User's Guide

JSCAPE MFT Monitor

Contents

Contents

Introduction 1

Overview

File transfer services are the backbone of many organizations data exchange processes. For an organization to function properly these critical file transfer services must offer reliability, high-performance and security.

The performance and reliability of file transfer services can greatly impact an organizations ability to conduct business with it's clients and trading partners. Left undetected, poor performing file transfer services can result in breaches of SLAs (Service Level Agreement), breakdown of internal processes, disappointed customers and possible loss of revenue.

Furthermore, file transfer services must be properly configured and secured in order to prevent possible data breaches. Failure to properly configure and secure file transfer services can lead to data breaches leaking sensitive data, violation of government compliance regulations and possible fines.

JSCAPE MFT Monitor is a software application developed to monitor the health and security of file transfer services. Using JSCAPE MFT Monitor you can ensure that file transfer services maintain a high level of reliability, performance and security.

Example Uses

- Detect and shutdown rogue file transfer services
- Identify network security and compliance violations in file transfer services
- Monitor availability and performance of file transfer services
- Test performance of file transfer services under heavy load
- Schedule automated network scans and performance monitors
- Receive customized email alerts

Evaluation Edition limitations

The evaluation version of JSCAPE MFT Monitor has the following limitations:

- Limited to user load of 3 users when running a Monitor.
- Limited to detecting 3 services when running a Scan.
- Schedulers are disabled for both Monitors and Scans.

Purchase JSCAPE MFT Monitor License

System requirements

- Sun or IBM JVM (Java Virtual Machine) 1.6 or above
- Windows XP/2003/Vista/2008/7/2012 (32 or 64 bit), Mac OS X, Solaris, Linux.

License

JSCAPE MFT MONITOR LICENSE STATEMENT AND LIMITED WARRANTY

IMPORTANT - READ CAREFULLY

This license statement and limited warranty constitutes a legal agreement ("License Agreement") between you (either as an individual or a single entity) and JSCAPE, LLC. ("JSCAPE") for the software product ("Software") identified above, including any software, media, and accompanying on-line or printed documentation.

BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT.

Introduction 1

Upon your acceptance of the terms and conditions of the License Agreement, JSCAPE grants you the right to use the Software in the manner provided below.

This Software is owned by JSCAPE and is protected by copyright law and international copyright treaty. Therefore, you must treat this Software like any other copyrighted material (e.g., a book), except that you may either make one copy of the Software solely for backup or archival purposes or transfer the Software to a single hard disk provided you keep the original solely for backup or archival purposes.

You may transfer the Software and documentation on a permanent basis provided you retain no copies and the recipient agrees to the terms of the License Agreement. Except as provided in the License Agreement, you may not transfer, rent, lease, lend, copy, modify, translate, sublicense, time-share or electronically transmit or receive the Software, media or documentation.

You acknowledge that the Software is a confidential trade secret of JSCAPE and therefore you agree not to reverse engineer, decompile, or disassemble the Software. You further acknowledge and agree that you may not use the Software to create any product or service that directly or indirectly competes with the Software or any JSCAPE service offering.

You acknowledge and agree that you may not use the Software in a SaaS (Software as a Service) environment without the explicit written permission of JSCAPE.

You acknowledge and agree that you may not use the Software for use in DOS (Denial of Service) attacks or against servers that you do not own and have explicit permission to perform load tests against.

ADDITIONAL LICENSE TERMS FOR SOFTWARE

EVALUATION EDITION

JSCAPE grants to you (either an individual or single entity) nonexclusive license to install and use the Software free of charge. You may redistribute the Software free of charge as long as the software and documentation are maintained in their original form.

PROFESSIONAL AND ENTERPRISE EDITIONS

JSCAPE grants to you (either an individual or single entity) non-exclusive license to install and use a single instance of Software on a single computer. Software may not be shared, installed or used concurrently on different computers without purchasing a separate license for each computer. If you wish to install multiple instances of Software then a separate license MUST be purchased for each instance of Software that is installed. If you are using any virtualization technology then a separate license MUST be purchased for each environment which uses Software.

LIMITED WARRANTY

JSCAPE warrants that the Software, as updated and when properly used, will perform substantially in accordance with the accompanying documentation, and the Software media will be free from defects in materials and workmanship, for a period of ninety (90) days from the date of receipt. Any implied warranties on the Software are limited to ninety (90) days. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

This Limited Warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Any replacement Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, JSCAPE AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING,

BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, WITH REGARD TO THE SOFTWARE, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM STATE/ JURISDICTION TO STATE/JURISDICTION.

LIMITATION OF LIABILITY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL JSCAPE OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF JSCAPE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

HIGH RISK ACTIVITIES

The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). JSCAPE and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraphs ©(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable.

GENERAL PROVISIONS

This License Agreement may only be modified in writing signed by you and an authorized officer of JSCAPE. If any provision of this License Agreement is found void or unenforceable, the remainder will remain valid and enforceable according to its terms. If any remedy provided is determined to have failed for its essential purpose, all limitations of liability and exclusions of damages set forth in the Limited Warranty shall remain in effect.

This License Agreement shall be construed, interpreted and governed by the laws of the State of Florida, U.S.A. This License Agreement gives you specific legal rights; you may have others which vary from state to state and from country to country. JSCAPE reserves all rights not specifically granted in this License Agreement.

TECHNICAL SUPPORT AND UPGRADES

Technical support and upgrades is available to all registered users free of charge for a period of one year after date of purchase. All technical support questions are to be submitted to the JSCAPE help desk available online at http://www.jscape.com/support/ for a prompt reply. Following the first year of use, users may optionally purchase an annual maintenance agreement ("Subscription") which entitles them to another year of free upgrades and technical support. The rate for Subscription is 30% of the current license fee.

INCORPORATED SOFTWARE

Introduction 1

This Software incorporates the JFreeChart library Copyright 2000-2006 by Object Refinery Limited and Contributors. The JFreeChart library may be found in the lib directory of the Software installation directory in the file named jfreechart.jar and is distributed under the terms of the LGPL.

This Software incorporates the JCommon library. The JCommon library may be found in the lib directory of the Software installation directory in the file named jcommon.jar and is distributed under the terms of the LGPL.

Version history

Release 3.1
Sep. 25, 2014

Enhancement: Added dashboard panel to track memory and thread statistics over time.

Release 3.0
Feb. 21, 2014

Enhancement: Replaced Java management client with web based interface.
Enhancement: Added ability to clear results for a scan or monitor.
Enhancement: Added wait period parameter to monitors which controls amount of time to wait before client disconnects.
Enhancement: Added ability to load credentials from a file for monitors.
Enhancement: Added ability to create administrative users for managing application using web interface.
Enhancement: Added ability to store monitor and scan results in a relational database.

Release 2.3
Jan. 4, 2013

Enhancement: Updated "Create" action for "Load" section of monitors to use random data rather than null data.
Bug Fix: Resolved issue where "Remote directory" for monitors was ignored.
Bug Fix: Resolved public key and client certificate authentication issue in SFTP and FTPS monitors.
Bug Fix: Resolved issue where making changes to "Key Authentication" section of a monitor did not activate "Save" button.

Release 2.2
Nov. 9, 2012

Enhancement: Renamed product to JSCAPE MFT Monitor.
Enhancement: Renamed Sessions module to Monitors.
Enhancement: Added scheduler support to Monitors.
Enhancement: Added Alerts support to Monitors.
Enhancement: Added Scans module to detect and audit file transfer services on a host or network.

Release 2.1
Apr. 12, 2012

Enhancement: Changed default file size in Create File dialog to 100KB.
Enhancement: Added visual indicator to sessions tree for failed sessions.
Enhancement: Updated right click context menu for sessions to include Run and Refresh options.
Enhancement: Updated default view for session to display Summary tab.
Enhancement: Change default logging directory so that each session run has it's own unique directory utilizing %name% and %datetime% variables.
Enhancement: Sessions view is now automatically updated to show latest session results.

Enhancement: Added ability to copy a session.
Enhancement: Added ability to delete session results.

Release 2.0
Mar. 16, 2012

Enhancement: Added ability to schedule load testing sessions.
Enhancement: Added support for AFTP (Accelerated File Transfer Protocol).

Release 1.2
Oct. 17, 2011

Enhancement: Added ability to create files of specified size for use in load testing.
Enhancement: Various performance enhancements to underlying client protocols.
Enhancement: Moved documentation online.
Bug Fix: Various bug fixes.

Release 1.1
Dec. 15, 2010

Enhancement: Added support for client certificates in FTPS protocol.
Enhancement: Added support for Windows 64 bit installer.

Release 1.0.18
Mar. 31, 2009

Enhancement: Old debug log files are cleared when running a session.
Bug Fix: Fixed issue with threads not running concurrently.

Release 1.0.14
Mar. 16, 2009

Initial release

Installing on Windows

To install JSCAPE MFT Monitor on a Windows platform perform the following:

1. Download and run the install.exe installation file for JSCAPE MFT Monitor.
2. Follow the steps in the installation wizard.
3. If you are running any firewall software make sure that it is setup to allow JSCAPE MFT Monitor to run.
4. Start the JSCAPE MFT Monitor service.
5. Launch web interface to configure your server.

See also

Launching web interface

Installing on Linux

RPM Console Installation

To install using the RPM file perform the following steps as a user with **root** privileges.

1. Place the install.rpm file in a directory on the destination server.

2. Install. Run the following command from the directory containing the RPM file you placed on your server:

```
rpm -ivh install.rpm
```

3. Configure Administration Service. Go to the `/opt/JSCAPE_MFT_Monitor` directory and run the following command:

```
./add-administrator -u [username] -p [password]
```

For example:

```
./add-administrator -u admin -p secret
```

This will configure your JSCAPE MFT Monitor instance, where `[username] [password]` are the credentials you will use when managing the server.

4. Start the JSCAPE MFT Monitor service. From the JSCAPE MFT Monitor installation directory run the following command:

```
./start_service.sh
```

The JSCAPE MFT Monitor service should now be running. To connect to this service and manage your server see the topics below.

ZIP Console Installation

1. Place the install.zip file in a directory on the destination server.

2. Install. Run the following command from the directory containing the ZIP file you placed on your server:

```
unzip install.zip
```

3. Configure Administration Service. Go to the JSCAPE MFT Monitor installation directory, located in the `JSCAPE_MFT_Monitor` directory relative to where the unzip command was executed, and run the following command:

```
./add-administrator -u [username] -p [password]
```

For example:

```
./add-administrator -u admin -p secret
```

This will configure your JSCAPE MFT Monitor instance, where [username] [password] are the credentials you will use when managing the server.

4. Start the JSCAPE MFT Monitor service. From the JSCAPE MFT Monitor installation directory run the following command:

```
./start_service.sh
```

The JSCAPE MFT Monitor service should now be running. To connect to this service and manage your server see the topics below.

See also

Launching web interface

Installing on Mac OS X

To install JSCAPE MFT Monitor on a Mac OS X platform perform the following:

1. Download and run the install.dmg installation file for JSCAPE MFT Monitor.

2. Follow the steps in the installation wizard.

3. If you are running any firewall software make sure that it is setup to allow JSCAPE MFT Monitor to run.

4. Start the JSCAPE MFT Monitor service. Service will start automatically following installation. If service is not started then you may start it manually as root user using the ./start_service.sh command from a terminal shell prompt.

In order to have service start automatically upon system reboot, edit the `/Library/LaunchDaemons/com.jscape.MFTMonitor.plist` file and set the value for the `OnDemand` parameter to `false`.

5. Verify that JSCAPE MFT Monitor is running using the following command from your shell prompt:

```
netstat -a | grep 30881
```

where 30881 is the HTTP listening port for JSCAPE MFT Monitor service.

6. Launch web interface and configure your server.

See also

Launching web interface

Installing on Solaris

ZIP Console Installation

1. Place the install.zip file in a directory on the destination server.

2. Install. Run the following command from the directory containing the ZIP file you placed on your server:

```
unzip install.zip
```

3. Configure Administration Service. Go to the JSCAPE MFT Monitor installation directory, located in the `JSCAPE_MFT_Monitor` directory relative to where the unzip command was executed, and run the following command:

```
./add-administrator -u [username] -p [password]
```

For example:

```
./add-administrator -u admin -p secret
```

This will configure your JSCAPE MFT Monitor instance, where [username] [password] are the credentials you will use when managing the server.

4. Start the JSCAPE MFT Monitor service. From the JSCAPE MFT Monitor installation directory run the following command:

```
./start_service.sh
```

The JSCAPE MFT Monitor service should now be running. To connect to this service and manage your server see the topics below.

See also

Launching web interface

Auto starting in Linux and Solaris 9 environments

For Linux environments you may have JSCAPE MFT Monitor start up automatically during system start-up by creating a service configuration file for JSCAPE MFT Monitor and placing it in your `/etc/init.d` directory. This same configuration file will be used for gracefully stopping JSCAPE MFT Monitor when shutting down the system. A sample service configuration file, `monitor`, has been placed in the `init.d` directory of your JSCAPE MFT Monitor installation.

Installing the service configuration file

1. As root user, copy the `monitor` sample service configuration file to your `/etc/init.d` directory.

2. Grant execute permissions to this file using the command:

```
chmod 755 monitor
```

3. Using a text editor, change the value of the `INSTALL_DIR` variable to the absolute path of your JSCAPE MFT Monitor installation directory. The default value for the `INSTALL_DIR` variable is `/opt/JSCAPE_MFT_Monitor` which is consistent with Linux RPM installations. Your installation directory may vary.

4. Set this script to be executed automatically upon system start-up using the following command(s):

Linux

```
/sbin/chkconfig --add monitor
```

Solaris 9

```
ln /etc/init.d/monitor /etc/rc3.d/Sxxmonitor

ln /etc/init.d/monitor /etc/rc0.d/Kxxmonitor
```

Note

If you are running under Ubuntu environment then the `chkconfig` command is not available. Instead you must run the following command as root user from `/etc/init.d` directory.

```
update-rc.d monitor defaults
```

Starting the service

From the `/etc/init.d` directory and as root user run the command `./monitor start` to start the service.

Stopping the service

From the `/etc/init.d` directory and as root user run the command `./monitor stop` to stop the service.

Restarting the service

From the `/etc/init.d` directory and as root user run the command `./monitor restart` to restart the service.

Auto starting in Solaris 10 environments

Solaris 10 uses SMF (Service Management Facility) for creating and managing services. To enable JSCAPE MFT Monitor as a service perform the following.

1. As `root` user, create a user and group named `mftmonitor`.

2. As `root` user, run the command `usermod -K defaultpriv=basic,net_privaddr mftmonitor` to grant `mftmonitor` user permissions to run services on ports less than 1024.

3. As `mftmonitor` user, run installer for Solaris as described in Installing on Solaris.

4. Open the sample SMF manifest file `monitor_smf.xml` found in the JSCAPE MFT Monitor installation directory using vi or other text editor.

