **Manage MFCs** page, you can select any discovered devices and take actions on them by using the **Actions** list.

Click the **Actions** list, then click one of the following action links:

- **Launch Dashboard**—Click to display the Media Flow Controller Console login page. Log in to display the dashboard page for that Media Flow Controller. The statistical information and the graphs show the usage for the selected Media Flow Controller. See [“Monitoring a Media Flow Controller Dashboard from MFA” on page 19](#) for details about launching a dashboard from Media Flow Activate.
- **Launch Secure Console**—Click to display the Secure Console page. Enter your login credentials to open an SSH connection to connect to Media Flow Controller directly from Media Flow Activate. See [“Launching the Media Flow Controller Secure Console from MFA” on page 20](#) for details about launching a Media Flow Controller secure console from Media Flow Activate.
- **Software Image Management**—Click to display the **Software Image Management** page. See [“Upgrading or Rolling Back the Media Flow Controller Software Image” on page 22](#) for details about upgrading or rolling back a Media Flow Controller software image.
- **Restore Device(s)**—You can choose to restore or remove the service configurations of the selected Media Flow Controllers. See [“Restoring Media Flow Controller Device Configuration” on page 24](#) for details about restoring a Media Flow Controller device configuration.
- **Replicate Device**—You can replicate or clone the device configuration of one Media Flow Controller to one or more Media Flow Controllers. See [“Replicating Media Flow Controller Device Configuration” on page 26](#) for details about replicating a Media Flow Controller device configuration.

- **Device Configuration**—Click to display the **Device Configuration** dialog box. See [“Configuring Devices” on page 51](#) for details about configuring the Media Flow Controller delivery interfaces.
- **Configure BGP**—Click to display the **Configure BGP** dialog box. See [“Configuring BGP-Based Traffic Steering” on page 53](#) for details about configuring BGP-based traffic steering in Media Flow Controllers.
- **Restart Service**—Click to display the **Restart Service** confirmation page. Click **Yes** to restart the delivery service on the selected device or devices. See [“Restarting Media Flow Controller Devices or Services” on page 27](#) for details about restarting services on Media Flow Controllers.
- **Restart Device(s)**—Click to display the **Restart Device(s)** confirmation page. Click **Yes** to restart the selected device or devices. See [“Restarting Media Flow Controller Devices or Services” on page 27](#) for details about restarting Media Flow Controller devices.
- **Tagging an Object**—Click **Tag Device(s)**, **Untag Device(s)**, or **View Tags** to tag, untag, or view tags, respectively. See [“Tagging Media Flow Controller Objects” on page 28](#) for details about tagging Media Flow Controller objects.

From the **Manage MFCs** page, you can also:

- **Manage or create design elements**—Click **Design Elements** from the left navigation panel to navigate to the Design Elements workspace. See *Understanding Access Log Profiles*, *Understanding Cache-Tuning Policies*, *Understanding Origin Maps*, *Understanding Policy Scripts*, and *Understanding Virtual Players* for information about design elements.
- **Manage or create delivery services for websites**—Click **Service Design** from the left navigation panel to navigate to the Service Design workspace. See *Service Design Overview* for information about the services that are supported from Media Flow Activate.
- **Provision existing services**—Click **Service Provisioning** from the left navigation panel to navigate to the Service Provisioning workspace. See *Provisioning Services Overview* for information about provisioning services to Media Flow Controllers.
- **Monitor the faults in Media Flow Controllers**—Click **Network Monitoring** from the left navigation panel to navigate to the Network Monitoring workspace. See [“Fault Monitoring with SNMP” on page 33](#) for monitoring faults in Media Flow Controllers.
- **Monitor the audit logs that are generated**—Click **Audit Logs** from the left navigation panel to navigate to the Audit Logs workspace. See [“Audit Logs Workspace Overview” on page 39](#) for information about monitoring the audit logs.
- **Check the status of the jobs that you are running**—Click **Job Management** from the left navigation panel to open the Job Management workspace > Jobs status page. You can check the status of the following job types: Provisioning, Restart Service, Software Upgrade, or Restart Devices. See [“Job Management Workspace Overview” on page 42](#) for information about monitoring the jobs that are initiated from Media Flow Activate



NOTE: See the *Juniper Networks Media Flow Controller Administrators Guide* for detailed information about the features described in this topic.

- Related Documentation**
- [Media Flow Activate Overview on page 4](#)
 - [Configuration Templates Overview on page 10](#)
 - [Quick Reference to Tasks in Media Flow Activate](#)

BGP Traffic Steering Overview

Media Flow Controller listens for HTTP requests and either serves the content from its local cache or fetches the requested content from origin servers. In this deployment, Media Flow Controller is exposed to much non-cacheable traffic that wastes valuable caching resources. The solution is to separate cacheable traffic from non-cacheable traffic to provide better bandwidth savings and throughput by efficiently using Media Flow Controller resources. The Border Gateway Protocol (BGP) traffic steering feature enables you to direct traffic from a peering router to Media Flow Controller by advertising certain destination IP addresses. You can use this feature in transparent and reverse proxy deployments.

- In transparent proxy deployment, you can use this feature as a replacement for the Policy Based Routing (PBR) feature, which is currently used to direct HTTP traffic from an access router to Media Flow Controller.
- In reverse proxy deployment, you can advertise a set of IP addresses mapped to different services or resource pools to an access router. This configuration can be used for load sharing within a POP.

To redirect cacheable traffic to Media Flow Controller:

1. Create a list of IP network addresses, so that any HTTP traffic intended for these IP addresses is redirected to Media Flow Controller. This list can be static or dynamic.

Media Flow Controller serves the requested object from its cache or fetches it from the origin servers.



NOTE: In networking terminology, this list of IP addresses is often called “IP whitelist.”

2. Configure the neighbors.

For example:

- Configure edge router A to which Media Flow Controller advertises the IP whitelist. Media Flow Controller acts as the next hop to this router for the IP addresses in the whitelist. This router must support basic BGP functionalities.
- Configure edge router B for Media Flow Controllers to forward any non-HTTP, non-RTSP, and non-RTMP traffic.

The flow of traffic is as follows:

- For request traffic with a destination IP address that is not listed in the whitelist, the access router A forwards the traffic to the server through the next-hop router B, bypassing Media Flow Controller. The return traffic takes the reverse path.
- For unwanted traffic (that is, non-HTTP, non-RSTP, and non-RTMP traffic) that is destined to the IP addresses that are listed in the whitelist, access router A forwards the traffic to Media Flow Controller, which then forwards it to the default next-hop router B. The return traffic uses the client address as the destination IP address and bypasses Media Flow Controller.
- For intended traffic that is destined to IP addresses that are listed in the whitelist (that is, HTTP, RSTP, or RTMP requests), if there is a cache hit, the object is served from the cache. If there is no cache hit, Media Flow Controller fetches the object from the origin server and serves the request.

When intended traffic is forwarded to the origin server, one of Media Flow Controller's own IP addresses is used to replace the client address as the source IP address. This ensures that the response traffic is routed to Media Flow Controller for caching.



TIP: Because there is a likelihood that unintended traffic can be sent to Media Flow Controllers and this traffic needs to be forwarded to the next-hop router, IP forwarding must be enabled on Media Flow Controllers. Use the `network connection ip-forward` command to enable IP forwarding.

Related Documentation

- [Configuring BGP-Based Traffic Steering on page 53](#)
- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- [Quick Reference to Tasks in Media Flow Activate](#)

Resource Pools Overview

When you want to use Media Flow Controller to host multiple tenants (customers or Web portals), it becomes necessary to allocate the available Media Flow Controller resources among these tenants depending on various criteria, such as whether they are silver, gold, or platinum customers. Using Media Flow Activate, you can create a resource pool to configure resources that are relevant for a tenant, such as the maximum bandwidth and the maximum allowed sessions.

Before you start configuring a resource pool, consider the following parameters:

- The maximum bandwidth that you want to allocate to a resource pool
- The maximum concurrent sessions that you want to permit for a resource pool

Because the resource pool is provisioned on Media Flow Controller, the preceding parameters cannot exceed the maximum resources available on the device and are identified by the “global resource pool.”

After you create the resource pools:

- Provision the resource pools to Media Flow Controller. This action partitions the available resources among these pools.
- Bind a reverse proxy service to the resource pool.

The preceding actions ensure that the incoming requests to the website or domain configured in the service do not exceed the limits set by the resource pool, thereby ensuring that the remaining resources are available for other services configured in the same Media Flow Controller. If no pool is configured, the service receives all the available resources.

For more information about resource pools, see the “Media Flow Controller Multi-Tenancy Management” section in the *Media Flow Controller Administrator's Guide*.

**Related
Documentation**

- [Creating Resource Pools on page 55](#)
- [Actions on Resource Pools on page 32](#)
- [Provisioning Resource Pools to MFC Devices on page 29](#)
- [Managing Resource Pool Associations on page 30](#)
- [Provisioning Services](#)
- [Media Flow Activate Overview on page 4](#)
- [Quick Reference to Tasks in Media Flow Activate](#)

Configuration Templates Overview

Using the Device Templates feature in Junos Space Network Application Platform, you can create Media Flow Controller–specific device templates to provision platform attributes in multiple Media Flow Controller devices. [Table 3 on page 14](#) lists the Media Flow Controller–specific attributes or CLI commands that are supported through this feature.

You use this feature when you want to configure those aspects of infrastructure that need to be provisioned before the Content Delivery Infrastructure (CDI) can provide content delivery services. This is because it is necessary that the server (physical or virtual) and the delivery application (Media Flow Controller) are configured correctly before the services are provisioned. Some of the configuration that you can set up before provisioning the services (namespaces) and their related attributes are: configuring the management IP address, and the TACACS and SNMP server addresses, bonding the Ethernet interfaces, and so on.

As a network operator, use device templates to:

- Develop and maintain a set of basic platform provisioning CLI commands as a template and provision the template to all new devices at the receiving (preparation) center before sending the devices for rack installation at the deployment location.

- Develop and maintain templates for different geographic locations or regions, server types (such as VXA or MX Series service card), or deployment types (such as an edge or midtier parent).

When you have device-specific values, you might want to consider a comma-separated value (CSV) file for a template definition. After you have created a CSV file, you must import it into Junos Space. See “Specifying Device-Specific Values in Definitions” in the *Junos Space Network Application Platform User Guide* for more information about creating a device-specific template definition.

Such one-time configuration commands are best suited to be part of device templates. You can also create a golden configuration for all devices in the network on the basis of locations, cache tier, and so on, which you can use to readily bring up a new device.



NOTE:

- The commands that are available through the Device Templates feature and the commands that are available through the MFA GUI are mutually exclusive. This ensures that there are no mismatches between the device template configuration and the configuration done through the MFA GUI.
- Template definition and deployment is Media Flow Controller version specific. That is, there are different template definition schemas published for different Media Flow Controller versions.

