



User's Guide

JSCAPE MFT Gateway

© 2016 JSCAPE LLC

Contents

Chapter 1	1 Introduction
	1 Overview
	1 Evaluation Edition limitations
	1 System requirements
	1 License
	3 Version history
Chapter 2	5 Installation
	5 Installation components
	6 Installing on Windows
	11 Installing on Linux
	14 Installing on Linux Z/OS
	14 Installing on Solaris
	15 Installing on AIX
	17 Installing on Mac OS X
	22 Auto-starting in Linux and Solaris 9 environments
	23 Auto-starting in Solaris 10 environments
	24 Running as non-root user in UNIX environments
	26 Running under IBM JVM
	26 Managing server remotely
Chapter 3	26 Server configuration
	26 Starting JSCAPE MFT Gateway Service
	27 Launching JSCAPE MFT Gateway Manager
	27 Adding proxy services
	30 Delegating network requests
	31 Setting logging preferences
	32 Setting health monitor preferences

Contents

	33	Monitoring HTTP/S services
	34	Viewing log data
	35	Setting IP based access
	36	Adding service clusters
	39	Setting URL rewrite rules
	44	Caching HTTP/S content
	45	Setting passive IP for FTP/S services
	46	Setting NAT host for HTTP/S services
Chapter 4	47	Key management
	47	Server keys
	47	Overview
	48	Generating a key
	50	Obtaining a trusted certificate
	52	Importing third party certificates
	53	Importing a key
	56	Exporting a certificate and/or public key
Chapter 5	57	Settings
	57	Administrator settings
	57	Web settings
	58	Email settings
	59	Control channel settings

Overview

JSCAPE MFT Gateway is a platform independent reverse proxy and load balancer server. JSCAPE MFT Gateway is optimized for use in the DMZ where it is placed in front of network services such as FTP/S (regular, implicit SSL, explicit SSL), SFTP/SSH/SCP and HTTP/S that are located on private internal networks. JSCAPE MFT Gateway is a perfect companion product to JSCAPE MFT Server offering a secure and high availability managed file transfer solution. In addition to the network protocols mentioned above, JSCAPE MFT Gateway may be used as a reverse proxy or load balancer to **any** TCP or UDP based protocol that does not require protocol translation.

Evaluation Edition limitations

The Evaluation Edition of JSCAPE MFT Gateway is fully functional offering all features found in the Enterprise Edition yet is limited to 5 concurrent connections.

Purchase JSCAPE MFT Gateway or submit a ticket to the Help Desk for licensing assistance.

System requirements

- Sun or IBM JVM (Java Virtual Machine) 1.6.x or above.
- Windows XP/2003/2008/2012/Vista/7, Mac OS 10.x, Solaris and Linux platforms.
- Recent versions (current, current -1) of Chrome, Firefox, Safari and IE web browsers.

License

JSCAPE MFT GATEWAY 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.

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 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.

ADDITIONAL LICENSE TERMS FOR SOFTWARE

ENTERPRISE EDITION

JSCAPE grants to you (either an individual or single entity) non-exclusive license to install and use a single instance of JSCAPE MFT Gateway Server on a single computer. JSCAPE MFT Gateway Agent, an agent for communicating with the control channel of JSCAPE MFT Gateway Server installation, may be installed on additional computers that you own without charge. If you wish to install multiple instances of JSCAPE MFT Gateway Server then a separate license MUST be purchased for each instance of JSCAPE MFT Gateway Server that is installed.

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 Delaware, 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

This Software incorporates various 3rd party libraries and open source software. These libraries and their respective license agreements may be found in the lib directory relative to the Software installation directory.

Version history

Version 3.3

Jun. 26, 2015

Enhancement: Added new service type HTTPS/HTTP which allows for proxying HTTPS connections to a target HTTP service.

Enhancement: Added ability to see connected agents from Control Channel module.

Improvement: Disabled Update, Start All and Stop All buttons in Services module when no services are listed.

Version 3.2

Sep. 25, 2014

Enhancement: Added dashboard for tracking threads, memory and connection statistics over time.

Enhancement: Added gateway.vmoptions file to define maximum memory allocation by JVM.

Version 3.1

Aug. 28, 2014

Enhancement: Added support for UDP services.

Version 3.0

Jun. 3, 2014

Enhancement: Added ability to delegate connections to registered agents.

Enhancement: Added numerous load balancing algorithms for use in clusters.
Enhancement: Added additional service types including SMTP, POP, MySQL and IMAP.
Enhancement: Added a health monitor that checks the availability of services and sends optional email notifications.
Enhancement: Added X-FORWARDED-FOR header to HTTP/S service requests.
Enhancement: Added content caching capabilities for HTTP/S protocols.
Enhancement: Various improvements to user interface.

Version 2.0

Dec. 9, 2013

Enhancement: Migrated from Java based to web based administrative user interface.

Version 1.8

Oct. 14, 2013

Enhancement: Added "IP binding time to live option" to cluster to control maximum amount of time remote IP are bound to client IP.
Enhancement: Added support for programmatic REST interface.
Enhancement: Added support for XCRC and MFMT commands in FTP/S protocols.
Bug Fix: Resolved performance issue in SFTP.

Version 1.7

Jun. 24, 2013

Enhancement: Added ability to ignore PASV/LPSV/EPSV IP in server response for FTP/S services.
Bug Fix: Resolved issue with CCC command for explicit and implicit FTPS services.
Bug Fix: Resolved issue with connecting to management service remotely on *NIX based installations.

Version 1.6

Sep. 7, 2012

Enhancement: Added ability to use a regular expression to exclude certain client IP addresses from using PASV IP address. This is useful in cases where internal FTP users using gateway should be treated differently than external users.
Bug Fix: Fixed issue where gateway would not properly detect that a server in a cluster was made unavailable.

Version 1.5

Apr. 27, 2012

Enhancement: Added ability to specify URL rewrite rules for HTTP/S protocols.
Enhancement: Added ability to specify NAT rewrite host address for HTTP/S protocols.
Bug Fix: Fixed issue transferring files and getting directory listings using FTPS in NAT environment.
Bug Fix: Fixed issue experienced when exchanging server keys between JSCAPE MFT Server and JSCAPE MFT Gateway.

Version 1.4

Feb. 22, 2012

Enhancement: Added support for exporting a private key from Key Manager.
Enhancement: Improved performance for processing HTTP/S requests.
Enhancement: Added support for URL rewriting when processing HTTP/S requests.
Bug Fix: Fixed issue with handling HTTP redirects.
Bug Fix: Fixed issues experienced when integrating with JSCAPE MFT Server HTTP/S services.

Version 1.3

Feb. 3, 2012

Enhancement: Replaced modal progress dialog with non-modal version so as to not interfere with other applications during long running processes.

Enhancement: Added support for HTTP redirects.

Update: Removed unused Client Keys tab from Key Manager.

Update: Removed ability to set SSL/TLS protocols used in FTPS and HTTPS services.

Bug Fix: Fixed issue when connecting to FTP/S services that utilized EPSV.

Bug Fix: Fixed issue when launching manager.html page where manager service was listening on 0.0.0.0 address.

Bug Fix: Removed unused "Remember current user" option from Settings > Connection panel.

Bug Fix: Fixed license key loading issue.

Bug Fix: Fixed issue with RAW clusters not recognized when creating a RAW service.

Bug Fix: Fixed issue with being able to import a private key.

Version 1.2

Jan. 14, 2012

Enhancement: Added support for multiple administrators.

Enhancement: Changed JSCAPE MFT Gateway Manager to be launched using Java WebStart via web interface.

Update: Changed product name from JSCAPE Reverse Proxy to JSCAPE MFT Gateway.

Bug Fix: Various bug fixes affecting SFTP and FTP/S protocols.

Version 1.1

Sep. 5, 2010

Enhancement: Added ability to rewrite absolute URL in HTTP content serviced by reverse proxy.

Enhancement: Added ability to set available ciphers for HTTPS service.

Enhancement: Added support for Windows 64 bit environment.

Version 1.0

Mar. 15, 2010

Initial release.

Installation components

JSCAPE MFT Gateway consists of two installable components which are JSCAPE MFT Gateway Server and JSCAPE MFT Gateway Agent. These components are described in more detail below.

JSCAPE MFT Gateway Server

This component is required and is typically installed on one or more servers in the DMZ in order to provide reverse proxy and clustering services.

JSCAPE MFT Gateway Agent

This component is optional and is typically installed on one or more servers within your internal network. It is generally **not installed on the same server** where the JSCAPE MFT Gateway Server component is installed as this would defeat its primary purpose. Its primary purpose is to perform network requests on behalf of JSCAPE MFT Gateway Server. While JSCAPE MFT Gateway Agent does establish an outbound connection to JSCAPE MFT Gateway Server via a control channel upon startup, no inbound connections

are ever made from JSCAPE MFT Gateway Server to JSCAPE MFT Gateway Agent. This is critical in environments where inbound connections to the internal network are restricted for security and/or compliance reasons.

Installing on Windows

Prior to installation it is recommended that you review the Installation components section to determine what components you will require. To install JSCAPE MFT Gateway on a Windows platform perform the following:

JSCAPE MFT Gateway Server

1. Download and run the `install.exe` installation file for JSCAPE MFT Gateway.
2. Installer launched. Click **Next** to continue.

Figure 36



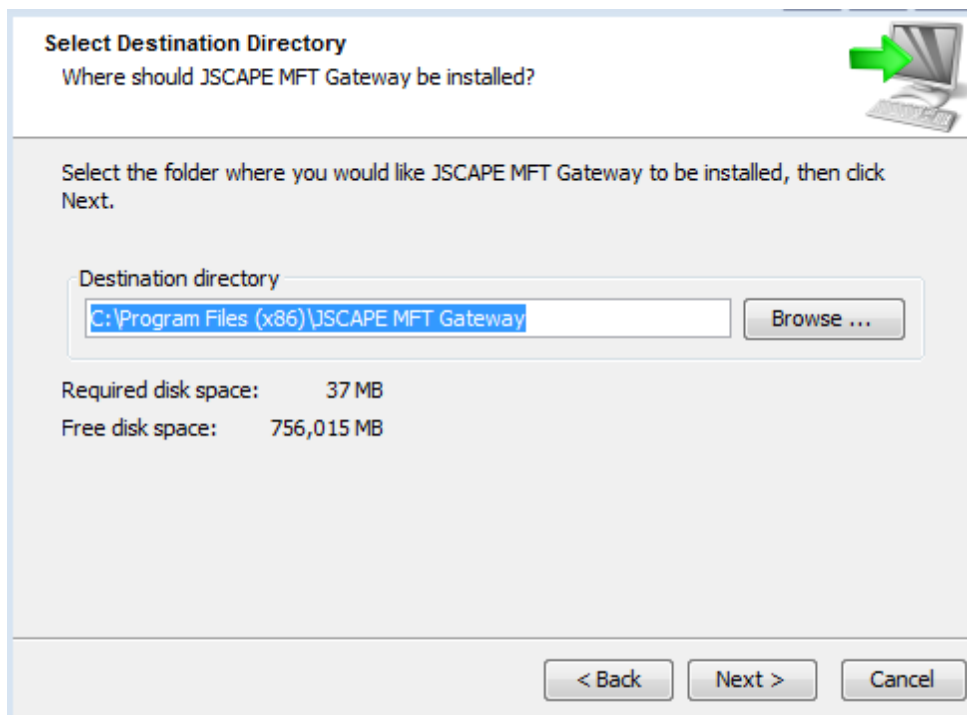
3. Review and accept License Agreement. Click **Next** to continue.

Figure 37



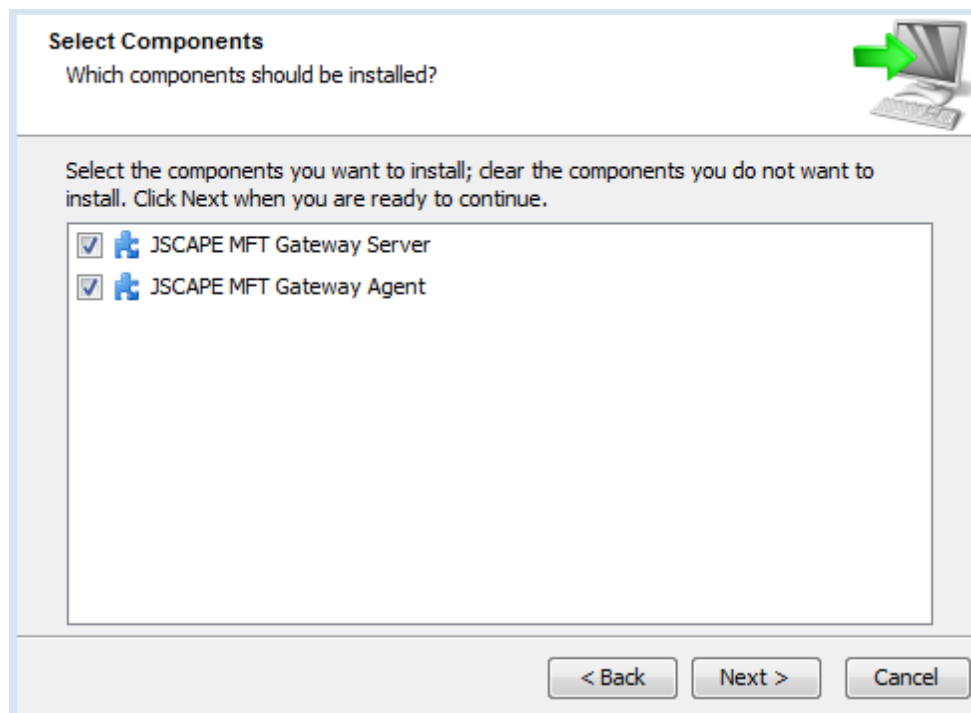
4. Select installation directory. Click **Next** to continue.

Figure 38



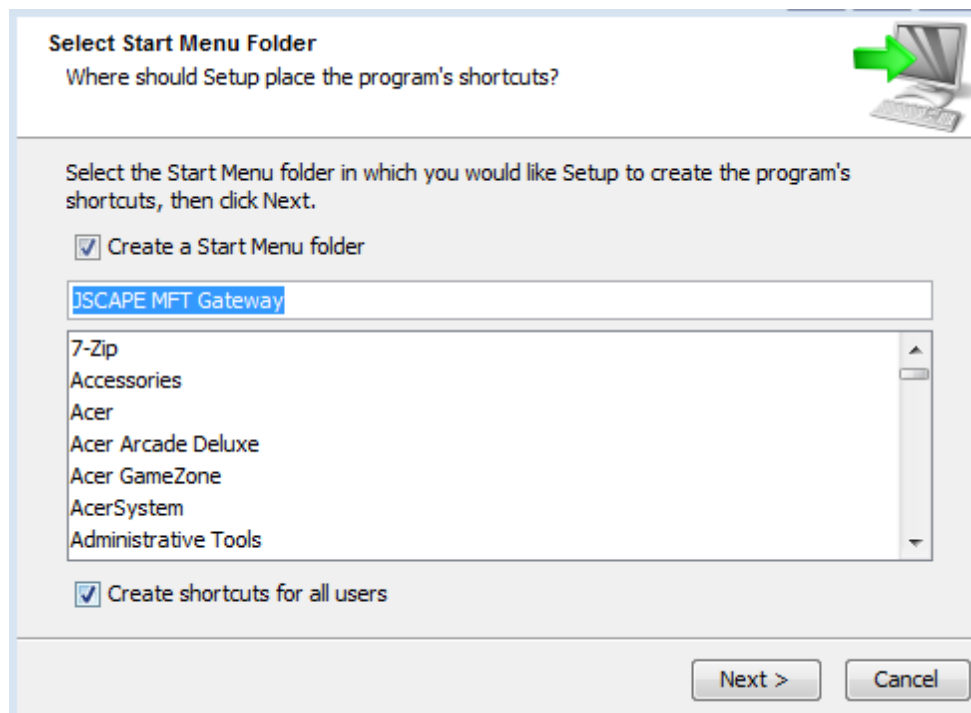
5. Select components to install. See Installation components for details. Click **Next** to continue.

