User's Guide

JSCAPE MFT Server

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Contents

Introduction

1

Overview

JSCAPE MFT Server is a platform independent managed file transfer server that supports AS2 (Drummond Certified), FTP, FTPS (FTP over SSL), SFTP (FTP over SSH), HTTP, HTTPS, OFTP (Odette Certified), TFTP, AFTP and WebDAV protocols. Features of JSCAPE MFT Server include:

Feature	Benefit
Platform Independent	Support for Windows, Linux, Solaris, and Mac OS X environments provides the flexibility of deploying anywhere within your organization.
Multiple Protocol Support	Support for AS2 (Drummond Certified), FTP, FTPS (FTP over SSL), SFTP, SCP (Secure Copy), TFTP, OFTP (Odette Certified), AFTP (Accelerated File Transfer Protocol), HTTP, HTTPS and WebDAV protocols means you can easily exchange data with your customers, regardless of their file transfer requirements.
Integrated Web File Transfer Client	Licensing and support costs are significantly reduced as there is no client software to install. Your clients need only a web browser in order to start transferring files. In addition, when using the integrated web client, users do not have to worry about strict internal firewall policies as most organizations do not restrict web based traffic.
Accelerated File Transfer	AFTP (Accelerated File Transfer Protocol) is a file transfer protocol developed by JSCAPE. AFTP is designed to accelerate file transfers over high speed networks that are unable to fully utilize network throughput due to high latency and packet loss. Under these conditions AFTP can accelerate file transfers up to 100 times faster than FTP and other file transfer protocols.
Web Document Viewer	JSCAPE Web Document Viewer simplifies content distribution by embedding a document viewer in the JSCAPE MFT Server web interface. With support for numerous document formats, users can view documents on the server without having to download or have supporting software installed.
Data Protection	Your sensitive data is protected during transit and at rest using high-grade OpenPGP and SSL encryption technologies. This is critical for many companies who are now subject to PCI-DSS, HIPAA and Sarbanes-Oxley data protection requirements.
Data Loss Prevention	Prevent the loss of sensitive data using an embedded DLP rules engine.
Ad-hoc File Transfers	Perform email based file transfers while avoiding the issues commonly experienced with large email attachments.

Triggers	Using triggers you can quickly automate business processes based on events and conditions. For example, whenever a file is received by a customer you may wish to automatically compress that file and then forward it via email to the corresponding account representative for further processing.
Authentication Integration	Authenticate users against existing LDAP, NTLM, Active Directory, PAM, SSO, RADIUS or relational database servers. This greatly simplifies the integration process, especially in organizations with a large number of users.
JMS	Publish subscribed server events to any JMS (Java Message Service) queue for further processing.
Administrative ACL	Restrict administrative users capabilities and data visibility using roles and tags.
Action API	Using triggers you can define one or more actions to be executed in response to matching events and event conditions. More than 80 built-in actions allow you to do everything from compress files, OpenPGP encrypt files, send emails and more. While this may be enough for most organizations, the Action API is a Java based API that allows you to define your own actions should you have more specialized needs. For example, let's say that you need to parse a PDF document upon upload and communicate the parsed data to another server via JMS. This can be easily accomplished using the Action API.
REST API	REST API are available for both client and administrative users. Using the REST API users can do everything from performing file transfers to managing the server.
Checkpoint and Restart Support	Large file transfers over the Internet are subject to occasional failure due to network related issues. In the event of a failed file transfer, checkpoint and restart support allows you to restart the transfer from the last byte of data successfully transferred versus re-transferring the entire file. This is critical in organizations that transfer very large files or have service level agreements with customers to transfer a file within a given time period.
Integrity Checksum	Checksum verification is a post file transfer process that verifies the integrity of files transferred. This is accomplished by comparing checksums of the file on both the sender and receiver sides ensuring that files are transferred correctly.
Email Notifications	Receive email notifications on the events that are important to you. For example, as a system

	administrator you may wish to be notified via email if a users account is disabled due to a successive number of invalid login attempts.
OpenPGP Encryption	Use OpenPGP encryption to ensure that your data is encrypted while at rest or to automatically decrypt files sent to you by your customers who use OpenPGP encryption.
Automated File Transfers	Automatically transfer files to/from the server using FTP/FTPS/SFTP/SCP protocols. This is perfect for use in situations where you must transfer files on a scheduled basis or based on other event conditions.
Database Logging	Using the database logging features you can ensure that all server activity is safely stored in a remote database.
Reverse Proxies	Map remote services to virtual directories on your server. This allows you to grant users access to remote services using a single sign-on account. Users no longer have to remember multiple hostnames, usernames and passwords. This feature is also very useful streaming data between a public server located in the DMZ and a private server located behind your firewall. Support for FTP/S, SFTP, Amazon S3, SMB and other protocols.
IP Access Rules	Lock down your server using access rules based on client IP address.
Virtual File System	Define a virtual file system, users and permissions without having to create users or permissions at the operating system level.
Multiple Domains	Create multiple virtual servers each with it's own set of users and permissions.
Remote Administration	Securely manage your server remotely from anywhere in the world.
Server and Account Management API	Java and REST based APIs for integrating account and server management functions within external applications.

System requirements

- Oracle/Sun or IBM JVM (Java Virtual Machine) 1.7 or above.
- Windows XP/2003/Vista/2008/7/2012, Mac OS 10.x, Solaris, Linux, Linux Z/OS and AIX 5.x/6.x/7.x platforms.
- Current and previous (Current -1) versions of IE, Firefox, Safari and Chrome browsers.

Introduction 1

Evaluation license limitations

The Evaluation Edition of JSCAPE MFT Server is fully functional offering all features found in the Enterprise Edition yet is limited to:

- 3 users/connections
- 3 trading partners
- 3 triggers and
- 1 domain.

To purchase the Professional or Enterprise Edition of JSCAPE MFT Server please go to http://www.jscape.com/secureftpserver/purchase.html to purchase a license or submit a ticket to the Help Desk for licensing assistance.

Upgrading

Existing users of commercial editions of JSCAPE MFT Server are entitled to 1 year of free upgrades and technical support. To obtain access to the latest version please contact JSCAPE via the Help Desk.

Upgrade Process - Graphical User Interface

This process is available only to versions 6.2 and above when using GUI installer. Upgrades may only be performed against versions 5.0 or above. If you are currently using a version prior to 5.0 then you must uninstall/delete current version and reinstall/reconfigure new version.

1. Run the GUI installer for JSCAPE MFT Server.
2. When prompted where to install JSCAPE MFT Server select the same installation directory as your current installation.
3. The installer for JSCAPE MFT Server will detect that a previous version of JSCAPE MFT Server is installed and will prompt you for a directory in which the current version may be backed up.
4. Continue with the installation process as normal. Once installation is complete your server configuration settings from previous version will be automatically migrated from previous version to current version.

Additional Notes

1. If you are managing your server remotely it is IMPORTANT that both the version of JSCAPE MFT Server Manager used matches the version of JSCAPE MFT Server you are managing.
2. Any logos or text label settings that you have made to web interface WILL NOT be migrated during upgrade process.
3. Note, for Windows environments the JSCAPE MFT Server service will revert to using the Local System account after an upgrade. If JSCAPE MFT Server is accessing shared network resources (e.g. UNC paths) then you may need to update JSCAPE MFT Server service to use an account with access.

Upgrade Process - Manual

Upgrades may only be performed against versions 5.0 or above. If you are currently using a version prior to 5.0 then you must uninstall/delete current version and reinstall/reconfigure new version.

Pre-9.3

1. Shutdown JSCAPE MFT Server Service and JSCAPE MFT Server Manager.
2. Backup current JSCAPE MFT Server installation directory.
3. Uninstall current version of JSCAPE MFT Server.
4. Install updated version of JSCAPE MFT Server making sure to **use same installation directory** as previous install.
5. Shutdown JSCAPE MFT Server Service and JSCAPE MFT Server Manager.
6. Copy `users, domains,` and `logs` directories from main installation directory of backup to current installation directory.
7. Copy `*.dat`, `*.cfg` (except `ssl*.cfg`), from main installation directory of backup to current installation directory.
8. Copy `license.lic` and `ssl*.cfg` files from main installation directory of backup to `etc` directory under current installation directory.
9. Copy "`-XmxNNNm`" line inside `server.vmoptions` file to new `server.vmoptions` file if the value of that parameter is bigger than the one in the new `server.vmoptions` file.
10. Copy `*.dat` from `etc` directory of backup to `etc` directory of current installation.
11. Copy any JDBC driver JAR files you have installed from backup `libs/jdbc` directory to `libs/jdbc` directory of current installation.
12. Copy any custom actions you have installed from backup `libs/actions` directory to `libs/actions` directory of current installation.
13. Copy any custom authentication or 3rd party JAR from backup `libs/ext` to `libs/ext` directory of current installation.
14. Run the `./js-database-configuration -configure` command from within the installation directory.
15. Run the `./js-db-migration` command from within the installation directory. This will migrate previous installation configuration data to new installation.
16. Restart JSCAPE MFT Server Service and JSCAPE MFT Server Manager.

Post 9.3

1. Shutdown JSCAPE MFT Server Service and JSCAPE MFT Server Manager.
2. Backup current JSCAPE MFT Server installation directory.
3. Uninstall current version of JSCAPE MFT Server.
4. Install updated version of JSCAPE MFT Server making sure to **use same installation directory** as previous install.
5. Copy any JDBC driver JAR files you have installed from backup `libs/jdbc` directory to `libs/jdbc` directory of current installation.
6. Copy any custom actions you have installed from backup `libs/actions` directory to `libs/actions` directory of current installation.
7. Copy any custom authentication or 3rd party JAR from backup `libs/ext` to `libs/ext` directory of current installation.
8. Copy `data` and `users` directories from backup into installation directory.
9. Copy contents of `etc` directory from backup to `etc` directory of current installation.
10. Copy `*.vmoptions` files from backup directory to current installation directory.
11. Run the `./js-database-configuration -update` command from within the installation directory.
12. Restart JSCAPE MFT Server Service and JSCAPE MFT Server Manager.

Additional Notes

1. If you are managing your server remotely it is **IMPORTANT** that both the version of JSCAPE MFT Server Manager used matches the version of JSCAPE MFT Server you are managing.
2. Any logos or text label settings that you have made to web interface WILL NOT be migrated during

upgrade process.

License

JSCAPE MFT SERVER 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.

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 offering.

ADDITIONAL LICENSE TERMS FOR SOFTWARE

EVALUATION LICENSE

JSCAPE grants to you (either an individual or single entity) nonexclusive license to install and use the Software free of charge for evaluation purposes in a non-production environment. 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 JSCAPE MFT Server on a single computer. JSCAPE MFT Server 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 JSCAPE MFT Server then a separate license MUST be purchased for each instance of JSCAPE MFT Server that is installed. If you are using any virtualization technology then a separate license MUST be purchased for each environment which uses JSCAPE MFT Server.

The JSCAPE MFT Server Manager, a client graphical user interface used for managing a JSCAPE MFT Server installation, as well as API libraries needed for communicating with an instance of JSCAPE MFT Server, may be installed on additional computers that you own without charge.

PRODUCT ACTIVATION

You may need to activate the Software through the use of the Internet. You agree that JSCAPE may use such measures for license management purposes and that JSCAPE may revoke a Software license if requested by you for purposes of moving Software to a different machine or for 60 days or more of non-payment of Software license fees.

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.

The above warranty DOES NOT apply to any BETA software, any software made available for testing or demonstration purposes, any temporary software modules or any software for which JSCAPE does not receive a license fee. All such software products are provided AS IS without any warranty whatsoever.

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://help.jscape.com 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.

CUSTOM DEVELOPMENT

JSCAPE may on occasion collaborate with you on the development of new features in the Software. In some cases this development may be done for a negotiated fee between you and JSCAPE. You acknowledge and agree that any such development is exclusive property of JSCAPE and waive any and all rights to intellectual property created as a result of aforementioned development.

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 *libs* directory relative to the Software installation directory.

Version history

Release 10.1
Jun. 30, 2017

Enhancement: Disabled From field for Ad-Hoc file transfers.
Enhancement: Added ability to enforce FIPS compliance when using TLS protocols as well as SFTP.
Enhancement: Added ability to set dynamic "Expires on" in user templates.
Enhancement: Improved the appearance of the management GUI home page
Enhancement: Improved the appearance of the management Login page.
Enhancement: Added the ability to use multiple methods of authentication.

Enhancement: Improved the Ad-Hoc email dialog.
Enhancement: Improved certificate security by enabling the Server Keys module to use SHA-2 when generating certificates.
Enhancement: Introduced minor improvements to the AS2 UI.
Enhancement: Incorporated additional ways for controlling bandwidth usage in the domain and user levels.
Enhancement: Added the ability to specify a remote path when setting up an Amazon S3 Trading Partner.
Enhancement: Added the ability to support hard quotas.
Enhancement: Added the ability to show/hide the My Account link and the Personal Information module.
Enhancement: Improved the Domain Autostart feature.
Enhancement: Removed Domain Startup from Role > Global Permissions to support the Domain Autostart improvement
Enhancement: Increased the Retry Limit for Trigger Actions.
Enhancement: Added the ability to support Themes in the web user interface.
Enhancement: Added the ability to specify how often the web user interface synchronizes with the global datastore.
Enhancement: Added the ability to add notes to Trigger Actions.
Enhancement: Imposed limits to the number of Trading Partners and Triggers supported in the Evaluation Edition.
Enhancement: Disabled tags by default and applied consistency to the Tags input field look and feel
Enhancement: Added the ability to show a unique session ID for each connection in the domain activity logs.
Update: Updated the H2 database library to 1.4.196
Bug Fix: Fixed issue where non-ASCII filenames of files are incorrectly encoded when the files are uploaded to the server via the Web GUI.
Bug Fix: Fixed issue where results in the Log Search Result dialog box fail to update after clicking the Re-Run button.

Release 10.0

Jan. 16, 2017

Enhancement: Achieved OFTP2 testing compliance with ODETTE.
Enhancement: Major upgrade of client web interface to use RESTful API calls and redesigned client web interface to use JQuery components matching the look and feel of current administrative web interface.
Enhancement: Added support for case-insensitive logins regardless of operating system.
Enhancement: Added ability to edit a service without having to manually delete/add a service.
Enhancement: Added built-in modules providing ability to authenticate administrators against 3rd party user repositories including databases, LDAP, NTLM, PAM and RADIUS.
Enhancement: Added ability to limit data connection modes for FTP/S to include Active, Passive or All.
Enhancement: Enabled diffie-hellman-group1-sha1 cipher by default for SFTP service.
Enhancement: Added a Create Drop Zone trigger action for use in the automation of provisioning drop zones.
Enhancement: Added User Password Reset Request trigger event.
Enhancement: Added ability to set minimum password age.
Enhancement: Added additional permissions to administrative roles to limit ability to access Description and Sessions modules for a domain as well as the ability to start/stop/pause/resume a domain.
Enhancement: Updated preferred cipher for SFTP reverse proxy to use blowfish-cbc for improved reverse proxy performance.
Enhancement: Added ability to support unauthenticated transfers in OFTP protocol using an option that binds unauthenticated users to a named account.
Enhancement: Added support for compression when defining an OFTP trading partner.
Enhancement: Added a new “domain” variable to Server > Settings > Email > Resources panel for referencing the domain in dynamically generated emails.
Enhancement: Added ability to debug an AS2 message that is sent manually from Send File dialog in AS2

Messages module using newly added “Debug file” input.
Enhancement: Added support for CRL (Certificate Revocation List) and additional key usage attributes to Server Keys module in Key Manager.
Enhancement: Added Generate Certificate button to Key Manager > Server Keys module, simplifying the process for replacing the certificate for an existing server key.
Enhancement: Added ability to manually send a positive or negative receipt in OFTP Messages module.
Enhancement: Added ability to manually send a certificate to a trading partner from the OFTP Messages module.
Enhancement: Added js-as2purge and js-oftppurge command line utilities for purging AS2 and OFTP messages from datastore.
Enhancement: Added customizable logo to ad-hoc file transfer download page.
Enhancement: Improved logging when performing server synchronization from Server > Settings > Failover module.
Enhancement: Added -exclude-log-searches parameter to js-db-migration utility to optionally exclude log searches during migration.
Enhancement: Added color coding to Directory Monitors module to visually indicate status of quotas.
Enhancement: Added ability to support multiple decryption and receipt signing keys in Server > Settings > Web > AS2 module.
Enhancement: Expanded width of dropdowns when selecting a reverse proxy.
Enhancement: Increased default heap memory size to 1024m during installation process to better reflect typical production environment requirements.
Enhancement: Updated date widget in Advanced Search dialog for client web interface.
Enhancement: Various GUI enhancements.
Bug Fix: Fixed potential high CPU utilization issue when server has performed a large number of file transfers in a short period of time.
Bug Fix: Fixed issue where file handle on .ssh/key.pub was not properly released after an SFTP public key authentication.
Bug Fix: Fixed issue where a blocked IP due to too many unsuccessful authentications may be unblocked after restarting the server.
Bug Fix: Fixed issue where data port for active FTP connections may not originate on proper port.
Bug Fix: Fixed issue with uploading large files using Java applet.
Bug Fix: Fixed database migration issue where the password expiration reminder may be resent erroneously to accounts.
Bug Fix: Fixed various database migration issues.
Bug Fix: Fixed log parsing issue experienced when user attempts to login using double quotes.
Bug Fix: Fixed performance issue with log searches that resulted in high CPU utilization and growing database.
Bug Fix: Fixed potential “bad string length” error experienced when downloading file from an ad-hoc link.
Bug Fix: Fixed issues with System Configuration Backup trigger action.
Bug Fix: Fixed status display issue with executed trigger actions.
Bug Fix: Fixed issue where logo may not be properly displayed in web interface when using IE browser.
Bug Fix: Fixed issue where reverse proxy connections were not getting reused and not timing out.
Bug Fix: Fixed performance issue with Java applet that resulted in loading delays.
Bug Fix: Fixed directory listing error experienced when using SFTPv4.
Bug Fix: Fixed issue with js-adddomain command line utility.
Bug Fix: Fixed memory leak experienced when using Trading Partner Directory Download Synchronization trigger action.
Bug Fix: Fixed content types sent for outgoing AS2 messages based on file extension.
Bug Fix: Fixed issue with AS2 where raw messages are retained regardless of whether option for retaining AS2 messages is enabled.
Bug Fix: Fixed issue with encrypting/decrypting large files using PGP and DSA cipher.

Release 9.3
Feb. 12, 2016

Enhancement: Added support for storing all configuration data in a global datastore. This is a major change in the way in which configuration data has been previously stored and more easily supports HA configurations.
Enhancement: Added ability to publish subscribed trigger events to a JMS queue.
Enhancement: Added support for custom authentication API when authenticating administrative users.
Enhancement: Added separate logging module for administrative actions.
Enhancement: Added fine grained access control module with support for roles and tags.
Enhancement: Added persistent storage for trigger event history.
Enhancement: Added file hashing extension support to SFTP service.
Enhancement: Added last login information to user interface for both client and administrative accounts.
Enhancement: Added current login information to user interface for administrative accounts.
Enhancement: Added js-adddropzone command line utility for the creation of Drop Zone.
Enhancement: Added support for RADIUS authentication.
Enhancement: Added support for HTTP Strict Transport Security (HSTS).
Update: Changed connection method of Java applet from using WebDAV to use REST client API.
Update: Moved ability to start/stop/resume all domains from Server menu to Domains tab in administrative client user interface.
Update: Java GUI no longer distributed with product, replaced with web based GUI.
Bug Fix: Fixed issue where the disk usage quota for a Directory Monitor was reported incorrectly.
Bug Fix: Fixed NullPointerException issue when attempting to reference a null trigger event variable.
Bug Fix: Fixed issue with js-importusers command line utility that incorrectly provisioned user in the event that "Allow password change" option was disabled for the selected User Template.
Bug Fix: Resolved issues with and made improvements to CAPTCHA display.

Release 9.2
Jul. 10, 2015

Enhancement: Improved performance for storing, rendering and searching of AS2 and OFTP messages.
Enhancement: Added OFTP messages module providing ability to see OFTP messages exchanged.
Enhancement: Added dashboard to web interface for tracking various performance metrics of server over time. Metrics include threads, heap memory, max memory, allocated memory, connections, uploads and downloads.
Enhancement: Added support for OpenID Connect standard in SSO authentication module and verified compatibility with Google Apps.
Enhancement: Updated Disable Inactive Accounts trigger action to include accounts that have never logged in.
Enhancement: Added ability to define From email header for AS2 messages.
Enhancement: Added option to edit immediately after copying a Trigger, User or Trading Partner.
Enhancement: Updated reports output format to be more consistent with administrative web interface.
Update: Updated code signing certificate for file transfer applet used in web interface.
Bug Fix: Resolved issue with GetGlobalVariable function not working properly when testing a condition in a trigger.
Bug Fix: Resolved various interoperability issues with SFTP clients.
Bug Fix: Resolved issue with passive ports not displayed correctly in web interface for FTP/S services.
Bug Fix: Resolved issue with SFTP related trigger actions where password authentication is preferred even though private key is specified.
Bug Fix: Resolved various minor issues.

Release 9.1
Feb. 13, 2015

Enhancement: Added ability to search tables in administrative web interface.

Enhancement: Added progress dialog to web interface when loading a domain.
Enhancement: Added Last Login column to Users table view.
Enhancement: Added status message to administrative web interface when saving changes.
Enhancement: Added support for TFTP and OFTP services.
Enhancement: Added support for Amazon S3, TFTP, OFTP, REST, IMAP, SMTP and POP3 in Trading Partners module.
Enhancement: Added support for various protocols to Reverse Proxies module including Amazon S3, REST, TFTP and OFTP.
Enhancement: Added pagination support to AS2 Messages and Contacts modules.
Enhancement: Added notification message to web interface when rebuild index process is started via Server > Settings > Search Index.
Enhancement: Minor updates to user interface for Reverse Proxies module.
Enhancement: Updated all data tables to use consistent data alignment best practices.
Enhancement: Added visual cues to the web administrative interface that prompt user to save changes in the event they attempt to navigate away from page without saving changes.
Enhancement: Added support to automatically detect whether JavaScript and/or cookies are enabled in client's browser.
Enhancement: Updated all drop-down GUI components in web administrative interface to be searchable.
Enhancement: Added XSS and CSRF validation to all requests in both client and administrative web interfaces.
Enhancement: Added js-syncstate command line utility for performing failover synchronization.
Enhancement: Added DateAdd, DateSubtract and DateFormat trigger functions for use in manipulating and formatting dates.
Enhancement: Added Key column in Services module to display the server encryption key used by a service.
Enhancement: Added Domains attribute to Server Key in Key Manager that displays a list of the domains currently using selected key.
Enhancement: Added ability to run actions asynchronously for a Trigger.
Enhancement: Added ability to view event details for an executed Trigger.
Enhancement: Added a unique event ID attribute that identifies the event used in the execution of a Trigger.
Enhancement: Added ability to require user to submit form data when uploading files via the client web interface.
Enhancement: Added alternative Label field to be used when presenting file upload forms to web based clients.
Update: Changed name of two-factor authentication service PhoneFactor to Microsoft Azure Multi-Factor Authentication.
Bug Fix: Resolved compatibility issue with OpenID CAS server.
Bug Fix: Resolved backward compatibility issue with 8.4.
Bug Fix: Resolved issue related to known SSLv3 (POODLE) vulnerability.
Bug Fix: Resolved issue where user is not automatically redirected to login page in event of session timeout.
Bug Fix: Resolve password compliance validation issue when creating or editing a user's password.
Bug Fix: Fixed issue where first entry of new user activity log file is written to previous log file when server is inactive for several days.
Bug Fix: Fixed performance issue with Directory Monitors module.
Bug Fix: Various interoperability fixes for AS2 protocol.
Bug Fix: Fixed issue with file uploads that use a form with option to prompt user for form data for each file uploaded in a batch.
Bug Fix: Various bug fixes for web administrative client interface.

Release 9.0

Jul. 8, 2014

Enhancement: Added web based administrative user interface.
Enhancement: Added support for password protected archives in ZIP related trigger actions.
Enhancement: Added ability to ignore trigger events when domain is paused or stopped.
Enhancement: Added CurrentTimeMillis event variable to all trigger events.
Enhancement: Added relevant AS2 event variables to External File Upload event.
Enhancement: Password field is now optional in SQL related trigger actions.
Enhancement: Added option to relevant authentication modules that converts username to lowercase/uppercase when creating virtual directory paths that rely on username information. Useful in environments where authentication is case-insensitive, but filesystem is case sensitive.
Enhancement: Added ability to download one or more files/directories from web interface as a ZIP archive.
Enhancement: Added ability to store ad-hoc file transfer details in a relational database.
Enhancement: Added ability to receive AS2 messages without requiring user credentials.
Enhancement: Added Data Connection Error event that is raised when data connection over FTP/S protocols experiences a timeout or other error.
Bug Fix: Resolved various miscellaneous issues.

Release 8.8

Dec. 2, 2013

Enhancement: Added Used variable to Directory Monitor Quota Exceeded event which captures the amount of storage data used.
Enhancement: Updated MIGLayout library used in JSCAPE MFT Server Manager.
Enhancement: Added ability to set optional Reply To address when sending ad-hoc emails.
Enhancement: Added support for optional web SSO authentication with support for SAML and OpenID authentication providers.
Enhancement: Added support for multipart emails when sending ad-hoc emails to include both text and HTML versions.
Enhancement: Added support for templates when sending ad-hoc emails.
Enhancement: Added support for Cc and Bcc headers when sending ad-hoc emails.
Enhancement: Added ability to set the Host and Port parameters when sending ad-hoc emails using Ad Hoc Email File Transfer trigger action.
Enhancement: Added ability to manage server, host, client and PGP keys from administrative web interface.
Enhancement: Added ability to request CAPTCHA information to be entered during login.
Enhancement: Added ability to display maximum number of downloads in ad-hoc email messages.
Enhancement: Added Sql Query trigger action that allows for exporting of database queries to a CSV file.
Enhancement: Updated FTP protocol implementation to improve memory usage.
Enhancement: Added User Detail metric to reporting module that aggregates and reports on data at user level.
Enhancement: Added warning message when user attempts to connect with JSCAPE MFT Server using a version of JSCAPE MFT Server Manager that is not compatible.
Enhancement: Added support for failover synchronization of ad-hoc file transfers.
Enhancement: Improved performance for large quantities of ad-hoc file transfers.
Enhancement: Improved Java applet file transfer client.
Enhancement: Remove Upload button from web interface if upload permissions are not enabled.
Enhancement: Added ability to restrict Banned Files entries to a Path that may be recursive.
Enhancement: Added time and throughput information to logging format and various reporting metrics.
Enhancement: Improved performance of ad-hoc file transfers.
Bug Fix: Resolved issue experienced by domain administrators when trying to edit a user from the web interface.
Bug Fix: Resolved issue with incorrect logo being used in web interface.
Bug Fix: Resolved issue with reverse proxies mapped to a remote SFTP service that resulted in reverse proxy being unavailable.
Bug Fix: Resolved issue with trading partners duplicated in user interface.

Bug Fix: Resolved issue with missing Revoke and Extend button text/image in web interface.
Bug Fix: Resolved issue with some SFTP uploads to server stalling at around 1GB.
Bug Fix: Miscellaneous bug fixes.

Release 8.7

Jul. 12, 2013

Enhancement: Added iOS client to Enterprise edition for use in transferring, viewing and sharing files.
Enhancement: Added support for AS2 service.
Enhancement: Added support for AS2 trading partners.
Enhancement: Added AS2 support to trading partner related trigger actions.
Enhancement: Improved SFTP service performance.
Enhancement: Improved error message returned in the event user attempts to use a previously used password that violates password compliance settings.
Enhancement: Trigger module now displays an error message in the event user tries to run a trigger that has not been saved.
Enhancement: Added Max connections/user option to Connections module.
Enhancement: Added ability to prefer AFTP protocol when using Java applet v.s. WebDAV protocol.
Enhancement: Ad-hoc file transfer passwords are now automatically trimmed to prevent validation errors during copy/paste.
Enhancement: Updated Branding URL module so that it is applied to Logout, Reset Password and Registration pages.
Enhancement: Added client REST API functions for retrieving tags.
Enhancement: Improved usability and syntax handling of functions and variables in Triggers module.
Enhancement: Added Delete On Upload/Delete On Download options to all Regex File Upload/Download trigger actions.
Enhancement: Improved resource editor in Server > Settings > Email > Resources panel.
Enhancement: Updated User and User Template panels to be more intuitive.
Enhancement: Redesigned Trading Partners user interface.
Enhancement: Added a js-triggersreport command line utility that will provide a report of all triggers, actions and settings.
Enhancement: Added support for various SHA2 MAC ciphers used in SFTP service.
Enhancement: Improved server0.log rotation logic so that it is not automatically rotated on restart.
Enhancement: Redesign of Domain Administration panels for User and User Template.
Enhancement: Added AuthenticationMethod property to User Login event.
Enhancement: Added asynchronous execution support to trigger definitions.
Bug Fix: Changed default encoding of Country attribute in server certificates from UTF8 to ASCII.
Bug Fix: Resolved zlib issue with SFTP service.
Bug Fix: Resolved a number of issues with File Transfer Command Line langage used in File Transfer Script trigger action.
Bug Fix: Resolved issue where rebuilding index causes tags to be lost.
Bug Fix: Resolved issue with Trading Partner Rename File action.
Bug Fix: Resolved issue with Trading Partner Create Directory action.
Bug Fix: Resolved issue where variables could not be used in the Email field for a user in a User Template.
Bug Fix: Resolved issue where HTTP sessions were not properly closed.
Bug Fix: Resolved issue where File Download event was fired for failed SFTP file downloads.
Bug Fix: Fixed performance issue experienced when navigating to a remote directory that is mapped to a reverse proxy when using Java applet.
Bug Fix: Updated indexing engine to prevent locking issues.
Bug Fix: The Runtime column in Triggers > Recent panel now displays updated time for running triggers.
Bug Fix: Resolved issue where settings in Server > Settings > Web > Resources were not being maintained across upgrades.
Bug Fix: Resolved issue displaying large PDF files in web document viewer.
Bug Fix: Resolved issue with case-insensitive user names.

Bug Fix: Resolved issue with testing reverse proxy mapped to a WebDAV service.
Bug Fix: Resolved issue authenticating with SSL based LDAP service.
Bug Fix: Resolved issue where user was able to tag non-existing files using REST API.
Bug Fix: Resolved issue with ReplaceAll function in Triggers module.
Bug Fix: Resolved issue where users are unable to download files that are tagged within a sub-directory.
Bug Fix: Resolved issue where users are unable to navigate to a tagged directory.
Bug Fix: Resolved exception thrown in Aftp Create Directory action.
Bug Fix: Resolved issue with Trading Partner Regex File Upload action.
Bug Fix: Resolved retry issue with Trading Partner related trigger actions.

Release 8.6
Mar. 8, 2013

Enhancement: Various performance improvements to AFTP protocol.
Enhancement: Added support for specifying default selected user interface option when logging in via web interface.
Enhancement: Updated SFTP and SCP related trigger actions to use extended cipher set.
Enhancement: Updated trigger actions to allow for use of variables in all input elements.
Enhancement: Improved SSL/TLS Cipher Suites panel for FTPS and HTTPS protocols.
Enhancement: Added support for disabling CAPTCHA during web based self-registration.
Enhancement: Added ability to prioritize, pause and resume a number of trigger actions.
Enhancement: Updated web interface to automatically save virtual paths and IP access rules when changed.
Enhancement: Updated SFTP trigger actions, reverse proxies and trading partners to support extended set of ciphers.
Enhancement: Updated client web interface to provide protection against CSRF (Cross-Site Request Forgery) attacks.
Enhancement: Updated web interface so the View icon is only enabled for those document types supported by web document viewer.
Enhancement: Updated web document viewer to display a user friendly error message in the event that a document cannot be displayed.
Enhancement: Added client REST API for use in performing file transfers, ad-hoc file transfers and contact management.
Enhancement: Added support for displaying SWF files in web document viewer.
Bug Fix: Resolved issue where administrator is unable to update a Contact name in JSCAPE MFT Server Manager.
Bug Fix: Resolved failover synchronization issues.
Bug Fix: Resolved issue where REST services are not automatically started after failover synchronization.
Bug Fix: Resolved unresponsive Cancel button when deleting a Contact, URL Branding or Drop Zone via the web interface.
Bug Fix: Resolved issue with canceling Check Email trigger action.
Bug Fix: Resolved class name obfuscation issues in management API.

Release 8.5
Jan. 11, 2013

Enhancement: Added REST API for use in managing JSCAPE MFT Server.
Enhancement: Added web administration interface for adding, deleting, starting, stopping and pausing domains.
Enhancement: Updated web document viewer to be automatically included as part of JSCAPE MFT Server Enterprise Edition release.
Enhancement: Added ability to specify whether ports are included in HTTP headers.
Enhancement: Added ability to tag multiple documents simultaneously via the web interface.

Enhancement: Added Run button to Directory Monitors module providing ability to run a directory monitor manually.
Enhancement: Improved performance for ad-hoc file transfers.
Enhancement: Added ability to optionally include all event properties as part of request in Http Request trigger action.
Enhancement: Automatically remove leading and trailing spaces from input fields in JSCAPE MFT Server Manager prior to saving.
Enhancement: Added ability to enable/disable display of certain sections in My Account page at User and User Template levels.
Enhancement: Added GetUserInfo function for use in trigger actions to retrieve information on a user account.
Enhancement: Added IsUserMemberOfGroup function for use in trigger actions to check if a user is a member of a group.
Enhancement: Updated Key Manager to prompt user to save keys if they attempt to exit Key Manager with unsaved changes.
Enhancement: Added optional Reply To field in Send Email action.
Enhancement: Updated client web interface in steps towards 508c compliance.
Enhancement: Numerous usability updates to Java applet used in web interface.
Bug Fix: Resolved issue with virtual paths being duplicated when a domain administrator adds a user via web interface.
Bug Fix: Resolved issue with users being unable to use WebDAV/Java applet when username contain @ symbol.
Bug Fix: Resolved issue with saving directory monitors.
Bug Fix: Resolved issue with LDAP authentication modules where LDAP port value was overridden with LDAP timeout value.
Bug Fix: Resolved issue with js-adduser command line utility where user password change rights were not matching that of the template used.
Bug Fix: Updated regular expression for US SSN to prevent identifying certain credit card data as US SSN.
Bug Fix: Resolved issue with password history not working correctly in some unique cases.
Bug Fix: Resolved issue with PGP encrypted virtual directories not working correctly.
Bug Fix: Resolved issue with importing and using PGP public keys.
Bug Fix: Resolved issue with default web view for accounts.
Bug Fix: Resolved issues in Zip Directory and System Configuration Backup actions that resulted in invalid ZIP archives being created.
Bug Fix: Resolved internal error message when trying to add a virtual path via web interface.
Bug Fix: Resolved issue experienced in some accounts requiring a password change on first time login.
Bug Fix: Resolved issue with Ad Hoc File Transfer action where incorrect port value of 0 may be used if email.url.host value is set but email.url.port value is not set.
Bug Fix: Resolved issue where incorrect error message displayed if user is denied access due to user level IP Access rules.
Bug Fix: Resolved issue where changes made by a domain administrator to the "Allow password change" option for an account are not saved when updating user via web interface.

Release 8.4
Aug. 14, 2012

Enhancement: Major upgrade to the JSCAPE MFT Server Manager user interface in order to more effectively support multiple domains and reduce overall memory and CPU consumption.
Enhancement: Added automatic ssl.cfg update to work with graphical installers using IBM JVM.
Enhancement: Added optional expiration date to ad-hoc file transfers allowing users to send non-expiring ad-hoc file transfers.
Enhancement: Added ability for users to register for new accounts using the web interface.
Enhancement: Improved update process so that customizations made to language files are not lost during an upgrade.

Enhancement: Added optional argument to specify a user template when using the js-adduser command line utility.
Enhancement: Added ability to test SMTP server settings and send a test email message.
Enhancement: Improved error message displayed when invalid credentials are entered and manual synchronization is performed.
Enhancement: Improved firewall support for remote JMX sessions providing settings for both server and registry ports.
Enhancement: Various performance enhancements made to the AFTP protocol.
Enhancement: Changed "Monitor interval (sec)" field for directory monitors to be optional allowing for directory monitors to be run on demand or on a scheduled basis using the newly added Run Directory Monitor trigger action.
Enhancement: Several updates to the Java applet user interface.
Enhancement: Various performance enhancements to SFTP protocol.
Enhancement: Updated triggers module to retain recent trigger history regardless of whether changes are made to triggers.
Bug Fix: Resolved issue where some command line utilities would raise an exception when used in combination with custom trigger actions.
Bug Fix: Resolved issue where user was unable to resume a canceled file transfer in Java applet window.
Bug Fix: Resolved issues experienced with reverse proxies when "Map current local directory to remote directory" option was enabled.
Bug Fix: Resolved variable expansion issue experienced in the email.lostpassword.body and email.lostpassword.subject resource properties.
Bug Fix: Resolved issue where PGP keys exported from JSCAPE MFT Server cannot be imported into GnuPG 2.x.
Bug Fix: Resolved issue where failover IP substitution does not work correctly under automatic synchronization.
Bug Fix: Resolved issue in Convert File trigger action where UNIX to MS-DOS conversions were not working correctly.
Bug Fix: Resolved issue where adding a duplicate account via JSCAPE MFT Server Manager correctly results in an error message but incorrectly lists duplicate account in users list.
Bug Fix: Resolved issue where "Current connections" and "Total connections since start" values reported by JSCAPE MFT Server Manager are corrupted from incoming WebDAV connections.

Release 8.3
May 9, 2012

Enhancement: Added support for streaming compression to AFTP protocol.
Enhancement: Added ability to use search results as argument to a report.
Enhancement: Added ability to re-run a report.
Enhancement: Updated syntax for functions to be consistent across trigger conditions and actions parameters.
Enhancement: Added GetPathSeparator function in triggers module to return the OS specific path separator used.
Enhancement: Disabled form auto-complete in web interface for sensitive fields.
Enhancement: Updated login and account reset password error messages to prevent attackers from trying to guess valid usernames.
Enhancement: Added HttpOnly flag to session cookie to prevent session information from being potentially exposed to scripts.
Enhancement: Added input validation for all fields in web interface to prevent potential XSS attacks.
Enhancement: Added old password verification when changing password via web interface, requiring that users enter their old password to set a new password.
Enhancement: New session ID is now generated after login when using web interface.
Enhancement: Exposed syslog service descriptor in management API.
Enhancement: Added check to prevent importing of certificates into key manager without a valid matching private key.

Enhancement: Improved memory consumption in Java applet and improved progress monitor when transferring directories.
Bug Fix: Resolved issue with DLP module that could release files that have been modified but not yet re-indexed.
Bug Fix: Resolved issue where user could not rename a file if download permissions were not granted.
Bug Fix: Resolved issue in SFTP protocol where IP may be blocked but user is still able to perform authentication attempts using an existing connection.
Bug Fix: Resolved memory leak issue when performing failover synchronization.
Bug Fix: Resolved issue with potential socket timeouts in automatic failover synchronization.
Bug Fix: Resolved issue of uploading files to server over SCP using wildcards.
Bug Fix: Resolved issue when using shared review capabilities in Acrobat Pro with WebDAV service.
Bug Fix: Resolved issue of no data being presented when generating report using same start date and end date arguments.
Bug Fix: Resolved issue regarding use of variables in email.password.subject property when performing ad-hoc file transfers.
Bug Fix: Resolved issue with FTPS protocol where if download permission is not granted and user attempts to download a file a data connection channel is never opened by server resulting in data channel timeout by some clients.
Bug Fix: Resolved issue with Run Process action hanging when using Windows powershell script.
Bug Fix: Resolved issue where the "Uploaded since start" value displayed in JSCAPE MFT Server Manager is incorrectly incremented by two for each file uploaded when using SFTP protocol.
Bug Fix: Resolved potential memory issue experienced when using verbose database logging.
Bug Fix: Resolved authentication issue experienced when connecting to ApacheDS LDAP service.
Bug Fix: Resolved issue with potential incorrect remote directory used in Trading Partner Regex File Download action.
Bug Fix: Resolved issue with IP/host not being properly saved when making changes to JMX settings.
Bug Fix: Resolved text label issue with dialog displayed in IE when attempting to overwrite an existing file.

Release 8.2
Feb. 20, 2012

Enhancement: Added support for listing available domains in a domain drop-down field when logging in via web interface.
Enhancement: Added AFTP file transfer actions to triggers module.
Enhancement: Added check to see whether a private key is in use before allowing key to be deleted from Key Manager.
Enhancement: Added sessionid variable which reports a unique session ID for user operations that are part of a user session. The sessionid variable is available for use in triggers module.
Enhancement: Added GetFileExists and GetFileSize functions to triggers module. These functions may be used to check whether a file exists and it's size.
Enhancement: Updated progress dialog from modal to non-modal.
Enhancement: Added ability to pause/resume in Running log view.
Enhancement: Added labels to date fields specifying expected date format.
Enhancement: Added support for PEM and PKCS#8 formats when exporting a private client key.
Enhancement: Added ability to export private server keys.
Enhancement: Added "none" to default list of supported compression types for SFTP service.
Update: Removed support for Flash uploads. All uploads are now performed using native file upload capabilities of browser.
Bug Fix: Resolved file locking issue in AFTP service.
Bug Fix: Resolved error with Chrome and IE browsers connecting using SSL.
Bug Fix: Resolved issue with Sftp File Upload action when Overwrite If File Exists option is enabled.
Bug Fix: Resolve line termination issue for directory listings when using FTP/S protocols.
Bug Fix: Resolved lexical processing error experienced with web upload form variables used in trigger conditions.

Bug Fix: Resolved issue experience when sending email to/from long email addresses.

Bug Fix: Resolved issue with incorrectly reported Current transfers value as reported in JSCAPE MFT Server Manager.

Bug Fix: Resolved issue in Ftp Regex File Download action that would attempt to download a matching directory.

Bug Fix: Resolved issue with importing SSH public keys.

Bug Fix: Resolved issue with non-existing file being returned in directory listings.

Release 8.1
Jan. 14, 2012

Enhancement: Complete rewrite of the AFTP protocol providing for accelerated file transfers over high latency networks.

Enhancement: Added support for password policies when generating passwords for ad-hoc email file transfers.

Enhancement: Updated UI for trading partners module.

Enhancement: Added ability to create a drop zone from the management API.

Enhancement: Added support for multi-word phrases when tagging files via web interface.

Enhancement: Added ability to specify what SSL/TLS protocols are used.

Enhancement: Added ability to specify a footer message that is appended to all ad-hoc email file transfers.

Enhancement: Added support for limiting what top level domains (TLD) and/or email addresses an ad-hoc email file transfer may be sent to.

Enhancement: Added additional reporting to activity log showing when a trigger is queued and finished.

Enhancement: Added host key verification support to FTPS, SFTP and SCP related actions and trading partners module.

Enhancement: Redesigned Key Manager and added section for managing host keys.

Update: Updated license agreement removing SaaS usage restriction.

Bug Fix: Resolved gradual memory leak experienced often over several weeks.

Bug Fix: Resolved CPU utilization issue when connecting to web server using IE 9 browser.

Bug Fix: Resolved issue where a trigger will not fire and nothing is reported to the log in cases where maximum trigger resource limit is reached.

Bug Fix: Fixed issue with dialog disappearing after uploading a file using a drop zone.

Bug Fix: Fixed issue with JMX service not properly releasing port when JMX service is disabled.

Release 8.0
Sep. 1, 2011

Enhancement: Added DLP (data loss prevention) module available in Enterprise edition.

Enhancement: Redesign of Logging module to provide more visibility into user activity.

Enhancement: Added support for OpenPGP encrypted virtual directories.

Enhancement: Added support for multiple administrators.

Enhancement: Improved memory performance for directory monitors.

Enhancement: Improved memory performance for search indexing.

Enhancement: Added ability to send passwords for ad-hoc file transfers out-of-band.

Enhancement: Added support for selecting multiple files for upload when using HTML user interface.

Enhancement: Added ability to extend scope of Banned Files module to include directories.

Enhancement: Implemented various usability and performance enhancements to user interface in JSCAPE MFT Server Manager application.

Enhancement: Added ability to create contacts while creating an ad-hoc file transfer.

Enhancement: Added Trading Partner Directory Upload Synchronization and Trading Partner Directory Download Synchronization actions.

Enhancement: Added passive setting for Directory Upload Synchronization and Directory Download Synchronization actions.

Enhancement: Added support for IPv6 addresses in web services.

Enhancement: Added ability to move files and folders on server using drag and drop.
Enhancement: Added a Disable Inactive Accounts action.
Enhancement: Added column sorting support to Recent tab in Triggers module.
Enhancement: Added ability to force a user to change their password upon first login via web interface.
Enhancement: Added optional Time Expression dialog for use in creating scheduled triggers when using Current Time event.
Enhancement: Updated a number of file transfer related actions in Triggers module moving advanced connection parameters to an Advanced tab.
Bug Fix: Fixed issue where AFTP UDP and AFTP TCP services could not listen on the same port.

Release 7.2
Apr. 18, 2011

Enhancement - Added experimental AFTP (Accelerated File Transfer Protocol) service designed to provide file transfers over low latency networks using UDP or TCP protocols.
Enhancement - Added support for SCP protocol to SFTP service.
Enhancement - Added status of domain next to domain node.
Enhancement - Added ability to pause a domain in order to stop accepting new connections.
Enhancement - Added js-copyusers utility that allows for copying or migrating users from one domain to another
Enhancement - Added ability to specify a private key for for SFTP Reverse Proxy and client certificate for FTPS Reverse Proxy.
Enhancement - Added server.vmoptions to System Configuration Backup action
Enhancement - Added a js-importcontacts utility for importing contacts
Enhancement - Added NewAccount attribute to Account Updated event in order to detect when a new account is created
Enhancement - Added js-pausedomain in order to stop accepting new connections
Enhancement - Added js-resumedomain to resume accepting new connections
Enhancement - Added ability to view and manage previous ad-hoc file transfers from the web user interface
Enhancement - Added ability to perform an orderly server shutdown
Enhancement - Added ability to specify whether existing files should be overwritten when uploading files to a drop zone
Change - Default service type to explicit SSL when adding a new FTP service
Bug Fix - Fixed issue where condition expression was rewritten when saved
Bug Fix - Fixed issue where triggers could be created without using a unique name.
Bug Fix - Fixed documentation issue in Trading Partners module
Bug Fix - Fixed required field error in File > Settings > Email section of JSCAPE MFT Server Manager
Bug Fix - Fixed issue with Run Process action where double quotes are not stripped before passing argument to executing program
Bug Fix - Fixed issue where Banned Files are banned from upload but not from renaming.

Release 7.1
Nov. 14, 2010

Enhancement: Redesign and improved usability of condition builder in triggers module.
Enhancement: Added context sensitive help to triggers module for events, event variables, actions and functions.
Enhancement: Added contact management capabilities for use in ad-hoc file transfers.
Enhancement: Added ability to specify IP Access restrictions at user level.
Enhancement: Added ability to view/manage active sessions for all protocols.
Enhancement: Added multiple concurrent file transfer support to Java applet interface.
Enhancement: Added Company attribute to user accounts.
Enhancement: Added API support for managing remote directories.
Enhancement: Added File Upload Quota Exceeded, File Download Quota Exceeded and File Transfer Quota Exceeded events that are fired when a transfer quota is exceeded.

Enhancement: Added ability to specify an optional command to be executed on remote FTP/S servers after login but prior to action execution for FTP/S related actions and trading partner definitions.
Enhancement: Added Twitter actions for sending direct messages and status updates.
Enhancement: Added ability to set session TTL for HTTP/S sessions.
Enhancement: Updated web interface so that Domain field is automatically populated in Lost Password screen if “Default domain” option is enabled.
Enhancement: Updated custom action API to support context sensitive help.
Enhancement: Updated tag cloud to be sorted in descending order.
Enhancement: Added ability to specify whether adaptive connection is used and whether subsystem reply is required in SFTP reverse proxy and SFTP action definitions.
Update: Renamed product to JSCAPE MFT Server to better reflect product capabilities.
Update: Replaced evaluation license with community license and changed limitations of community license to support up to 5 users/connections and 1 domain with all other functionality enabled.
Update: Changed reverse proxy definition to load optional private key used in SFTP and FTPS protocols from a file rather than load from “Server Keys” module.
Bug Fix: Resolved issue where trigger would not show up with Failed status under Recent tab of triggers module when using an invalid function definition.
Bug Fix: Resolved issue where datastore location could not be changed for a domain.
Bug Fix: Resolved issue with drop zones where uploading to a drop zone may not upload to the correct directory.
Bug Fix: Resolved issue with user passwords that contained a % character.
Bug Fix: Added missing image to Manage Tags button in web interface.
Bug Fix: Removed .svn directories from product distribution.

Release 7.0
Aug. 18, 2010

Enhancement: Added ability to tag/search documents with keywords using the web interface for improved searching.
Enhancement: Added ability to store the credentials for remote systems using a new admin module called Trading Partners.
Enhancement: Added ability to retry outgoing emails if failure occurs initially.
Enhancement: Added ability to allow a user to belong to more than one group.
Enhancement: Added ability to allow a user to connect to a different JSCAPE MFT Server without having to stop/start the JSCAPE MFT Server Manager.
Enhancement: Added ability to list & enable/disable users using the command line API**.**
Enhancement: Added ability to stop an administrator being able to delete their own account.
Enhancement: Added ability to manage large numbers of users via the GUI without sacrificing performance.
Enhancement: Added ability to import existing public keys and have them automatically converted to X.509 format.
Bug Fix: Fixed issue with API Doc and actual functionality being out of sync for AbstractAction.
Bug Fix: Fixed issue with Trigger concurrency limit now set per trigger and not across all triggers as previously.
Bug Fix: Fixed issue with Automatic login no longer working.
Bug Fix: Fixed issue with Default connection being overwritten, rather it should add a new connection to the list when adding a connection.

Release 6.6
Jun. 7, 2010

Enhancement: Added ability to check disk quota before a file upload (web interface) to ensure that disk quota will not be exceeded.
Enhancement: Added ability to store the last login date for a user.
Enhancement: Added ability to migrate changed text labels (web interface) so that they also appear post-upgrade.

Enhancement: Added ability to access the server version number as a function in trigger actions.
Enhancement: Added ability to access the user group as a function in trigger actions.
Enhancement: Added ability to access the users root directory as a function in trigger actions.
Enhancement: Added ability to disable a user account as an action.
Enhancement: Added ability to define global parameters available to all trigger actions as a function.
Enhancement: Added ability to limit the number of concurrent triggers.
Enhancement: Added ability to print a report of all users and their attributes.
Enhancement: Added ability to list inactive/active users via the management API.
Enhancement: Added ability to specify a Secondary LDAP server for failover authentication purposes.
Enhancement: Added ability to remove an IP from IP Access list without domain restart.
Enhancement: Added option to specify if a remote file should overwritten (web interface).
Enhancement: Added ability to run a report showing expiring encryption keys.
Enhancement: Added ability to specify domains to startup on initialization.
Enhancement: Added ability to synchronize sub-folders when synchronizing directories in Directory Upload Synchronization and Directory Download Synchronization actions.
Enhancement: Added ability to set user permissions via the command line in js-adduser, js-adduserdir, js-addgroup and js-addgroupdir utilities.
Enhancement: Added ability to disable/resume file upload operation.
Enhancement: Added ability to cancel an upload when viewing a form.
Enhancement: Added ability to ensure that a user has download access before sending an email
Enhancement: Added ability to upload files anonymously using a Drop Zones module.
Enhancement: Added ability to specify multiple custom logos at a domain level using URL Branding module.
Enhancement: Added option to specify a section (Storage or My Account) to redirect users to upon login (web interface).
Enhancement: Added option to confirm overwriting existing files within applet.
Enhancement: Changed behavior of IP Access Rules Updated and IP Blocked events so that events are only fired if IP does not already exist in IP Access list..
Bug Fix: Fixed issue with missing comments against some API's.

Release 6.5
Mar. 31, 2010

Enhancement: Added js-passwd command line utility for use in changing account passwords.
Enhancement: Added ability to see recent (last 1000) trigger executions
Enhancement: Added ability to pass original event information to Trigger Error event using variables and Trigger Error Message field.
Enhancement: Added ability to enable/disable ad-hoc email at the domain level.
Update: Removed update of directory monitor quotas when uploading/deleting files in order to avoid potential performance issues related to quota synchronization.
Bug Fix: Resolved issue with Check Email action where unique message ID used in storing messages contained illegal filename characters.
Bug Fix: Resolved issue experienced when using Adobe Flash upload component in Internet Explorer browser.

Release 6.4.0.4
Jan. 18, 2010

Enhancement: Added ability to use built-in functions within trigger actions.
Enhancement: Added ability to limit the user interface options available when using web client.
Enhancement: Added Login.FOOTER variable to File > Settings > Web > Resources for use in defining a footer in login page.
Enhancement: Added Zip Regex File action for use in creating ZIP file based on regular expression.
Enhancement: Added ability to define multiple connection settings in File > Settings > Connection panel for use in managing many remote servers.

Enhancement: Added restart script to server.
Bug Fix: Fixed issue with files not being properly overwritten when using SFTP reverse proxy.
Bug Fix: Fixed NullPointerException error experienced when upgrading previous version.

Release 6.3.0.6
Dec. 15, 2009

Enhancement: Added ability to specify banned files for upload.
Enhancement: Added ability to limit days of week and times that users may connect.
Enhancement: Added ability to specify continue argument without specifying login credentials when integrating web interface with external applications.
Enhancement: Added ability to password protect ad-hoc email links.
Enhancement: Removed requirement for specifying user account password in Ad Hoc Email File Transfer action.
Bug Fix: Fixed issue with ad-hoc email hostname used when server is installed in NAT environment.
Bug Fix: Fixed issue with ad-hoc email links becoming invalid if user changes account password.
Bug Fix: Fixed issue with creating reports.

Release 6.2.0.24
Nov. 17, 2009

Enhancement: Added upgrade wizard to GUI installer.
Enhancement: Added Rename permissions flag to virtual directories.
Enhancement: Improved parsing of ssl.cfg file.
Update: Changed private client key export so that both keystore and key are password protected.
Bug Fix: Resolved issue with 0 bytes of data being reported in log file for ASCII downloads.
Bug Fix: Resolved line termination issue with directory listing commands in FTP/S protocols.

Release 6.2.0
Nov. 9, 2009

Enhancement: Added ability to specify link expiration range when performing ad-hoc email file transfers via web interface.
Enhancement: Improved performance for updating directory monitor and bandwidth quotas.
Enhancement: Added ability to require secondary level of authentication using client certificates in HTTP/S and WebDAV/S protocols.
Enhancement: Added ability to set cipher strength used in SSL protocols.
Enhancement: Added "Server name" field to File > Settings > Web panel. This may be used to specify an alternative host name when server is behind a NAT protected firewall in order to prevent leaking of internal IP information.
Enhancement: Added Ad Hoc Email File Transfer action for performing ad-hoc email file transfers programmatically.
Bug Fix: Resolved issue with temporary files not being deleted that were created during indexing of PDF documents.

Release 6.1.0.60
Oct. 16, 2009

Enhancement: Added ability to specify a continue parameter in automatic login via URL.
Update: Added JavaDoc for Action and AbstractAction classes.
Bug Fix: Fixed issue with SSL and LDAP authentication modules.
Bug Fix: Fixed issue with phone authentication module.

Release 6.1.0.53
Oct. 5, 2009

Enhancement: Added ability to execute Current Time event triggers on demand.
Update: Changed maximum timeout values for FTP/S and SFTP protocols to 999 minutes.
Bug Fix: Fixed issue with public key authentication in SFTP protocol.

Release 6.1.0.50
Sep. 28, 2009

Enhancement: Added Copy Regex File and Move Regex File trigger actions.
Enhancement: Added Tar Directory action for creating a TAR archive of a directory.
Enhancement: Added Append File action for appending messages to a file.
Enhancement: Updated all SFTP related actions so that password is optional, providing support for password-less public key authentication.
Enhancement: Added ability to disable a trigger.
Enhancement: Updated Maximum password age field in Compliance panel to support up to 999 days.
Enhancement: Added ability to retrieve event variables within custom action code.
Enhancement: Added ability to sign and view signatures for OpenPGP keys.
Enhancement: Added ability to specify a hostname in Passive IP field allowing for IP resolution when using a dynamic IP.
Enhancement: Added Ftp Rename File, Ftps Rename File and Sftp Rename File trigger actions.
Enhancement: Added Ftp Create Directory, Ftps Create Directory and Sftp Create Directory trigger actions.
Enhancement: Added ability to specify JDBC connection pool size and time-to-live for connections in Database Log and DB Datastore modules.
Enhancement: Added ability to select multiple files for upload in HTML user interface using optional Flash plug-in.
Enhancement: Added ability to automatically start domain/services on failover server after synchronization.
Enhancement: Added additional information to server log to detect source of failed user authentications.
Enhancement: Added ability to set expected successful return code(s) using a regular expression in Run Process trigger action.
Update: Changed logging level for client read timeout messages so they only show up in log with FINE logging level enabled.
Update: Changed "Test parameters" functionality in LDAP Query Authentication module to check filter parameters in addition to user authentication.
Update: Changed default setting for ""Create account if not found" option in various authentication modules to enabled.
Update: Various updates to API JavaDoc.
Update: Changed behavior in Failover module so that production server will startup even if failover server is down.
Bug Fix: Fixed issue with NTLM Authentication settings not being displayed properly when using multiple domains.
Bug Fix: Fixed issue with improper server response to EPSV command.
Bug Fix: Fixed issue with Delete Files Older Than property in Delete Files trigger action.
Bug Fix: Fixed issue with with logos not being updated properly in IE browser when using multiple domains with different logos.