“Device Templates” in the *Junos Space Network Application Platform User Guide* contains detailed instructions on creating and deploying template definitions and templates. Briefly, the process to deploy a template to Media Flow Controller devices is as follows:

Before you begin:

- Make sure you have the appropriate permissions. You need the **Template Design Manager** role to create and publish template definitions. Typically, the user with the **Template Manager** role selects a template definition and creates a template from it to configure one or more devices.
- You must not use your browser’s Back and Forward buttons to navigate the **Device Templates** pages.
- You must configure all the supported Media Flow Controller properties in one single template.
- You must upload the MFC 12.2.4 configuration schema file (config.xsd file) to Junos Space Network Application platform and set this schema as the default schema. You must contact the Juniper Networks technical support team to obtain this file.

Perform the following steps to upload this configuration schema file to Junos Space Network Application platform:

- a. Download this configuration schema file to your system.
- b. From the Junos Space Network Platform GUI, select **Platform > Administration > Manage DMI Schemas > Update Schema**. The **Schema Update** page displays.

- c. From the **Schema Update** page, click the **Browse** button adjacent to the **Archived Schemas File** field and select the configuration file from your system.
- d. Click **Upload**. This file appears under the **Available Updates (already installed versions are pre-selected)** area.
- e. Select the **Enable Schema Overwrite** check box.
- f. From the **Available Updates (already installed versions are pre-selected)** area, select this configuration file and click **Install**.
- g. After the successful installation of the schema, click **Manage DMI Schemas**. The **Manage DMI Schemas** page is displayed.

To verify whether the schema has been successfully installed, see the corresponding job in the Job Management workspace.
- h. From the **Manage DMI Schemas** page, select this configuration file.
- i. From the **Actions** list, click **Set Default Schema** to set this schema as the default schema.

1. On the **Create Definition** page, create a template definition.

To complete this task, follow the instructions mentioned in “Creating a Template Definition” in the *Junos Space Network Application Platform User Guide*.

When you create a template definition, make sure that you:

- a. Select the **Media Flow** device family.
- b. Select the appropriate **OS Version**. The Device Templates feature is supported for Media Flow Controller devices running version 12.2.4 or later.
- c. Use the search function to quickly locate a specific configuration option. For more information about locating a specific configuration option, see “Finding Configuration Options” in the *Junos Space Network Application Platform User Guide*.
- d. Set device-specific values, if needed. For more information about setting device-specific values, see “Specifying Device-Specific Values in Definitions” in the *Junos Space Network Application Platform User Guide*.

The template definition file that you create is an XML file. The template definition file contains its own schema and is different from the device configuration schema. A template definition can be exported, modified, and imported to the same or a new Junos Space server. For more information about template definitions, see “Template Definitions” in the *Junos Space Network Application Platform User Guide*.

2. Publish the template definition. For more information about publishing a template definition, see “Publishing and Unpublishing a Template Definition” in the *Junos Space Network Application Platform User Guide*.
3. Define a configuration template or a variable-based configuration template with a fixed set of configuration commands from the template definition.

For example, to map a license to a device, you need to provision a variable-based configuration template. Junos Space configuration templates provide you with an

option of marking this configuration value as “device-specific.” Typically, template designers use a comma-separated value (CSV) file to provide device-specific values in a template definition.

You can also use rules to supplement the device-specific value capability supplied by CSV files. Specify rules to resolve device-specific values at the time of deployment. You can use rules in addition to or instead of CSV files.

To create a template, follow the instructions mentioned in “Creating a Template” in the *Junos Space Network Application Platform User Guide*. Ensure that you select a **MEDIA-FLOW** template.



TIP:

Before you deploy the device template:

- Select the template that is most appropriate for your requirement from the **Manage Templates** page.
- User must create a single template for each “mfc-cluster” object as the template deployment is not additive and if you create and deploy a new template for each feature under the same “mfc-cluster” object to a device, the previous template deployed for that ‘mfc-cluster’ object is undeployed, even if the subsequent template contains only additional parameter settings.

4. Deploy the template to one or more Media Flow Controllers either on demand or at a scheduled time in the future. You can select the Media Flow Controllers one by one or filter them using their tags. Each publishing is handled as a Junos Space job. When a configuration template is published to multiple Media Flow Controllers, the publishing status for each Media Flow Controller is displayed in a separate row in the Job Management workspace.

This deployment action also allows you to validate the template against the device family and against the device. For more information about deploying a template, see “Deploying a Template” in the *Junos Space Network Application Platform User Guide*.

After you deploy the template, if you want to:

- View the list of devices to which a template has been deployed, select **View Template Deployment** from the **Actions** list.
- Verify the extent to which a template and the device to which the template has been deployed match, select **Audit Log Config** from the **Actions** list.

For troubleshooting, see “Troubleshooting” under “Device Templates” in the *Junos Space Network Application Platform User Guide*.

[Table 3 on page 14](#) lists the Media Flow Controller CLI commands that are supported through the Device Templates feature:

Table 3: MFC CLI Commands Supported Through Junos Space Configuration Templates

CLI Commands	Description
license install	Activate features with license keys.
Hostname	Set the system's hostname.
ip name-server	Add a name server.
ip default-gateway	Set the default gateway.
ip route	Add a static route.
ip domain-list	Add a domain name to use when resolving hostnames.
ntp server	Set the NTP server. This command can be deleted or disabled.
clock timezone	Set the timezone. This command can be deleted or disabled.
ssh client user <user> authorized-key sshv2 <key>	Set SSH client authentication.
ssh server enable listen	Set SSH server configuration.
snmp-server	Set up the SNMP server, such as IPv4 SNMP Host, community string, listen interface, syscontact, and syslocation. These parameters are configurable through device templates. Trap port, trap version, and enabling all traps cannot be configured through device templates and are set to their default values. This command can be deleted or disabled.
tacacs-server host	Allow configuration of up to three TACACS server hosts and their attributes—that is, shared secret and timeout for every individual host. The remaining attributes are set to their default values. This command can be deleted or disabled.
logging	Set the system log configuration to specify local and remote logging and severity levels. This command can be deleted or disabled.

Table 3: MFC CLI Commands Supported Through Junos Space Configuration Templates (*continued*)

CLI Commands	Description
ram-cache cache-size-MB dict-size-MB small-buffers scale-factor <i>number</i> small-attribute size <i>number</i> count <i>number</i>	Configure RAM cache options. The small-attribute command can be deleted or disabled.
telnet-server enable	Enable telnet.
service snapshot mod-delivery enable service status mod-delivery include disk	Tune mod-delivery service–related parameters. Enable snapshot (core file) to be generated when the mod-delivery service crashes. Enable considering pre-read status before declaring the system status UP.
network connection concurrent session	Configure network layer parameters.
network connection origin failover use-dns-response	The network connection concurrent session command can be deleted or disabled.
name-resolver cache-timeout (auto random seconds)	This command is not needed if the Media Flow Controller CLI command is fixed to set “auto” as the default value.

- Related Documentation**
- [Media Flow Activate Overview on page 4](#)
 - *Quick Reference to Tasks in Media Flow Activate*

PART 2

Administration

- [Managing and Monitoring Media Flow Controllers with Media Flow Activate on page 19](#)

CHAPTER 2

Managing and Monitoring Media Flow Controllers with Media Flow Activate

- [Monitoring a Media Flow Controller Dashboard from MFA on page 19](#)
- [Launching the Media Flow Controller Secure Console from MFA on page 20](#)
- [Upgrading or Rolling Back the Media Flow Controller Software Image on page 22](#)
- [Restoring Media Flow Controller Device Configuration on page 24](#)
- [Replicating Media Flow Controller Device Configuration on page 26](#)
- [Restarting Media Flow Controller Devices or Services on page 27](#)
- [Tagging Media Flow Controller Objects on page 28](#)
- [Provisioning Resource Pools to MFC Devices on page 29](#)
- [Managing Resource Pool Associations on page 30](#)
- [Actions on Resource Pools on page 32](#)
- [Fault Monitoring with SNMP on page 33](#)
- [Audit Logs Workspace Overview on page 39](#)
- [Job Management Workspace Overview on page 42](#)

Monitoring a Media Flow Controller Dashboard from MFA

- Purpose** Media Flow Activate allows you to view the **Dashboard** for any selected Media Flow Controller.
- Action** From the Manage MFCs page, select a device. On the **Actions** list, select **Launch Dashboard**. The Login page for the selected Media Flow Controller is displayed. Log in to see the Dashboard page of the Management Console for that Media Flow Controller.
- Meaning** The Dashboard provides usage information for the system.
- Statistics**
- **Cumulative since**—Time this Media Flow Controller has been running without reboot or shutdown
 - **GB delivered**—Total byte count of all objects that Media Flow Controller has delivered since running

- **Cache hit ratio**—Number of objects that Media Flow Controller has served from the RAM or disk divided by the total number of objects served; this includes the following parameters:
 - **Bandwidth**—Total number of bytes delivered from the RAM or disk divided by the total number of bytes delivered
 - **Number of Requests**—Total number of objects delivered from the RAM or disk divided by the total number of objects delivered (irrespective of their size)
- **Objects Delivered**—Total number of objects served by this Media Flow Controller since running

Graphs

- **Open Connections**—Media Flow Controller connections to the client, both HTTP and RTSP, and origin manager connections (om-session)
- **Weekly Bandwidth Savings**—Saved bandwidth—that is, bandwidth used by traffic that did not come from the origin server
- **Cache Throughput**—Bandwidth and place from which data was served
- **Cache Tier Throughput**—Green indicates that data is served from cache; yellow indicates that data is promoted from cache; red indicates that data is evicted from cache



NOTE: See the *Juniper Networks Media Flow Controller Administrators Guide* for detailed information about the Media Flow Controller dashboard.

Related Documentation

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- [Quick Reference to Tasks in Media Flow Activate](#)

Launching the Media Flow Controller Secure Console from MFA

You can use the **Launch Secure Console** feature in Media Flow Activate to open an SSH session to connect to a previously discovered Media Flow Controller. After you connect to a device, a terminal window is opened for that SSH connection in which you can enter CLI commands to monitor or troubleshoot the device.

Because this feature initiates the SSH session from the Junos Space server (rather than from your browser), it provides a secure and reliable connection to Media Flow Controller. You can establish separate SSH connections to one or more Media Flow Controllers simultaneously. A separate window is spawned for each SSH connection. However, only one SSH session per Media Flow Controller can be established at a time.

To open an SSH connection to Media Flow Controller, the following conditions must be met:

- Media Flow Controller should have been previously discovered in Media Flow Activate. That is, you can establish SSH connections only to those Media Flow Controllers that are displayed in Media Flow Activate.
- SSH v2 is enabled on Media Flow Controller.
- The status of Media Flow Controller is “UP.”
- A valid username and password have been configured on the Media Flow Controller.
- The **terminal type** parameter is set to **console**, **dumb**, or **ansi**. If **terminal type** is set to **ansi**, make sure that the **Terminal length** parameter is set to a value of **999**.