Figure 39



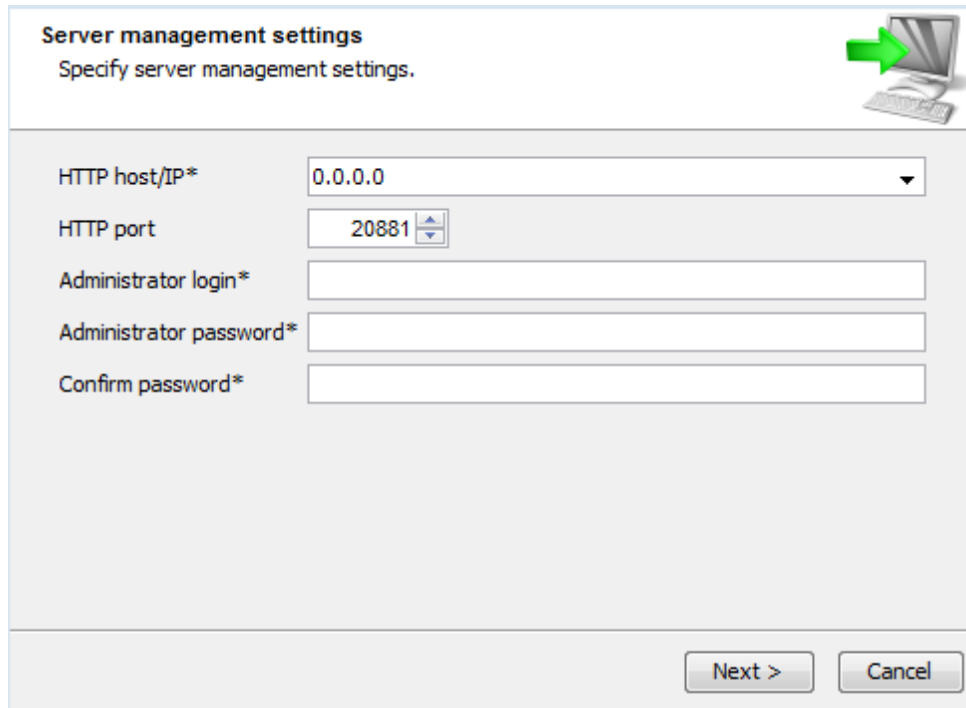
6. Select Start Menu Folder. Click **Next** to continue.

Figure 40



7. Set management server settings. This screen is displayed only if JSCAPE MFT Gateway Server component is installed. Click **Next** to continue.

Figure 41



Server management settings
Specify server management settings.

HTTP host/IP* 0.0.0.0

HTTP port 20881

Administrator login*

Administrator password*

Confirm password*

Next > Cancel

HTTP host/IP - The IP address that management server will listen on. The special address 0.0.0.0 is the default and typical configuration listening on all available IP addresses.

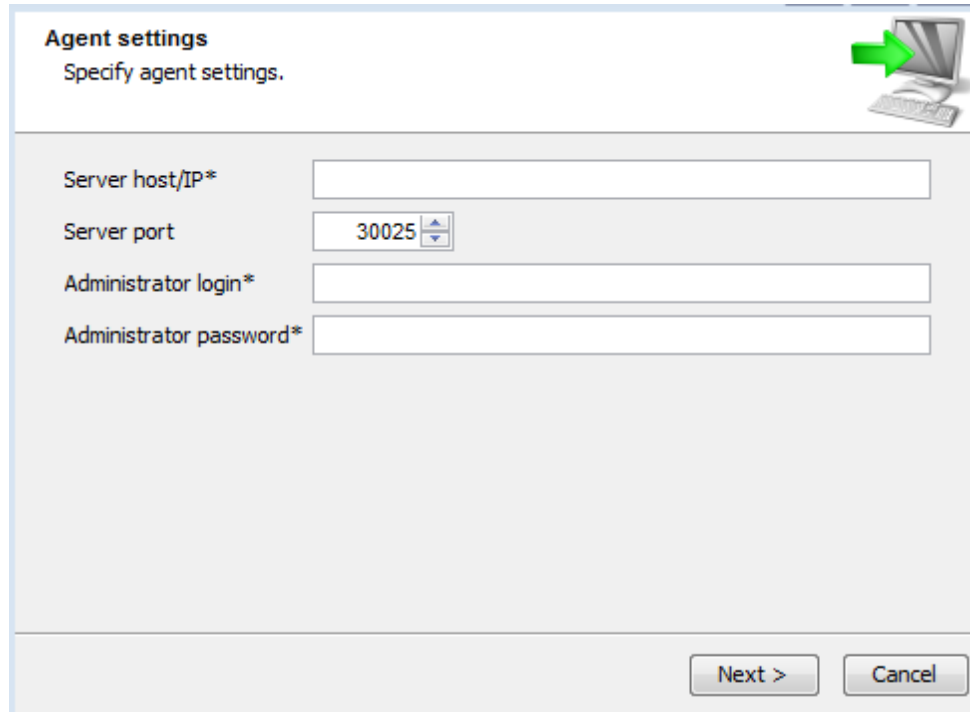
HTTP port - The port that management server will listen on.

Administrator login - The username to use for accessing management server.

Administrator password - The password to use for accessing management server.

8. Set agent connection settings. This screen is displayed only if JSCAPE MFT Gateway Agent component is installed. Click **Next** to continue.

Figure 42



The image shows a Windows-style dialog box titled "Agent settings" with the subtitle "Specify agent settings." In the top right corner, there is a green arrow pointing right towards a computer icon. The dialog contains four input fields: "Server host/IP*" (a text box), "Server port" (a spinner box set to 30025), "Administrator login*" (a text box), and "Administrator password*" (a text box). At the bottom right, there are two buttons: "Next >" and "Cancel".

Server host/IP - This is the IP address of JSCAPE MFT Gateway Server. Note, if you used special address of 0.0.0.0 when configuring JSCAPE MFT Gateway Server you must use an actual reachable IP address for this value instead of 0.0.0.0 as the address 0.0.0.0 is only valid for listening purposes.

Server port - This is the address that control channel for JSCAPE MFT Gateway Server is listening on. *
Note, by default the control channel is not enabled in JSCAPE MFT Gateway Server and must be configured separately after initial installation, after which the JSCAPE MFT Gateway Agent must be restarted. See Control channel settings for details.

Administrator login - The username to use for accessing management server.

Administrator password - The password to use for accessing management server.

9. Congratulations! You have successfully installed JSCAPE MFT Gateway. Click Finish to launch the web based administration application. See Launching JSCAPE MFT Gateway Manager for details.

Figure 43



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

See also

Launching JSCAPE MFT Gateway Manager

Installing on Linux

Prior to installation it is recommended that you review the Installation components section to determine what components you will require. Installation instructions for each component are provided below.

RPM Console Installation

JSCAPE MFT Gateway Server

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 -iv install.rpm
```

3. Add administrative user. Go to the `/opt/JSCAPE_MFT_Gateway` directory and run the following command:

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

For example:

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

This will configure JSCAPE MFT Gateway, where [username] and [password] are the administrative credentials you will use when connecting to the service.

4. **Startup Administration Service.** From the /opt/JSCAPE_MFT_Gateway directory run the following command:

```
./server start
```

JSCAPE MFT Gateway Agent

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 -iv install.rpm
```

3. Enable control channel for JSCAPE MFT Gateway Server. See Control channel settings for details.

4. **Set agent connection settings.** From the /opt/JSCAPE_MFT_Gateway directory run the following command:

```
./agent-configuration -host [ip] -port [port] -user [username] -pwd [password]
```

For example:

```
./agent-configuration -host 10.0.0.1 -port 30025 -user admin -pwd secret
```

This will configure JSCAPE MFT Gateway Agent, where [ip] and [port] are the control channel IP and port for JSCAPE MFT Gateway Server and [username] and [password] are administrative credentials you will use when connecting to the control channel.

5. **Startup JSCAPE MFT Gateway Agent Service.** From the JSCAPE MFT Gateway installation directory run the following command:

```
./agent start
```

ZIP Console Installation

JSCAPE MFT Gateway Server

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. **Add administrative user.** Go to the JSCAPE MFT Gateway installation 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 JSCAPE MFT Gateway, where [username] and [password] are the administrative credentials you will use when connecting to the service.

4. Startup JSCAPE MFT Gateway Service. From the JSCAPE MFT Gateway installation directory run the following command:

```
./server start
```

JSCAPE MFT Gateway Agent

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. Enable control channel for JSCAPE MFT Gateway Server. See Control channel settings for details.
4. Set agent connection settings. Go to the JSCAPE MFT Gateway installation directory relative to where the `unzip` command was executed, and run the following command:

```
./agent-configuration -host [ip] -port [port] -user [username] -pwd [password]
```

For example:

```
./agent-configuration -host 10.0.0.1 -port 30025 -user admin -pwd secret
```

This will configure JSCAPE MFT Gateway Agent, where [ip] and [port] are the control channel IP and port for JSCAPE MFT Gateway Server and [username] and [password] are administrative credentials you will use when connecting to the control channel.

5. Startup JSCAPE MFT Gateway Agent Service. From the JSCAPE MFT Gateway installation directory run the following command:

```
./agent start
```

See also

Launching JSCAPE MFT Gateway Manager

Installing on Linux Z/OS

See also

Running under IBM JVM

Installing on Linux

Installing on Solaris

Prior to installation it is recommended that you review the Installation components section to determine what components you will require. Installation instructions for each component are provided below.

ZIP Console Installation

To install using the ZIP file perform the following steps as a user with root privileges. If you plan on running JSCAPE MFT Gateway as a non-root user under Solaris 10 or above, please consult the topic Auto-starting in Solaris 10 environments topic before continuing.

JSCAPE MFT Gateway Server

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. Add administrative user. Go to the JSCAPE MFT Gateway installation 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 JSCAPE MFT Gateway, where `[username]` and `[password]` are the administrative credentials you will use when connecting to the service.

4. Startup JSCAPE MFT Gateway Service. If you are auto-starting using an SMF script you may skip this step. From the JSCAPE MFT Gateway installation directory run the following command:

```
./server start
```

JSCAPE MFT Gateway Agent

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. Enable control channel for JSCAPE MFT Gateway Server. See Control channel settings for details.
4. Set agent connection settings. Go to the JSCAPE MFT Gateway installation directory relative to where

the unzip command was executed, and run the following command:

```
./agent-configuration -host [ip] -port [port] -user [username] -pwd [password]
```

For example:

```
./agent-configuration -host 10.0.0.1 -port 30025 -user admin -pwd secret
```

This will configure JSCAPE MFT Gateway Agent, where [ip] and [port] are the control channel IP and port for JSCAPE MFT Gateway Server and [username] and [password] are administrative credentials you will use when connecting to the control channel.

5. Startup JSCAPE MFT Gateway Agent Service. From the JSCAPE MFT Gateway installation directory run the following command:

```
./agent start
```

See also

Launching JSCAPE MFT Gateway Manager

Installing on AIX

Prior to installation it is recommended that you review the Installation components section to determine what components you will require.

ZIP Console Installation

JSCAPE MFT Gateway Server

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

1. Place the `install.zip` file in a directory on the destination server.
2. Install. Run the following commands from the directory containing the ZIP file you placed on your server:

```
unzip install.zip
```

3. AIX systems are typically configured to run the IBM JVM, therefore it is necessary to make some changes to the `etc/ssl.cfg` file in order to instruct the JVM on what security provider and encryption algorithm to use for starting up the JSCAPE MFT Gateway Service. See Running under IBM JVM for

complete details and instructions.

4. Add administrative user. Go to the JSCAPE MFT Gateway installation directory relative to where the `tar` 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 JSCAPE MFT Gateway, where `[username]` and `[password]` are the administrative credentials you will use when connecting to the service.

5. Startup Administration Service. From the JSCAPE MFT Gateway installation directory run the following command:

```
./server start
```

JSCAPE MFT Gateway Agent

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. AIX systems are typically configured to run the IBM JVM, therefore it is necessary to make some changes to the `etc/ssl.cfg` file in order to instruct the JVM on what security provider and encryption algorithm to use for starting up the JSCAPE MFT Gateway Service. See *Running under IBM JVM* for complete details and instructions.

4. Enable control channel for JSCAPE MFT Gateway Server. See *Control channel settings* for details.

5. Set agent connection settings. Go to the JSCAPE MFT Gateway installation directory relative to where the `unzip` command was executed, and run the following command:

```
./agent-configuration -host [ip] -port [port] -user [username] -pwd [password]
```

For example:

```
./agent-configuration -host 10.0.0.1 -port 30025 -user admin -pwd secret
```

This will configure JSCAPE MFT Gateway Agent, where `[ip]` and `[port]` are the control channel IP and port for JSCAPE MFT Gateway Server and `[username]` and `[password]` are administrative credentials you will use when connecting to the control channel.

6. Startup JSCAPE MFT Gateway Agent Service. From the JSCAPE MFT Gateway installation directory run the following command:

```
./agent start
```

See also

Launching JSCAPE MFT Gateway Manager

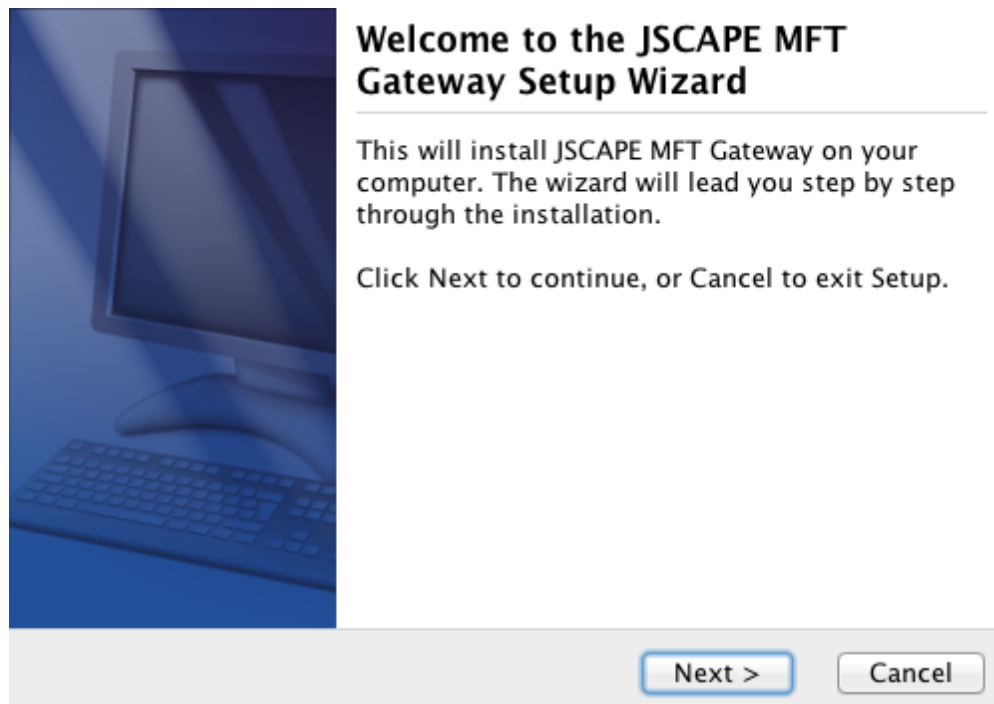
Installing on Mac OS X

Prior to installation it is recommended that you review the Installation components section to determine what components you will require. To install JSCAPE MFT Gateway on a Mac OS X platform perform the following:

JSCAPE MFT Gateway Server

1. Download and run the `install.dmg` installation file for JSCAPE MFT Gateway.
2. Installer launched. Click `Next` to continue.

