

Your Question

Article: 00109

Question:

Configuring the IronPort log format for treatment by Net Report

Net Report Answer

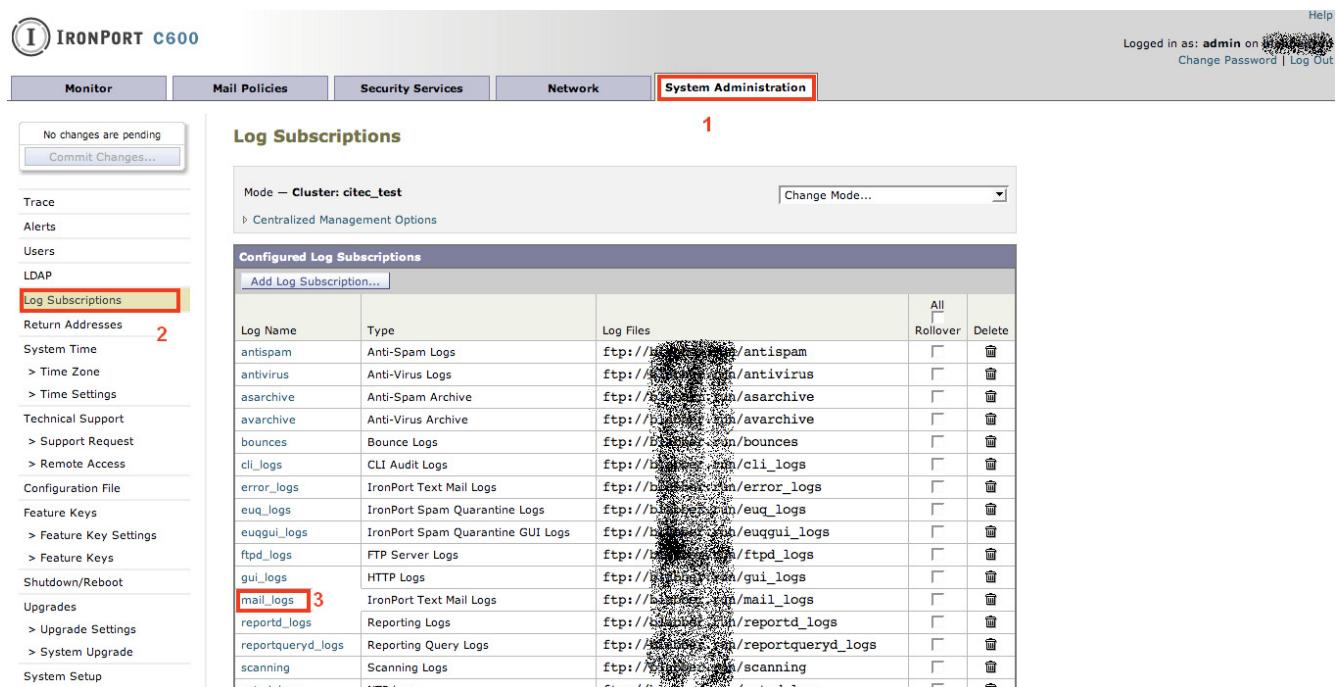
Introduction

This Article explains how to configure your IronPort device's log format for treatment by Net Report

Please follow the steps below:

Steps

1. Connect to your Iron Port device.
2. Select the **System Administration** tab.
3. Select **Log Subscriptions** from the menu in the left pane.
4. Select the Log Name "mail_logs".