You can set the **terminal type** by running the following commands (make sure that you perform this task before running any other CLI commands on the SSH console):

- a. After you log in to Media Flow Controller, type **enable**.

The following is displayed: **Media Flow Controller host name #**

- b. Type **configure terminal**.

The following is displayed: **Media Flow Controller host name (config) #**

- c. Type **terminal type console** to set up the **terminal type**.



TIP: By default, if you are inactive, you are automatically logged out of the SSH console after five minutes. To prevent this automatic log out due to inactivity, select **Platform > Administration > Manage Applications > (Choose) Network Application Platform > (action) Modify Application Settings > (link) User > Automatic logout after inactivity** and set the value to 30 minutes.

To launch the secure console of Media Flow Controller:

1. From the left navigation panel, click the plus sign (+) adjacent to **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. Select Media Flow Controller.
3. On the **Actions** list, select **Launch Secure Console**. The **SSH to Device** page is displayed.
The **IP** field displays the IP address of the selected Media Flow Controller and is typically unavailable.
4. In the **Username** and **Password** fields, enter the administrator login credentials of the selected Media Flow Controller. The name and password must match the name and password configured on Media Flow Controller.
5. Click **Connect** to establish an SSH session with the selected Media Flow Controller. A terminal window opens in a non-modal pop-up with an SSH connection opened on the selected Media Flow Controller.



NOTE: You might encounter the error messages “Unable to Connect,” “Authentication Error,” or “Connection Lost or Terminated,” which are displayed as standard text in the terminal window. When an error occurs, all other functionality in the terminal window is stopped. If you encounter such an error, close the terminal window and open a new SSH session.

6. From the terminal window prompt, enter CLI commands to monitor or troubleshoot the device.



NOTE: See the “Secure Console” section of the *Junos Space Network Application Platform User Guide* for detailed information about this feature. For more information about the Media Flow Controller CLI commands, see the *Media Flow Controller CLI Command Reference Guide*.

Related Documentation

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- [Quick Reference to Tasks in Media Flow Activate](#)

Upgrading or Rolling Back the Media Flow Controller Software Image

Using Media Flow Activate, you can upgrade or roll back the software running on Media Flow Controllers. Both these operations interrupt the content delivery services and therefore require the network operations center (NOC) operators to gracefully take the Media Flow Controllers “out of service” for maintenance before performing an upgrade or a rollback.

Typically, a fresh Media Flow Controller containing two partitions has the same version of the software image installed on both partitions (that is, in active and standby partitions). To perform an upgrade, you can download the latest software image in the standby partition and start Media Flow Controller with this software image. However, if you find that the upgraded image is unstable or for some other reason you want to revert to the previous running image, Media Flow Activate provides the capability to roll back to the previous software image and configuration that was in use before it was upgraded. This image and the corresponding configuration are available in the standby partition.



NOTE:

Before you begin an upgrade or a rollback:

- Ensure that you have the URL of the software upgrade image when you want to perform an upgrade.
- The Connection Status of the Media Flow Controllers is up.

To perform a software upgrade on selected Media Flow Controllers by using Media Flow Activate:

1. From the left navigation panel, click **Media Flow Devices**.
2. Select the Media Flow Controllers and click **Software Image Management**.
3. In the **Download & Install** field, enter the URL of the image to be downloaded (a newer version of the image from what is currently running in Media Flow Controllers). You can select one of the following protocols for the download: **HTTP, HTTPS, SCP, FTP, SFTP, and TFTP**.
4. Click **Ok**. A pop-up is displayed with a status message, “**Please click on Job Id to view details,**” and the job ID. Click the job ID to check whether the Media Flow Controllers have successfully downloaded and copied the image to their standby partitions.
5. Select the Media Flow Controllers to which you have downloaded the new image and click **Software Image Management**.
6. Click **Boot standby image** to reboot Media Flow Controllers with the new image.
7. Click **Ok**. Media Flow Controllers reboot with the image in the standby partition. A pop-up is displayed with a status message, “**Please click on Job Id to view details,**” and the job ID. Click the job ID to check whether the upgrade was successful. If the upgrade was a failure, then Media Flow Controller automatically reboots with the image that was running previously. In this case, you may have to retry upgrading the Media Flow Controllers.

If the upgrade is successful, the partition with the upgraded image becomes the active partition, whereas the other partition with the previous image becomes the standby partition. After you verify that the upgrade has been successful, make sure that you put the Media Flow Controllers back into service. The upgrade preserves the current saved configurations.

To roll back to the software image version from which it was upgraded, you can select the Media Flow Controllers and click **Boot standby image**. Media Flow Controller reboots with the image in the standby partition. A pop-up is displayed with a status message, “**Please click on Job Id to view details,**” and the job ID. Click the job ID to check whether the rollback was successful.



NOTE: When you initiate an upgrade or a rollback on multiple Media Flow Controllers, the job that is created comprises several subjobs; each subjob represents the user-initiated action for a single Media Flow Controller. From the Job Management workspace, select the main job to view details about the subjobs, such as whether they were successful or not.

Related Documentation

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- [Quick Reference to Tasks in Media Flow Activate](#)

Restoring Media Flow Controller Device Configuration

You can restore configurations within Media Flow Controller when it has experienced a hardware failure (such as a root disk crash) resulting in the loss of configuration data stored on the device. After the hardware is restored, either by replacing the FRU or the entire server, you can use Media Flow Activate to rapidly restore the services delivered by that device.

This section describes the process of restoring the device configuration of Media Flow Controller after a complete (non-recoverable) failure or corruption of the Media Flow Controller configuration file.



NOTE: Restore the device configuration only after you have restored the Media Flow Controller platform configuration (infrastructure-level configuration) by using the configuration templates stored in Media Flow Activate or manually.

The Media Flow Activate GUI provides you with the following options:

- **Restore service(s)**—This action restores the service configurations on the selected devices.

Media Flow Activate maintains a configuration database, which serves as the source of reference for configuration-related information. So, when you choose to restore the configuration of a device, Media Flow Activate restores the configuration from this database rather than from the device itself.

- **Remove all services**—This action removes the service configurations from the selected devices. Note that this action does not set the devices to the factory default configuration. It only wipes out or resets the existing service-specific configuration.

To restore or remove the device configuration:

1. Click **Media Flow Devices**.
2. Select the Media Flow Controllers whose configuration must be restored or removed.
3. From the **Actions** list, select either **Restore service(s)** to restore the services or **Remove all services** to remove the services from the Media Flow Controllers. A new job is created and a message with the job ID is displayed. Click the job ID to know whether the action is a success or a failure.

If the job is successful, then the following configurations are restored or removed:

- Content Ingest services
- HTTP Reverse Proxy services
- Network Optimization services
- Access log profiles

- Cache-tuning policies
- Policy scripts
- Origin maps
- Resource pools
- Virtual players

Usually, the following configurations are not restored or removed:

- Interface configuration
- Device configuration
- BGP configuration
- Space configuration templates

Example Workflow for Restoring Device Configuration

Consider that you want to restore the device configuration of Media Flow Controller, MFC-A. Perform the following steps to restore the device configuration:

1. Delete all the existing service-specific configurations by clicking **Remove all services** so that there are no conflicts while restoring the configuration of MFC-A.
2. Use Junos Space configuration templates to restore the platform-level configuration of MFC-A. In addition, manually restore the BGP, device, and interface configuration of MFC-A by using the UI.
3. Click **Restore service(s)** to restore the service configuration of MFC-A with the configuration stored in the Media Flow Activate database.

Related Documentation

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- *Quick Reference to Tasks in Media Flow Activate*

Replicating Media Flow Controller Device Configuration

From Media Flow Activate, you can replicate or clone the device configuration from one Media Flow Controller to several Media Flow Controllers. This operation is useful when new Media Flow Controllers are added to the network to expand capacity or replace a failed device. You can quickly replicate standard configuration templates on the new devices.



NOTE: Replicate the device configuration only after you have replicated the Media Flow Controller platform configuration (infrastructure-level configuration) by using the configuration templates stored in Media Flow Activate or manually.

To replicate a device configuration:

1. Click **Media Flow Devices**.
2. Select the Media Flow Controller whose configuration must be replicated.
3. On the **Actions** list, select **Replicate Device**.
4. Select the Media Flow Controllers on which the device configuration must be replicated.
5. Click **Replicate**. A new job is created and a message with the job ID is displayed. You can click the job ID to know whether the replication job is a success or a failure. If the new device contains any previous resource pool configuration, then this action fails. This prevents any accidental overwrites.

Media Flow Activate maintains a configuration database, which serves as the source of reference for configuration-related information. So, when you choose to replicate the configuration of a device, Media Flow Activate replicates the configuration from this database rather than from the device itself.

If the job is successful, then the following configurations are replicated in the selected Media Flow Controllers:

- Content Ingest services
- HTTP Reverse Proxy services
- Network Optimization services
- Access log profiles
- Cache-tuning policies
- Policy scripts
- Origin maps
- Resource pools (both global and user-defined resource pool configurations)
- Virtual players

Usually, the following configurations are not replicated because they are unique to a device:

- Interface configuration
- Device configuration
- BGP configuration
- Space configuration templates—In this case, the Template feature provides the facility to set device-specific values and hence there is no need of replication.

If the purpose of replication is to replace the servers with a higher-performance server, then after the new server is put in service, one or more of the existing servers that were cloned or replicated can be removed from service.

**Related
Documentation**

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- *Quick Reference to Tasks in Media Flow Activate*

Restarting Media Flow Controller Devices or Services

You can restart selected Media Flow Controller devices or the delivery services on them by using Media Flow Activate.

Restarting a Media Flow Controller brings down all services; restarting services on a Media Flow Controller stops media delivery services.

To restart selected Media Flow Controllers by using Media Flow Activate:

1. From the left navigation panel, click the plus sign (+) adjacent to **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. Select the discovered devices that you want to restart.
3. On the **Actions** list, select **Restart Device(s)**. The **Restart Device(s)** configuration page is displayed.
4. Click **Yes** to proceed with the restart and close the window. Click **No** to cancel the restart and close the window. The selected Media Flow Controllers are restarted; there is no progress bar or completion message, but the status on the Manage MFCs page changes.

To restart services on selected Media Flow Controllers by using Media Flow Activate:

1. From the left navigation panel, click the plus sign (+) adjacent to **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. Select the discovered devices on which you want to restart a service.
3. On the **Actions** list, select **Restart Service** from the list of available actions. The **Restart Service** configuration page is displayed.

4. Select the **Delivery Service** and **Content Ingest Service** options as needed and click **Restart**.
5. Click **Yes** to proceed with the restart and close the window. Click **No** to cancel the restart and close the window. A job is created. You can view the status of the job in the **Job Management** workspace.



NOTE: See the *Juniper Networks Media Flow Controller Administrators Guide* for detailed information about restarting services and devices.