Figure 44



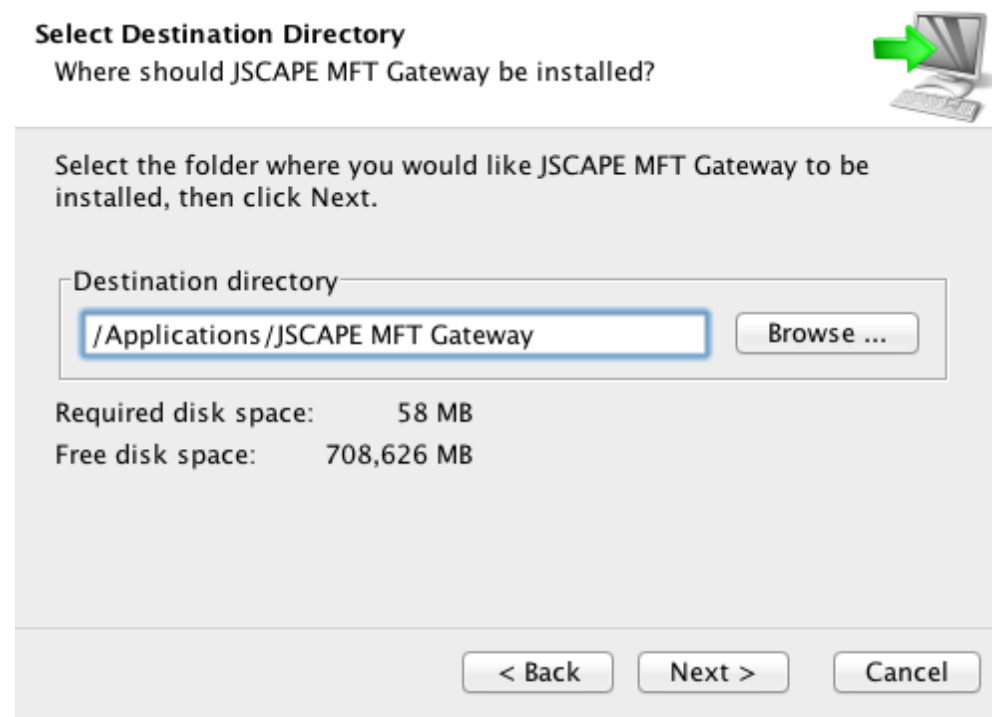
3. Review and accept License Agreement. Click `Next` to continue.

Figure 45



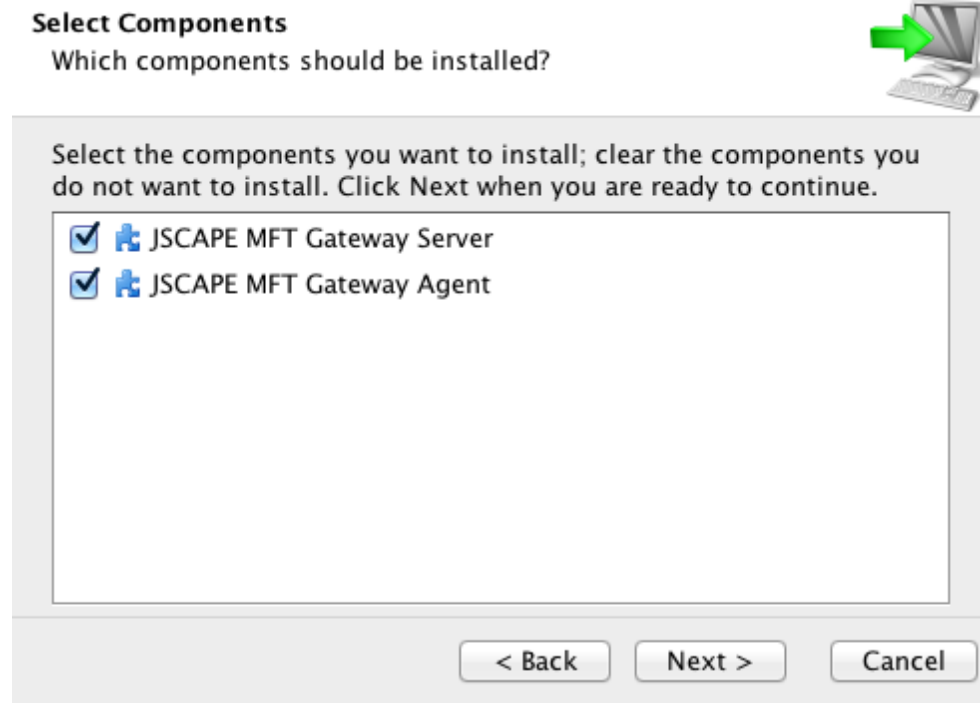
4. Select installation directory. Click **Next** to continue.

Figure 46



5. Select components to install. See Installation components for details. Click **Next** to continue.


Figure 47



6. Set management server settings. This screen is displayed only if JSCAPE MFT Gateway Server component is installed. Click **Next** to continue.

Figure 48

Server management settings
Specify server management settings.



HTTP host/IP*	<input type="text" value="0.0.0.0"/>
HTTP port	<input type="text" value="20881"/>
Administrator login*	<input type="text"/>
Administrator password*	<input type="password"/>
Confirm password*	<input type="password"/>

HTTP host/IP - The IP address that management server will listen on. The special address 0.0.0.0 is the default and typical configuration listening on all available IP addresses.

HTTP port - The port that management server will listen on.


Administrator login - The username to use for accessing management server.

Administrator password - The password to use for accessing management server.

7. Set agent connection settings. This screen is displayed only if JSCAPE MFT Gateway Agent component is installed. Click **Next** to continue.

Figure 49

Agent settings
Specify agent settings.



Server host/IP*	<input type="text"/>
Server port	<input type="text" value="30025"/> <input type="button" value="↑"/> <input type="button" value="↓"/>
Administrator login*	<input type="text"/>
Administrator password*	<input type="password"/>

Next > Cancel

Server host/IP - This is the IP address of JSCAPE MFT Gateway Server. Note, if you used special address of 0.0.0.0 when configuring JSCAPE MFT Gateway Server you must use an actual reachable IP address for this value instead of 0.0.0.0 as the address 0.0.0.0 is only valid for listening purposes.

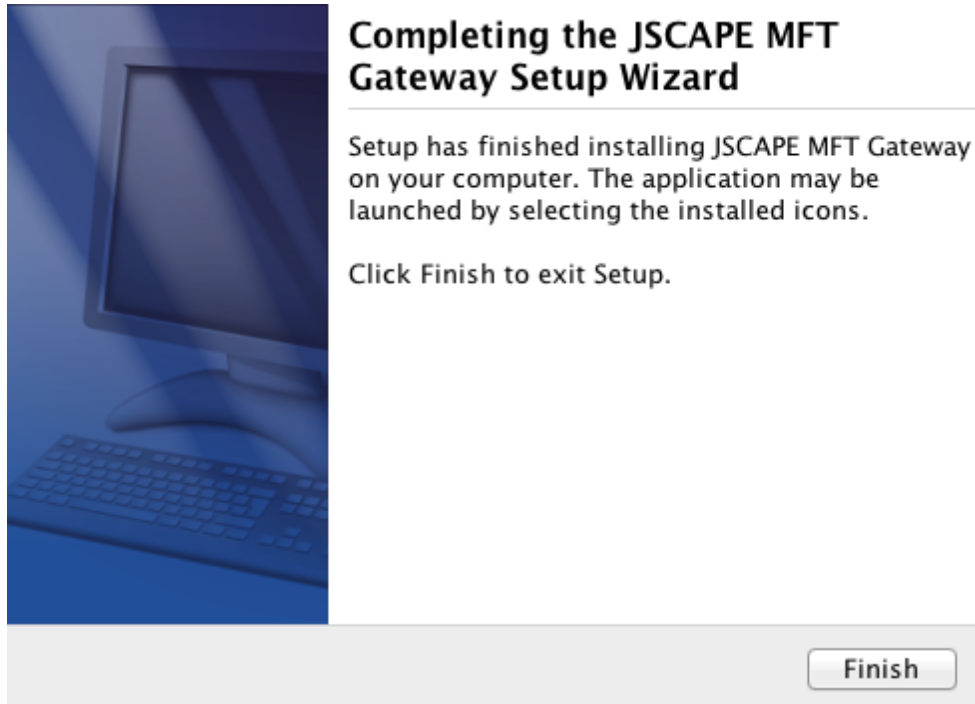
Server port - This is the address that control channel for JSCAPE MFT Gateway Server is listening on. *
Note, by default the control channel is not enabled in JSCAPE MFT Gateway Server and must be configured separately after initial installation, after which the JSCAPE MFT Gateway Agent must be restarted. See Control channel settings for details.

Administrator login - The username to use for accessing management server.

Administrator password - The password to use for accessing management server.

8. Congratulations! You have successfully installed JSCAPE MFT Gateway. Click Finish to launch the web based administration application. See Launching JSCAPE MFT Gateway Manager for details.

Figure 50



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

10. In order to have service start automatically upon system reboot edit the `/Library/LaunchDaemons/com.j scape.MFTGateway.plist` file and set the value for the `OnDemand` parameter to `false`.

See also

Launching JSCAPE MFT Gateway Manager

Auto-starting in Linux and Solaris 9 environments

For Linux and Solaris 9 environments you may have the JSCAPE MFT Gateway Service start up automatically during system startup by creating a service configuration file for JSCAPE MFT Gateway Service and placing it in your `/etc/init.d` directory. This same configuration file will be used for gracefully stopping the JSCAPE MFT Gateway Service when shutting down the system. A sample service configuration file, `gateway`, has been placed in the `init.d` directory of your JSCAPE MFT Gateway installation.

Installing the service configuration file

1. As `root` user, copy the `gateway` sample service configuration file to your `/etc/init.d` directory.
2. Grant execute permissions to this file using the command `chmod 755 gateway`
3. Using a text editor, change the value of the `INSTALL_DIR` variable to the absolute path of your JSCAPE MFT Gateway installation directory. The default value for the `INSTALL_DIR` variable is `/opt/JSCAPE_MFT_Gateway` which is consistent with Linux RPM installations. Your installation directory may

vary.

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

Linux

```
/sbin/chkconfig --add gateway
```

Solaris 9

```
ln /etc/init.d/mftgateway /etc/rc3.d/Sxxgateway
```

```
ln /etc/init.d/mftgateway /etc/rc0.d/Kxxgateway
```

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 gateway defaults
```

Starting the service

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

Stopping the service

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

Restarting the service

From the `/etc/init.d` directory and as root user run the command `./gateway 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 Gateway as a service perform the following.

1. As root user, create a user and group named `mftgateway`.
2. As root user, run the command `usermod -K defaultpriv=basic,net_privaddr mftgateway` to grant `mftgateway` user permissions to run services on ports less than 1024.
3. As `mftgateway` user, run installer for Solaris as described in Installing on Solaris.
4. Open the sample SMF manifest file `gateway_smf.xml` found in the JSCAPE MFT Gateway installation directory using `vi` or other text editor.
5. Change references to `/opt/JSCAPE_MFT_Gateway` with the absolute path of JSCAPE MFT Gateway installation directory.
6. As root user, validate SMF manifest file using `svccfg validate gateway_smf.xml` command.
7. As root user, import SMF manifest file using `svccfg import gateway_smf.xml` command.

8. As `root` user, enable service using `svcadm enable svc:/application/mftgateway:default` command.
9. Check that service was started successfully and not in maintenance using `svcs -x mftgateway:default` command.
10. Verify that JSCAPE MFT Gateway Service is running using `netstat -na | grep 20881` 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>

Running as non-root user in UNIX environments

Solaris 10 and above systems

If you are running under Solaris 10 or above then you may run as non-root using the provided example SMF script. Please see the following topic for details.

Auto-starting in Solaris 10 environments

Solaris 9 and Linux/UNIX systems

The simplest method for installing and running JSCAPE MFT Gateway is to do so as the `root` user. However in some UNIX based environments you may want or need to run JSCAPE MFT Gateway as a user other than `root`. Should you decide to go this route there are certain issues to consider when installing and configuring JSCAPE MFT Gateway.

Filesystem permissions

When running JSCAPE MFT Gateway as a non-root system user ensure that this user is granted full access to the JSCAPE MFT Gateway installation directory and all sub-directories.

Port redirection

As a general rule, UNIX based (Linux, Solaris, Mac OS X) programs that bind to ports less than 1024 must be run as root user. For example, the standard port for FTP is port 21 requiring that you run JSCAPE MFT Gateway as `root` user in order to bind and listen on this port for incoming requests. One solution that gets you around this restriction is to have your server run on ports > 1024. For example, you might set your reverse proxy FTP service to run on port 2121 instead of port 21 in order to be able to run JSCAPE MFT Gateway as a non-root user. There may however be a case where you want to be able to run JSCAPE MFT Gateway as a non-root user while also using ports less than 1024. The two methods available are Port redirection using `xinetd` and Port redirection using `iptables` which are discussed below.

Port redirection using xinetd

The `xinetd` Internet service daemon is installed on most UNIX based systems and offers a feature that allows for port redirection. Using this port redirection feature you could for example redirect incoming requests on port 21 to port 2121 thus allowing you to run your reverse proxy FTP service as a non-root user on port 2121 while still being able to accept redirected requests from port 21. To setup `xinetd` to perform

this redirection go to your `/etc/xinetd.d` directory and create a new service configuration file named `mftgateway` (as root user) the contents of which are displayed below.

```
# Redirects any requests on port 21

# to port 2121 (where JSCAPE MFT Gateway is listening)

service mftgateway

{
    socket_type      = stream

    protocol        = tcp

    user            = root

    wait            = no

    port            = 21

    redirect         = localhost 2121

    disable         = no
}
```

Next you will need to restart the `xinetd` service to load this service. On most UNIX based systems this can be done by issuing the following command.