5. Change references to `/opt/JSCAPE_MFT_Monitor` with the absolute path of JSCAPE MFT Monitor installation directory.

6. As `root` user, validate SMF manifest file using `svccfg validate monitor_smf.xml` command.

7. As `root` user, import SMF manifest file using `svccfg import monitor_smf.xml` command.

8. As `root` user, enable service using `svcadm enable svc:/application/mftmonitor:default` command.

9. Check that service was started successfully and not in maintenance using `svcs -x mftmonitor:default` command.

10. Verify that JSCAPE MFT Monitor is running using `netstat -na | grep 30881` command.

See also

For more information on creating services using SMF please see the following links:

http://www.sun.com/software/solaris/howtoguides/smfmanifesthowto.jsp

http://www.sun.com/software/solaris/howtoguides/servicemgmthowto.jsp

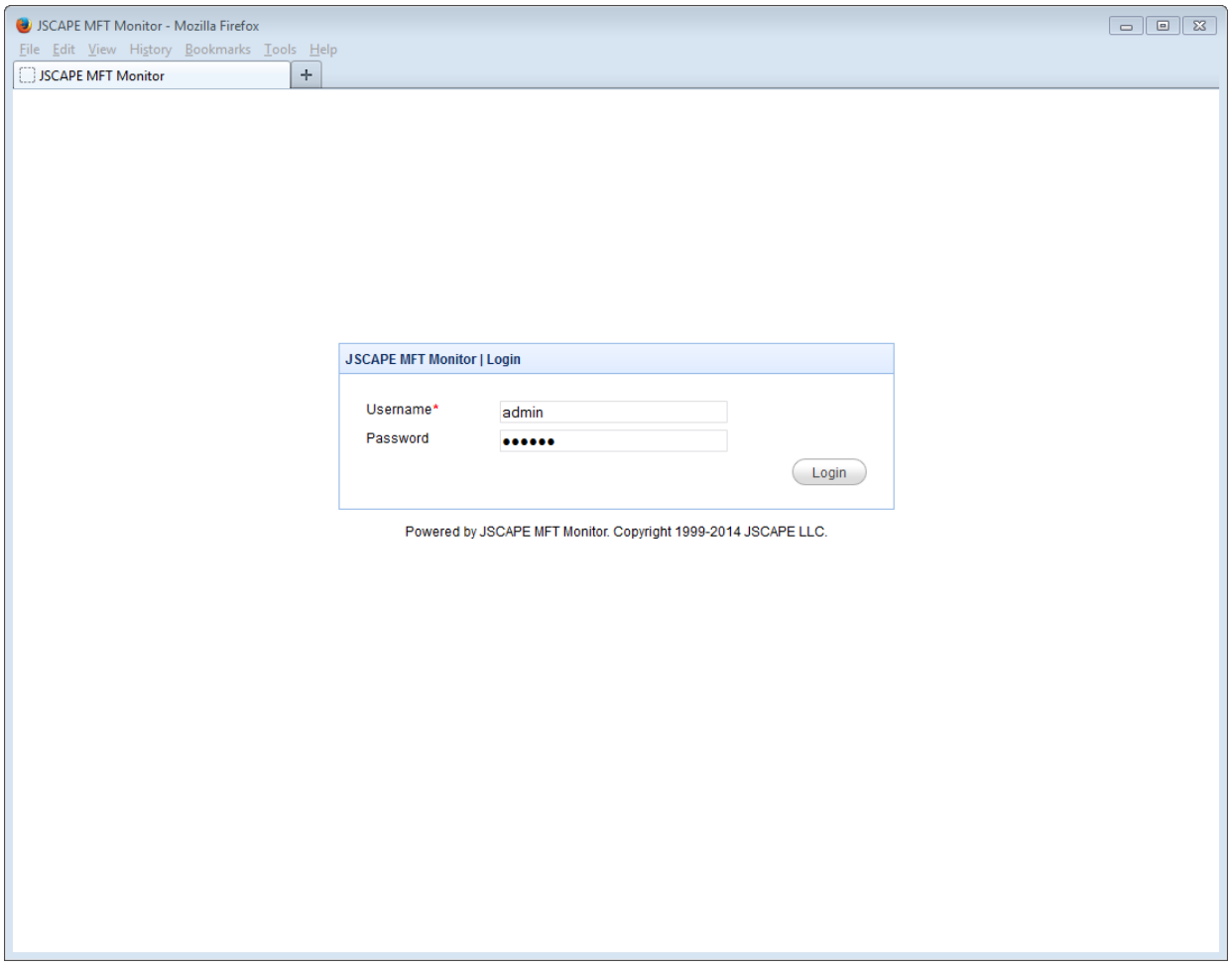
Launching web interface

To launch the web based user interface for managing JSCAPE MFT Monitor, navigate to `http://[hostname]:[port]` where `[hostname]` and `[port]` are the IP address and port that JSCAPE MFT Monitor is listening on. Using default values as an example:

http://localhost:30881

This will display the login page for JSCAPE MFT Monitor. To login enter the administrative credentials that you supplied when first installing JSCAPE MFT Monitor and click the "Login" button.

Figure 25



Usage

3

Monitors

Overview

Monitors may be used to check the health and performance of file transfer services.

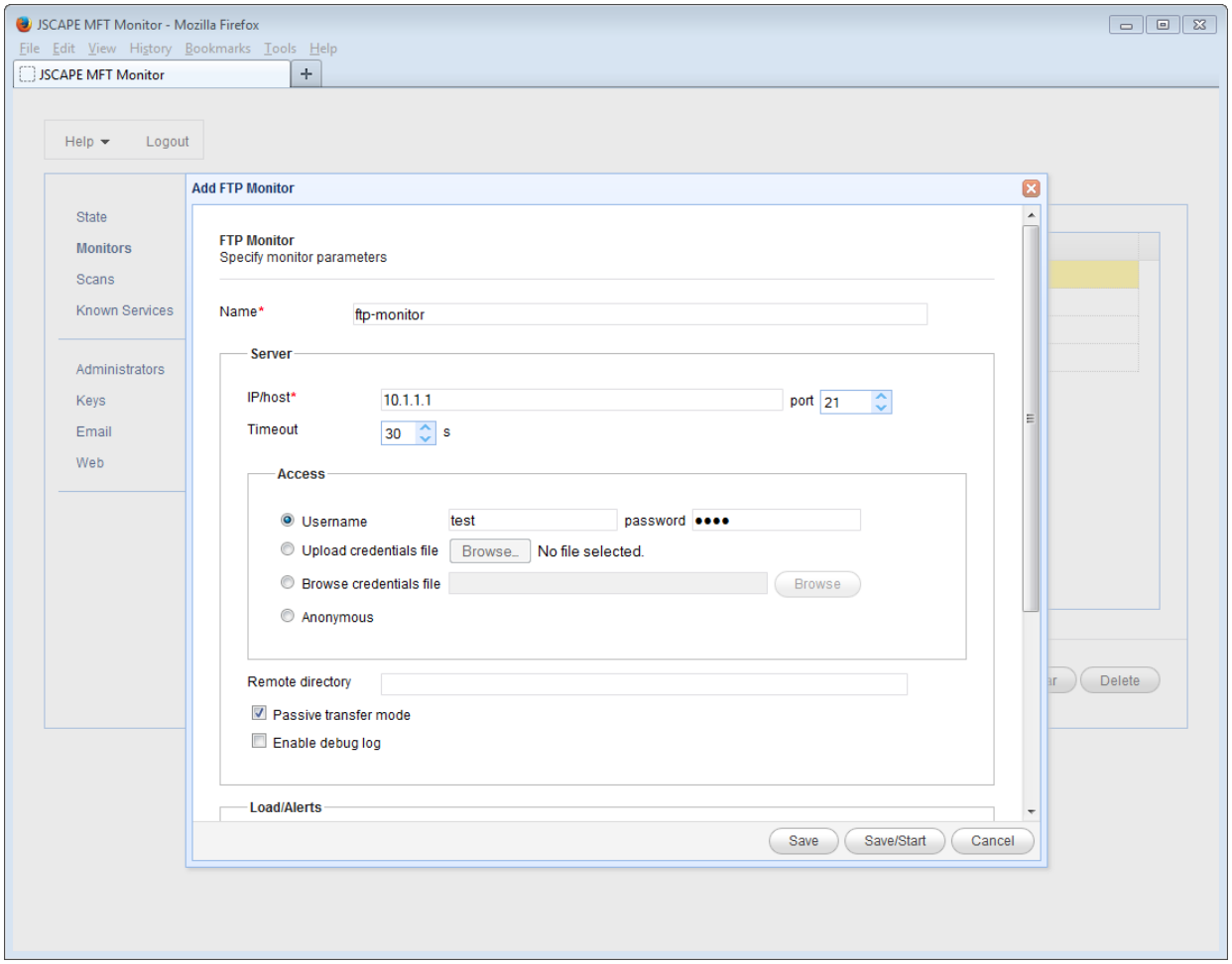
Example Uses

- Monitor availability and performance of file transfer services
- Test performance of file transfer services behave under heavy load
- Schedule automated performance monitors
- Receive customized email alerts

Creating a monitor

To create a new monitor navigate to "Monitors" in the web interface and click the "Add" button. Enter monitor Name, Server, Load/Alerts information and click the Save button.

Figure 1



Name - Unique name for monitor configuration.

Server

Connection type - The connection protocol to use. Available types are FTP, FTP/SSL (AUTH TLS), FTP/Implicit SSL, SFTP/SSH and AFTP.

Anonymous - For use in FTP and FTPS connections only. If selected client session will connect anonymously. Server must be configured to allow anonymous connections.

Passive transfer mode - For use in FTP and FTPS connections only. If selected client session will perform data transfers using passive (PASV) mode. Deselect to use active (PORT) mode.

Remote directory - The remote directory in which to place uploaded file. Default is user root directory.

Enable debug log - Enables debug mode of client sessions. Debug log of each client connection can be seen in "Results" by clicking "Log" button for desired session.

Private Key

For use in SFTP/FTPS connections where client key authentication is used.

Access

Username - The client session username.

Password - The client session password.

Upload credentials file - Upload a credentials file to be used. Each session will read next line from credentials file with username and password supplied in comma delimited format. Example below.

```
user1,pass1
user2,pass2
user3,pass3
...
```

Browse credentials file - Select credentials file from location on server. Each session will read next line from credentials file with username and password supplied in comma delimited format. Example below.

```
user1,pass1
user2,pass2
user3,pass3
...
```

Anonymous - Connect using anonymous credentials using username of "anonymous" and random password.

Load

File - The local file to be uploaded to server and subsequently downloaded from server. A file upload/download will be performed in order to collect throughput statistics.

Users - The number of client user sessions to simulate.

Ramp up period - The amount of time (in milliseconds) to wait before initiating each client user session. The lower the value the more quickly client sessions are initiated resulting in higher number of concurrent

connections.

Wait period - The amount of time (in milliseconds) to wait before disconnecting each client user session.

Use unique filename - If checked then a unique filename is used when transferring file.

Delete file after transfer - If checked then file is deleted from server after transfer.

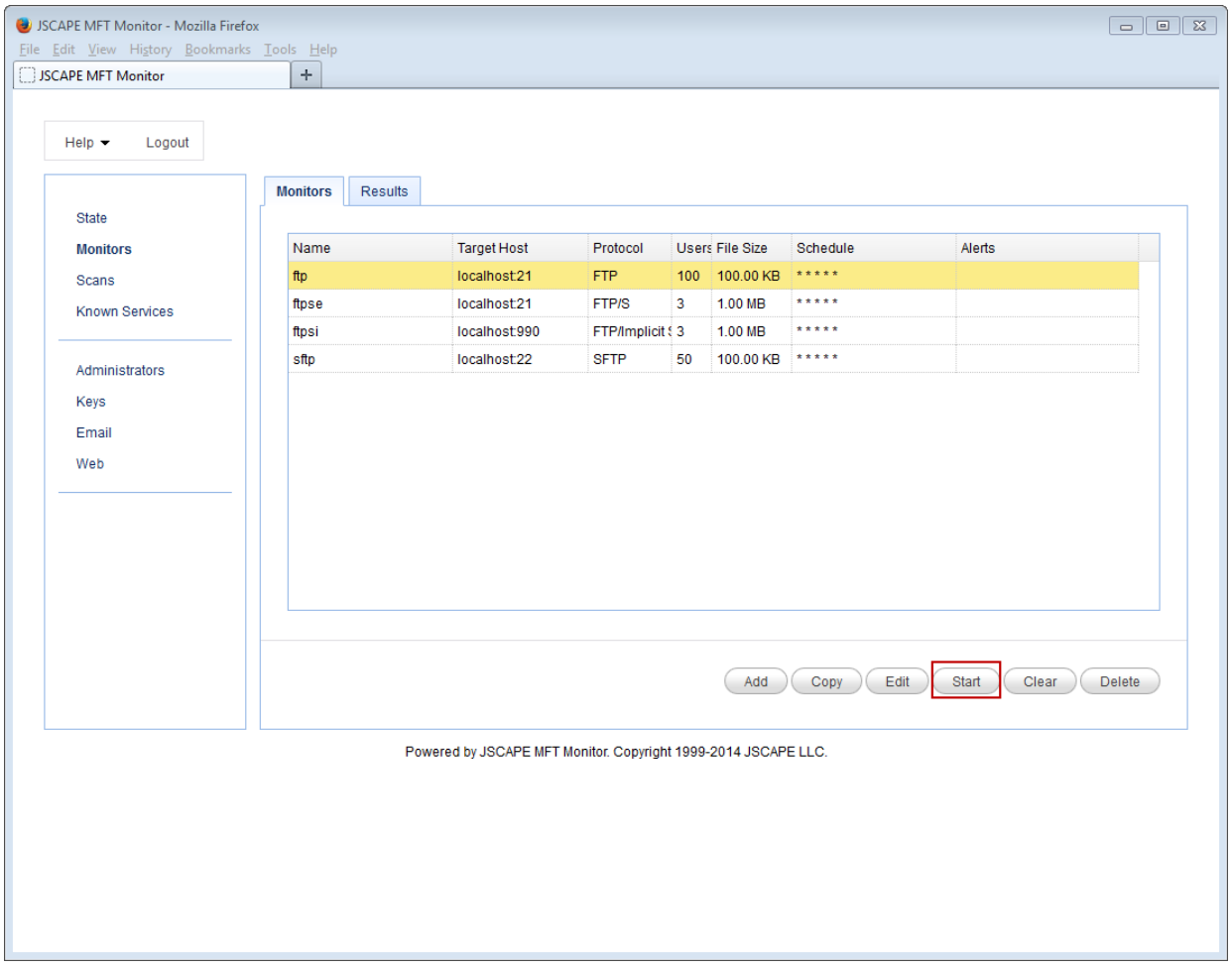
Alerts

Receive email alerts when certain conditions are met.

Manually running a monitor

To manually run a monitor, first select desired monitor from "Monitors" module in JSCAPE MFT Monitor. Next, click the "Start" button for the monitor. Status of monitor can be seen in the "Results" tab.