Related Documentation

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- *Quick Reference to Tasks in Media Flow Activate*

Tagging Media Flow Controller Objects

Tagging allows you to label and categorize objects from an application workspace manage inventory landing page. Subsequently, you can view and use these tags to easily search for multiple objects to view their status or perform a bulk action on them without having to select each object individually.

To tag objects, you navigate to the application workspace manage inventory landing page (such as Media Flow Devices, Service Design), select the objects that are to be tagged, and select **Tag** on the **Actions** list.



TIP: When you specify the tag name, make sure that it does not start with a space; contain a comma, double quotation marks, or parentheses; or exceed 255 characters.

The tags that you create are private and hence are visible only to you. However, to share the tags with other users, you need the “Tag Administrator” privileges.

For detailed instructions about tagging an object, refer to the “Tagging an Object” section in the *Junos Space Network Application Platform User Guide*.

After you tag the object, you can perform the following actions:

- **Filtering inventory using tags**—To perform an operation on multiple objects, tag the objects with an identical tag name and later filter them using the specific tag. After all the objects are listed, you can perform the permitted actions from the **Actions** list after selecting them.

To filter Media Flow Controller objects by using a tag:

1. On the workspace inventory page, from the **Search** list (usually located at the upper-right corner of the page), select **Tags**.

2. From the adjacent list, select the tag name. Alternatively, in the list, you can type the first letter of the tag to narrow down the list.

The inventory page displays only the objects that are tagged with the selected tag.

- Viewing tags—The **View Tags** action from application workspace inventory pages allows you to see all the tags that you have assigned to a managed object. You must first tag a managed object to see its tags. The tags that are displayed are those that are created by you (private tags) and those that are shared (public tags).

To view the tags assigned to an inventory object, navigate to the application workspace manage inventory landing page, select the object, and select **View Tags** on the **Actions** list.

For detailed instructions about viewing the tags associated with a managed object, refer to the “Viewing Tags” section in the *Junos Space Network Application Platform User Guide*.

- Untagging an object—You can untag or remove a tag from an object on a workspace inventory page. You can select only one object at a time to untag.

To untag an object, navigate to the application workspace manage inventory landing page, select the object, and select **Untag** on the **Actions** list. From the dialog box, select the tags to untag.

Related Documentation

- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- *Quick Reference to Tasks in Media Flow Activate*

Provisioning Resource Pools to MFC Devices

After creating a resource pool, you have to provision it on Media Flow Controller devices to ensure that the configured resources are reserved for that pool from the available system resources.

1. From the left navigation panel, click the plus sign (+) adjacent to **Media Flow Devices**.
2. Click **Manage Resource Pools**. The Manage Resource Pools page is displayed.
3. Select the resource pools.
4. On the **Actions** list, select **Provision Resource Pool**. The **Provision Resource Pool to Device** dialog box appears.

This dialog box displays all the available devices (**Device Name** column) to which you can provision the resource pool, including their IP addresses (**IP Address** column), whether they are up (**Connections Status** column), and the list of pools (**Current Resource Pool List** column) that have been previously provisioned on the device.

It is recommended that you provision the resource pools on those devices that are up. When a device is down, the provisioning may not be a success.

Additionally, click **View** under the **Current Resource Pool List** column to view the list of pools that were previously provisioned on a specific device before provisioning additional pools to the device.



CAUTION: While provisioning, make sure that the resources allocated to a resource pool do not exceed the available system resources.

5. Select the devices to which you want to provision the resource pools.

Use the **Search** option to display specific Media Flow Controllers by filtering using their names or tags.

6. Click **Next**. The selected pools and the selected devices are displayed. If you want to make any modification to this list, click **Previous** and make changes, as needed.
7. Click **Provision**. The **Job Information** dialog box appears with a job ID.
8. Click the job ID to check whether the provisioning job was successful or click **OK** to exit.

If the job is not successful, the possible causes could be one of the following:

- Devices were not up.
- Resource pool allocation exceeded the available system resources (global pool) for a certain device.

Related Documentation

- [Managing Resource Pool Associations on page 30](#)
- [Provisioning Services](#)
- [Actions on Resource Pools on page 32](#)
- [Creating Resource Pools on page 55](#)
- [Resource Pools Overview on page 9](#)
- [Media Flow Activate Overview on page 4](#)
- [Quick Reference to Tasks in Media Flow Activate](#)

Managing Resource Pool Associations

You can view the association of the resource pools to Media Flow Controller servers to which they have been provisioned and take suitable actions, such as reprovisioning them if the earlier provisioning had failed.

From the **Manage Resource Pool Associations** page, you can:

- Reprovision the resource pools

Typically, you reprovision the resource pools when you have made changes to the existing configuration and want the new configuration to take effect or if the previous provisioning had failed.

- Delete the resource pools

Typically, you delete the resource pools when they are no longer used or needed. This action causes the resources allocated to the resource pools to be automatically returned to the global resource pool.



CAUTION: If a reverse proxy service has been successfully provisioned to a resource pool, deprovision the service before deleting the resource pool.

To perform these actions:

1. From the **Manage Resource Pools** page, select the resource pool.
2. On the **Actions** list, select **Manage Resource Pool Associations**. The **Manage Resource Pool Associations** dialog box appears.

This dialog box lists the devices on which the resource pool was provisioned and indicates whether the provisioning was successful. Use the **Search** option to display specific Media Flow Controllers by filtering using their names or tags.



TIP: Provisioning a resource pool to a device is successful only when the device is “In Sync” status. Verify the device status in the **Managed Status** column before provisioning.

3. Select the device and perform one of the following tasks:

- Click **Provision Again** to reprovision the resource pools.

The **Job Information** dialog box appears. Click the job ID to view the job's status or click **Ok** to exit.

- Click **De-provision** to deprovision the resource pools. You are prompted for a confirmation. Click **Yes** to deprovision the resource pools or **No** to exit.



CAUTION: If a reverse proxy service has been successfully provisioned to a resource pool, deprovision the service before deleting the resource pool.

- Click **Cancel** to exit.

Related Documentation

- [Provisioning Services](#)
- [Provisioning Resource Pools to MFC Devices on page 29](#)
- [Actions on Resource Pools on page 32](#)
- [Creating Resource Pools on page 55](#)
- [Resource Pools Overview on page 9](#)
- [Media Flow Activate Overview on page 4](#)

- *Quick Reference to Tasks in Media Flow Activate*

Actions on Resource Pools

From the **Manage Resource Pools** page, you can perform the following actions on resource pools by clicking the links on the **Actions** list. You have to select the resource pools before performing any actions on them:

- **Modify Resource Pool**—Other than the resource pool name, you can modify all the configuration settings, such as the maximum bandwidth that you want to allocate to the resource pool, the maximum concurrent sessions that it can support, and the description.

You can modify only one resource pool at a time.

- **Delete Resource Pool(s)**—Delete one or more resource pools.

If the resource pool is provisioned to a device, deprovision the resource pool before deleting it.

- **Provision Resource Pool**—Provision the resource pools on Media Flow Controller servers. See [“Provisioning Resource Pools to MFC Devices” on page 29](#) for more information about provisioning the resource pools.

- **Manage Resource Pool Associations**—View the association of a resource pool to the Media Flow Controller servers to which it has been provisioned. You can reprovision the resource pool or deprovision it from Media Flow Controller servers depending on the actions that you choose to perform. See [“Managing Resource Pool Associations” on page 30](#) for more information about managing the resource pools associated with Media Flow Controllers.

You can manage only one resource pool at a time.

- **Tag It**—Tag the resource pools.
- **View Tags**—View the tags associated with a specific resource pool.
- **Untag It**—Untag the selected tags from the specific resource pool.

For more information about tagging, see [“Tagging Media Flow Controller Objects” on page 28](#).

Related Documentation

- [Provisioning Resource Pools to MFC Devices on page 29](#)
- [Managing Resource Pool Associations on page 30](#)
- [Provisioning Services](#)
- [Creating Resource Pools on page 55](#)
- [Resource Pools Overview on page 9](#)
- [Media Flow Activate Overview on page 4](#)

Fault Monitoring with SNMP

To provide network monitoring capabilities, Junos Space Network Application Platform is integrated with a third-party tool called OpenNMS. The OpenNMS network management application platform provides solutions for enterprises and carriers. Junos Space Network Application Platform on which OpenNMS is installed exposes some functionality of OpenNMS through the Network Monitoring workspace. The default performance management configuration of OpenNMS for Media Flow Activate enables you to quickly view basic device statistics, such as device availability and interface availability for the entire Media Flow Network through the OpenNMS dashboard landing page. As a Media Flow Network administrator or Data Center administrator, you can monitor the performance statistics of individual Media Flow Controller devices as well as networkwide aggregated statistics using the OpenNMS dashboard. You can also configure OpenNMS to display critical events, such as delivery outages, on the same dashboard.

For more information about OpenNMS configuration-related information, see the “Network Monitoring” section in the *Junos Space Network Application Platform User Guide*.



CAUTION: Although you can access additional OpenNMS functionality by customizing its XML files, editing these files can affect the functionality of the Network Monitoring workspace. Juniper Networks does not support changes to OpenNMS.

In order to facilitate fault monitoring from the **Network Monitoring** workspace:

- When Media Flow Controllers are discovered from the Junos Space GUI, they are automatically added to the list of monitored devices or nodes on OpenNMS.
- All the basic monitoring capabilities, such as the ICMP ping for device outage, interface availability, and service outages, are supported for Media Flow Controllers.
- Media Flow Controllers are configured to send traps or notifications to OpenNMS when significant events occur on the Media Flow Controller devices. The list of Media Flow Controller events that can be tracked from the OpenNMS dashboard are listed in [Table 4 on page 35](#) and [Table 5 on page 37](#).

Before you start monitoring the Media Flow Controller, make sure that the SNMP server host IP address of the Media Flow Controller is set to the Junos Space server IP address. You can use the Junos Space device template feature to provision this configuration to multiple Media Flow Controllers (**Device Templates > Create Definition > Media Flow > Configuration > Services > Mfc cluster > System > Monitoring > Snmp server > Host > Ip address**).

For more information about all the operations that you can perform from the **Network Monitoring** workspace, see the “Network Monitoring UI” section in the *Junos Space Network Application Platform User Guide*. The following list of actions should help you get started:

- Select **Node List** and click one of the displayed nodes to view:

- General status of the node
- Recent events that occurred in the node
- Recent outages that occurred in the node
- Notifications
- SNMP attributes
- Availability of the interfaces



TIP: If you have recently modified the host name of a Media Flow Controller, it is possible that this node may not be displayed in the nodes list. Resynchronize the nodes to update this list. Select **Network Monitoring > Node List > Resync Nodes > Confirm** to complete this task.