```
/sbin/service xinetd restart
```

You will now be able to accept requests on port 21 which are then redirected to your listening port of 2121. By leaving the `mftgateway` service configuration file in the `/etc/xinetd.d` directory this redirection will automatically take place whenever you restart your system.

Port redirection using iptables

A solution available in systems running Linux kernel 2.4 and above is to use `iptables`. `iptables` offers the same approach as `xinetd` but with less process overhead since `iptables` is compiled into the kernel rather than running as a separate process. To see if `iptables` is running on your system run the following command as root user.

```
/sbin/service iptables status
```

If it is running you will see a list of tables displayed to the console.

Using our original example, create a new redirection rule that will redirect incoming requests on port 21 to port 2121 by issuing the following command as root user.

```
/sbin/iptables -t nat -A PREROUTING -j REDIRECT -p tcp --destination-port 21:21 --to-ports 2121
```

This will redirect port requests until you restart your system. To ensure that this rule is used after a

system restart save the rule by issuing the following command as `root` user.

```
/sbin/service iptables save
```

See also

Auto-starting in Linux and Solaris 9 environments

Auto-starting in Solaris 10 environments

Running under IBM JVM

For systems configured to run using the IBM JVM it is necessary to make some changes to the `etc/ssl.cfg` file in order to instruct the JVM on what security provider and encryption algorithm to use for starting up the JSCAPE MFT Gateway Service. Using a text editor, update the `etc/ssl.cfg` file as follows.

IBM JVM 1.6 and above

```
algorithm=IbmX509
provider=IBMJSSE2
```

Upon saving changes to this file restart the JSCAPE MFT Gateway Service so the changes may take effect.

Managing server remotely

JSCAPE MFT Gateway may be managed locally or remotely via the web based administrative interface. To launch JSCAPE MFT Gateway Manager open your web browser and type in the following URL:

```
http://host:port
```

Where `host` and `port` are the HTTP host/IP and HTTP port that you used during the installation process. If you used the host/IP of `0.0.0.0` then any valid IP address on the machine that the software was installed on may be used.

Starting JSCAPE MFT Gateway Service

In order to manage JSCAPE MFT Gateway you must first start the JSCAPE MFT Gateway Service. This service allows you to manage the JSCAPE MFT Gateway using your web browser.

Windows

You may start the service by going to your `Control Panel > Administrative Tools > Services` and starting the JSCAPE MFT Gateway service. Alternatively you may start the service from the JSCAPE MFT Gateway program group by clicking on `Administrative Tools > Start Service`.

Linux / UNIX / Mac OS X

Go to the JSCAPE MFT Gateway installation directory. For Linux RPM installations this is `/opt/JSCAPE_MFT_Gateway`. For UNIX and non-RPM Linux installations this is the directory that you selected during installation. To start the JSCAPE MFT Gateway Service run the following command as a user with super-user (e.g. `root`) privileges:

```
./start_service.sh
```

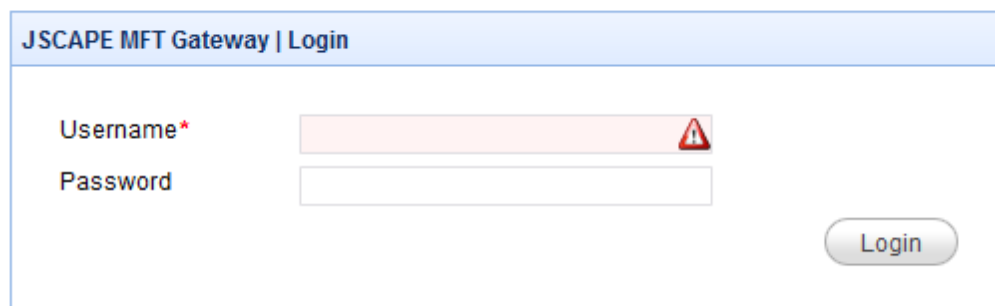
Launching JSCAPE MFT Gateway Manager

JSCAPE MFT Gateway may be managed locally or remotely via the web based administrative interface. To launch JSCAPE MFT Gateway Manager open your web browser and type in the following URL:

http://host:port

Where host and port are the HTTP host/IP and HTTP port that you used during the installation process. If you used a console based installer (e.g. Linux, Solaris) then the default port is 20881. If you used the host/IP of 0.0.0.0 then any valid IP address on the machine that the software was installed on may be used. Enter the administrative credentials that were used during the installation process and click `Login` to continue.

Figure 1

The image shows a web-based login form for JSCAPE MFT Gateway. The form has a light blue header bar with the text "JSCAPE MFT Gateway | Login". Below the header, there are two input fields: "Username*" and "Password". The "Username*" field has a red warning icon to its right. To the right of the "Password" field is a "Login" button. The form is enclosed in a light blue border.

Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.

Adding proxy services

A reverse proxy service is an IP/Host, Port and Protocol combination that accepts client FTP/S, TCP (e.g. SFTP) or HTTP/S connection requests. To view existing reverse proxy services click on the `Services` node. A list of services are displayed.

Figure 2

Help Logout

State

Services

Clusters

IP Access

Logging

Health Monitor

Administrators

Keys

Email

Web

Control Channel

Services FTP/S TCP HTTP/S

Protocol	Local Host	Local Port	Remote Address / Cluster	Agent Delegation	State	Uptime	Current Connections	Total Connections
FTP	0.0.0.0	2121	10.0.0.8:21	non-delegated	running	3 sec.	0	0

Update

Start All

Stop All

Add

Start

Stop

Delete

Powered by JScape MFT Gateway. Copyright 1999-2014 JScape LLC.

Protocol - The protocol used. See Protocol types.

Local Host - The local IP that connections are accepted on.

Local Port - The local port that connections are accepted on.

Remote Address / Cluster - The remote host:port or cluster that connections are forwarded to.

Agent Delegation - Indicates whether connections are delegated to listening agents or handled by gateway directly.

State - The state of service (running, stopped).

Uptime - The total uptime since service start.

Current Connections - The current number of active connections.

Total Connections - The total number of connections since service start.

Protocol types

FTP - Forwards standard unencrypted FTP connections.

FTPS - Forwards both standard unencrypted FTP connections and encrypted explicit SSL connections using AUTH TLS or AUTH SSL client commands.

Implicit FTPS - Forwards only encrypted implicit SSL connections.

HTTP - Forwards HTTP connections to target HTTP service.

HTTPS - Forwards HTTPS connections to target HTTPS service.

HTTPS/HTTP - Forwards HTTPS connections to target HTTP service

IMAP4 - Forwards plain IMAP4 connections.

SFTP/SSH - Forwards SFTP/SSH connections.

SMTP - Forwards plain SMTP connections.

MySQL - Forwards plain MySQL connections.

POP3 - Forwards plain POP3 connections.

TCP - Forwards connections without any protocol translation performed (Read and Write).

TCP/SSL - Forwards SSL encrypted connections without any protocol translation performed (Read and Write).

UDP - Forwards connections without any protocol translation performed (Read and Write).

Add service

Figure 3

Add FTP Proxy Service

Proxy Service
Specify service parameters

Local host* port

☒ Remote host port timeout sec

☐ Cluster

☐ Delegate connections to available agents

☐ Ignore PASV/LPSV/EPSV IP of server host

Add Cancel

Protocol - The protocol used. See Protocol types.

Local host - The local IP that connections are accepted on.

Local port - The local port that connections are accepted on.

Remote host - The remote host/IP that connections are forwarded to.

Remote port - The remote port that connections are forwarded to.

Cluster - The cluster to forward connections to. This is used for load balancing purposes.

Delegate connections to available agents - If checked then connections will be handled by connected agents rather than by gateway directly.

Ignore PASV/LPSV/EPSV IP of server host - Ignores the IP address returned by server when issuing PASV, LPSV or EPSV commands to server. Instead the IP address that gateway is connected to will be used. This is only applicable to FTP/S protocols.

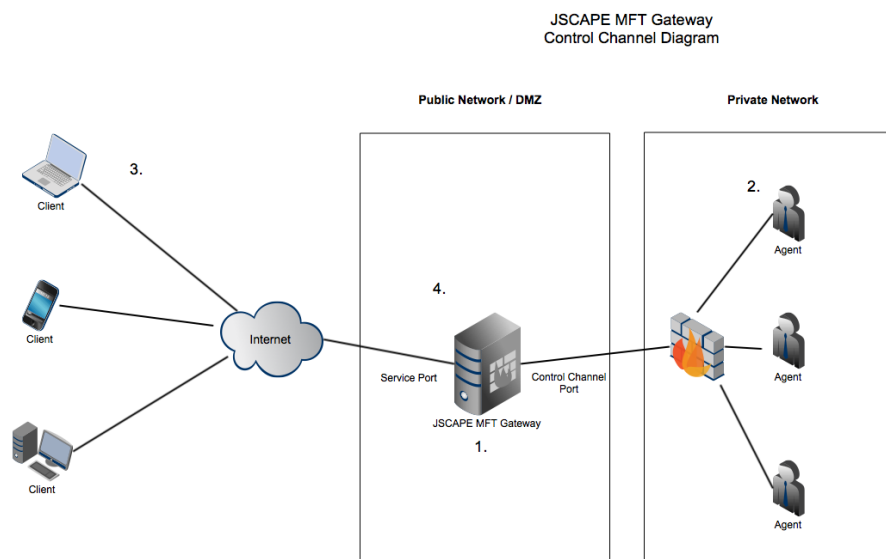
See also

Adding service clusters

Delegating network requests

You can optionally delegate network requests from JSCAPE MFT Gateway Server to one or more registered instances of JSCAPE MFT Gateway Agent. This option is used primarily in environments where inbound network connections from the DMZ to the internal network are prohibited due to network security or regulatory compliance requirements. A visual and description of the network communication flows between client, JSCAPE MFT Gateway Server, JSCAPE MFT Gateway Agent and target server are provided in *Figure 51* below.

Figure 51



1. Reverse proxy service is created in JSCAPE MFT Gateway Server with `Delegate connections to available agents` option enabled.
2. Control channel is enabled in JSCAPE MFT Gateway Server. See Control channel settings for details.
2. JSCAPE MFT Gateway Agent software is installed on one or more machines in private network.
3. Client establishes connection to service port in JSCAPE MFT Gateway Server e.g. for FTP this may be port 21.
4. JSCAPE MFT Gateway Server recognizes that this reverse proxy service has `Delegate connections to available agents` option enabled and assigns request to an available agent (using round-robin algorithm if more than one agent is available).
5. JSCAPE MFT Gateway Server then instructs agent to establish connection to target server and creates

a tunnel between client, JSCAPE MFT Gateway Server, JSCAPE MFT Gateway Agent and target server/port.

See also

Installation components
Control channel settings

Setting logging preferences

JSCAPE MFT Gateway logs all domain activity to a log directory or JDBC accessible database.

File Log
Database Log

File Log

Logs all server activity to a directory rotating log using specified frequency.

Figure 4

Help ▾ Logout

State
Services
Clusters
IP Access
Logging
Health Monitor

Administrators
Keys
Email
Web
Control Channel

Logging View Log

Show File log

Log directory* var/log Browse

Rotate log ☒ Daily ☐ Weekly ☐ Monthly ☐ Size reaches 10 MB

Apply Cancel

Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.

Log directory - The directory where to store log files.

Rotate logs - The frequency in which to rotate log files.

Database Log

Logs all server activity to a JDBC accessible database. To use the Database log option you must first create the database on your database server. Scripts for creating a database may be found in the `etc` directory of your JSCAPE MFT Gateway installation. Scripts for MySQL, Microsoft SQL Server and Oracle are provided in the files named `mysql.sql`, `mssql.sql` and `oracle.sql` respectively. Libraries for JDBC drivers must be placed in the `lib/jdbc` directory of your JSCAPE MFT Gateway installation, the

JSCAPE MFT Gateway Service restarted in order for the new drivers to be loaded.

Figure 5

The screenshot displays the JSCAPE MFT Gateway configuration interface. On the left is a sidebar menu with options: State, Services, Clusters, IP Access, Logging (selected), Health Monitor, Administrators, Keys, Email, Web, and Control Channel. The main content area is titled 'Logging' and includes a 'View Log' button. Below this, there's a 'Show' dropdown menu set to 'Database log'. The configuration fields for the database connection are as follows:

JDBC driver class*	com.mysql.jdbc.Driver
JDBC database URL*	jdbc:mysql://localhost/mftgateway
Username	admin
Password	••••
Connections pool size	10
Connection time-to-live	1 min

At the bottom right of the configuration area is a 'Test Parameters' button. Below the configuration area are 'Apply' and 'Cancel' buttons. The footer text reads: 'Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.'

JDBC driver class - The JDBC driver class name.

JDBC database URL - The JDBC URL used to connect to the database. The above example demonstrates connecting to a MySQL database. Contact your database vendor for access to JDBC libraries and assistance on specifying the JDBC URL.

User - The username to connect with when authenticating with JDBC database.

Password - The password to connect with when authenticating with JDBC database.

Connections pool size - The maximum number of connections in database pool.

Connection time-to-live - The maximum amount of time in minutes that the database connection can live in the pool without activity.

Test Parameters - Tests database connection using the specified JDBC settings.

Setting health monitor preferences

JSCAPE MFT Gateway includes a health monitor that when will routinely check the availability of reverse proxy services. If a service is not available it will be temporarily removed from use in any clusters and an optional alert email message will be sent.

Figure 33

The screenshot shows the 'Health Monitor' configuration panel. On the left is a sidebar menu with options: State, Services, Clusters, IP Access, Logging, Health Monitor (selected), Administrators, Keys, Email, Web, and Control Channel. At the top of the main panel, there are 'Help' and 'Logout' links. The 'Health Monitor' section contains the following settings:

- Interval:** A dropdown menu showing '3600' with a 'sec' unit label.
- Retry:** A dropdown menu showing '3' with a 'time(s)' unit label.
- Enable email notifications to:** A checkbox that is checked, followed by a text input field containing 'admin@domain.com' and a 'Details' button.

At the bottom right of the panel are 'Apply' and 'Cancel' buttons. Below the panel, a footer line reads: 'Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.'

Interval - The frequency in seconds to check service availability.

Retry - The number of times to retry service check before a service is considered unavailable.

Enable email notifications to - If enabled, alerts will be sent to the specified email address regarding service availability.

Monitoring HTTP/S services

All services are monitored using the settings defined in the Health Monitor panel. HTTP/S services include additional monitoring features that will check the response from the HTTP/S server to validate that the status code and body content returned contains the information expected. This can be configured when adding any HTTP/S service.

Figure 35

Delegate connections to available agents - If checked then connections will be handled by connected agents rather than by gateway directly.

Monitor path - The relative URL to request when performing health monitor check. The value "/" will return the home page for this HTTP/S service.

Status regexp - Regular expression to compare HTTP response code against. For HTTP, 3 digit status codes starting with a 2 are considered successful.

Body regexp - Regular expression to compare HTTP response body against. In general, this should be some text that you expect to see in the requested monitor path.

Enable URL rewriting - If checked HTTP headers and/or content will be rewritten by gateway according to selected rewrite rules.

Viewing log data

Log data may be viewed using any text editor or SQL client depending on the logging datastore specified. Optionally you may use the `View Log` tab found in the `Logging` node of the JSCAPE MFT Gateway to view the latest log activity. Using the `View Log` tab you may view up to the last 1000 records of log activity.

Figure 6



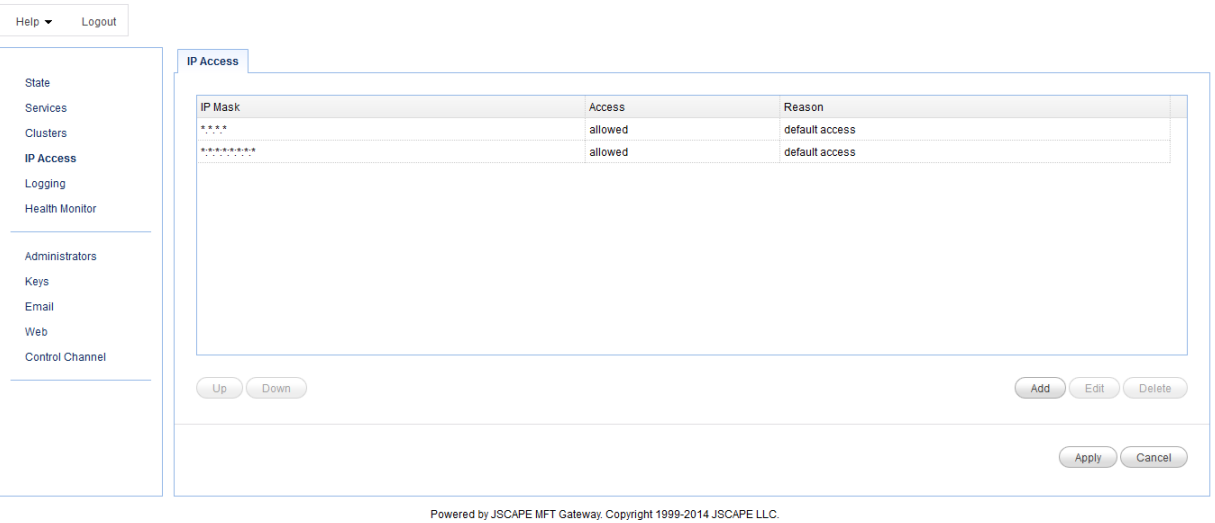
Setting IP based access

As an improved security measure you may define what IP addresses are allowed or disallowed access to your proxy services. To view a list of IP access rules click on the IP Access node.

Add IP access rule

IP mask examples

Figure 7



Add IP access rule

To add an access rule click on the Add button in the lower right corner. This will display the Add IP Access Rule dialog.

Figure 8

Add IP Access Rule

IP Access Rule
Specify access rule parameters

IP mask* ⚠

Reason

☒ Access allowed

Add Cancel

IP mask - The IP address or IP address mask to allow or deny access.

Reason - Reason access is allowed or denied.

Access allowed - Select to have access allowed, otherwise access will be denied for selected IP mask.

IP mask examples

Examples of valid IP masks are as follows:

192.168.1.1 - Allows/Blocks a single IP address

192.168.1.* - Allows/Blocks all IP addresses in a class C IP block.

192.168.*.* - Allows/Blocks all IP addresses in a class B IP block.

..*.* - Allows/Blocks all IP addresses.

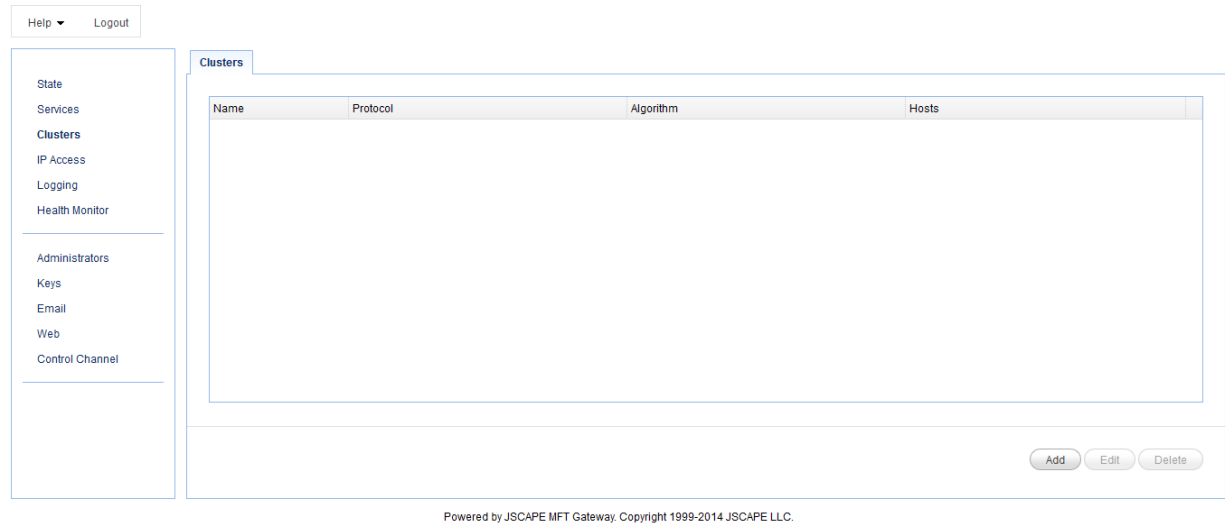
Adding service clusters

A service cluster is used for load balancing purposes and consists of one or more services. When adding a reverse proxy service you have the option setting the remote host to a fixed IP address or hostname or to use a service cluster. If a service cluster is used then incoming connections are reverse proxied to hosts in the service cluster using the specified load balancing algorithm. To view service clusters click on the **Clusters** node in JSCAPE MFT Gateway Manager.

Add service cluster

Load balancing algorithms

Figure 9



Name - The name of the service cluster.

Protocol - The protocol used by the service cluster.

Algorithm - The algorithm used for load balancing the cluster.

Hosts - The hosts in the service cluster.

Add service cluster

To add a service cluster go to the Clusters node of JSCAPE MFT Gateway Manager and click on the **Add** button. Next, enter a cluster **Name**, **Protocol** and load balancing **Algorithm** you wish to use. Lastly, Add the target hosts you would like to be part of the cluster and click **Add** to complete.

Figure 10

Add Cluster

Cluster
Specify cluster parameters

Name* mycluster

Protocol FTP

Algorithm Round Robin

IP binding time to live 60 min

Host	Port	Weight	Status

Up Down

Add Edit Delete

Add Cancel

Name - The name of the service cluster.

Protocol - The protocol used by the service cluster.

Algorithm - The load balancing algorithm to use for this cluster.

IP binding time to live - The maximum amount of time that a client is bound to a host in cluster. While a client is bound to host, all future requests from client will be redirected to host.

Load balancing algorithms

Round Robin - All nodes are treated equally and assigned requests in the order they are listed

Weighted Round Robin - Just like Round Robin but with the ability to favor individual nodes and assign them more connections based on a "Weight"

Random - All nodes treated equally and assigned requests with no regard to the order that they are listed

Least Connections - Favors nodes with the least number of current connections

Weighted Least Connections - Like Least Connections but with the ability to favor individual nodes and assign them more connections based on a "Weight"

Setting URL rewrite rules

When reverse proxying HTTP/S protocols JSCAPE MFT Gateway can optionally automatically rewrites HTTP headers and/or content using rewrite rules that you specify. For example, you may wish to trap HTTP responses containing the target host/port and replace them with the local host/port of the gateway. This can be especially important in cases where HTML content returned by HTTP/S service contains both relative and absolute URL references.

Managing Rewrite Rules

Setting Rewrite Rules

Pre-Installed Rewrite Rules

Rewrite Rules for JSCAPE MFT Server Integration

Relative URL Example