Figure 2

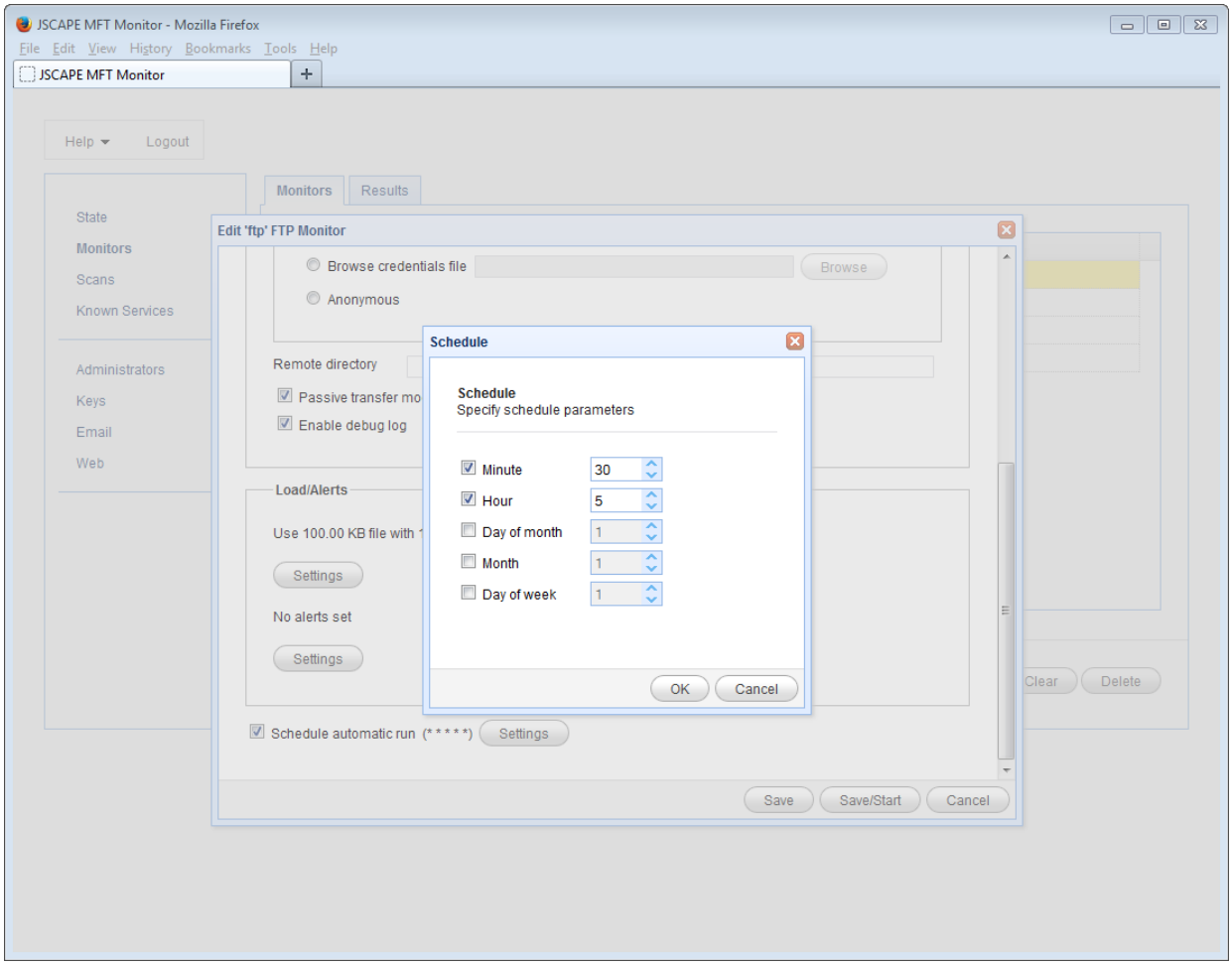


Scheduling a monitor

To schedule a monitor to be run on a one-time or recurring basis first select the desired monitor and click "Edit". Next, scroll to the bottom of the dialog and enable the "Schedule automatic run" checkbox. Lastly, enter the date/time conditions for which this monitor should be run and click Save.

The settings shown in *Figure 13* below are an example of a monitor to be run every day at 5:30 AM local time.

Figure 13



Hour - The hour of the day.

Minute - The minute of the hour.

Day of month - The day of the month.

Month - The month of the year.

Day of week - The day of the week where the 1st day of the week is Sunday.

Examples

5:00 AM every day

Hour = 5
Minute = 0
Day of Month = *
Month = *
Day of Week = *

3:30 PM every Sunday

Hour = 15
Minute = 30
Day of Month = *
Month = *
Day of Week = 1

First day of the month, every month at 1 AM

Hour = 1
Minute = 0
Day of Month = 1
Month = *
Day of Week = *

Receiving email alerts

Email alerts may be sent based on conditions that you configure in the Alerts module. To enable an alert go to the Alerts section for the desired monitor. Next, enable alerts by clicking the desired checkbox(es) setting alert conditions (if available), delivery address and message settings. Upon the next run of monitor, for each alert condition that is met an email alert will be sent.

Note

Before enabling email alerts ensure that you have defined SMTP server settings in Settings > Email.

Figure 11

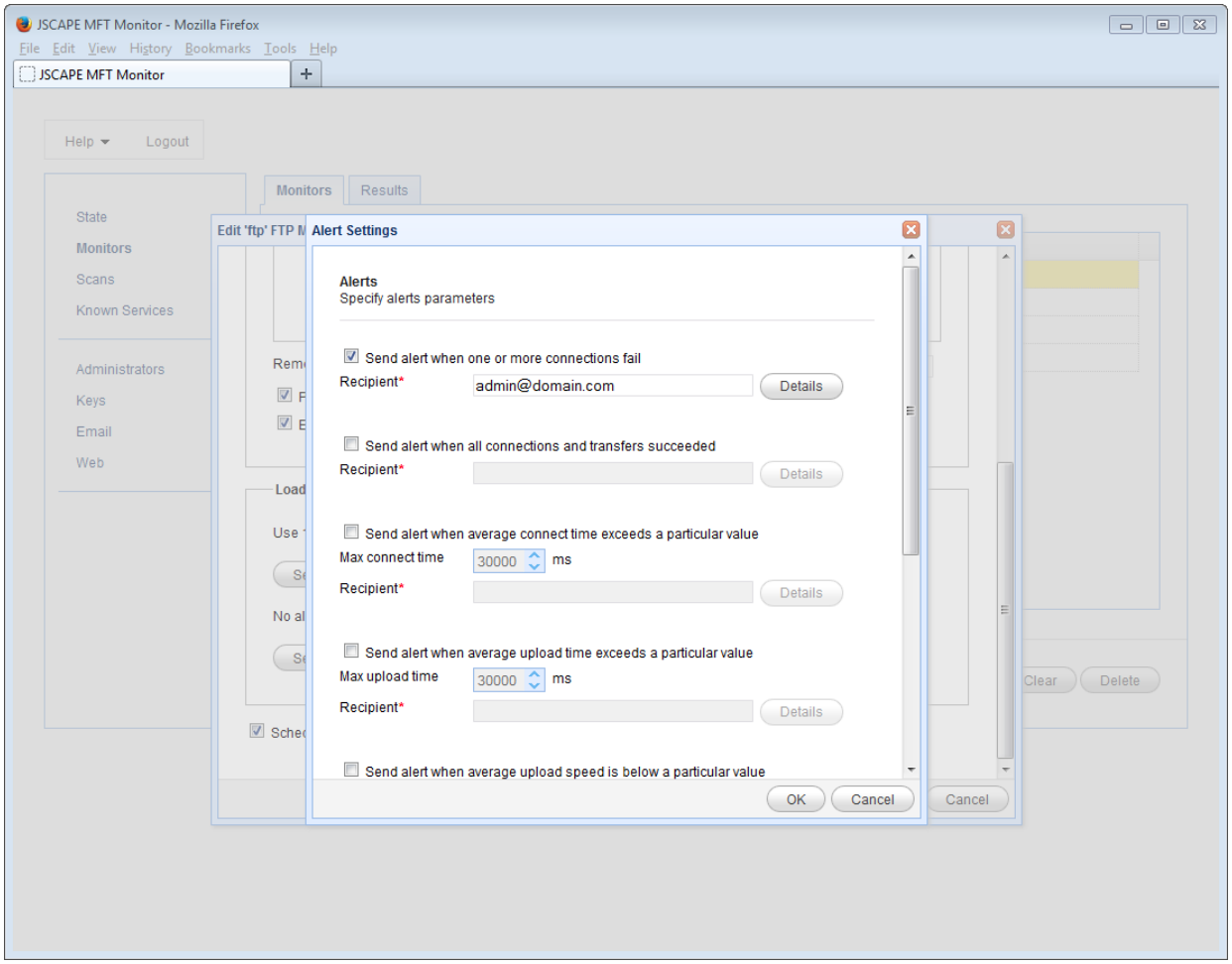
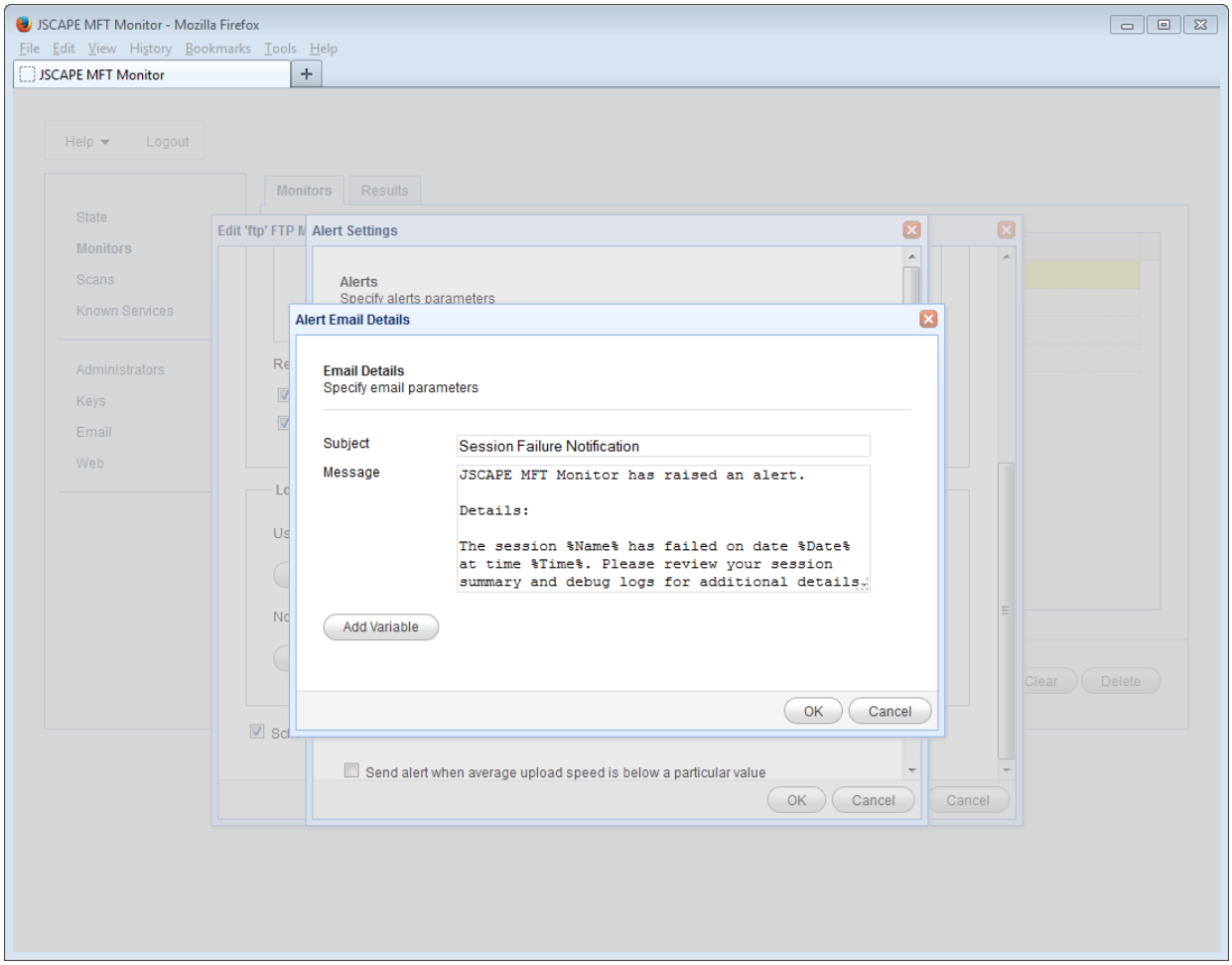

JSCAPE MFT Monitor - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JSCAPE MFT Monitor
Help
Logout
State
Monitors
Scans
Known Services
Administrators
Keys
Email
Web
Monitors
Results
Edit 'ftp' FTP M
Alert Settings
Alerts
Specify alerts parameters
Send alert when one or more connections fail
Recipient*
admin@domain.com
Details
Send alert when all connections and transfers succeeded
Recipient*
Details
Send alert when average connect time exceeds a particular value
Max connect time
30000
ms
Recipient*
Details
Send alert when average upload time exceeds a particular value
Max upload time
30000
ms
Recipient*
Details
Send alert when average upload speed is below a particular value
OK
Cancel
Cancel
Clear
Delete

Figure 12



See also

Settings > Email

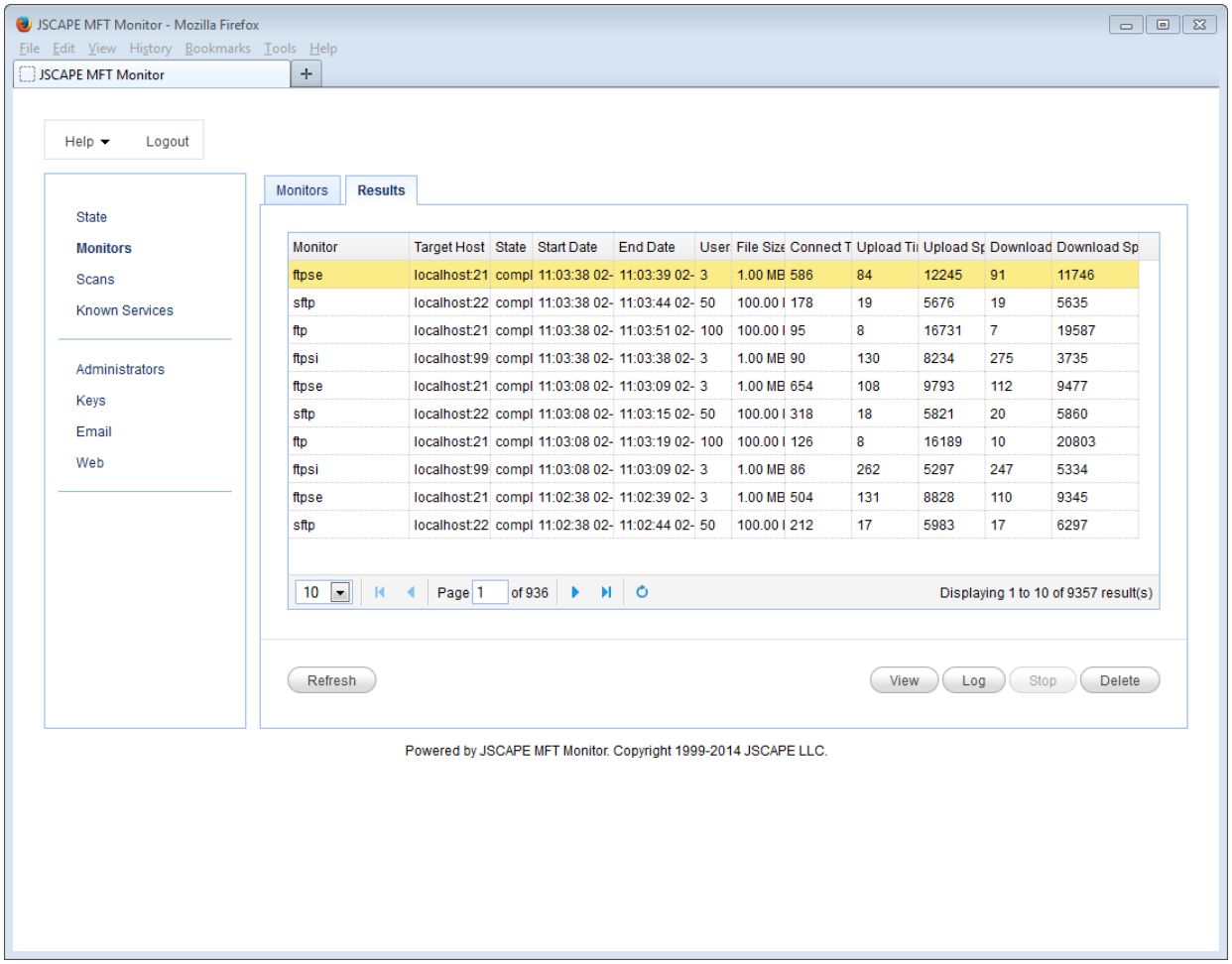
Viewing monitor results

To view the session results for a monitor, navigate to the Monitors > Results page in JSCAPE MFT Monitor. To view the results of a session select desired session and click the "View" button.