- Select **Search** to search for a specific node.
- Select **Dashboard** to open the OpenNMS dashboard.
- Select **Events** to view the events that occurred within the network. From the **Events** page that is displayed, select **View all events** to view all the events. In the tabular view, click the **Severity**, **Node**, or **Time** column heading to sort the data in ascending or descending order. For more information about these events, see the “Events” section in the *Junos Space Network Application Platform User Guide*.



NOTE: Every change in the network can be considered an event. An event is raised in OpenNMS as a result of receiving an SNMP Trap from a Media Flow Controller device. If you do not receive an event that occurred in any of the Media Flow Controller device that you are monitoring, make sure that the corresponding SNMP trap is enabled through the Media Flow Controller CLI command (mentioned at the end of this topic).

- Select **Alarms** to view significant events that occurred on the network. From the **Alarms** page that is displayed, select **All alarms (summary)** or **All alarms (detail)** to view the shorter or detailed version of all the alarms. For more information about alarms, see the “Alarms” section in the *Junos Space Network Application Platform User Guide*.

From Media Flow Activate, you can view the alarms that are specific to each Media Flow Controller from the **Media Flow Devices** inventory landing page:

1. Click **Media Flow Devices** to view the list of Media Flow Controllers.
2. Select the Media Flow Controller whose alarms you want to view.
3. From the **Actions** list, select **View Service Alarms**. The alarms that are specific to the device are displayed.

Table 4 on page 35 lists the SNMP alarm events of severity levels—critical, major, and minor (in that order), which are displayed on the OpenNMS dashboard. To view the

corresponding clear alarm events (alarms that indicate that the system has recovered from events of higher severity levels), see [Table 5 on page 37](#).

Table 4: SNMP Alarm Events

SNMP Event or Trap (Alarm Event)	Severity Level	Description	Log Message
jmfcFanFailure	Critical	The system fan has stopped functioning.	jmfcFanFailure trap received
jmfcPowerSupplyFailure	Critical	The system power supply has failed.	jmfcPowerSupplyFailure trap received
jmfcSmartError	Critical	SMART has sent an event about a possible disk error.	jmfcSmartError trap received
jmfcUnexpectedShutdown	Critical	The system has shut down unexpectedly.	jmfcUnexpectedShutdown trap received
jmfcServiceCrash	Major	One of the monitored services is down due to a crash.	jmfcServiceCrash trap received jmfcServiceName= <i>name</i>
jmfcCpuUtilHigh	Major	The aggregate CPU utilization across all CPUs is high.	jmfcCpuUtilHigh trap received jmfcCpuUtil=%parm[#1]% jmfcCpuUtilErrThreshold=%parm[#2]%;
jmfcDiskSpaceLow	Major	Free disk space is low.	jmfcDiskSpaceLow trap received jmfcDiskName=%parm[#1]% jmfcDiskFreeSpace=%parm[#2]% jmfcDiskSpaceErrThreshold=%parm[#3]
jmfcOriginNodeDown	Major	One of the nodes in the cluster is down.	jmfcOriginNodeDown trap received
jmfcApplCpuUtilHigh	Major	CPU utilization of core HTTP Engine is high.	jmfcApplCpuUtilHigh trap received jmfcAppMaxCpuUtil=%parm[#1]% jmfcAppMaxCpuUtilErrThreshold=%parm[#2]%
jmfcServiceExit	Major	One of the services managed by Process Manager has exited unexpectedly, but has not left a core file.	jmfcServiceExit trap received jmfcServiceName=%parm[#1]%
jmfcServiceLivenessFailure	Major	Process Manager has detected that a process has hung and is set to restart.	jmfcServiceLivenessFailure trap received jmfcServiceName=%parm[#1]%
jmfcCacheHitRatioLow	Minor	Cache hit ratio is low.	jmfcCacheHitRatioLow trap received jmfcCacheHitRatio=%parm[#1]% jmfcCacheHitRatioErrThreshold=%parm[#2]%

Table 4: SNMP Alarm Events (*continued*)

SNMP Event or Trap (Alarm Event)	Severity Level	Description	Log Message
jmfcMemUtilizationHigh	Minor	Memory utilization on the system is high.	jmfcMemUtilizationHigh trap received jmfcMemUtil=%parm[#1]% jmfcMemUtilErrThreshold=%parm[#2]%
jmfcNetUtilizationHigh	Minor	Network utilization on the system is high.	jmfcNetUtilizationHigh trap received jmfcNetIntfUtilCurrent=%parm[#1]% jmfcNetIntfUtilErrThreshold=%parm[#2]%
jmfcDiskIOHigh	Minor	Disk I/O on the system is high.	jmfcDiskIOHigh trap received jmfcDiskName=%parm[#1]% jmfcDiskORate=%parm[#2]% jmfcDiskORateErrThreshold=%parm[#3]%
jmfcCacheBandwidthUsageHigh	Minor	The cache bandwidth usage is high.	jmfcCacheBandwidthUsageHigh trap received jmfcCacheBw=%parm[#1]% jmfcCacheBwErrThreshold=%parm[#2]%s
jmfcOriginBandwidthUsageHigh	Minor	The origin bandwidth usage is high.	jmfcOriginBandwidthUsageHigh trap received jmfcOriginBw=%parm[#1]% jmfcOriginBwErrThreshold=%parm[#2]%
jmfcDiskBandwidthUsageHigh	Minor	The disk bandwidth usage is high.	jmfcDiskBandwidthUsageHigh trap received. jmfcDiskName=%parm[#1]% jmfcDiskBW=%parm[#2]% jmfcDiskBWErrThreshold=%parm[#3]%
jmfcConnectionRateHigh	Minor	The connection rate is high.	jmfcConnectionRateHigh trap received jmfcConnectionRateCurrent=%parm[#1]% jmfcConnectionRateErrThreshold=%parm[#2]%
jmfcTransactionRateHigh	Minor	The HTTP transaction rate is high.	jmfcTransactionRateHigh trap received jmfcTransactionRateCurrent=%parm[#1]% jmfcTransactionRateErrThreshold=%parm[#2]%
jmfcPagingHigh	Minor	The paging activity is high.	jmfcPagingHigh trap received jmfcPagingCurrent=%parm[#1]% jmfcPagingErrThreshold=%parm[#2]%
jmfcResourcePoolUsageHigh	Minor	The usage of a resource pool has exceeded its defined upper limit.	jmfcResourcePoolUsageHigh trap received jmfcResourcePoolName=%parm[#1]% jmfcResourcePoolBandwidth=%parm[#2]% jmfcResourcePoolActiveConns=%parm[#3]%
jmfcResourcePoolUsageLow	Minor	The usage of a resource pool has fallen lower than its defined lower limit.	jmfcResourcePoolUsageLow trap received jmfcResourcePoolName=%parm[#1]% jmfcResourcePoolBandwidth=%parm[#2]% jmfcResourcePoolActiveConns=%parm[#3]%

Table 5 on page 37 lists the alarm events that indicate that the system has recovered from events of higher severity levels.

Table 5: SNMP Clear Alarm Events

SNMP Event or Trap (Clear Alarm Event)	Severity Level	Description	Log Message
jmfcServiceUp	Cleared	One of the monitored services is restarted.	jmfcServiceUp trap received, Clearing Service Crash Alarm. jmfcServiceName= <i>name</i>
jmfcFanStatusOK	Cleared	The fan status is okay.	jmfcFanStatusOK trap received, Clearing Fan Failure Alarm.
jmfcPowerSupplyOk	Cleared	The system power supply is restored.	jmfcPowerSupplyOk trap received, Clearing Power Supply Alarm.
jmfcCacheHitRatioOk	Cleared	Cache hit ratio is normal.	jmfcCacheHitRatioOk trap received, Clearing Cache Hit Ratio Low Alarm. jmfcCacheHitRatio=%parm[#1]% jmfcCacheHitRatioClrThreshold=%parm[#2]%
jmfcCpuUtilOk	Cleared	The aggregate CPU utilization across all CPUs has fallen back to normal.	jmfcCpuUtilOk trap received, Clearing CPU Utilization High Alarm. jmfcCpuUtil=%parm[#1]% jmfcCpuUtilClrThreshold=%parm[#2]%
jmfcDiskSpaceOk	Cleared	Free disk space is normal.	jmfcDiskSpaceOk trap received, Clearing Disk Space Alarm. jmfcDiskName=%parm[#1]% jmfcDiskFreeSpace=%parm[#2]% jmfcDiskSpaceClrThreshold=%parm[#3]%
jmfcMemUtilizationOk	Cleared	Memory utilization on the system has come down to the normal level.	jmfcMemUtilizationOk trap received, Clearing High Memory Utilization Alarm. jmfcMemUtil=%parm[#1]% jmfcMemUtilClrThreshold=%parm[#2]%
jmfcNetUtilizationOk	Cleared	Network utilization on the system has come down to the normal level.	jmfcNetUtilizationOk trap received, Clearing Net Utilization High Alarm. jmfcNetIntfUtilCurrent=%parm[#1]% jmfcNetIntfUtilClrThreshold=%parm[#2]%
jmfcDiskIOOk	Cleared	Disk I/O on the system has come down to the normal level.	jmfcDiskIOOk trap received, Clearing Disk IO High Alarm. jmfcDiskName=%parm[#1]% jmfcDiskIORate=%parm[#2]% jmfcDiskIORateClrThreshold=%parm[#3]%
jmfcOriginNodeUp	Cleared	One of the failed nodes in the cluster is up, clearing Origin Node Down Alarm.	jmfcOriginNodeUp trap received
jmfcApplCpuUtilOk	Cleared	CPU utilization of core HTTP Engine has fallen back to normal.	jmfcApplCpuUtilOk trap received, Clearing App. Utilization High Alarm. jmfcAppMaxCpuUtil=%parm[#1]% jmfcAppMaxCpuUtilClrThreshold=%parm[#2]%
jmfcCacheBandwidthUsageOk	Cleared	The cache bandwidth usage has come down within normal limits.	jmfcCacheBandwidthUsageOk trap received, Clearing Cache Bandwidth Usage High Alarm. jmfcCacheBw=%parm[#1]% jmfcCacheBwClrThreshold=%parm[#2]%

Table 5: SNMP Clear Alarm Events (*continued*)