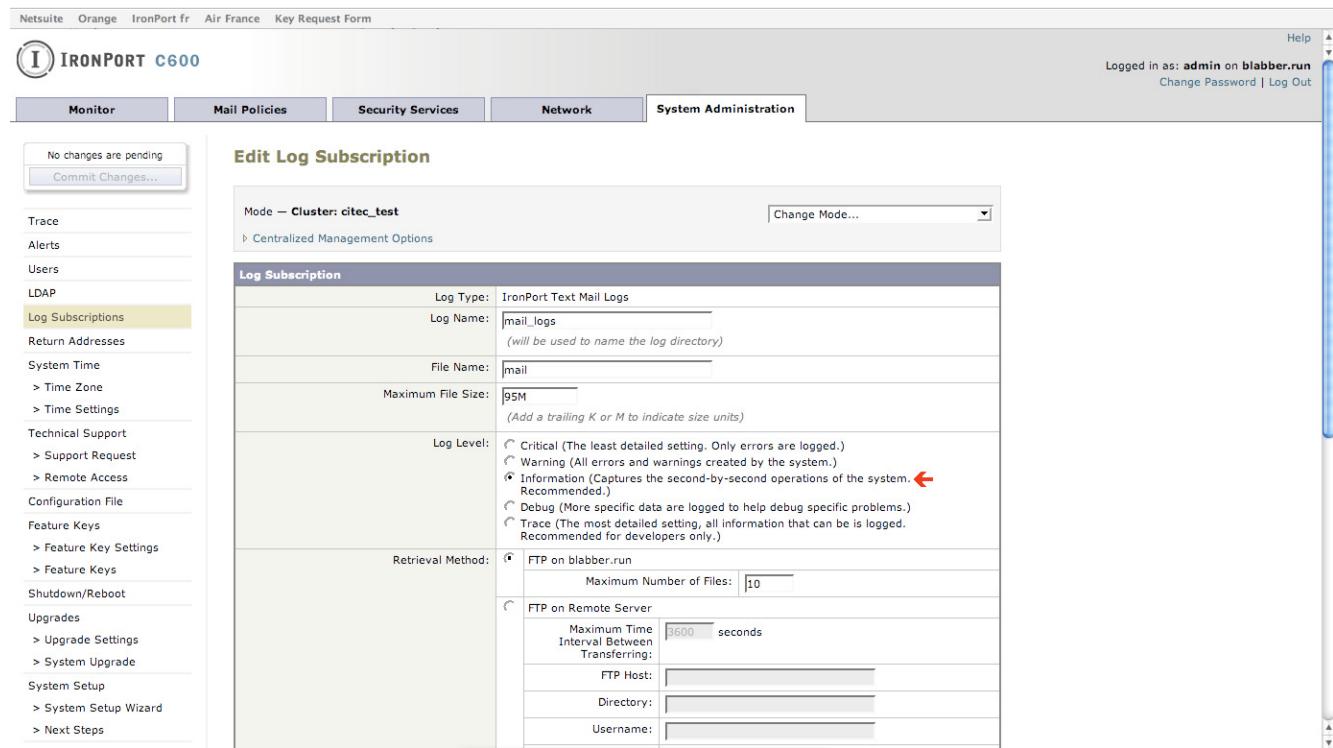


The screenshot shows the IronPort C600 web interface. The top navigation bar includes links for Monitor, Mail Policies, Security Services, Network, and System Administration (which is highlighted with a red box). On the far right, it shows the user is logged in as 'admin' and provides links for Help, Change Password, and Log Out.

The main content area has a sidebar on the left with various management links, some of which are grouped under a red box labeled '2'. The main panel displays the 'Log Subscriptions' configuration page. At the top of this panel, there is a dropdown menu set to 'Mode — Cluster: citec_test' and a 'Change Mode...' button. Below this is a section titled 'Configured Log Subscriptions' with a 'Add Log Subscription...' button. The main table lists log subscriptions with columns for Log Name, Type, Log Files, All Rollover, and Delete. One row in the table is highlighted with a red box and labeled '3', corresponding to the third step in the instructions. The table contains the following data:

Log Name	Type	Log Files	All	Rollover	Delete
antispam	Anti-Spam Logs	ftp://[REDACTED]/antispam	<input type="checkbox"/>		
antivirus	Anti-Virus Logs	ftp://[REDACTED]/antivirus	<input type="checkbox"/>		
asarchive	Anti-Spam Archive	ftp://[REDACTED]/asarchive	<input type="checkbox"/>		
avararchive	Anti-Virus Archive	ftp://[REDACTED]/avararchive	<input type="checkbox"/>		
bounces	Bounce Logs	ftp://[REDACTED]/bounces	<input type="checkbox"/>		
cli_logs	CLI Audit Logs	ftp://[REDACTED]/cli_logs	<input type="checkbox"/>		
error_logs	IronPort Text Mail Logs	ftp://[REDACTED]/error_logs	<input type="checkbox"/>		
eugq_logs	IronPort Spam Quarantine Logs	ftp://[REDACTED]/eugq_logs	<input type="checkbox"/>		
eugui_logs	IronPort Spam Quarantine GUI Logs	ftp://[REDACTED]/eugui_logs	<input type="checkbox"/>		
ftpd_logs	FTP Server Logs	ftp://[REDACTED]/ftpd_logs	<input type="checkbox"/>		
gui_logs	HTTP Logs	ftp://[REDACTED]/gui_logs	<input type="checkbox"/>		
mail_logs	IronPort Text Mail Logs	ftp://[REDACTED]/mail_logs	<input type="checkbox"/>		
reportd_logs	Reporting Logs	ftp://[REDACTED]/reportd_logs	<input type="checkbox"/>		
reportqueryd_logs	Reporting Query Logs	ftp://[REDACTED]/reportqueryd_logs	<input type="checkbox"/>		
scanning	Scanning Logs	ftp://[REDACTED]/scanning	<input type="checkbox"/>		
control_logs	NTP Logs	ftp://[REDACTED]/control_logs	<input type="checkbox"/>		

5. Select the **Information log level.**



No changes are pending
Commit Changes...

Trace
Alerts
Users
LDAP
Log Subscriptions
Return Addresses
System Time
> Time Zone
> Time Settings
Technical Support
> Support Request
> Remote Access
Configuration File
Feature Keys
> Feature Key Settings
> Feature Keys
Shutdown/Reboot
Upgrades
> Upgrade Settings
> System Upgrade
System Setup
> System Setup Wizard
> Next Steps

Mode — Cluster: citec_test
Change Mode...