Release 6.0
July 27, 2009

Enhancement: Added support for document (MS Word, Excel, PDF, text, HTML) indexing and searching via web interface.
Enhancement: Added ability to bypass password aging compliance at user level.
Enhancement: Added PGP fingerprint information to PGP view dialog.
Enhancement: Added ability to resize all dialogs in JSCAPE MFT Server Manager.
Enhancement: Added ability for users to generate public keys for use in public key authentication (SFTP) from web interface.

Enhancement: Added number of files deleted information to log when executing Delete Files action.
Bug Fix: Fixed issue with trigger flow when one or more actions fail.
Bug Fix: Fixed issue with "Browse subdirs" directory permissions.
Bug Fix: Fixed issue with File Upload event not being fired when using UNC paths.
Bug Fix: Fixed issue with password change reminder being sent at wrong time.
Bug Fix: Fixed issue with regular expressions in Delete Files action.
Bug Fix: Fixed issue with automatic inactivity logout dialogs in web interface.
Bug Fix: Fixed issue with copying User/Group in JSCAPE MFT Server Manager.
Bug Fix: Fixed issue with editing virtual path that uses a reverse proxy.
Bug Fix: Fixed issue with User Login event fired when login fails.

Release 5.2
Jun. 2, 2009

Enhancement: Added support for submitting custom form data when uploading files via HTML user interface.
Enhancement: Added ability to set syslog facility.
Enhancement: Added integration support for JSCAPE Web Document Viewer product. This product allows users to view documents on the server using a web based embedded document viewer.
Enhancement: Added integration support for JSCAPE MFT Server Plugin for Outlook. This product allows users to perform ad-hoc email file transfers directly from Outlook email clients.
Enhancement: Added ability to copy a group.
Enhancement: Added ability to copy a user.
Enhancement: Added IPv6 support for all protocols.
Bug Fix: Fixed issue with File Upload event being fired twice when using a reverse proxy.
Bug Fix: Fixed path editing issue in JSCAPE MFT Server Manager
Bug Fix: Fixed issue with trigger action information being lost during upgrade.

Release 5.1
Mar. 30, 2009

Enhancement: Added support for enabling/disabling passive transfers in all FTP/FTPS related trigger actions.
Enhancement: Added retry interval property to all file transfer trigger actions to define the wait period before retrying a file transfer.
Enhancement: Added extension field to phone number.
Enhancement: Changed adhock.email.prebody variable in File > Settings > Email > Resources of JSCAPE MFT Server Manager to use user's real name.
Enhancement: Added UsernameEmail and UsernameName variables to all trigger events that have Username variable. These events allow for retrieval of the user's email address and real name respectively.
Bug Fix: Fixed issue in WebDAV protocol and Java Applet with properly escaping filenames.
Bug Fix: Fixed issue in that server was using random source port instead of expected port 20 for non-passive transfers.
Bug Fix: Fixed NullPointerException experienced when using Database Query Authentication module.
Bug Fix: Fixed append issue experienced when using SFTP protocol.

Release 5.0
Feb. 23rd, 2009

Enhancement: Improved performance for PGP encryption and decryption actions.
Enhancement: Added token-less two-factor authentication support.
Enhancement: Improved performance for directory monitors.
Enhancement: Added ability to define a file latency period for a directory monitor.

Enhancement: Added ability to assign a directory monitor to a user.
Enhancement: Added check for whether file is being currently written to in a directory monitor.
Enhancement: Added ability to view bandwidth quotas and directory monitor quotas for a user via web interface.
Enhancement: Added built-in support for Spanish, French, German and Russian to web interface.
Enhancement: Updated LDAP Query Authentication module to support using different LDAP user credentials for authentication and search.
Enhancement: Added js-sendmessage command line utility for emailing all accounts for a domain.
Enhancement: Updated custom authentication API to support validation of client IP address.
Change: Updated system requirements to JVM 1.5 and above.
Bug Fix: Fixed issue with not returning error when creating a directory that already exists using FTP/S or SFTP protocols.
Bug Fix: Fixed issue with setting bandwidth quotas under Professional license type.
Bug Fix: Fixed issue with Run Process trigger action.

Release 4.5
Jan. 26th, 2009

Enhancement: Added ability to hide domain and/or specify default domain used in web interface.
Enhancement: Added ability to accept multiple delivery addresses in ad-hoc email file transfer module.
Bug Fix: Fixed issue experienced when installing only the JSCAPE MFT Server Manager component using GUI installer.
Bug Fix: Fixed issue with setting user bandwidth quotas under Professional edition.
Bug Fix: Fixed issue with expiration date information sent in password reminders.
Bug Fix: Fixed issue with resuming file transfers in SFTP protocol.

Release 4.4
Dec. 26, 2008

Enhancement: Added Delete Accounts action to Triggers module for deleting expired or disabled accounts.
Enhancement: Added email address to manage users view in web interface.
Bug Fix: Fixed email notification service so email.url.host is used if entered.
Bug Fix: Fixed issue with PGP encrypting/decrypting files.
Bug Fix: Fixed issue with Send Email action throwing a NullPointerException.
Bug Fix: Fixed issue with backuplog command line utility.
Bug Fix: Fixed API so that ssl.cfg is used when using JVM other than that provided by Sun Microsystems.

Release 4.3
Nov. 14, 2008

Enhancement: Added NTLM authentication support.
Change: Renamed example dsa and rsa keys to example_dsa and example_rsa.
Bug Fix: Fixed issue with MD5 and SHA1 hashes generated when using MD5Hasher and SHA1Hasher classes in authentication modules.

Release 4.2
Nov. 7, 2008

Enhancement: Added optional syslog reporting support.
Enhancement: Added js-ipaccess command line utility to manage IP access list.
Enhancement: Increased maximum available retry limits in FTP, FTPS and SFTP file transfer trigger actions from 3 to 9.
Enhancement: Change server behavior so adding or deleting an IP access rule does not require a domain restart.
Enhancement: Added regular expression support for event integer values when creating trigger conditions.

Enhancement: Added ability to set domain administration rights when creating a user template.
Enhancement: Added PAM Authentication module to support authenticating users against native UNIX user databases.
Enhancement: Improved ease of use for entering IP addresses when defining services.
Enhancement: Added ability to automatically unblock an IP address after a certain period of time of being blocked due to too many unsuccessful logins.
Enhancement: Added ability to automatically re-enable an account after a certain period of time of being disabled due to too many unsuccessful logins.
Bug Fix: Fixed trigger timeout issue where if an action ran for more than an hour subsequent actions would not be processed.
Bug Fix: Fixed issue with password policies not being enforced when creating users via web user interface.
Bug Fix: Fixed issue with creating a directory, renaming files or emailing multiple files in HTML user interface when using Windows Vista and IE7.
Bug Fix: Fixed issue in js-adduser command line utility.
Bug Fix: Fixed issue in js-adduserdir command line utility.
Bug Fix: Fixed issue with being unable to download files via HTML user interface that contain special characters.
Bug Fix: Fixed performance issue experienced when assigning accounts to a group.
Bug Fix: In File > Settings > Email panel of JSCAPE MFT Server Java Management API client keys were listed instead of OpenPGP keys.
Bug Fix: Fixed memory issue experienced when adding more than 25 domains.

Release 4.1
Jul. 21, 2008

Enhancement: Updated behavior of ManagerSubsystem.addAccount to throw an exception if the account already exists and added ManagerSubsystem.setAccount method for use in overwriting an existing account.
Enhancement: Updated PGP Encrypt File and PGP Decrypt File actions to allow specifying a destination directory or file.
Enhancement: Added Name property to all Directory Monitor File related events to contain filename.
Enhancement: Added ability to automatically redirect all HTTP requests to HTTPS.
Enhancement: Added default log and datastore directories when creating a domain.
Enhancement: Added js-deldomain command line utility.
Enhancement: Changed default SSH version banner displayed to SFTP clients.
Bug Fix: Fixed issue with automatic startup process on Mac OS X platforms.
Bug Fix: Fixed issue with saving users with all password compliance options enabled.
Bug Fix: Fixed behavior of "Block IP after" option found in Connections node of JSCAPE MFT Server Manager. Change has been made so that client connection is closed before blocking client IP address.
Bug Fix: Fixed issue with directory listings returned when hosting server on Mac OS X platform.
Bug Fix: Fixed virtual folder permissions issue experienced when multiple virtual folders are assigned to a single user and virtual folders share a common path.
Bug Fix: Fixed issue with clients that request key re-exchange for long SFTP file transfers.
Bug Fix: Fixed issue with being unable to add users or reset passwords when password policies are enabled.

Release 4.0
Jun. 18, 2008

Enhancement: Added ability for users to reset lost password via web interface.
Enhancement: Improved GUI implementation for managing PGP keys.
Enhancement: Added web based account management features allowing user to change their own contact information.

Enhancement: Added ability to assign users limited domain administration capabilities via web interface.
Enhancement: Added support for Linux Z/OS platform.
Enhancement: Added ability to create user templates.
Enhancement: Updated Add Group and Edit Group dialogs to allow for selection of a Reverse Proxy.
Enhancement: Added js-adddomain command line utility to add a domain.
Enhancement: Added js-addserviceftp command line utility to add FTP service.
Enhancement: Added js-addservicesftp command line utility to add SFTP service.
Enhancement: Added js-addservicehttp command line utility to add HTTP and HTTPS services.
Enhancement: Added js-addservicewebdav command line utility to add WebDAV service.
Enhancement: Added js-importusers command line utility to perform bulk import of users from CSV file.
Enhancement: Added js-enablehttp command line utility to enable HTTP service.
Enhancement: Added js-enablehttps command line utility to enable HTTPS service.
Enhancement: Added js-startdomain command line utility to start domain.
Enhancement: Added js-stopdomain command line utility to stop domain.
Change: Renamed Resources node in JSCAPE MFT Server Manager to Reverse Proxies.
Bug Fix: Fixed issue with password compliance settings being applied globally instead of at domain level.
Bug Fix: Fixed issue with not being able to accept HTTP/S connections when running server on Windows Vista platform.
Bug Fix: Fixed issue with not being able to view reports when running server on Windows Vista platform.
Bug Fix: Fixed issue with SFTP service being unable to accept connections from older SFTP clients that use 1.99 as the software version in SSH client banner.
Bug Fix: Fixed issue with SFTP service being unable to accept uploads for non-existent files using some older SFTP clients.

Release 3.8
Feb. 12, 2008

Enhancement: Added support for IBM JVM 1.4.2 and above.
Enhancement: Added support for AIX 5.x and 6.1 platforms.
Enhancement: Improved auto-start documentation and example SMF script for Solaris platforms.
Enhancement: Added support for ZLIB compression in SFTP protocol.
Enhancement: Added ability to specify send and receive buffer sizes for FTP/S and SFTP protocols.
Enhancement: Added ability to define password policies.
Enhancement: Added several command line utilities for managing users.
Enhancement: Added ability to perform on-demand synchronization of server configuration and account data.
Enhancement: Added atomic file writing support when updating server configuration and account data.
Enhancement: Added support for multiple management connections.
Enhancement: Added ability to limit connections to administrative service based on client IP address.
Bug Fix: Fixed drive sorting bug found in Java applet interface.

Release 3.7
Dec. 28, 2007

Enhancement: Added ability define transfer quotas at the user level.
Enhancement: Added `LocalDir` event properties to any server events which have `LocalPath` event property.
Enhancement: Added `User Password Changed` event to detect when user changes their password.
Enhancement: Added ability to retrieve additional information from database query for use in setting up user in Database Query Authentication module.
Enhancement: Added support for WebDAV resources.
Enhancement: Added ability to run reports using a username filter.
Enhancement: Added ability to define enabled SSL ciphers for FTPS, HTTPS and secure WebDAV

services.
Bug Fix: Fixed issue with FTP/S service returning 0 bytes in response to SIZE filename command if file did not exist.
Bug Fix: Changed response code from 151 to 150 for passive data transfers in response to LIST command which caused a problem with some FTP/S clients.
Bug Fix: Fixed issue experienced when uploading large ASCII files.
Bug Fix: Fixed issue with saving settings for LDAP Query Authentication module.
Bug Fix: Fixed memory leak experienced in WebDAV service.
Bug Fix: Fixed SQL and LDAP injection vulnerability found when using Database Query Authentication or LDAP Query Authentication modules.
Bug Fix: Fixed issue with establishing a data connection to client using different source IP other than that of control channel.
Bug Fix: Fixed issue with encryption keys used in client PGP 6.5.8.
Bug Fix: Fixed issue when uploading large recursive directories using Java applet.
Bug Fix: Fixed table sorting issue in JSCAPE MFT Server Manager.
Bug Fix: Fixed XSS vulnerability.
Bug Fix: Fixed issue with ad-hoc email downloads that only allows downloads that were part of a pre-authenticated session.
Bug Fix: Fixed error in Top Hosts reporting metric.

Release 3.6
Nov. 7, 2007

Enhancement: Added ability to create directory on server if it does not exist when creating a virtual path.
Enhancement: Added email address property to user account. This value will be used as the default From address value when using ad-hoc email file transfers.
Enhancement: Moved various properties from WebDAV service to `File > Settings > WebDAV` in JSCAPE MFT Server Manager.
Enhancement: Moved various properties from HTTP service to `File > Settings > HTTP` in JSCAPE MFT Server Manager.
Enhancement: Added protocol level debugging support to Resources.
Enhancement: Moved virtual paths for user accounts to it's own tab named `Paths` in `Edit user account` dialog.
Enhancement: Added time elapsed, time remaining and transfer speed information to progress bar in HTML user interface.
Enhancement: Added wildcard support to LIST, MLST and MLSD command in FTP/S protocols.
Enhancement: Added support for MFMT and MFCT commands in FTP/S protocols.
Enhancement: Various enhancements made to WebDAV Java applet.
Enhancement: Added ability to copy an existing trigger.
Enhancement: Added ability to resume an interrupted transfer in WebDAV Java applet.
Enhancement: Added sorting capabilities to Directory Monitors, Reports, Groups and Resources sections of JSCAPE MFT Server Manager.
Enhancement: Added ability to disable ASCII/Binary option in HTML user interface.
Bug Fix: Fixed hanging progress bar experienced in HTML based user interface if user loses Internet connectivity during file upload. User now receives an error message indicating that the connection was lost.
Bug Fix: Fixed data timeout channel issue experienced during large file transfer when using FTP/S protocols and non-passive connection.

Release 3.5
Oct. 22, 2007

Enhancement: Added ability to define a secondary JSCAPE MFT Server failover server to which all primary

server configuration details are synchronized. Failover servers may be chained together to form a cluster.
Enhancement: Added ability to specify directory quotas when using a Directory Monitor.
Enhancement: Added asynchronous logging support to file and database logs.
Enhancement: Added Log Action option to all events that determine whether action success or failure will be logged.
Enhancement: Added optional automatic logout capabilities to HTML user interface which detects long periods of inactivity.
Enhancement: Added ability to disable showing of hotkeys on buttons in HTML user interface.
Enhancement: Added support for importing chained certificates in Key Manager.
Enhancement: Added implicit SSL support to LDAP authentication modules.
Enhancement: Added Second and Millisecond properties to all events.
Enhancement: Added File Upload Started, File Download Started, File Upload Aborted and File Download Aborted events.
Enhancement: Added list of server network interfaces to Help > About screen.
Enhancement: Added System Configuration Backup action that may be used in a trigger to backup server configuration files.
Bug Fix: Fixed issue with Services node in JSCAPE MFT Server Manager which displayed multiple instances of the same service.
Bug Fix: Fixed issue with displaying JavaHelp contents in environments running Java 1.6.
Bug Fix: Fixed issue with some browsers experienced when using ftp:// style URL to access FTP services.

Release 3.4
Sep. 12, 2007

Enhancement: Added ad-hoc email file transfer support to web interface allowing users to send emails to an email address along with web based links to selected files.
Enhancement: Added ability to specify text resources and logos independently for each domain.
Enhancement: Added domain level file transfer quotas for a user defined period of time.
Enhancement: Added MODE Z support to FTP/S protocols allowing for ZIP compressed file transfers and directory listings.
Enhancement: Added ability for users to change their account password via the web interface.
Enhancement: Added Trigger Error event that may be used for detecting and responding to failure in a trigger action.
Enhancement: Added "Prompt for password on connect" option to File > Settings > Connection panel which requires that user provide administrative password when launching JSCAPE MFT Server Manager client or when connecting using API.
Bug Fix: Fixed issue in Send Email action where From and To fields were swapped when sending an email.
Bug Fix: Fixed issue with PGP encryption keys where files encrypted using public keys imported from 3rd party PGP clients could not always be decrypted by those PGP clients.
Bug Fix: Fixed issue in 3.3 release where IE displayed error when trying to download files via HTTPS.
Bug Fix: Fixed issue in HTTP and WebDAV services where domain was reported as stopped even though it was running.
Bug Fix: Fixed issue experienced when generating certificate signing requests in Key Manager.

Release 3.3
Jul. 27, 2007

Enhancement: Added ability to generate certificate signing request (CSR) using Key Manager.
Enhancement: Added password hashing support to Database Query Authentication and LDAP Query Authentication services.
Enhancement: Added ability to forcefully disconnect and optionally disable an active user session/account using Kick User button in Users node.
Enhancement: Added ability for users to change their password using FTP or FTPS protocols.
Enhancement: Added ability to authenticate users using Custom User Authentication API.

Enhancement: Added ability to sort users by name, login or connection status.
Enhancement: Added support for PGP keys in Key Manager.
Enhancement: Added ability to specify SFTP/SSH version information in Services > SFTP panel.
Enhancement: Updated PGP related actions to use keys found in Key Manager.
Enhancement: Removed Send PGP Email action and incorporated PGP email operations into existing Send Email action.
Enhancement: Removed PGP Sign File action and incorporated file signing into PGP Encrypt File action.
Enhancement: Removed PGP Verify File action and incorporated signature verification into PGP Decrypt File action.
Enhancement: Added compression and PEM output support to PGP Encrypt File action.
Enhancement: Added requirement to bind public keys to users when using SFTP/SSH protocol combined with public-key authentication.
Bug Fix: Fixed issue in HTML user interface to prevent users from being able to view cached version of directory listing after clicking "Logout".
Bug Fix: Fixed issue experienced in IE7 HTML user interface when clicking on "Add" or "Remove" buttons.
Bug Fix: Fixed issue experienced with setting passive port range.

Release 3.2.5
Jun. 30, 2007

Enhancement: Updated jscape init.d script to support SUSE, Ubuntu and RedHat operating systems.
Bug Fix: Fixed issue experienced with WS_FTP client when using SFTP protocol.
Bug Fix: Fixed potential file corruption issue experienced when uploading file using SFTP protocol.
Bug Fix: Improved FTP/S protocols so that command channel timeout is not observed when client is performing a file transfer.

Release 3.2
Jun. 27, 2007

Enhancement: Added "Cancel" button to HTML file transfer user interface allowing users to cancel file uploads.
Enhancement: Updated Java Applet to include graphical buttons for performing basic actions such as Rename, Delete, Create Directory etc.
Enhancement: Updated HTML user interface to display file sizes in more user friendly format.
Enhancement: Added customizable "Add" and "Remove" text next to add and remove buttons in HTML user interface.
Enhancement: Added customizable "Logged in as" text to web user interface.
Bug Fix: Fixed issue with renaming files in HTML user interface when using IE.
Bug Fix: Fixed issue with multiple domains using database resources.
Bug Fix: Fixed issue where editing an action in a trigger could cause improper re-ordering of actions.

Release 3.1
May 27, 2007

Enhancement: Added support for WebDAV service.
Enhancement: Added Java applet client to web interface.
Enhancement: Updated look and feel of HTML based user interface.
Enhancement: Added Directory Monitors feature to monitor one or more local directories for changes.
Enhancement: Updated authentication panels in JSCAPE MFT Server Manager to give user more flexibility in specifying default login directory.
Enhancement: Added support for AES and other ciphers to SFTP protocol.
Enhancement: Added ability to specify Logout URL for HTTP services at domain level.
Enhancement: Added several new trigger event variables for capturing date/time and domain name.
Enhancement: Added a new Run Process action that can be used in a trigger to execute local processes.
Enhancement: Updated Delete Directory action, adding ability to specify that only files older than a certain

age be deleted.
Enhancement: Improved performance for file uploads.
Enhancement: Added source-code API examples to the api-examples directory of JSCAPE MFT Server installation directory.
Enhancement: Added more text properties to File > Settings > Web > Resource panel.
Change: Changed license key format.
Bug Fix: Fixed issue with SFTP clients connecting using unsupported protocol version.
Bug Fix: Fixed issue with importing SSH keys generated using ssh-keygen command.
Bug Fix: Fixed issue with virtual directories containing invalid characters such as * and ?.

Release 3.0
April 9, 2007

Enhancement: Added support for SFTP (FTP over SSH) service.
Enhancement: Added support for client SSL certificates for use in FTPS (FTP over SSL) services.
Enhancement: Added DMZ support using Resources.
Enhancement: Added Directory Download Synchronization action. This action allows users to synchronize local directories with remote FTP/FTPS/SFTP resources.
Enhancement: Added Directory Upload Synchronization action. This action allows users to synchronize remote FTP/FTPS/SFTP resources with a local directory.
Enhancement: Added Ftp Delete Directory and Ftp Delete File actions for deleting directories and files on remote FTP servers.
Enhancement: Added Ftps Delete Directory and Ftps Delete File actions for deleting directories and files on remote FTP servers using FTPS (FTP over SSL).
Enhancement: Added Sftp Delete Directory and Sftp Delete File actions for deleting directories and files on remote SSH servers using SFTP (FTP over SSH).
Enhancement: Added Ftp Regex File Upload and Ftp Regex File Download actions for transferring files to/from FTP server using a regular expression.
Enhancement: Added Ftps Regex File Upload and Ftps Regex File Download actions for transferring files to/from FTP server using a regular expression and FTPS (FTP over SSL).
Enhancement: Added Sftp Regex File Upload and Sftp Regex File Download actions for transferring files to/from SSH server using a regular expression and SFTP (FTP over SSH).
Enhancement: Added Send PGP Email action for sending OpenPGP encrypted email messages.
Enhancement: Added Zip Directory action for compressing the contents of a directory into a zip archive.
Enhancement: Added Run Report action for re-running an existing report.
Enhancement: Modified Check Email action to automatically verify/decrypt OpenPGP encrypted email messages.
Enhancement: Updated Copy Directory action allowing users to specify the level of copy performed.
Enhancement: Updated Delete Directory action allowing users to specify the level of delete performed.
Enhancement: Updated Send Email action allowing for sending of email using secure SSL encrypted connection.
Enhancement: Updated Send Email action to include optional receipt notification upon recipient opening email message.
Enhancement: Changed Add Domain process so that services are automatically started after adding a domain.
Enhancement: Changed File > Settings > Connection panel so connection is automatically established upon changing connection parameters.
Enhancement: Improved database reports allowing users to specify a Start Date and End Date range.
Enhancement: Added variable support to Authentication panel where appropriate.
Enhancement: Improved date validation components in manager GUI.
Enhancement: Added External File Upload and External File Download event types to monitor outbound and inbound file transfers made using triggers/actions.
Enhancement: Added events to capture administrative actions including Group Deleted, Group Updated, IP Access Rules Updated, Resource Deleted, Resource Updated, User Deleted, User Updated.
Enhancement: Improved formatting in reports.

Enhancement: Added additional metrics to reports including Top External Uploads, Top External Downloads, Top Email Attachments Sent and Top Email Attachments Received.
Enhancement: Changed command channel timeout for FTP services to automatically detect activity on data channel.
Enhancement: Added verbose logging support for all services.
Enhancement: Added automatic login support to Web services using URL parameters.
Enhancement: Added support for optionally redirecting user to a different URL in Web service when clicking Logout button.
Enhancement: Added true regular expression support to File Transfer Script action.
Bug Fix: Fixed issue in Convert File action.
Bug Fix: Fixed timestamp issue encountered when using database logging.
Bug Fix: Fixed memory issue experienced when trying to view large log record sets stored in relational database.
Bug Fix: Fixed issue experience when using multiple JDBC drivers simultaneously.

Release 2.1
December 13, 2006

Enhancement: Added authentication module for authenticating users against relational databases, LDAP or Active Directory services.
Enhancement: Added ability to schedule one-time-only or recurring actions using Current Time event and triggers.
Enhancement: Added ability to store activity logs in a relational database.
Enhancement: Added checkpoint restart and checksum verification to file transfer actions.
Enhancement: Added ability to specify up to three attachments in Send Email action.
Enhancement: Improved GUI screens in triggers section used in obtaining action variables.
Enhancement: Improved API for defining custom actions allowing you to specify the type of GUI components used when accepting input.
Enhancement: Added File Transfer Script action which consists of an easy-to-use file transfer scripting language that may be used in triggers.
Enhancement: Added Check Email action which checks for email against a POP or IMAP account, stores original message to a directory and extracts any attachments from message and stores these to a separate directory.
Enhancement: No longer necessary to specify driver class for JDBC database drivers.
Enhancement: Added debug logging support to network related actions such as Send Email, Ftp File Upload, Sftp File Upload etc.
Bug Fix: Fixed JSCAPE MFT Server Web Client compatibility issues with IE 5.2 and Safari browsers in Mac OS X.

Release 2.0
November 2, 2006

Enhancement: Added support for triggers and over 30 different actions.
Enhancement: Added reporting module to report on log data.
Enhancement: Added ability to add remote FTP resources and map those resources to virtual paths.
Enhancement: Added ability to import existing keys stored in PKCS#12 files.

Release 1.2
August 16, 2006

Enhancement: Added JSCAPE MFT Server Web Client component to accept web based FTP connections.
Enhancement: Added JavaHelp to JSCAPE MFT Server Manager.
Enhancement: Added service configuration script to be placed in /etc/init.d directory of UNIX environments to assist in auto-starting.

Enhancement: Changed logging format to use W3C for improved reporting capabilities.
Enhancement: Added ability to specify log rotation period.
Enhancement: Changed data serialization method used.
Enhancement: Added keyboard mnemonics to JSCAPE MFT Server Manager.
Enhancement: Updated JSCAPE MFT Server Manager so it is no longer necessary to manually stop server prior to applying changes.

Release 1.1
June 22, 2006

Minor bug fixes

Release 1.0
June 15, 2006

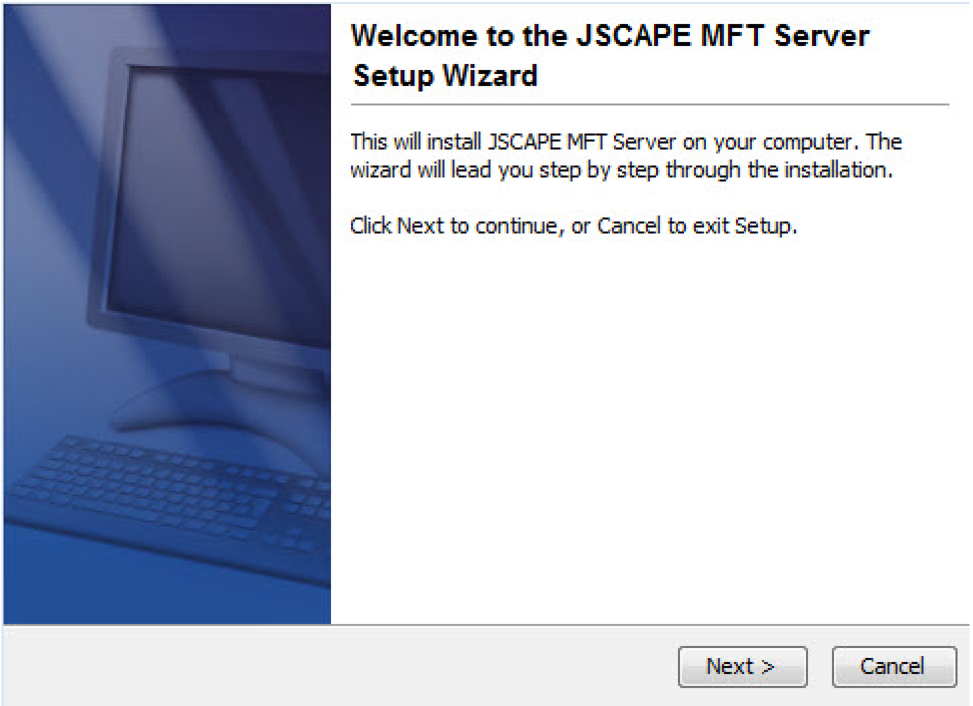
Initial production release.

Installing on Windows

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

1. Download and run the `install.exe` installation file for JSCAPE MFT Server. Click `Next` to continue.

Figure 173



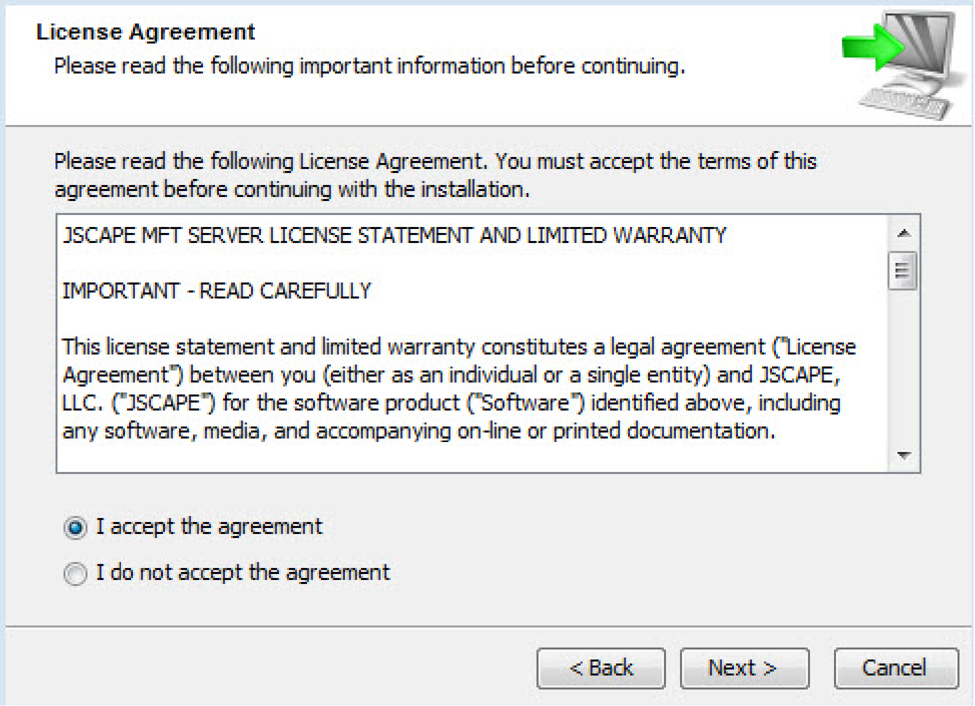
Welcome to the JSCAPE MFT Server Setup Wizard

This will install JSCAPE MFT Server on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

2. Read and accept license agreement. Click `Next` to continue.

Figure 174



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

JSCAPE MFT SERVER LICENSE STATEMENT AND LIMITED WARRANTY

IMPORTANT - READ CAREFULLY

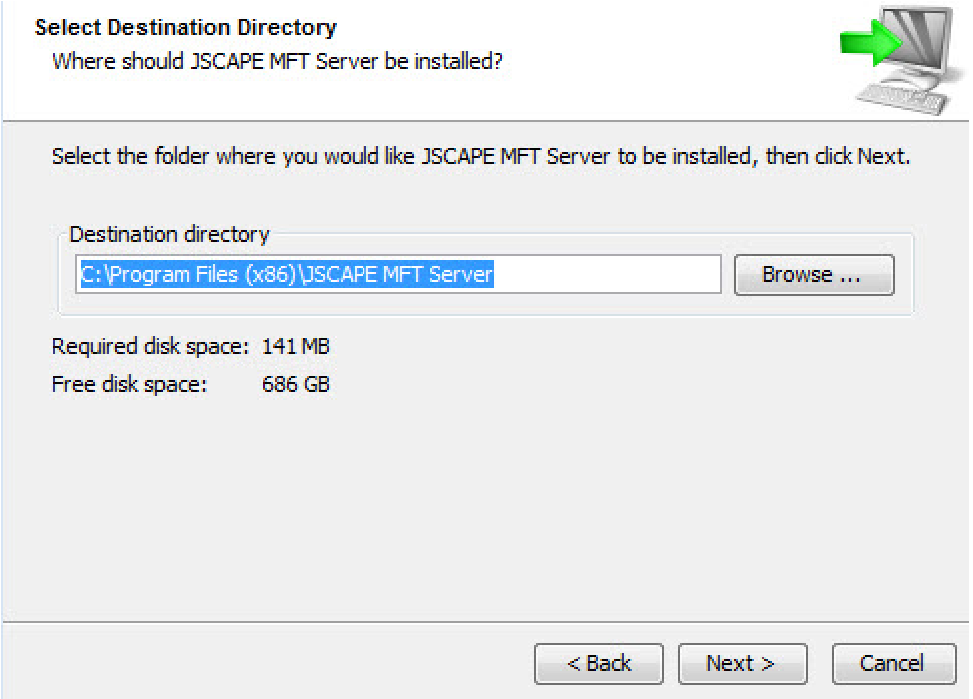
This license statement and limited warranty constitutes a legal agreement ("License Agreement") between you (either as an individual or a single entity) and JSCAPE, LLC. ("JSCAPE") for the software product ("Software") identified above, including any software, media, and accompanying on-line or printed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

● I accept the agreement

○ I do not accept the agreement

3. Select installation directory. Click `Next` to continue.

Figure 175



Select Destination Directory

Where should JSCAPE MFT Server be installed?

Select the folder where you would like JSCAPE MFT Server to be installed, then click Next.

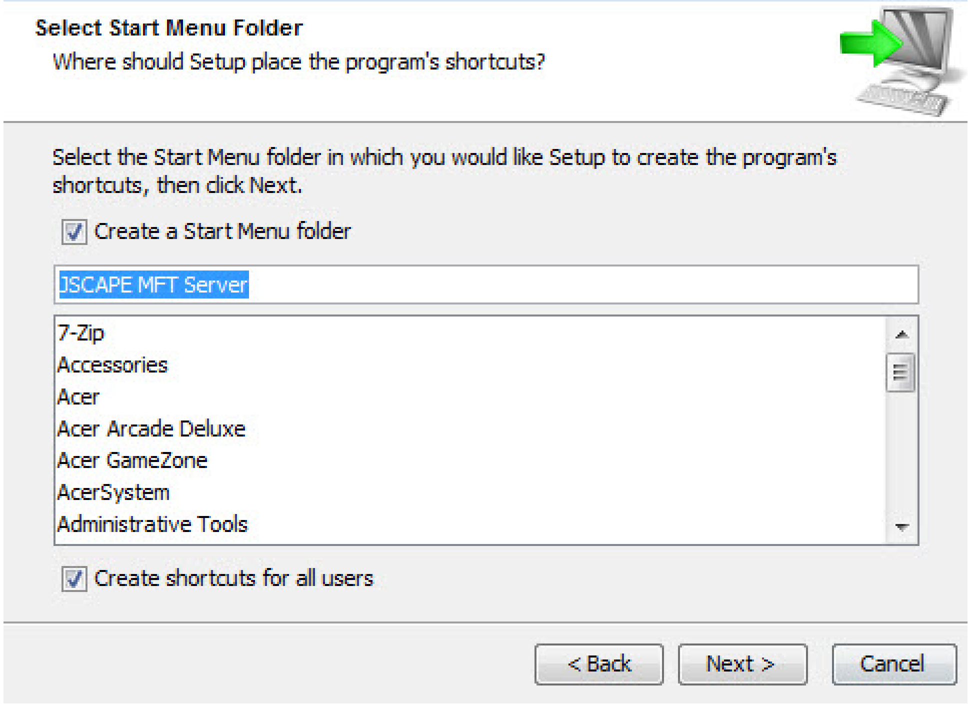
Destination directory: C:\Program Files (x86)\JSCAPE MFT Server

Required disk space: 141 MB

Free disk space: 686 GB

4. Enter name of Start Menu Folder. Click `Next` to continue.

Figure 177



Select Start Menu Folder

Where should Setup place the program's shortcuts?

Select the Start Menu folder in which you would like Setup to create the program's shortcuts, then click Next.

☑ Create a Start Menu folder

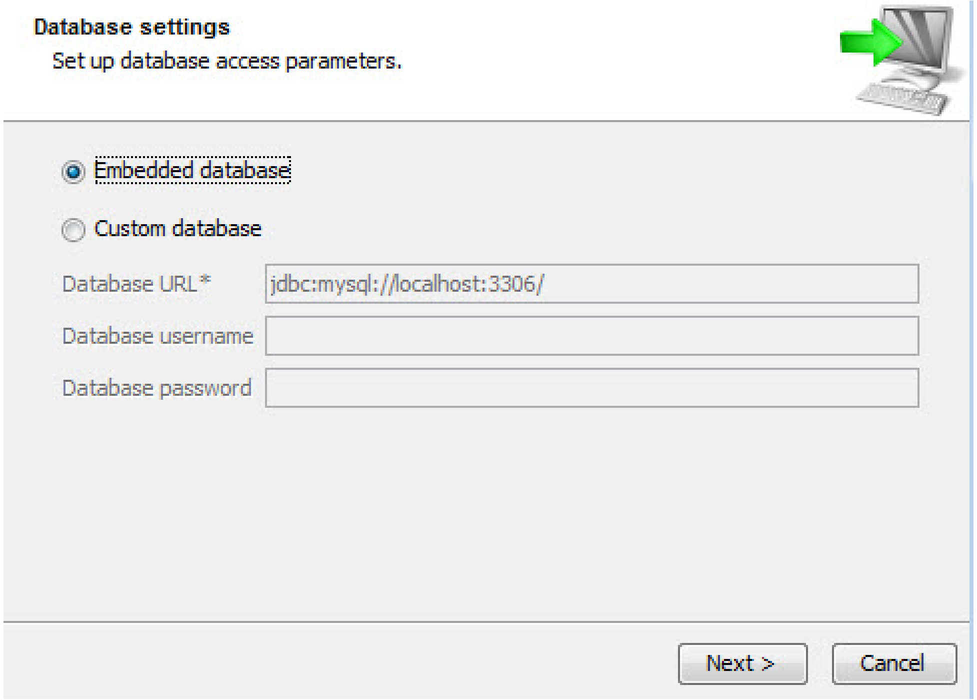
JSCAPE MFT Server

7-Zip
Accessories
Acer
Acer Arcade Deluxe
Acer GameZone
AcerSystem
Administrative Tools

☑ Create shortcuts for all users

5. Configure datastore where server configuration data will be located.

Figure 212



Database settings

Set up database access parameters.

● Embedded database

○ Custom database

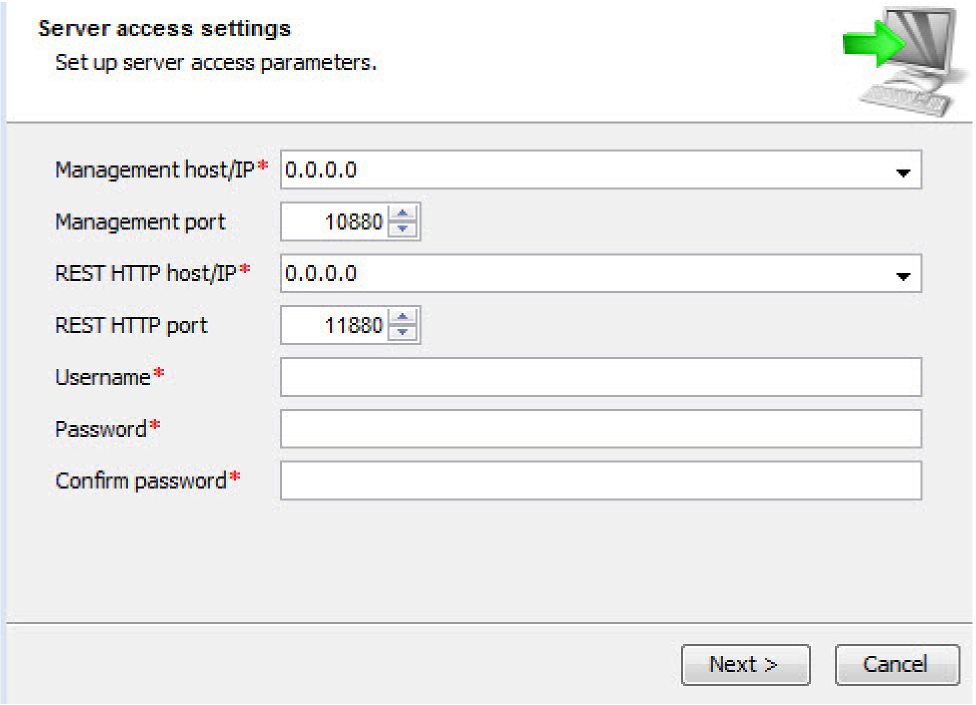
Database URL* jdbc:mysql://localhost:3306/

Database username

Database password

6. Configure management/REST services and administrative credentials.

Figure 178



Server access settings

Set up server access parameters.

Management host/IP* 0.0.0.0

Management port 10880

REST HTTP host/IP* 0.0.0.0

REST HTTP port 11880

Username*

Password*

Confirm password*

Management host/IP - The IP address that management service should listen on. The IP address `0.0.0.0` is a special address that instructs service to listen on all available network interfaces.

Management port - The port that management service should listen on. Default port is `10880`.

REST HTTP host/IP - The IP address that REST web service should listen on. The IP address `0.0.0.0` is a special address that instructs service to listen on all available network interfaces.

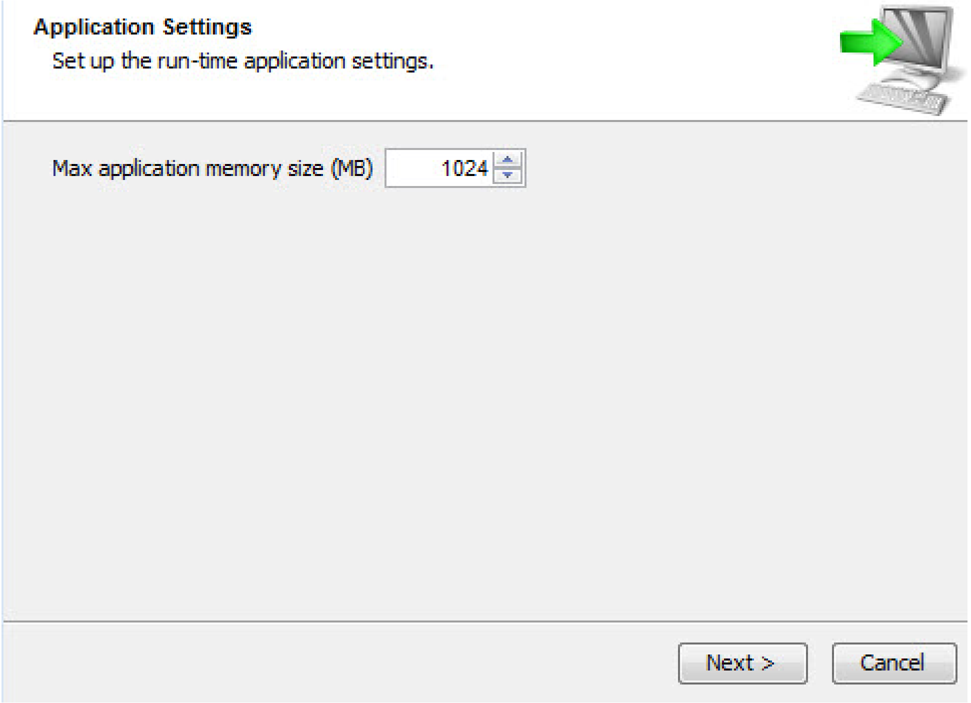
REST HTTP port - The port that REST web service should listen on. Default port is `11880`.

Username - Administrative username for managing services.

Password - Administrative password for managing services.

7. Set allocated application memory. Minimum allocated memory is 512MB with recommended value of 1024MB or more.

Figure 179



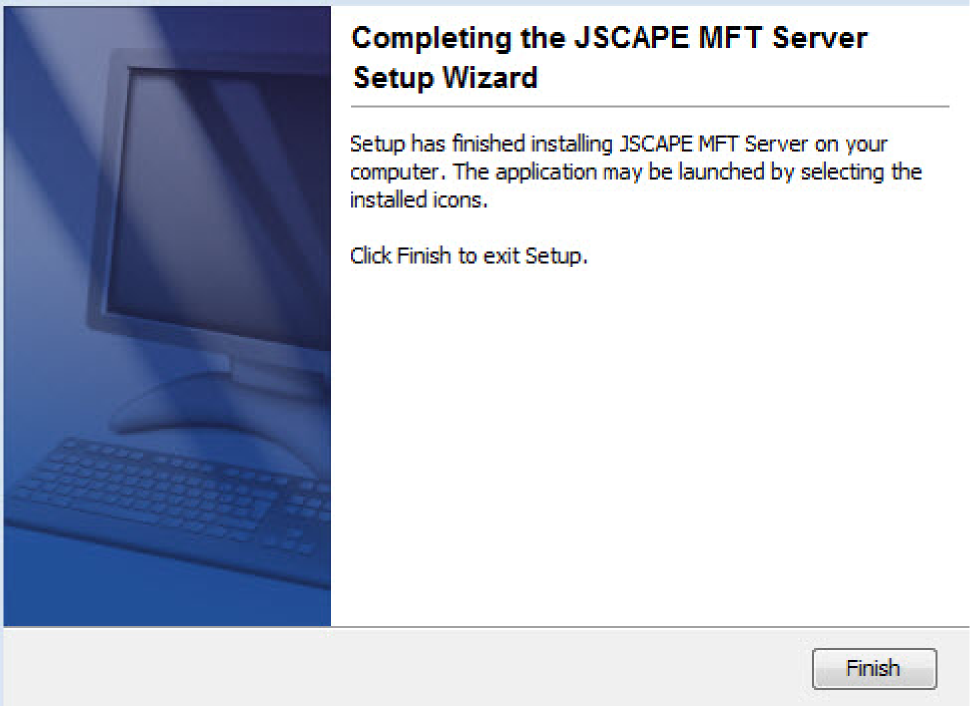
Application Settings

Set up the run-time application settings.

Max application memory size (MB) 1024

7. Launch JSCAPE MFT Server Manager to configure your server.

Figure 180



Completing the JSCAPE MFT Server Setup Wizard

Setup has finished installing JSCAPE MFT Server on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

8. If you are running any firewall software make sure that it is setup to allow JSCAPE MFT Server to run. For firewalls that use application whitelisting, add the application `server.exe` located in the JSCAPE MFT Server installation directory.

Installation

2

See also

Server configuration > Launching the administrative client

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 -iv install.rpm
```

3. Configure and initialize database. Go to the `/opt/JSCAPE_MFT_Server` directory and run the following commands.

```
./js-database-configuration -configure
```

```
./js-database-configuration -init
```

4. Add an administrative user. Go to the `/opt/JSCAPE_MFT_Server` directory and run the following command.

```
./js-addadmin -db -username [username] -password [password] -sa
```

For example

```
./js-addadmin -db -username admin -password secret -sa
```

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

```
./js-server-configuration -host [ip address] -port [port] -timeout [timeout
in seconds]
```

For example:

```
./js-server-configuration -host 0.0.0.0 -port 10880 -timeout 60
```

This will configure your JSCAPE MFT Server Service , where `[ip address]` and `[port]` are the IP/port that you want the JSCAPE MFT Server Service to listen on, and `[timeout in seconds]` is the timeout value for this service. The defaults port for JSCAPE MFT Server Service is `10880`.

Note, the IP address `0.0.0.0` is a special address that instructs the service to listen on all available network interfaces.

6. Configure the Web/REST settings. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following command:

```
./js-web-configuration -host [REST ip address] -port [REST port] -timeout
[timeout in minutes]
```

For example:

```
./js-web-configuration -host 0.0.0.0 -port 11880 -timeout 10
```

This service is what you will connect to using the JSCAPE MFT Server Manager to manage your server.

7. Configure the credentials used when invoking command line utilities. Go to the `/opt/JSCAPE_MFT_Server` directory and run the following command:

```
./js-client-configuration -host [host] -port [port] -timeout [timeout in
seconds] -user [username] -password [password]
```

For example:

```
./js-client-configuration -host 0.0.0.0 -port 10880 -timeout 60 -user admin -
password admin
```

8. Startup Administration Service. From the `/opt/JSCAPE_MFT_Server` directory run the following command:

```
./start_service.sh
```

The JSCAPE MFT Server Service should now be running. To connect to this service and manage your server see the following topics:

Server configuration > Launching the administrative client

Auto-starting in UNIX environments

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 and initialize database. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following commands:

```
./js-database-configuration -configure

./js-database-configuration -init
```

4. Add an administrative user. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following command:

```
./js-addadmin -db -username [username] -password [password] -sa
```

For example

```
./js-addadmin -db -username admin -password secret -sa
```

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

```
./js-server-configuration -host [ip address] -port [port] -timeout [timeout
in seconds]
```

For example:

```
./js-server-configuration -host 0.0.0.0 -port 10880 -timeout 60
```

This will configure your JSCAPE MFT Server Service , where `[ip address]` and `[port]` are the IP/port that you want the JSCAPE MFT Server Service to listen on, and `[timeout in seconds]` is the timeout value for this service. The defaults port for JSCAPE MFT Server Service is `10880`.

Note, the IP address `0.0.0.0` is a special address that instructs the service to listen on all available network interfaces.

6. Configure the Web/REST settings. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following command:

```
./js-web-configuration -host [REST ip address] -port [REST port] -timeout
[timeout in minutes]
```

For example:

```
./js-web-configuration -host 0.0.0.0 -port 11880 -timeout 10
```

This service is what you will connect to using the JSCAPE MFT Server Manager to manage your server.

7. Configure the credentials used when invoking command line utilities. Go to the `/opt/JSCAPE_MFT_Server` directory and run the following command:

```
./js-client-configuration -host [host] -port [port] -timeout [timeout in
seconds] -user [username] -password [password]
```

For example:

```
./js-client-configuration -host 0.0.0.0 -port 10880 -timeout 60 -user admin -
password admin
```

8. Startup Administration Service. From the `/opt/JSCAPE_MFT_Server` directory run the following command:

```
./start_service.sh
```

The JSCAPE MFT Server Service should now be running. To connect to this service and manage your server see the following topics:

Server configuration > Launching the administrative client

Auto-starting in UNIX environments

Installing on Linux Z/OS

See also

Running under IBM JVM
Installing on Linux

Installing on Solaris

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 Server as a non-root user under Solaris 10 or above, please consult the topic Auto-starting in Solaris 10 environments topic before continuing.

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 and initialize database. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following commands:

```
./js-database-configuration -configure
```

```
./js-database-configuration -init
```

4. Add an administrative user. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following command:

```
./js-addadmin -db -username [username] -password [password] -sa
```

For example

```
./js-addadmin -db -username admin -password secret -sa
```

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

```
./js-server-configuration -host [ip address] -port [port] -timeout [timeout
in seconds]
```

For example:

```
./js-server-configuration -host 0.0.0.0 -port 10880 -timeout 60
```

This will configure your JSCAPE MFT Server Service , where `[ip address]` and `[port]` are the IP/port that you want the JSCAPE MFT Server Service to listen on, and `[timeout in seconds]` is the timeout value for this service. The defaults port for JSCAPE MFT Server Service is `10880`.

Note, the IP address `0.0.0.0` is a special address that instructs the service to listen on all available network interfaces.

6. Configure the Web/REST settings. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following command:

```
./js-web-configuration -host [REST ip address] -port [REST port] -timeout
[timeout in minutes]
```

For example:

```
./js-web-configuration -host 0.0.0.0 -port 11880 -timeout 10
```

This service is what you will connect to using the JSCAPE MFT Server Manager to manage your server.

7. Configure the credentials used when invoking command line utilities. Go to the `/opt/JSCAPE_MFT_Server` directory and run the following command:

```
./js-client-configuration -host [host] -port [port] -timeout [timeout in
seconds] -user [username] -password [password]
```

For example:

```
./js-client-configuration -host 0.0.0.0 -port 10880 -timeout 60 -user admin -
password admin
```

7. Startup JSCAPE MFT Server Service. From the JSCAPE MFT Server installation directory run the following command:

```
./start_service.sh
```

Installation 2

The JSCAPE MFT Server Service should now be running. To connect to this service and manage your server see the following topics:

Server configuration > Launching the administrative client

Auto-starting in Solaris 10 environments

Auto-starting in UNIX environments

Installing on AIX

ZIP Console Installation

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 command from the directory containing the ZIP file you placed on your server:

```
unzip install.zip
```

3. Configure and initialize database. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following commands:

```
./js-database-configuration -configure
```

```
./js-database-configuration -init
```

4. Add an administrative user. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following command:

```
./js-addadmin -db -username [username] -password [password] -sa
```

For example

```
./js-addadmin -db -username admin -password secret -sa
```

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

```
./js-server-configuration -host [ip address] -port [port] -timeout [timeout
in seconds]
```

For example:

```
./js-server-configuration -host 0.0.0.0 -port 10880 -timeout 60
```

This will configure your JSCAPE MFT Server Service , where `[ip address]` and `[port]` are the IP/port that you want the JSCAPE MFT Server Service to listen on, and `[timeout in seconds]` is the timeout value for this service. The defaults port for JSCAPE MFT Server Service is `10880`.

Note, the IP address `0.0.0.0` is a special address that instructs the service to listen on all available network interfaces.

AIX systems are typically configured to run the IBM JVM, therefore it is necessary to make some changes to various configuration files in order to instruct the JVM on what security provider and encryption algorithm to use for starting up the JSCAPE MFT Server Service.

See Running under IBM JVM for complete details and instructions.

6. Configure the Web/REST settings. Go to the JSCAPE MFT Server installation directory, located in the `JSCAPE_MFT_Server` directory relative to where the unzip command was executed, and run the following command:

```
./js-web-configuration -host [REST ip address] -port [REST port] -timeout
[timeout in minutes]
```

For example:

```
./js-web-configuration -host 0.0.0.0 -port 11880 -timeout 10
```

This service is what you will connect to using the JSCAPE MFT Server Manager to manage your server.

7. Configure the credentials used when invoking command line utilities. Go to the `/opt/JSCAPE_MFT_Server` directory and run the following command:

```
./js-client-configuration -host [host] -port [port] -timeout [timeout in
seconds] -user [username] -password [password]
```

For example:

```
./js-client-configuration -host 0.0.0.0 -port 10880 -timeout 60 -user admin -
password admin
```

8. Startup JSCAPE MFT Server Service. From the JSCAPE MFT Server installation directory run the following command:

```
./start_service.sh
```

The JSCAPE MFT Server Service should now be running. To connect to this service and manage your server see the following topics:

Server configuration > Launching the administrative client

Auto-starting in UNIX environments

Installation

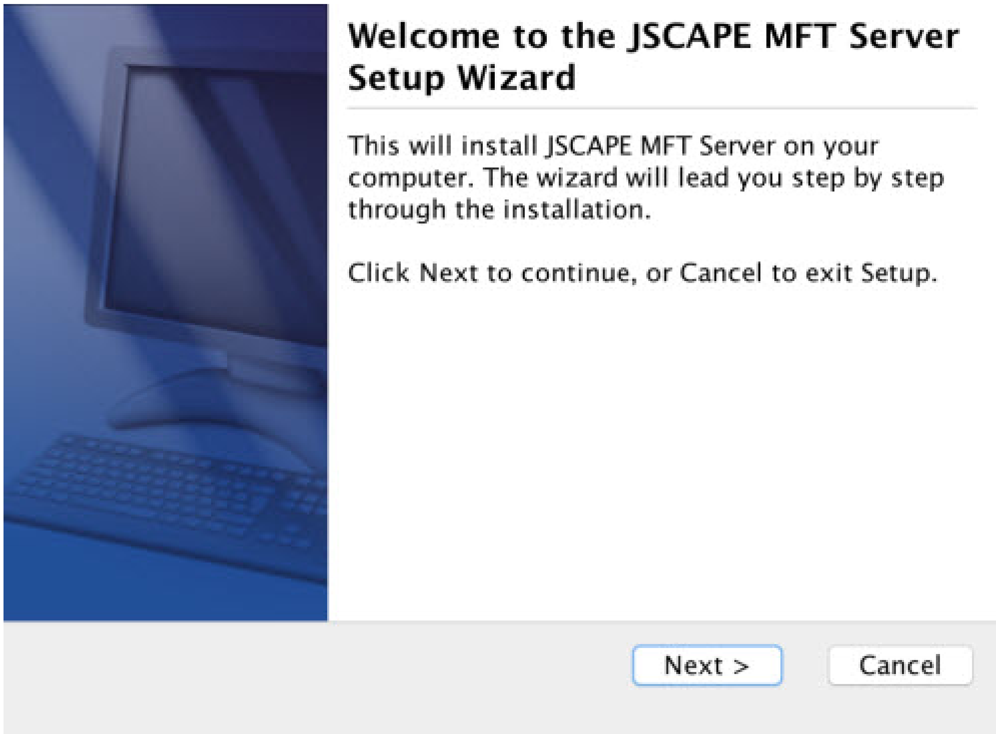
2

Installing on Mac OS X

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

1. Download and run the `install.dmg` installation file for JSCAPE MFT Server. Click `Next` to continue.

Figure 181



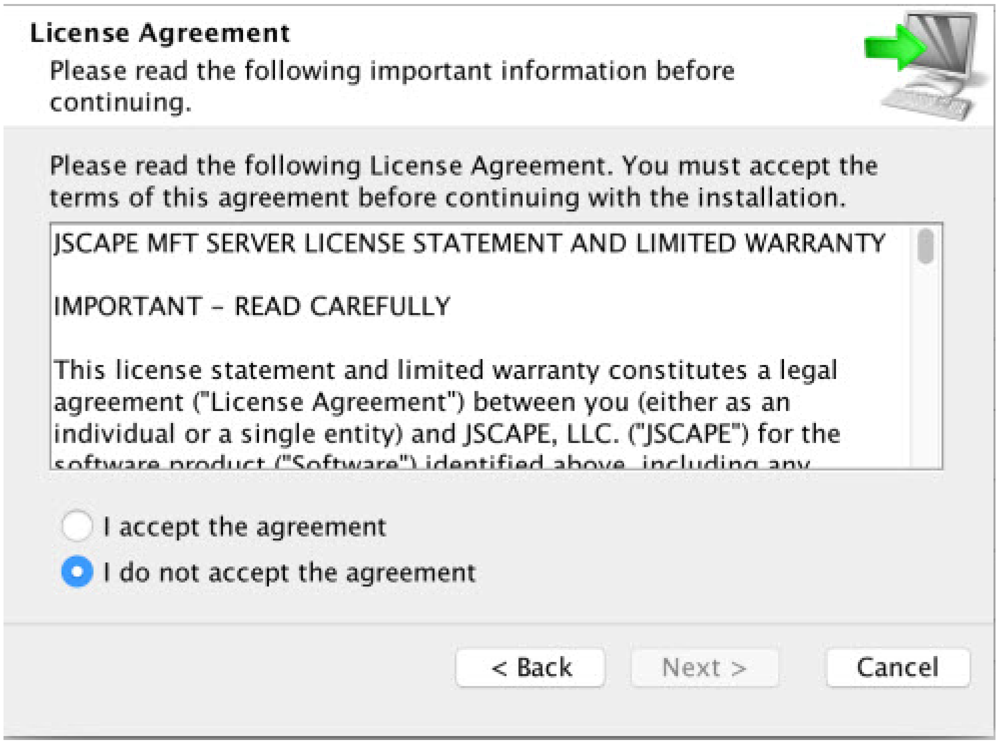
Welcome to the JSCAPE MFT Server Setup Wizard

This will install JSCAPE MFT Server on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

2. Read and accept license agreement. Click `Next` to continue.

Figure 182



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

JSCAPE MFT SERVER LICENSE STATEMENT AND LIMITED WARRANTY

IMPORTANT – READ CAREFULLY

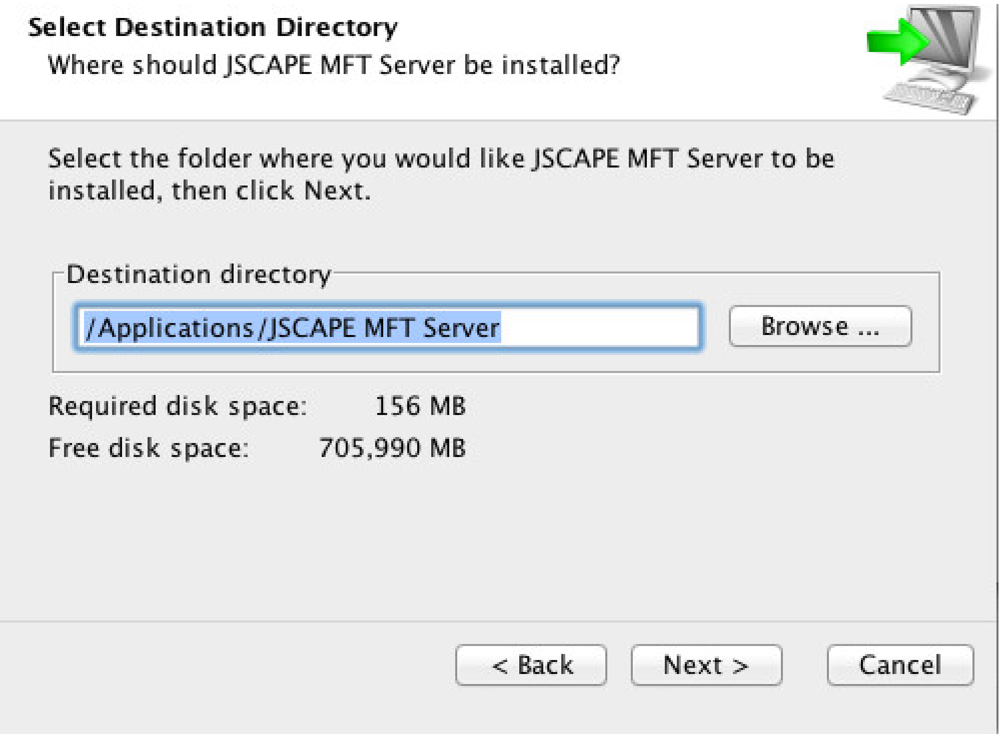
This license statement and limited warranty constitutes a legal agreement ("License Agreement") between you (either as an individual or a single entity) and JSCAPE, LLC. ("JSCAPE") for the software product ("Software") identified above, including any

○ I accept the agreement

● I do not accept the agreement

3. Select installation directory. Click `Next` to continue.

Figure 183



Select Destination Directory

Where should JSCAPE MFT Server be installed?

Select the folder where you would like JSCAPE MFT Server to be installed, then click Next.

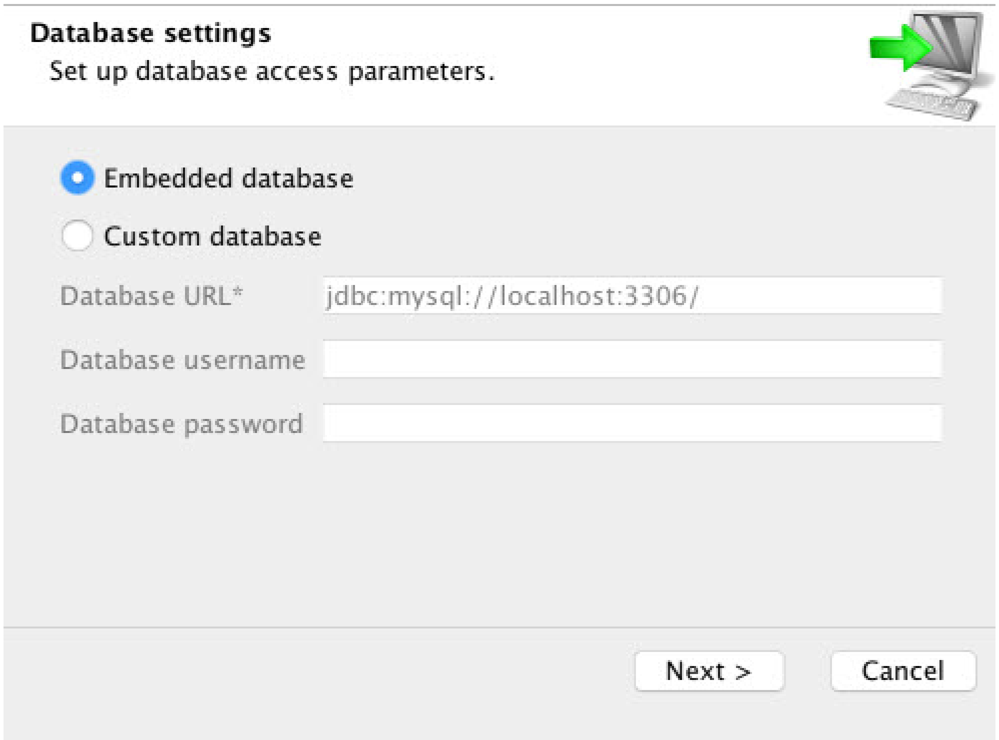
Destination directory: /Applications/JSCAPE MFT Server

Required disk space: 156 MB

Free disk space: 705,990 MB

4. Configure datastore where server configuration data will be located.

Figure 226



Database settings

Set up database access parameters.

● Embedded database

○ Custom database

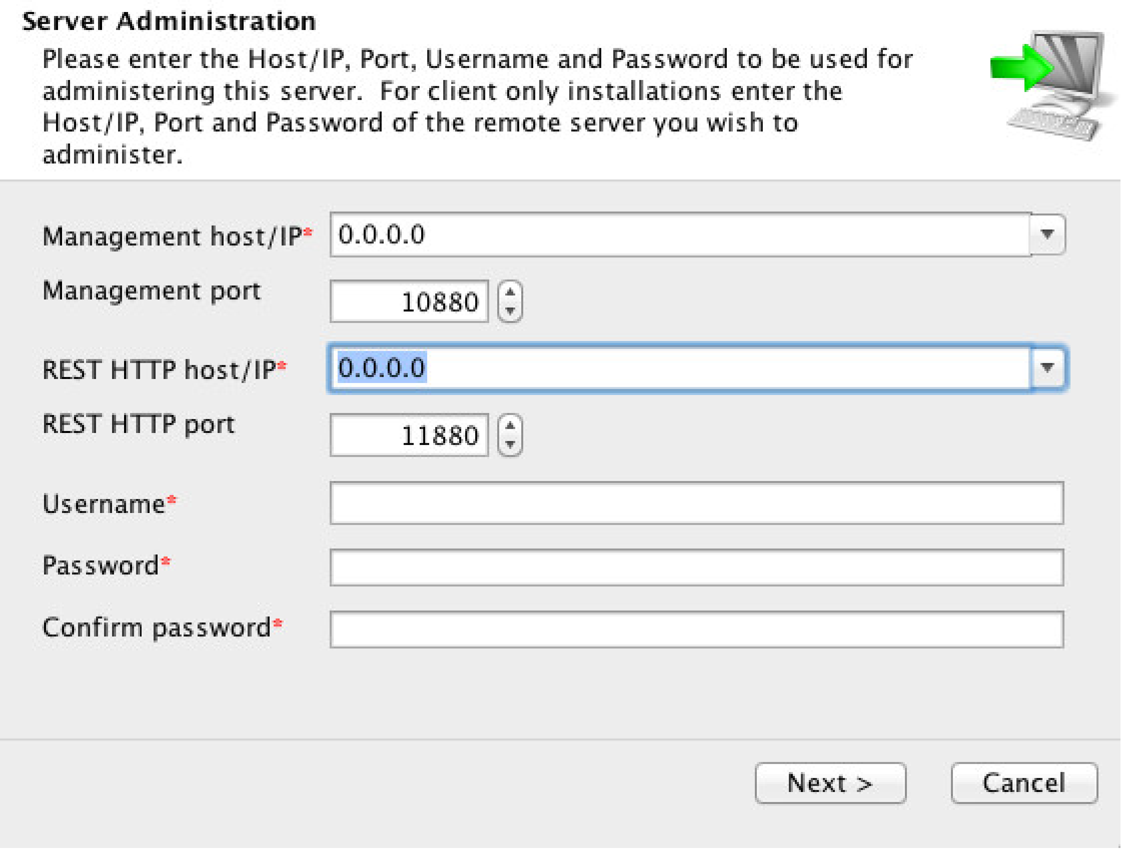
Database URL* jdbc:mysql://localhost:3306/

Database username

Database password

5. Configure management/REST services and administrative credentials.

Figure 185



Server Administration

Please enter the Host/IP, Port, Username and Password to be used for administering this server. For client only installations enter the Host/IP, Port and Password of the remote server you wish to administer.

Management host/IP* 0.0.0.0

Management port 10880

REST HTTP host/IP* 0.0.0.0

REST HTTP port 11880

Username*

Password*

Confirm password*

Management host/IP - The IP address that management service should listen on. The IP address `0.0.0.0` is a special address that instructs service to listen on all available network interfaces.

Management port - The port that management service should listen on. Default port is `10880`.

REST HTTP host/IP - The IP address that REST web service should listen on. The IP address `0.0.0.0` is a special address that instructs service to listen on all available network interfaces.

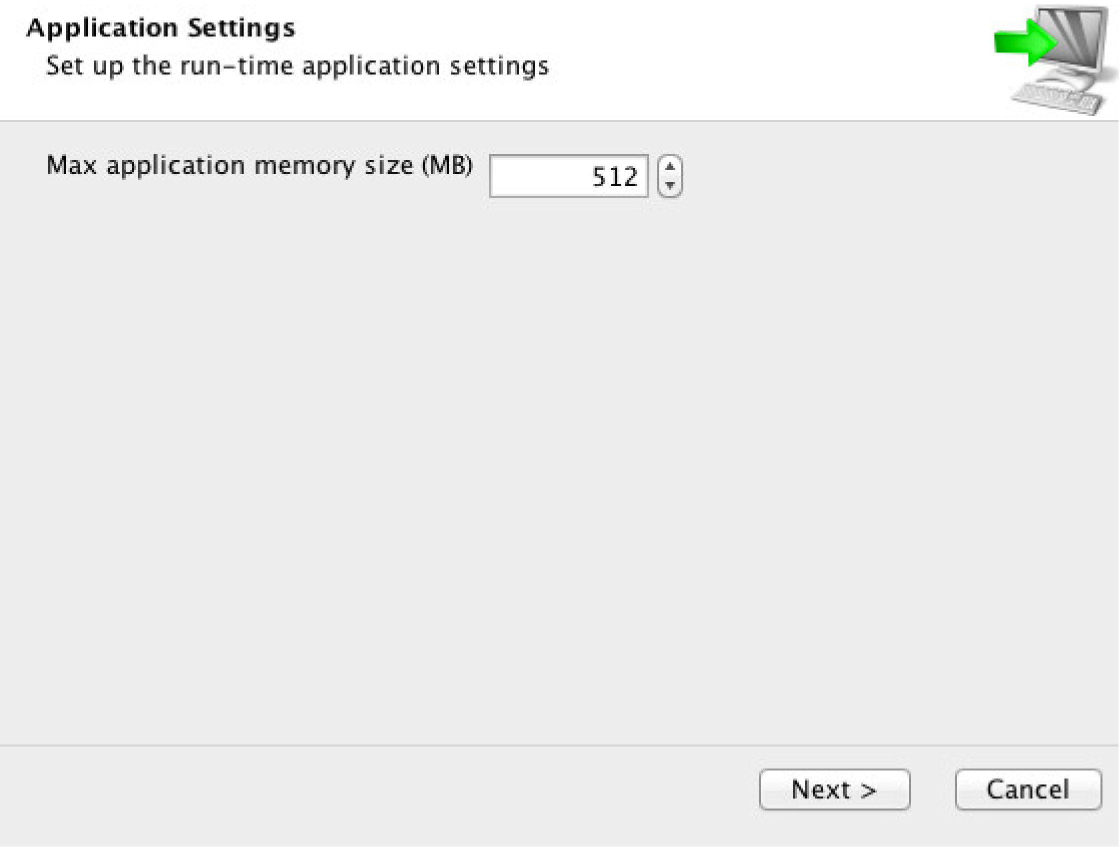
REST HTTP port - The port that REST web service should listen on. Default port is `11880`.

Username - Administrative username for managing services.

Password - Administrative password for managing services.

6. Set allocated application memory. Minimum allocated memory is 512MB with recommended value of 1024MB or more for servers under heavy load.

Figure 186



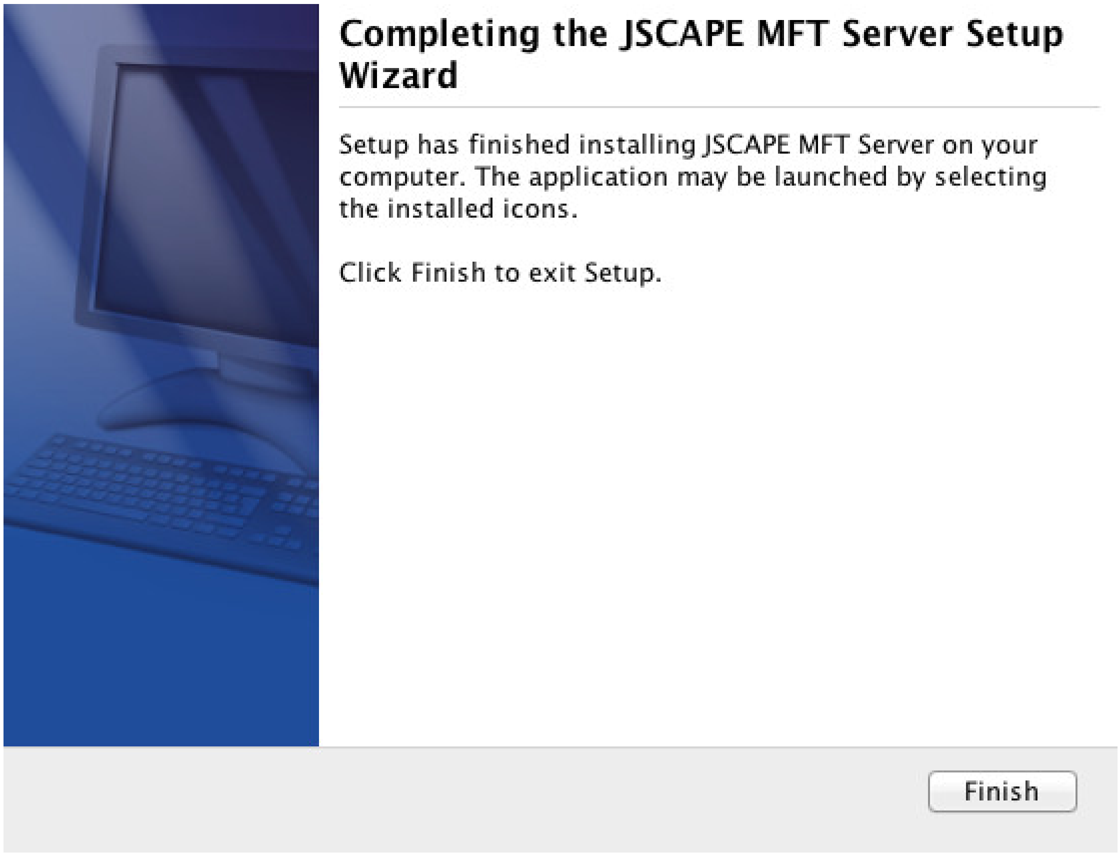
Application Settings

Set up the run-time application settings

Max application memory size (MB) 512

7. Launch JSCAPE MFT Server Manager to configure your server.

Figure 187



Completing the JSCAPE MFT Server Setup Wizard

Setup has finished installing JSCAPE MFT Server on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

8. Start the JSCAPE MFT Server 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.MFTServer.plist` file and set the value for the `OnDemand` parameter to `false`.

9. Verify that JSCAPE MFT Server Service is running using the following commands from your shell prompt:

```
netstat -a | grep 10880
netstat -a | grep 11880
```

where `10880` is the listing port for JSCAPE MFT Server Service, and `11880` is listening port for REST web service.

See also

Server configuration > Launching the administrative client

Installation 2

Auto-starting in Linux and Solaris 9 environments

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

Installing the service configuration file

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

2. Grant execute permissions to this file using the command `chmod 755 jscape`

3. Using a text editor, change the value of the `INSTALL_DIR` variable to the absolute path of your JSCAPE MFT Server installation directory. The default value for the `INSTALL_DIR` variable is `/opt/JSCAPE_MFT_Server` 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 jscape
```

Solaris 9

```
ln /etc/init.d/jcsape /etc/rc3.d/Sxxjscape
ln /etc/init.d/jcsape /etc/rc0.d/Kxxjscape
```

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 jscape defaults
```

Starting the service

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

Stopping the service

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

Restarting the service

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

See also

Running as non-root user in UNIX environments

Auto-starting in Solaris 10 environments

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

1. As `root` user, create a user and group named `jscape`.
2. As `root` user, run the command `usermod -K defaultpriv=basic,net_privaddr jscape` to grant `jscape` user permissions to run services on ports less than 1024.
3. As `jscape` user, run installer for Solaris as described in Installing on Solaris.
4. Open the sample SMF manifest file `jscape_smf.xml` found in the JSCAPE MFT Server installation directory using `vi` or other text editor.
5. Change references to `/opt/JSCAPE_MFT_Server` with the absolute path of JSCAPE MFT Server installation directory.
6. As `root` user, validate SMF manifest file using `svccfg validate jscape_smf.xml` command.
7. As `root` user, import SMF manifest file using `svccfg import jscape_smf.xml` command.
8. As `root` user, Check for default Solaris FTP service using command `netstat -na | grep 21` If you wish to disable this service you may do so using `svcadmin disable ftp:default` command.
9. As `root` user, enable service using `svcadm enable svc:/application/jscape:default` command.
10. Check that service was started successfully and not in maintenance using `svcs -x jscape: default` command.
11. Verify that JSCAPE MFT Server Service is running using `netstat -na | grep 10880` command.

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 Server is to do so as the `root` user. However in some UNIX based environments you may want or need to run JSCAPE MFT Server 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 Server.

Filesystem permissions

When running JSCAPE MFT Server as a non-root system user ensure that this user has user or group level permissions granting them full access to the virtual directories that you define for your JSCAPE MFT Server users. Additionally this user should be granted full access to the JSCAPE MFT Server installation directory, logging directory, user datastore directory and all supporting files within these 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 Server 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 ftp service to run on port 2121 instead of port 21 in order to be able to run JSCAPE MFT Server as a non-root user. There may however be a case where you want to be able to run JSCAPE MFT Server 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 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 `jscape` (as `root` user) the contents of which are displayed below.

```
# Redirects any requests on port 21
# to port 2121 (where JSCAPE MFT Server is listening)
service jscape
{
        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 `jscape` 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 UNIX environments

Running under IBM JVM

For systems configured to run using the IBM JVM it is necessary to make some changes to various configuration files in order to instruct the JVM on what security provider and encryption algorithm to use for starting up the JSCAPE MFT Server Service. Using a text editor, update the following files relative to the installation directory as follows.

ssl.cfg

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

webapp/filetransfer/META-INF/Owasp.CsrfGuard.properties

```
org.owasp.csrfguard.PRNG=IBMSecureRandom
org.owasp.csrfguard.PRNG.Provider=IBMJCE
```

webapp/management/META-INF/Owasp.CsrfGuard.properties

```
org.owasp.csrfguard.PRNG=IBMSecureRandom
org.owasp.csrfguard.PRNG.Provider=IBMJCE
```

Upon saving changes to these files restart the JSCAPE MFT Server Service so the changes may take effect.

Additional libraries needed for OpenPGP

If you are planning to use the OpenPGP features that are included as part of JSCAPE MFT Server, then you may need to install the JCE Unlimited Strength Jurisdiction Policy Files distributed by Oracle. OpenPGP features may work without this process, but only for PGP keys of limited strengths.

Due to export restriction the version of the policy files bundled by default with the JDK allow "strong" but limited cryptography to be used. The "unlimited strength" policy files contain no restrictions on the cryptographic strengths.

Download Unlimited Strength Jurisdiction Policy Files

http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html (JVM 1.6)

http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html (JVM 1.7)

http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html (JVM 1.8)

Installation

1. Determine the location of the JVM/JDK you are using by opening the `.install4j\inst_jre.cfg` file located in your JSCAPE MFT Server installation directory. This file will contain the path to the JRE used when running JSCAPE MFT Server.

Example

```
c:\program files\java\jre
```

2. Extract the contents of the Unlimited Strength Jurisdiction Policy Files to a temporary directory.

3. Copy the `local_policy.jar` and `US_export_policy.jar` files extracted in the previous step to the `lib\security` directory of your JRE making sure to backup previous versions of these jar files should you decide to revert back to the previous installation.

Example

```
c:\program files\java\jre\lib\security
```

4. Restart both the JSCAPE MFT Server Service and JSCAPE MFT Server Manager.

Additional libraries needed for SFTP ciphers

If you are planning to use the non-default ciphers that are included as part of JSCAPE MFT Server SFTP service, then you may need to install the JCE Unlimited Strength Jurisdiction Policy Files distributed by Oracle.

The default ciphers that are supported by the SFTP service include blowfish-cbc, 3des-cbc, none. If you are only using the default enabled ciphers then installing the Unlimited Strength Jurisdiction Policy Files is not necessary.

Examples of non-default ciphers that require installing the Unlimited Strength Jurisdiction Policy Files include but are not limited to aes, twofish, serpent, idea and cast.

Due to export restriction the version of the policy files bundled by default with the JDK allow "strong" but limited cryptography to be used. The "unlimited strength" policy files contain no restrictions on the cryptographic strengths.

Download Unlimited Strength Jurisdiction Policy Files

http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html (JVM 1.6)

http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html (JVM 1.7)

http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html (JVM 1.8)

Installation

1. Determine the location of the JVM/JDK you are using by opening the `.install4j\inst_jre.cfg` file located in your JSCAPE MFT Server installation directory. This file will contain the path to the JRE used when running JSCAPE MFT Server.

Example

```
c:\program files\java\jre
```

2. Extract the contents of the Unlimited Strength Jurisdiction Policy Files to a temporary directory.

3. Copy the `local_policy.jar` and `US_export_policy.jar` files extracted in the previous step to the `lib\security` directory of your JRE making sure to backup previous versions of these jar files should you decide to revert back to the previous installation.

Example

```
c:\program files\java\jre\lib\security
```

4. Restart both the JSCAPE MFT Server Service and JSCAPE MFT Server Manager.

Starting the JSCAPE MFT Server Service

In order to manage the JSCAPE MFT Server you must first start the JSCAPE MFT Server Service. This service allows you to manage the JSCAPE MFT Server using JSCAPE MFT Server Manager.

Windows

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

Linux / UNIX / Mac OS X

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

```
./start_service.sh
```

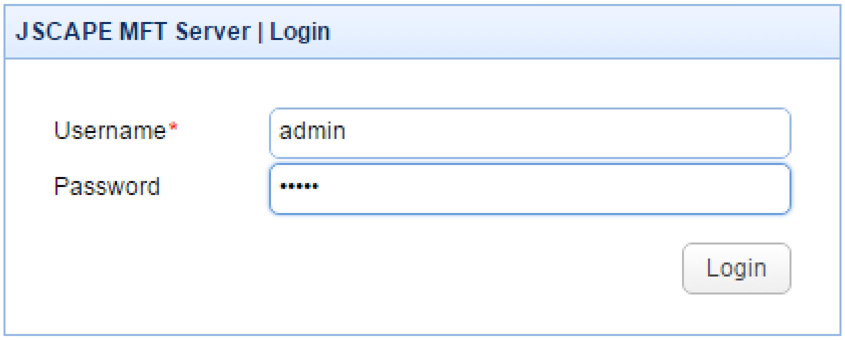
Launching the JSCAPE MFT Server Manager

The JSCAPE MFT Server Manager is a web based application which may be used to manage your instance of JSCAPE MFT Server. You may start JSCAPE MFT Server Manager by pointing your web browser to `http://[hostname]:[port]` where `[hostname]` is the IP address or hostname and `[port]` is the listening port of the REST management web service defined during the installation process. The default port is 11880.

e.g. `http://127.0.0.1:11880`

Upon successfully connecting to REST management service, you will be prompted for an administrative username and password to login. These credentials are those that you defined during the installation process.

Figure 172

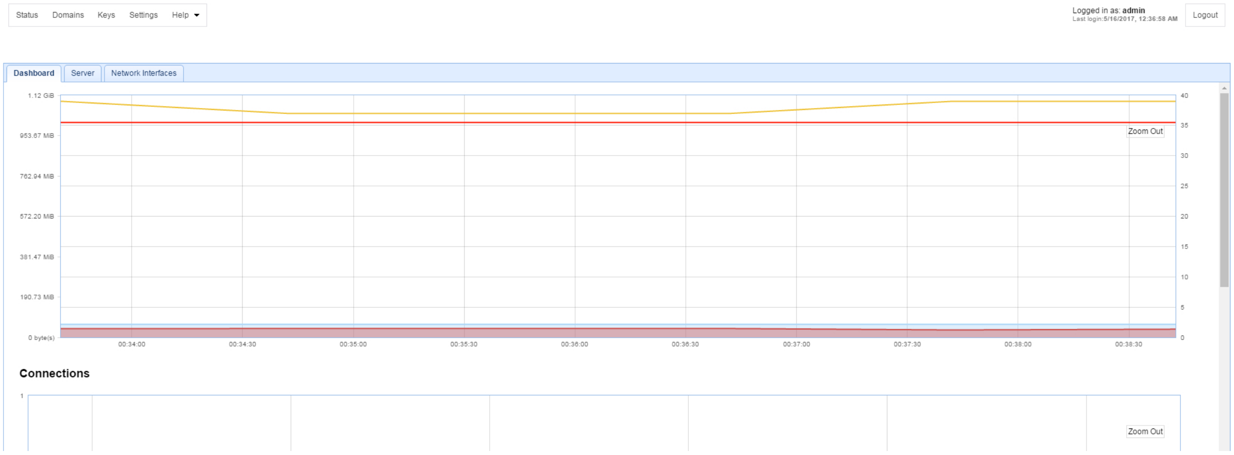


JSCAPE MFT Server | Login

Username* admin

Password •••••

Figure 1



Logged in as: **admin**
Last login:5/16/2017, 12:36:58 AM

See also

[Starting the service](#)

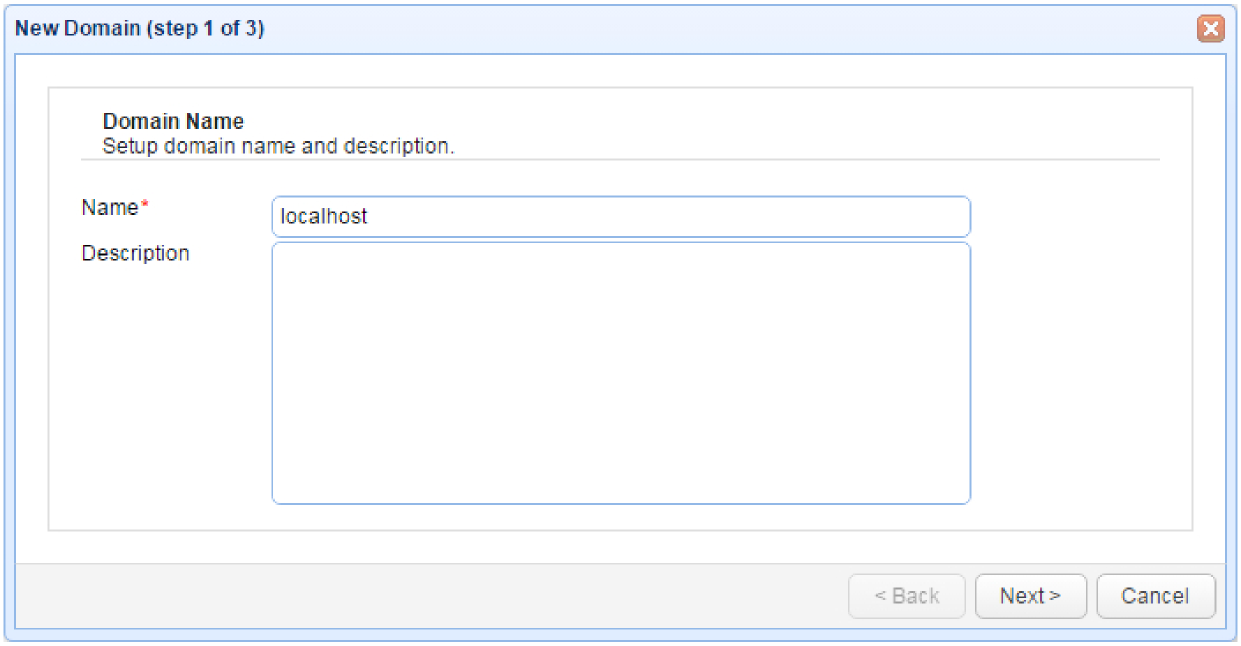
Creating a domain

You may create a domain using the JSCAPE MFT Server Manager.

Step 1

Using JSCAPE MFT Server Manager click `Domains` from the main menu and then click the `Add` button. The `New Domain` wizard is displayed. This wizard allows you to quickly create a new domain with one service and minimum settings. You may later customize the domain to meet your needs by selecting the domain from the `Domains` tab and clicking `Edit` button.

Figure 2



New Domain (step 1 of 3)

Domain Name
Setup domain name and description.

Name* localhost

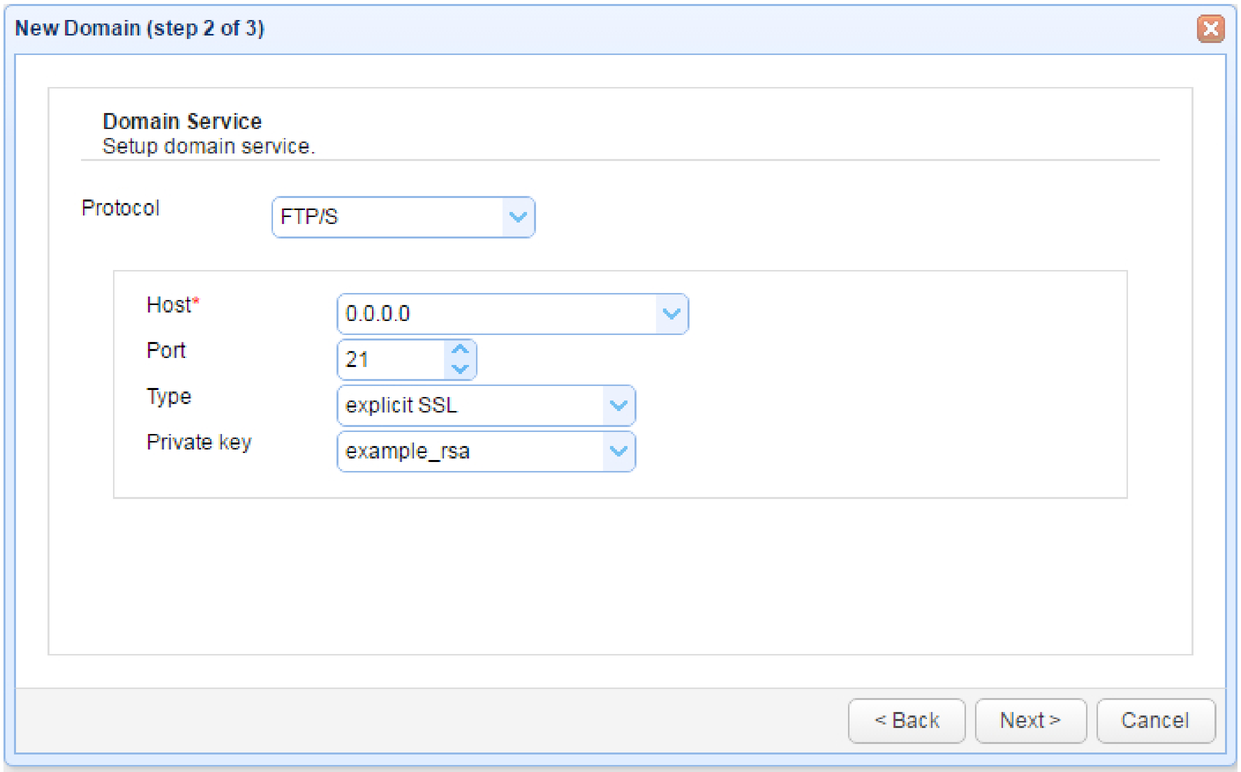
Description

Name - A unique name you wish to give this domain. Make sure to choose the name carefully as it may not be changed once created.

Description - A description of this domain.

Step 2

Figure 3



New Domain (step 2 of 3)

Domain Service
Setup domain service.

Protocol: FTP/S

Host*: 0.0.0.0
Port: 21
Type: explicit SSL
Private key: example_rsa

Protocol - The service type to add.

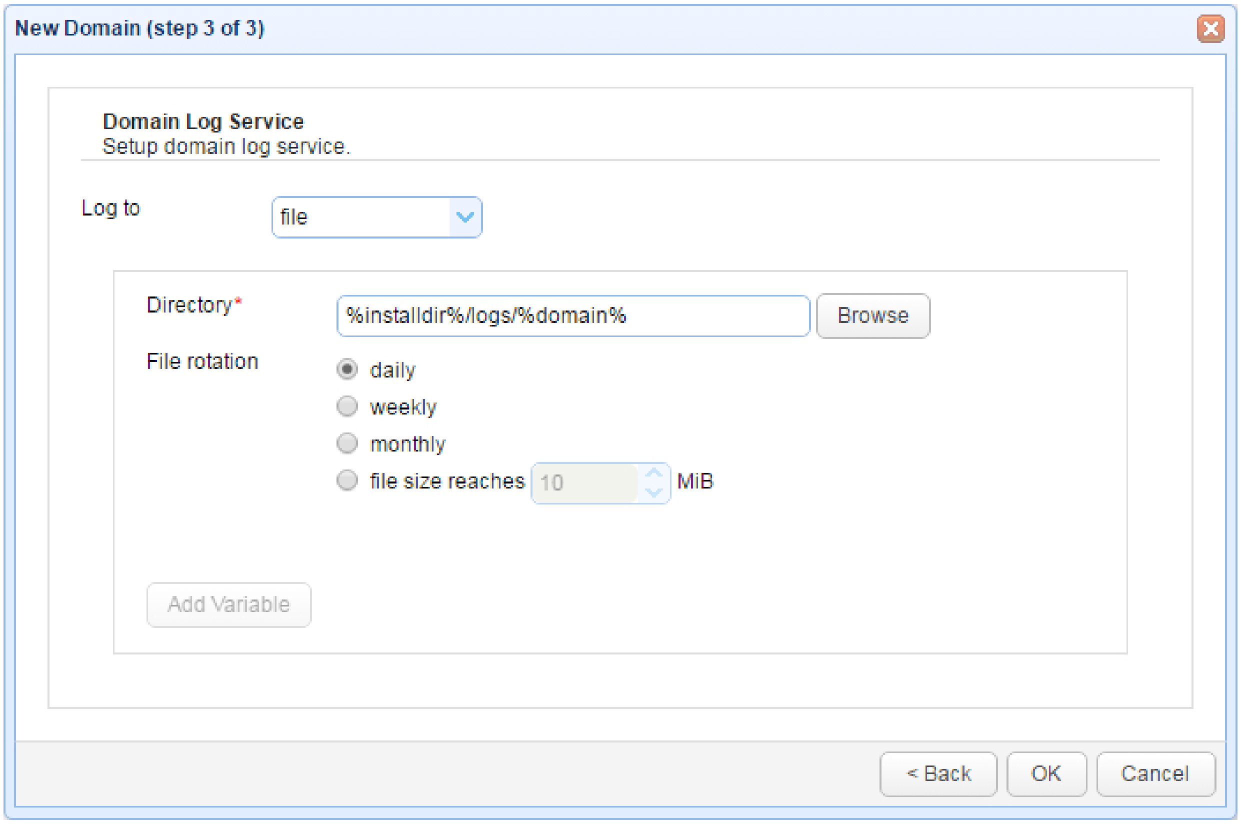
Host - The IP address that this service will listen on.

Port - The port that this service will listen on.

Private key - The private key that this service will use for encrypting communications. Available only when adding services that use encrypted communications e.g. FTPS, SFTP, AFTP etc.

Step 3

Figure 5



New Domain (step 3 of 3)

Domain Log Service
Setup domain log service.

Log to: file

Directory*: %installdir%/logs/%domain%

File rotation:
● daily
○ weekly
○ monthly
○ file size reaches 10 MiB

Log to - `file` to log user activity to a directory or `database` to log user activity to a JDBC accessible database.

Directory - The directory where to store log files. (file log)

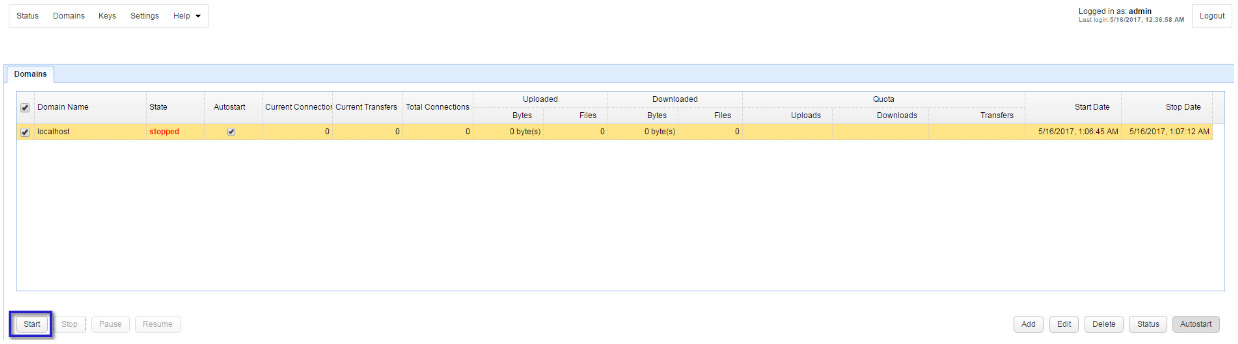
File rotation - The frequency in which to rotate log files. (file log)

Add Variable - Variables available for use in Directory field.

Starting a domain

Using JSCAPE MFT Server Manager select the domain you wish to start and click the `Start` button located in the lower left of your screen.

Figure 6



Logged in as: **admin**
Last login:5/16/2017, 12:36:58 AM

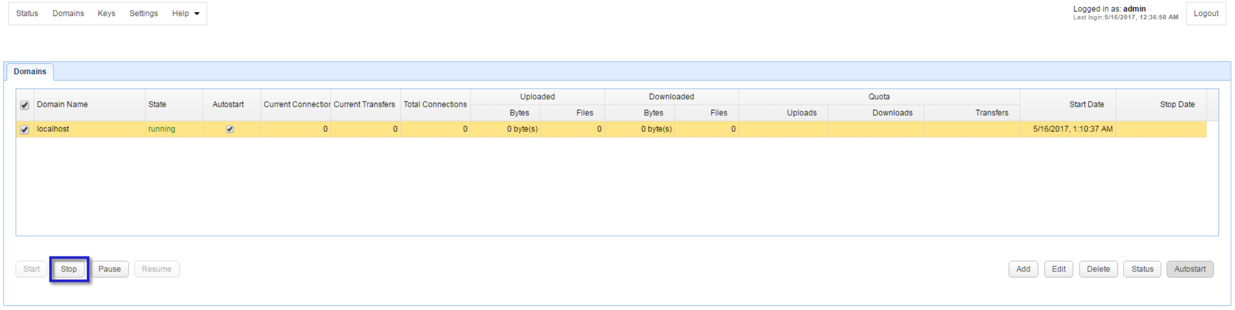
☑	Domain Name	State	Autostart	Current Connectior	Current Transfers	Total Connections	Uploaded		Downloaded		Quota			Start Date	Stop Date
							Bytes	Files	Bytes	Files	Uploads	Downloads	Transfers		
☑	localhost	stopped	☑	0	0	0	0 byte(s)	0	0 byte(s)	0				5/16/2017, 1:06:45 AM	5/16/2017, 1:07:12 AM

Server configuration 3

Stopping a domain

Using the JSCAPE MFT Server Manager select the domain you wish to stop and click the `Stop` button located in the lower left of your screen.

Figure 133

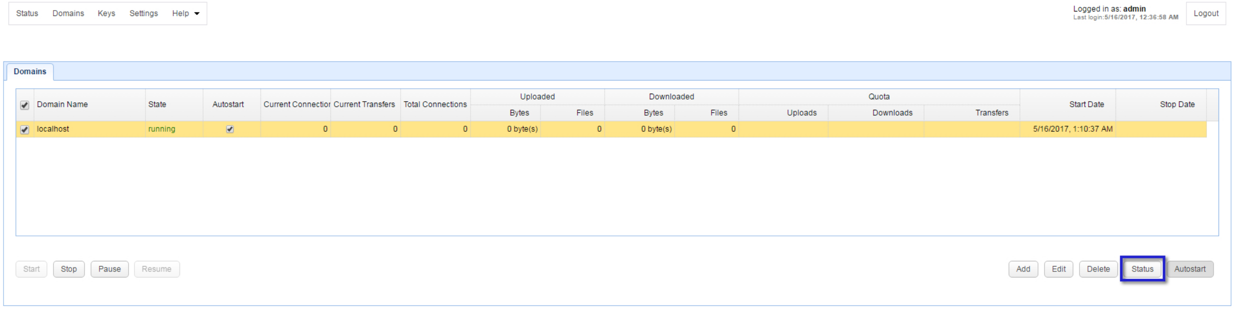


☑	Domain Name	State	Autostart	Current Connectior	Current Transfers	Total Connections	Uploaded		Downloaded		Quota			Start Date	Stop Date
							Bytes	Files	Bytes	Files	Uploads	Downloads	Transfers		
☑	localhost	running	☑	0	0	0	0 byte(s)	0	0 byte(s)	0				5/16/2017, 1:10:37 AM	

Viewing domain status

Using the JSCAPE MFT Server Manager select the domain you wish to view status for. Each column for the selected domain provides information on it's status. For additional information you may click the `Status` button.

Figure 234



☑	Domain Name	State	Autostart	Current Connectior	Current Transfers	Total Connections	Uploaded		Downloaded		Quota			Start Date	Stop Date
							Bytes	Files	Bytes	Files	Uploads	Downloads	Transfers		
☑	localhost	running	☑	0	0	0	0 byte(s)	0	0 byte(s)	0				5/16/2017, 1:10:37 AM	

Domain Name - The name of domain.

State - Indicates current status of domain as running or stopped.

Autostart - Indicates whether the domain is set to start automatically upon startup

Current Connections - The current number of client sessions connected to domain.

Current Transfers - The current number of file transfers in progress.

Total Connections - The total number of client sessions since start date.

Uploaded Bytes - The total number of bytes uploaded since start date.

Uploaded Files - The total number of files uploaded since start date.

Downloaded Bytes - The total number of bytes downloaded since start date.

Downloaded Files - The total number of files downloaded since start date.

Uploads Quota - The current upload quota if upload quota is enabled.

Downloads Quota - The current download quota if download quota is enabled.

Transfers Quota - The current transfer quota if transfer quota is enabled.

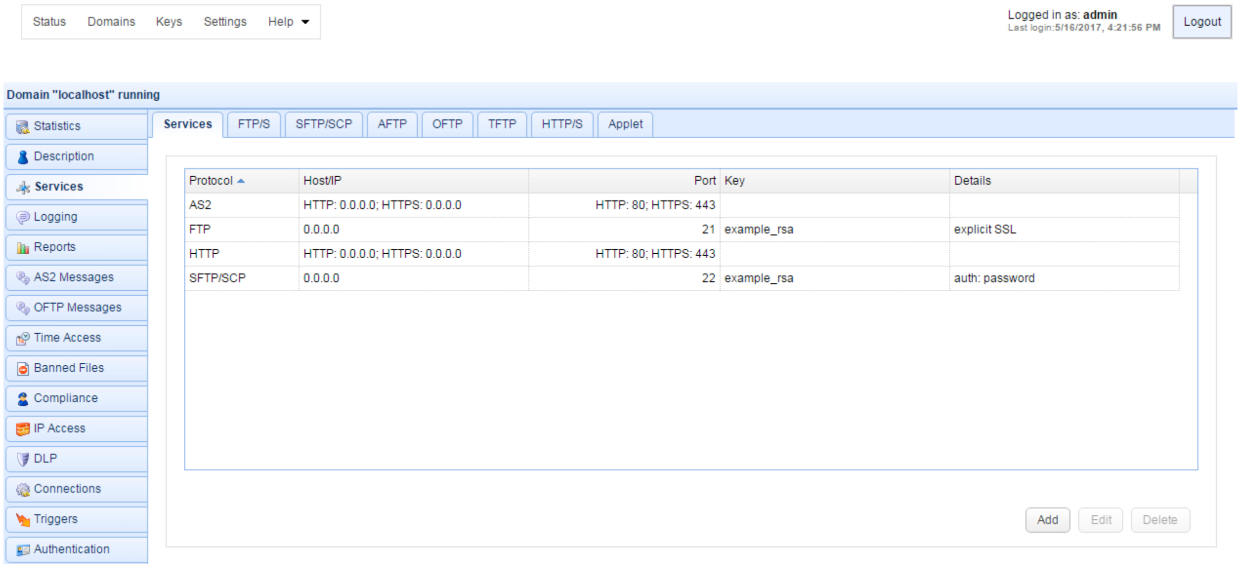
Start Date - The date/time server was started.

Stop Date - The date/time server was stopped.

Adding services

A service is an IP/Host, Port and Protocol combination that accepts client requests. To view existing services for a domain, select the desired domain and click the `Edit` button. Next, select the `Services` node. A list of services for the domain are displayed.

Figure 9



Protocol ▲	Host/IP	Port	Key	Details
AS2	HTTP: 0.0.0.0; HTTPS: 0.0.0.0	HTTP: 80; HTTPS: 443		
FTP	0.0.0.0	21	example_rsa	explicit SSL
HTTP	HTTP: 0.0.0.0; HTTPS: 0.0.0.0	HTTP: 80; HTTPS: 443		
SFTP/SCP	0.0.0.0	22	example_rsa	auth: password

Protocol - The service protocol. Available protocols are AFTP, AS2, FTP/S, HTTP/S, OFTP, SFTP/SCP, TFTP, WebDAV/S.

Host/IP - The IP address that this service will listen on.

Port - The port that this service will listen on.

Key - The private encryption key that this service will use for encrypted communications.

Details - Any additional details for this service.

Service types

AFTP - Accelerated File Transfer Protocol developed by JSCAPE. Runs on top of UDP protocol and provides fast file transfers over networks with high latency and/or packet loss characteristics.

AS2 - Accepts incoming AS2 messages.

FTP regular - Accepts standard unencrypted FTP connections.

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

FTP forced explicit SSL - Accepts only encrypted explicit SSL connections using AUTH TLS or AUTH SSL client commands.

FTP implicit SSL - Accepts only encrypted implicit SSL connections.

HTTP/S - Accepts HTTP and/or encrypted HTTPS connections.

OFTP - Accepts incoming OFTP (Odette File Transfer Protocol) connections.

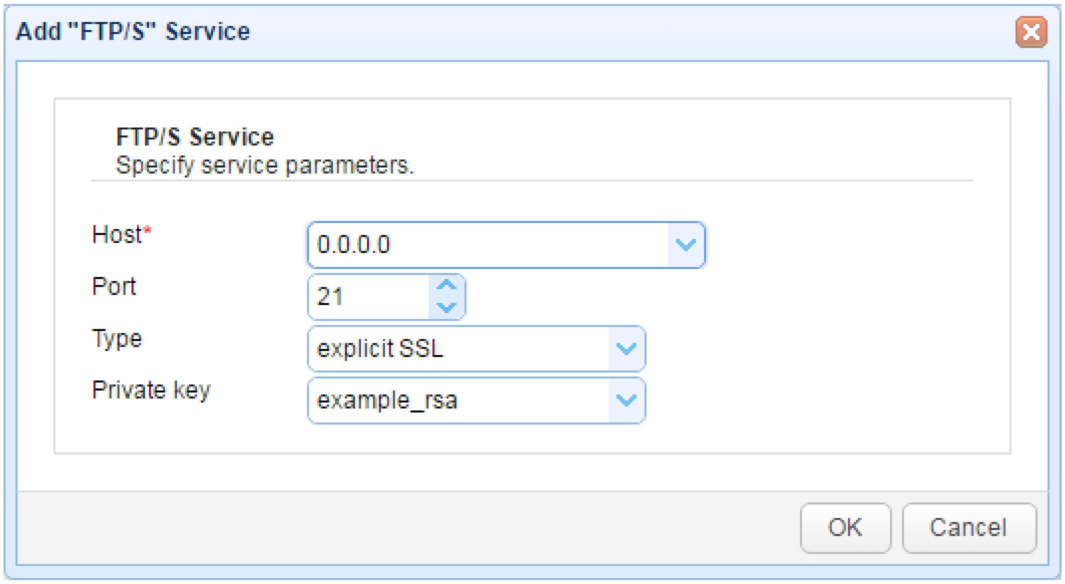
SFTP/SCP - Accepts encrypted SFTP (FTP over SSH) connections and SCP (Secure Copy)

TFTP - Accepts TFTP (Trivial File Transfer Protocol) connections.

WebDAV/S - Accepts WebDAV connections.

Add service

Figure 10



Add "FTP/S" Service

FTP/S Service
Specify service parameters.

Host*	0.0.0.0
Port	21
Type	explicit SSL
Private key	example_rsa

Protocol - The service protocol. Available protocols are AFTP, AS2, FTP/S, HTTP/S, OFTP, SFTP/SCP, TFTP, WebDAV/S.

Host - The IP address that this service will listen on.

Port - The port that this service will listen on.

Type - The protocol(s) that this service will accept connections for. (FTP)

Private key - The private encryption key that this service will use for encrypted communications.

Edit service

To edit a service select the service you wish to edit and click the "Edit" button.

Delete service

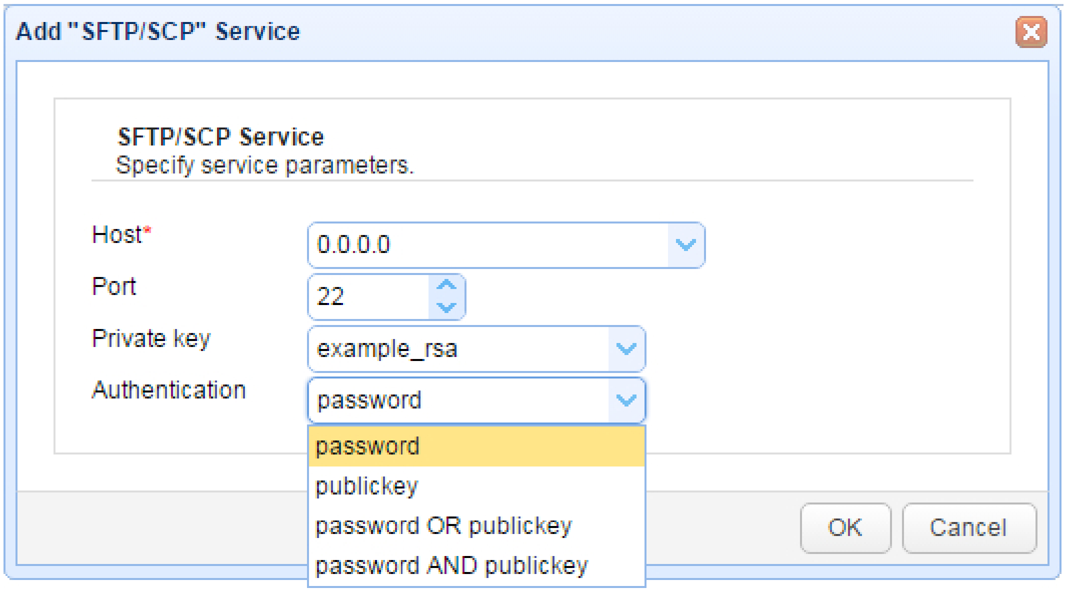
To delete a service select the service you wish to delete and click the "Delete" button.

Setting SFTP/SSH authentication mode

The SFTP/SCP service supports various forms of user authentication. These include `password`, `publickey`, `password OR publickey` and `password AND public key`.

Authentication modes

Figure 76



Add "SFTP/SCP" Service

SFTP/SCP Service
Specify service parameters.

Host*: 0.0.0.0
Port: 22
Private key: example_rsa
Authentication: password

Host - The IP address that this service will listen on.

Port - The port that this service will listen on.

Private key - The encryption key that this server will use for SSH communications.

Authentication - The authentication mode clients must use when connecting to SFTP/SCP service.

Authentication modes

password - User must authentication with password only.

publickey - User must authentication with a private key that corresponds with public key installed on server.

password OR publickey - User must authenticate with password OR with a private key that corresponds with public key installed on server.

password AND publickey - User must authenticate with password AND with a private key that corresponds with public key installed on server.