SNMP Event or Trap (Clear Alarm Event)	Severity Level	Description	Log Message
<code>jmfcOriginBandwidthUsageOk</code>	Cleared	The origin bandwidth usage has come down within normal limits.	<code>jmfcOriginBandwidthUsageOk</code> trap received, Clearing Origin Bandwidth Usage High Alarm. <code>jmfcOriginBw=%parm[#1]%</code> <code>jmfcOriginBwClrThreshold=%parm[#2]%</code>
<code>jmfcDiskBandwidthUsageOk</code>	Cleared	The disk bandwidth usage has come down within normal limits.	<code>jmfcDiskBandwidthUsageOk</code> trap received, Clearing Disk Bandwidth Usage High Alarm. <code>jmfcDiskName=%parm[#1]%</code> <code>jmfcDiskBW=%parm[#2]%</code> <code>jmfcDiskBWClrThreshold=%parm[#3]%</code>
<code>jmfcConnectionRateOk</code>	Cleared	The connection rate has come down within normal limits.	<code>jmfcConnectionRateOk</code> trap received, Clearing Connection Rate High Alarm. <code>jmfcConnectionRateCurrent=%parm[#1]%</code> <code>jmfcConnectionRateClrThreshold=%parm[#2]%</code>
<code>jmfcTransactionRateOk</code>	Cleared	The HTTP transaction rate has come down within normal limits.	<code>jmfcTransactionRateOk</code> trap received, Clearing Transaction Rate High Alarm. <code>jmfcTransactionRateCurrent=%parm[#1]%</code> <code>jmfcTransactionRateClrThreshold=%parm[#2]%</code>
<code>jmfcPagingOk</code>	Cleared	The paging activity has come down to normal level.	<code>jmfcPagingOk</code> trap received, Clearing Paging High Alarm. <code>jmfcPagingCurrent=%parm[#1]%</code> <code>jmfcPagingClrThreshold=%parm[#2]%</code>
<code>jmfcResourcePoolHighUsageOK</code>	Cleared	The usage of a resource pool has fallen back to its normal limit.	<code>jmfcResourcePoolHighUsageOK</code> trap received, Clearing Resource Pool usage High Alarm. <code>jmfcResourcePoolName=%parm[#1]%</code> <code>jmfcResourcePoolBandwidth=%parm[#2]%</code> <code>jmfcResourcePoolActiveConns=%parm[#3]%</code>
<code>jmfcResourcePoolLowUsageOK</code>	Cleared	The usage of a resource pool has come up to its normal limit.	<code>jmfcResourcePoolLowUsageOK</code> trap received, Clearing Resource Pool Usage Low Alarm. <code>jmfcResourcePoolName=%parm[#1]%</code> <code>jmfcResourcePoolBandwidth=%parm[#2]%</code> <code>jmfcResourcePoolActiveConns=%parm[#3]%</code>

You can execute the following commands to view and enable events and alarms in a Media Flow Controller device:

- **show snmp events *cr***—View the list of SNMP events that are enabled.
- **snmp-server traps event *event-name cr***—Enable a specific SNMP event.
- **show stats alarm *cr***—View the list of alarms that are enabled.
- **stats alarm *alarm-ID* [enable|clear|event-repeat|rate-limit|falling|rising]**—Enable a specific alarm.

Related Documentation

- [Media Flow Activate Overview on page 4](#)

- *Quick Reference to Tasks in Media Flow Activate*

Audit Logs Workspace Overview

From the Audit Logs workspace, with the Audit Log Administrator role, you can monitor tasks initiated by users from the Junos Space GUI. Any user-initiated task that is performed from the Media Flow Activate GUI is recorded in the Audit Log database with information about the user who initiated the task, the time of the request, the device that was used, a list of modifications or changes, and so on. The Audit Logs workspace displays this information in two views: graphical and tabular. In the graphical view, you can view data on a daily, weekly, or monthly basis. The tabular view displays audit log entries.

The following actions generate audit logs in Junos Space:

- User logins and logouts
- User timeouts
- Authentication failures
- Each operation attempted by a logged-in MFA GUI user

Non-user-initiated activities, such as device-driven activities, are not logged in the Audit Log database.

From this workspace, you can perform the following tasks:

- **Viewing audit log statistics**—You can use the following graphs to monitor user activity.
 - The **Audit Log Statistical Graph** pie chart displays all tasks that have been performed and logged in all Junos Space applications over a specific period of time. You can view Audit Log statistics by task type, user, workspace, and application.

You can control how data is displayed on the pie chart by selecting the category and time scale. The category determines what statistical log graph is displayed, whereas the time scale bar allows you to select the time period for which the log data is displayed. You can click a sector within the pie to drill down to audit log details. For more information about the audit log statistical graph, see the "Viewing the Dynamic Audit Log Statistical Graph" section in the *Junos Space Network Application Platform User Guide*. Following is a brief overview of the data that is displayed when you choose a category:

- **Task**—Shows all tasks within the selected time frame. You can click a task within the pie to view the users who performed this task or the IP addresses from which this task was performed. Click **Overview** to go back to the first-level chart—that is, to view all the tasks within the selected time frame.
- **User**—Shows all users using the system within the selected time frame. Click a user to view the tasks performed by that user. Click **Overview** to go back to the first-level chart.

- **Workspace**—Shows all workspaces used in the selected time frame
- **Application**—Shows all applications for which audit logs were logged within the selected time frame. Click **REST** to view the audit logs generated for Media Flow Activate—this is because, internally, all user-initiated tasks from the Media Flow Activate GUI invokes the corresponding REST APIs to complete the tasks. In the tabular display of log entries, the **Description** column provides details about the API that was invoked. For example, this column displays something like **POST: /api/juniper/mfa/definitions-management/rproxy-definitions/**.
- The **Top 10 Active Users in 24 hours** graph displays the top 10 Junos Space users who performed the most tasks over 24 hours. For more information about this graph, see the “Viewing Audit Log Statistics” section in the *Junos Space Network Application Platform User Guide*.
- **Viewing audit logs**—This workspace provides a tabular view of audit log entries, displaying the following information:
 - **User Name**—Login ID of the user
 - **User IP**—IP address of the machine from which the user logged in
 - **Task**—Name of the performed task
Examples: **Login, Logout, HTTP POST**, and so on
 - **Timestamp**—Time when the task is executed or when the job is scheduled
Example: **Oct 20, 2012 11:12:03 AM UTC+05:30**
 - **Result**—Result of the executed task
Examples: **Success, 200, 202**, and so on
 - **Description**—Simple description of the audit log
Examples:
 - **Login Succeeded**
 - **POST: /api/space/device-management/devices/262148/exec-rpc**
 - **Change request created successfully with Id : 295053**
 - **Job: POST: /api/juniper/mfa/device-management/mfdevices/rproxy/bulk-provision/**—Such log entries typically include a job ID, which you click to view details about the job.
 - **Job ID**—ID of the job being scheduled (If the task performed is a scheduled job, you can view the job details by clicking the Job ID link in the Audit Log table.)

On the **View Audit Logs** page, you can perform the following actions:

- Click the column headings to sort the data in ascending or descending order.
- Enter a search criterion in the textbox adjacent to the **Search** icon to filter the logs.

- Select an audit log entry and click the **Display Quick View** icon next to the **Actions** list to view the summary of the audit log entry, which includes the list of affected objects. If no objects are affected, then the summary view displays **None**.

For more information, see the “Viewing Audit Logs” section in the *Junos Space Network Application Platform User Guide*.

- **Archiving and purging jobs**—With the **Archive/Purge** feature, you can manage your Junos Space log volume, which enables you to archive log files and then purge those log files from the Junos Space database. For each **Archive/Purge** operation, the archived log files are saved in a single file, in CSV format. The audit logs can be saved to a local server or a remote network host. When you archive data to a local server, the archived log files are saved to the default directory, `/var/lib/mysql/archive`. To specify the remote archive location, use the IP address of the remote machine. The default filename of the archived file is `JunosSpaceAuditLog_yyyy-mm-dd_hh-mm-ss.csv.gz`, where `yyyy-mm-dd_hh-mm-ss` is the date and time up to when all the audit logs recorded are archived and purged from the database.



NOTE: The date and time in the archive filename may differ from your local client's time zone. This is because the Audit Logs workspace displays the Junos Space server time zone, whereas your local client may be located in a different time zone.

The archived file includes information such as:

- Timestamp
- UTC Time
- User IP
- Application
- Task
- Result
- Description
- Job ID
- Username

To view the local time instead of the UTC time in the archived audit log file, follow the instructions in the “Converting the Audit Log File UTC Timestamp to Local Time in Microsoft Excel” section in the *Junos Space Network Application Platform User Guide*.

For more information about archiving and purging audit logs, see the “Archiving and Purging Audit Logs” section in the *Junos Space Network Application Platform User Guide*.

- **Exporting audit logs**—The audit logs export feature enables you to download entire or partial audit logs in CSV format so that you can view the audit logs in a separate application or save them on another machine for future use, without purging them from the system. For more information about exporting audit logs, see the “Exporting Audit Logs” section in the *Junos Space Network Application Platform User Guide*.

From the Media Flow Activate GUI, select one of the following options:

- **Export all audit logs**—To export all audit logs
- **Export audit logs filtered by date range**—To export audit logs that are logged within the specified time frame
- **Export audit logs as displayed on View Audit Logs table**—(Default) On the View Audit Logs page, you can filter audit logs on the basis of multiple criteria. The criteria you choose determine which audit log data is exported.

The audit logs are exported as CSV files (for example, **AuditLogs_2012-10-25_11-14-56.csv**). They are not removed from the database after they are exported.

Troubleshooting and Additional Information About Audit Logs

Some troubleshooting tips and other sundry information for audit logs are as follows:

- If an action is not completed due to validation errors, the action is not logged in the audit log.
- If an action fails due to database errors, the action is logged in the audit log with a result of “Failure”.
- If an audit log fails to be recorded due to exceptions, the corresponding error logs and debug logs are created in the **server.log** file. In this case, search for error logs and debug logs under “AuditlogRecorderBean” class.
- Audit log archive and purge actions may fail due to insufficient server disk space or due to errors in performing scp to remote server. The error details can be viewed from the Job Management workspace for the specific archive and purge jobs.
- In case of scp errors, the archived file is still created in the **/var/lib/mysql/archive** subdirectory in the Junos Space server.

Related Documentation

- [Media Flow Activate Overview on page 4](#)
- [Job Management Workspace Overview on page 42](#)
- *Quick Reference to Tasks in Media Flow Activate*

Job Management Workspace Overview

With the Job Management workspace, you can monitor the status of all jobs. A job is a user-initiated action that is performed on a Junos Space object. Each job is assigned a unique job ID that serves to identify the job. For more information about managing jobs from this workspace, see “Job Management” in the *Junos Space Network Application Platform User Guide*.

From Media Flow Activate, the following actions initiate jobs:

- From the **Media Flow Devices** inventory landing page:

- Upgrading or rolling back a software
- Replicating a device configuration
- Restarting a service
- Restarting devices
- Restoring a device configuration
- Provisioning, reprovisioning, or deprovisioning the resource pools
- Configuring an interface for transparent or reverse proxy services
- Configuring a bonded interface
- From the **Service Design** inventory landing page:
 - Provisioning, reprovisioning, or deprovisioning services
- From the **Service Provisioning** inventory landing page:
 - Provisioning services

When you initiate an action on multiple devices from Media Flow Activate, the main job that is created comprises several subjobs. Each subjob represents a user-initiated action for a single device. For example, when you provision a service on three devices, four jobs are created, of which three are subjobs representing the provisioning of the specific service on a single device. Starting from MFA Release 3.0, you can view the status of the subjobs (whether they are successful or not) by clicking the main job. The pop-up that appears lists the subjobs with job IDs, the devices on which the action is performed, whether the job is a success or a failure, and any other special messages that provide additional information when the job is a failure. The status of the main job is shown as successful only when all its subjobs have been completed successfully.