```

```

Absolute URL Example

```

```

Relative URL references are easily handled by JSCAPE MFT Gateway without the need to perform any URL rewriting. Absolute URL references however must be rewritten so that HTTP/S requests are sent through JSCAPE MFT Gateway rather than accessed directly by the client browser.

Managing URL Rewrite Rules

URL rewrite rules can be managed in the `Services > HTTP/S > URL Rewrite Rules...` section of JSCAPE MFT Gateway Manager. A list of commonly used rules are provided with the default installation that should meet most user needs. To add your own custom rules click on the `Add` button.

Figure 25

Name - A unique name.

Description - Description of this rewrite rule.

Direction - The direction of the HTTP message. Valid values are client-server (i.e. HTTP/S request), server-client (i.e. HTTP/S response) or any direction.

Scope - The scope that should be used when applying rewrite rule. Valid values are headers (i.e. HTTP headers), content (i.e. HTTP/S response content such as web pages) and headers and content. Please note that the only valid scope for client-server requests (i.e. HTTP/S request) is headers. For HTTP/S responses, content will only be modified for the following content types: text/html, text/css, text/javascript.

Find regexp - Regular expression to match when searching HTML content. This field may also make use of variables available when clicking the `Add Variable` button.

Replace regexp - Regular expression to replace matching content found when searching HTML content. This field may also make use of variables available when clicking the `Add Variable` button.

Setting URL Rewrite Rules

By default URL rewriting is **NOT** enabled for HTTP/S services. This means that HTTP/S response content and HTTP/S request/response headers will **NOT** be modified. If the HTTP/S response content being served contains absolute URL then you may need to enable URL rewriting. URL rewrite rules for an HTTP/S service may be enabled only when **adding** a service under the `Services` node of JSCAPE MFT Gateway Manager.

Figure 27

Add HTTP Proxy Service

Proxy Service
Specify service parameters

Local host* port

☒ Remote host port timeout sec

☐ Cluster

Monitor path*

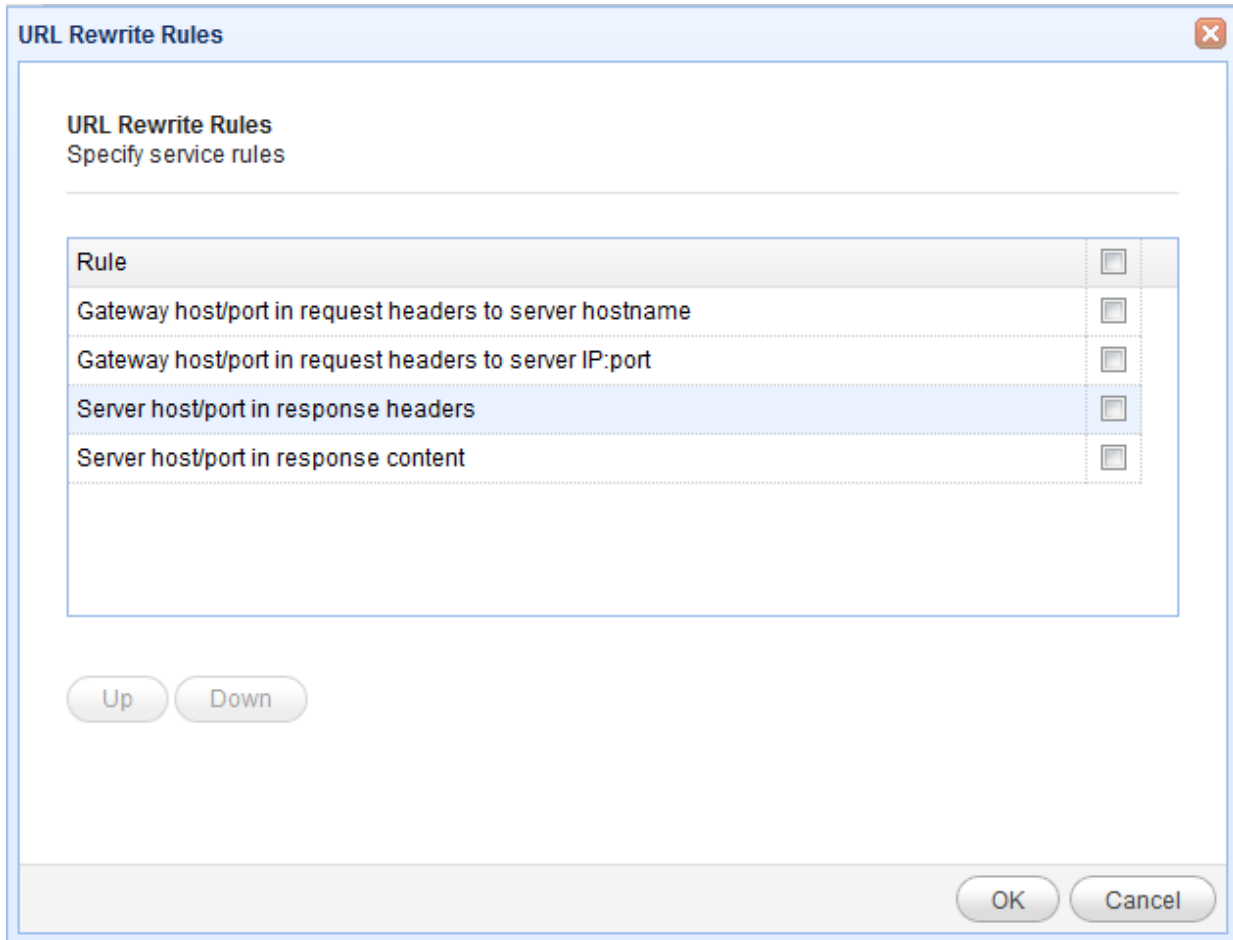
Status regexp*

Body regexp

☒ Enable URL rewriting

1. Check the `Enable URL rewriting` option.
2. Click the `Settings...` button to define what URL rewrite rules will be used.

Figure 28



1. Check the rules you wish to have enabled.
2. Use the `Up` and `Down` buttons to set the order in which URL rewrite rules are processed. **Note** - Each rewrite rule will operate on the modified content of any previous rewrite rules executed so it is **important** that rewrite rules be specified in the correct order.

Pre-Installed Rewrite Rules

There are a number of pre-installed rewrite rules that you can use for your HTTP/S services. These should meet the majority of needs when reverse proxying HTTP/S services. Note that while these rewrite rules are pre-installed they are not automatically enabled for HTTP/S services. It is **important** that you clearly understand what each rewrite rule is doing, otherwise you may end up with unexpected results.

Rule #1

Name: Gateway host/port in request headers to server hostname

Description: Replaces outer (i.e. public facing) hostname and/or IP and optional port of the gateway with that of target server hostname in HTTP request headers.

Find regexp: ({GATEWAY_OUTER_IP}:{GATEWAY_PORT}) | ({GATEWAY_OUTER_HOSTNAME} :
{GATEWAY_PORT}) | (localhost:{GATEWAY_PORT}) | ({GATEWAY_OUTER_IP}) |
({GATEWAY_OUTER_HOSTNAME}) | (localhost)

Replace regexp: {SERVER_HOSTNAME}

Scope: HEADERS

Direction: CLIENT_SERVER

Note, this rule **should** be used on services running on default ports (80,443). This rule **should not** be used in combination with *Rule #2*.

Rule #2

Name: Gateway host/port in request headers to server IP:port

Description: Replaces outer (i.e. public facing) hostname and/or IP and optional port of the gateway with that of target server IP and port in HTTP request headers.

Find regexp: ({GATEWAY_OUTER_IP}:{GATEWAY_PORT}) | ({GATEWAY_OUTER_HOSTNAME} :
{GATEWAY_PORT}) | (localhost:{GATEWAY_PORT}) | ({GATEWAY_OUTER_IP}) |
({GATEWAY_OUTER_HOSTNAME}) | (localhost)

Replace regexp: {SERVER_IP}:{SERVER_PORT}

Scope: HEADERS

Direction: CLIENT_SERVER

Note, this rule **should** be used on services running on non-default ports (other than 80,443). This rule **should not** be used in combination with *Rule #1*.

Rule #3

Name: Server host/port in response headers

Description: Replaces hostname and/or IP and optional port of the target server with that of outer (i.e. public facing) IP and port of the gateway in HTTP response headers.

Find regexp: ({SERVER_IP}:{SERVER_PORT}) | ({SERVER_HOSTNAME} : {SERVER_PORT}) | ({SERVER_IP}) |
({SERVER_HOSTNAME})

Replace regexp: {GATEWAY_OUTER_IP}:{GATEWAY_PORT}

Scope: HEADERS

Direction: SERVER_CLIENT

Note, this rule **should** be used for most services.

Rule #4

Name: Server host/port in response content

Description: Replaces hostname and/or IP and optional port of the target server with that of outer (i.e. public facing) IP and port of the gateway in HTTP response content.

Find regexp: ({SERVER_IP} : {SERVER_PORT}) | ({SERVER_HOSTNAME} : {SERVER_PORT}) | ({SERVER_IP}) | ({SERVER_HOSTNAME})

Replace regexp: {GATEWAY_OUTER_IP} : {GATEWAY_PORT}

Scope: CONTENT

Direction: SERVER_CLIENT

This rule has the same regular expressions used in *Rule #3* but is applied to the content only. The reason for providing separate rules is that there is noticeable performance improvement for web sites where there is no need for content rewriting. For maximum performance, this rule **should not** be used except when needed.

Rewrite Rules for JSCAPE MFT Server Integration

For HTTP/S services running on default ports you should use the following Pre-Installed Rewrite Rules.

Rule #1, Rule #3, Rule #4

For HTTP/S services running on non-default ports you should use the following Pre-Installed Rewrite Rules.

Rule #2, Rule #3, Rule #4

Caching HTTP/S content

Caching HTTP/S content on JSCAPE MFT Gateway can significantly improve performance. When content is cached on JSCAPE MFT Gateway the content is automatically served to the requesting user without requiring a second request to the target HTTP/S service. To enable caching for HTTP/S services go to the *Services > HTTP/S* panel, check the *Enable cache in directory* option. Content is automatically cached according to the standards defined in RFC 2616.

Figure 34

The screenshot shows the JSCAPE MFT Gateway configuration interface. On the left is a sidebar menu with options: State, Services, Clusters, IP Access, Logging, Health Monitor, Administrators, Keys, Email, Web, and Control Channel. The main panel has tabs for Services, FTP/S, TCP, and HTTP/S. The FTP/S tab is active, showing settings for Connection timeout (60 sec), NAT host (empty field), and a checkbox for 'Enable cache in directory /var/http-cache' with a 'Browse' button. Below these are buttons for 'SSL/TLS Ciphers' and 'URL Rewrite Rules'. At the bottom right are 'Apply' and 'Cancel' buttons. A footer note states: 'Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.'

Setting passive IP for FTP/S services

You may be running JSCAPE MFT Gateway in an environment where FTP/S services listen on an internal address but are accessible to external users (e.g. via the Internet) using NAT (Network Address Translation).

For example, let's assume that your FTP reverse proxy service is listening on an internal IP address of 192.168.1.1 but is only accessible to external users using the external IP address 200.200.200.200. When FTP/S clients connect to this FTP service and attempt to perform a directory listing or transfer a file a passive connection is typically used. In a passive connection the client sends the PASV command and the server responds with the IP address and port that the client should connect to perform the requested action. If the FTP reverse proxy service is listening on an internal IP address then it will return this IP address in its response to the client.

Using the example IP addresses above, the problem here is that since 192.168.1.1 is an internal address it is non-routable to external users connecting over the Internet, likely resulting a connection timeout when the client tries to perform the requested action. To resolve this issue you must instruct JSCAPE MFT Gateway to use the passive IP address 200.200.200.200 rather than 192.168.1.1 when responding to passive requests. This can be achieved via the Services > FTP/S > Passive IP field in JSCAPE MFT Gateway Manager.

Figure 31

The screenshot shows the configuration page for FTP/S services in the JSCAPE MFT Gateway. The left sidebar contains navigation links: State, Services, Clusters, IP Access, Logging, Health Monitor, Administrators, Keys, Email, Web, and Control Channel. The main content area has tabs for Services, FTP/S, TCP, and HTTP/S. Under the FTP/S tab, there are several configuration fields: Command channel timeout (60 sec), Data channel timeout (30 sec), Passive IP (200.200.200.200), and a checkbox for 'Do not use Passive IP for client IP matching regexp'. Below these are four checked checkboxes: 'Passive port range' (3000 to 4000), 'Block bounce attack', 'Block PASV attack', and 'Shutdown server SSL for CCC command'. There is also a checkbox for 'Shutdown client SSL for CCC command'. At the bottom right, there are 'Apply' and 'Cancel' buttons. A footer note states: 'Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.'

Command channel timeout - The time in seconds that a client may remain inactive on command channel before server forcefully disconnects client.

Data channel timeout - The time in seconds that a client may remain inactive on data channel before server forcefully disconnects client.

Passive IP - The IP address to use in response to passive client requests.

Do not use Passive IP for client IP matching regexp - Passive IP will not be used for clients connecting from IP matching the specified regular expression. This is useful in cases where you do not want internal users to have passive connection re-routed to an external IP address.

Passive port range - The passive port range to use in response to passive client requests. If not enabled a random port range will be used. Ensure that this port range is open on any firewall that may be in front of the gateway.

Block bounce attack - If enabled FTP/S services will only be allowed to make PORT requests to originating host.

Block PASV attack - If enabled users will only be allowed to connect to passive data ports that are initiated by same client on command channel.

Shutdown server SSL for CCC command - If enabled server must properly shutdown SSL connections for command channel when issuing CCC command.

Shutdown client SSL for CCC command - If enabled client must properly shutdown SSL connections for command channel when issuing CCC command.

SSL/TLS Ciphers - The SSL/TLS ciphers enabled for FTP/S services.

Setting NAT host for HTTP/S services