See also

Client keys overview
Using public key authentication in SFTP/SSH

Using public key authentication in SFTP/SSH

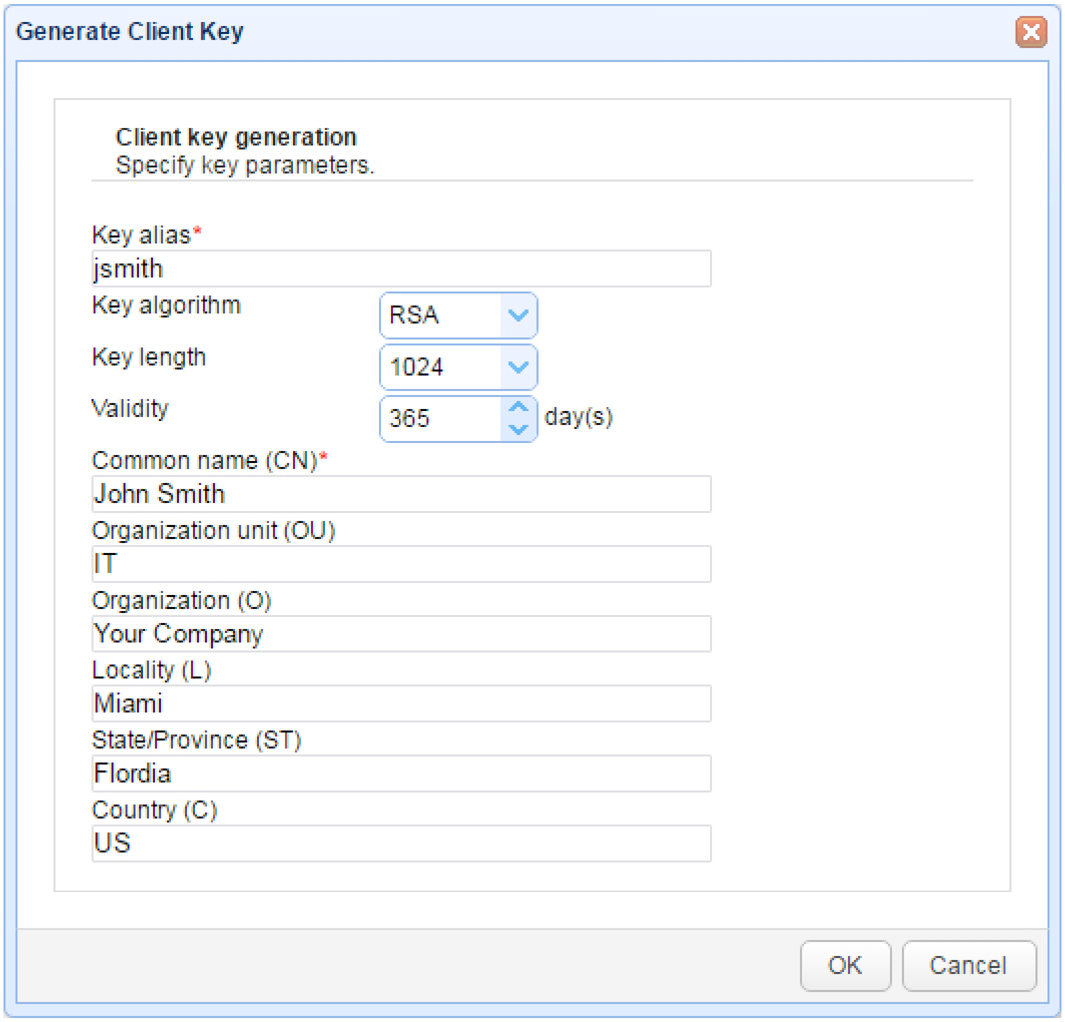
The SFTP/SCP service supports public key authentication. In public key authentication the client authenticates with the server using a username and private key (optionally password protected) accessible only to the user. For increased security the SFTP/SCP service may be configured to require **both** a private key and the account password. In order to use public key authentication the SFTP/SCP service must be configured properly (See Setting SFTP/SSH authentication mode) and a public key must be associated with the user.

To associate a public key with a user you may store the key in the centralized `Key Manager`, or you can allow the user to manage their own key (See Web user interface for details). To create a key using the `Key Manager` follow the steps below.

Create a client key

1. Go to `Keys > Client Keys` panel and click on the `Generate` button to create a new client key. When prompted for a `Key alias` it is recommended you enter the username that you would like to associate this key with. For the `Type` and `Length` fields you may leave these as the default values or select from options provided. Click `OK` to continue.

Figure 75



Generate Client Key

Client key generation
Specify key parameters.

Key alias*: jsmith

Key algorithm: RSA

Key length: 1024

Validity: 365 day(s)

Common name (CN)*: John Smith

Organization unit (OU): IT

Organization (O): Your Company

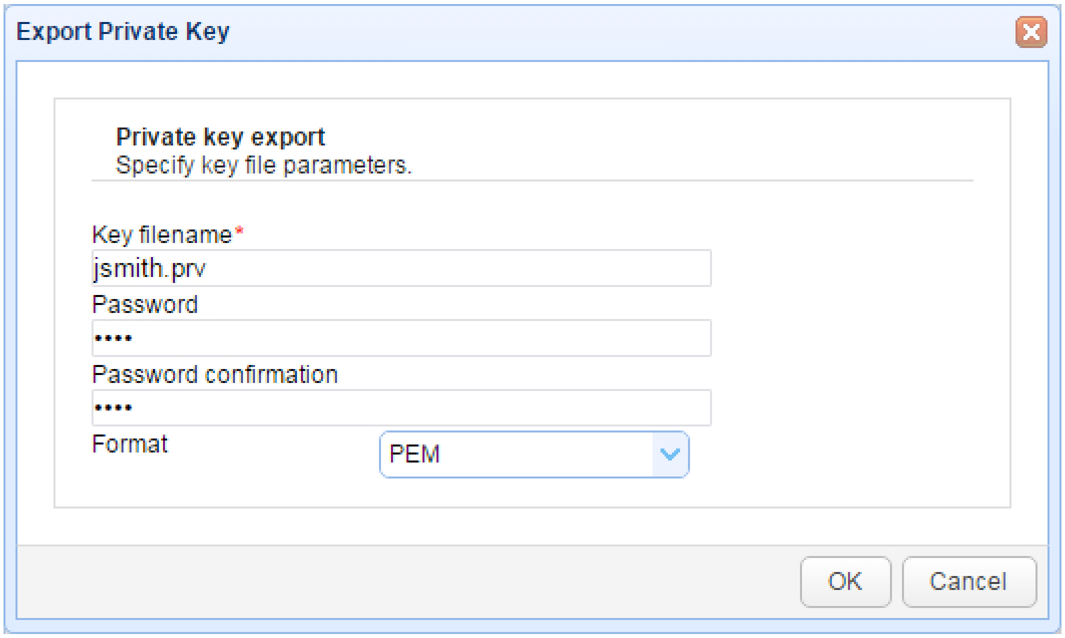
Locality (L): Miami

State/Province (ST): Flordia

Country (C): US

2. Next you will need to export the private key. This is the key you will use in your SFTP/SCP client for authenticating with the SFTP/SCP service. When exporting private key select the PEM file type format. If your SFTP/SCP client requires a different format you may select that format from the available `Format` options. Click `OK` to export your private key and add client key to the `Client Keys` listing.

Figure 103

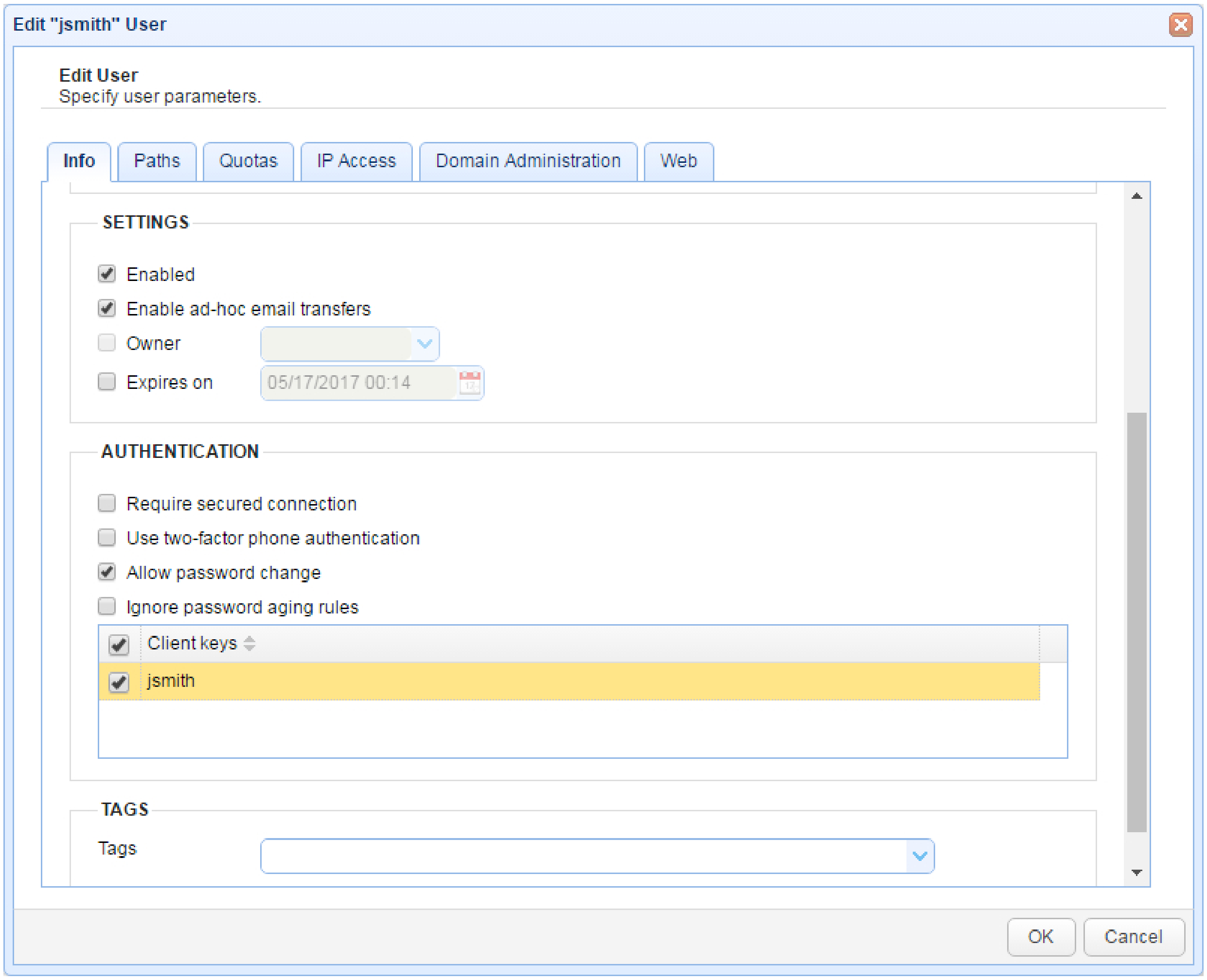


Private key export
Specify key file parameters.

Key filename*
jsmith.prv
Password
••••
Password confirmation
••••
Format PEM

3. The next step is to bind this client key to the user. This allows this client key to be used by this user for authentication purposes. Navigate into the domain where this user belongs to, go to the `Users` node, select the user for this key and click `Edit` button. In the `Client keys` section check the client key that you created earlier and click `OK`.

Figure 105



Edit "jsmith" User

Edit User
Specify user parameters.

SETTINGS

☑ Enabled
☑ Enable ad-hoc email transfers
□ Owner
□ Expires on 05/17/2017 00:14

AUTHENTICATION

□ Require secured connection
□ Use two-factor phone authentication
☑ Allow password change
□ Ignore password aging rules

☑	Client keys
☑	jsmith

TAGS

Tags

4. Next you must add the SFTP/SCP service with the option to allow authentication using public keys. If you have already done this then you may skip this step. Otherwise, go to the `Services` node, select the `Add` button and select the SFTP/SCP protocol. Set the `Authentication` option for service to use one of the `publickey` options and click `OK`. In case you already have an existing SFTP/SCP service but that service is using `password` authentication, select that SFTP/SCP service, click the `Edit` button, and then change the `Authentication` to any of the `publickey` options.

5. You have successfully enabled public key authentication for the SFTP/SCP service. To authenticate, instruct your SFTP/SCP client to use the private key you exported in Step 2. Some SFTP/SCP clients, e.g. Putty, use a proprietary private key format. Therefore it may be necessary that you convert the PEM formatted key to the client proprietary key format prior to connecting. For Putty client you may use the `puttygen.exe` utility to make this conversion.

See also

Setting SFTP/SSH authentication mode

Server configuration 3

Setting logging preferences

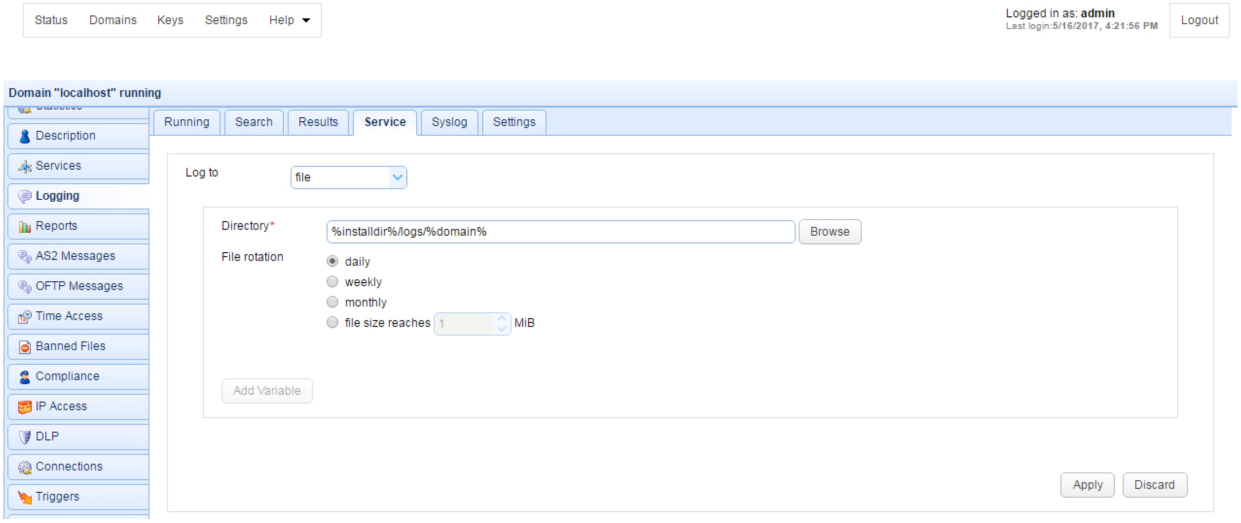
JSCAPE MFT Server logs all user activity to a log directory or JDBC accessible database. To configure logging preferences go to the `Logging` node in JSCAPE MFT Server Manager for the desired domain.

[File Log](#)
[Database Log](#)
[Syslog](#)
[Verbose Logging](#)
[Restoring a Database Log](#)

File Log

Logs all server activity to a directory.

Figure 12



Logged in as: **admin**
Last login:5/16/2017, 4:21:56 PM

Domain "localhost" running

Log to: file

Directory*: %installdir%/logs/%domain%

File rotation:
● daily
○ weekly
○ monthly
○ file size reaches 1 MiB

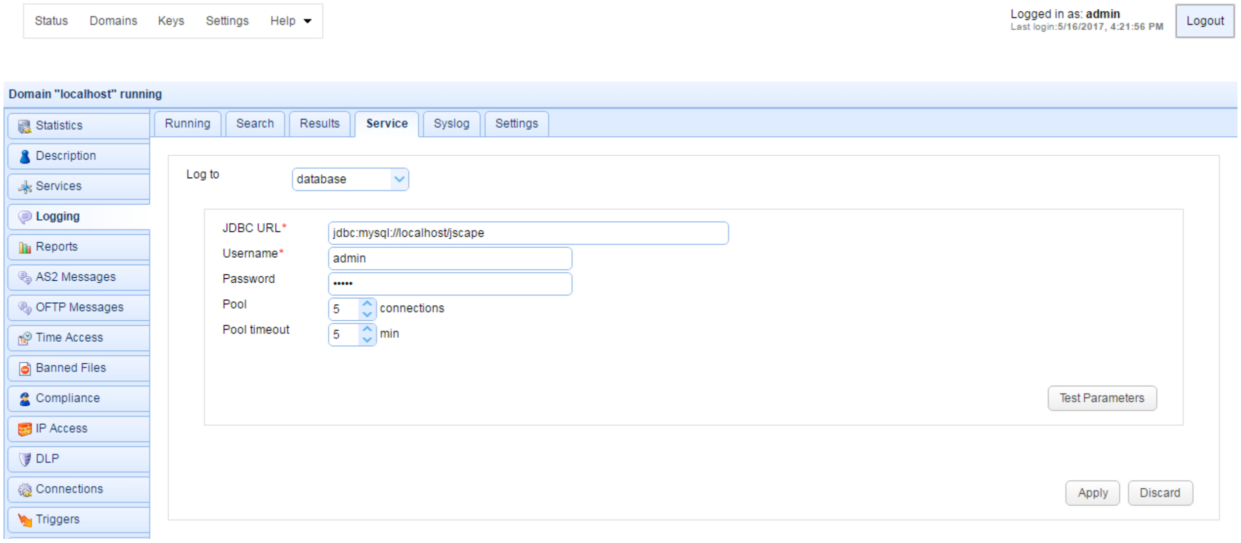
Directory - The directory where to store log files.

File rotation - 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 and necessary tables on your database server and register the appropriate database driver with JSCAPE MFT Server. Example database schema for MySQL, Microsoft SQL Server and Oracle are provided in the files `etc/mysql.sql`, `etc/mssql.sql` and `etc/oracle.sql` respectively. Libraries for JDBC drivers must be placed in the `libs/jdbc` directory of your JSCAPE MFT Server installation, the JSCAPE MFT Server Service restarted and the JDBC driver class registered in `Settings > JDBC Drivers` in order for the database to be accessible to JSCAPE MFT Server.

Figure 63



Logged in as: admin
Last login:5/16/2017, 4:21:56 PM

Domain "localhost" running

Log to: database

JDBC URL*: jdbc:mysql://localhost/jscape
Username*: admin
Password: •••••
Pool: 5 connections
Pool timeout: 5 min

JDBC 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.

Username - The username to connect with when authenticating with database.

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

Pool - The maximum number of connections in database pool.

Pool timeout - 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 settings.

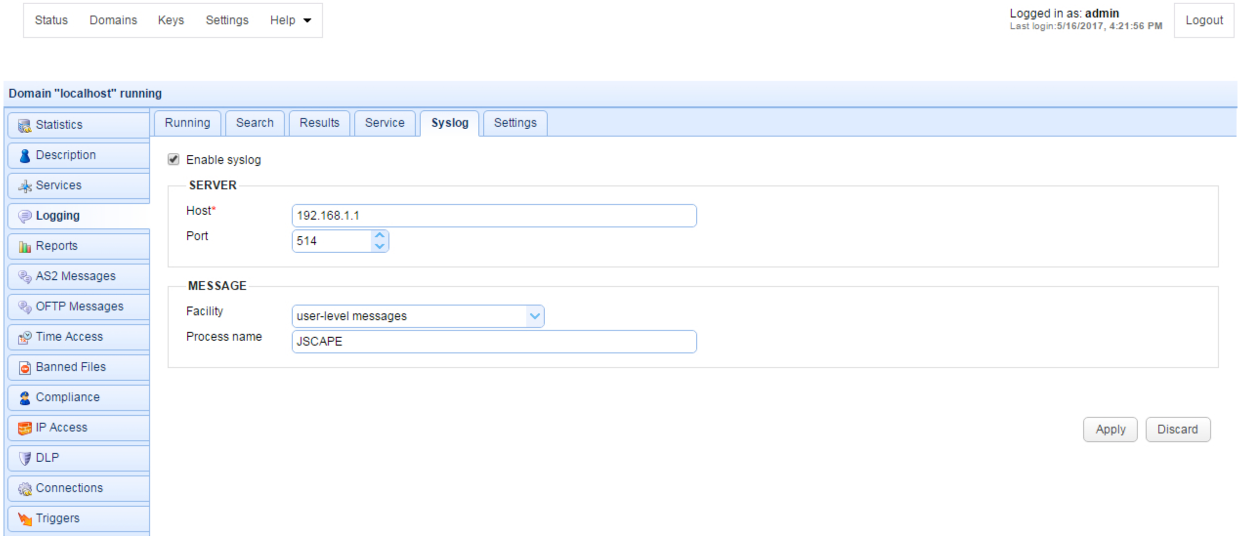
See also

JDBC settings

Syslog

Logs all activity to a syslog daemon **in addition to** your existing File Log or Database Log settings. To use the Syslog option you must have an existing syslog daemon running. This may be a local or remote syslog daemon.

Figure 116



☑ Enable syslog

SERVER

Host* 192.168.1.1

Port 514

MESSAGE

Facility user-level messages

Process name JSCAPE

Host - The IP address of syslog daemon.

Port - The port of syslog daemon.

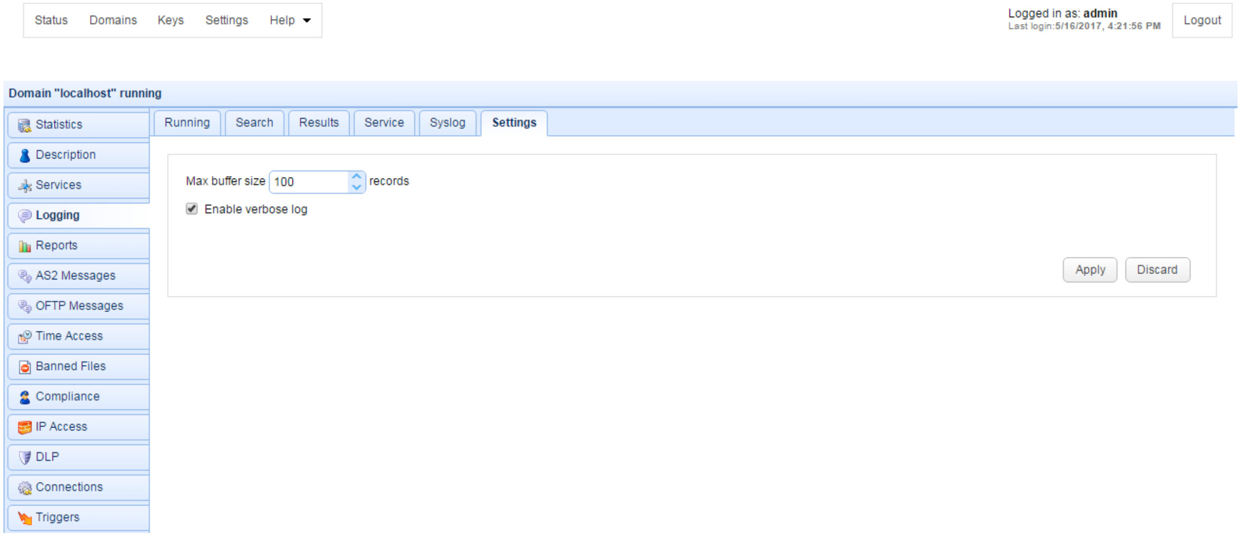
Facility - The syslog facility to use.

Process name - Process name tag to apply to all log messages sent to syslog daemon.

Verbose Logging

If you need to debug a connection related issue it is often helpful to enable verbose logging. This can be enabled using the `Settings` tab and checking the `Enable verbose log` option. This option is disabled by default and should **only** be used for temporary debugging purposes as verbose logging contains a lot of information that can significantly slow performance and increase the size of log files.

Figure 65



Max buffer size 100 records

☑ Enable verbose log

Restoring a Database Log

In the event that the database server cannot be contacted logging data will be directed to a temporary file located in the `backups` directory of your JSCAPE MFT Server installation. To move the contents of this temporary log file to your database use the `backuplog` command providing the domain that you wish to restore. The `backuplog` executable may be found in your JSCAPE MFT Server installation directory.

Example

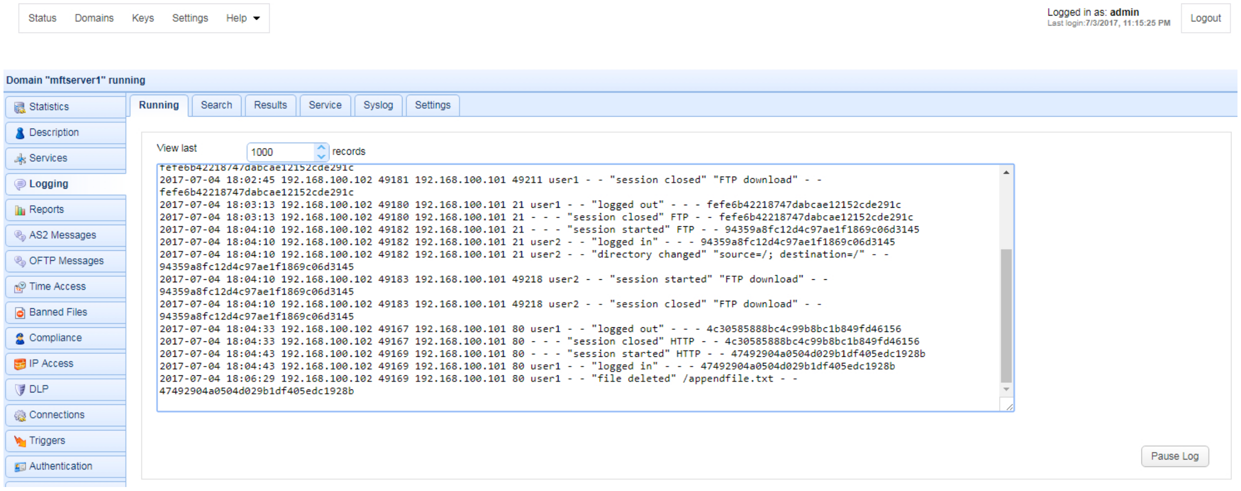
```
backuplog -domain localhost
```

The above command moves the contents of the temporary log file for domain `localhost` to the log database assigned to this domain.

Viewing log data

Log data may be viewed using any text editor or SQL client depending on the logging datastore used. Optionally you may use the `Logging > Running` tab of JSCAPE MFT Server Manager to view up to the last 1000 records of log activity.

Figure 39



View last 1000 records

```
fefe6b42218747dabcae12152cde291c
2017-07-04 18:02:45 192.168.100.102 49181 192.168.100.101 49211 user1 - - "session closed" "FTP download" - -
fefe6b42218747dabcae12152cde291c
2017-07-04 18:03:13 192.168.100.102 49180 192.168.100.101 21 user1 - - "logged out" - - - fefe6b42218747dabcae12152cde291c
2017-07-04 18:03:13 192.168.100.102 49180 192.168.100.101 21 - - - "session closed" FTP - - fefe6b42218747dabcae12152cde291c
2017-07-04 18:04:10 192.168.100.102 49182 192.168.100.101 21 - - - "session started" FTP - - 94359a8fc12d4c97ae1f1869c06d3145
2017-07-04 18:04:10 192.168.100.102 49182 192.168.100.101 21 user2 - - "logged in" - - - 94359a8fc12d4c97ae1f1869c06d3145
2017-07-04 18:04:10 192.168.100.102 49182 192.168.100.101 21 user2 - - "directory changed" "source=/; destination=/" - -
94359a8fc12d4c97ae1f1869c06d3145
2017-07-04 18:04:10 192.168.100.102 49183 192.168.100.101 49218 user2 - - "session started" "FTP download" - -
94359a8fc12d4c97ae1f1869c06d3145
2017-07-04 18:04:10 192.168.100.102 49183 192.168.100.101 49218 user2 - - "session closed" "FTP download" - -
94359a8fc12d4c97ae1f1869c06d3145
2017-07-04 18:04:33 192.168.100.102 49167 192.168.100.101 80 user1 - - "logged out" - - - 4c30585888bc4c99b8bc1b849fd46156
2017-07-04 18:04:33 192.168.100.102 49167 192.168.100.101 80 - - - "session closed" HTTP - - 4c30585888bc4c99b8bc1b849fd46156
2017-07-04 18:04:43 192.168.100.102 49169 192.168.100.101 80 - - - "session started" HTTP - - 47492904a0504d029b1df405edc1928b
2017-07-04 18:04:43 192.168.100.102 49169 192.168.100.101 80 user1 - - "logged in" - - - 47492904a0504d029b1df405edc1928b
2017-07-04 18:06:29 192.168.100.102 49169 192.168.100.101 80 user1 - - "file deleted" /appendfile.txt - -
47492904a0504d029b1df405edc1928b
```

View last X records - The number of records you want to view from end of domain log.

Pause/Resume Log - Pauses/resumes running view of log.

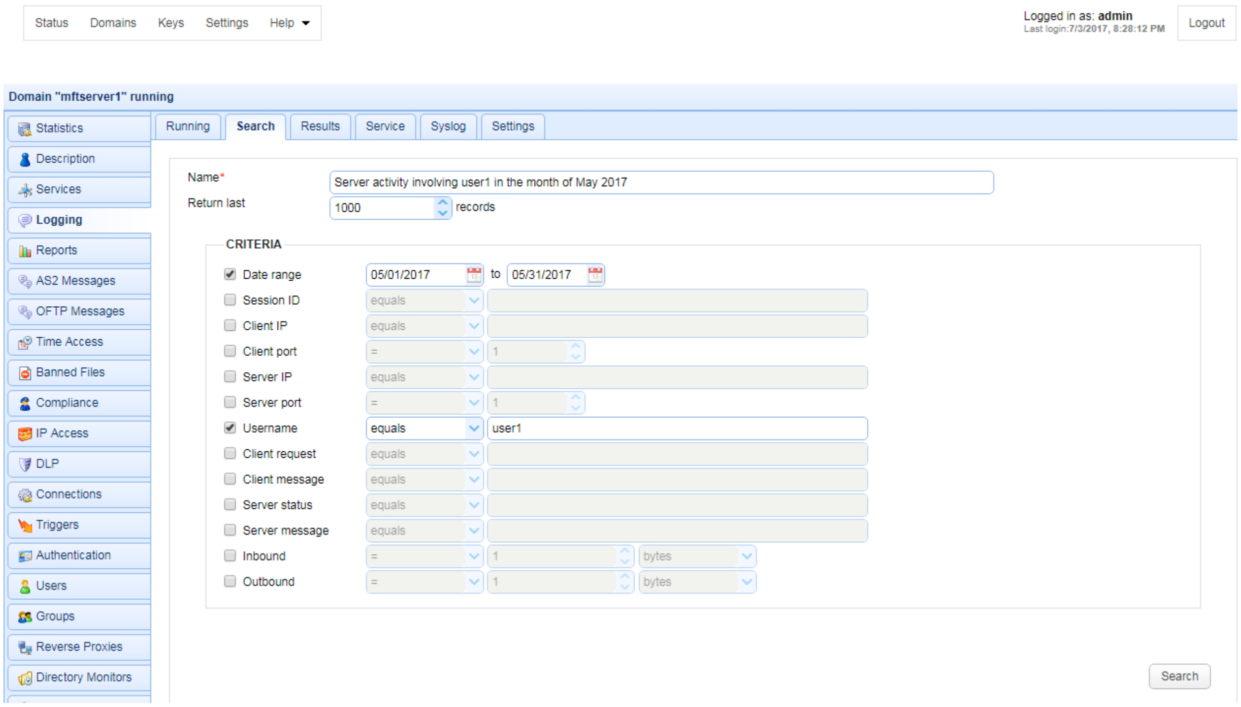
Server configuration 3

Running a search against log data

You may run a search against log data and narrow the results by applying a set of criteria. The criteria may include any combination of the following:

- Date range
- Session ID
- Client IP
- Client port
- Server IP
- Server port
- Username
- Client request
- Client message
- Server status
- Inbound
- Outbound

To run a search, go to `Logging > Search` and then give the search a descriptive name. Select one or more criteria, select each criterion's corresponding comparison operator (e.g. =, !=, >, contains, matches, etc.), and then enter a value for that criteria. When done, click the `Search` button.



Logged in as: **admin**
Last login:7/3/2017, 8:28:12 PM

Domain "mftserver1" running

Name*: Server activity involving user1 in the month of May 2017

Return last: 1000 records

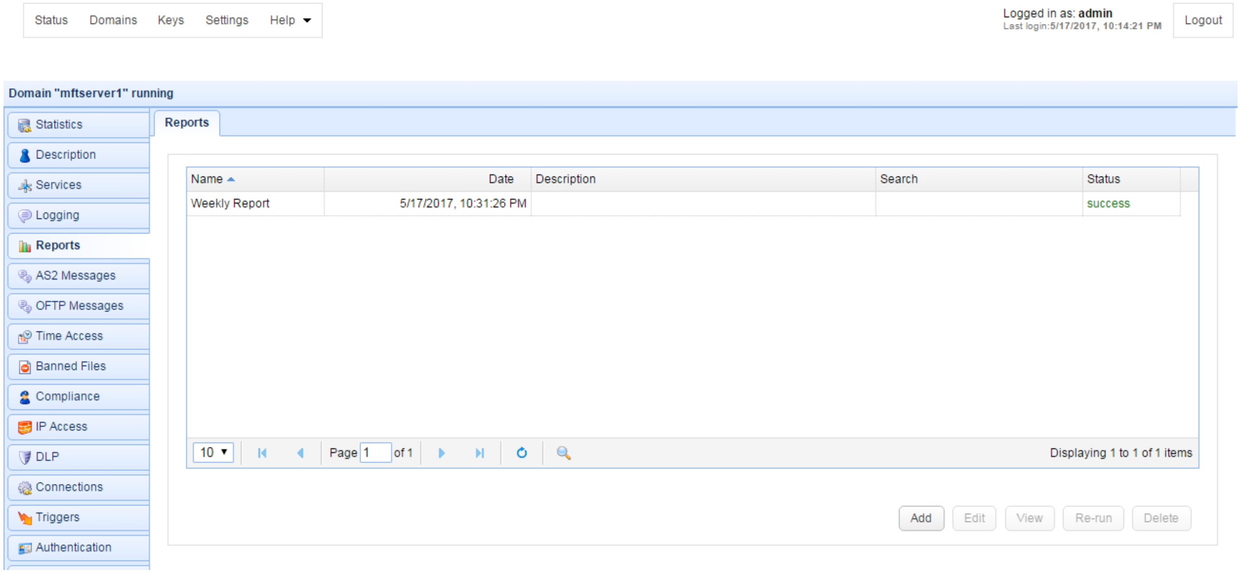
CRITERIA

☑ Date range	05/01/2017	to	05/31/2017
☐ Session ID	equals		
☐ Client IP	equals		
☐ Client port	=	1	
☐ Server IP	equals		
☐ Server port	=	1	
☑ Username	equals	user1	
☐ Client request	equals		
☐ Client message	equals		
☐ Server status	equals		
☐ Server message	equals		
☐ Inbound	=	1	bytes
☐ Outbound	=	1	bytes

Reporting on log data

To create a report click on the `Reports` node for the desired domain. A list of existing reports will be displayed.

Figure 38



Name	Date	Description	Search	Status
Weekly Report	5/17/2017, 10:31:26 PM			success

Name - The name of the report.

Date - The date the report was created.

Description - The report description.

Search - The optional search result used to generate this report.

Status - The percentage of report completed.

Refresh - To refresh the current report view and update report status.

Add - Add a report.

Edit - Edit a report.

View - View selected report.

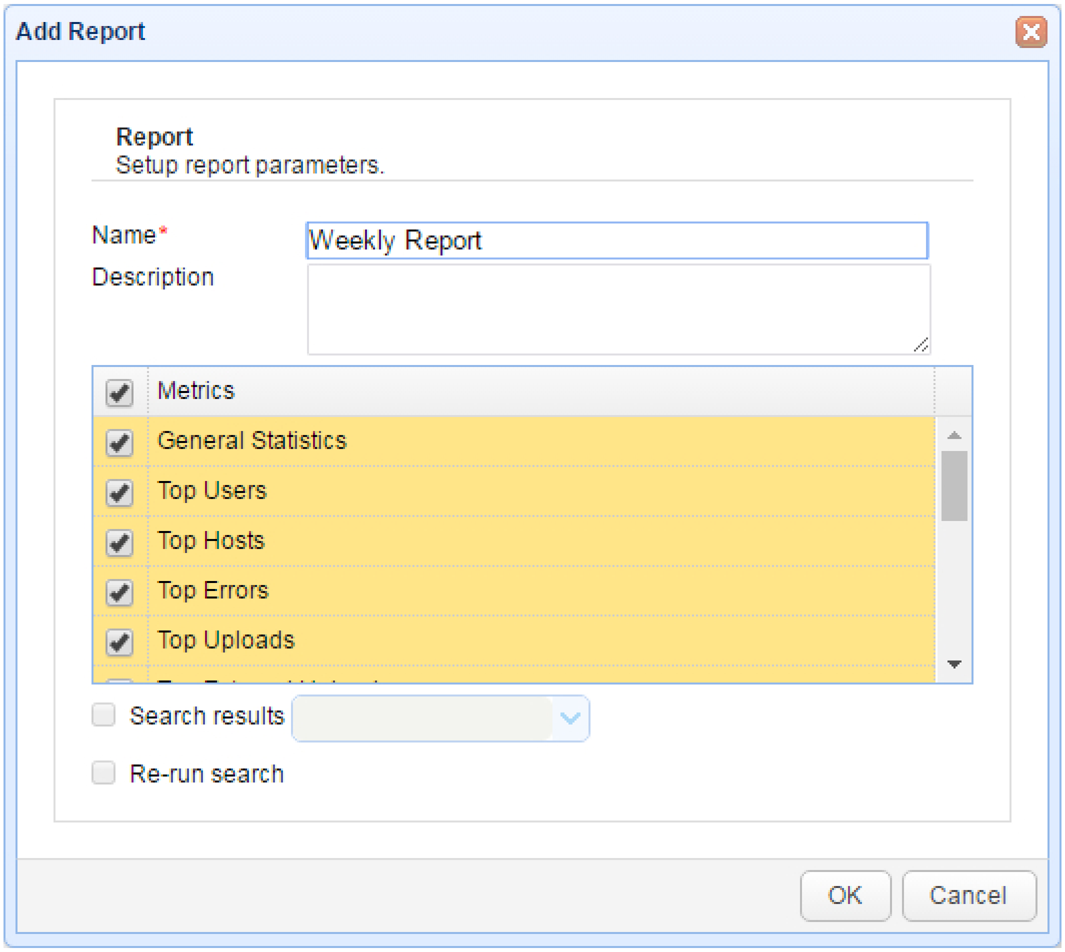
Re-run - Re-run selected report.

Delete - Delete selected report.

Adding a report

Click on the Add button. The `Add Report` dialog is displayed.

Figure 45



Add Report

Report
Setup report parameters.

Name* Weekly Report

Description

☑ Metrics
☑ General Statistics
☑ Top Users
☑ Top Hosts
☑ Top Errors
☑ Top Uploads

□ Search results

□ Re-run search

Name - A unique name for this report.

Description - A description of this report.

Metrics - The metrics you wish to include in this report.

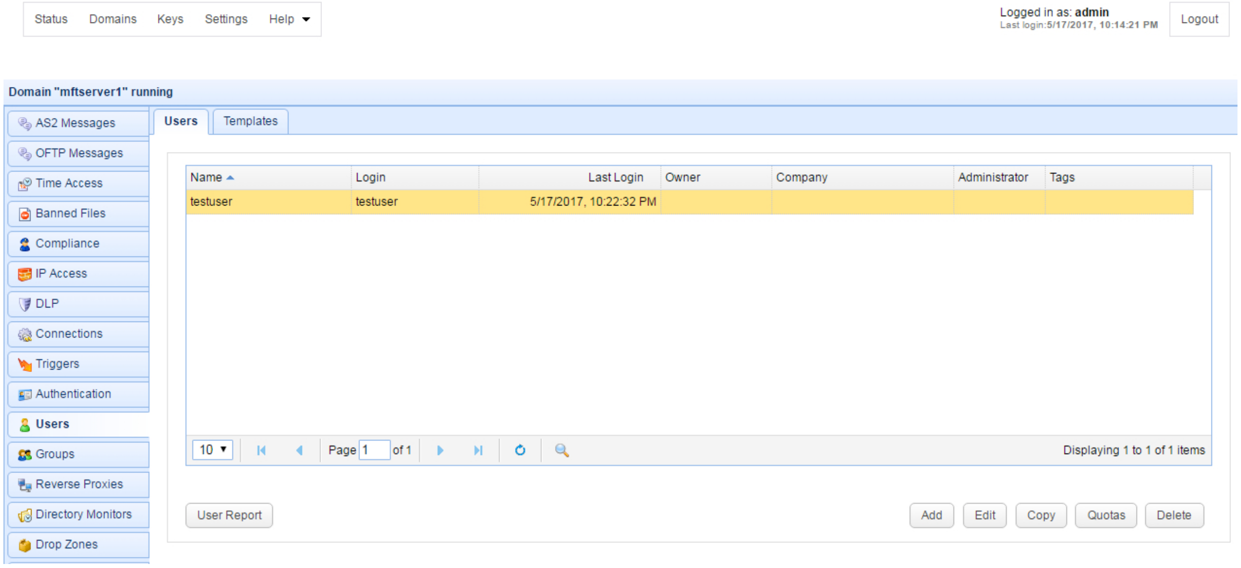
Search results - A search result to use when running this report.

Re-run search - Enable if you wish to re-run search results.

Adding users

A user is a valid account that may login to a domain's service. To view a list of users click on the `Users` node for the desired domain.

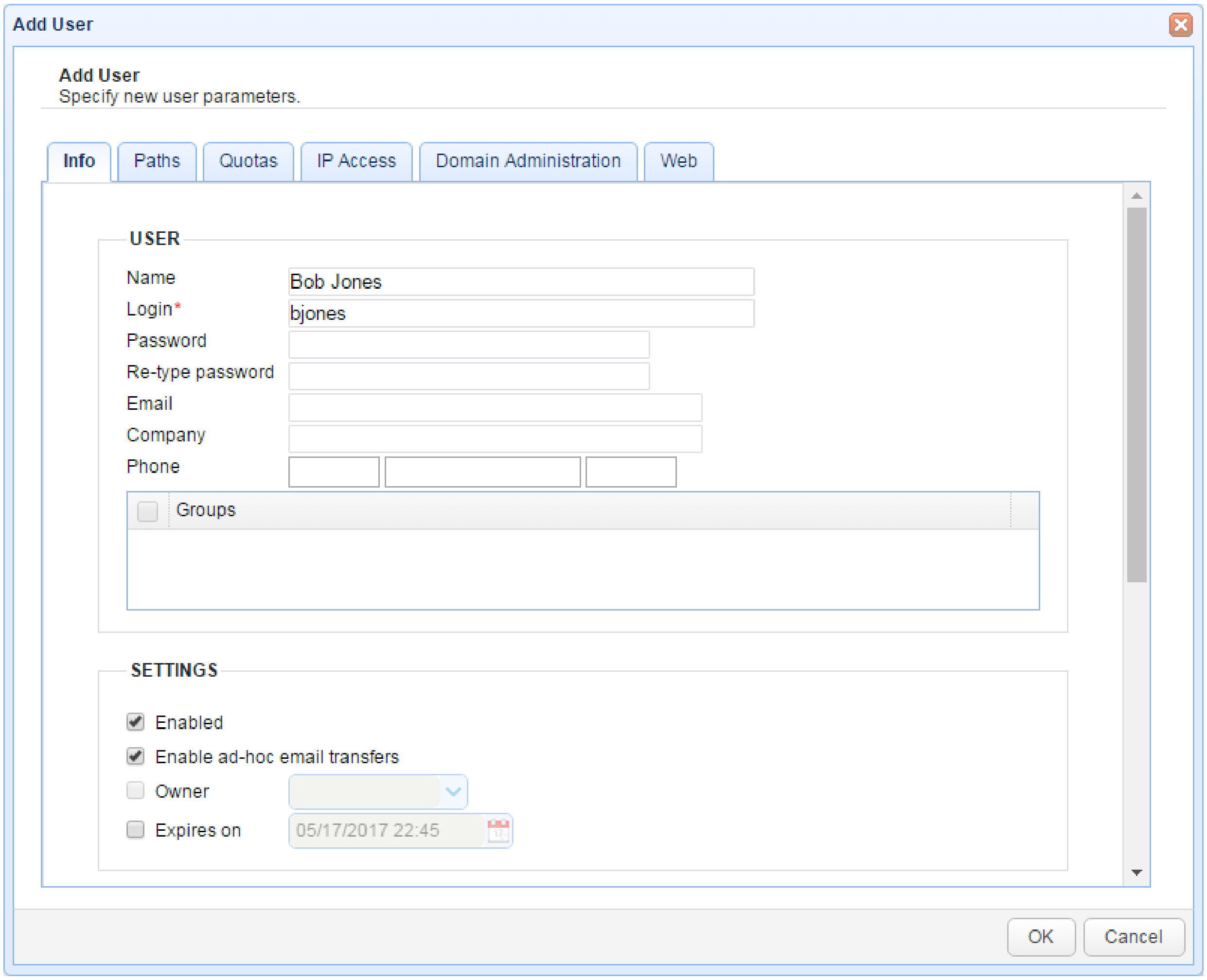
Figure 15



Name	Login	Last Login	Owner	Company	Administrator	Tags
testuser	testuser	5/17/2017, 10:22:32 PM				

To add a user click on the `Add` button in the lower right corner. Choose a `Template` or accept the `Default` template and then click the `OK` button. The `Add User` dialog will be displayed.

Figure 16



USER

Name: Bob Jones

Login*: bjones

Password:

Re-type password:

Email:

Company:

Phone:

□ Groups

SETTINGS

☑ Enabled

☑ Enable ad-hoc email transfers

□ Owner

□ Expires on 05/17/2017 22:45

User

Name - The full name of this user.

Login - The login name for this user.

Password - The password for this user.

Re-type password - The password for this user.

Email - Optional email address for this user.

Company - The company that this user is associated with.

Phone - The phone number for this user. The first field is the country code (e.g. "1" for United States) and the second field is the telephone number including any area code, the third field is the phone extension. This field is used primarily in conjunction with Phone Authentication.

Groups - Optional groups that this user is a member of.

Settings

Enabled - Check to enable this account.

Enable ad-hoc email transfers - Check to allow user to perform ad-hoc email transfers via HTTP interface.

Owner - Optional login of user who owns/manages this account.

Expires on - Date that this account expires (leave blank for non-expiring account).

Authentication

Require secured connection - Check to force user to login using secure protocol (e.g. FTPS/SFTP/HTTPS).

Use two-factor phone authentication - Check to require user to use two-factor phone authentication.

Allow password change - Check to allow user to change their password.

Ignore password aging rules - Check to disable password aging rules for this user.

Client keys - Optional public-keys bound to this user for purposes of public-key authentication in SFTP/ SSH protocol, or client certificate authentication in SSL protocols.

Tags

Tags may be used to limit visibility of users to administrators that are assigned a role containing specified tag.

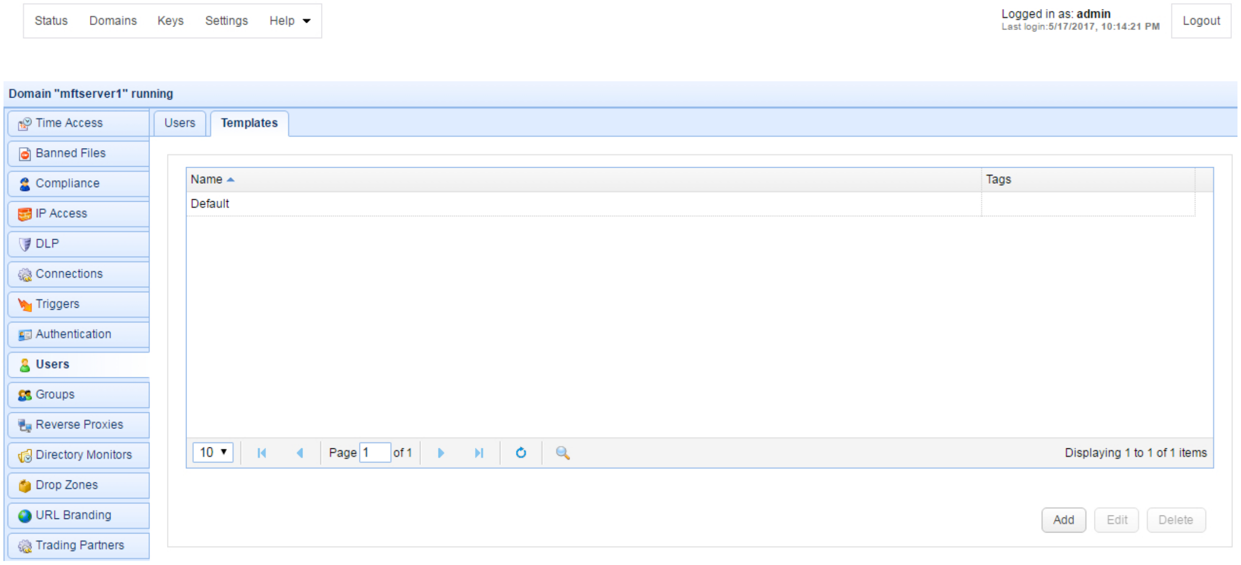
See also

Phone Authentication
Managing administrative tags

Defining user templates

A user template is a template that is used for creating users. To view a list of available templates click the `Users > Templates` panel for the desired domain.

Figure 112

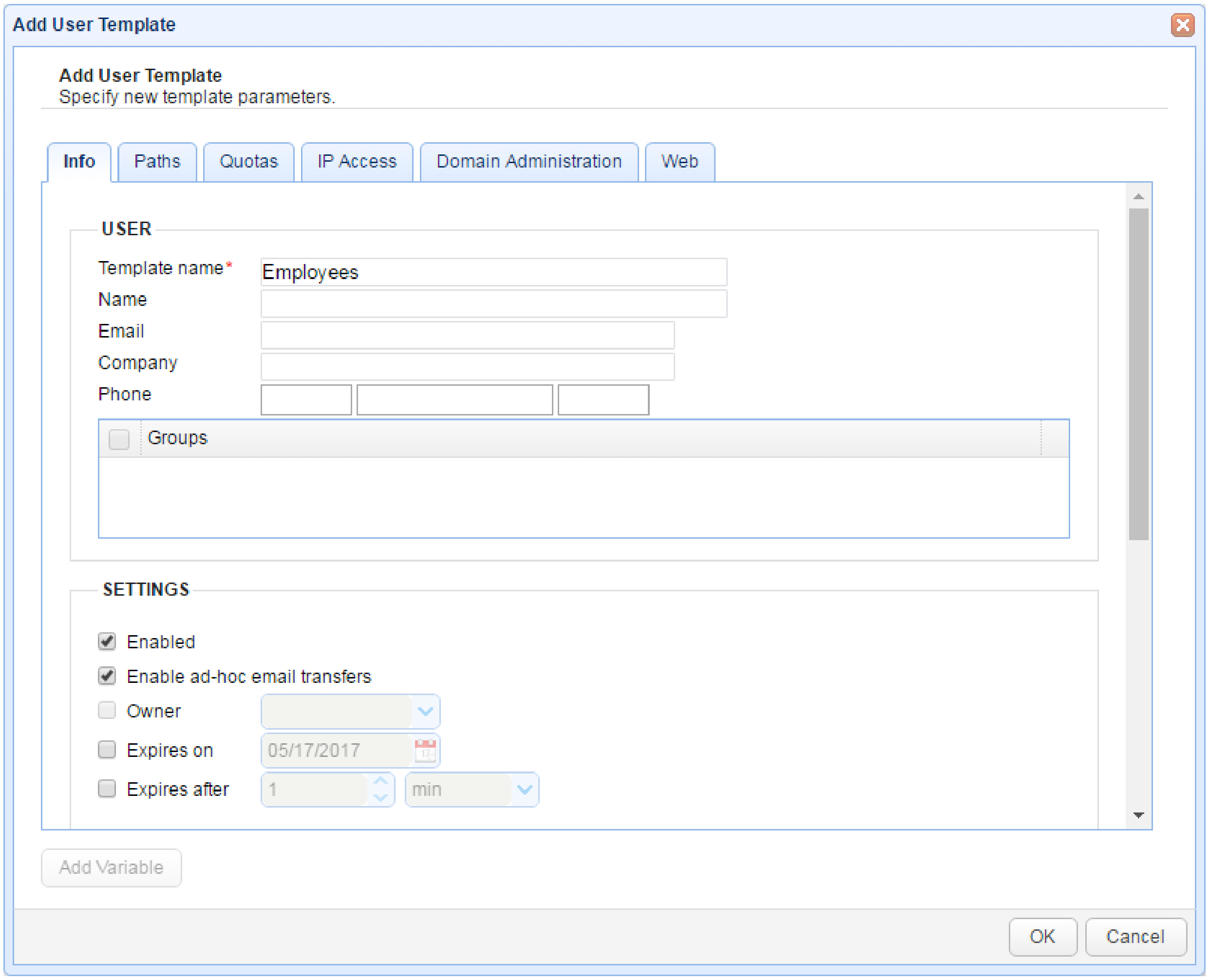


Name	Tags
Default	

Displaying 1 to 1 of 1 items

To add a user template click on the Add button in the lower right corner. The `Add User Template` dialog will be displayed.

Figure 113



Add User Template
Specify new template parameters.

USER

Template name*	Employees
Name	
Email	
Company	
Phone	

□ Groups

SETTINGS

☑ Enabled
☑ Enable ad-hoc email transfers
□ Owner
□ Expires on 05/17/2017
□ Expires after 1 min

User

Template name - The name of this template.

Name - The full name of this user.

Email - Optional email address for this user.

Company - The company that this user is associated with.

Phone - The phone number for this user. The first field is the country code (e.g. 1 for United States) and the second field is the telephone number including any area code, the third field is the phone extension. This field is used primarily in conjunction with Phone Authentication.

Groups - Optional groups that this user is a member of.

Settings

Enabled - Check to enable this account.

Enable ad-hoc email transfers - Check to allow user to perform ad-hoc email transfers via HTTP interface.

Owner - Optional login of user who owns/manages this account.

Expires on - Date that this account expires (leave blank for non-expiring account).

Expires after - Maximum number of minutes, hours, or days this account will remain active

'Expires on' and 'Expires after' can't be enabled at the same time.

Authentication

Require secured connection - Check to force user to login using secure protocol (e.g. FTPS/SFTP/HTTPS).

Use two-factor phone authentication - Check to require user to use two-factor phone authentication.

Allow password change - Check to allow user to change their password.

Ignore password aging rules - Check to disable password aging rules for this user.

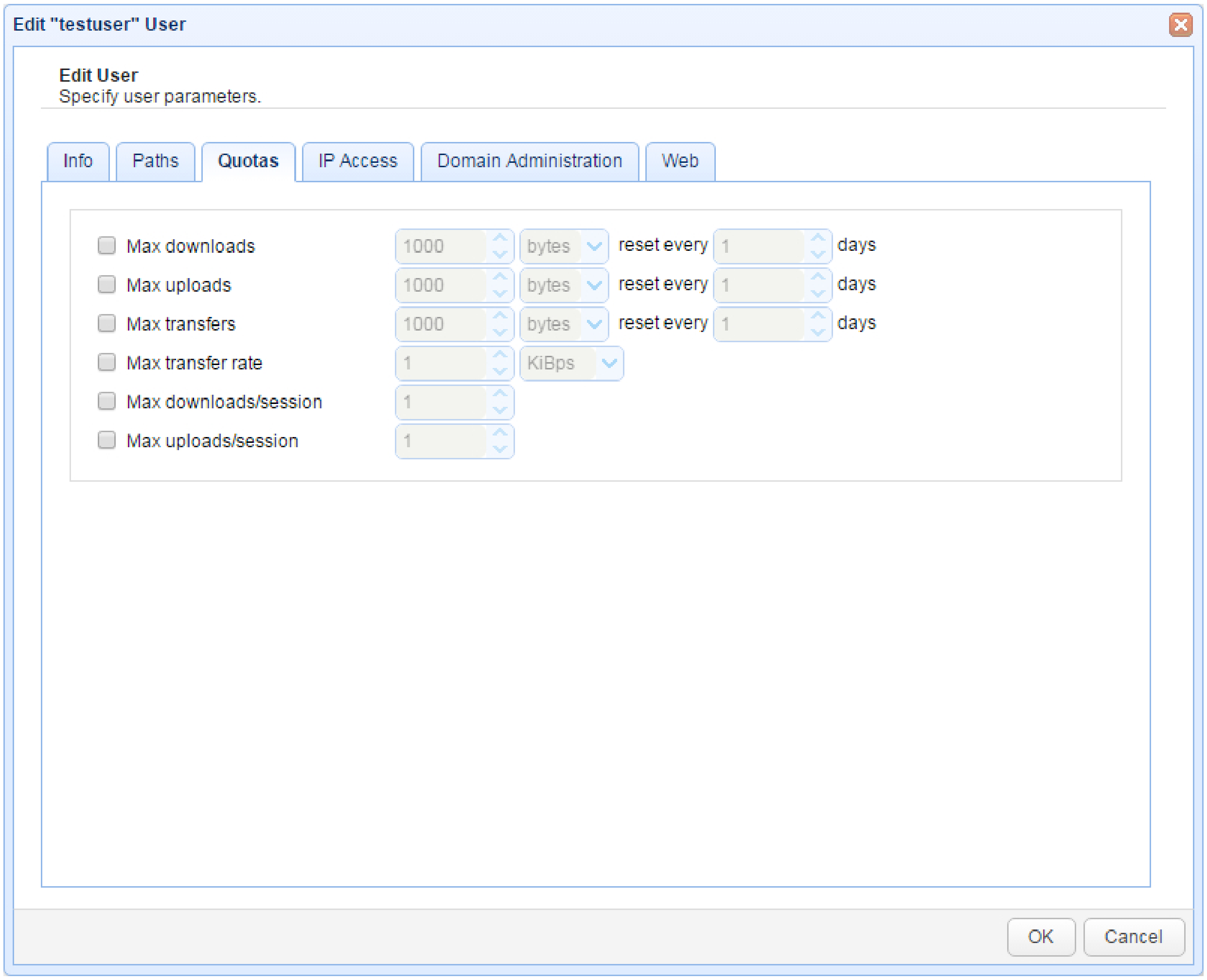
Client keys - Optional public-keys bound to this user for purposes of public-key authentication in SFTP/SSH protocol.