Related Documentation

- [Upgrading or Rolling Back the Media Flow Controller Software Image on page 22](#)
- [Restarting Media Flow Controller Devices or Services on page 27](#)
- [Provisioning Resource Pools to MFC Devices on page 29](#)
- [Managing Resource Pool Associations on page 30](#)
- *Provisioning Services*
- *Managing Provisioned Services*
- [Media Flow Activate Overview on page 4](#)
- *Quick Reference to Tasks in Media Flow Activate*

PART 3

Configuration

- [Configuring Media Flow Controllers with Media Flow Activate on page 47](#)

CHAPTER 3

Configuring Media Flow Controllers with Media Flow Activate

- [Configuring MFC Device Interfaces on page 47](#)
- [Configuring Bonded Interfaces on page 49](#)
- [Configuring Devices on page 51](#)
- [Configuring BGP-Based Traffic Steering on page 53](#)
- [Creating Resource Pools on page 55](#)

Configuring MFC Device Interfaces

Typically, eth0 is used for management, eth1 for origin fetch, and other interfaces for traffic.

To configure an MFC device interface:

1. From the left navigation panel, click **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. Select the discovered device for which you want to configure the interfaces.
3. On the **Actions** list, select **Configure Interfaces**. The **Interface Configuration** page is displayed. All available interfaces are also displayed.
4. In the **Interfaces** section, select the interface that you want to configure and click **Edit**. The **Edit Physical Interface** page is displayed.



NOTE: When you edit a loopback interface, you can change only the secondary address parameters. Other parameters are not configurable.

5. On the **Edit Physical Interface** page, perform the following tasks:
 - In the **IPv4 Address** field, enter an IP address.
 - In the **Subnet Mask** field, enter an appropriate subnet mask.
 - Next to the **Secondary Address List** section, click **Add** to add a list of secondary addresses. The **Add Secondary Address List** page is displayed.

6. On the **Add Secondary Address List** page that is displayed, perform the following tasks:
 - In the **Index** field, enter an appropriate value. You can enter only integers in this field.
 - In the **IPv4 Address** field, enter the secondary address.
 - In the **Subnet Mask** field, enter a subnet mask.
 - Select the **ARP** check box.
 - Click **Add**. You are taken to the **Edit Physical Interface** page.
7. On the **Edit Physical Interface** page, in the **Link Options** section, perform the following tasks:
 - In the **MTU** field, add an appropriate value. You can enter a value from 0 through 65,535 bytes. The default value is **1500** bytes.

This sets the largest number of bytes that a frame can carry.
 - From the **Speed** list, select the appropriate speed. The default is **AUTO NEGOTIATION**.
 - From the **Duplex** list, select the appropriate mode. The default is **Auto**.
 - Select the **ARP** and **DHCP** check boxes.

DHCP allows new network devices to be automatically supplied with an IP address and other information, depending on the setup of the DHCP server. Media Flow Controller does not contain a primary DHCP interface by default. Setting a primary interface ensures that DHCP messages arrive only on that interface. If you select the **DHCP** check box, the values you entered in the **IP Address** and **Subnet Mask** fields are not used.
 - Click **OK**.

You can enable an interface by selecting the interface and clicking the **Enable** button. Click **OK** on the confirmation page. A new job is created. At any point, you can select the interface that you have enabled and click **Disable** to disable the interface.

**Related
Documentation**

- [Configuring Bonded Interfaces on page 49](#)
- [Configuring Devices on page 51](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- [Media Flow Activate Overview on page 4](#)
- *Quick Reference to Tasks in Media Flow Activate*

Configuring Bonded Interfaces

Configure bonded interfaces to create a port channel or aggregated link for load distribution across links and increased link availability.



NOTE: Only one bonded interface is allowed. Up to four interfaces can be bonded in a single bonded interface configuration.

To configure a bonded interface:

1. From the left navigation panel, click **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. Select the discovered device for which you want to configure a bonded interface.
3. On the **Actions** list, select **Configure Interfaces**. The **Interface Configuration** page is displayed. All available interfaces are also displayed.
4. In the **Bonded Interface** section, click **Add**. The **Add Bonded Interface** page displays.
5. On the **Bond Config** tab, specify the following information:
 - In the **Name** field, enter a name for the bonded interface.
 - In the **Description** field, enter a description for the bonded interface.
 - From the **Available** section, select the individual interfaces and use the right arrow to move them to the **Selected** section.
 - In the **Bonding Attributes** section, from the Mode list, select the bonding mode. The different modes supported include:
 - **BALANCE_RR**—This is a “Round-robin” mode, which sends TCP/IP packets belonging to the same session across multiple links. Out-of-order TCP packets coming through different links are retransmitted. This mode supports load balancing and failover. This is the default.
 - **BALANCE_XOR_LAYER3_PLUS_4**—In this mode, traffic to a particular network peer goes across multiple links, although packets belonging to a single connection or session do not span multiple links. This mode supports load balancing and failover. In this mode, a link is selected on the basis of the TCP port and IP address.
 - **LINK_AGG_LAYER3_PLUS_4**—This mode allows the automatic negotiation of port bundling to form a single logical channel between Link Aggregation Control Protocol (LACP) links. This mode also supports load balancing and failover.
 - In the **Up Delay Time** field, enter a value in milliseconds. You can enter a value from 0 through 92,23,37,20,36,85,47,75,807 milliseconds. The default value is 0 milliseconds.

This is the wait period before enabling a slave after detecting a link recovery.

- In the **Down Delay Time** field, enter a value in milliseconds. You can enter a value from 0 through 92,23,37,20,36,85,47,75,807 milliseconds. The default value is **0** milliseconds.

This is the wait period before disabling a slave after a link failure is detected.

- In the **Link Monitoring Time** field, enter a value in milliseconds. You can enter a value from 0 through 92,23,37,20,36,85,47,75,807 milliseconds. The default value is **100** milliseconds.

This is the frequency at which the links are monitored.

6. On the **Interface Configuration** tab, specify the following information:

- In the **IP Address** field, enter an IP address
- In the **Subnet Mask** field, enter an appropriate subnet mask.
- Next to the **Secondary Address List** section, click **Add** to add a list of secondary addresses. The **Add Secondary Address List** page is displayed.

On the **Add Secondary Address List** page, specify the following information:

- a. In the **Index** field, enter an appropriate value. You can enter only integers in this field.
 - b. In the **IP Address** field, enter the secondary address.
 - c. In the **Subnet Mask** field, enter a subnet mask.
 - d. Select the **ARP** check box.
 - e. Click **Add**.
- In the **Link Options** section, in the **MTU** field, enter an appropriate value.

This sets the largest number of bytes a frame can carry. You can enter a value from 0 through 65,535 bytes. The default value is **1500** bytes.

- Select the **ARP** and **DHCP** check boxes.

DHCP allows new network devices to be automatically supplied with an IP address and other information, depending on the setup of the DHCP server. Media Flow Controller does not contain a primary DHCP interface by default. Setting a primary interface ensures that DHCP messages arrive only on that interface. If you select the **DHCP** check box, the values you entered in the **IP Address** and **Subnet Mask** fields are not used.

7. Click **Add**.

You can modify the bonded interfaces by selecting the bonded interface and clicking the **Edit** button. You can also enable the bonded interface by selecting the interface and clicking the **Enable** button. Click **OK** on the Confirmation page. A new job is created. At any point in time, if you want to disable the bonded interface, select the bonded interface and click the **Disable** button.

You can delete a bonded interface by selecting the bonded interface and clicking the **Delete** button.

- Related Documentation**
- [Configuring MFC Device Interfaces on page 47](#)
 - [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
 - [Media Flow Activate Overview on page 4](#)
 - [Quick Reference to Tasks in Media Flow Activate](#)

Configuring Devices

You configure delivery interfaces for Media Flow Controller devices to specify which interfaces to use for media traffic. In this configuration, you also select the Proxy mode for selected devices. The Proxy mode can be **T-Proxy** for transparent proxy or **R-Proxy** for reverse proxy.

Transparent proxies cache popular content and optimize backhaul network utilization. You make the cache look transparent by spoofing the origin server IP address in the response to the client and spoofing the client IP address in the request to the origin server. A transparent proxy requires no browser configuration and is not visible to end users.

Reverse proxies cache and deliver content for a set of domains; client requests are routed to a configured IP address. This setup reduces network and CPU load on an origin server by serving previously retrieved content and enhances user experience by decreasing latency.

Before you begin, you need to know which interfaces you want to use for media delivery. Typically, eth0 is reserved for management and eth1 is reserved for origin server traffic.

To configure delivery interfaces on selected Media Flow Controllers:

1. From the left navigation panel, click **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. From the list of Media Flow Controllers that are listed on the Manage MFCs page, select the Media Flow Controller that you want to configure.
3. On the **Actions** list, select **Device Configuration**. The **Device Configuration** page is displayed.
4. For **Proxy mode**:
 - Select **T-Proxy** to configure the interface for transparent proxy services. This sets the selected Media Flow Controller interfaces for delivery (**delivery protocol http interface <client_traffic_NIC>**) and enables them for transparent proxy (**delivery protocol http transparent <client_traffic_NIC> enable**).
 - Select **R-Proxy** to configure the interface for reverse proxy services. This sets the selected Media Flow Controller interfaces for delivery (**delivery protocol http interface <client_traffic_NIC>**).
5. In the **Select Delivery Interfaces** area, from the **Available** pane, double-click the interfaces you want to receive and respond to delivery requests. Each double-clicked interface moves to the **Selected** pane.

6. In the **Origin Lookup** section, in the **Connection Timeout** field, enter an appropriate value in seconds. You can enter a value from 6 through 120 seconds. The default value is **10** seconds.
7. Select the **Use multiple IP address in DNS response** check box.
8. If you want Media Flow Controller to authenticate the origin server before downloading content, select the **Enable SSL Authentication** check box. If this feature is enabled, the origin server is authenticated every time a transaction is initiated with the origin server by Media Flow Controller. Media Flow Controller uses the trusted Certification Authority (CA) certificates that are configured in the device for this purpose. In addition, there are a few more configuration steps that you have to perform to enable this feature for reverse proxy and content ingest services. These configuration steps are listed in the *Creating HTTP Reverse Proxy Services* and *Creating Content Ingest Services* sections.
9. In the **Log File Handling** area, in the **Purge Frequency** field, enter the number of hours for which you want to store the log files in Media Flow Controller. The log files are purged when this value is reached. The default value is six hours. That is, Media Flow Controller deletes files that are older than six hours and retains files that are less than six hours. By default, the log files are stored in the LogExport folder from which they are purged. If you have previously configured any value for this parameter in Media Flow Controller (either through the MFA GUI or CLI), the UI displays this value in this field, instead of the default value.