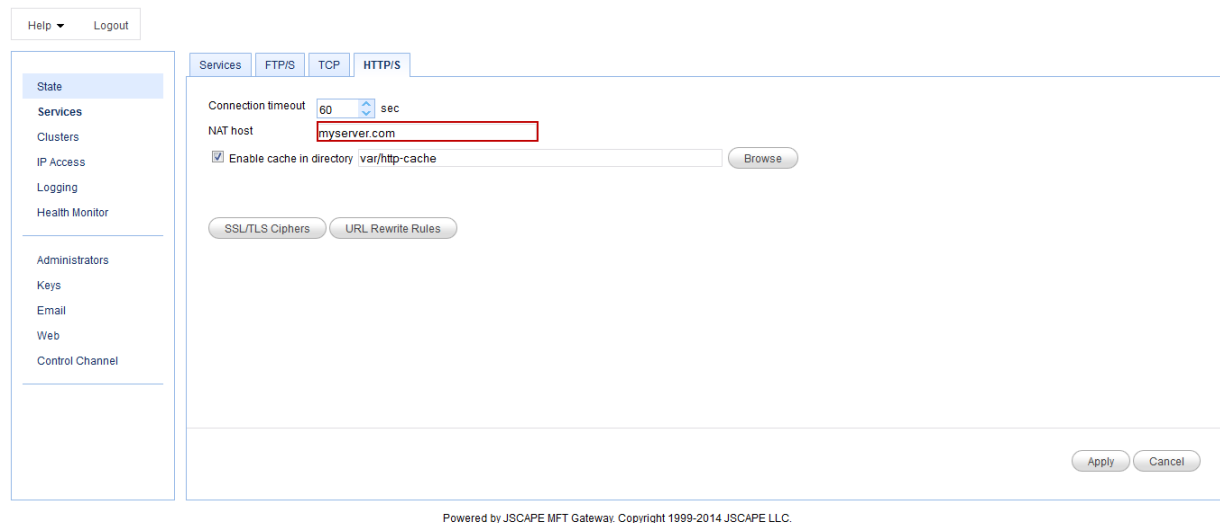
You may be running JSCAPE MFT Gateway in an environment where HTTP/S services listen on an internal address but are accessible to external users (e.g. via the Internet) using NAT (Network Address Translation).

For example, let's assume that your HTTP reverse proxy service is listening on an internal IP address of

192.168.1.1 and is reverse proxying to the external host `someotherserver.com`. Furthermore, via NAT translation, the server running your HTTP reverse proxy service is accessible to external users using the host `myserver.com`. When loading `myserver.com` users are reverse proxied to `someotherserver.com`. Any absolute URL in HTTP headers or HTML content (*provided URL rewriting is enabled*) that references `someotherserver.com` is rewritten with the IP address `192.168.1.1`.

The problem here is that since `192.168.1.1` is an internal address it is non-routable to external users connecting over the Internet, likely resulting in some broken links and images when rendered in the client browser. To resolve this issue you must instruct JSCAPE MFT Gateway to use the external address `myserver.com` rather than `192.168.1.1` when performing URL rewrites. This can be achieved via the `Services > HTTP/S > NAT host` field in JSCAPE MFT Gateway Manager.

Figure 30

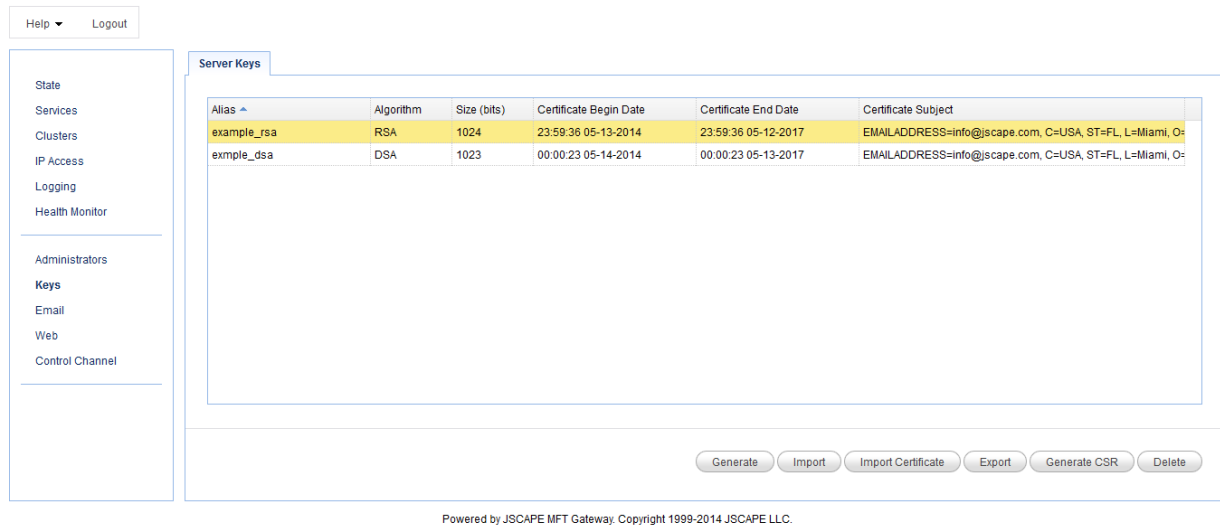


Server keys

Overview

JSCAPE MFT Gateway includes support for SSL encrypted connections. In order to take advantage of encryption services you must create one or more server keys that may be used for encrypting your sessions. Key management is accomplished via the `Server Keys` node.

Figure 11



Note

Some server keys are installed by default with JSCAPE MFT Gateway. These are meant only for testing purposes and should **NOT** be deployed to a production environment.

Generating a key

To generate a private key open the Key Manager by selecting the Keys option from the main menu. The Server Keys panel will be displayed. Click on the `Generate` button. The `Generate Key` dialog is displayed.

Figure 11

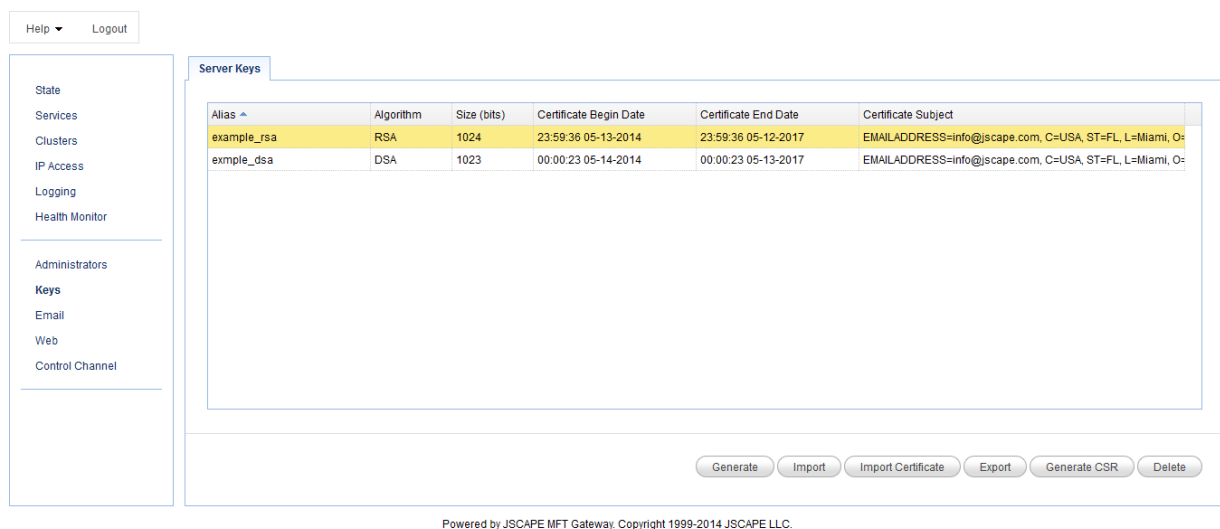
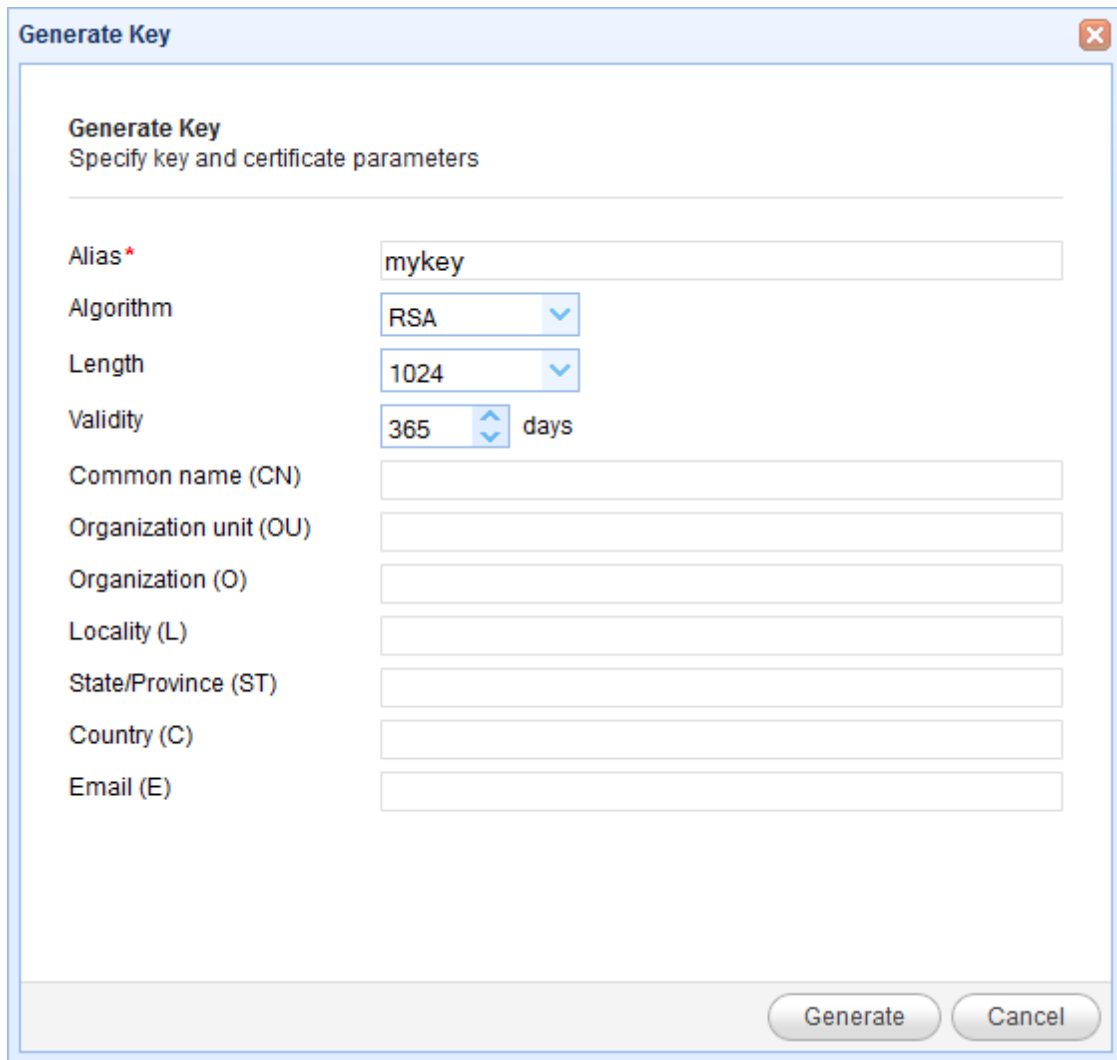


Figure 12



The image shows a 'Generate Key' dialog box with a title bar containing a close button. The main area is titled 'Generate Key' with a subtitle 'Specify key and certificate parameters'. It contains several input fields: 'Alias*' with the value 'mykey', 'Algorithm' with a dropdown menu showing 'RSA', 'Length' with a dropdown menu showing '1024', and 'Validity' with a spinner box showing '365' and the unit 'days'. Below these are seven empty text boxes for 'Common name (CN)', 'Organization unit (OU)', 'Organization (O)', 'Locality (L)', 'State/Province (ST)', 'Country (C)', and 'Email (E)'. At the bottom right are 'Generate' and 'Cancel' buttons.

Alias - Alias you wish to assign to the key.

Algorithm - The algorithm used in generating this key. Valid options are RSA and DSA.

Length - The length of the key in bytes. Valid options are 1024 and 2048.

Validity - The number of days this key is valid.

Common name - The name you wish to assign this key. Typically the domain name this key will server e.g. ftp.domain.com

Organization unit - The unit within your organization that this key will be used for e.g. IT.

Organization - Your organization name.

Locality - Your city.

State/Province - Your state or province.

Country - Your 2 character country code e.g. "US".

Email - Your email address.

Obtaining a trusted certificate

If you decide to offer SSL services you have the option of generating your own self-signed certificate in JSCAPE MFT Gateway Manager, or you can create a certificate signing request (CSR) and have your certificate signed by a third party known as a certificate authority (CA).

Note

When using your own self-signed certificate clients may display a warning message letting the user know that the certificate in use is not signed by a known CA. This is not an error but rather a warning to the user that the certificate has not been validated by a trusted authority. If you wish to avoid this message you should create a certificate signing request have that certificate signed by a trusted certificate authority.

Generating a private key

The first step in obtaining a CA signed certificate is to generate your own server key. The most important thing to understand when generating your server key is that the "Common name" field should match the domain name that clients will use when connecting to your services. For example, if your services will be served under the domain `ftp.mydomain.com` then this is the value you should use in your `Common name (CN)` field when generating your private key.

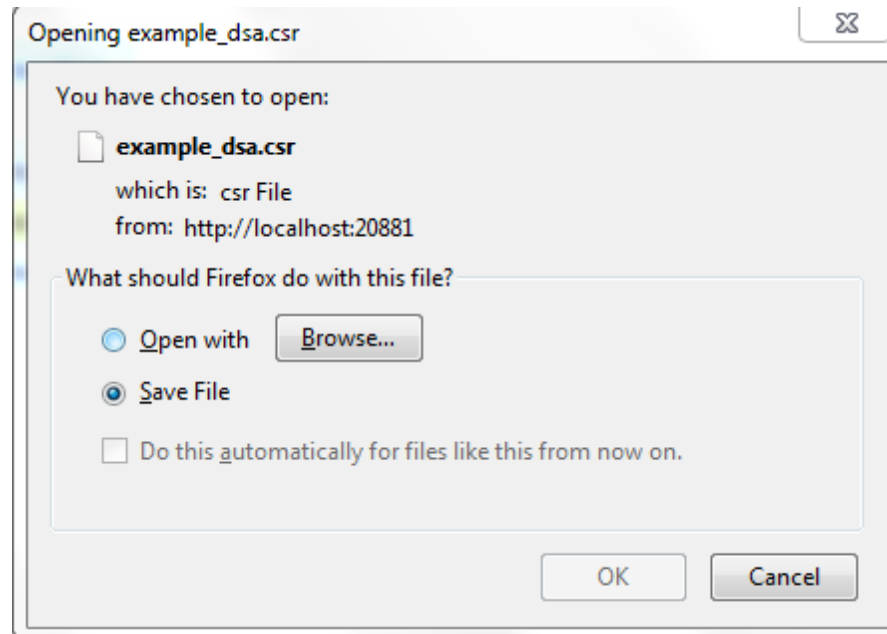
See also

Generating a key

Generating a CSR

The next step is to create a certificate signing request for your server key. The CSR will be used by the CA in order to create a signed certificate. To generate a CSR, highlight the desired server key in the `Server Keys` panel and click the `Generate CSR` button. Your CSR will be generated and a dialog will prompt you to save the file.

Figure 13



Submitting CSR to CA

The next step is to submit your CSR to the CA for use in generating your signed certificate. Please consult your CA for instructions on how to accomplish this. Your CA may ask you in which format you would like the certificate. If this option is presented to you select the "Other", "Apache" or "Java" option to receive the certificate in a standard format. To request a JSCEPE signed certificate please visit the following:

https://www.securepaynet.net/gdshop/ssl/ssl.asp?prog_id=423530&ci=1789&

Importing signed certificate

The last step is to import the signed certificate issued to you by your CA. To import the signed certificate select the server key that was used to generate the CSR and click the `Import Certificate` button. You will be prompted for the path of the certificate file issued to you by your CA.

Figure 14

**Note**

Some CA issue an intermediate certificate in addition to a signed certificate. If your certificate came with an intermediate certificate you will need to append the contents of the intermediate to the signed certificate issued to you by your CA. If your certificate did not come with an intermediate certificate you may skip these steps.

1. Open your signed certificate and intermediate certificate files using a text editor e.g. notepad or vi.
2. Copy the full contents of the intermediate certificate and append to the end of signed certificate file.
3. Save signed certificate and continue with process of importing signed certificate.

File - The file containing signed certificate.

File password - The password protecting certificate. Leave blank if none.

Alias in file - The certificate alias in file. Leave blank if none.

Verifying signed certificate

Upon successfully installing your signed certificate you can verify that it is working by connecting using any SSL enabled client and viewing the certificate details. You should notice in the certificate details that the CA is listed as a trusted authority for the certificate.

Importing third party certificates

If you have your JSCAPE MFT Gateway server private key signed by a certificate authority (CA) such as Thawte, Verisign or JSCAPE you may import the issued certificate using the `Import Certificate` button.

Note

Some CA issue an intermediate certificate in addition to a signed certificate. If your certificate came with an intermediate certificate you will need to append the contents of the intermediate to the signed certificate

issued to you by your CA. If your certificate did not come with an intermediate certificate you may skip these steps.

1. Open your signed certificate and intermediate certificate files using a text editor e.g. notepad or vi.
2. Copy the full contents of the intermediate certificate and append to the end of signed certificate file.
3. Save signed certificate and continue with process of importing signed certificate.

Importing a third party certificate

1. Click `Keys`.
2. Select existing server key that you wish to import certificates for.
3. Click `Import Certificates` button.

Figure 14



File - The file containing signed certificate.

File password - The password protecting certificate. Leave blank if none.

Alias in file - The certificate alias in file. Leave blank if none.

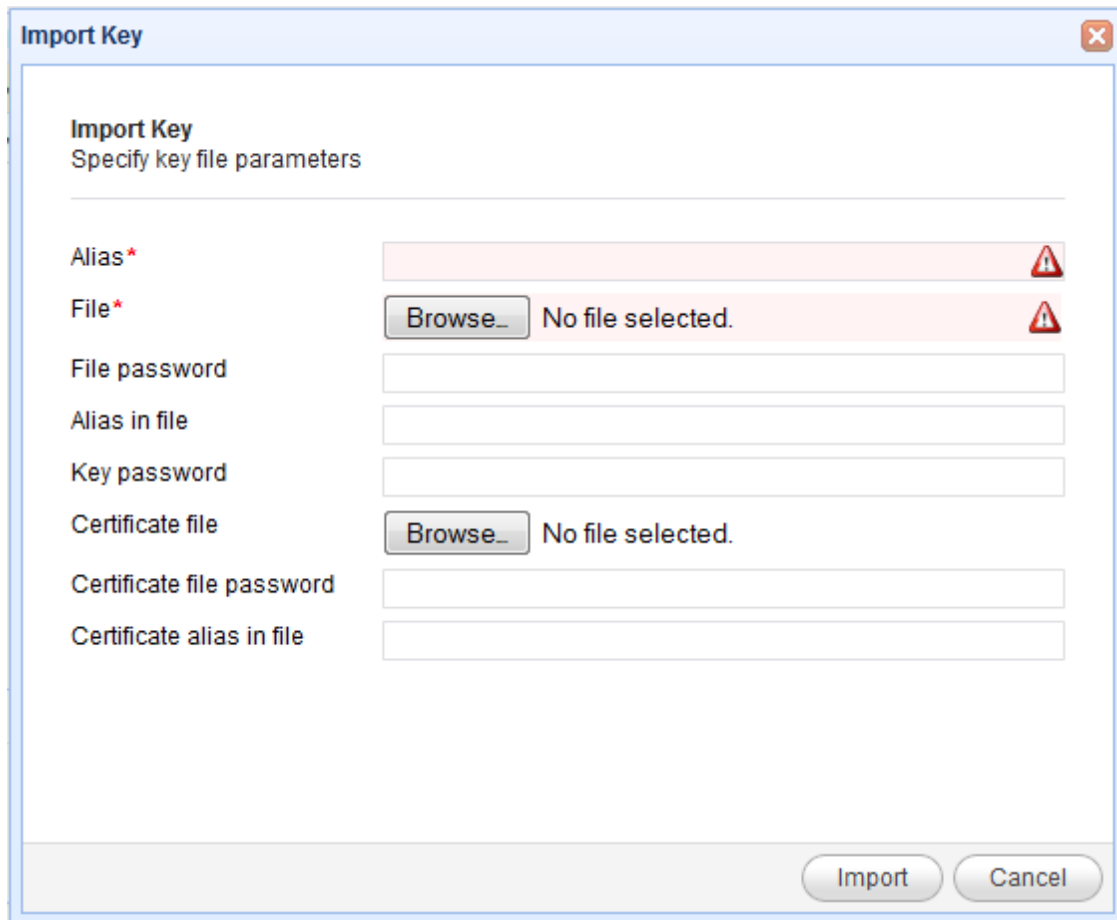
Verifying signed certificate

Upon successfully importing your certificate you can verify that it is working by connecting using any SSL enabled client and viewing the certificate details. You should notice in the certificate details that the CA is listed as a trusted authority for the certificate.


Importing a key


You may import existing server keys and certificates for use in encrypting SSL connections. To import an existing key/certificate pair click the `Keys` option from the main menu. The `Server Keys` panel will be displayed. Click on the `Import` button. The `Import Key` dialog is displayed.

Figure 19

The image shows a Java Swing dialog box titled "Import Key" with a close button (X) in the top right corner. The dialog has a subtitle "Specify key file parameters". It contains several input fields and buttons. The "Alias*" field is a text box with a red warning icon. The "File*" field has a "Browse..." button and the text "No file selected." with a red warning icon. The "File password" field is a text box. The "Alias in file" field is a text box. The "Key password" field is a text box. The "Certificate file" field has a "Browse..." button and the text "No file selected.". The "Certificate file password" field is a text box. The "Certificate alias in file" field is a text box. At the bottom right, there are "Import" and "Cancel" buttons.

Import Key
Specify key file parameters

Alias* 

File* No file selected. 

File password

Alias in file

Key password

Certificate file No file selected.

Certificate file password

Certificate alias in file

Alias - The local key alias which will be used for storing key in the servers local keystore. This may be any value of your choice.

File - The private key file to import from.

File password - The password protecting the keystore. Leave blank if none.

Alias in file - The private key alias in keystore. Leave blank if none.

Key password - The password protecting the private key. Leave blank if none.

Certificates file - The certificate file to import from. In case of PKCS#12 and JKS keystores this may be the same as "Key file" path.

Certificates file password - The password protecting certificate file. Leave blank if none. In case of PKCS#12 and JKS keystores this may be the same as "Key file password" value.

Certificates alias in file - The certificate alias in keystore. Leave blank if none. In case of PKCS#12 and JKS keystores this may be the same as "Key alias in file" value.

Note

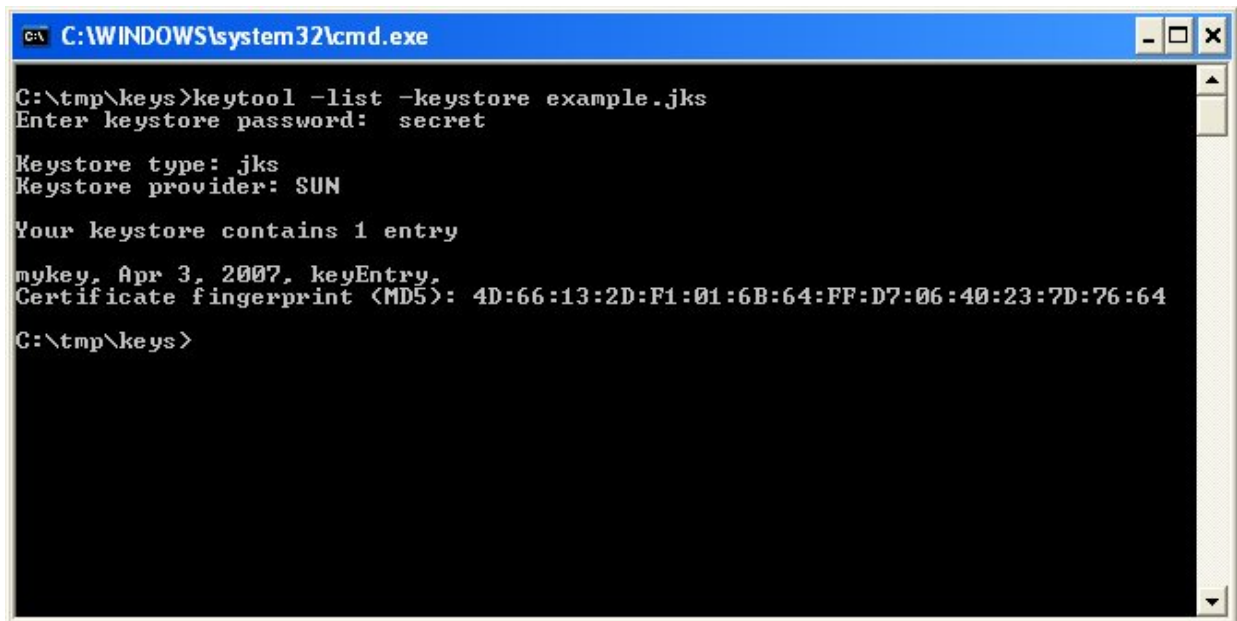
If you are unsure of the alias for the source keystore this may be obtained as follows:

JKS keystore

From your command line issue the following command in the directory that contains the keystore.