Defining user quotas

Although bandwidth usage can be controlled at the domain level (see Setting connection preferences), it can also be controlled at the user account level. Unlike the connection restrictions set at the domain level, which are aggregate values of all connections for a given domain regardless of protocol, restrictions set at the user account only apply to a specific user. These user-level restrictions, known as quotas, are for an aggregate of all connections of a given user regardless of protocol.

Limit at User level is soft, whereas limit at Connection level is hard. To explain, a User level limit may be exceeded IF there is a Connection level limit that is not fully utilized. This is taking into consideration the idea of a dynamic bandwidth allocation algorithm that allocates bandwidth to greedy connections that may not be used by other connections. For example, lets say you have a Connection level "Max transfer" limit of 5000 Kbps and a User level "Max transfer" limit of 500 Kbps with only 2 active user connections. The Connection limit is hard in that only 5000 Kbps may be allocated between the 2 users, however the User level limit of 500 Kbps is soft in that it may be exceeded to more efficiently use the available bandwidth.

To assign quotas for a user, go to the `Users` node for the desired domain, select the user you wish to assign quotas to, click the `Edit` button and go to the `Quotas` tab.



Edit "testuser" User

Edit User
Specify user parameters.

□ Max downloads	1000	bytes	reset every	1	days
□ Max uploads	1000	bytes	reset every	1	days
□ Max transfers	1000	bytes	reset every	1	days
□ Max transfer rate	1	KiBps			
□ Max downloads/session	1				
□ Max uploads/session	1				

Max downloads - The maximum download size for a specified number of days. Once the download quota is exceeded, no further downloads are allowed until the transfer quota is reset.

Max uploads - The maximum upload size for a specified number of days. Once the upload quota is exceeded, no further uploads are allowed until the transfer quota is reset.

Max transfers (MB) - The maximum transfer size for a specified number of days. If the transfer quota is exceeded, no further file transfers are allowed until transfer quota is reset. Transfers are the combined sum of uploads and downloads.

Max transfer rate - The maximum transfer rate for this user. This limit applies to the aggregate of all connections by this user, regardless of protocol. This quota can be set in KBps, MBps, or GBps.

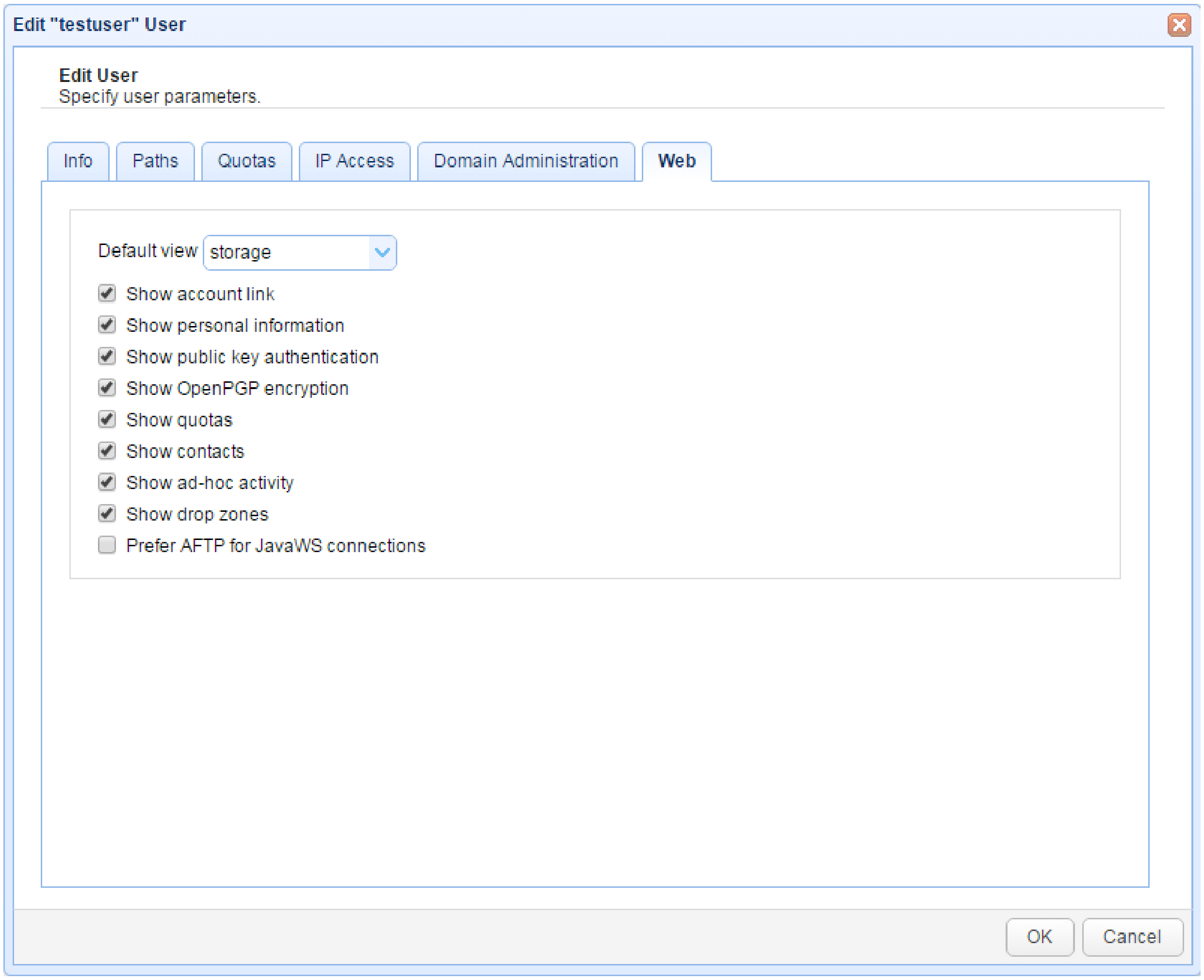
Max downloads/session - The maximum number of downloads this user is allowed per session.

Max uploads/session - The maximum number of uploads this user is allowed per session.

Specifying what the user sees in the Web UI

You may specify which section (Storage or MyAccount) the user sees upon login in the Web user interface. You may also prevent the user from viewing certain sections/items/features.

To specify what the user sees in the Web user interface, go to the `Users` node for the desired domain, select the user whose web viewing privileges you wish to customize, click the `Edit` button and go to the `Web` tab.



Edit "testuser" User

Edit User
Specify user parameters.

Default view: storage

- ☑ Show account link
- ☑ Show personal information
- ☑ Show public key authentication
- ☑ Show OpenPGP encryption
- ☑ Show quotas
- ☑ Show contacts
- ☑ Show ad-hoc activity
- ☑ Show drop zones
- ☐ Prefer AFTP for JavaWS connections

Default view (`Storage` or `MyAccount`) - Sets what the user sees upon login in the web user interface.

Show account link - Shows/hides the My Account link

Show personal information - Shows/hides the `Personal Information` module in the `My Account` page. If this is unchecked, the user will only be able to change his/her password via the "`Reset password`" link on the main login page and only if the "`Allow password change`" option is enabled for this user.

Show public key authentication - Shows/hides the `Public Key Authentication` module in the `My Account` page.

Show OpenPGP encryption - Shows/hides the `OpenPGP Encryption` module in the `My Account` page.

Show quotas - Shows/hides the `Quotas` module in the `My Account` page.

Show contacts - Shows/hides the `Contacts` module in the `My Account` page.

Show ad-hoc activity - Shows/hides the `Ad-Hoc Activity` module in the `My Account` page.

Show drop zones - Shows/hides the `Drop Zones` module in the `My Account` page.

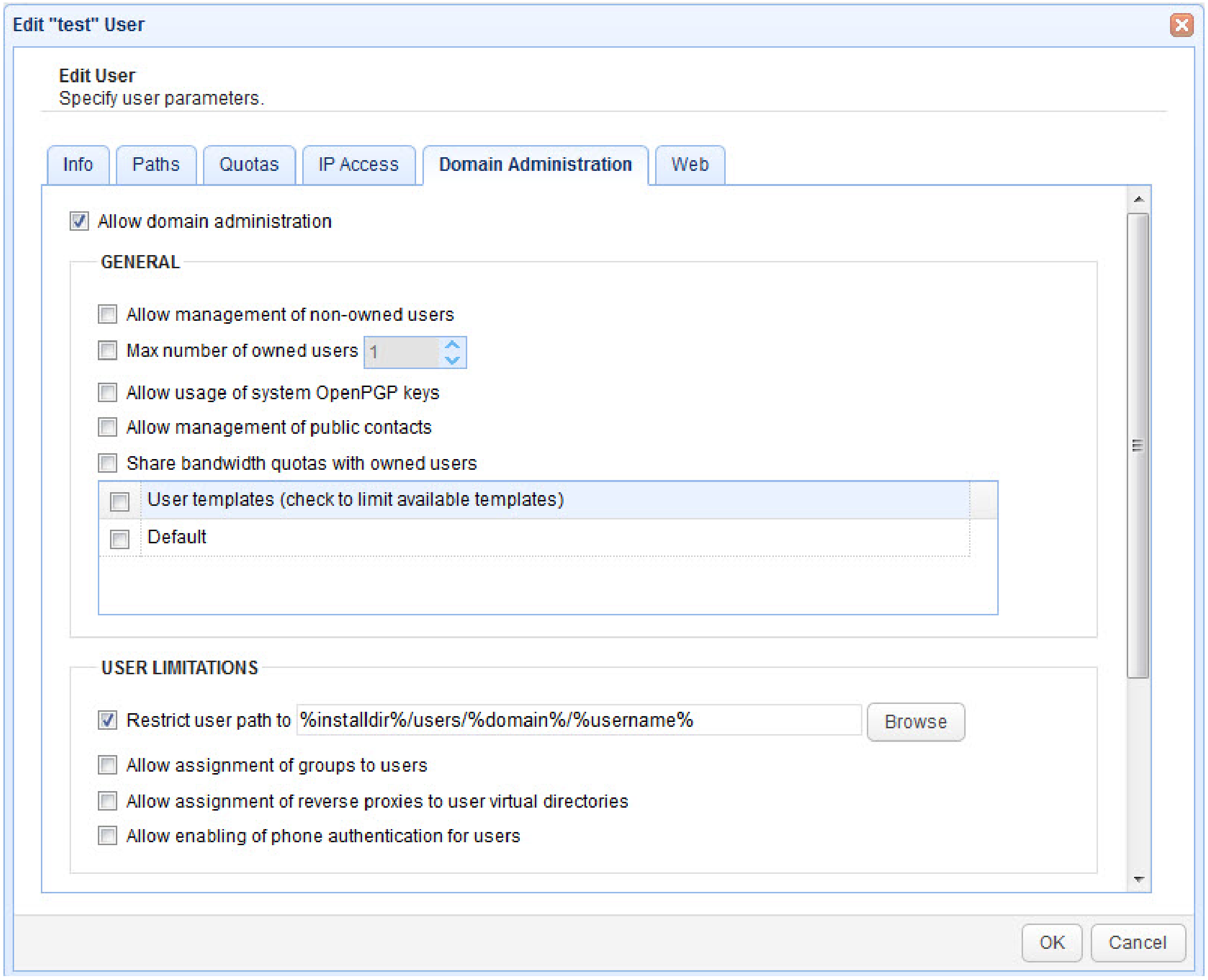
Prefer AFTP for JavaWS connections - If the AFTP protocol is enabled in the domain the user belongs to, the user will be automatically connected to JSCAPE MFT Server via the AFTP protocol when logging into the web user interface via the JavaWS.

Assigning domain administrators

A domain administrator can manage and create users using **limited** account management features available found in the user web interface. For more extensive administrative features consider creating an administrative account with an optional role to limit administrative capabilities.

To assign domain administration privileges for a user go to the `Users` node for the desired domain, select the user you wish to assign domain administration rights to, click the `Edit` button and go to the `Domain Administration` tab.

Figure 114



Edit "test" User

Edit User
Specify user parameters.

☑ Allow domain administration

GENERAL

□ Allow management of non-owned users

□ Max number of owned users 1

□ Allow usage of system OpenPGP keys

□ Allow management of public contacts

□ Share bandwidth quotas with owned users

□	User templates (check to limit available templates)
□	Default

USER LIMITATIONS

☑ Restrict user path to %installdir%/users/%domain%/%username%

□ Allow assignment of groups to users

□ Allow assignment of reverse proxies to user virtual directories

□ Allow enabling of phone authentication for users

Allow domain administration - Enables/disables if user is a domain administrator.

General

Allow management of non-owned users - If checked then user can manage any accounts for the domain. Otherwise user can only manage accounts that are "owned" by this user.

Max number of owned users - The maximum number of users this user may create/own.

Allow usage of system OpenPGP keys - If enabled user will be able to view OpenPGP keys created in `Key Manager`.

Allow management of public contacts - If enabled user will be able to create/manage public contacts visible by all users for the domain.

Share bandwidth quotas with owned users - If checked then all owned users bandwidth rolls up to domain administrator user bandwidth quota where the sum of owned user bandwidth may not exceed that of the domain administrator bandwidth quota.

User templates - The templates that domain administrator may use when creating a user.

User Limitations

Restrict user paths to - If checked then user can only create virtual directories with the specified path or below.

Allow assignment of groups to users - If checked user can assign a user to a group.

Allow assignment of reverse proxies to user virtual directories - If checked user can map virtual directories to a reverse proxy.

Allow enabling of phone authentication for users - If checked then user can enable/disable the `Use phone authentication` option for users.

Drop Zones / URL Branding

Allow management of drop zones - If enabled then user can create drop zones.

Allow management of URL brandings - If checked then user can create URL branding links.

Max number of drop zones - The maximum number of drop zones that user can create.

Max number of URL brandings - The maximum number of URL branding links that user can create.

See also

Web user interface
Managing administrators
Managing administrative roles

Setting authentication preferences

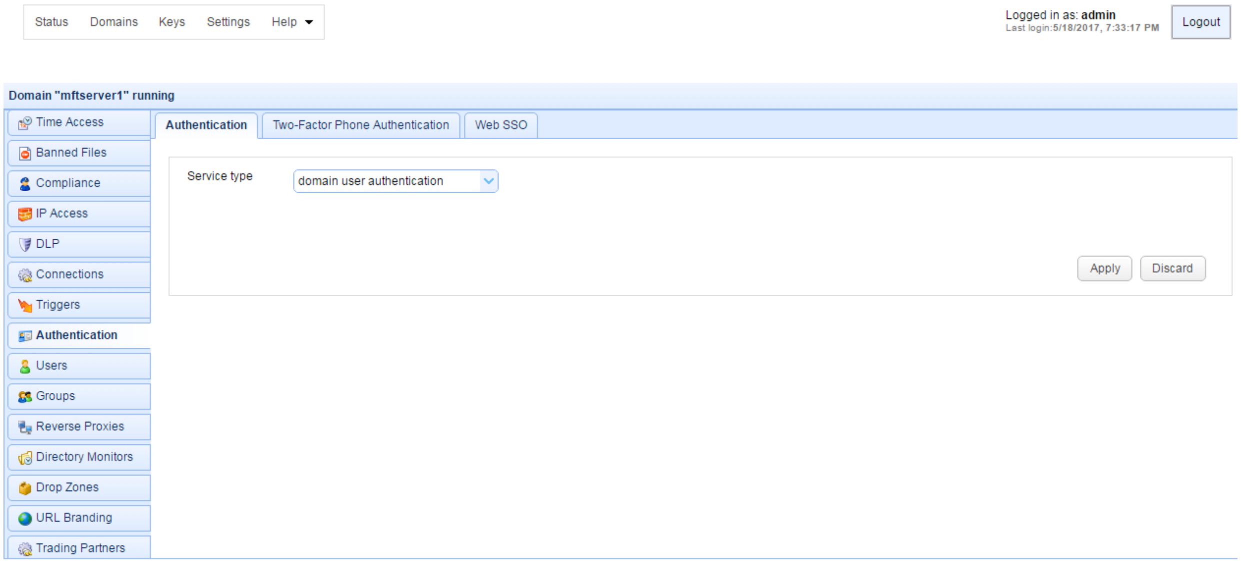
Users may authenticate with JSCAPE MFT Server using a variety of different authentication protocols. To view the current authentication method used click on the `Authentication` node for the desired domain.

Domain User Authentication
Database Authentication
Database Query Authentication
LDAP Authentication
LDAP Query Authentication
LDAP Filter Grammar
NTLM Authentication
PAM Authentication
RADIUS Authentication
Custom Authentication
Multiple Authentication
Password Hashing
Phone Authentication
Web SSO

Domain User Authentication

`Domain User Authentication` is the most basic form of authentication, authenticating against local user accounts created for the domain using JSCAPE MFT Server Manager.

Figure 58

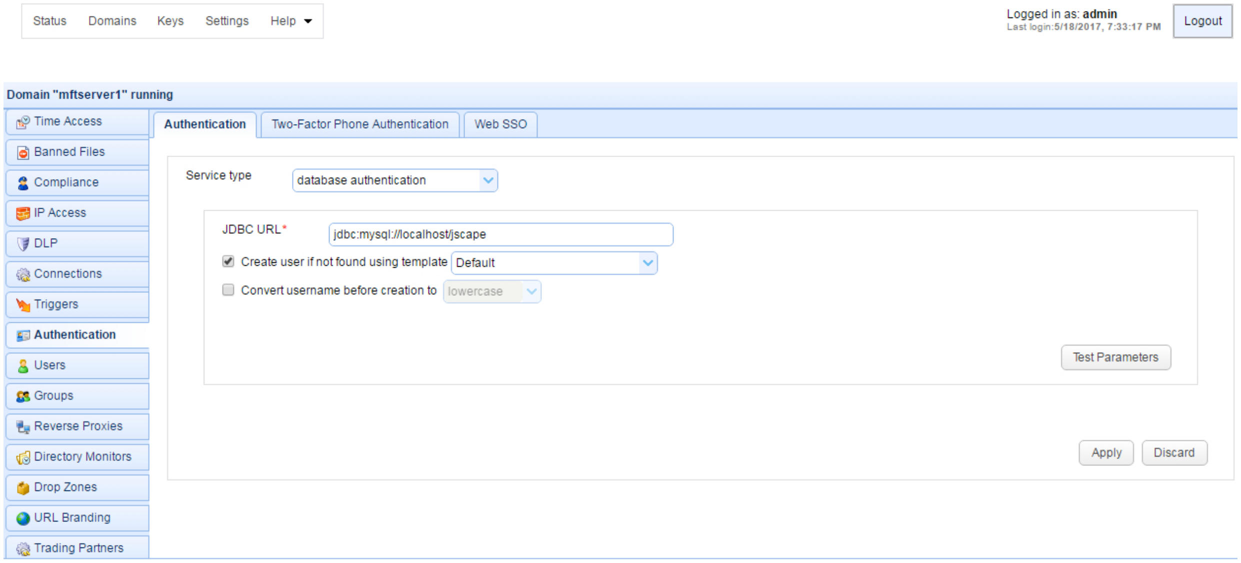


Service type: domain user authentication

Database Authentication

`Database Authentication` allows you to authenticate a user based on whether the user has credentials to connect to a database. When connecting to the supplied JDBC URL the username and password provided at time of login are used to login to the JDBC URL. If user authenticates successfully with the JDBC URL then user is considered a valid user of the JSCAPE MFT Server service.

Figure 59



Service type: database authentication

JDBC URL*: jdbc:mysql://localhost/jscape

☑ Create user if not found using template: Default

□ Convert username before creation to: lowercase

JDBC URL - The JDBC URL used to connect to the database. Libraries for JDBC drivers must be placed in the `libs/jdbc` directory of your JSCAPE MFT Server installation, the JSCAPE MFT Server Service restarted and the JDBC driver class registered in `Settings > JDBC Drivers` in order for the database to be accessible to JSCAPE MFT Server.

Create user if not found using template - This allows for accounts to be created automatically upon

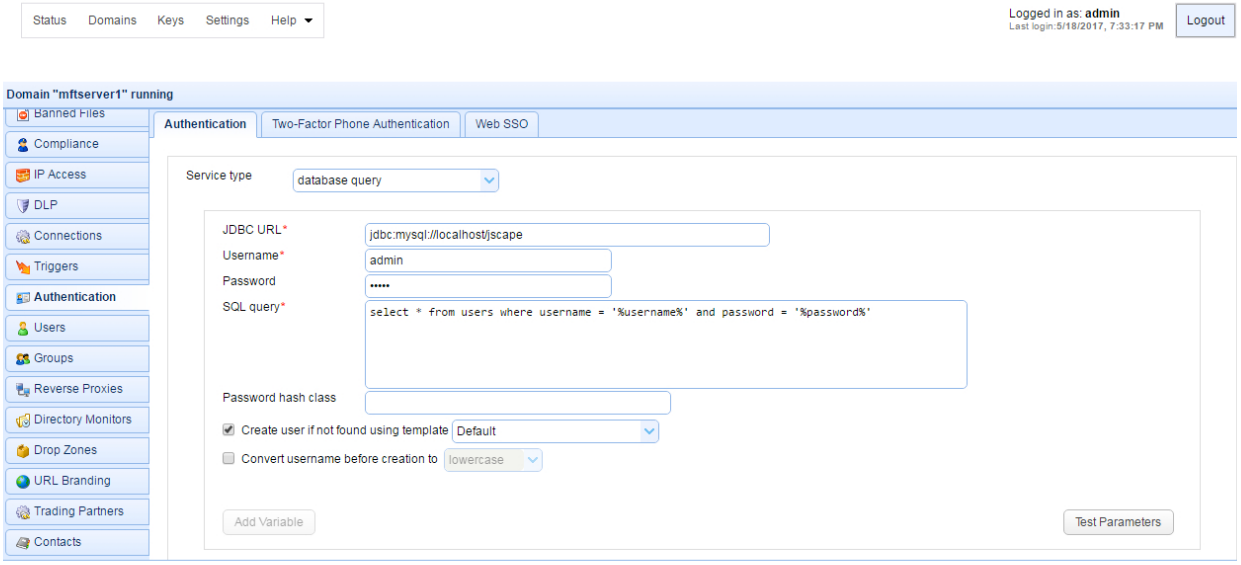
successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

Database Query Authentication

`Database Query Authentication` allows you to authenticate a user based on the results of a database query. If one or more records are returned from the query then the user is successfully authenticated.

Figure 60



Service type: database query

JDBC URL*: jdbc:mysql://localhost/jscape

Username*: admin

Password: •••••

SQL query*:

```
select * from users where username = '%username%' and password = '%password%'
```

Password hash class:

☑ Create user if not found using template: Default

☐ Convert username before creation to: lowercase

JDBC URL - The JDBC URL used to connect to the database.   Libraries for JDBC drivers must be placed in the `libs/jdbc` directory of your JSCAPE MFT Server installation, the JSCAPE MFT Server Service restarted and the JDBC driver class registered in `Settings > JDBC Drivers` in order for the database to be accessible to JSCAPE MFT Server

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

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

SQL query - The query to perform to authenticate the user.   There are two special variables that may be used when performing the database query `%username%` and `%password%` which refer the username and password passed in during the authentication process. Note, SQL queries and stored procedures may be used, however stored procedures which make use of output parameters **may not** be used. The variables `%username%` and `%password%` are treated as strings so **must** be enclosed in single quotes.

Hash password class - The Java class to use for hashing password before passing to `SQL query`. If no class is specified then password will be passed to `SQL query` in clear text.

Create user if not found using template - This allows for accounts to be created automatically upon

successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

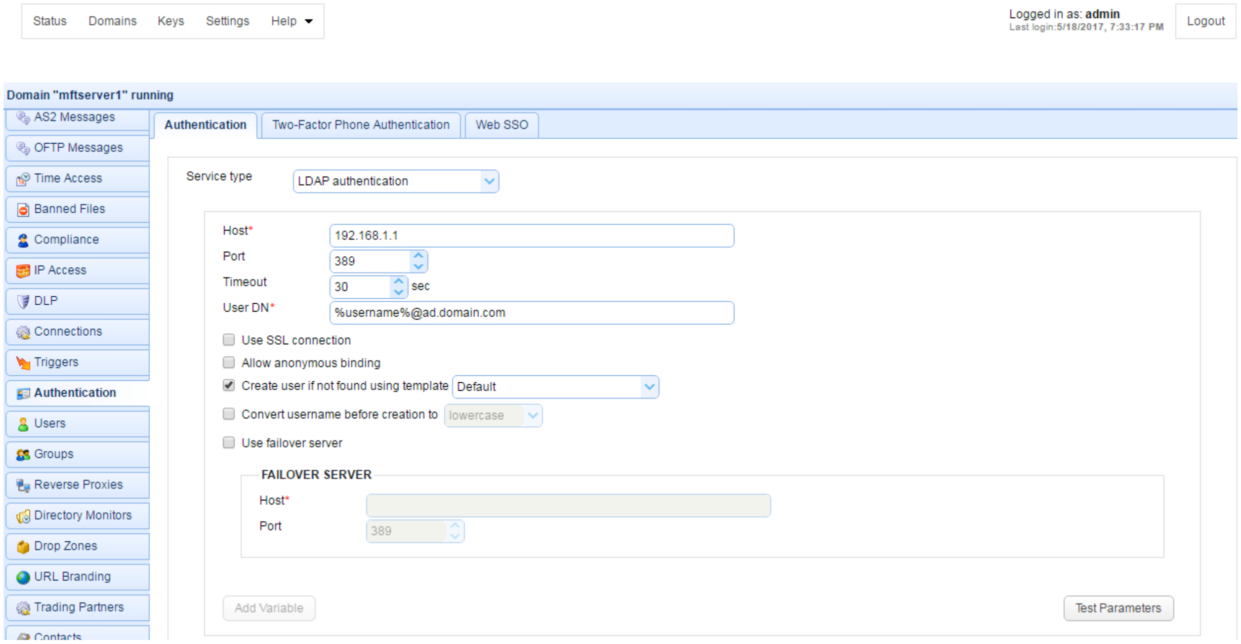
See also

Password Hashing

LDAP Authentication

`LDAP User Authentication` allows you to authenticate a user based on whether the user has the credentials to connect to the LDAP or Active Directory service.

Figure 61



Service type: LDAP authentication

Host*: 192.168.1.1

Port: 389

Timeout: 30 sec

User DN*: %username%@ad.domain.com

☐ Use SSL connection

☐ Allow anonymous binding

☑ Create user if not found using template: Default

☐ Convert username before creation to: lowercase

☐ Use failover server

FAILOVER SERVER

Host*:

Port: 389

Host - The hostname or IP address of the LDAP service.

Port - The port of the LDAP service.

Timeout - The connection timeout when connecting to LDAP service.

User DN - The users distinguished name for authenticating with the LDAP service. The variable `%username%` may be used which refers to the username passed in during the authentication process.

Use SSL connection - Connect to LDAP server using SSL connection.

Allow anonymous binding - Sets whether user can bind anonymously to LDAP directory.

Create account if not found using template - This allows for accounts to be created automatically upon

successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

Use failover server - If enabled and primary LDAP server is inaccessible then authentication will be attempted against failover server.

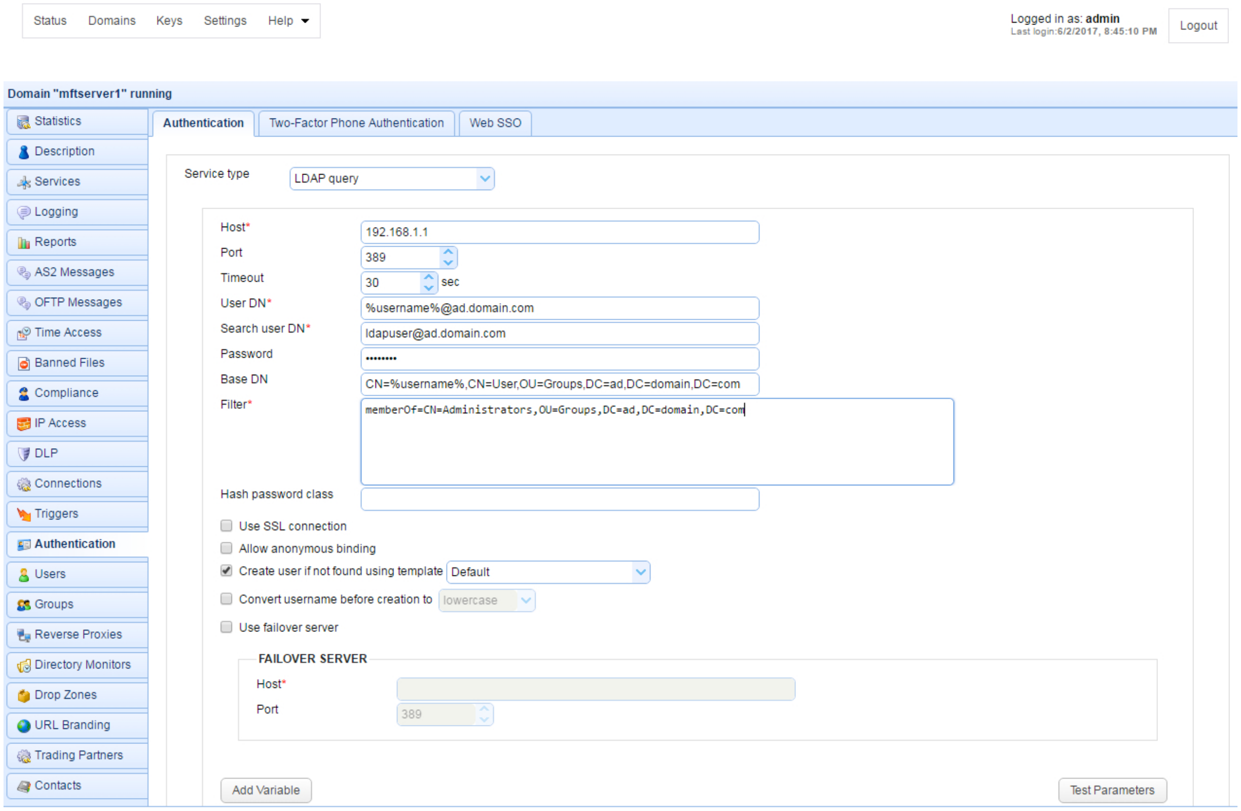
LDAP Query Authentication

`LDAP Query Authentication` allows you to authenticate a user based on the results of a LDAP query and is a two step authentication process.

1. User is authenticated against LDAP server using the `User DN` field and the password supplied by user when authenticating against JSCAPE MFT Server file transfer service.
2. Query is performed using credentials supplied in `Search user DN` and `Password` fields. Note, these credentials **may** be different than the credentials used in Step 1. For example, a case where these might be different is where the `User DN` does not have the needed permissions to perform the query but the `Search User DN` does.

If one or more records are returned from the query then the user is successfully authenticated.

Figure 62



Domain "mftserver1" running

Service type: LDAP query

Host*: 192.168.1.1
Port: 389
Timeout: 30 sec
User DN*: %username%@ad.domain.com
Search user DN*: ldapuser@ad.domain.com
Password: ••••••••
Base DN: CN=%username%,CN=User,OU=Groups,DC=ad,DC=domain,DC=com
Filter*: memberOf=CN=Administrators,OU=Groups,DC=ad,DC=domain,DC=com
Hash password class:

☐ Use SSL connection
☐ Allow anonymous binding
☑ Create user if not found using template: Default
☐ Convert username before creation to: lowercase
☐ Use failover server

FAILOVER SERVER
Host*:
Port: 389

Host - The hostname or IP address of the LDAP service.

Port - The port of the LDAP service.

Timeout - The connection timeout when connecting to LDAP service.

User DN - The users distinguished name for authenticating with the LDAP service.

Search user DN - The user distinguished name used for performing LDAP search query.

Password - The user password for performing LDAP search query.

Base DN - The base distinguished name in which to perform the filter.

Filter - The filter to execute using the LDAP filter syntax. There are two special variables that may be used when performing the database query, `%username%` and `%password%` which refer the username and password supplied by the user during the authentication process.

Hash password class - The Java class to use for hashing password before passing to filter. If no class is specified then password will be passed to `Filter` in clear text.

Use SSL connection - Connect to LDAP server using SSL connection.

Allow anonymous binding - Sets whether user can bind anonymously to LDAP directory.

Create user if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

Use failover server - If enabled and primary LDAP server is inaccessible then authentication will be attempted against failover server.

See also

Password Hashing

LDAP Filter Grammar

When using `LDAP Query Authentication` you must define a filter that will be used to identify the record you are searching for. The syntax of LDAP filters are defined in RFC 2254. The table below provides a list of valid expressions and their meanings.

Symbol	Filter	Example	Example matches
=	Equality	(sn=Smith)	Surname of Smith only.
>	Greater than	(sn>Smith)	Any surname that alphabetically follows Smith.
>=	Greater than or equal to	(sn>=Smith)	Any surname that includes or

			alphabetically follows Smith.
<	Less than	(sn<Smith)	Any surname that alphabetically precedes Smith.
<=	Less than or equal to	(sn<=Smith)	Any surname that includes or alphabetically precedes Smith.
=*	Presence	(sn=*)	All surnames (all entries with the sn attribute).
=*	Substring	(sn=Smi*)	Any matching substring of Smith.
&	And	(& (sn=Smith) (cn=John))	Surname of Smith and common name of John.
|	Or	(| (sn=Smith) (sn=Jones))	Surname of Smith or Jones.
!	Not	(! (sn=Smith))	Surname not equal to Smith.

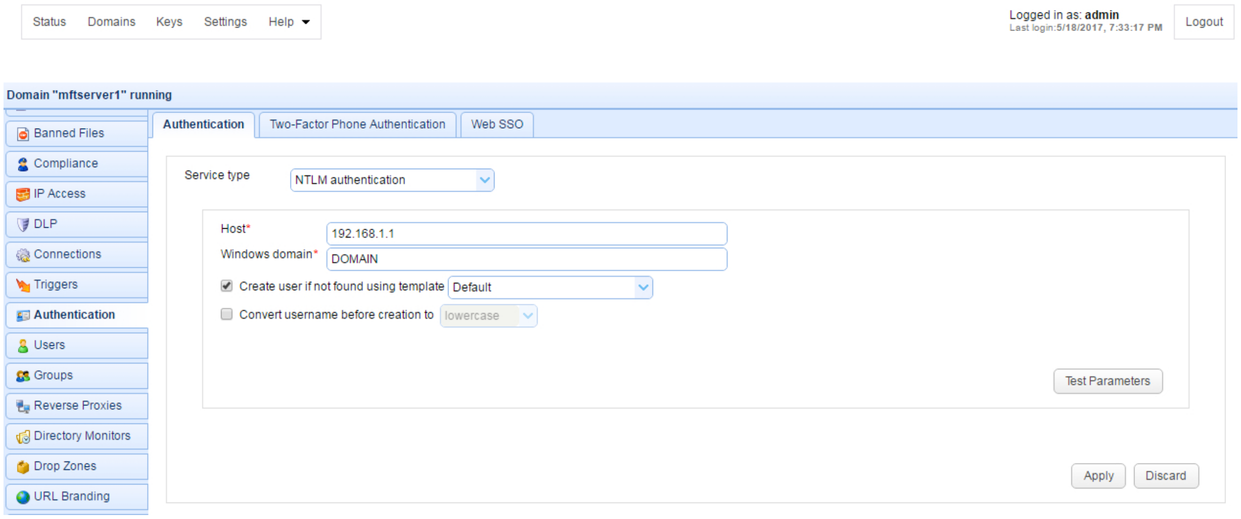
See also

[Authenticating with Microsoft Active Directory]

NTLM Authentication

Using `NTLM Authentication` you may authenticate against an existing Windows domain.

Figure 118



Logged in as: admin
Last login:5/18/2017, 7:33:17 PM

Domain "mftserver1" running

Service type: NTLM authentication

Host*: 192.168.1.1

Windows domain*: DOMAIN

☑ Create user if not found using template: Default

☐ Convert username before creation to: lowercase

Host - The IP address of Windows domain controller.

Windows domain - The name of the Windows domain to which users belong.

Create account if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

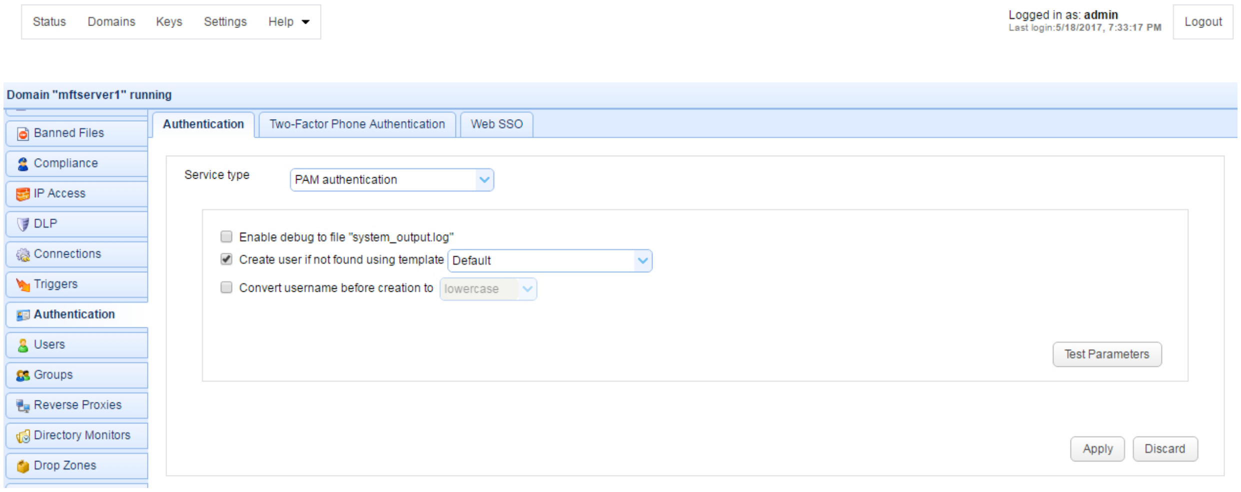
Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

PAM Authentication

Using `PAM Authentication` you may authenticate against an existing UNIX PAM user repository. In order to use the PAM Authentication module you must install some native libraries that allow JSCAPE MFT Server to communicate with your PAM user repository.

1. Download the JPam library for your operating system.
2. Copy the native library to the Java Native Libary Path. See the Native Library Installation Location table for details. Note, Step 1 in the JPam instructions should be ignored as the `jpam.jar` file already exists in the `libs` directory of your JSCAPE MFT Server installation. Additionally, JPam instructions state you may optionally place native library in same directory as the `jpam.jar` file instead of the Java Native Library Path. This is incorrect. For JPam to work with JSCAPE MFT Server you **must** place native library in the Java Native Library Path and **not** in the `libs` directory of JSCAPE MFT Server.
3. Configure JPam for use by editing the `net-sf-jpam` file and copying it to to `/etc/pam.d` directory.
4. Restart JSCAPE MFT Server Service.
5. Using JSCAPE MFT Server Manager go to the `Authentication` node and set the `Service type` to `PAM authentication` and enable other options. See Figure 117.
6. Click `Test Parameters` button to test.

Figure 117



Logged in as: admin
Last login:5/18/2017, 7:33:17 PM

Domain "mftserver1" running

Service type: PAM authentication

□ Enable debug to file "system_output.log"
☑ Create user if not found using template: Default
□ Convert username before creation to: lowercase

Enable debug to file system_output.log - Sends debugging information to file `system_output.log` in installation directory.

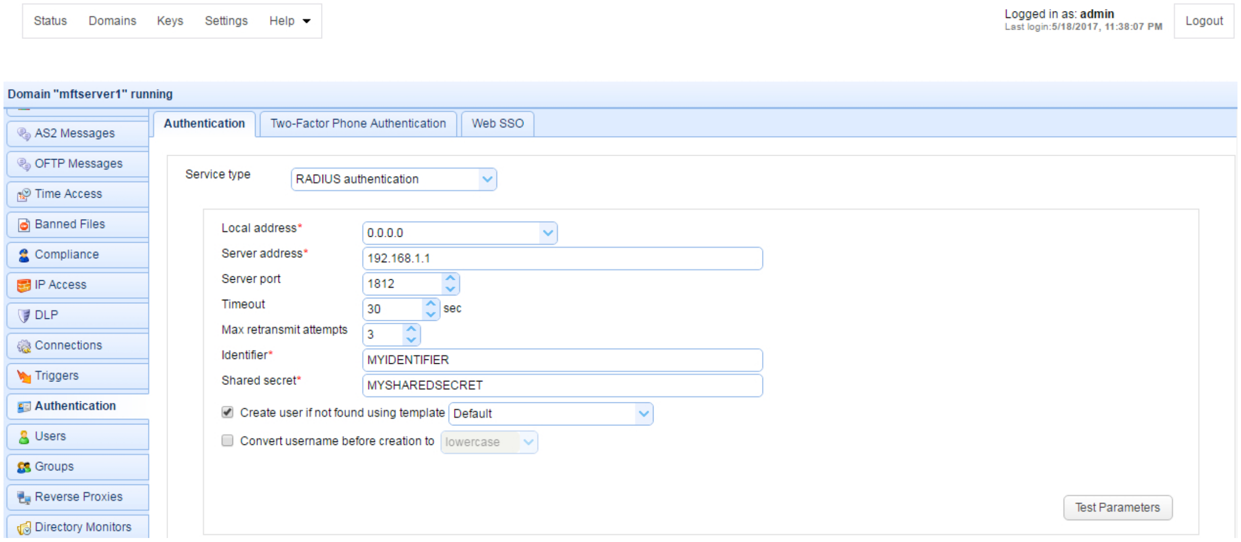
Create user if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

RADIUS Authentication

Using `RADIUS authentication` you may authenticate against an existing RADIUS server.

Figure 208



Service type: RADIUS authentication

Local address*: 0.0.0.0

Server address*: 192.168.1.1

Server port: 1812

Timeout: 30 sec

Max retransmit attempts: 3

Identifier*: MYIDENTIFIER

Shared secret*: MYSHAREDSECRET

☑ Create user if not found using template: Default

☐ Convert username before creation to: lowercase

Local address - The local UDP address for socket binding.

Server address - The server address of RADIUS server.

Server port - The server port of RADIUS server.

Timeout - The timeout in seconds for connecting to RADIUS server.

Max retransmit attempts - The maximum number of retransmission attempts when there is no response from the RADIUS server

Identifier - The identifier value of the RADIUS server.

Shared secret - The shared secret value of the RADIUS server.

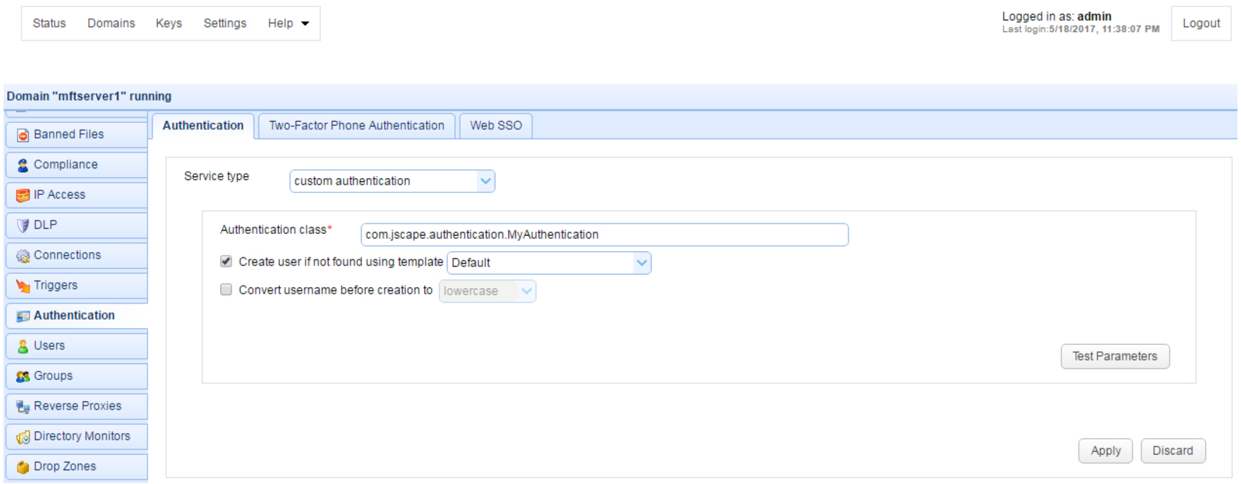
Create account if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

Custom Authentication

Using `custom authentication` you may define your own custom authentication class.

Figure 86



Logged in as: admin
Last login:5/18/2017, 11:38:07 PM

Domain "mftserver1" running

Service type: custom authentication

Authentication class*: com.jscape.authentication.MyAuthentication

☑ Create user if not found using template: Default

☐ Convert username before creation to: lowercase

Authentication class - The custom authentication class name.

Create user if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

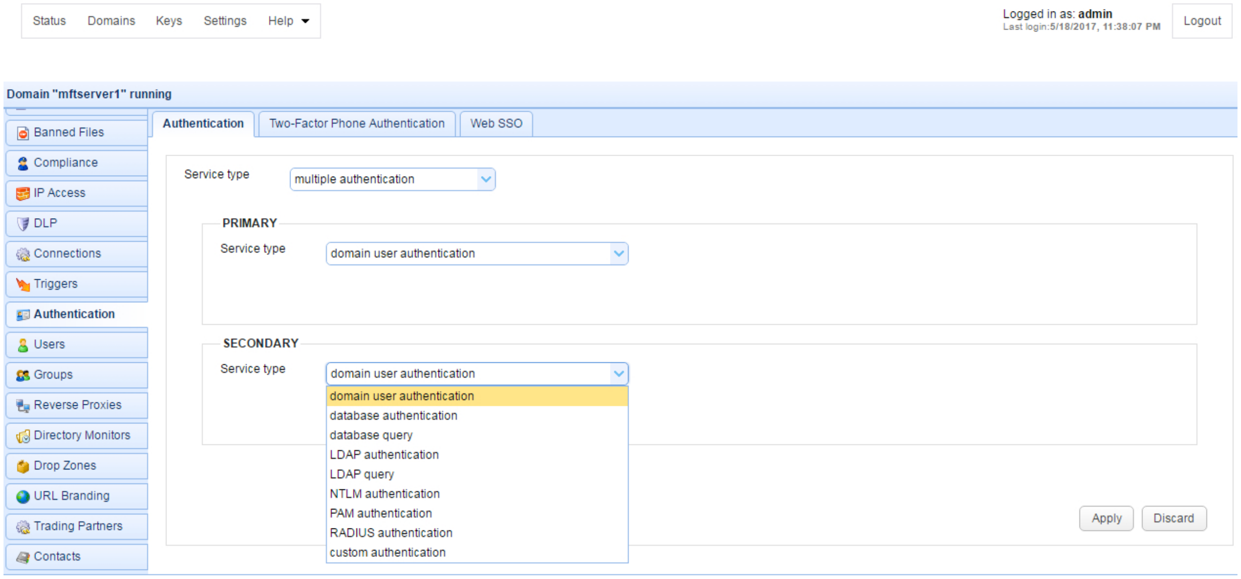
See also

Authenticating using custom authentication API

Multiple Authentication

`Multiple authentication` enables you to authenticate users using multiple authentication service types. One example use case is when you have some internal users who need to be authenticated using `LDAP authentication` and some external users who need to be authenticated using `domain user authentication`.

Figure 235



Domain "mftserver1" running

Service type: multiple authentication

PRIMARY

Service type: domain user authentication

SECONDARY

Service type: domain user authentication

- domain user authentication
- database authentication
- database query
- LDAP authentication
- LDAP query
- NTLM authentication
- PAM authentication
- RADIUS authentication
- custom authentication

Note Multiple authentication is NOT 2-factor authentication or multi-factor authentication.

When you choose `Multiple Authentication`, you need to define a `Primary` and `Secondary` authentication type. The configuration details of each service type are the same as those described above.

When authenticating, the user is first authenticated against the `Primary` service. If the authentication is successful, the user is granted access. If the authentication fails, a second authentication attempt is made against the `Secondary` service. If the second authentication also fails, then the user is denied access; otherwise, access is granted.

Note For purposes of IP blocking/banning and raising of User Login event, this should only happen either after successful login OR after both Primary and Secondary authentication methods have been attempted.

Password Hashing

The `Database Query Authentication` and `LDAP Query Authentication` services both support optional password hashing. Many databases and LDAP repositories store passwords in a hashed format. This is a security measure used in order to protect user credentials should a database or LDAP repository be compromised. JSCAPE MFT Server includes some built-in classes that may be used for hashing a password before it is sent for authentication against a database or LDAP repository. These classes are `com.jscape.inet.mft.authentication.MD5Hasher` and `com.jscape.inet.mft.authentication.SHA1Hasher` which offer MD5 and SHA1 hashes respectively. Note, the hashes provided by the `MD5Hasher` and `SHA1Hasher` classes are provided in lowercase format.

Some databases or LDAP repositories may store passwords in a salted hash format. In a salted hash format the password is combined with other data (the salt) prior to being hashed. Salted hash passwords are typically used in an effort to avoid brute-force password attacks should the database or LDAP repository be compromised. Password salting is generally application dependent, therefore should you need to use a salted password it is necessary to write your own password hasher using the JSCAPE MFT Server API. To implement your own password hashing provider you must perform the following:

1. Create a Java class which implements the `com.jscape.inet.mft.authentication.Hasher` class.

2. Overload the `public String createHash(String login, String password)` method, returning the hashed value.

3. Create a JAR file that contains the compiled version of your `com.jscape.inet.mft.authentication.Hasher` implementation. To compile your authentication class you will need to include the `ftpserver.jar` library in your classpath. The `ftpserver.jar` library may be found in the `libs` directory for JSCAPE MFT Server.

4. Place the JAR file created in step 3 into the `libs` directory of your JSCAPE MFT Server installation.

5. Shutdown any open instances of JSCAPE MFT Server Manager and restart the JSCAPE MFT Server Service.

6. In the `Hash password class` field of the `Database Query Authentication` or `LDAP Query Authentication` service enter the full classname, including package name of your hash provider.

Phone Authentication

The `Phone Authentication` module in JSCAPE MFT Server provides tokenless two-factor authentication support for your user accounts. This is a very secure method of authenticating users in that it combines something users know (their username/password) with something they have (a telephone or cellphone). Using the `Phone Authentication` module ensures that even if a user's password is stolen their account cannot be compromised.

How it works

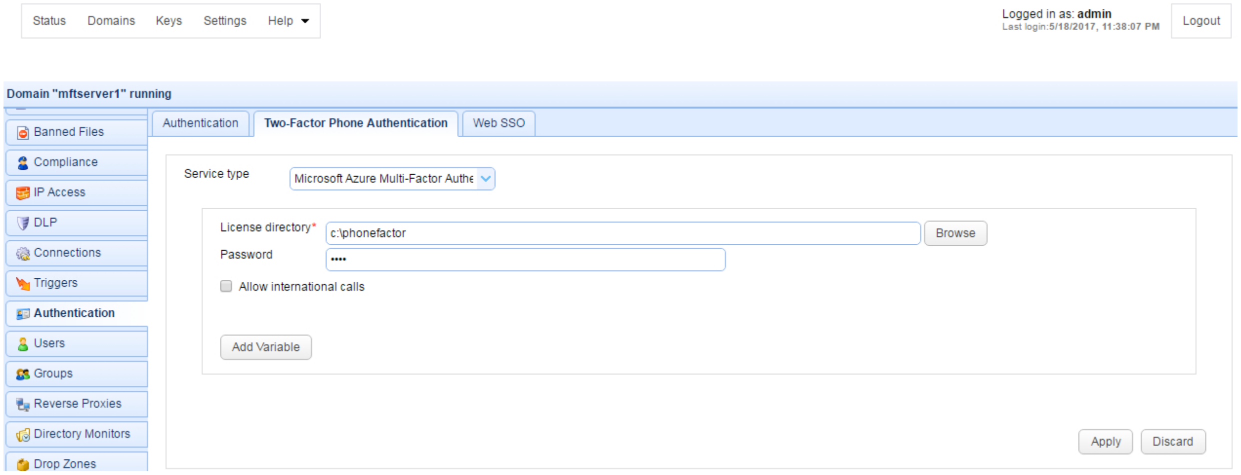
1. User authenticates with JSCAPE MFT Server service as normal.
2. User instantly receives a phone call from `Two-Factor Authentication` service asking user to confirm this is a valid login.
3. Upon confirmation, user is logged into their account.

Enabling Phone Authentication

1. Select the `Two-Factor Authentication` tab and the `Service type` you wish to use.
2. Enter details for service and click `Apply`.
3. Enable the `Use phone authentication` option for those user accounts that you want to use this service.

Microsoft Azure Multi-Factor Authentication (a.k.a PhoneFactor) is a multi-factor authentication service provided by Microsoft. To use this service you must first create an Azure account and Download Azure Multi-Factor Authentication SDK for Java. Upon downloading the SDK, extract the ZIP archive and copy the files `license.xml` and `cert.p12` to the `License directory`. See Figure 119.

Figure 119



Logged in as: admin
Last login:5/18/2017, 11:38:07 PM

Domain "mftserver1" running

Service type: Microsoft Azure Multi-Factor Authe

License directory*: c:\phonefactor

Password: ••••

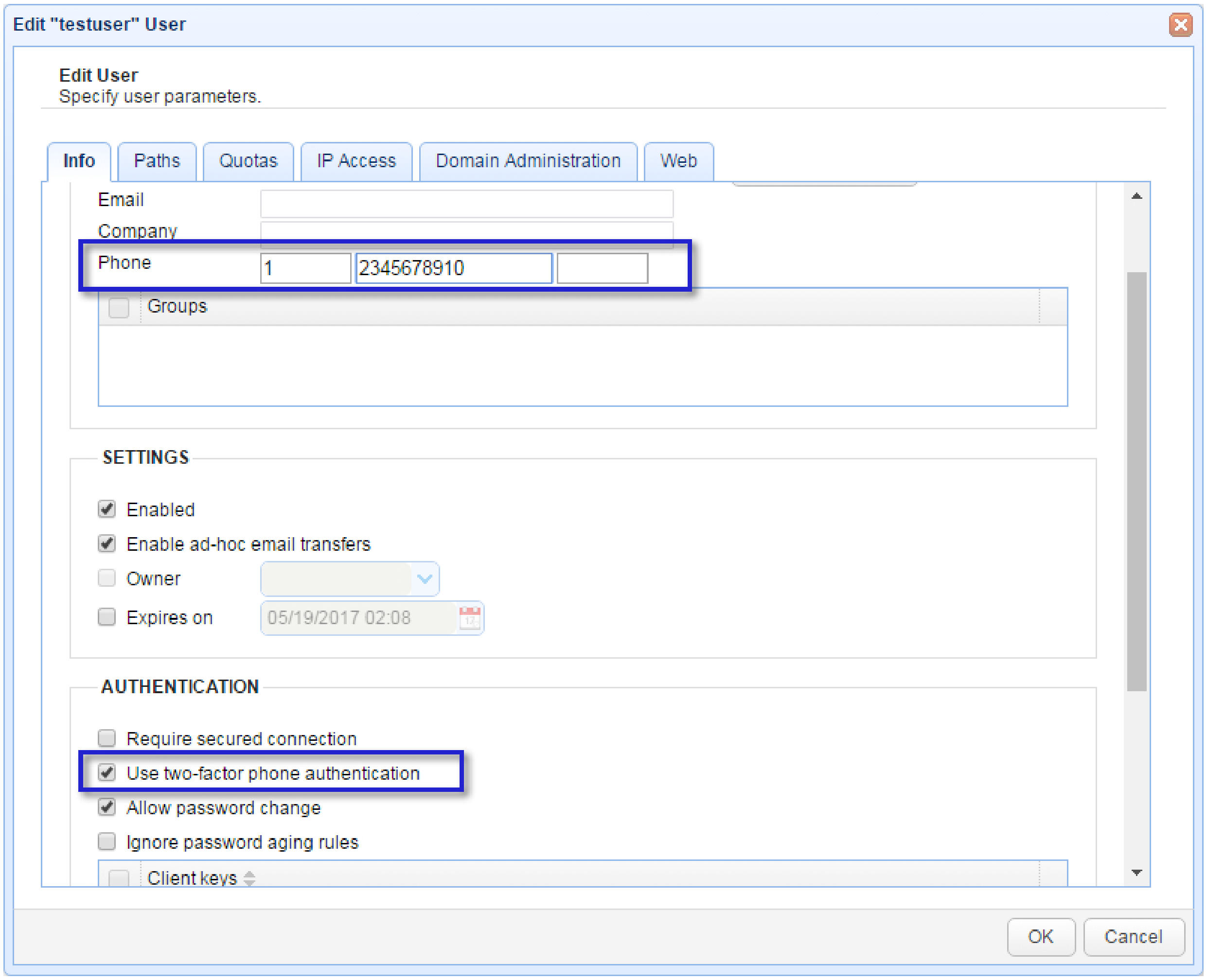
☐ Allow international calls

License directory - The directory containing your Microsoft Azure Multi-Factor Authentication SDK license and private key files.

Password - Your Microsoft Azure Multi-Factor Authentication account password. This password can be found in the private-key-password.txt file that was provided as part of the Microsoft Azure Multi-Factor Authentication download.

Allow international calls - If checked fee based calls may be made to areas outside of the free Global Services locations defined by Microsoft Azure Multi-Factor Authentication.

Figure 120



Edit "testuser" User

Edit User
Specify user parameters.