If you have configured both **Purge Frequency** and **Log Partition Size Limit**, Media Flow Controller purges the log files when one of the criteria is met (whichever comes first).

To disable time-based purging, set the purge frequency to zero. You can enter a value from 1 through 24 hours. The default value is **6** hours.

10. In the **Log Partition Size Limit** field, specify the percentage of disk size that the LogExport folder can reach. The log files within this folder are purged when this value is reached. The default value is **85%**. That is, when the LogExport folder size is 85% of the disk size, Media Flow Controller purges all the log files within this folder. After the purge, the log files are lost. We recommend that you store the log files in an external server at regular intervals. If you have previously configured any value for this parameter in Media Flow Controller (either through the MFA GUI or CLI), the UI displays this value in this field, instead of the default value. You can configure a value from 0.001 through 100%.

If you have configured both **Purge Frequency** and **Log Partition Size Limit**, Media Flow Controller purges the log files when one of the criteria is met (whichever comes first).

11. Select the **Enable Log Pull** check box.
12. In the **User Authentication Key** field, provide the authentication key to enable an external client to automatically pull access log files from Media Flow Controller's LogExport folder without password authentication.

Only the LogTransfer user is allowed to log in to Media Flow Controller by using the SFTP protocol. Follow the instructions listed in the "Using SSH in Automated Scripts (CLI)" section of the *Juniper Networks Media Flow Controller Administrators Guide* to generate the SSH key for this user from an external client.



CAUTION: To generate the access log files, it is necessary that you configure the access log profile first and then associate the log profile with a reverse proxy service. For more information about creating an access log profile and associating it with a reverse proxy service, see *Creating Access Log Profiles* and *Creating HTTP Reverse Proxy Services*, respectively.

13. Click **Configure**.
14. Click **Ok** on the confirmation page. The selected interfaces are configured for the selected mode of delivery.



NOTE: See the *Juniper Networks Media Flow Controller Administrators Guide* for detailed information about access log profiles.

Related Documentation

- *Creating Access Log Profiles*
- *Creating HTTP Reverse Proxy Services*
- *Creating Content Ingest Services*
- [Restarting Media Flow Controller Devices or Services on page 27](#)
- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- *Quick Reference to Tasks in Media Flow Activate*

Configuring BGP-Based Traffic Steering

Border Gateway Protocol (BGP)–based traffic steering allows Media Flow Controller to receive only cacheable traffic by advertising certain IP addresses through BGP to the peering router.

To configure BGP routing on Media Flow Controller:

1. From the left navigation panel, click **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. Select the discovered device in which you want to configure BGP.
3. On the **Actions** list, select **Configure BGP**. The **Configure BGP** page is displayed.
4. On the **Configure BGP** page, enter information in the following fields:

- **Local AS**—Enter the number of the autonomous system to which Media Flow Controller belongs. Specify a value between 1 and 4,294,967,295. This number identifies Media Flow Controller to other BGP routers.

An autonomous system is a group of routers and their associated networks operating under a single technical administration. This system appears as a single entity to external systems. Each autonomous system is assigned an identifying number by an Internet registry or a network provider. This number identifies the router (in this case, Media Flow Controller) to other BGP routers.

This field is mandatory. The AS number cannot be changed after it is configured because it is a unique identifier. If you need to change the AS number, disable BGP and then configure the AS number again.

- **Local Router ID**—Enter the IP address that identifies Media Flow Controller.
- **Keepalive interval**—Enter the BGP keepalive interval in seconds. The default value is **60** seconds. It is recommended that you enter a value from 7 through 21,845 seconds.

The keepalive time indicates how often Media Flow Controller sends a keepalive message to the neighboring router to indicate that it is still alive. BGP systems exchange keepalive messages to determine whether a link or host has failed or is no longer available.

- **Hold Time**—Enter the hold time in seconds. If a keepalive message is not received by Media Flow Controller from a BGP peer within the hold time, then the peer is marked down. The hold time must be at least three times the keepalive interval. The default value is **180** seconds. It is recommended that you enter a value from 21 through 65,535 seconds.
- **Redistribute connected networks**—Select to dynamically advertise directly connected networks.

For example, consider a number of logical interfaces (such as loopback interfaces) added to a physical interface. One way to advertise all these interfaces is to add them one by one from the **List of static network addresses to advertise** area. The other simpler option is to add the physical interface to the list of advertised static IP addresses and enable this feature, whereby any logical interface connected with this physical interface is automatically advertised to the BGP peers by Media Flow Controller.

- **List of peer routers**—Add a list of peering routers (BGP neighbors or BGP peers) by clicking **Add** and providing the IP addresses and AS numbers of the routers. Media Flow Controller establishes TCP connections with its peers by using the IP addresses provided in the configuration list. It is mandatory that you configure at least one peer router.

Media Flow Controller can have both external and internal peers. A peer is considered external if its AS number differs from Media Flow Controller's own AS number.

To remove a peer, select a peer and then click **Remove**.

- **List of static network addresses to advertise**—Add a list of destination IP addresses to advertise, such that any traffic intended for these IP addresses is redirected to

Media Flow Controller. Media Flow Controller serves the requested objects from its cache or fetches them from the origin servers. Click **Add** or **Remove** to add or remove network IP addresses.

- Click **Configure** to enable BGP traffic steering. If BGP is previously configured on Media Flow Controller, then click the **Reconfigure** or **Disable** button to reconfigure the existing BGP configuration or disable BGP traffic steering, respectively. Alternatively, click **Cancel** to close the configuration page.

**Related
Documentation**

- [BGP Traffic Steering Overview on page 8](#)
- [Media Flow Activate Overview on page 4](#)
- [Understanding Media Flow Controller Management with Media Flow Activate on page 6](#)
- *Quick Reference to Tasks in Media Flow Activate*

Creating Resource Pools

You create a resource pool when you want to host multiple tenants on Media Flow Controller and want to partition the available system resources among these tenants. With resource pools, you can configure the maximum bandwidth and the maximum number of concurrent sessions that must be permitted for a tenant.

To configure a resource pool:

1. From the left navigation panel, click the plus sign (+) adjacent to **Media Flow Devices**. The **Manage MFCs** page is displayed.
2. Click the plus sign (+) adjacent to **Manage Resource Pools**.
3. Click **Add Resource Pool**. The **Add Resource Pool** page is displayed. Enter information in the following fields:
 - **Resource Pool Name**—Name of the resource pool, which must be unique
 - **Description**—(Optional) Description of the resource pool
 - **Max Bandwidth(Mbps)**—Maximum bandwidth that you want to reserve for this resource pool, in Mbps
 - **Max Concurrent Sessions**—Maximum number of incoming client sessions supported by this resource pool
4. Click **Ok**, **Cancel**, or **Reset**. **Ok** instantiates the values you set, **Cancel** closes the page, and **Reset** returns all values to their defaults.

You are returned to the Manage Resource Pools page. If you created a resource pool, you see the newly created resource pool on this page.

Against each resource pool, you can view the configured maximum bandwidth and maximum allowed sessions, whether the resource pool is provisioned to the Media Flow

Controller server, the users who created and modified the resource pool, and when it was last modified.

When you associate a reverse proxy service with this resource pool, the incoming traffic to the website or domain is bound by the parameters defined by the resource pool.

**Related
Documentation**

- [Actions on Resource Pools on page 32](#)
- [Provisioning Resource Pools to MFC Devices on page 29](#)
- [Managing Resource Pool Associations on page 30](#)
- *Provisioning Services*
- [Resource Pools Overview on page 9](#)
- [Media Flow Activate Overview on page 4](#)
- *Quick Reference to Tasks in Media Flow Activate*

PART 4

Index

- [Index on page 59](#)

Index

Symbols

#, comments in configuration statements.....	ix
(), in syntax descriptions.....	ix
< >, in syntax descriptions.....	viii
[], in configuration statements.....	ix
{ }, in configuration statements.....	ix
(pipe), in syntax descriptions.....	ix

A

action	
resource pool.....	32
audit log.....	39

B

BGP traffic steering	
overview	8
bonded interface	
configuring for Media Flow Controller.....	49
braces, in configuration statements.....	ix
brackets	
angle, in syntax descriptions.....	viii
square, in configuration statements.....	ix

C

comments, in configuration statements.....	ix
configuration template.....	10
configuring	
BGP based traffic steering.....	53
Media Flow Controller bonded interface.....	49
Media Flow Controller device.....	51
Media Flow Controller device interface.....	47
resource pool.....	55
conventions	
text and syntax.....	viii
curly braces, in configuration statements.....	ix
customer support.....	ix
contacting JTAC.....	ix

D

device	
configuring BGP based traffic steering.....	53
configuring for Media Flow Controller.....	51
device interface	
configuring for Media Flow Controller.....	47
device template.....	10
documentation	
comments on.....	ix

F

fault	
monitoring.....	33
font conventions.....	viii

J

job management.....	42
---------------------	----

L

launching	
a secure console.....	20
Media Flow Controller dashboard.....	19

M

managing	
resource pool.....	30
manuals	
comments on.....	ix
Media Flow Activate	
audit log.....	39
BGP traffic steering.....	8
configuration template.....	10
configuring	
BGP based traffic steering.....	53
Media Flow Controller bonded	
interface.....	49
Media Flow Controller device.....	51
Media Flow Controller device	
interface.....	47
resource pool.....	55
device template.....	10
discovering device.....	4
fault monitoring.....	33
job management.....	42
launch Media Flow Controller dashboard.....	19
launch secure console.....	20
managing	
resource pool.....	30
Media Flow Controller management.....	6

Media Flow Controller version requirement.....	4
overview.....	4
provisioning	
resource pool.....	29
removing Media Flow Controller	
configuration.....	24
replicating Media Flow Controller	
configuration.....	26
resource pool.....	9
actions.....	32
restart Media Flow Controller device or	
service.....	27
restoring Media Flow Controller	
configuration.....	24
rolling back Media Flow Controller.....	22
tagging object.....	28
upgrading Media Flow Controller.....	22
monitoring	
Media Flow Controller.....	19
performance.....	33

O

object	
tagging	28

P

parentheses, in syntax descriptions.....	ix
provisioning	
resource pool.....	29

R

removing	
Media Flow Controller configuration.....	24
replicating	
Media Flow Controller configuration.....	26
resource pool	
actions	32
configuring	55
managing.....	30
overview	9
provisioning.....	29
restarting	
Media Flow Controller device.....	27
Media Flow Controller service.....	27
restoring	
Media Flow Controller configuration.....	24
rolling back	
Media Flow Controller.....	22

S

secure console	
launching.....	20
support, technical See technical support	
syntax conventions.....	viii

T

tagging	
object.....	28
technical support	
contacting JTAC.....	ix

U

upgrading	
Media Flow Controller.....	22