```
keytool -list -keystore example.jks
```

Figure 20



This will list one or more entries which each column in the entry delimited by a comma. The first column in the entry is the key alias.

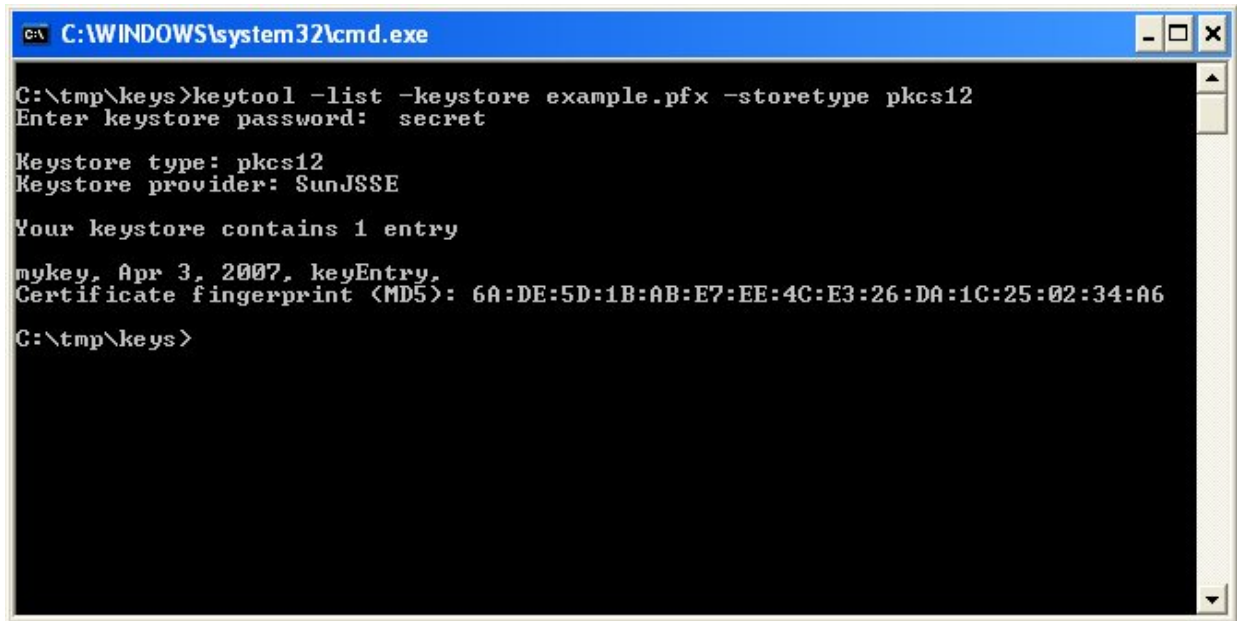
In the above example the key alias is "mykey".

PKCS#12 keystore

From your command line issue the following command in the directory that contains the keystore.