Email
Company
Phone 1 2345678910

□ Groups

SETTINGS

☑ Enabled
☑ Enable ad-hoc email transfers
□ Owner
□ Expires on 05/19/2017 02:08

AUTHENTICATION

□ Require secured connection
☑ Use two-factor phone authentication
☑ Allow password change
□ Ignore password aging rules
□ Client keys

Note

Make sure that you enter the country code and phone number (including any area code) in the Phone field for your users using this service. The first field is your country code (1 for the United States), the second field is your phone number (including any area code), the third field is an optional extension. It is important that you **do not** include any non-numeric values in your phone number (e.g. hyphens, parenthesis etc.). This will be the number that is called when performing phone authentication.

Web SSO

SSO (Single-Sign-On) is a method by which users can login to one service (identity provider) and automatically be granted access to other services (service provider) without the need to login separately to these other services. An example of this would be logging into Google Apps and automatically be granted access to your JSCAPE MFT Server account without the need for a separate login. In the example screenshot below (Figure 171) Google Apps would serve as the identity provider and your JSCAPE MFT Server instance as the service provider. JSCAPE MFT Server provides support for web based SSO using SAML, OpenID and OpenID Connect compliant identity providers. Please consult the documentation of your identity provider for details on how to enable/configure SSO.

Login URL

To perform a web SSO login use the following URL format:

```
https://[hostname]/sso/[domainname]/login
```

For example, if your hostname is `1.2.3.4` and your domain is `mydomain` this URL would look as follows:

```
https://1.2.3.4/sso/mydomain/login
```

If you have already authenticated with your identity provider then you will be automatically logged into JSCAPE MFT Server. If not, then you will be redirected to the Sign-in URL for your identity provider. After authenticating with your identity provider you will be automatically logged into JSCAPE MFT Server.

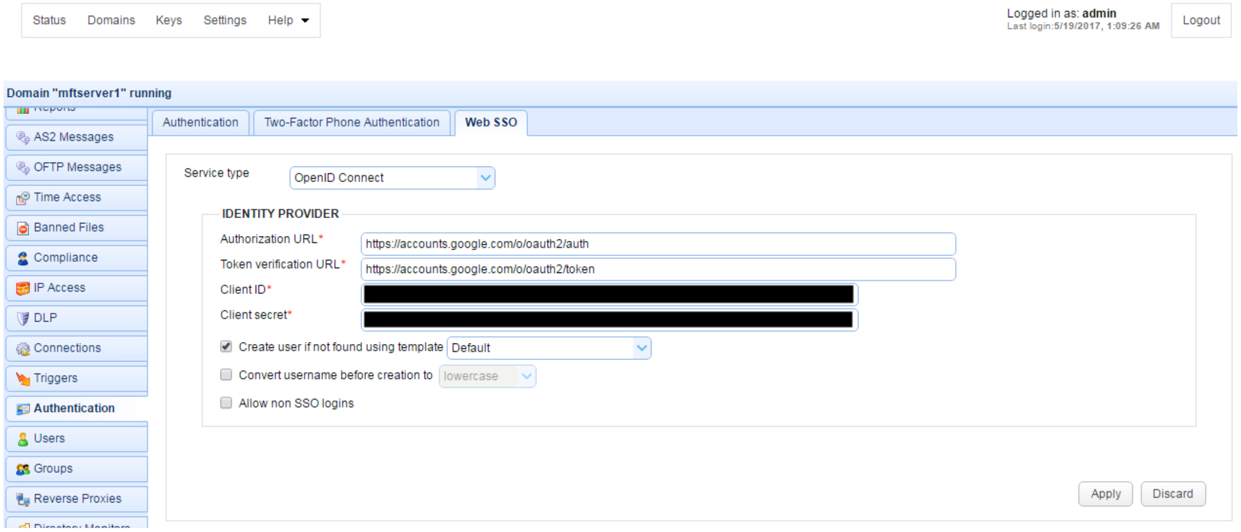
Note

SSO applies only to web based sessions. Other protocols (FTP/S, SFTP, WebDAV, AFTP etc.) will authenticate users using the defined authentication service for the domain.

OpenID Connect Example (Google Identity Platform)

The example provided below is for connecting with the Google Identity Platform. Sensitive information has been masked in the screenshot below.

Figure 171



Logged in as: **admin**
Last login:5/19/2017, 1:09:26 AM

Domain "mftserver1" running

Service type: OpenID Connect

IDENTITY PROVIDER

Authorization URL*: https://accounts.google.com/o/oauth2/auth
Token verification URL*: https://accounts.google.com/o/oauth2/token
Client ID*: [redacted]
Client secret*: [redacted]

☑ Create user if not found using template: Default
□ Convert username before creation to: lowercase
□ Allow non SSO logins

Authorization URL - The URL used for signing into the identity provider.

Token verification URL - The URL for verifying tokens.

Client ID - Your client ID for connecting with identity provider.

Client secret - Your client secret for connecting with identity provider.

Create user if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template. The `Name` and `Login` properties for the account created will automatically be set to the `openid.identity` attribute value.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

Allow non SSO logins - If enabled, user may login using either SSO or other authentication service

Authenticating with Microsoft Active Directory

Microsoft Active Directory is an LDAP service that may be used by external applications to authenticate users against a Microsoft domain. To use Active Directory for authentication purposes you may use any of the LDAP service types provided in the `Authentication` node of JSCAPE MFT Server Manager.

Verifying Active Directory Installation
Obtaining Zone Name
Setting Authentication Details
Testing Connection
Firewall Configuration

Verifying Active Directory Installation

Prior to using LDAP you must first verify that you have Active Directory properly installed on the server you are authenticating against. To see if it is enabled on the server go to `Start > Programs > Administrative Tools > Active Directory Users and Computers`. If you do not see this menu option then it is likely you don't have Active Directory installed on this server. Please consult your Microsoft documentation for instructions on how to install and configure Active Directory.

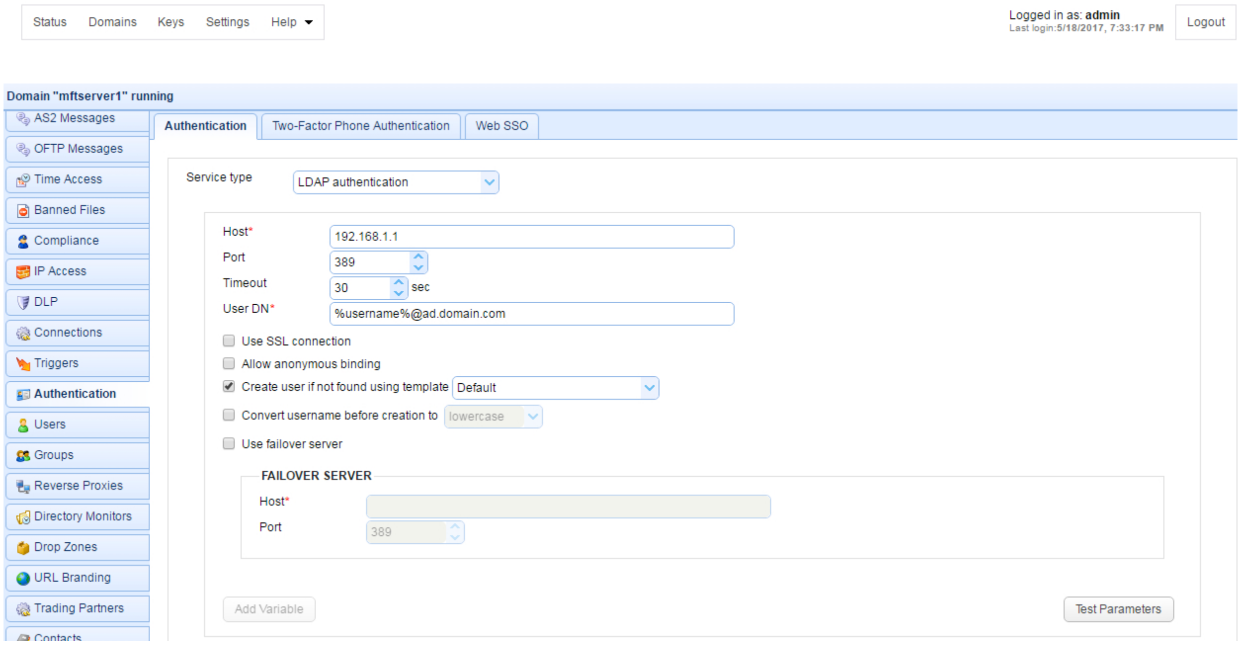
Obtaining Zone Name

Open the Active Directory manager from `Start > Programs > Administrative Tools > Active Directory Users and Computers`. Here you should node with a name like `ad.domain.com` or something similar. This is your zone name and will be used when setting your authentication details in JSCAPE MFT Server Manager. Beneath this zone you should see a `Users` folder that lists all the users for this system. You may have other folders in this directory. Please make note of the folder that contains the users you wish to authenticate with as this will be needed when constructing your `User DN`.

Setting Authentication Details

Using JSCAPE MFT Server Manager go to the `Authentication` node and set the `Service type` to `LDAP authentication`. Enter the connection details for your Active Directory service.

Figure 61



Service type: LDAP authentication

Host*: 192.168.1.1

Port: 389

Timeout: 30 sec

User DN*: %username%@ad.domain.com

□ Use SSL connection

□ Allow anonymous binding

☑ Create user if not found using template: Default

□ Convert username before creation to: lowercase

□ Use failover server

FAILOVER SERVER

Host*:

Port: 389

Host - The hostname or IP address of the LDAP service.

Port - The port of the LDAP service.

Timeout - The connection timeout when connecting to LDAP service.

User DN - The users distinguished name for authenticating with the LDAP service. The variable `%username%` may be used which refers to the username passed in during the authentication process.

Use SSL connection - Connect to LDAP server using SSL connection.

Allow anonymous binding - Sets whether user can bind anonymously to LDAP directory.

Create user if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

Use failover server - If enabled and primary LDAP server is inaccessible then authentication will be attempted against failover server.

Testing Connection

To test your Active Directory connection click the `Test Parameters` button on this panel and enter a valid username/password for the Active Directory service when prompted.

Firewall Configuration

You may need to change your server configuration to allow inbound requests on port 389. If needed this can be done via the `Control Panel > Network Connections` menu in Windows. From here right-click on the desired network interface and click the `Properties > Advanced > Settings` menu option. In the `Exceptions` tab add port 389 to allow inbound connections to this port.

See also

[Setting authentication preferences]

Authenticating using custom authentication API

The custom authentication API provides you with a way to authenticate users using your own business rules. The custom authentication API is recommended when the other built-in authentication modules (Database, LDAP, Domain) do not meet your needs. To implement your own authentication provider you must perform the following:

1. Create a class which implements the `com.jscape.inet.mft.subsystems.authentication.AuthenticationService` class.

2. Overload the `public void authenticate(Credentials creds)` method, throwing a `com.jscape.inet.mft.subsystems.authentication.AuthenticationException` exception if authentication fails.

3. Create a JAR file that contains the compiled version of your `com.jscape.inet.mft.subsystems.authentication.AuthenticationService` implementation. To compile your authentication class you will need to include the `ftpserver.jar` library in your classpath. The `ftpserver.jar` library may be found in the `libs` directory for JSCAPE MFT Server.

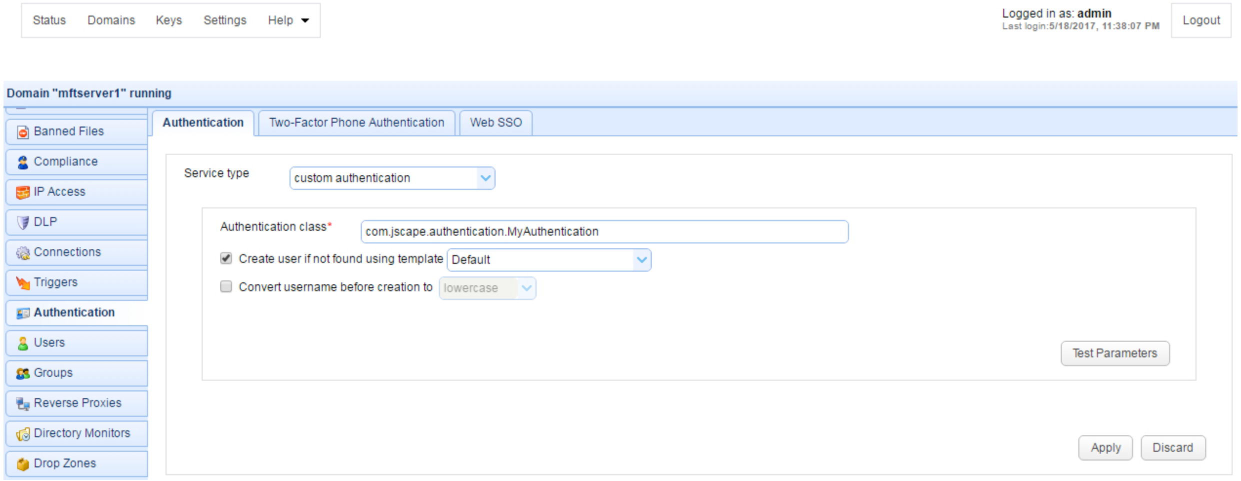
4. Place the JAR file created in Step 3 as well as any needed 3rd party JAR files into the `libs/ext` directory of your JSCAPE MFT Server installation.

5. Restart the JSCAPE MFT Server Service.

6. Open JSCAPE MFT Server Manager and select the `Authentication` node.

7. Change `Service type` to `custom authentication`. Type in the class name created in Step 1 into the `Authentication class` field.

Figure 86



Logged in as: **admin**
Last login:5/18/2017, 11:38:07 PM

Domain "mftserver1" running

Service type: custom authentication

Authentication class*: com.jscape.authentication.MyAuthentication

☑ Create user if not found using template: Default

☐ Convert username before creation to: lowercase

Authentication class - The custom authentication class name.

Create user if not found using template - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified User Template.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified User Template.

Example

```
package test.jscape;

import com.jscape.inet.mft.subsystems.authentication.AuthenticationException;
import com.jscape.inet.mft.subsystems.authentication.Credentials;
import com.jscape.inet.mft.subsystems.authentication.AuthenticationService;

/**
 * Example class to implement IP/user based authentication
 */
public class UserIPAuthentication implements AuthenticationService {

      private static final String username = "jsmith";
      private static final String password = "secret";
      private static final String ip = "127.0.0.1";

      /**
       * Authenticate user credentials
       */
      public void authenticate(Credentials creds) throws
AuthenticationException {
            if(creds.getLogin().equals(username) && creds.getPassword()
.equals(password)
                        && creds.getClientIp().equals(ip)) {
                  // ignore
            } else {
                  throw new AuthenticationException("Authentication failed: "
+ creds.getLogin() +
                              ":" + creds.getClientIp() + ":" +
creds.getPassword());
            }
      }
}
```

The example above authenticates successfully if the username is "jsmith", the password is "secret" and the client IP address is "127.0.0.1".

See also

Setting authentication preferences

Server configuration 3

Adding anonymous user accounts

For security reasons anonymous access by default is not enabled. To enable anonymous access simply create a new user account with the login name of `anonymous` and an empty password.

See also

Adding users

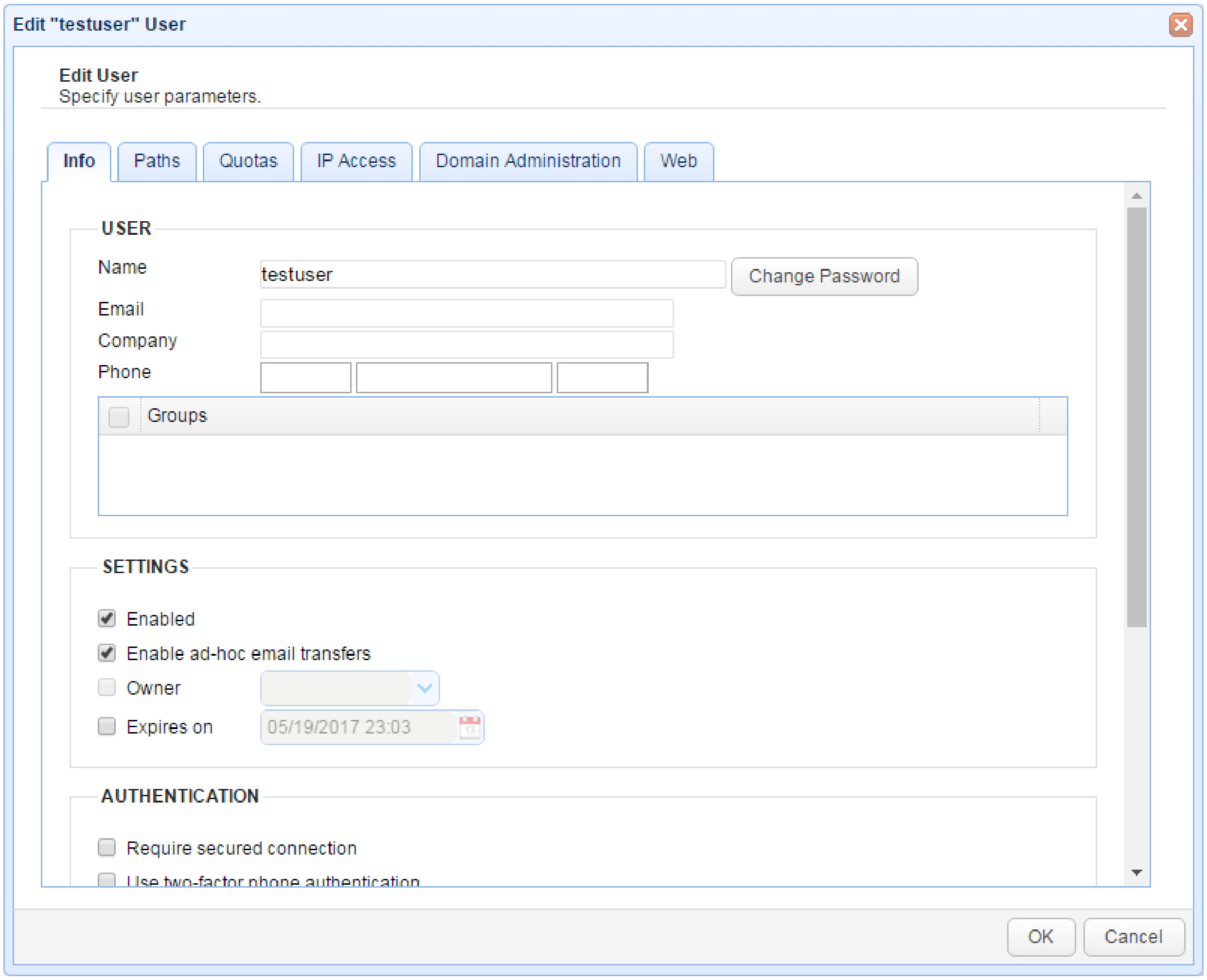
Defining virtual paths

Virtual paths are virtual file system paths that map to a physical path on your domain and have their own set of permissions. This allows you to have complete control over what resources users may access on your domain without having to manage users and permissions at the OS level. Virtual paths may be defined at the `User`, `User Template` or `Group` levels. Defining virtual paths at the `Group` or `User Template` level is recommended when you want to assign multiple users the same set of virtual paths.

Creating virtual paths for a User account

1. From the `Users` node select the user you wish to define the virtual paths for and click the `Edit` button. The `Edit User` dialog is displayed.

Figure 236



Edit "testuser" User

Edit User
Specify user parameters.

USER

Name: testuser

Email:

Company:

Phone:

□ Groups

SETTINGS

☑ Enabled

☑ Enable ad-hoc email transfers

□ Owner

□ Expires on 05/19/2017 23:03

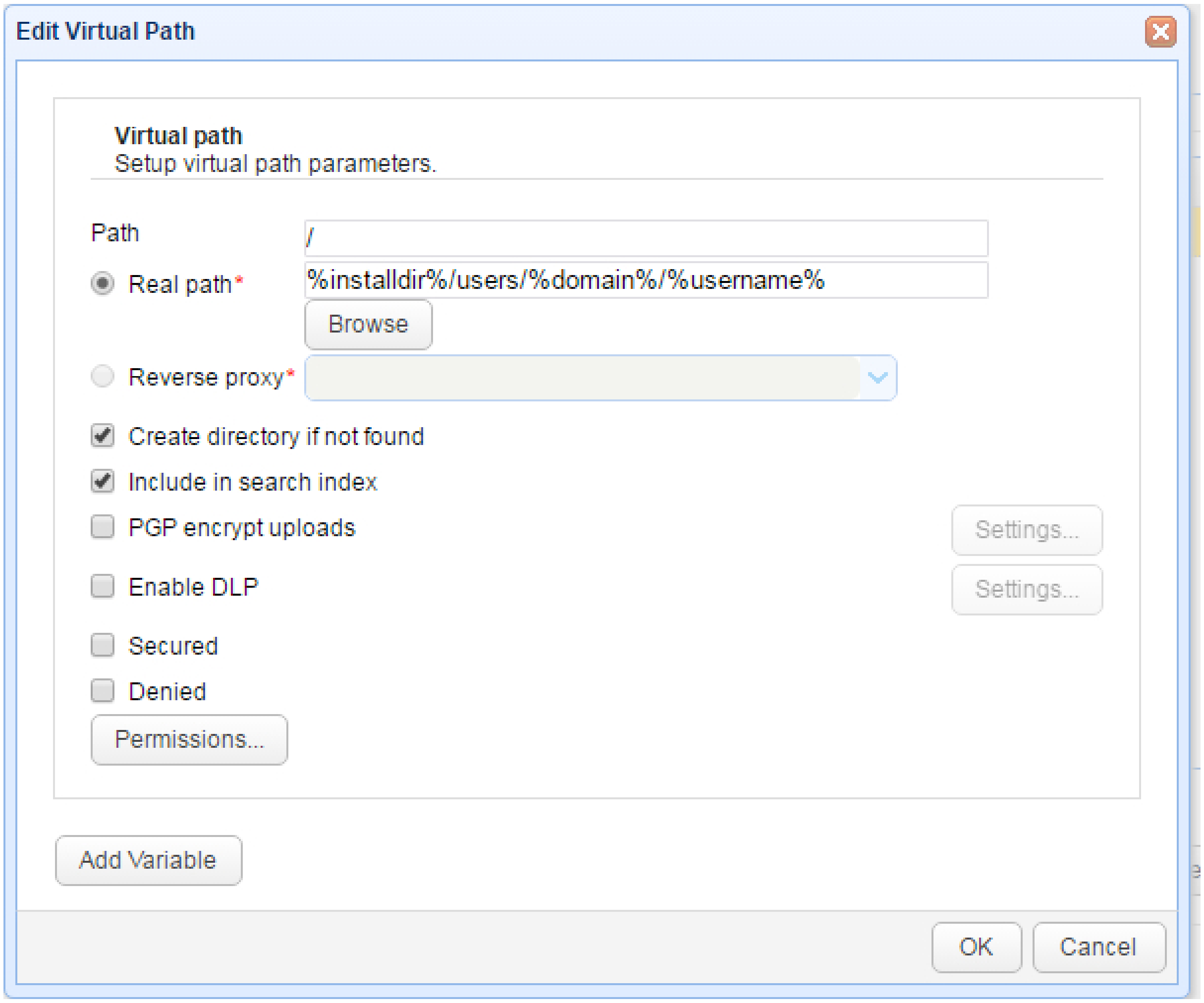
AUTHENTICATION

□ Require secured connection

□ Use two-factor phone authentication

2. Click on the `Paths` tab to see a list of virtual paths for this user. To add a new virtual path click on the Add button.

Figure 42



Edit Virtual Path

Virtual path
Setup virtual path parameters.

Path: /

● Real path*: %installdir%/users/%domain%/%username%

○ Reverse proxy*

☑ Create directory if not found

☑ Include in search index

☐ PGP encrypt uploads

☐ Enable DLP

☐ Secured

☐ Denied

Path - The virtual path that will be made available to the User account. Virtual paths should always start with a slash `/` character. For example a valid virtual path might be `/docs`

Real path - The real path on your domain that this virtual path maps to.

Reverse Proxy - If you are mapping this path to a reverse proxy then select it here.

Create directory if not found - Creates directory on server if not found when accessed by user.

Include in search index - If checked files in directory will be indexed for search purposes.

Permissions - Check the permissions that this user will be granted for the virtual path.

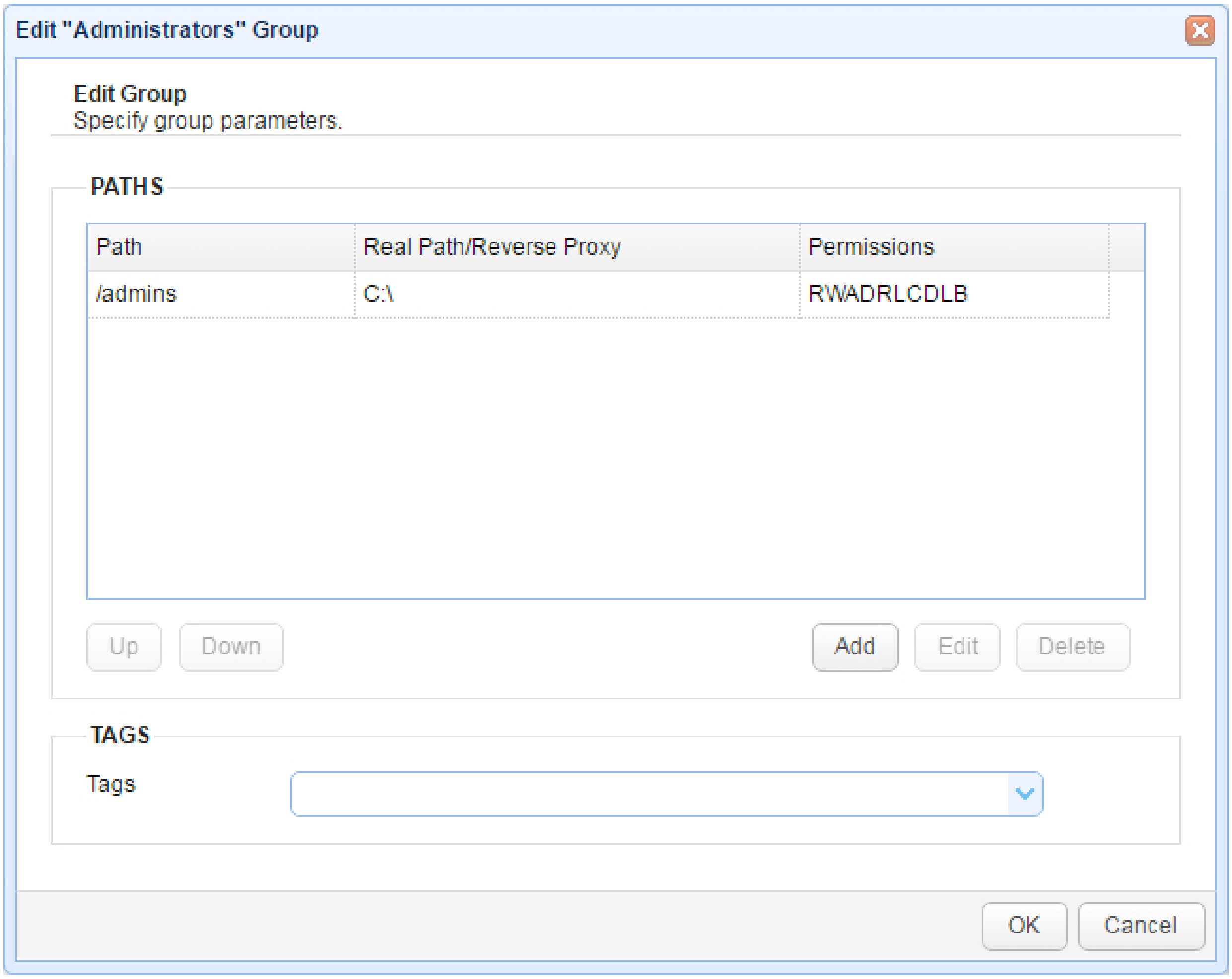
3. To finish, click `OK`. Your new virtual path will be displayed in the virtual path listing for the user account.

Creating virtual paths for a Group

When creating a virtual path for a group, all users who are members of the group will have access to the virtual path.

1. From the `Groups` node select the group you wish to define the virtual paths for and click the `Edit` button. The `Edit Group` dialog is displayed.

Figure 43



Edit "Administrators" Group

Edit Group
Specify group parameters.

PATHS

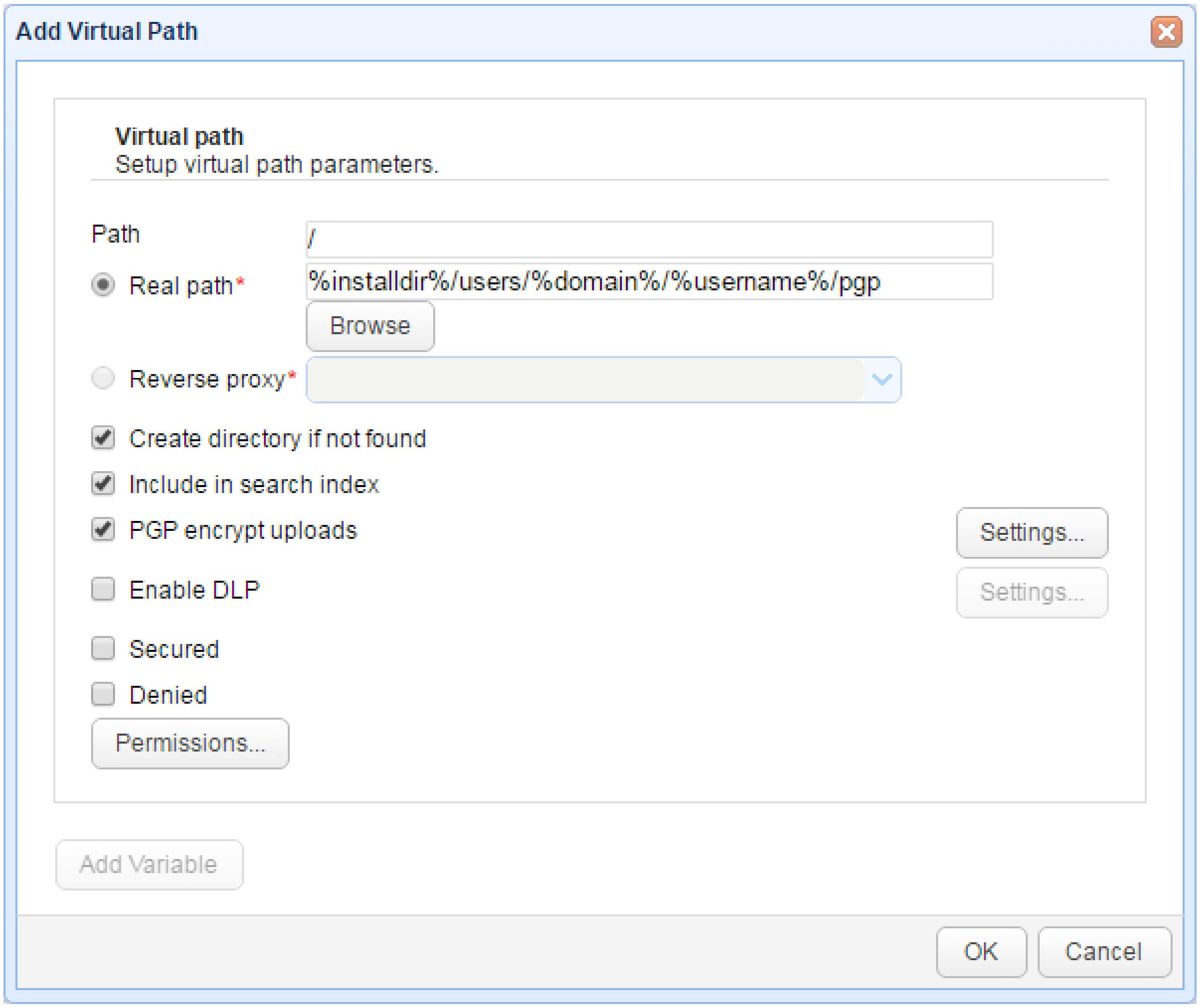
Path	Real Path/Reverse Proxy	Permissions
/admins	C:\	RWADRLCDLB

TAGS

Tags

2. A list of virtual paths is displayed at the bottom of the screen for this group. To add a path click the `Add` button.

Figure 191



Add Virtual Path

Virtual path
Setup virtual path parameters.

Path: /

● Real path*: %installdir%/users/%domain%/%username%/pgp

○ Reverse proxy*:

☑ Create directory if not found

☑ Include in search index

☑ PGP encrypt uploads

□ Enable DLP

□ Secured

□ Denied

Path - The virtual path that will be made available to the User account. Virtual paths should always start with a slash `/` character. For example a valid virtual path might be `/docs`

Real path - The real path on your domain that this virtual path maps to.

Reverse Proxy - If you are mapping this path to a reverse proxy then select it here.

Create directory if not found - Creates directory on server if not found when accessed by user.

Include in search index - If checked files in directory will be indexed for search purposes.

PGP encrypt uploads - Files uploaded to this directory will be automatically PGP encrypted using specified key.

Enable DLP - Files downloaded from this directory are subject to DLP rules.

Secured - If checked, this directory may only be accessed using secure protocols (FTPS, SFTP, HTTPS etc.).

Denied - If checked, this directory may not be accessed. This option is typically used to override the behavior of a parent directory, where access to parent directory is granted but access to this sub-directory is denied.

Permissions - Check the permissions that this user will be granted for the virtual path.

3. To finish, click `OK`. Your new virtual path will be displayed in the virtual path listing for the Group.

Variables

Variables may be used in `Path` and `Real Path` fields for purposes of creating dynamic paths. Available variables are described below.

`installdir` - The absolute path of JSCAPE MFT Server installation directory.

`domain` - The domain that this user/group belongs to.

`sessionid` - Unique session ID for the user. This ID is unique for each login.

`username` - The username of connected user.

`group` - The optional group name that this user belongs to. Note, this variable is deprecated and is provided only for backwards compatibility. Users may belong to more than one group. This variable will return only the first group that user belongs to if found.

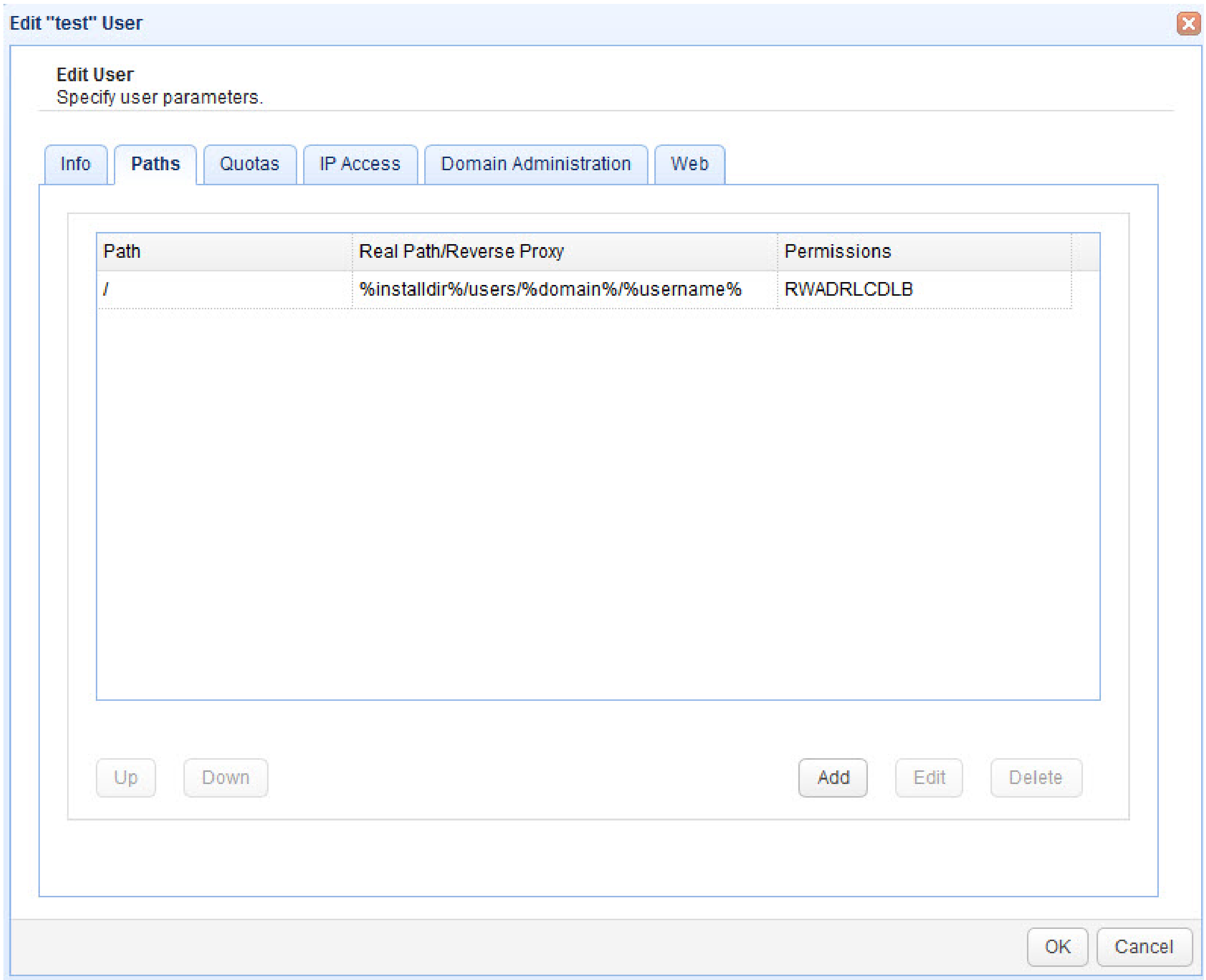
`queryattr[‘name’]` - If LDAP or Database authentication methods are used this will return the attribute of the matching record found during authentication. For example, if user is authenticating against a relational database using the query `select name from users where username = '%username%' and password = '%password%'` the variable `queryattr['name']` would return the matching `name` value returned by the database query.

Virtual path permissions

In the `Permissions` column of a virtual path you will find a series of letters and optional dashes. In the event one or more permissions are not granted this will be represented by a dash (-) character, indicating the specified permission has been taken away. A character map defining these letters in order of occurrence is provided below.

R - Download file
W - Upload file
A - Append file
D - Delete file
R - Rename file
L - List files
C - Make dir
D - Delete dir
L - List subdirs
B - Browse subdirs

Figure 134



Edit "test" User

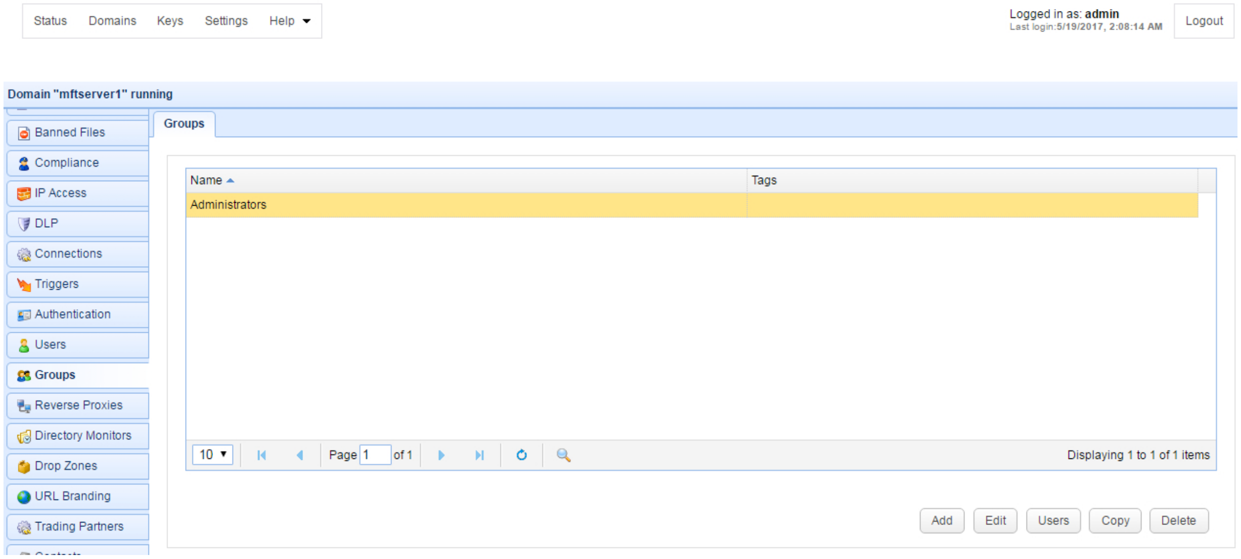
Edit User
Specify user parameters.

Path	Real Path/Reverse Proxy	Permissions
/	%installdir%/users/%domain%/%username%	RWADRLCDLB

Adding groups

A group is a named set of virtual directories and file system permissions that may be assigned to zero or more user accounts. This is useful in the event you wish to manage permissions for multiple users based on user roles. To view a list of groups click on the `Groups` node for the desired domain.

Figure 26



Domain "mftserver1" running

Groups

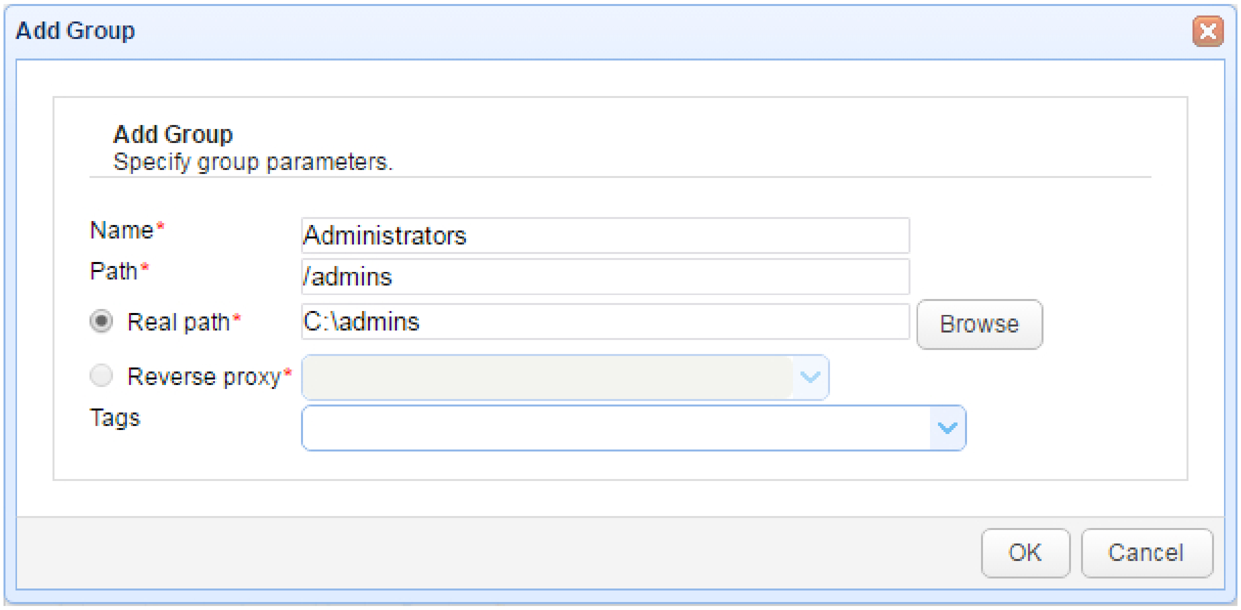
Name	Tags
Administrators	

10 Page 1 of 1 Displaying 1 to 1 of 1 items

Add Group

To add a group click on the Add button in the lower right corner. The Add Group dialog will be displayed.

Figure 27



Add Group
Specify group parameters.

Name* Administrators
Path* /admins
● Real path* C:\admins
○ Reverse proxy*
Tags

Name - The unique name for this group.

Path - The unique virtual path for this group.

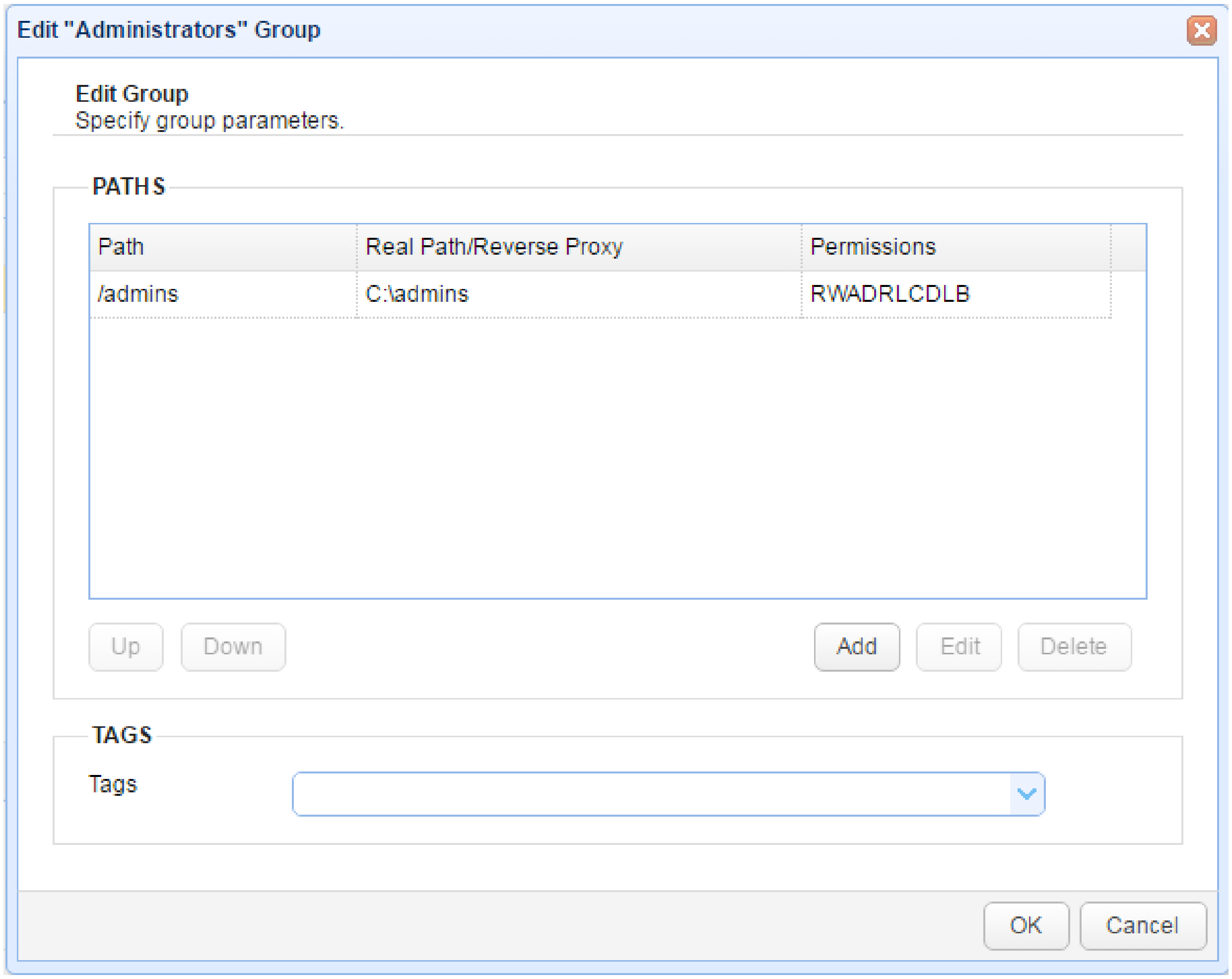
Real path - The real physical directory for this path. Note: You will be able to add more virtual paths and permissions using the Edit Group function.

Reverse proxy - The reverse proxy to associate with this path.

Edit Group

To edit a group, highlight the group name you would like to edit and click the `Edit` button. The `Edit Group` dialog is displayed.

Figure 31



Edit "Administrators" Group

Edit Group
Specify group parameters.

PATHS

Path	Real Path/Reverse Proxy	Permissions
/admins	C:\admins	RWADRLCDLB

TAGS

Tags

Path - The virtual path.

Real Path/Reverse Proxy - The real path or reverse proxy this path is mapped to.

Permissions - The permission settings for this path.

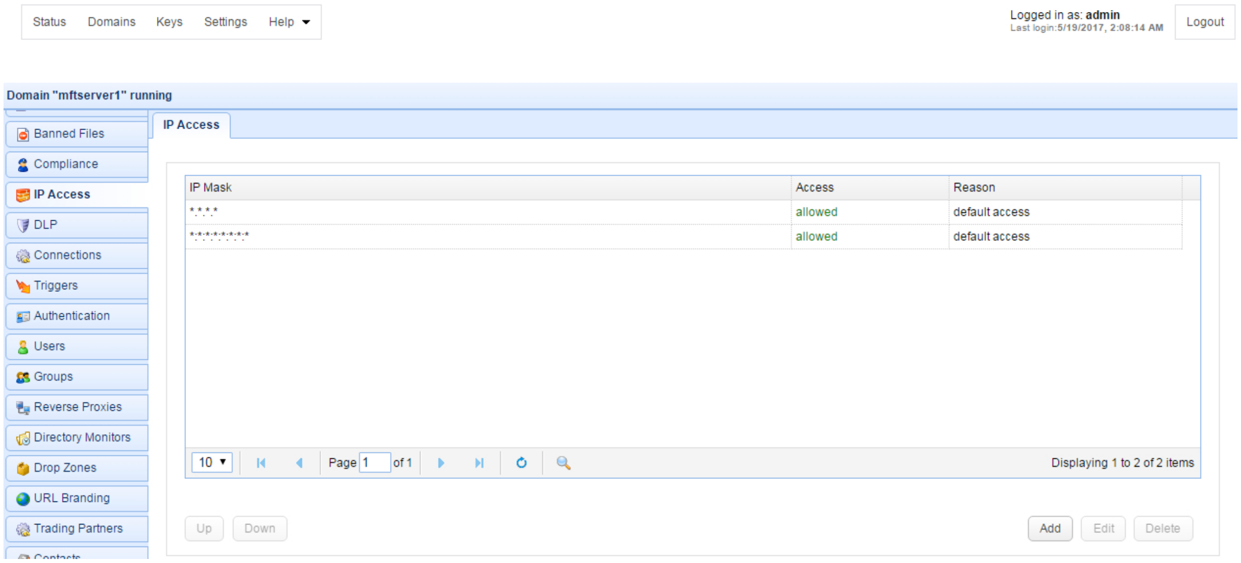
Setting IP based access

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

Add IP access rule
IP mask examples

Figure 29

Server configuration 3



IP Mask	Access	Reason
..*.*	allowed	default access
::*:*:*:*:*:*	allowed	default access

Displaying 1 to 2 of 2 items

IP Mask - The IP address mask.

Access - Indicates whether access is allowed or denied.

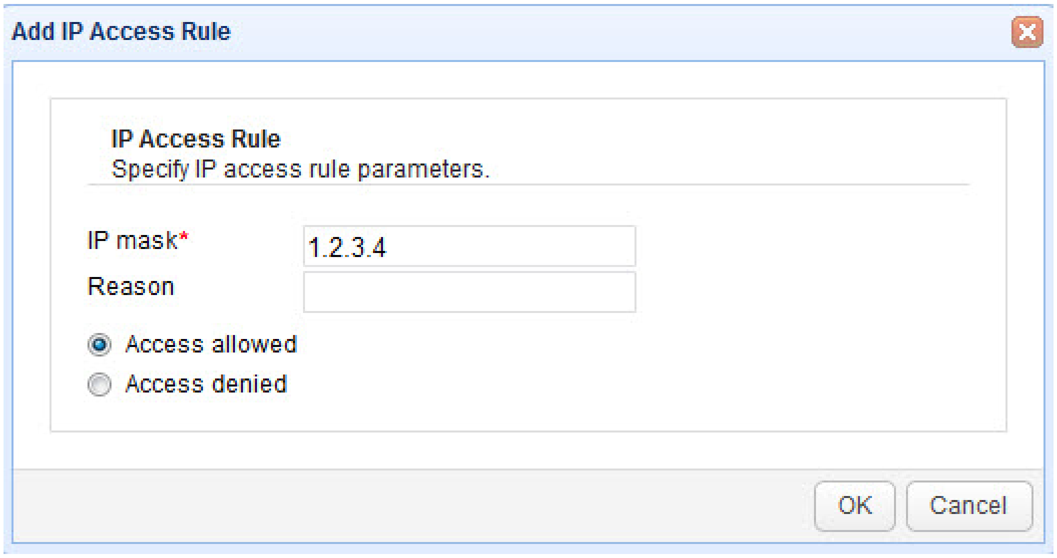
Reason - The reason access is allowed or denied.

Access rules are processed in the order listed. For each connection the first matching access rule will be used. Therefore it is important that the access rules be ordered correctly to prevent a user from being mistakenly denied or granted access. You may use the `Up` and `Down` buttons to order these access rules to suit your needs.

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 30



IP Access Rule
Specify IP access rule parameters.

IP mask*: 1.2.3.4
Reason:

● Access allowed
○ Access denied

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.

Access denied - Select to have access denied.

IP mask examples

Examples of valid IP masks are as follows:

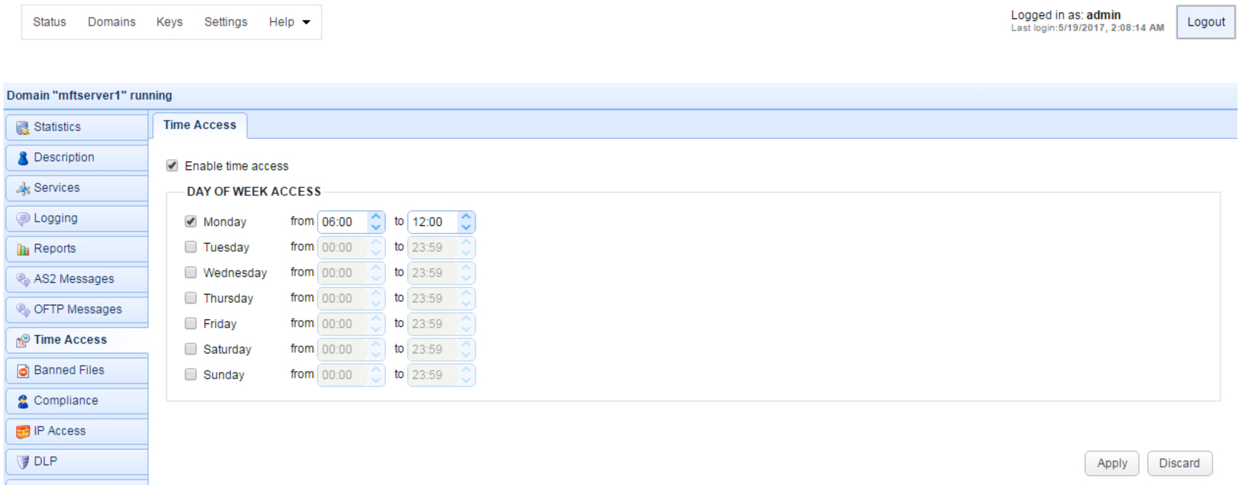
`192.168.1.1` - Allows/Blocks a single IP address
`192.168.1.*` - Allows/Blocks all IP addresses in a class C IP block.
`192.168.*.*` - Allows/Blocks all IP addresses in a class B IP block.
`*.*.*.*` - Allows/Blocks all IP addresses.

Setting time based access

You may limit the time of day that users may connect to your services. To enable these settings go to the `Time Access` node for the desired domain. If a day is enabled, then users may only access services between the period specified for that day. If a day is not enabled then there is no restriction on what time of day the user may access services. Dates/times are based on the current local time on the server.

For example, in *Figure 131* below users may access services Tuesday thru Sunday without restriction. On Mondays user may only connect between 6:00 AM and 12:00 noon local time.

Figure 131



Logged in as: admin
Last login:5/19/2017, 2:08:14 AM

Domain "mftserver1" running

☑ Enable time access

DAY OF WEEK ACCESS

☑ Monday	from	06:00	to	12:00
☐ Tuesday	from	00:00	to	23:59
☐ Wednesday	from	00:00	to	23:59
☐ Thursday	from	00:00	to	23:59
☐ Friday	from	00:00	to	23:59
☐ Saturday	from	00:00	to	23:59
☐ Sunday	from	00:00	to	23:59

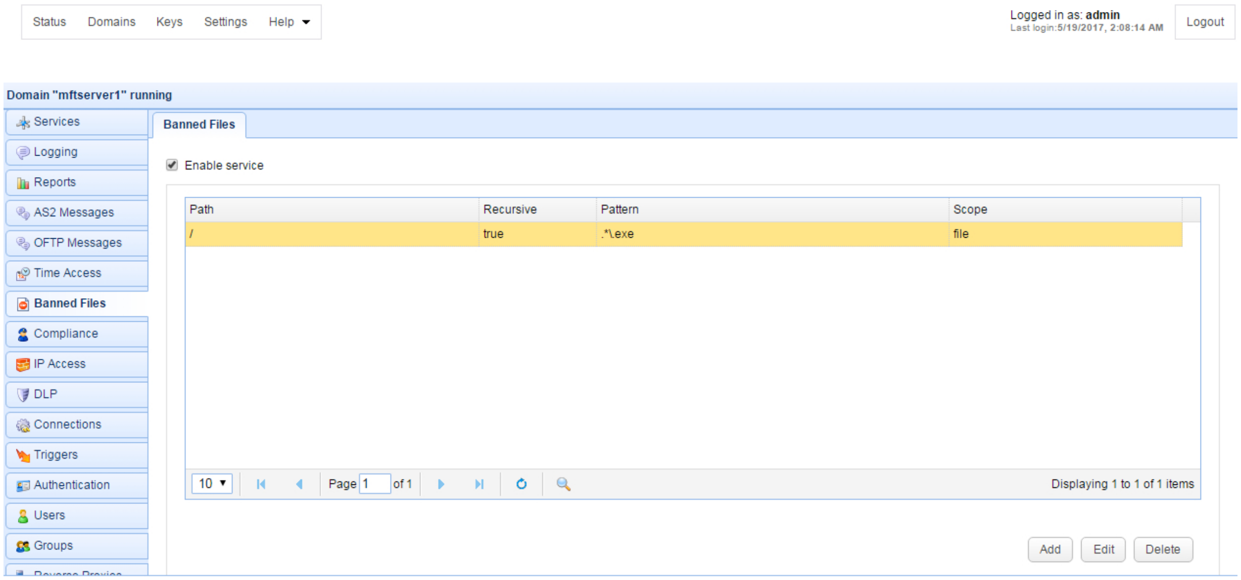
Enable time access - Enables or disables time based access.