Summary

This panel displays a high level summary of the session including load settings and average connect, throughput, upload and download times.

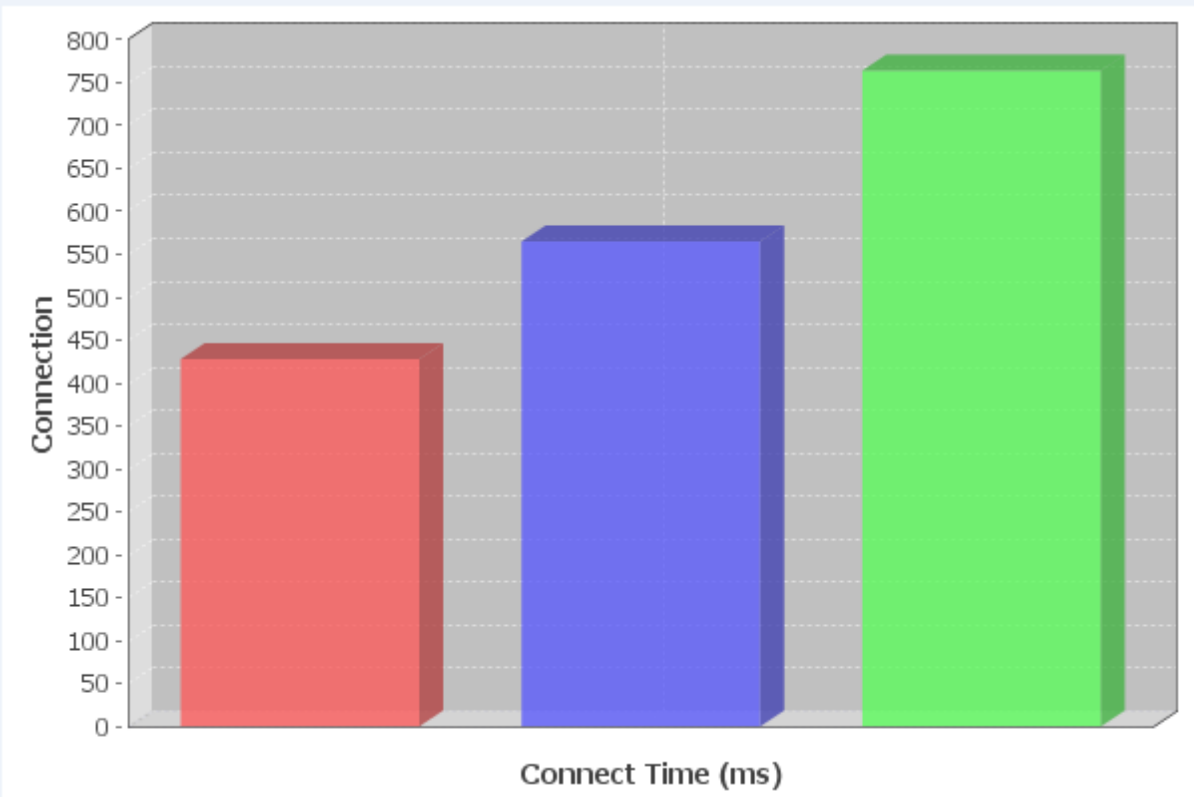
Figure 3



Connect Time

This panel includes a graph of the connection time for each user session.

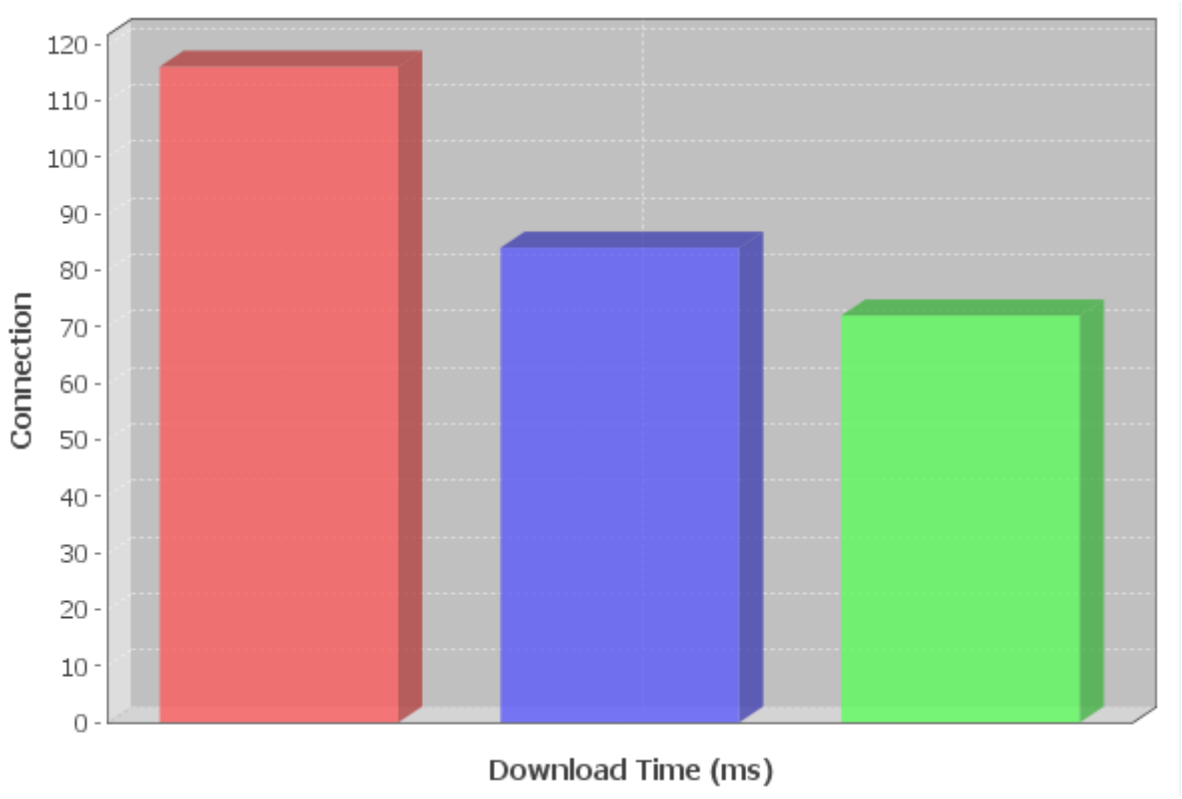
Figure 4



Download Time

This panel includes a graph of the download time for each user session.

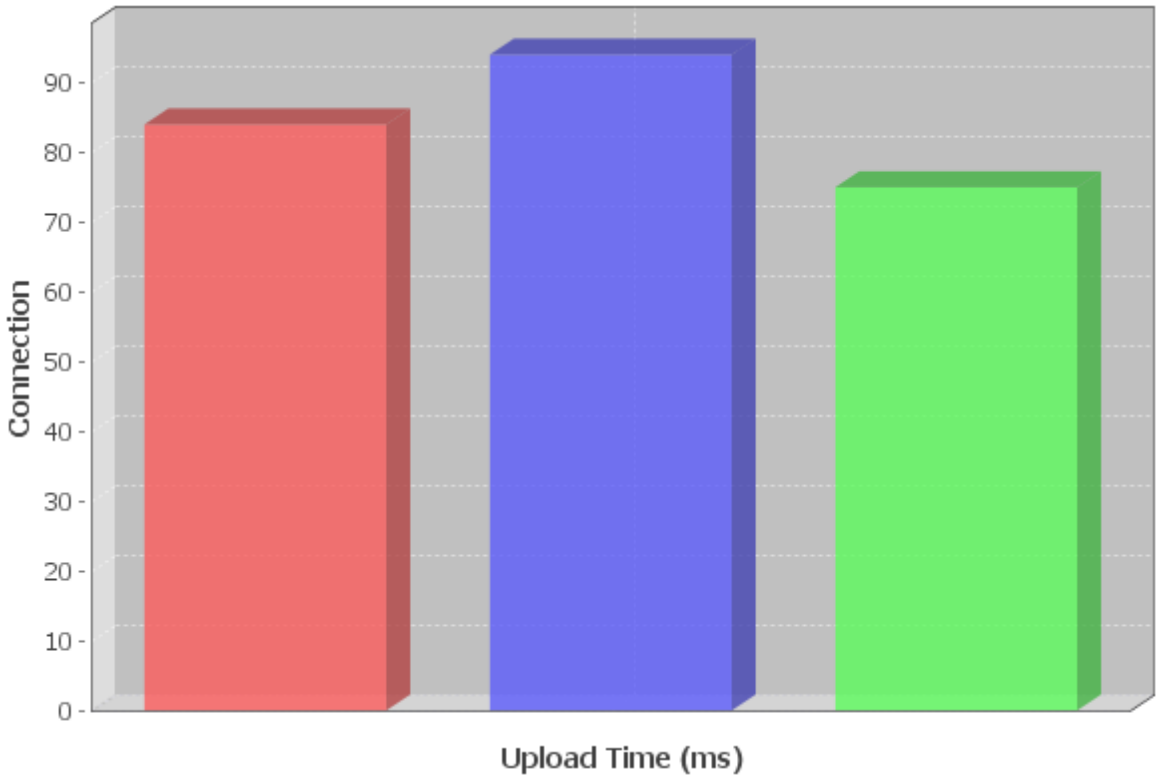
Figure 5



Upload Time

This panel includes a graph of the upload time for each user session.

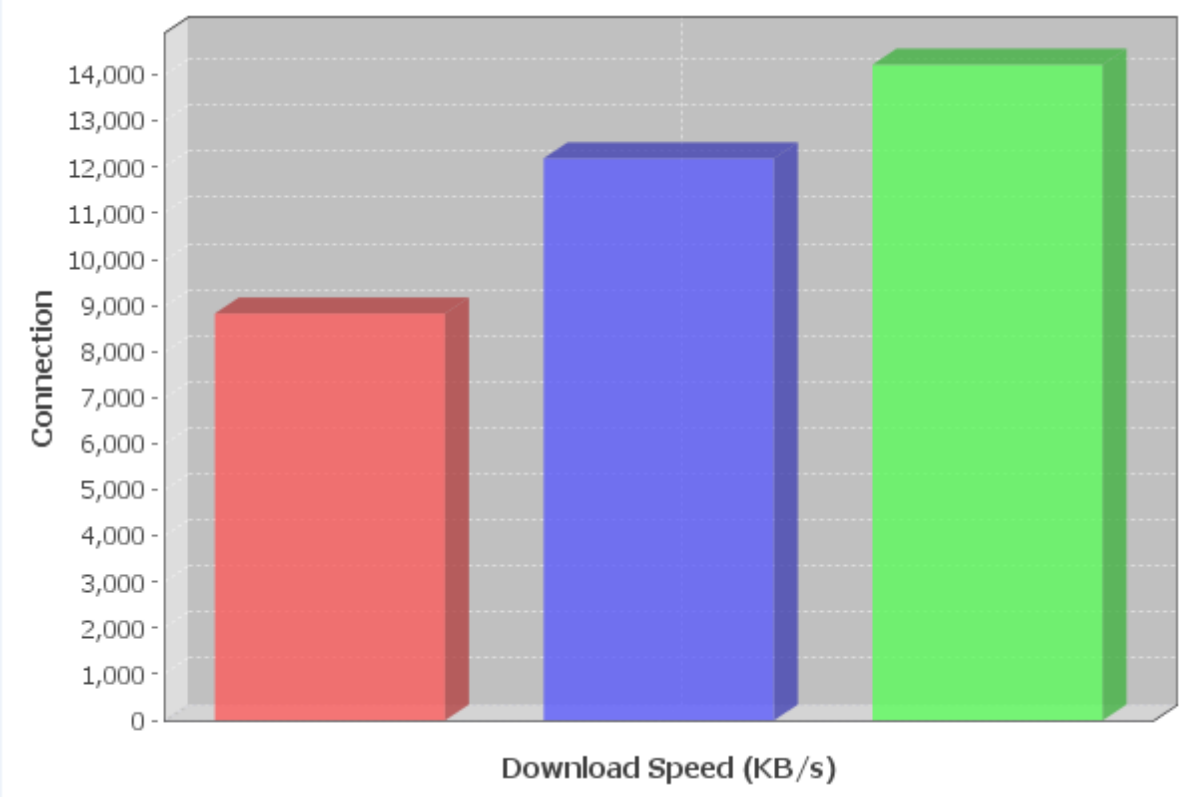
Figure 6



Download Speed

This panel includes a graph of the download speed (KB/s) for each user session.