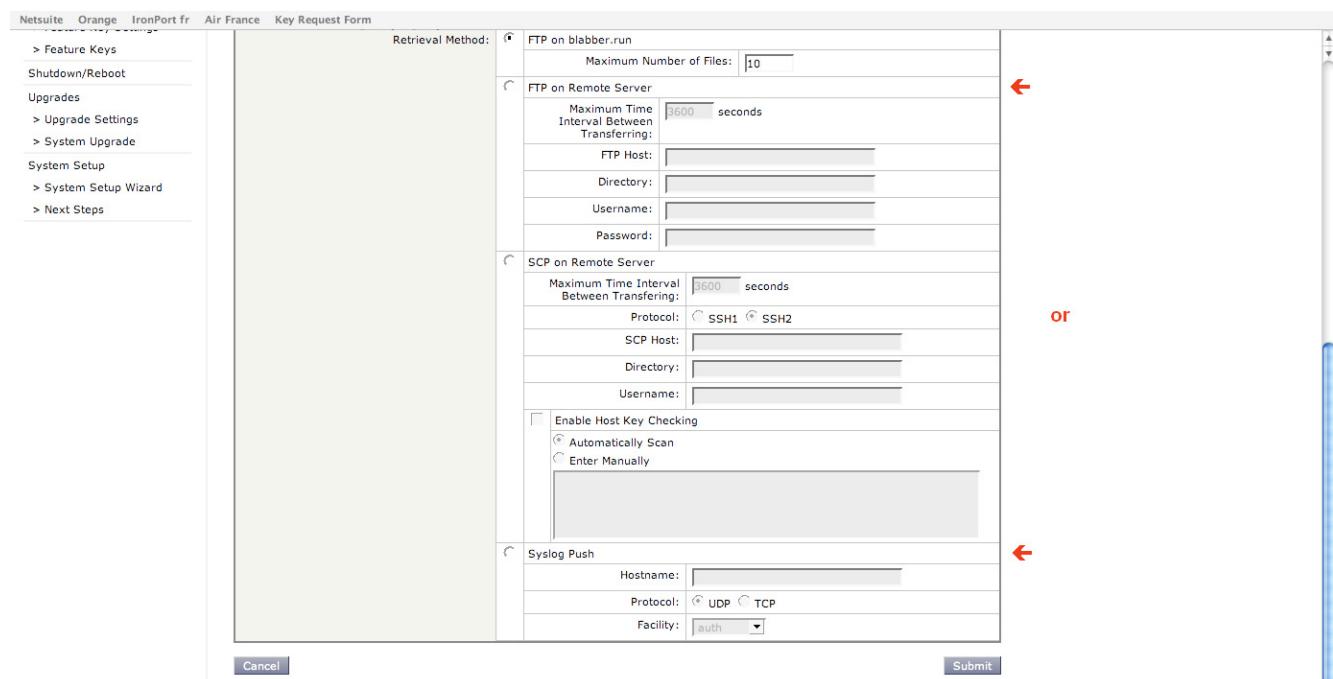
Centralized Management Options

Edit Log Subscription

Log Subscription

Log Type:	IronPort Text Mail Logs
Log Name:	mail_logs (will be used to name the log directory)
File Name:	mail
Maximum File Size:	95M (Add a trailing K or M to indicate size units)
Log Level:	<input checked="" type="radio"/> Critical (The least detailed setting. Only errors are logged.) <input type="radio"/> Warning (All errors and warnings created by the system.) <input checked="" type="radio"/> Information (Captures the second-by-second operations of the system. Recommended.) <input type="radio"/> Debug (More specific data are logged to help debug specific problems.) <input type="radio"/> Trace (The most detailed setting, all information that can be is logged. Recommended for developers only.)
Retrieval Method:	<input checked="" type="radio"/> FTP on blabber.run Maximum Number of Files: 10
	<input type="radio"/> FTP on Remote Server Maximum Time Interval Between Transferring: 3600 seconds FTP Host: Directory: Username: Password:

- 6. Select for logs to be sent by **FTP on Remote Server**.**
- 7. Select the connection information relating to the FTP server which you have installed on the Net Report Server.**
- 8. For real-time log treatment, select the **Syslog Push** option.**
- 9. Select the UDP option button. (to send the logs directly to the IP Address of the Net Report Server).**



Netsuite Orange IronPort fr Air France Key Request Form

Retrieval Method:

- FTP on blabber.run
Maximum Number of Files: 10
- FTP on Remote Server
Maximum Time Interval Between Transferring: 3600 seconds
FTP Host:
Directory:
Username:
Password:
- SCP on Remote Server
Maximum Time Interval Between Transferring: 3600 seconds
Protocol: SSH1 SSH2
SCP Host:
Directory:
Username:
 Enable Host Key Checking
 Automatically Scan
 Enter Manually

Syslog Push
Hostname:
Protocol: UDP TCP
Facility: auth

Cancel Submit