Setting banned files

You may limit the files that a user can upload based on filename. To enable these settings go to `Banned Files` node for desired domain. If enabled then uploading files matching any of the regular expressions will be disallowed.

For example, in *Figure 132* below, users may not upload files with a `.exe` extension.

Figure 132



☑ Enable service

Path	Recursive	Pattern	Scope
/	true	.*\.exe	file

Displaying 1 to 1 of 1 items

Path - The virtual directory path to which this rule should be applied.

Recursive - If enabled, this rule will be applied to all directories beneath virtual directory path.

Pattern - The regular expression to use for this rule.

Scope - The scope of this rule.

See also

[Regular expression reference]

Setting connection preferences

There are various connection preferences that may be used to define how users may connect to domain services you create. These preferences may be managed under the `Connections` and `Services` nodes.

[General Connection Settings]
[FTP Connection Settings]
[SFTP/SCP Connection Settings]
[AFTP Connection Settings]
[OFTP Connection Settings]
[TFTP Connection Settings]

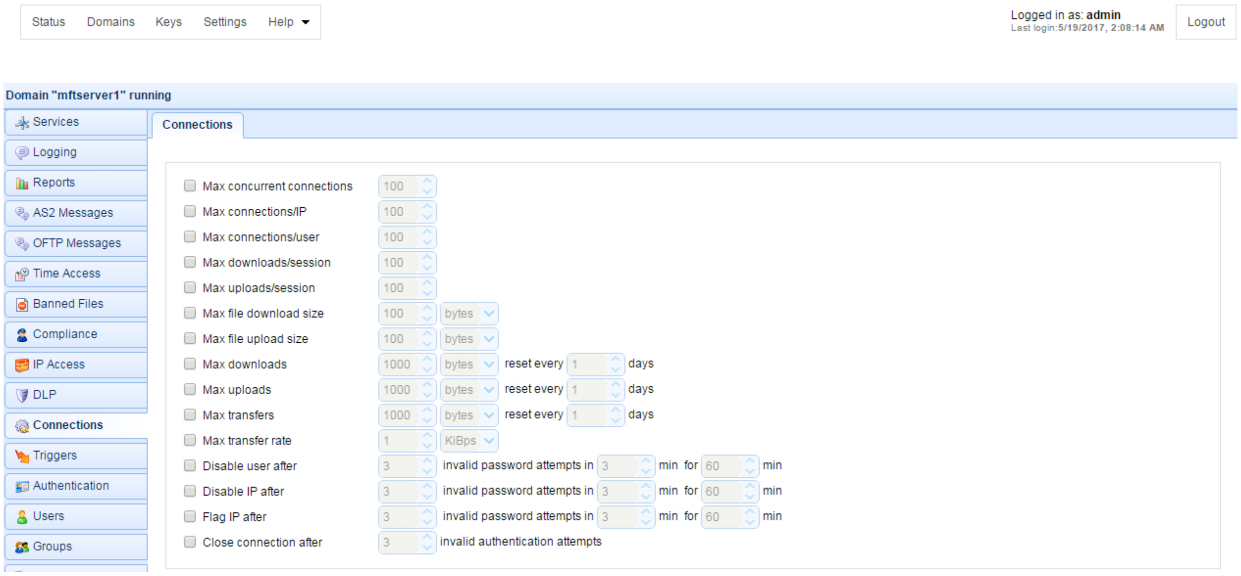
Server configuration 3

HTTP/S Connection Settings
WebDAV/S Connection Settings

General Connection Settings

General connection settings apply to all file transfer protocols including AS2, FTP/S, SFTP/SCP, HTTP/S, WebDAV and AFTP and may be set using the `Connections` node.

Figure 28



□ Max concurrent connections 100
□ Max connections/IP 100
□ Max connections/user 100
□ Max downloads/session 100
□ Max uploads/session 100
□ Max file download size 100 bytes
□ Max file upload size 100 bytes
□ Max downloads 1000 bytes reset every 1 days
□ Max uploads 1000 bytes reset every 1 days
□ Max transfers 1000 bytes reset every 1 days
□ Max transfer rate 1 KiBps
□ Disable user after 3 invalid password attempts in 3 min for 60 min
□ Disable IP after 3 invalid password attempts in 3 min for 60 min
□ Flag IP after 3 invalid password attempts in 3 min for 60 min
□ Close connection after 3 invalid authentication attempts

Max concurrent connections - The maximum number of concurrent connections allowed. Note: This value may not exceed the concurrent connection limit of your license type.

Max connections/IP - The maximum number of active connections from a single client IP address.

Max connections/user - The maximum number of active connections from a single user.

Max downloads/session - The maximum number of downloads per client session.

Max uploads/session - The maximum number of uploads allowed per client session.

Max file download size (MB) - The maximum file download size in MB.

Max file upload size (MB) - The maximum file upload size in MB.

Max uploads (MB) - Defines an upload quota for the domain that is reset every N days. If upload quota is exceeded no further uploads are allowed until upload quota is reset.

Max downloads (MB) - Defines a download quota for the domain that is reset every N days. If download quota is exceeded no further downloads are allowed until download quota is reset.

Max transfers (MB) - Defines a transfer quota for the domain that is reset every N days. If transfer quota is exceeded no further file transfers are allowed until transfer quota is reset. Transfers are the combined sum of uploads and downloads.

Max transfer rate - The maximum transfer rate for the entire domain. This limit applies to the aggregate of all connections for a given domain, regardless of protocol. This value can be set in KBps, MBps, or GBps.

Disable user after X invalid password attempts in Y min - Disables account for a certain period of time if too many login attempts fail within a certain period of time.

Disable IP after X invalid password attempts in Y min - Blocks IP from further access for a certain period of time if too many login attempts fails within a certain period of time.

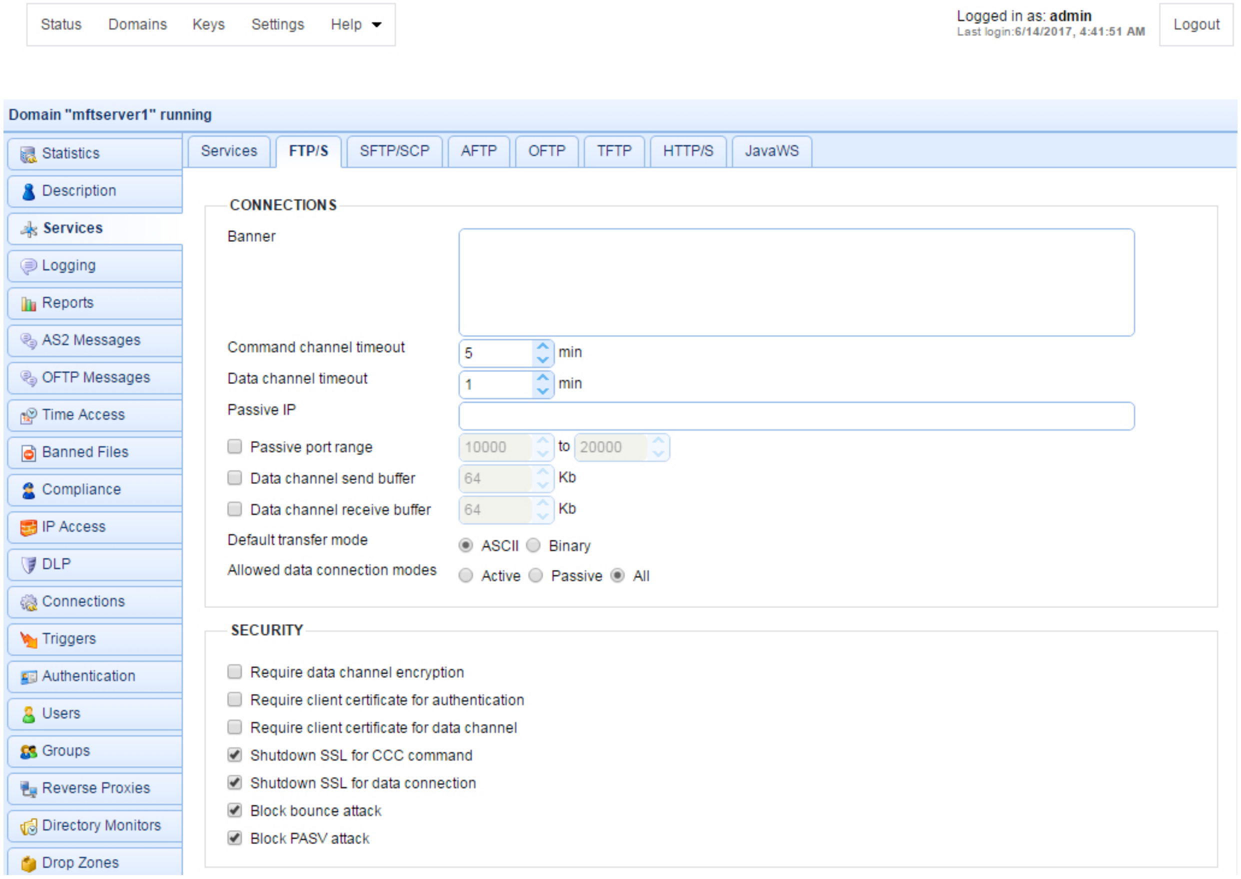
Flag IP after X invalid password attempts in Y min - Flags IP for a certain period of time if too many login attempts fails within a certain period of time. Note, flagging an IP has no affect on the users ability to connect. This will result in an `IP Flagged` event being raised and is intended primarily for integrating with other applications such as JSCAPE MFT Gateway.

Close connection after - Closes a connection after a specified number of invalid authentication attempts is reached while performed over that connection.

FTP/S Connection Settings

FTP/S connection settings may be managed under the `Services > FTP/S` panel.

Figure 70



CONNECTIONS

Banner

Command channel timeout 5 min

Data channel timeout 1 min

Passive IP

□ Passive port range 10000 to 20000

□ Data channel send buffer 64 Kb

□ Data channel receive buffer 64 Kb

Default transfer mode ● ASCII ○ Binary

Allowed data connection modes ○ Active ○ Passive ● All

SECURITY

□ Require data channel encryption

□ Require client certificate for authentication

□ Require client certificate for data channel

☑ Shutdown SSL for CCC command

☑ Shutdown SSL for data connection

☑ Block bounce attack

☑ Block PASV attack

Connections

Banner - The banner to display to FTP clients.

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

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

Passive IP - The IP to use when responding to PASV client requests.

Passive port range - The port range on the server to use for servicing PASV client requests.

Data channel send buffer - The size of send buffer for data channel. Default is send buffer size for JVM.

Data channel receive buffer - The size of receive buffer for data channel. Default is the receive buffer size for JVM.

Default transfer mode - The default transfer mode to be used by server in the event that client does not specify transfer mode.

Allowed connections modes - The allowed connection modes for file transfers and directory listings.

Security

Require data channel encryption - If enabled client will be required to encrypt data channel when using FTPS (FTP over SSL) protocol.

Require client certificate for authentication - If enabled users authenticating using FTPS (FTP over SSL) will be required to authenticate using data encrypted with a private key that maps to a server installed client certificate.

Require client certificate for data channel - If enabled users requesting data transfer using FTPS (FTP over SSL) will be required to supply data encrypted with a private key that maps to a server installed client certificate.

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

Shutdown SSL for data connection - If enabled client must properly shutdown SSL data connections.

SSL/TLS Ciphers - The SSL/TLS ciphers to enable for FTPS (FTP over SSL) services.

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

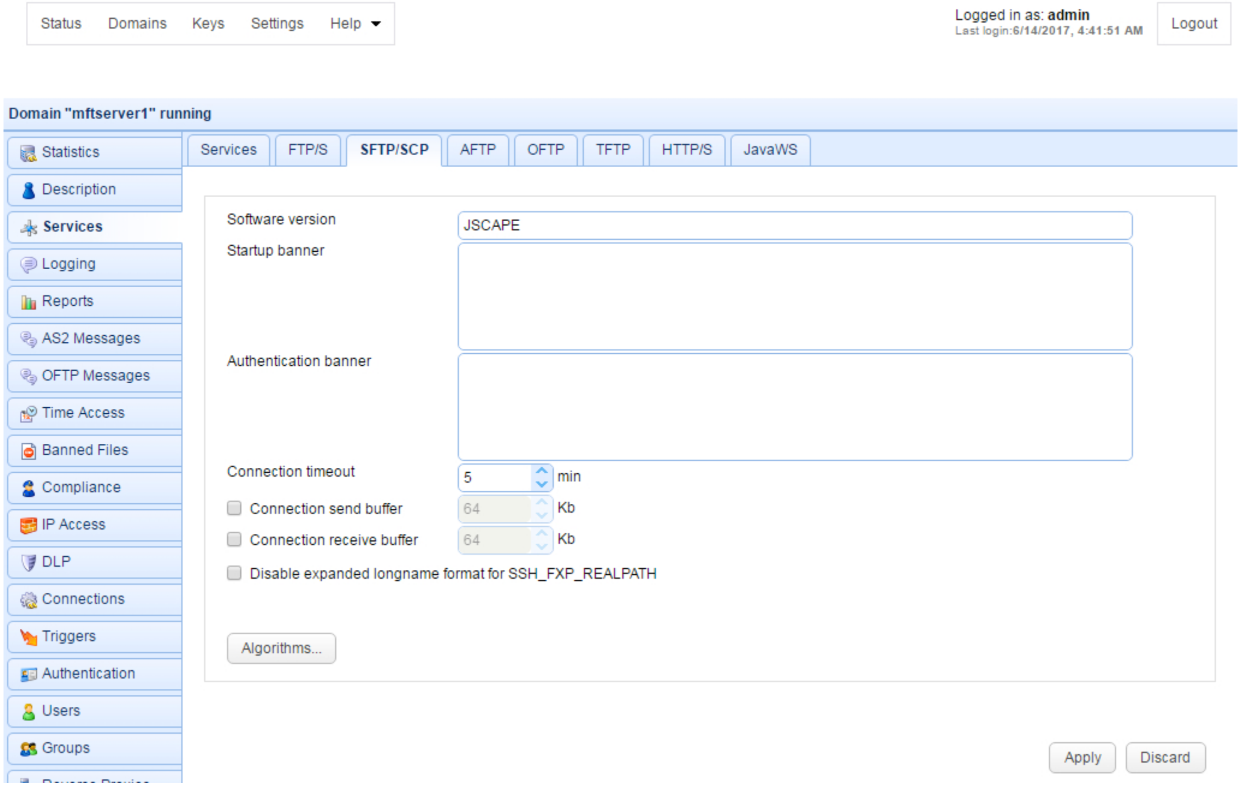
Block PASV attack - If enabled users will only be allowed to connect to passive data ports that are initiated by same client on command channel.

SFTP/SCP Connection Settings

SFTP/SCP connection settings may be managed under the `Services > SFTP/SCP` panel.

Figure 71

Server configuration



Software version: JSCAPE

Startup banner:

Authentication banner:

Connection timeout: 5 min

□ Connection send buffer: 64 Kb

□ Connection receive buffer: 64 Kb

□ Disable expanded longname format for SSH_FXP_REALPATH

Software version - The SSH version banner displayed when connecting. Note, it is important that this not contain any spaces.

Startup banner - The banner to display to SFTP clients prior to displaying SSH version banner.

Authentication banner - The banner to display to SFTP clients prior to displaying authentication prompt.

Connection timeout - The time in minutes that client connection may remain inactive before server forcefully disconnects client.

Connection send buffer - The size of send buffer. Default is send buffer size for JVM.

Connection receive buffer - The size of receive buffer. Default is the receive buffer size for JVM.

Disable expanded longname format for SSH_FXP_REALPATH - May be required for some SFTP clients that cannot handle long paths in SSH_FXP_REALPATH packets.

Algorithms - Lists all algorithms and ciphers, their order of preference and whether they are enabled.

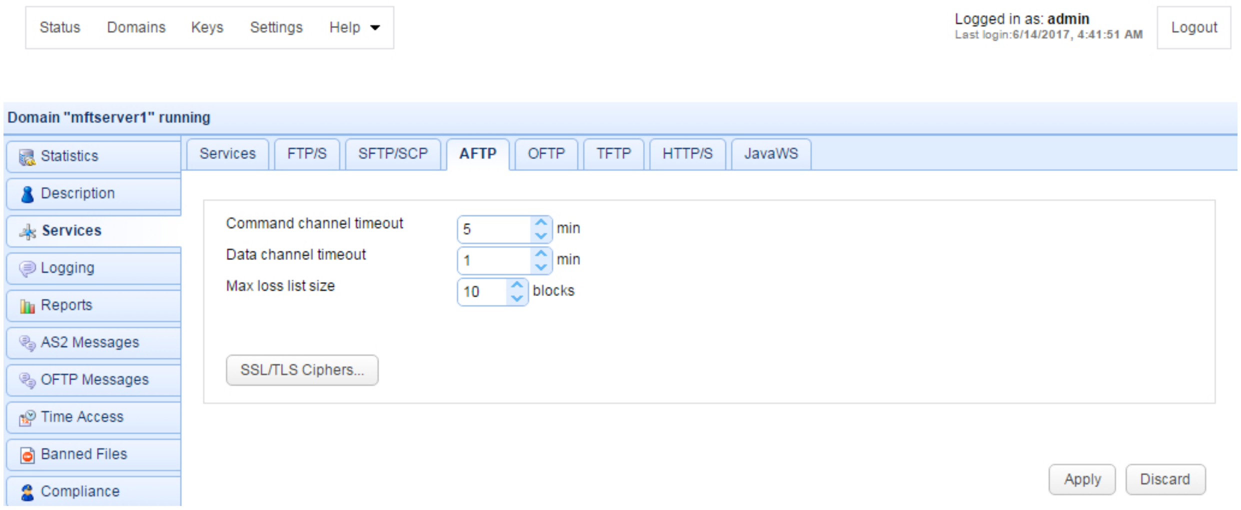
See also

Additional libraries needed for SFTP ciphers

AFTP Connection Settings

AFTP connection settings may be managed under the `Services > AFTP` panel.

Figure 163



Logged in as: admin
Last login:6/14/2017, 4:41:51 AM

Domain "mftserver1" running

Command channel timeout 5 min
Data channel timeout 1 min
Max loss list size 10 blocks

Connection channel timeout (min) - The time in minutes that client channel (TCP) connection may remain inactive before server forcefully disconnects client.

Data channel timeout (min) - The time in minutes that client data (UDP) connection may remain inactive before server forcefully disconnects client.

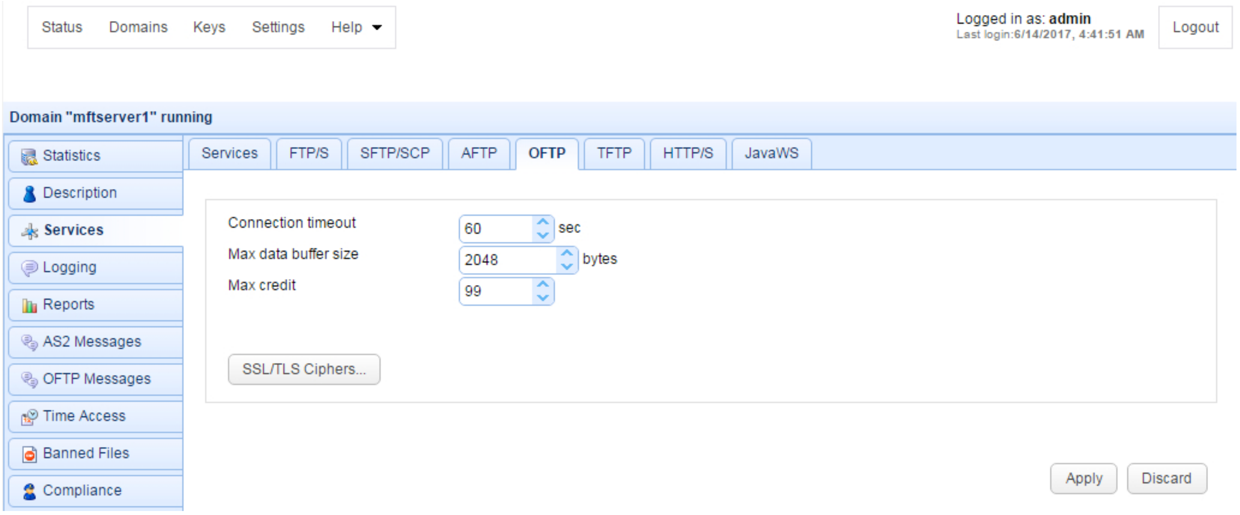
Max loss list size - The maximum number of lost blocks of data that may exist in memory for a client session.

SSL/TLS Ciphers - The SSL/TLS ciphers to enable for AFTP services.

OFTP Connection Settings

OFTP connection settings may be managed under the `Services > OFTP` panel.

Figure 192



Logged in as: admin
Last login:6/14/2017, 4:41:51 AM

Domain "mftserver1" running

Connection timeout 60 sec
Max data buffer size 2048 bytes
Max credit 99

Connection timeout - Connection channel timeout (min) - The time in minutes that client channel (TCP) connection may remain inactive before server forcefully disconnects client.

Max data buffer size - The maximum data buffer size for OFTP connections.

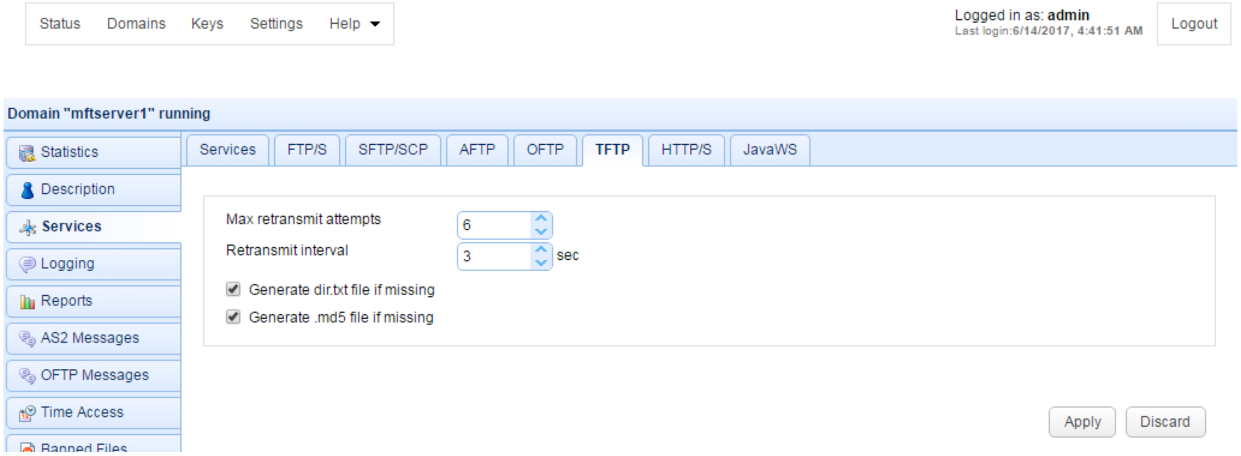
Max credit - The maximum number of packets that client may send to server before receiving an acknowledgment from server that is it ready to receive more data.

SSL/TLS Ciphers - The SSL/TLS ciphers to enable for OFTP services.

TFTP Connection Settings

TFTP connection settings may be managed under the `Services > TFTP` panel.

Figure 193



Max retransmit attempts: 6

Retransmit interval: 3 sec

☑ Generate dir.txt file if missing

☑ Generate .md5 file if missing

Max retransmit attempts - The maximum number of times that sender may unsuccessfully send a message before failure.

Retransmit interval - The retransmission interval (seconds) between each message retransmission attempt.

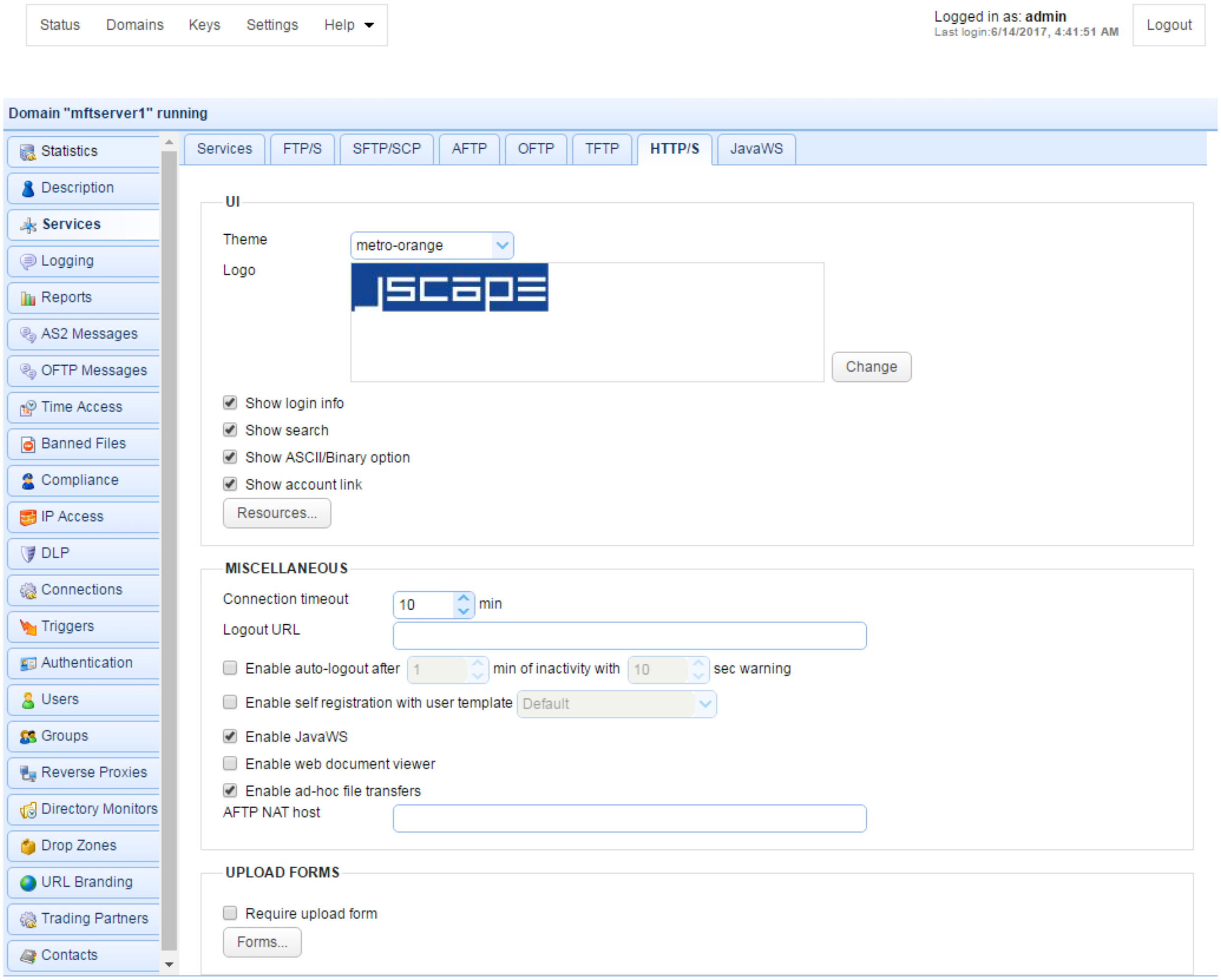
Generate dir.txt file if missing - If checked client may request the file dir.txt to obtain a directory listing of available files.

Generate .md5 file if missing - If checked client may request any filename with a .md5 extension to obtain an MD5 hash of filename contents.

HTTP/S Connection Settings

HTTP/S connection settings may be managed under the `Services > HTTP/S` panel.

Figure 89



UI

Theme: metro-orange

Logo

☑ Show login info

☑ Show search

☑ Show ASCII/Binary option

☑ Show account link

MISCELLANEOUS

Connection timeout: 10 min

Logout URL:

□ Enable auto-logout after 1 min of inactivity with 10 sec warning

□ Enable self registration with user template Default

☑ Enable JavaWS

□ Enable web document viewer

☑ Enable ad-hoc file transfers

AFTP NAT host:

UPLOAD FORMS

□ Require upload form

Theme - The color theme used for the buttons, menus, tabs, and other GUI elements.

Logo - The logo displayed in upper left corner when using HTML user interface.

Show login info - If checked, the current username and domain is displayed in upper right.

Show search - If checked searches on indexed documents may be performed.

Show ASCII/Binary option - If checked, user has option of uploading files in both ASCII and binary modes. If unchecked only binary is allowed by default and user does not have ability to change this setting.

Show account link - If checked the My Account link is displayed in upper right allowing users to change their account contact information.

Resources… - The current language resource file. Language resource files are used for specifying alternative user interface labels based on client browser default language.

Connection timeout - The connection timeout for HTTP requests in minutes.

Logout URL - The URL to redirect user to upon clicking Logout link.

Enable auto-logout after - If checked, user will be automatically logged out after X minutes of inactivity with grace period of Y seconds.

Enable self-registration with user template - Enables new users to self-register. The properties of the newly created user account will depend on the template chosen from the drop-down list.

Enable JavaWS - If checked, JavaWS interface is enabled for WebDAV connections.

Enable web document viewer - If checked web document viewer is enabled.

Enable ad-hoc file transfers - If checked ad-hoc file transfers will be enabled for the domain.

Show buttons shortcuts - If checked, button shortcuts (e.g. F2, F5, F7) are displayed on buttons.

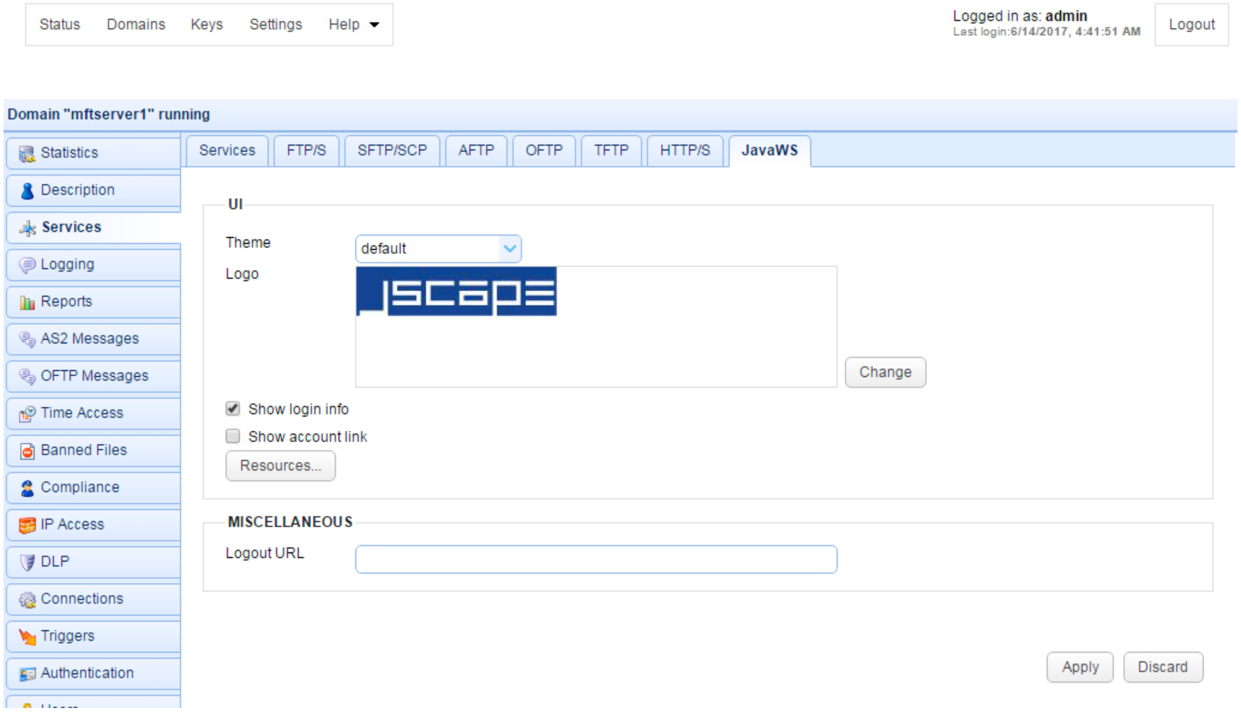
AFTP NAT Host - The host to use when connecting to AFTP service using JavaWS.

Forms... - Forms available during file upload when using HTML user interface.

JavaWS Connection Settings

JavaWS connection settings may be managed under the `Services > JavaWS` panel.

Figure 90



Logged in as: admin
Last login:6/14/2017, 4:41:51 AM

Domain "mftserver1" running

UI

Theme: default

Logo

☑ Show login info

☐ Show account link

MISCELLANEOUS

Logout URL:

Theme - The color theme used for the buttons, menus, tabs, and other GUI elements.

Logo - The logo displayed in upper left corner when using JavaWS user interface.

Show login info - If checked, the current username and domain is displayed in upper right.

Show account link - If checked the My Account link is displayed in upper right allowing users to change their account contact information.

Resources... - The current language resource file. Language resource files are used for specifying alternative user interface labels based on client browser default language.

Logout URL - The URL to redirect user to upon clicking Logout link.

Backing up server configuration files

JSCAPE MFT Server configuration data is stored in a relational database which is defined in the `Settings > Datastore` panel. By default JSCAPE MFT Server includes a pre-installed local database that is responsible for storing this data. This database and it's files may be found in the `<installdir>/data` directory. Other important configuration settings such as license file and startup parameters are located in the `<installdir>/etc` directory. In performing a backup you should backup **both** of these directories.

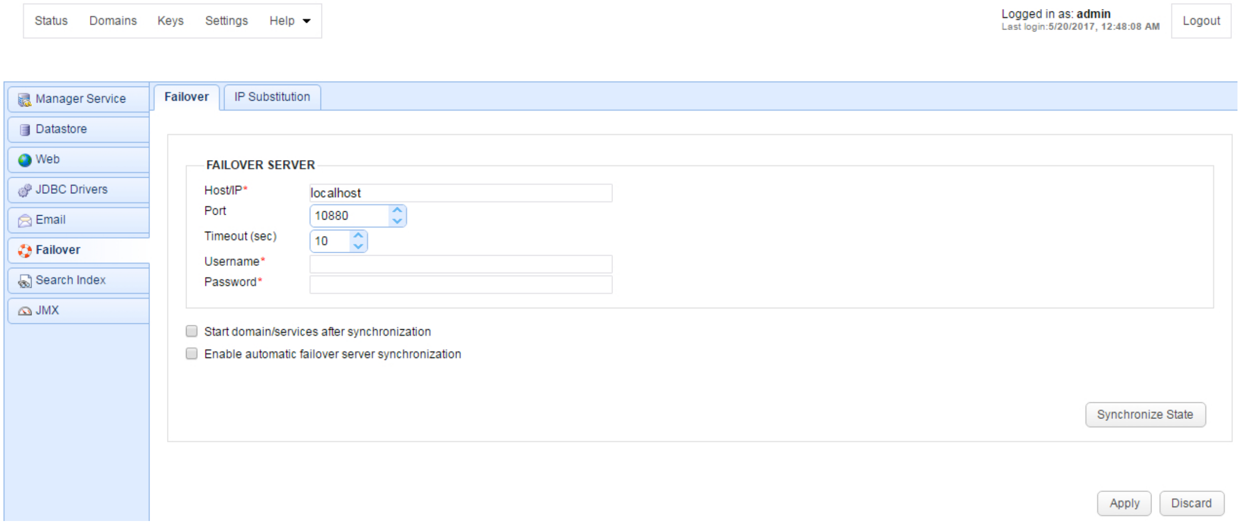
If you are using a datastore other than the default pre-installed database provided then please consult your database vendor documentation for details on how to perform a backup of the database. In addition to backing up your database you should also backup the `<installdir>/etc` directory as mentioned above.

To automatically backup your server configuration files on a scheduled basis, create a trigger using the `Current Time` event and `System Configuration Backup` action. Note, the `System Configuration Backup` action **will not** backup datastore that do not use the pre-installed default database.

Defining a failover server

JSCAPE MFT Server may be configured to synchronize all configuration changes to a failover server. The purpose of a failover server is that in the event the production server goes down the failover server can quickly take over the duties of the production server. To define a failover server go to `Settings > Failover` panel.

Figure 93



FAILOVER SERVER

Host/IP* localhost

Port 10880

Timeout (sec) 10

Username*

Password*

□ Start domain/services after synchronization

□ Enable automatic failover server synchronization

Host/IP - The hostname or IP address of the failover server.

Port - The port running the JSCAPE MFT Server Service on the failover server.

Timeout - The timeout for connecting to failover server.

Username - The JSCAPE MFT Server Service username for the failover server.

Password - The JSCAPE MFT Server Service password for the failover server.

Start domain/services after synchronization - Check to start domain and services on failover machine after synchronization.

Enable automatic failover server synchronization - Check to automatically synchronize configuration data to failover server when changes are made on production server.

IP Substitution - IP mapping which replaces all Services matching specified IP with corresponding Substitution IP during synchronization. This is useful in cases where the failover server needs a service to listen on a different IP than is used by the production server.

Failover considerations

There are a few things you must consider when defining a failover server in JSCAPE MFT Server Manager.

1. With failover mode enabled an active connection is maintained between the primary server and the administrative service of the failover server. This connection ensures that whenever configuration changes are made to primary server that they are automatically synchronized to failover server. In order to see the changes on failover server you may need to refresh data displayed in JSCAPE MFT Server Manager. This can be done by selecting the `Home` menu item.

2. Upon synchronization of data from primary server to failover server the domain and web services on failover server are NOT automatically started (unless the "Start domain/services after synchronization" is enabled). This is by design. The reasoning behind this is that in the event you are using database logs you may not want duplicate log information to be sent from failover server to database log whenever server configuration is updated. Therefore when switching to failover server you will need to first enable any web services in `Settings > Web` section of JSCAPE MFT Server Manager and start the domain.

3. User directories and data are **not** copied during failover synchronization. This process should be managed by your SAN (Storage Area Network) or via manual synchronization.

If failover synchronization fails further synchronization may be disabled to prevent possible performance issues. You may identify this event by creating a trigger to capture the `Failover Synchronization` event and adding a condition to check whether the `Success` variable is equal to `true`. You may then add one or more actions to the trigger in order to respond to this condition e.g. `Send Email`.

On-demand synchronization

JSCAPE MFT Server also supports on-demand synchronization. This is slightly different than failover mode in that an active connection is not maintained between the source and destination server. This allows you to perform a one-time synchronization of server configuration files to destination server by clicking the `Synchronize State` button. The `Synchronize State` button is enabled only when the `Enable automatic failover synchronization` checkbox is not checked.

On Demand v.s. Automatic Synchronization

As described above, on demand synchronization is performed when clicking the `Synchronize State` button. Automatic synchronization is performed when the `Enable automatic failover server synchronization` option is enabled. There are some important differences between the behavior of on demand v.s. automatic synchronization that should be noted.

1. When using on demand synchronization all domains on failover server are first deleted. Next, the production server copies all it's domains to the failover server. This is known as a full synchronization and ensures that both servers are running an exact copy.

2. When using automatic synchronization each event on the production server is sent to the failover server where it is processed. For example, if a user is added on the production server then this event is sent to the failover server where the user is also added, keeping the two servers in sync in real-time. This is known as a partial synchronization. This process is more efficient than doing a full on demand synchronization because only the changes made on the production server are synchronized rather than sending all production server configuration data.

Note, the synchronization process is one direction only, from production server to failover server. Changes made on the failover server are not automatically synchronized back to production server. If for some reason you must synchronize data from failover to production (e.g. you need to recover your production server after using failover server in production mode) then an on demand synchronization must be performed as follows:

1. Disable failover module on production server. This ensures that when performing on demand synchronization you do not create an endless synchronization loop.

2. On failover server, enable failover synchronization setting failover server to production host.

3. On failover server, click the `Synchronize State` button to perform on demand synchronization.

4. On failover server, disable failover synchronization.

5. Load production server and verify that data has been synchronized correctly.

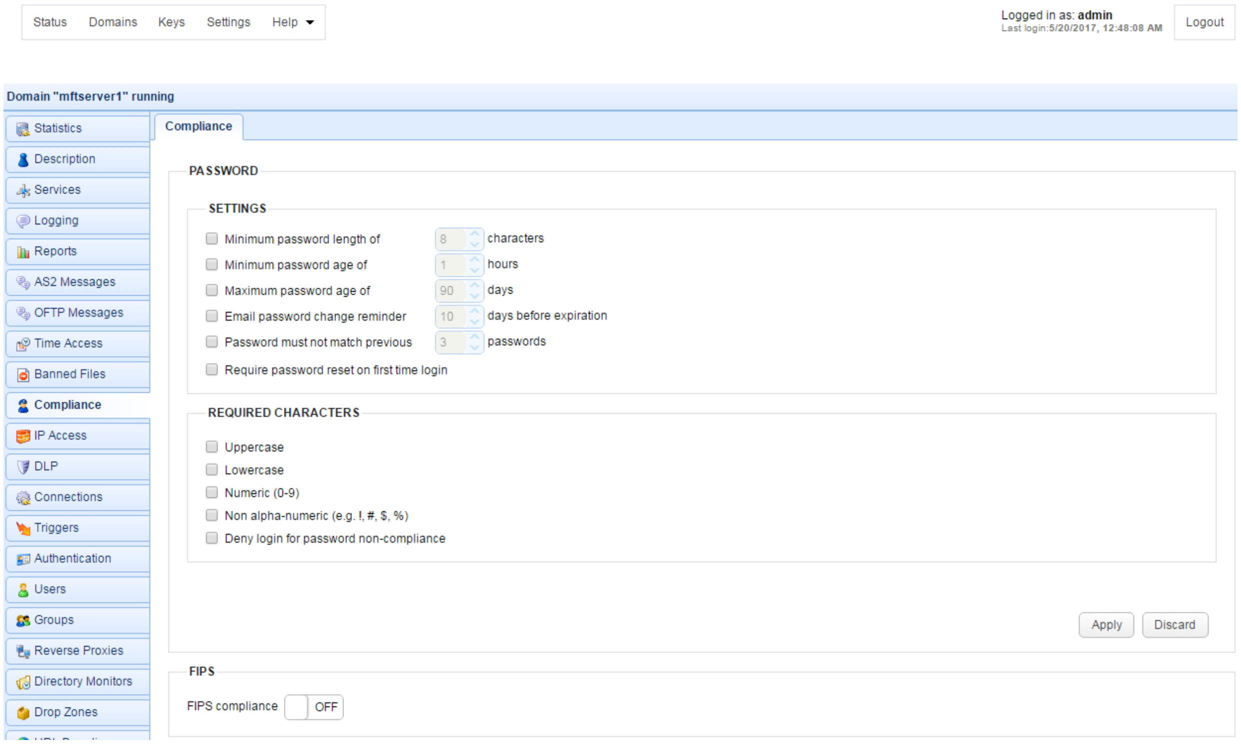
6. Enable failover module on production server setting failover server to failover host.

Server configuration 3

Defining password compliance

JSCAPE MFT Server may be configured to require that user passwords meet certain requirements. To configure password requirements, click on the `Compliance` node in JSCAPE MFT Server Manager.

Figure 106



PASSWORD

SETTINGS

- □ Minimum password length of 8 characters
- □ Minimum password age of 1 hours
- □ Maximum password age of 90 days
- □ Email password change reminder 10 days before expiration
- □ Password must not match previous 3 passwords
- □ Require password reset on first time login

REQUIRED CHARACTERS

- □ Uppercase
- □ Lowercase
- □ Numeric (0-9)
- □ Non alpha-numeric (e.g. !, #, $, %)
- □ Deny login for password non-compliance

FIPS

FIPS compliance OFF

Minimum password length of - Requires that password contain the minimum number of defined characters.

Minimum password age of - Sets a minimum to the number of hours at which passwords may be changed. Administrators will be able to change passwords regardless of this setting.

Maximum password age of - Requires that user passwords be changed before reaching maximum password age. This option can be overridden at the user level by enabling the `Ignore password aging rules` option.

Email password change reminder - Emails a password change reminder to the email address associated with user the defined number of days before password reaches maximum password age. To function correctly an SMTP server must be configured under `Settings > Email` in JSCAPE MFT Server Manager. Note, email reminders are sent daily, approximately 10 minutes after start of JSCAPE MFT Server and every 24 hours thereafter.

Password must not match previous - Requires that new passwords must not match the defined number of previous passwords.

Require password reset on first time login - Requires new users to reset their passwords the first time they login.

Deny login for password non-compliance - If enabled, user password will be verified at time of login to check that it meets compliance requirements. If it matches user password but does not meet compliance requirements then user will be denied login.

Required characters - Passwords must contain the selected characters.

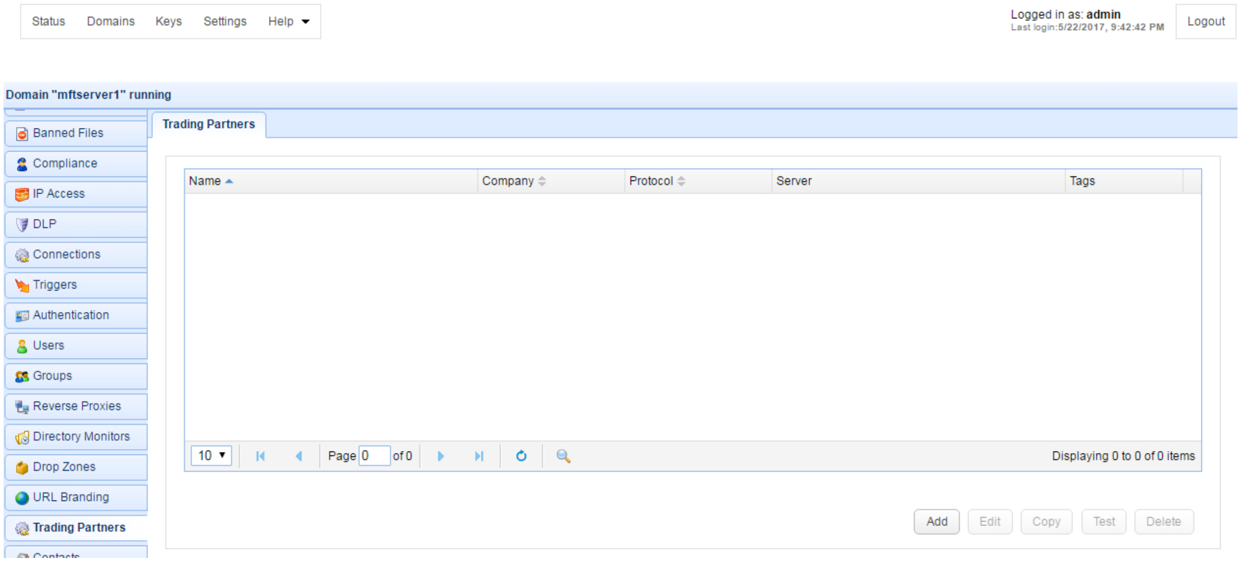
FIPS compliance - If switched ON, administrators will not be allowed to change allowed ciphers, whether through the GUI or administrative API.

Adding trading partners

A trading partner is defined as a remote service that you want to regularly exchange data with. Trading partner information may be used in triggers when performing scheduled or event based file transfers. The purpose of the trading partner module is to centralize remote host credentials so that they can be reused within trigger actions. Used properly, if a remote host changes their hostname or credentials you only need to update the trading partner details rather than update all trigger actions that depend on this host.

To add a trading partner select the `Trading Partners` node within JSCAPE MFT Server Manager and click on the `Add` button.

Figure 142


Logged in as: admin
Last login:5/22/2017, 9:42:42 PM

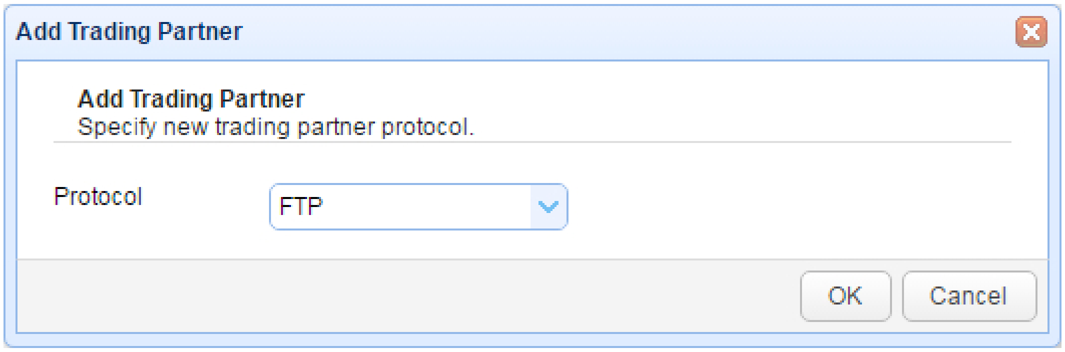
Domain "mftserver1" running

Name	Company	Protocol	Server	Tags

Displaying 0 to 0 of 0 items

Select a file transfer protocol for this trading partner.

Figure 237



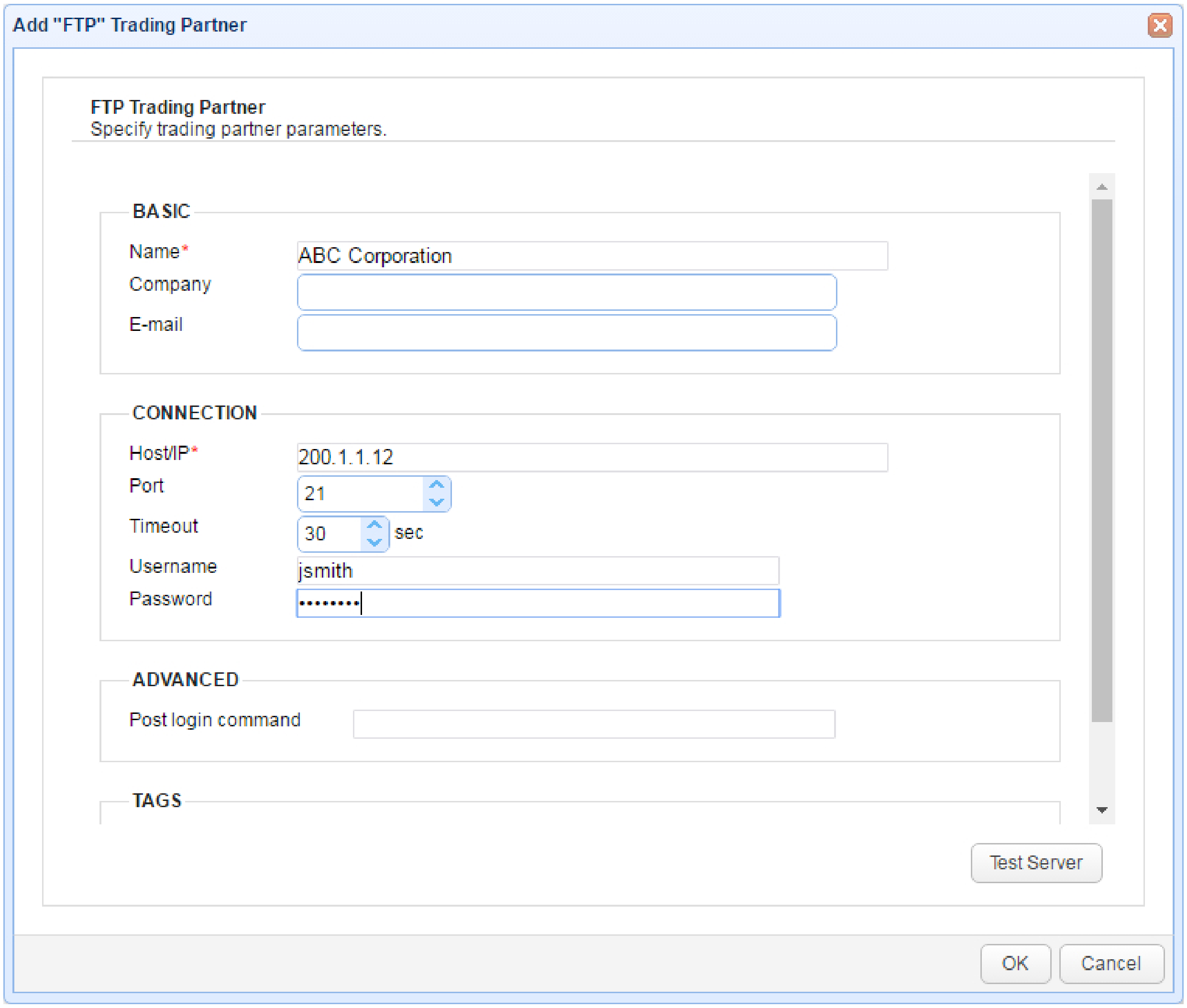
Add Trading Partner

Add Trading Partner
Specify new trading partner protocol.

Protocol: FTP

Enter pertinent details for this trading partner.

Figure 143



Add "FTP" Trading Partner

FTP Trading Partner
Specify trading partner parameters.

BASIC

Name*	ABC Corporation
Company	
E-mail	

CONNECTION

Host/IP*	200.1.1.12
Port	21
Timeout	30 sec
Username	jsmith
Password	••••••••

ADVANCED

Post login command	

TAGS

Basic

Name - A unique name to assign to this trading partner.

Company - The name of the company that this trading partner represents.

E-mail - The primary email address for this trading partner.

Connection

Details vary based on the protocol selected.

Tags

Tags - Use tags to limit which administrators have access to this trading partner.

Using trading partners in triggers

There are a number of file transfer related trigger actions that can use trading partner credentials in their work. These include the following actions.

Trading Partner Create Directory
Trading Partner Delete Directory
Trading Partner Delete File
Trading Partner Directory Download
Trading Partner Directory Upload
Trading Partner File Download
Trading Partner File Upload
Trading Partner Rename File

See also

Trigger management

Monitoring server resources using JMX

The JMX service included with JSCAPE MFT Server allows you to more closely monitor usage of CPU and memory resources. It is meant to be used with a Java profiling application such as VisualVM.

Connecting via JMX

In order to connect via JMX you will need to provide a connection URL. Please use the format provided below.

```
service:jmx:rmi://[hostname]:[serverport]/jndi/rmi://[hostname]:
[registryport]/server
```

where `[hostname]` and `[port]` are the hostname and port that JMX service is listening on. Note, if you are listening on host/IP `0.0.0.0` then you will need to replace the hostname in the URL with the actual IP address of the server. Also, it is important that when connecting remotely that both the `Server port` and `Registry port` are allowed inbound connections for any firewall.

JMX Credentials

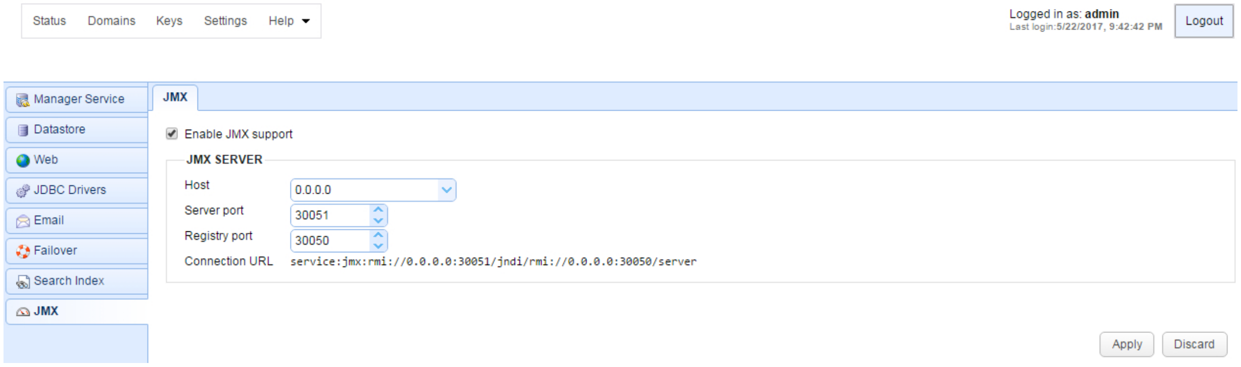
Server configuration 3

To connect via JMX you must provide valid administrator credentials. Administrators for JSCAPE MFT Server are defined in `Settings > Manager Service > Administrators` in JSCAPE MFT Server Manager.

Configuring JMX

The JMX service may be configured in `Settings > JMX` in JSCAPE MFT Server Manager.