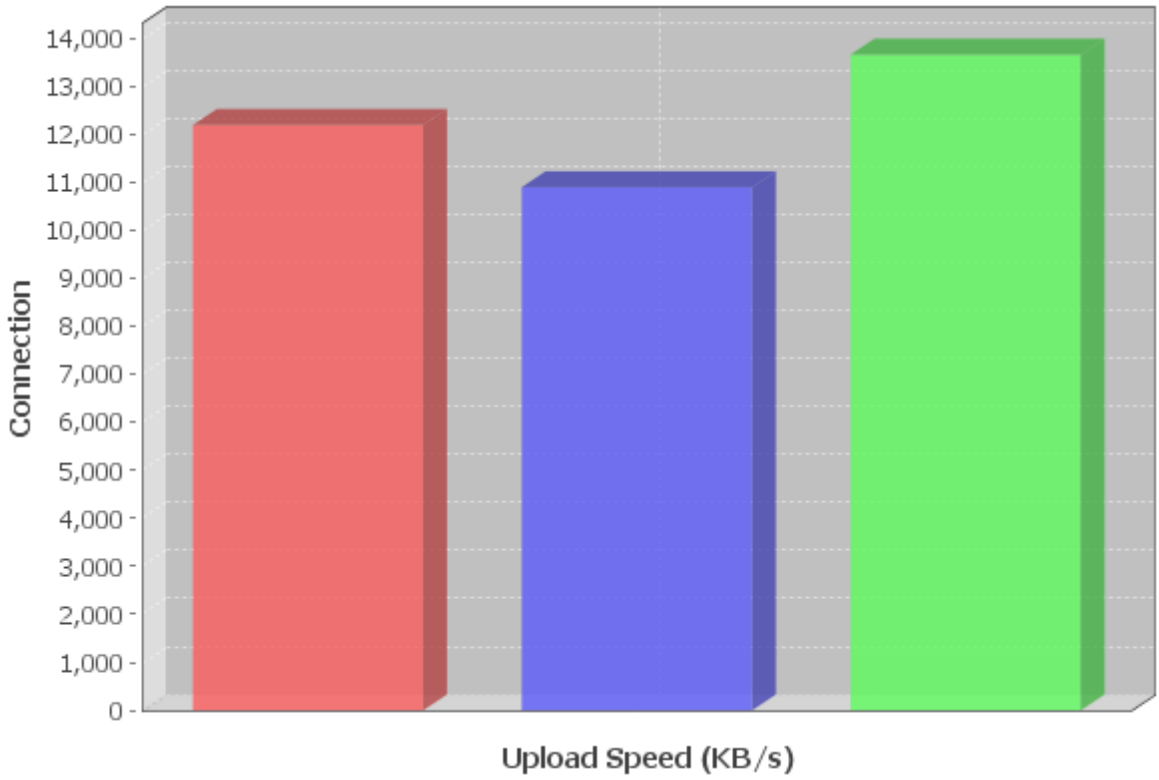
Figure 7



Upload Speed

This panel includes a graph of the upload speed (KB/s) for each user session.

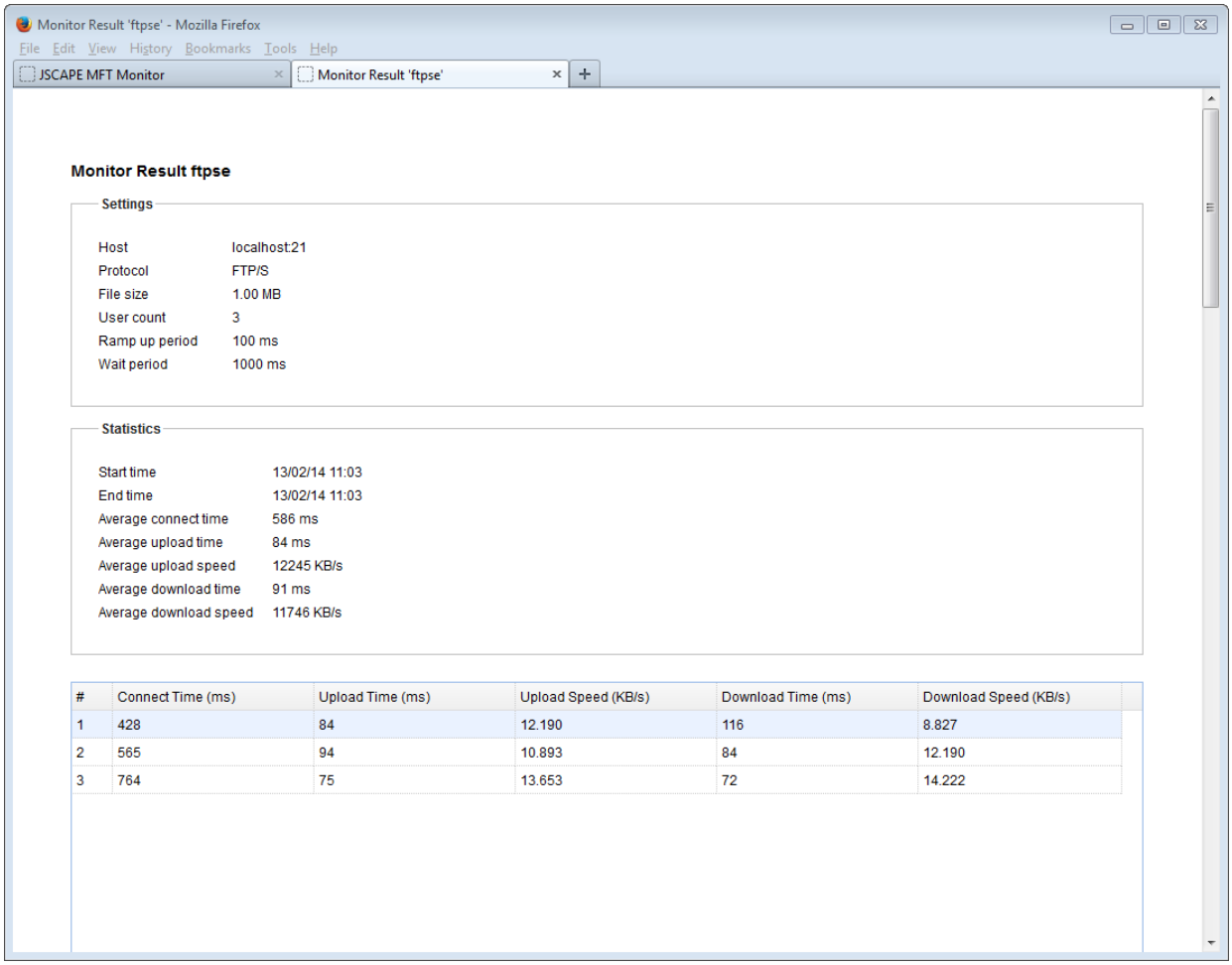
Figure 8



Connections

This panel shows the connect, upload and download times in ms (milliseconds) for each user session.

Figure 9



Load Testing

Overview

Load testing is a way to simulate heavy user and/or network load against your file transfer services. The results of a load test can help you to identify and resolve potential stress points in file transfer services before they become a problem. The Monitors module in JSCAPE MFT Monitor allows you to run manual or scheduled load tests against your file transfer services. This section will discuss some of the topics that you should consider when performing a load test.

See also

Setting up a load test environment

How a load test works

Setting up a load test environment

In any load test it is important that the environment used closely match the environment which will be used by actual users. Failure to do so may result in unreliable load test data. Below are some tips in setting up a load test environment that will achieve the best results.

Tips

1. **DO NOT** run JSCAPE MFT Monitor on the same machine as the server you running the load tester against. Depending on the number of concurrent users, JSCAPE MFT Monitor can consume a large

number of CPU and network resources. This can affect your server ability to process client connections thus skewing load test data.
2. **DO** use a separate dedicated machine to from which to run JSCAPE MFT Monitor. Each concurrent connection made by JSCAPE MFT Monitor will consume a small amount of memory, network resources and CPU. For the most accurate results it is important that the machine you are running the load test from not be busy with other high priority processes.
3. **DO** tests under varying network conditions. Depending on location of the server, a user who is connecting to your server over the Internet may have a different experience than users connecting from an internal network.

How a load test works

JSCAPE MFT Monitor performs a load test by simulating several client sessions to the server you are testing against. Each client session performs the following tasks:

1. Establish connection.
2. Upload file.
3. Download file.
4. Disconnect.

The number of client sessions, and the speed and concurrency with which client sessions are initiated during a load test depends on monitor settings in JSCAPE MFT Monitor.

During the load test performance data is collected by JSCAPE MFT Monitor. Upon completion of the load test, data is used to generate a report to help you gauge the performance and scalability of the server you are testing under various conditions.

Scans

Overview

Scans may be used to audit file transfer services on the network.

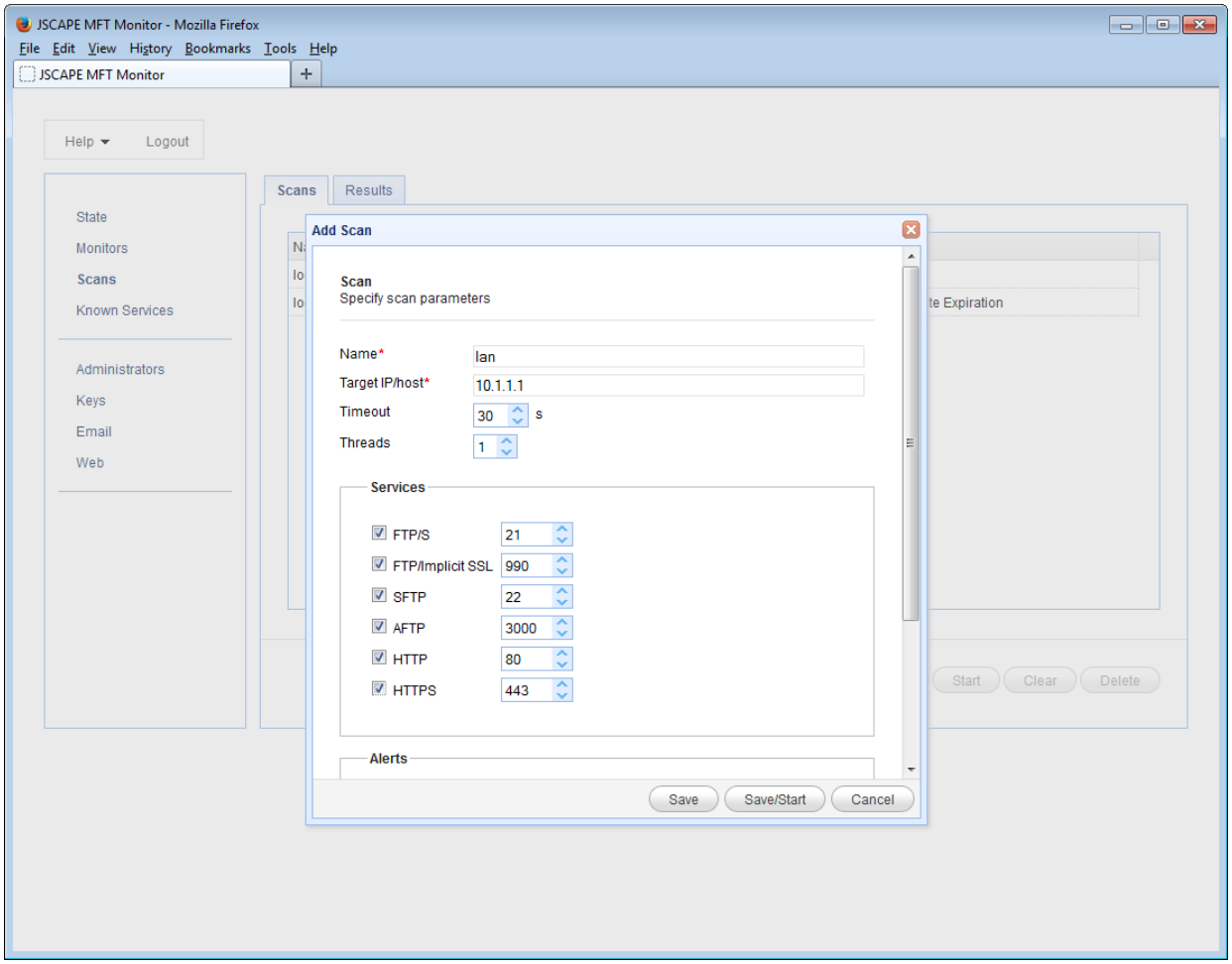
Example Uses

- Detect and shutdown rogue file transfer services
- Identify network security and compliance violations in file transfer services
- Detect file transfer services with expired/expiring SSL certificates
- Schedule automated network scans
- Receive customized email alerts

Creating a scan

To create a new scan, navigate to the "Scans" module and click the "Add" button. Enter scan Name, Target IP/host and Services information and click the "Save" button.

Figure 14



Name - The name of this scan.

Target IP/host - The IP address or network to scan. Valid values are as follows:

Single Address - e.g. 192.168.0.102

Comma Delimited Addresses - e.g. 192.168.0.102,192.168.0.103,192.168.0.104

CIDR (Classless Inter-Domain Routing) - e.g. 192.168.0.2/32

Timeout - The connection timeout used when scanning network services.

Threads - The number of threads to use when scanning network services.

Services

FTP/S - Plain FTP and FTPS using Explicit SSL

FTP/Implicit SSL - FTPS using Implicit SSL

SFTP - SSH (Secure Shell) using SFTP

AFTP - Accelerated File Transfer Protocol (JSCAPE)

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol using SSL

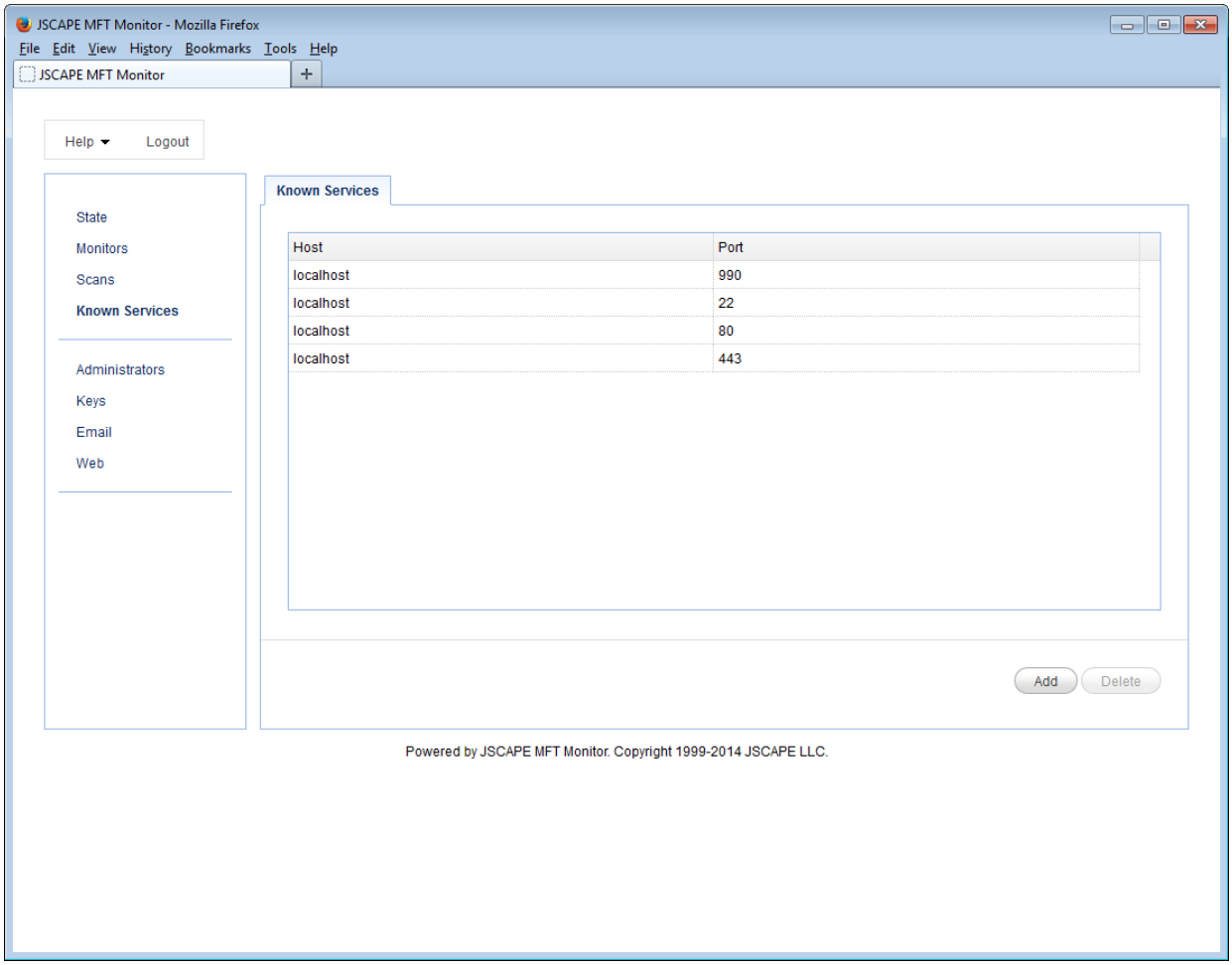
Alerts

Receive email alerts when certain conditions are met.