```
keytool -list -keystore example.pfx -storetype pkcs12
```

Figure 21



```
C:\WINDOWS\system32\cmd.exe

C:\tmp\keys>keytool -list -keystore example.pfx -storetype pkcs12
Enter keystore password: secret

Keystore type: pkcs12
Keystore provider: SunJSSE

Your keystore contains 1 entry

mykey, Apr 3, 2007, keyEntry,
Certificate fingerprint (MD5): 6A:DE:5D:1B:AB:E7:EE:4C:E3:26:DA:1C:25:02:34:A6

C:\tmp\keys>
```

This will list one or more entries which each column in the entry delimited by a comma. The first column in the entry is the key alias.

In the above example the key alias is "mykey".

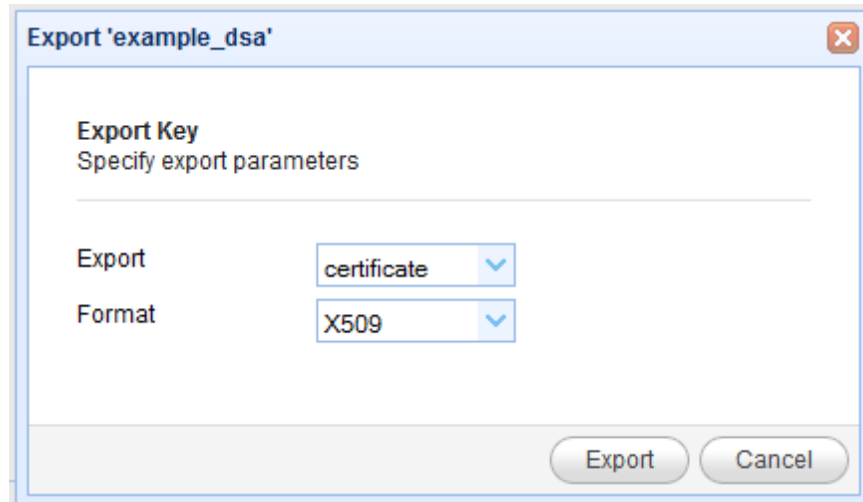
See also

Generating a key

Exporting a certificate and/or public key

You may export existing server key certificates and/or public keys for use by clients in validating trusted services or for having a third party certificate authority e.g. Thawte, Verisign or JSCAPE sign your certificate. To export an existing server certificate and/or public key click the Keys option from the main menu. The **Server Keys** panel will be displayed. Select a server key and click on the **Export** button. The **Export** dialog is displayed.

Figure 18



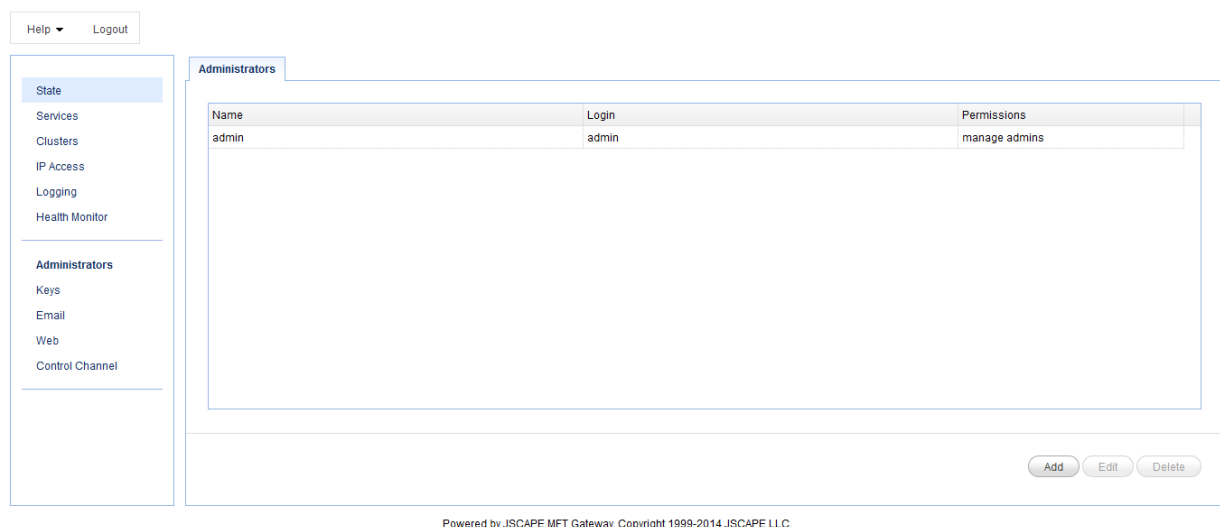
Export - The item to export (certificate, public key, private key).

Format - The format in which to export selected item.

Administrator settings

The `Administrators` node may be used to define the administrators who may manage JSCAPE MFT Gateway.

Figure 29



Web settings

The `Web` node may be used to change the web service settings used to load JSCAPE MFT Gateway Manager.

Figure 22

The screenshot shows the 'Web' settings tab in the JSCAPE MFT Gateway. The left sidebar contains a menu with 'State' selected, and sub-items: Services, Clusters, IP Access, Logging, Health Monitor, Administrators, Keys, Email, Web, and Control Channel. The main content area has the following settings:

- ☒ HTTP host: 0.0.0.0, port: 20881
- ☐ HTTPS host: 0.0.0.0, port: 20882, key: example_rsa
- Session timeout: 30 min

At the bottom right are 'Apply' and 'Cancel' buttons. At the very bottom, a footer reads: 'Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.'

HTTP host - The host and port settings for HTTP service.

HTTPS host - The host and port settings for HTTPS service.

HTTPS key - The SSL key to use for HTTPS service.

Session timeout - The amount of time before HTTP/S sessions timeout when managing gateway via web interface.

Email settings

The `Email` node defines the SMTP server that will be used by the `Health Monitor` for sending email notifications.

Figure 32

The screenshot shows the 'Email' settings tab in the JSCAPE MFT Gateway. The left sidebar is the same as in the previous screenshot, with 'Email' now selected. The main content area has the following settings:

- ☒ Enable email service
- Email Server**
 - Host/IP: smtp.gmail.com, port: 25
 - Protocol: SSL/TLS
 - Username: test@domain.com
 - Password: ****
 - Debug file: [empty], with a 'Browse' button
- Message**
 - From: test@domain.com

At the bottom left is a 'Test' button. At the bottom right are 'Apply' and 'Cancel' buttons. At the very bottom, a footer reads: 'Powered by JSCAPE MFT Gateway. Copyright 1999-2014 JSCAPE LLC.'

Email Server

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

Port - The port of the SMTP server.

Protocol - The type of connection to use. PLAIN indicates a plain-text SMTP session. SSL and START-TLS are encrypted SMTP sessions. Consult your SMTP server documentation for details on what connection types are supported.

Username - Optional username to use if SMTP server requires authentication.

Password - Optional password to use if SMTP server requires authentication.

Debug file - Optional debug file for use in debugging SMTP server problems.

Message

From - From address used when sending emails.

See also

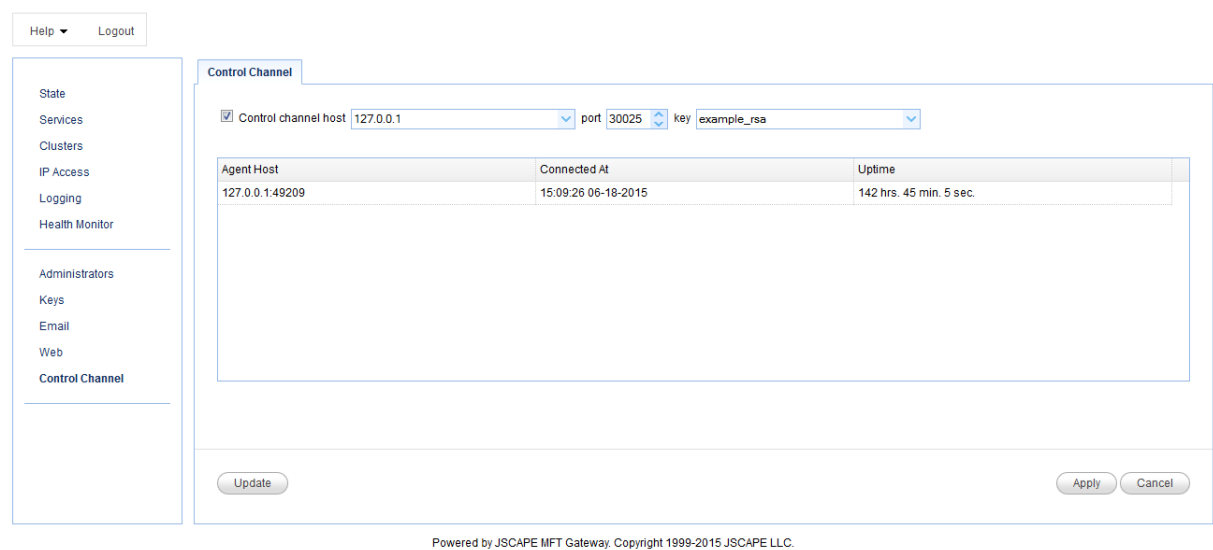
Setting health monitor preferences

Control channel settings

The `Control Channel` node may be used to define the control channel service in JSCAPE MFT Gateway Server. The control channel service is an optional service that can be used for delegating network requests to one or more agents running in the private internal network. See [Delegating network requests](#) for details.

In order to use the control channel service in JSCAPE MFT Gateway Server you must install one or more instances of JSCAPE MFT Gateway Agent on servers that typically would reside in your private internal network. See [Installation components details](#).

Figure 52



Control channel host - The IP address that control channel service will listen on. The special IP address of

0.0.0.0 may be used to listen on all available IP addresses.

Port - The port that control channel service will listen on.

Key - The server key that will be used for encrypting communications between the agent and control channel service.

See also

- Installation components
- Delegating network requests

© © 2016 JSCAPE LLC.
All rights reserved.

Product and company names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. The author assumes no responsibility with regard to the performance or use of these products. All understandings, agreements, or warranties, if any, take place directly between the vendors and the prospective users. Every effort has been made to ensure that the information in this manual is accurate. The author is not responsible for printing or clerical errors.

The product described in this manual incorporates copyright protection technology that is protected by method claims of certain U.S. patents and other intellectual property rights.

This user manual was created with Help & Manual.