Setting known services

When performing a scan, you may wish to be alerted when an unknown service is detected. This is particularly important in detecting possible rogue file transfer services. In the Known Services module you may add valid known services. Services listed in the Known Services panel will not raise a Unknown Service alert when performing a scan.

Figure 23



Scanning multiple hosts

To scan multiple hosts, there are a couple options when populating the IP Address field.

1. Enter a comma delimited list of IP addresses.

e.g.

192.168.0.102,192.168.0.103

2. Enter a CIDR (Classless Inter-Domain Routing) address.

e.g.

192.168.0.0/24

The above CIDR will include the entire class C network 192.168.0.0 - 192.168.0.255

CIDR Reference *(External Link)*

Improving scan performance

There are a couple methods by which you can improve the amount of time it takes to perform a scan.

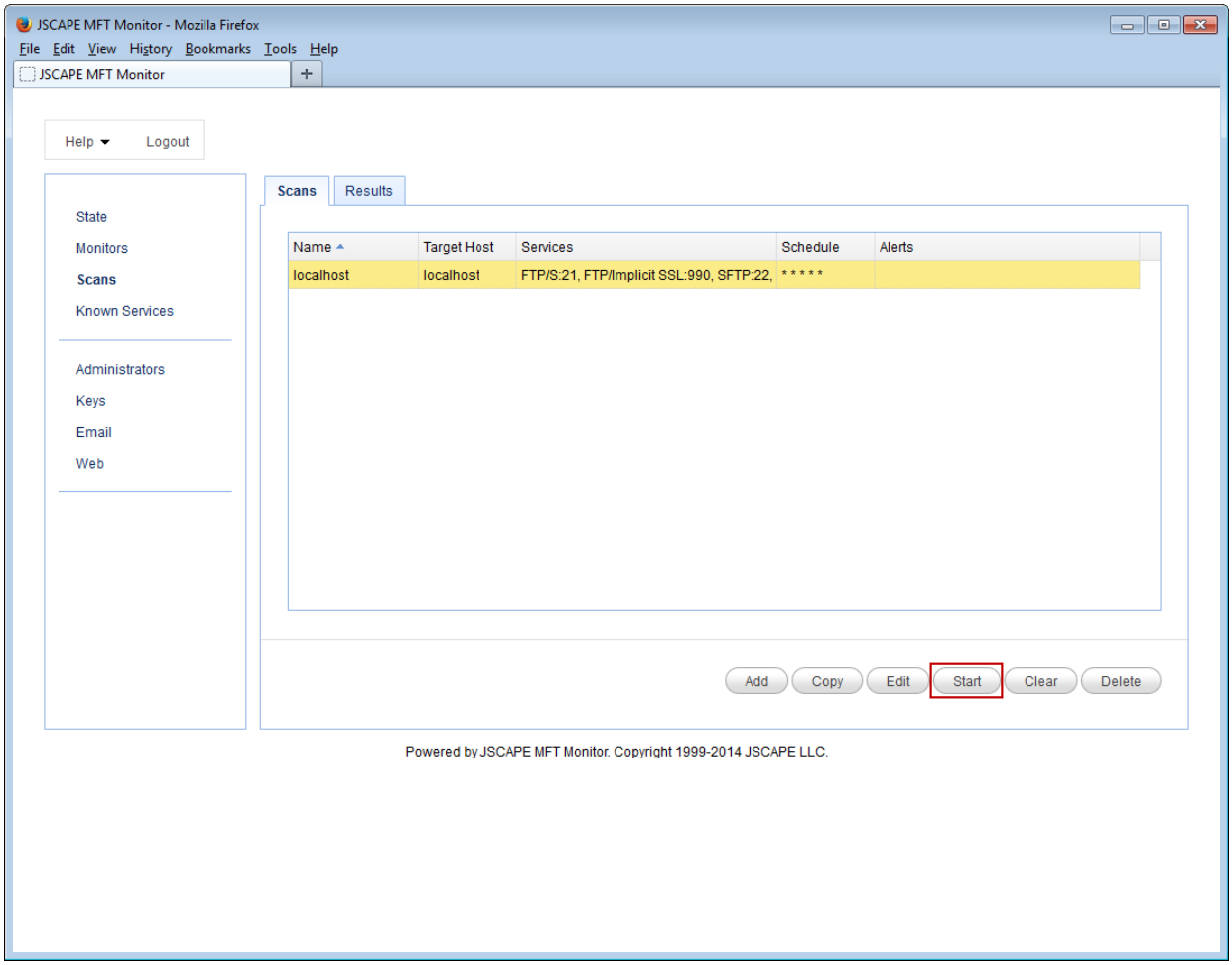
1. Reduce Connection Timeout - The longer the connection timeout the longer it will take a thread to abort a connection for a non-existing service. The connection timeout should be long enough so that services don't go undetected, yet short enough so that threads are left waiting too long.

2. Increase Thread Count - The more threads you have performing a scan the quicker the scan can complete. Each thread takes up a small amount of CPU and memory so the number of threads should be large enough to provide the best level of performance, but small enough so that they do not take over the system.

Manually running a scan

To manually run a scan, first select the scan from the Scans module in JSCAPE MFT Monitor. Next, click the "Start" button for the scan. Status of scan can be seen in the "Results" tab.

Figure 15

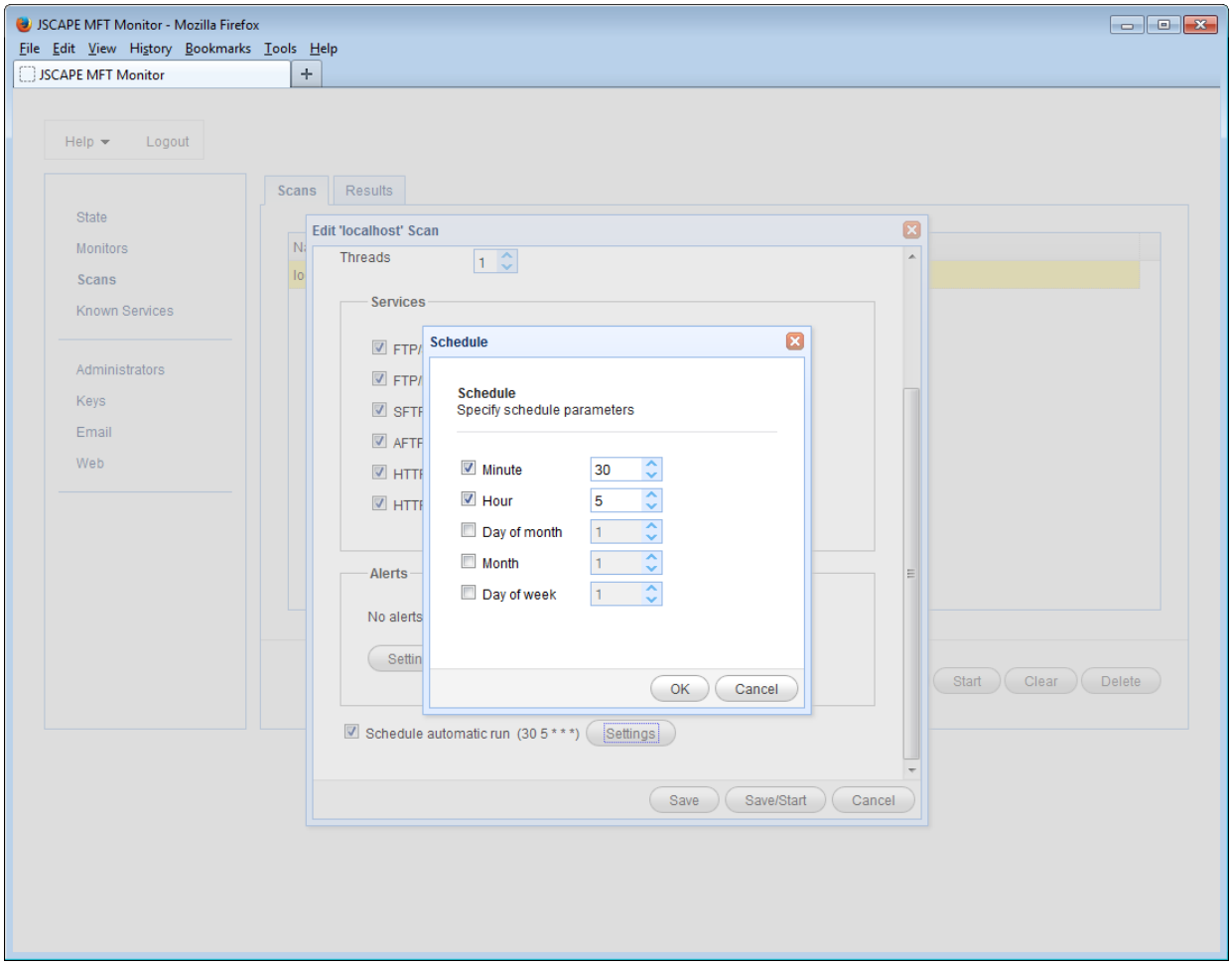


Scheduling a scan

To schedule a scan to be run on a one-time or recurring basis first select the desired scan and click "Edit". Next, scroll to the bottom of the dialog and enable the "Schedule automatic run" checkbox. Lastly, enter the date/time conditions for which this scan should be run and click "Save".

The settings shown in *Figure 16* below are an example of a scan to be run every day at 5:30 AM local time.

Figure 16



Hour - The hour of the day.

Minute - The minute of the hour.

Day of Month - The day of the month.

Month - The month of the year.

Day of Week - The day of the week where the 1st day of the week is Sunday.

Examples

5:00 AM every day

Hour = 5
Minute = 0
Day of Month = *
Month = *
Day of Week = *

3:30 PM every Sunday

Hour = 15

Minute = 30
Day of Month = *
Month = *
Day of Week = 1

First day of the month, every month at 1 AM

Hour = 1
Minute = 0
Day of Month = 1
Month = *
Day of Week = *

Receiving email alerts

Email alerts may be sent based on conditions that you configure in the Alerts module. To enable an alert go to the Alerts section for the desired scan. Next, enable alerts by clicking the desired checkbox(es) setting alert conditions (if available), delivery address and message settings. Upon the next run of scan, for each alert condition that is met an email alert will be sent.

Note

Before enabling email alerts ensure that you have defined SMTP server settings in Settings > Email.

Figure 17

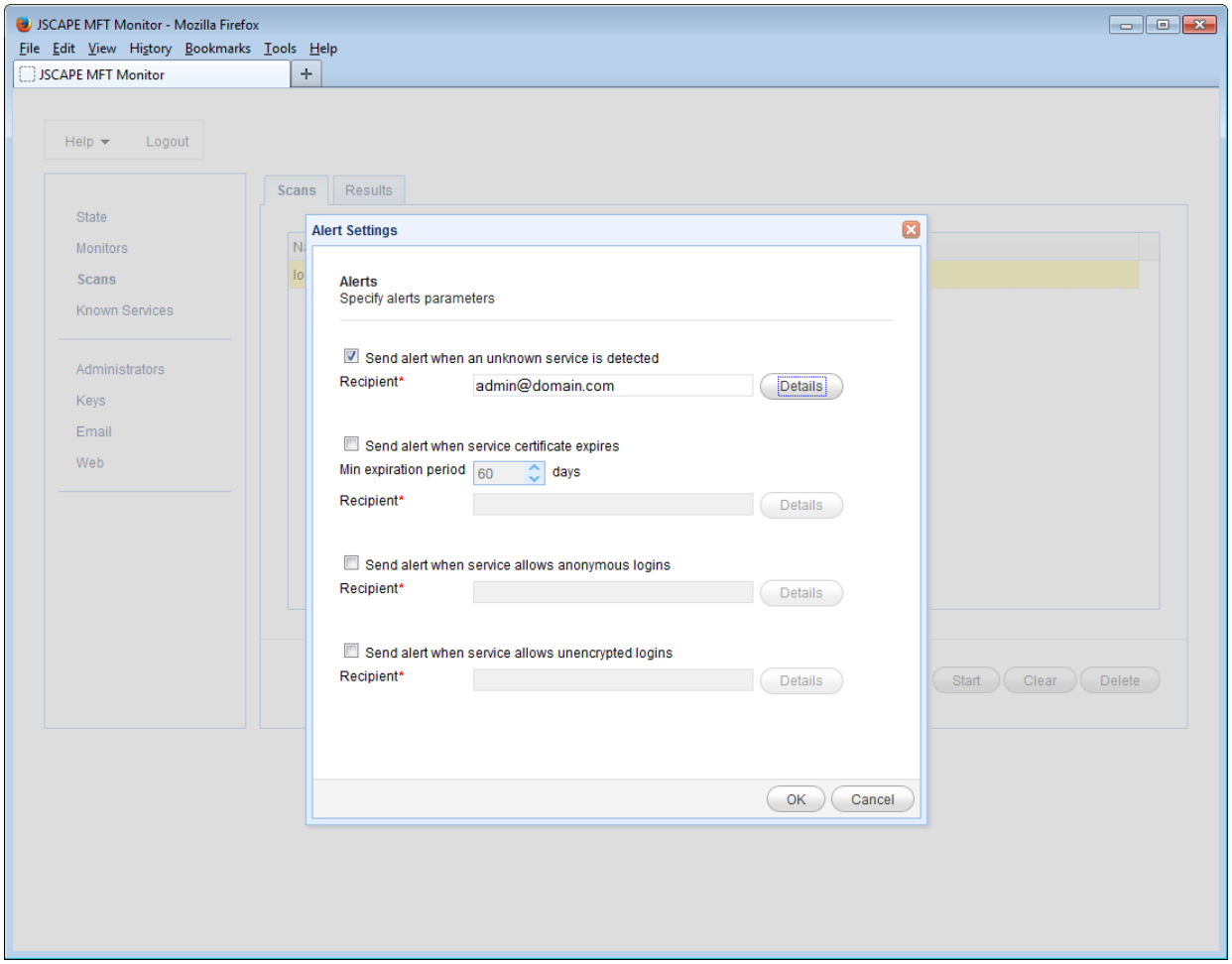
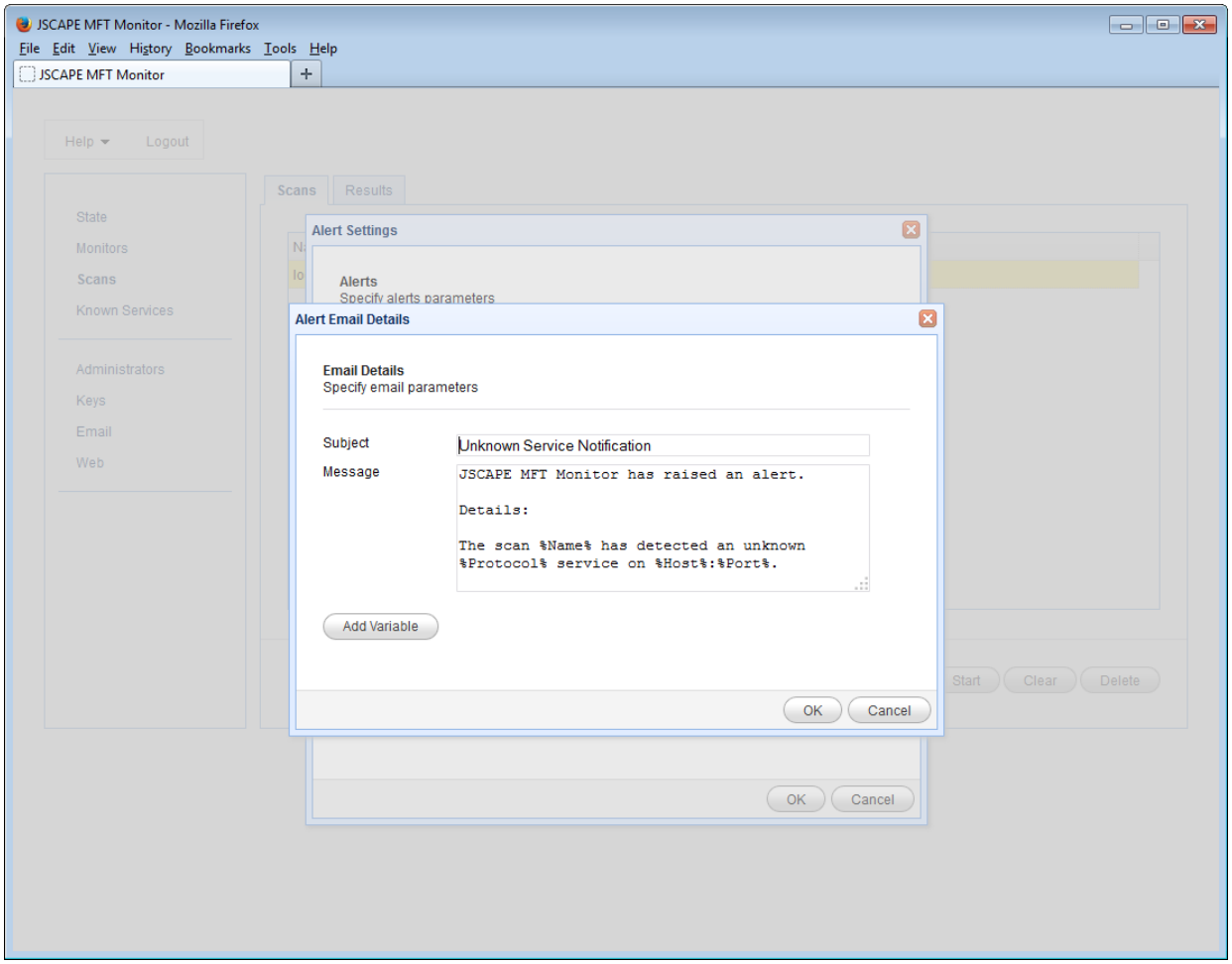

JSCAPE MFT Monitor - Mozilla Firefox
File Edit View History Bookmarks Tools Help
JSCAPE MFT Monitor
Help
Logout
State
Monitors
Scans
Known Services
Administrators
Keys
Email
Web
Scans
Results
Start
Clear
Delete
Alert Settings
Alerts
Specify alerts parameters
Send alert when an unknown service is detected
Recipient*
admin@domain.com
Details
Send alert when service certificate expires
Min expiration period
60
days
Recipient*
Details
Send alert when service allows anonymous logins
Recipient*
Details
Send alert when service allows unencrypted logins
Recipient*
Details
OK
Cancel

Figure 18



See also

Settings > Email

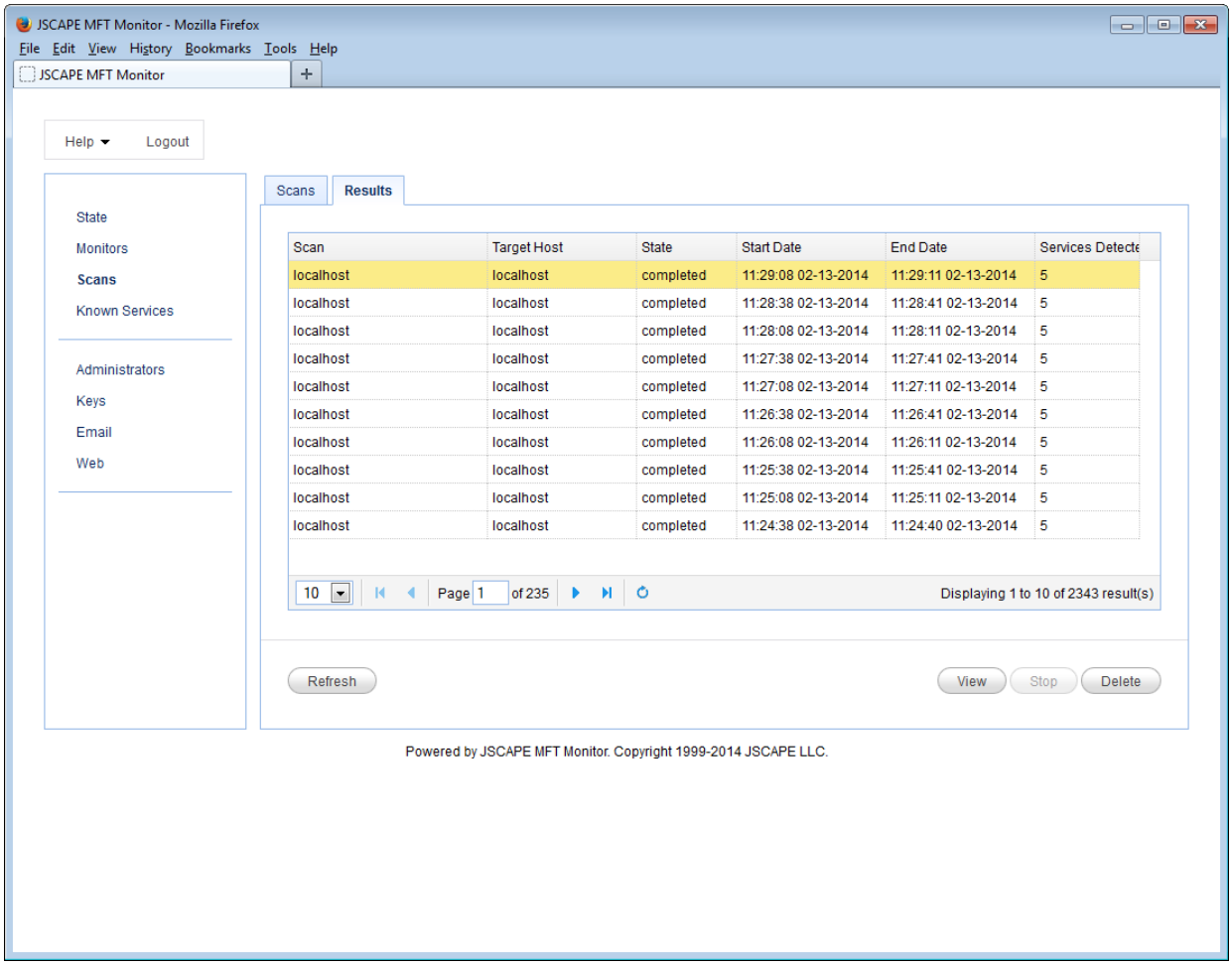
Viewing scan results

To view the session results for a scan, navigate to the Scans > Results page in JSCAPE MFT Monitor. To view the results of a session, select desired session and click the "View" button.

Summary

This panel displays a high level summary of the session including IP address, services scanned, number of hosts scanned and number of services detected.

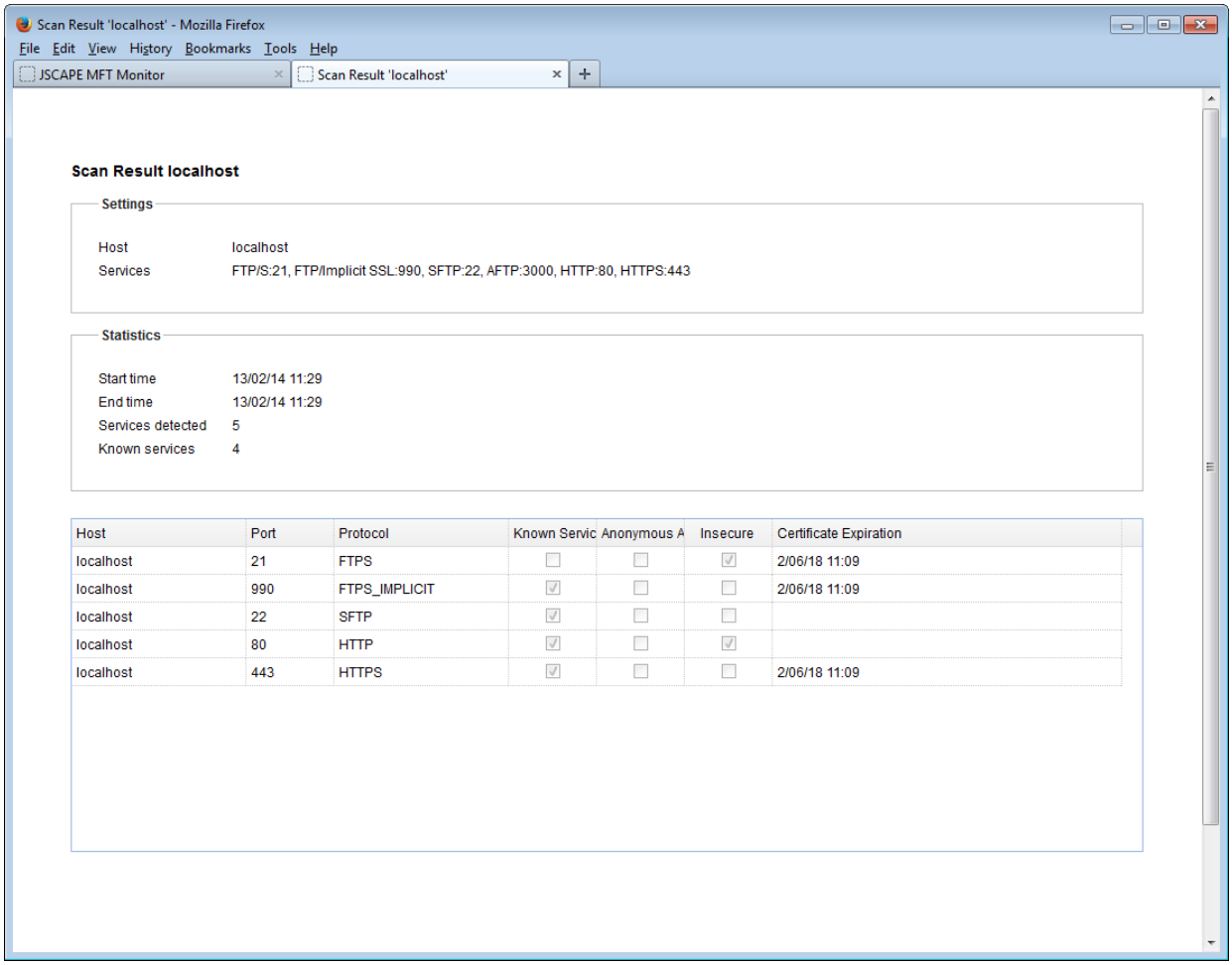
Figure 19



Hosts

This panel displays the services detected for the scan along with information about each service.

Figure 20



Host - The IP address that service is running on.

Port - The port that service is running on.

Protocol - The protocol that service is running.

Anonymous Access - If anonymous login is enabled. (FTP/S, SFTP)

Insecure - If non-encrypted login is allowed. (FTP/S)

Known Service - If Host/Port is a known service.

Certificate Expiration - Date of SSL certificate expiration. (MM/DD/YYYY)

See also

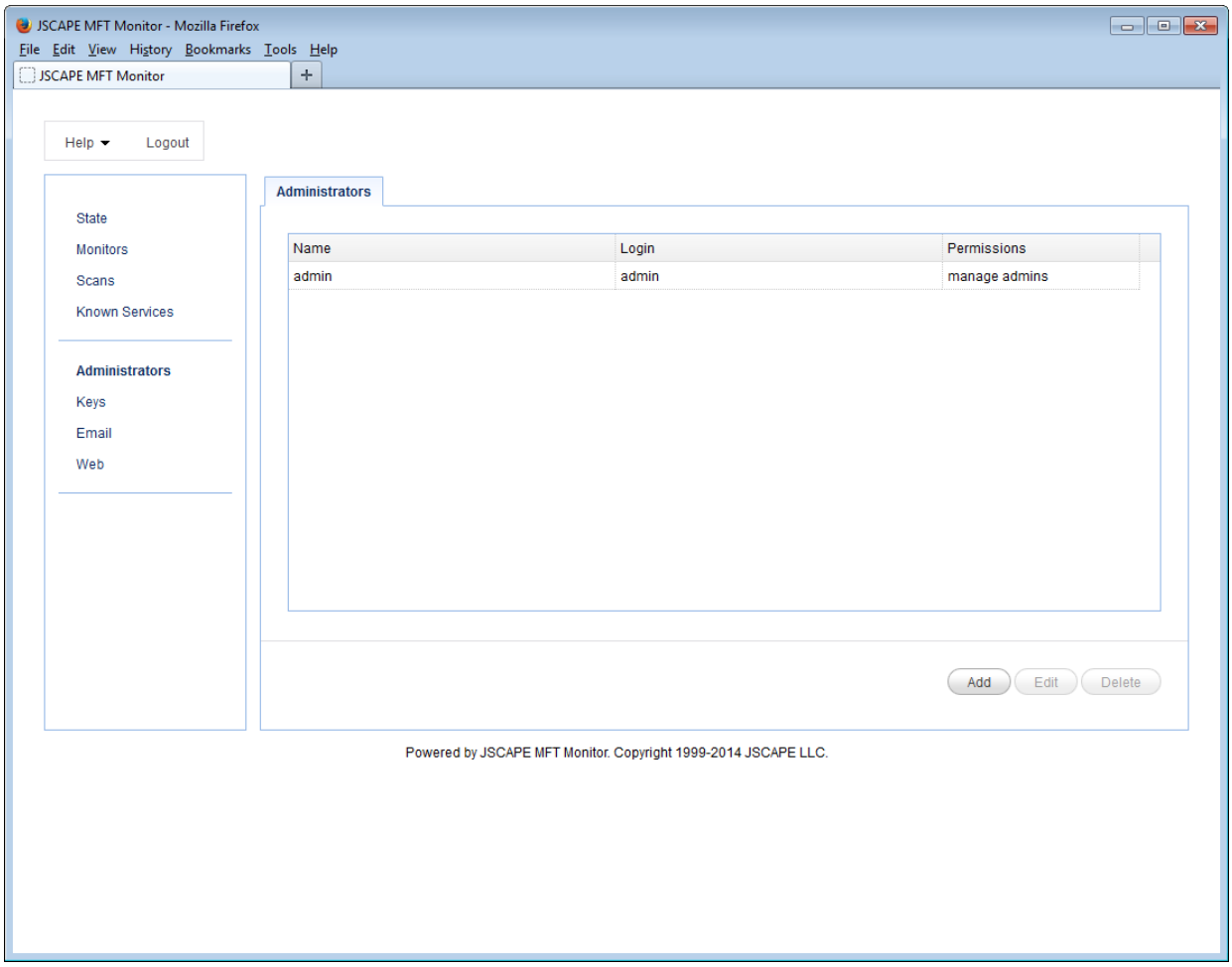
Settings > Known Services

Settings

Administrators

Administrators are users who may manage your instance of JSCAPE MFT Monitor from the web administrative interface. To add a new administrator navigate to the "Administrators" page and click on the "Add" button.

Figure 26



Name - The administrator's name.

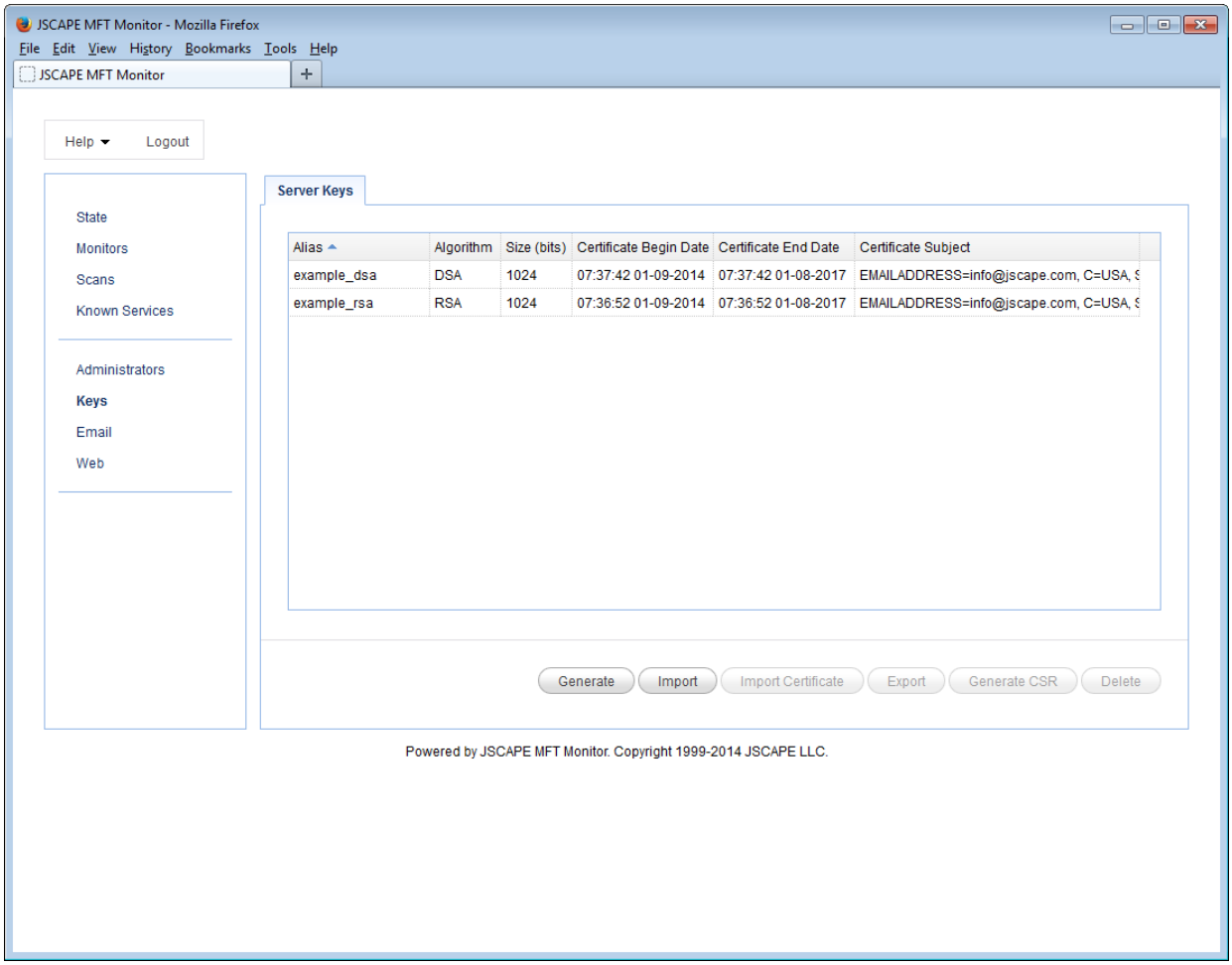
Login - The administrator's username.

Permissions - The administrator's permissions. Manage admins indicates that this administrator can manage other administrators.

Keys

The "Keys" module may be used for configuring SSL server keys and certificates to be used by the HTTPS web service. A pair of example keys have been provided for your convenience. You should create your own server keys when enabling HTTPS services.

Figure 27



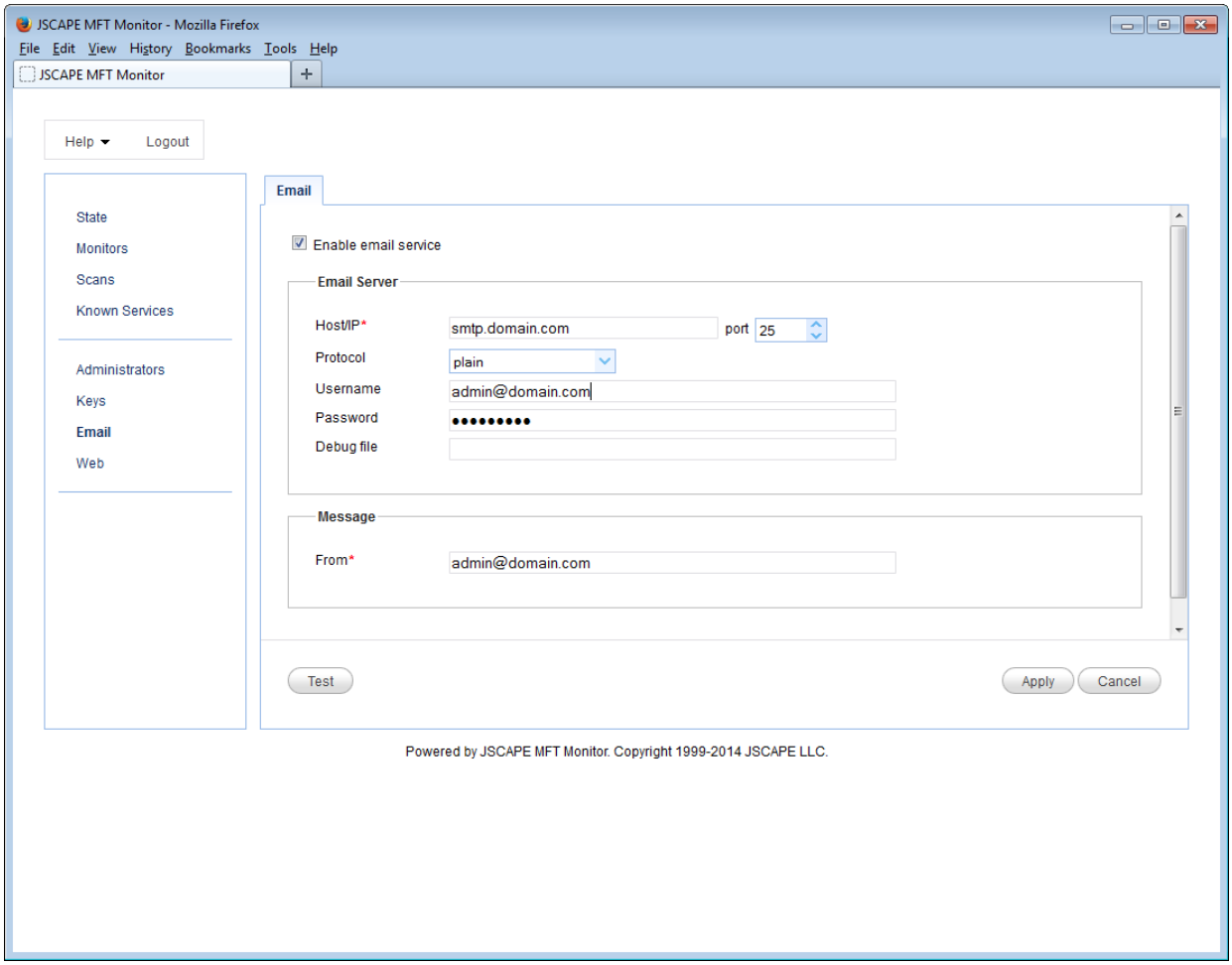
See also

Web

Email

The Email panel may be used to configure the SMTP server used for sending email alerts.

Figure 22



Email Server

Host/IP - The hostname or IP address of SMTP server.

Port - The port of SMTP server.

Protocol - The connection type to use when connecting to SMTP server. Supported types include plain, SSL and start TLS.

Username - The username used to authenticate against SMTP server.

Password - The password used to authenticate against SMTP server.

Debug file - The server side debug file to use when debugging SMTP server connections.

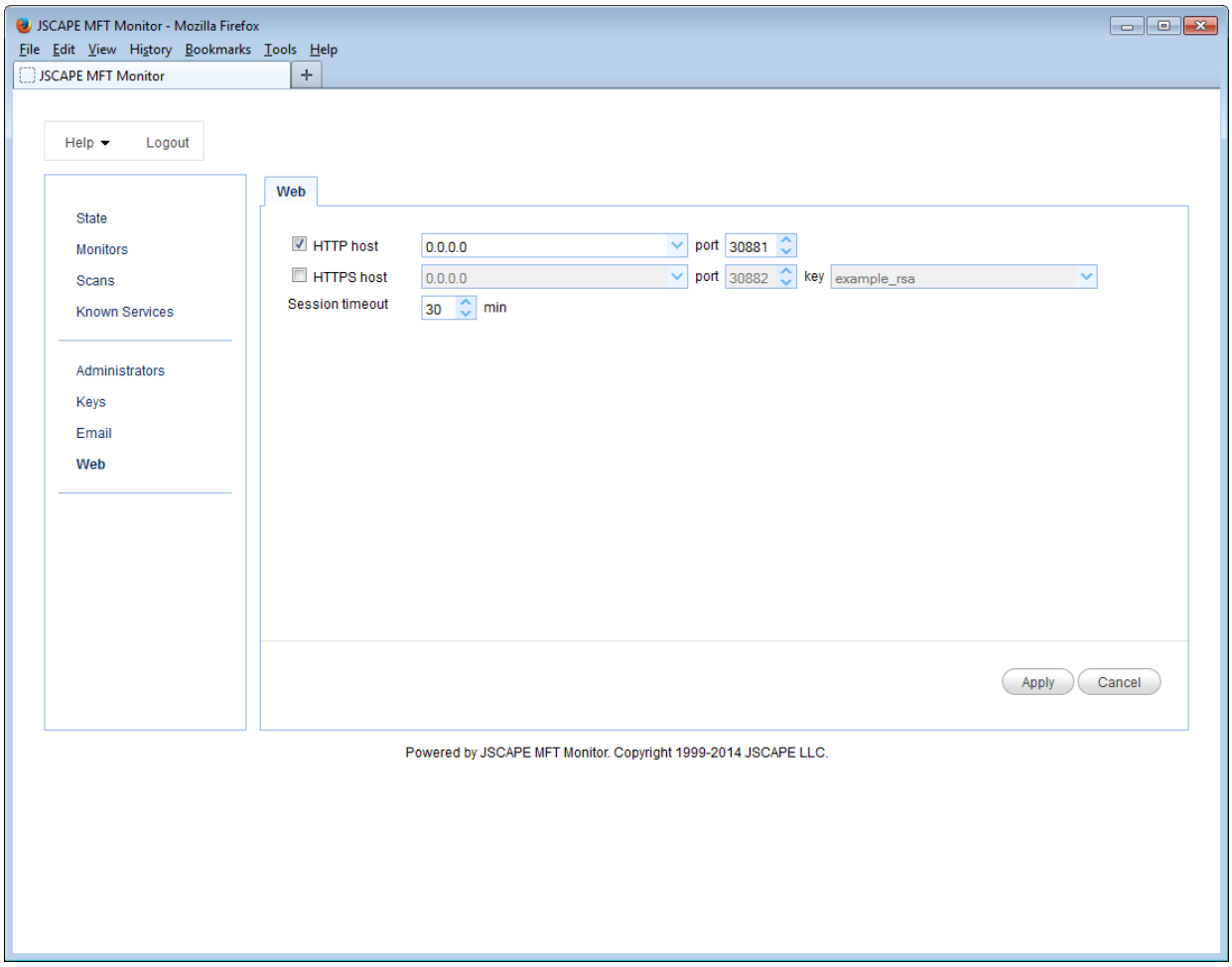
Message

From - The From address used when sending email alert.

Web

The "Web" module may be used to define the web based management service(s) for JSCAPE MFT Monitor.

Figure 28



HTTP host/port - The host and port combination for HTTP service.

HTTPS host/port - The host and port combination for HTTPS service.

Key - The server key used in encrypting HTTPS communications.

See also

Keys