Figure 157



☑ Enable JMX support

JMX SERVER

Host: 0.0.0.0

Server port: 30051

Registry port: 30050

Connection URL: `service:jmx:rmi://0.0.0.0:30051/jndi/rmi://0.0.0.0:30050/server`

Performing backups of server configuration data

It is recommended that you perform a regularly scheduled backup of your JSCAPE MFT Server configuration and user files. This may be performed using the `System Configuration Backup` action as part of a trigger.

Manual Backup

To perform a manual backup of JSCAPE MFT Server create a ZIP archive of the JSCAPE MFT Server installation directory. This archive may be used for disaster recovery purposes.

Automatic Backup

1. Using JSCAPE MFT Server Manager create a trigger that uses the `Current Time` event. When specifying the `Condition` use a time expression to set the time(s) of day that you would like the trigger to run.
2. When prompted to select the action, select the `System Configuration Backup` action and populate the required fields.
3. Click `OK` and `Apply` to save the trigger.
4. Select the trigger and click `Run` to verify that the backup archive is created successfully. This archive may be used for disaster recovery purposes.

See also

Backing up server configuration files

AS2 (Applicability Statement 2) 4

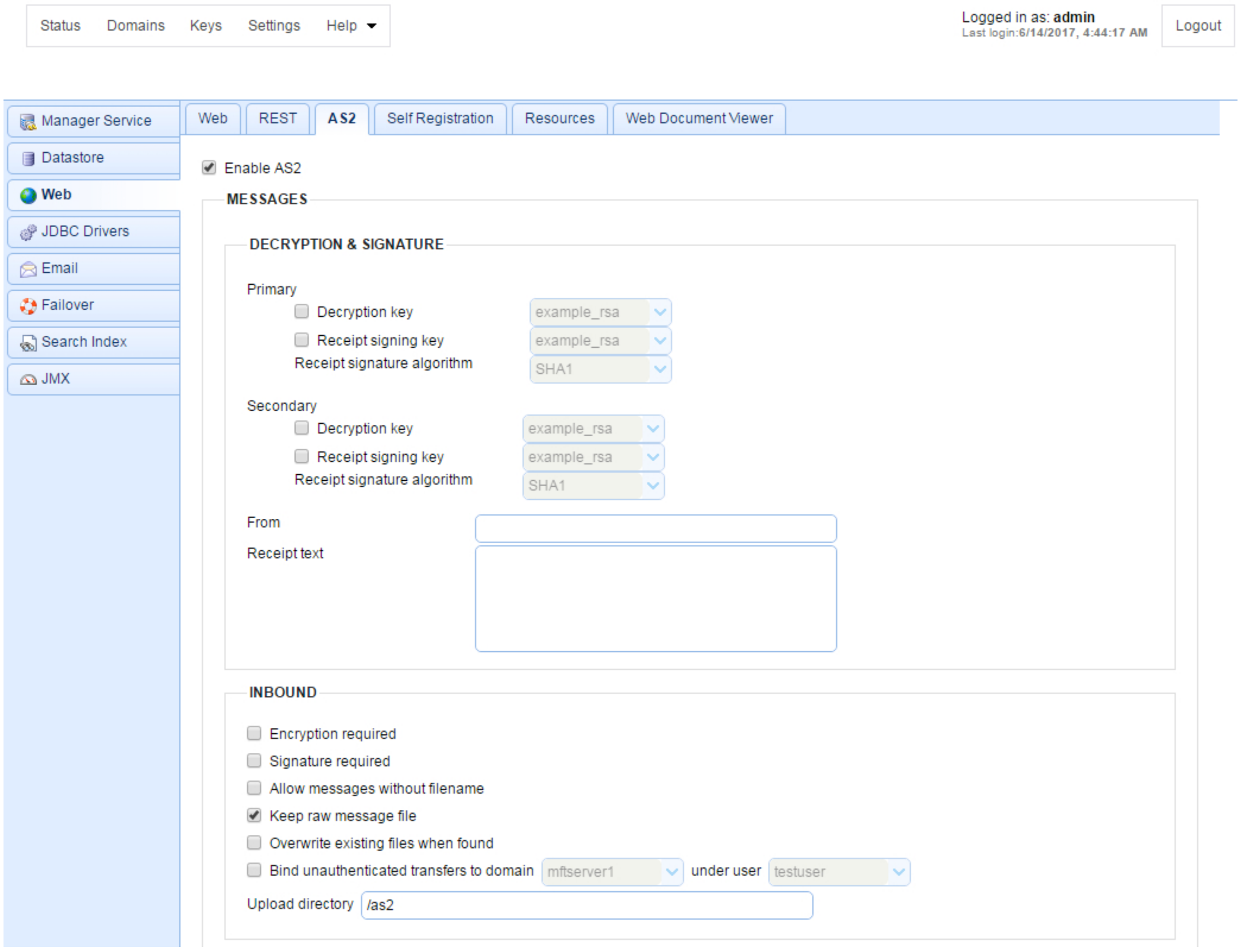
Overview

AS2 (Applicability Statement 2) is a specification for sending messages securely and reliably using HTTP/S. JSCAPE MFT Server provides support for both sending and receiving AS2 messages and is a Drummond Certified ™ product.

Enabling AS2

AS2 runs over HTTP/S. In order to enable AS2 you must first enable the HTTP/S service(s) in JSCAPE MFT Server. See [Enabling web based file transfers](). To enable AS2 go to `Settings > Web > AS2` panel in JSCAPE MFT Server Manager, check the `Enable AS2` option and set the required parameters.

Figure 165



☑ Enable AS2

MESSAGES

DECRYPTION & SIGNATURE

Primary

☐ Decryption key: example_rsa

☐ Receipt signing key: example_rsa

Receipt signature algorithm: SHA1

Secondary

☐ Decryption key: example_rsa

☐ Receipt signing key: example_rsa

Receipt signature algorithm: SHA1

From

Receipt text

INBOUND

☐ Encryption required

☐ Signature required

☐ Allow messages without filename

☑ Keep raw message file

☐ Overwrite existing files when found

☐ Bind unauthenticated transfers to domain: mftserver1 under user: testuser

Upload directory: /as2

Enable AS2 - Check to enable receipt of AS2 messages.

Messages

Decryption & Signature

Primary Decryption key - This is the private key that will be used to decrypt AS2 messages encrypted using the corresponding public key. This key is sourced from the Server Keys panel in Key Manager.

Primary Receipt signing key - This is the private key that will be used to sign MDN receipts in response to messages decrypted using the Primary Decryption key . This key is sourced from the Server Keys panel in Key Manager.

Primary Receipt signature algorithm - This is the message signing algorithm used when sending MDN receipts using the Primary receipt signing key.

Secondary Decryption key - This is the private key that will be used to decrypt AS2 messages encrypted using the corresponding public key. This key is sourced from the Server Keys panel in Key Manager.

Secondary Receipt signing key - This is the private key that will be used to sign MDN receipts in response to messages decrypted using the Secondary Decryption key . This key is sourced from the Server Keys panel in Key Manager.

Secondary Receipt signature algorithm - This is the message signing algorithm used when sending MDN receipts using the Secondary receipt signing key.

From - The From header used when sending MDN receipts.

Receipt text - Additional information to include in AS2 receipts.

Inbound

Encryption required - If checked all incoming AS2 messages must be encrypted.

Signature required - If checked all incoming AS2 messages must be signed.

Allow messages without filename - If checked incoming AS2 messages may optionally have a filename attribute. If no filename attribute is provided a unique timestamp based filename will be automatically generated. If unchecked AS2 messages must have a filename attribute.

Keep raw message file - If checked, AS2 messages will be stored in their raw format under `var/as2/incoming` and `var/as2/outgoing` directories. This can be useful for debugging purposes, however if this directory is left to grow it may impact overall system performance.

Overwrite existing files when found - If checked and file already exists with matching filename attribute then file will be overwritten. If unchecked and file already exists AS2 message will be rejected.

Bind unauthenticated transfers to domain X under user Y - If checked, incoming AS2 messages that do not include user credentials will be mapped to the specified domain and user. If unchecked then all incoming AS2 messages **MUST** include user credentials.

Upload directory - The directory relative to users root directory where AS2 message data will be stored.

Receiving AS2 messages

In order to receive AS2 messages you **MUST** first enable the AS2 service both in `Settings > Web > AS2` (See Enabling AS2) and in the Services module (See Adding services). Additionally you **MUST** create an AS2 trading partner with a `To ID` value that is equal to the incoming `As2From` header for the incoming AS2 message. See Adding trading partners. This ensures that the trading partner is a known and trusted connection. When receiving an AS2 message JSCAPE MFT Server will iterate through available AS2 trading partners to identify a match. If no matching trading partner is found then the AS2 message will be rejected.

Lastly, you must provide connection parameters for JSCAPE MFT Server to your trading partners. A guide to these parameters has been provided below.

Connection Parameters

URL

```
http[s]://hostname[:port]/as2/incoming/
```

where hostname is the hostname or IP address and port is the port as set in Settings > Web panel of JSCAPE MFT Server Manager.

e.g.

https://192.168.1.1:443/as2/incoming/

Username

username@domain

where username is the user Login and domain is the JSCAPE MFT Server domain to which the user belongs. In the event that you are using the `Bind unauthenticated transfers to user` option in the `Settings > Web > AS2` panel then your trading partner may connect without supplying any credentials.

e.g.

test@localhost

Password

The password for the specified username. In the event that you are using the `Bind unauthenticated transfers to user` option in the `Settings > Web > AS2` panel then your trading partner may connect without supplying any credentials.

e.g.

secret

From ID

This can be any value that uniquely identifies where the AS2 message is coming from.

e.g.

MyTradingPartner

To ID

This can be any value that uniquely identifies where the AS2 message is being sent to.

e.g.

Encryption key

If message encryption is used then message should be encrypted with recipients public key.

Signing key

If message signing is used then message should be signed with senders private key.

MDN receipt

Both synchronous and asynchronous modes are supported.

Processing AS2 messages

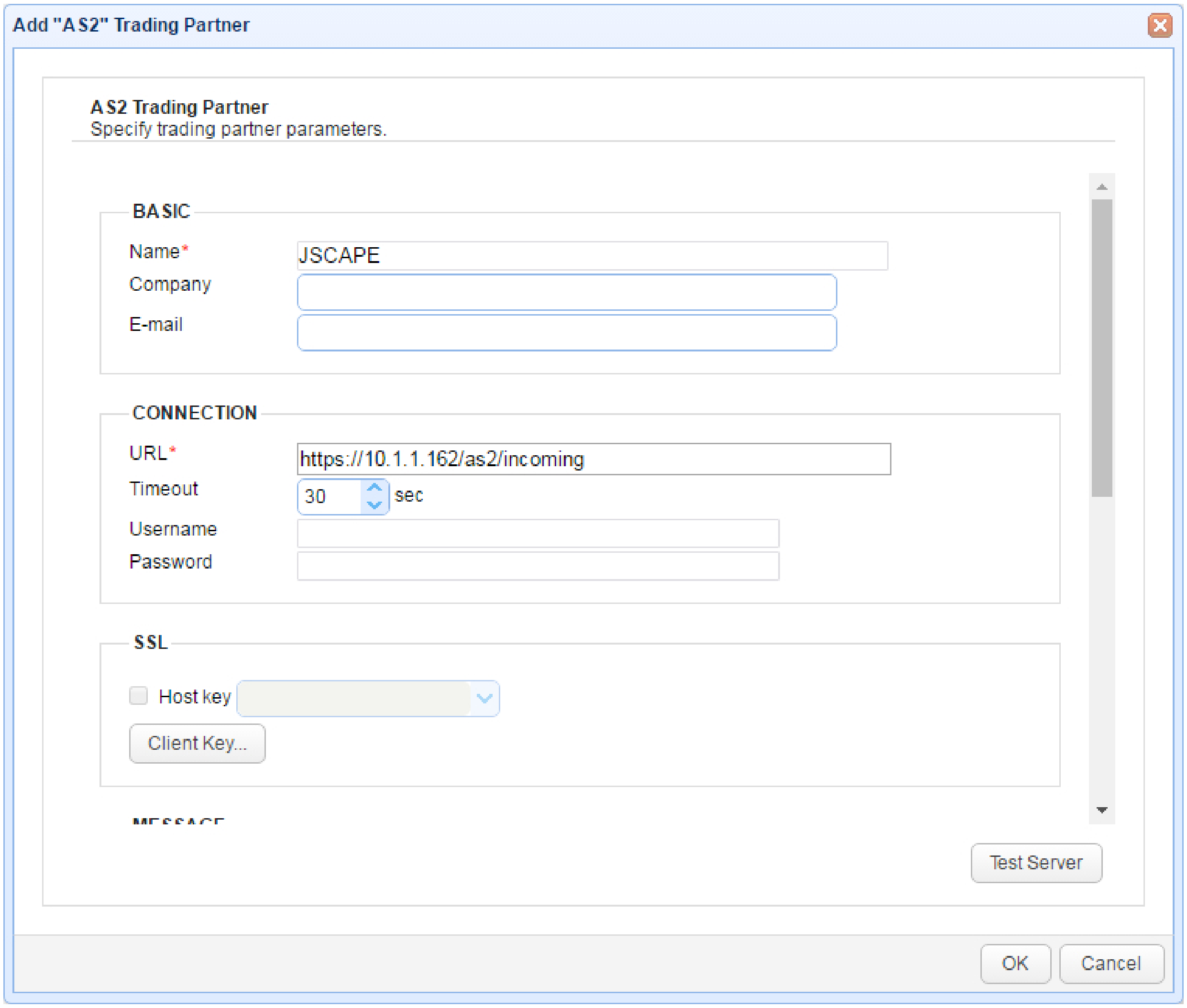
As AS2 messages are received they will be processed according to the settings in the `Settings > Web > AS2` panel. AS2 message data will be stored in the `Upload directory` (See `Settings > Web > AS2`) relative to users root directory. A history of all AS2 messages can be seen in the AS2 Messages module for your domain.

Sending AS2 messages

In order to send an AS2 message you must first create an AS2 trading partner. See Adding trading partners. See *Figure 166* below for an example AS2 trading partner. In this example the trading partner is another instance of JSCAPE MFT Server. AS2 messages may be sent manually from the `AS2 Messages` module or automatically in response to server events using the `Triggers` module and related actions.

Creating an AS2 Trading Partner

Figure 166



Add "AS2" Trading Partner

AS2 Trading Partner
Specify trading partner parameters.

BASIC

Name* JSCAPE

Company

E-mail

CONNECTION

URL* https://10.1.1.162/as2/incoming

Timeout 30 sec

Username

Password

SSL

□ Host key

Connection

URL - The URL of AS2 HTTP/S service.

Timeout - The timeout in seconds for establishing a connection to AS2 service.

Username - The optional username to use when logging into AS2 service. Credentials will be submitted using HTTP basic authentication. Note, when connecting to an instance of JSCAPE MFT Server running AS2 service you must provide credentials with username in the form of `username@domain`, unless the `Bind unauthenticated transfers to user` option is checked in `Settings > Web > AS2` for which no credentials are required.

Password - The optional password to use when logging into AS2 service.

SSL

Host key - The host key to use when validating HTTPS certificate of server. This key is sourced from Host Keys tab in Key Manager.

Client key - The client key to use when authenticating with HTTPS server.

Message

From ID - This can be any alpha-numeric value (no spaces) that uniquely identifies where the AS2 message is coming from.

To ID - This can be any alpha-numeric value (no spaces) that uniquely identifies where the AS2 message is being sent to.

Receipt - The method of MDN receipt. Both synchronous and asynchronous modes are supported. In synchronous mode JSCAPE MFT Server will send the AS2 message and read the MDN receipt in a single connection. In asynchronous mode JSCAPE MFT Server will send the AS2 message along with instructions to the recipient on where to send the MDN receipt once the AS2 message is processed. Asynchronous MDN receipts are sent to JSCAPE MFT Server over HTTP/S via the URL `http(s)://[host]:[port]/as2/receipts` where `[host]` and `[port]` are the IP address and port that the JSCAPE MFT Server AS2 service is listening on. * Note, when using asynchronous mode it is important that the IP address that your AS2 service is listening on is publicly available. If for example you are using the special address `0.0.0.0` or an internal NAT address then you will need to instruct JSCAPE MFT Server to use a different address when sending out asynchronous MDN URL, otherwise the recipient may not be able to post the MDN receipt. This can be achieved in `Settings > Web > Server name`, setting this value to the public IP address or hostname of your JSCAPE MFT Server instance.

Prefer HTTPS receipt delivery URL - If checked (default) then the URL provided for asynchronous MDN receipts will use HTTPS service if available.

Receipt signature required - If checked then recipient must respond with an MDN receipt.

Receipt timeout - The timeout for receiving an MDN receipt. This applies to synchronous mode only.

Encryption key - The public key/certificate to use for encrypting AS2 messages. This is sourced from Host Keys panel in Key Manager.

Encryption algorithm - The encryption algorithm used for encrypting AS2 messages.

Signing key - The private key to use for signing AS2 messages. This is sourced from Server Keys panel in Key Manager.

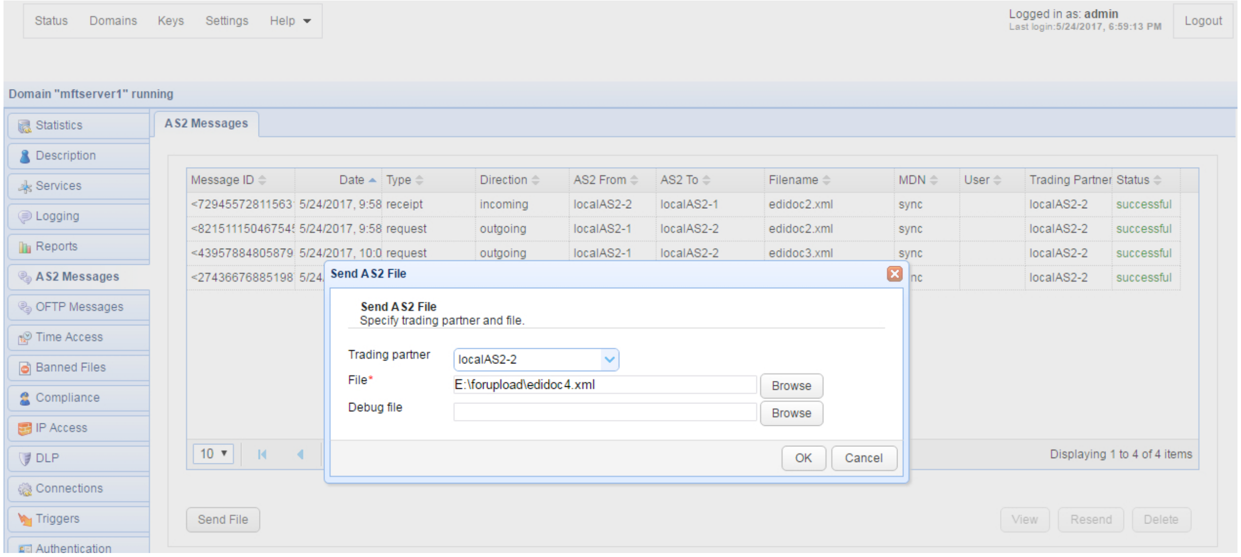
Signature algorithm - The algorithm used for signing AS2 messages.

Enable compression - If checked AS2 messages will be sent compressed.

Sending an AS2 message manually

To send an AS2 message manually go to the AS2 Messages module for your domain and click the "Send File" button. You will be prompted for the file and AS2 trading partner to send the message to.

Figure 167



Domain "mftserver1" running

Message ID	Date	Type	Direction	AS2 From	AS2 To	Filename	MDN	User	Trading Partner	Status
<72945572811563	5/24/2017, 9:58	receipt	incoming	localAS2-2	localAS2-1	edidoc2.xml	sync		localAS2-2	successful
<82151115046754	5/24/2017, 9:58	request	outgoing	localAS2-1	localAS2-2	edidoc2.xml	sync		localAS2-2	successful
<43957884805879	5/24/2017, 10:0	request	outgoing	localAS2-1	localAS2-2	edidoc3.xml	sync		localAS2-2	successful
<27436676885198	5/24,						nc		localAS2-2	successful

Send AS2 File

Send AS2 File
Specify trading partner and file.

Trading partner: localAS2-2
File*: E:\forupload\edidoc4.xml [Browse]
Debug file: [Browse]

[OK] [Cancel]

Trading partner - The AS2 trading partner to send file to.

File - The file to send.

Debug file - Optional debug file useful in troubleshooting AS2 connections.

Sending an AS2 message automatically

You can send an AS2 message automatically in response to server events using the `Triggers` module and the `Trading Partner File Upload` or `Trading Partner Regex File Upload` actions. See Triggers.

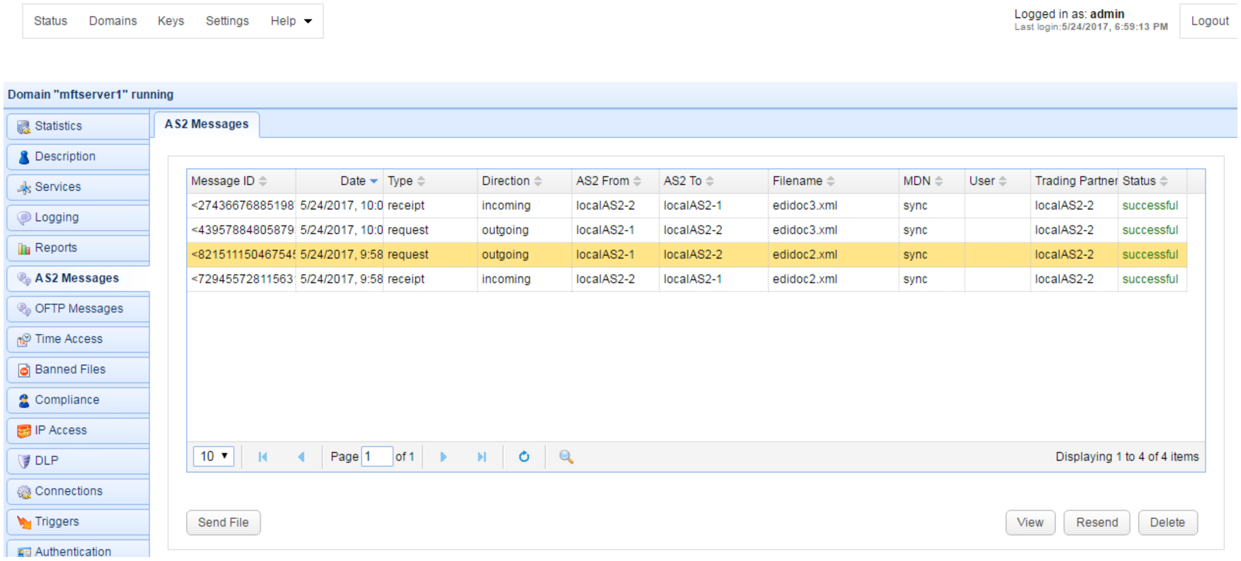
Resending an AS2 message

To manually resend an AS2 message, select the desired message from the AS2 Messages module and click the `Resend` button. Note, only messages of type `request` may be resent.

Viewing AS2 messages

A history of all AS2 messages sent and received for a domain can be found in the `AS2 Messages` module in JSCAPE MFT Server Manager.

Figure 168

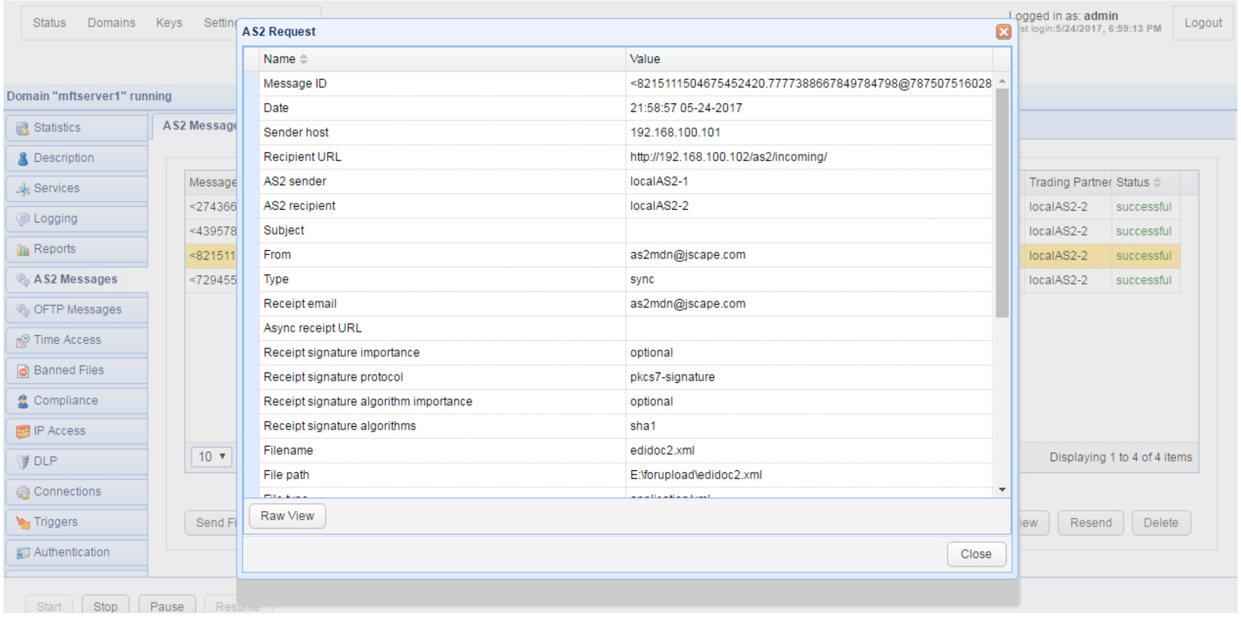


Message ID	Date	Type	Direction	AS2 From	AS2 To	Filename	MDN	User	Trading Partner	Status
<27436676885198	5/24/2017, 10:0	receipt	incoming	localAS2-2	localAS2-1	edidoc3.xml	sync		localAS2-2	successful
<43957884805879	5/24/2017, 10:0	request	outgoing	localAS2-1	localAS2-2	edidoc3.xml	sync		localAS2-2	successful
<82151115046754!	5/24/2017, 9:58	request	outgoing	localAS2-1	localAS2-2	edidoc2.xml	sync		localAS2-2	successful
<72945572811563	5/24/2017, 9:58	receipt	incoming	localAS2-2	localAS2-1	edidoc2.xml	sync		localAS2-2	successful

View AS2 message details

To view the details of any AS2 message, select the desired message and click the `View` button.

Figure 169



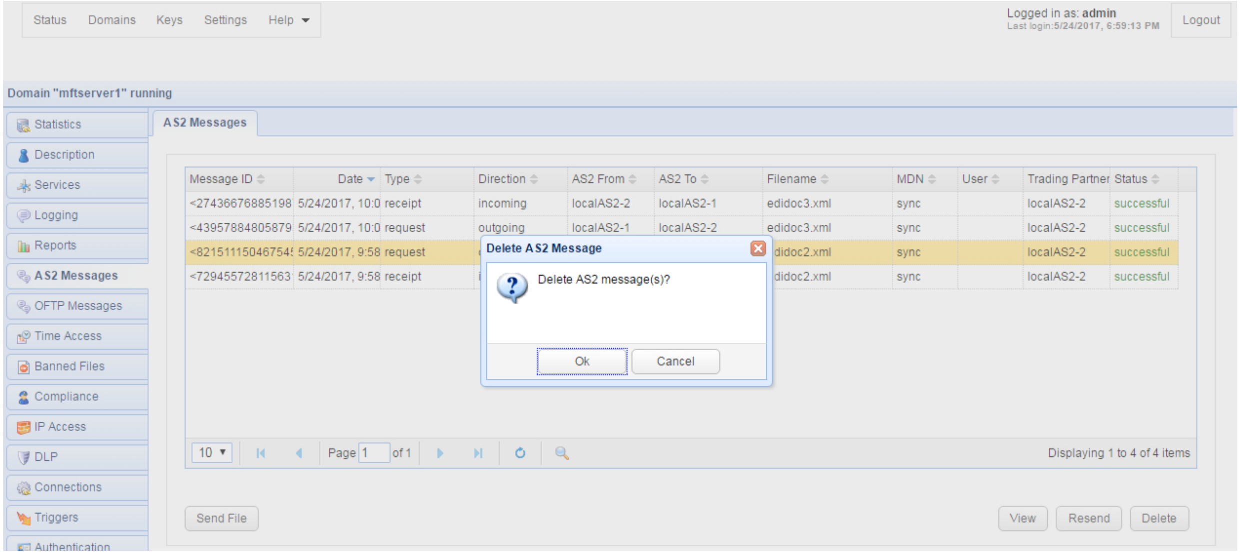
Name	Value
Message ID	<8215111504675452420.7777388667849784798@787507516028
Date	21:58:57 05-24-2017
Sender host	192.168.100.101
Recipient URL	http://192.168.100.102/as2/incoming/
AS2 sender	localAS2-1
AS2 recipient	localAS2-2
Subject	
From	as2mdn@jscape.com
Type	sync
Receipt email	as2mdn@jscape.com
Async receipt URL	
Receipt signature importance	optional
Receipt signature protocol	pkcs7-signature
Receipt signature algorithm importance	optional
Receipt signature algorithms	sha1
Filename	edidoc2.xml
File path	E:\forupload\edidoc2.xml

Deleting AS2 messages

You may wish to delete/purge AS2 messages from your system in order to save storage space. To do so, select the desired messages you wish to delete (hold shift key to select multiple message) and click the `Delete` button. A confirmation dialog will be displayed asking you to confirm deletion.

Figure 170

AS2 (Applicability Statement 2)



Domain "mftserver1" running

Message ID	Date	Type	Direction	AS2 From	AS2 To	Filename	MDN	User	Trading Partner	Status
<27436676885198	5/24/2017, 10:0	receipt	incoming	localAS2-2	localAS2-1	edidoc3.xml	sync		localAS2-2	successful
<43957884805879	5/24/2017, 10:0	request	outgoing	localAS2-1	localAS2-2	edidoc3.xml	sync		localAS2-2	successful
<82151115046754	5/24/2017, 9:58	request				didoc2.xml	sync		localAS2-2	successful
<72945572811563	5/24/2017, 9:58	receipt	i			didoc2.xml	sync		localAS2-2	successful

Delete AS2 Message

Delete AS2 message(s)?

Ok Cancel

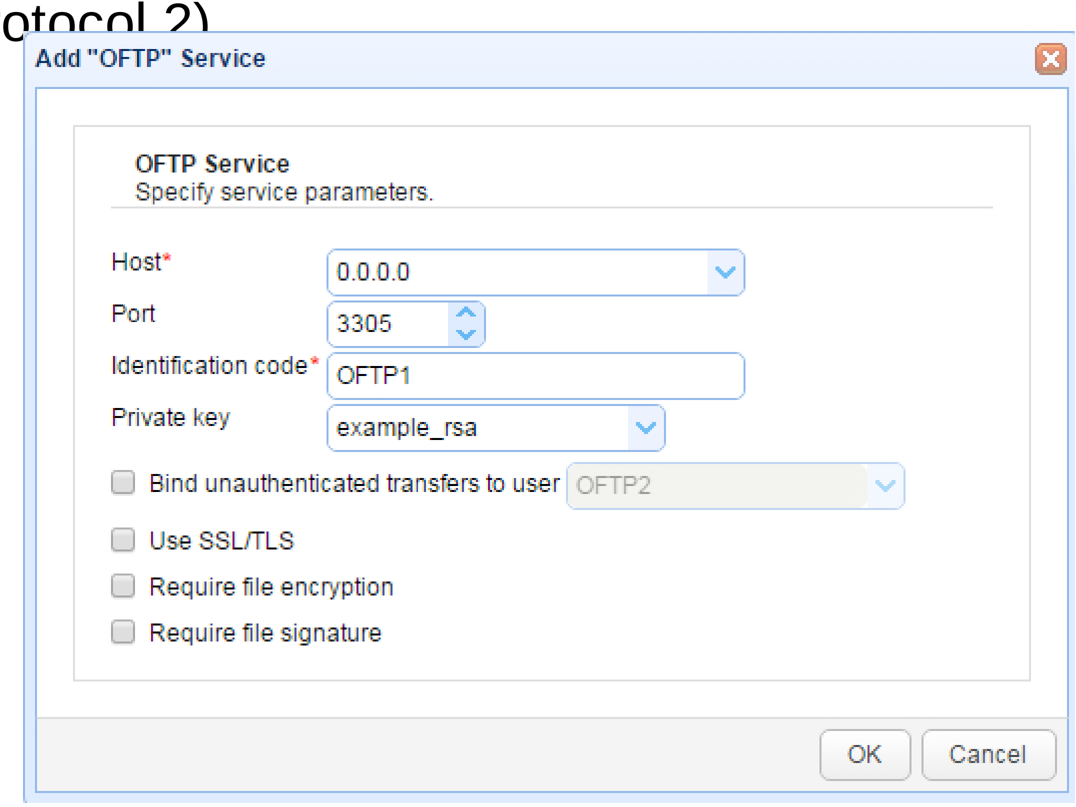
Overview

OFTP2 (Odette File Transfer Protocol 2) is a specification (RFC 5024) for securely exchanging messages between automotive companies, particularly in Europe. JSCAPE MFT Server provides support for both sending and receiving OFTP2 messages and has successfully passed interoperability testing with Odette.

Enabling OFTP2

To enable OFTP go to the `Services` module for your domain, click the `Add` button, and select `OFTP` from the protocol drop-down list (See Adding services). Enter pertinent details once the Add OFTP Service dialog is displayed.

Figure 216



Add "OFTP" Service

OFTP Service
Specify service parameters.

Host* 0.0.0.0

Port 3305

Identification code* OFTP1

Private key example_rsa

□ Bind unauthenticated transfers to user OFTP2

□ Use SSL/TLS

□ Require file encryption

□ Require file signature

Host/IP - The IP address that this service will listen on. Use the address 0.0.0.0 to listen on all available network interfaces.

Port - The port that this service will listen on.

Identification code - The code used to identify this OFTP service.

Private key - The private encryption key that this service will use for encrypted communications.

Bind unauthenticated transfers to user - If checked, binds connections made without credentials (username/password) to a specific username.

Use SSL/TLS - If checked, connections must be made securely using SSL/TLS.

Require file encryption - If checked, file transfers must be encrypted.

Require file signature - If checked, file transfers must be signed.

Receiving OFTP2 messages

In order to receive OFTP2 messages you must first enable the OFTP2 service. See Enabling OFTP2. Additionally you **MUST** create an OFTP trading partner with a `Destination ID` value that is equal to the incoming `InitiatorIdentificationCode` header for the incoming OFTP2 message. See Adding trading partners. This ensures that the trading partner is a known and trusted connection. When receiving an OFTP2 message JSCAPE MFT Server will iterate through available OFTP trading partners to identify a match. If no matching trading partner is found then the OFTP2 message will be rejected.

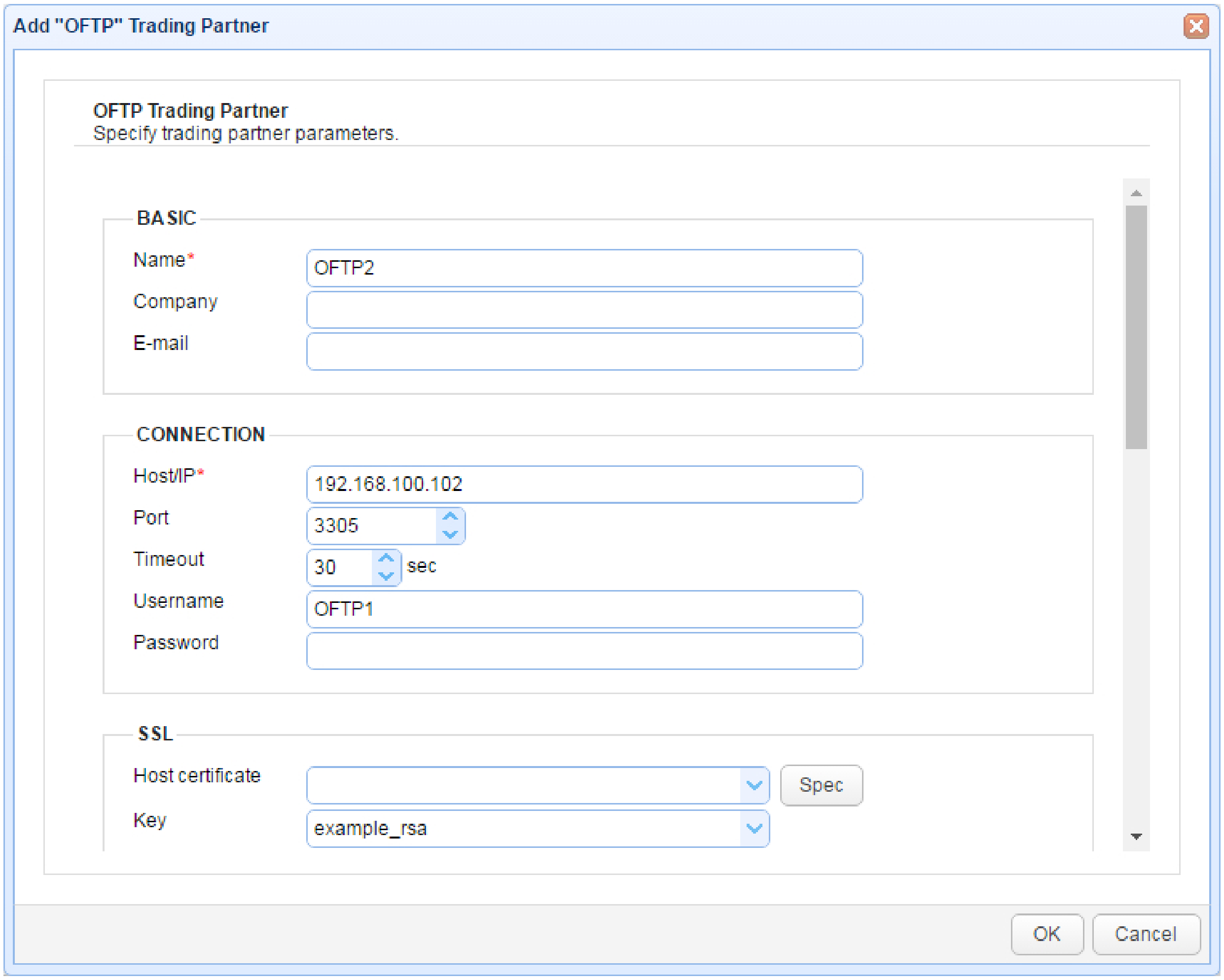
Lastly, you must provide connection parameters for JSCAPE MFT Server to your trading partners. The parameters needed will vary depending on the OFTP2 vendor software, however a list of available parameters may be found in Sending OFTP2 messages.

Sending OFTP2 messages

In order to send an OFTP2 message you must first create an OFTP trading partner. See Adding trading partners. See *Figure 225* below for an example OFTP trading partner. OFTP2 messages may be sent manually from the `OFTP Messages` module or automatically in response to server events using the `Triggers` module and related actions.

Creating an OFTP Trading Partner

Figure 225



Add "OFTP" Trading Partner

OFTP Trading Partner
Specify trading partner parameters.

BASIC

Name*	OFTP2
Company	
E-mail	

CONNECTION

Host/IP*	192.168.100.102
Port	3305
Timeout	30 sec
Username	OFTP1
Password	

SSL

Host certificate	
Key	example_rsa

Basic

Name - A unique name identifying this trading partner.

Company - Company name for this trading partner.

Email - Email address for this trading partner.

OFTP2 (ODETTE File Transfer Protocol 2)

5

Connection

Connection

Host/IP - The hostname or IP address of the OFTP service.

Port - The port of the OFTP service.

Timeout - The timeout in seconds for establishing a connection to OFTP service.

Username - The username to use when logging into OFTP service.

Password - The password to use when logging into OFTP service.

SSL

Host certificate - The host certificate to use when validating SSL certificate of server. This key is sourced from Host Keys tab in Key Manager. Empty value indicates that any host certificate will be trusted.

Client key - The client key to use when authenticating with SSL service. This key is sourced from the Server Keys tab in Key Manager.

Advanced

Destination ID - The trading partner OFTP ID.

Authentication certificate - The peer certificate used for OFTP secure authentication operation. This certificate is sourced from Client Keys in Key Manager.

Authentication key - The private key used in secure authentication operation. This key is sourced from Server Keys in Key Manager.

File encryption certificate - The peer certificate used for encrypting outbound files sent to this trading partner. This certificate is sourced from Client Keys in Key Manager.

File decryption key - The private key used for decrypting files received from this trading partner. This key is sourced from Server Keys in Key Manager.

File signing key - The private key used for signing outbound files sent to this trading partner. This key is sourced from Server Keys in Key Manager.

File signature verification certificate - The peer certificate used for verifying signature of inbound files received from this trading partner. This certificate is sourced from Client Keys in Key Manager.

Receipt signing key - The private key used for signing outbound receipts sent to this trading partner. This key is sourced from Server Keys in Key Manager.

Receipt signature verification certificate - The peer certificate used for signature verification of inbound receipts received from this trading partner. This certificate is sourced from Client Keys in Key Manager.

Cipher suite - The cipher suite name used for outbound file encryption.

Enable SSL - Enables SSL protection for this trading partner connection.

Enable secure authentication - Enables OFTP secure authentication phase during protocol handshake. See Authentication certificate and Authentication key options.

Enable file compression - Enables outbound file compression.

Enable file encryption - Enables outbound file encryption.

Enable file signing - Enables outbound file signing.

Automatically generate receipt in server mode - Enables automatic receipt generation for incoming files in server mode. Disabling this option allows for generation of receipts manually.

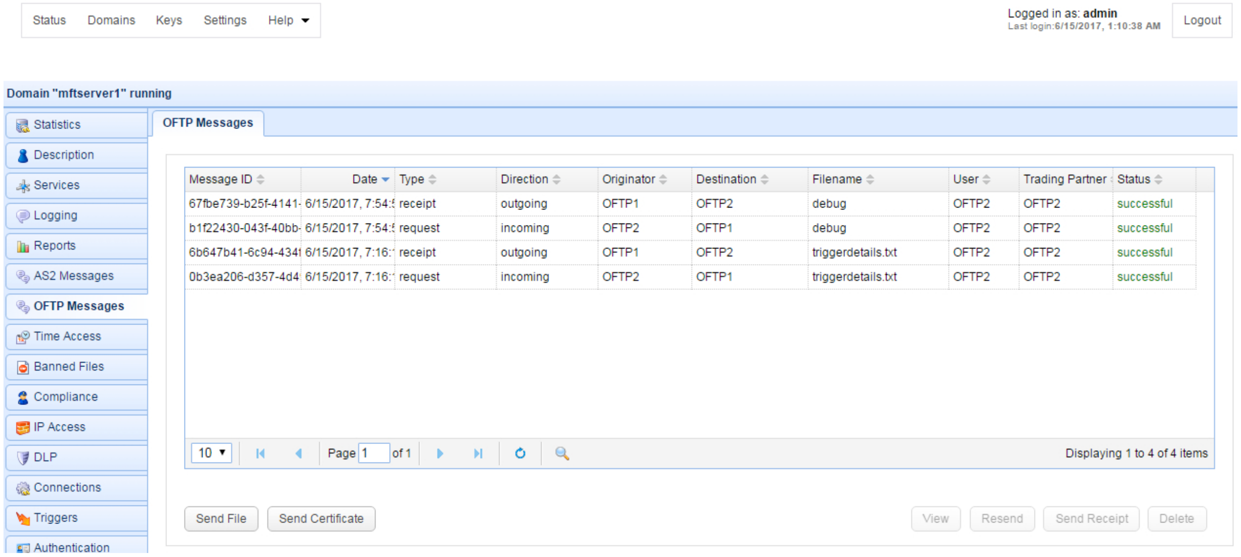
Allow certificate exchange - Allows OFTP certificate exchange procedure with this partner. Disabling this option will reject any incoming certificate exchange requests for this partner.

Allow relay - Allows for receiving of files from this partner with destination OFTP ID that is different from the local OFTP ID. Files received under these conditions will not be placed to the local virtual file system but will be forwarded to the final target destination when the opportunity presents itself.

Viewing OFTP2 messages

To view an OFTP2 message navigate to the `OFTP Messages` module for the desired domain. Select the desired message and click the `View` button.

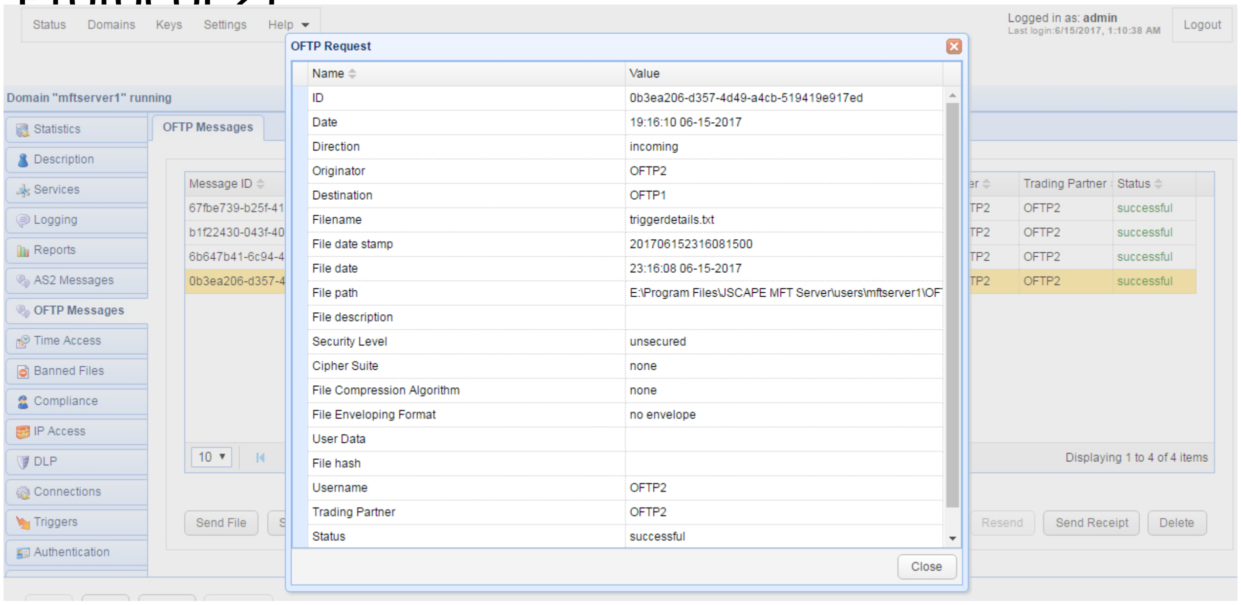
Figure 222



Message ID	Date	Type	Direction	Originator	Destination	Filename	User	Trading Partner	Status
67fbe739-b25f-4141-	6/15/2017, 7:54:5	receipt	outgoing	OFTP1	OFTP2	debug	OFTP2	OFTP2	successful
b1f22430-043f-40bb-	6/15/2017, 7:54:5	request	incoming	OFTP2	OFTP1	debug	OFTP2	OFTP2	successful
6b647b41-6c94-434	6/15/2017, 7:16:	receipt	outgoing	OFTP1	OFTP2	triggerdetails.txt	OFTP2	OFTP2	successful
0b3ea206-d357-4d4	6/15/2017, 7:16:	request	incoming	OFTP2	OFTP1	triggerdetails.txt	OFTP2	OFTP2	successful

Figure 223

OFTP2 (ODETTE File Transfer Protocol 2)



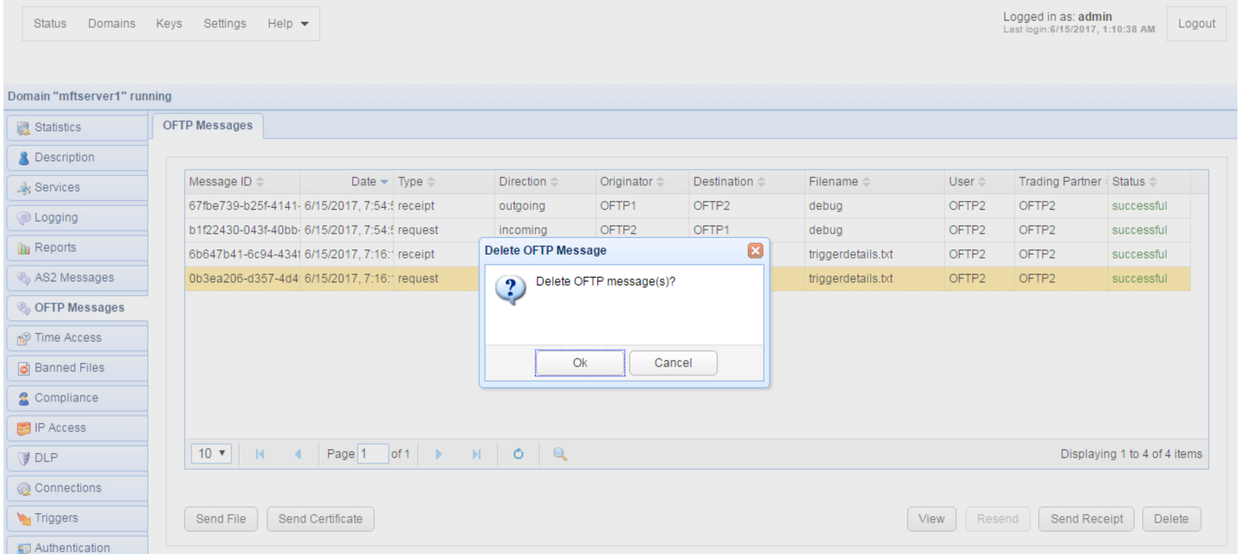
OFTP Request

Name	Value
ID	0b3ea206-d357-4d49-a4cb-519419e917ed
Date	19:16:10 06-15-2017
Direction	incoming
Originator	OFTP2
Destination	OFTP1
Filename	triggerdetails.txt
File date stamp	20170615231608150O
File date	23:16:08 06-15-2017
File path	E:\Program Files\JSCAPE MFT Server\users\mftserver1\OF
File description	
Security Level	unsecured
Cipher Suite	none
File Compression Algorithm	none
File Enveloping Format	no envelope
User Data	
File hash	
Username	OFTP2
Trading Partner	OFTP2
Status	successful

Deleting OFTP2 messages

You may wish to delete/purge OFTP2 messages from your system in order to save storage space. To do so, select the desired messages you wish to delete (hold shift key to select multiple message) and click the `Delete` button. A confirmation dialog will be displayed asking you to confirm deletion.

Figure 224



Message ID	Date	Type	Direction	Originator	Destination	Filename	User	Trading Partner	Status
67fbe739-b25f-4141-	6/15/2017, 7:54:5	receipt	outgoing	OFTP1	OFTP2	debug	OFTP2	OFTP2	successful
b1f22430-043f-40bb-	6/15/2017, 7:54:5	request	incoming	OFTP2	OFTP1	debug	OFTP2	OFTP2	successful
6b647b41-6c94-434	6/15/2017, 7:16:1	receipt				triggerdetails.txt	OFTP2	OFTP2	successful
0b3ea206-d357-4d4	6/15/2017, 7:16:1	request				triggerdetails.txt	OFTP2	OFTP2	successful

Delete OFTP Message

Delete OFTP message(s)?

Ok Cancel

Overview

Triggers are a very powerful feature that allow you to listen for events and respond with actions if conditions are met. For example, whenever a file is uploaded by a certain user you may wish to have this file OpenPGP encrypted and then have an email notification sent to another user within your organization with the details of this upload.

Example Uses

Automate routine file transfer tasks.

Trigger management 6

Email notification of key events.

Automate OpenPGP encryption/decryption of transferred files.

Automate compression/decompression of transferred files.

See also

Adding triggers
Using time based triggers
Manually executing time based triggers
Writing conditions
Testing conditions
Event types
Action types
Defining custom action types
File Transfer Script Language

Trigger lifecycle

To benefit fully from the use of triggers you may find it helpful to understand the lifecycle of a trigger. This is explained below.

1. Raise event

The first step in trigger lifecycle starts with an event. There are a number of events that can be listened for in a trigger. Examples of these are provided below.

`Current Time`

This event is automatically raised every minute and can be used for scheduling triggers.

`File Upload`

This event is raised anytime a file is uploaded via on of the file transfer services provided by the server.

`User Login`

This event is raised anytime a user attempts to login to the server.

For a complete list of available events please see the `Event type` field when adding or editing a trigger.

2. Identify matching triggers

The next step in the trigger lifecycle is to identify those enabled triggers that are listening for the event type raised. For example, in the case where a `File Upload` event is fired all triggers listening for the `File Upload` event will be identified.

3. Filter trigger conditions

Next in the trigger lifecycle is to filter those matching triggers even further, excluding those that do not match trigger conditions that may have been specified. To explain, each event has a set of properties that are set when the event is raised. These properties can be accessed in trigger conditions and trigger actions using event variables. For example, a trigger may choose to listen only for `File Upload` events where the login of the user that uploaded the file matches a specific value.

Example Condition

```
Username = "test"
```

Note, each event has different event variables available to it. For example, the `File Upload` event has a `LocalPath` variable that may be used to identify the absolute path of the file uploaded. This variable however is not available in the `User Login` event.

To see what variables are available for each event type please use the `Variables` button when adding a condition or the `Add Variable` button when adding an action to a trigger.

See also

Writing conditions

4. Prepare for execution

Now that triggers have been identified and filtered, the next step is to prepare for the execution of those triggers.

Each trigger may be executed in asynchronous (concurrently) or synchronous (sequentially) mode depending on the settings for the individual trigger. At this point in the lifecycle, these triggers are split into two separate queues, one for asynchronous triggers and another for synchronous triggers. Those triggers in the asynchronous queue are executed first, followed by those in the synchronous queue. Those triggers in the synchronous queue are executed in the order they are defined in the `Triggers` module of JSCAPE MFT Server. The order of execution for synchronous triggers can be controlled using the `Order` button with those triggers located at the top taking priority.

Note, depending on the optional settings in the `Triggers > Settings` panel of JSCAPE MFT Server you may limit the number of triggers that will execute concurrently. Those triggers that are waiting to be executed will have a status of `pending` in the `Triggers > Recent` panel of JSCAPE MFT Server.

5. Execute trigger

For each trigger there are one (1) or more actions to execute. These actions are executed in sequence.

In the event that an action fails a `Trigger Error` event is raised and subsequent actions will not be executed. To listen for these errors a separate trigger that listens for the `Trigger Error` event may be used. Triggers that fail execution will have a status of `failed` in the `Triggers > Recent` panel of

JSCAPE MFT Server.

Triggers that successfully execute will have a status of `completed` in the `Triggers > Recent` panel of JSCAPE MFT Server.

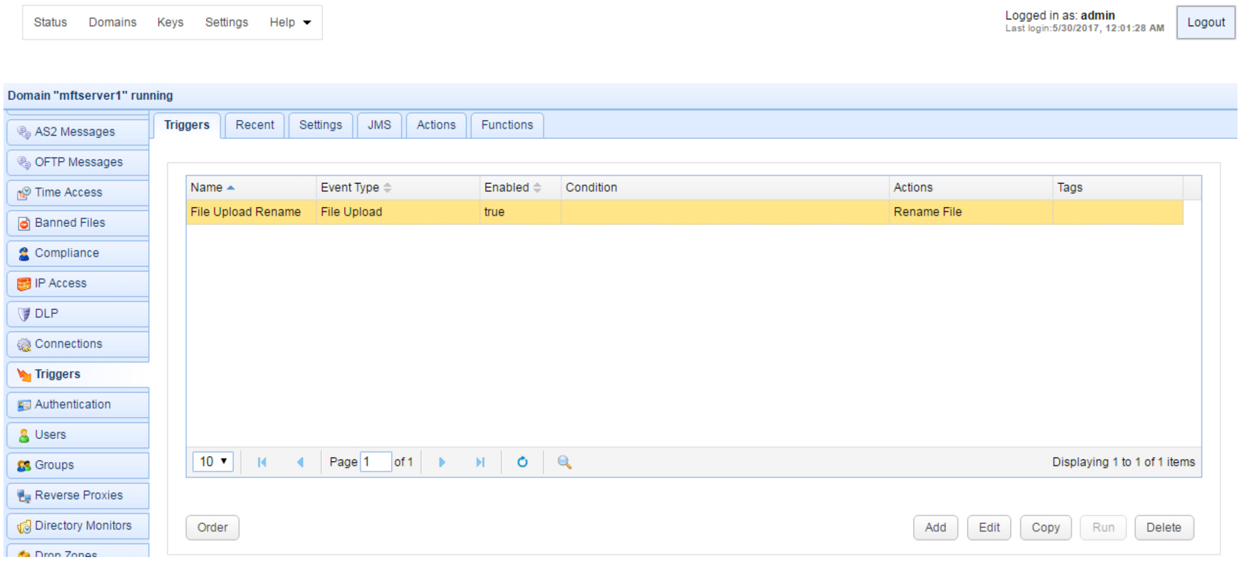
6. Log results

The full lifecycle of a trigger is written to the server log for historical and auditing purposes. You may also view the status of the most recent one thousand (1000) triggers in the `Triggers > Recent` panel of JSCAPE MFT Server.

Adding triggers

A trigger is a method of listening for events and responding with actions based on whether conditions are met. To view a list of triggers click on the `Triggers` node for the desired domain.

Figure 34



Logged in as: admin
Last login:5/30/2017, 12:01:28 AM

Domain "mftserver1" running

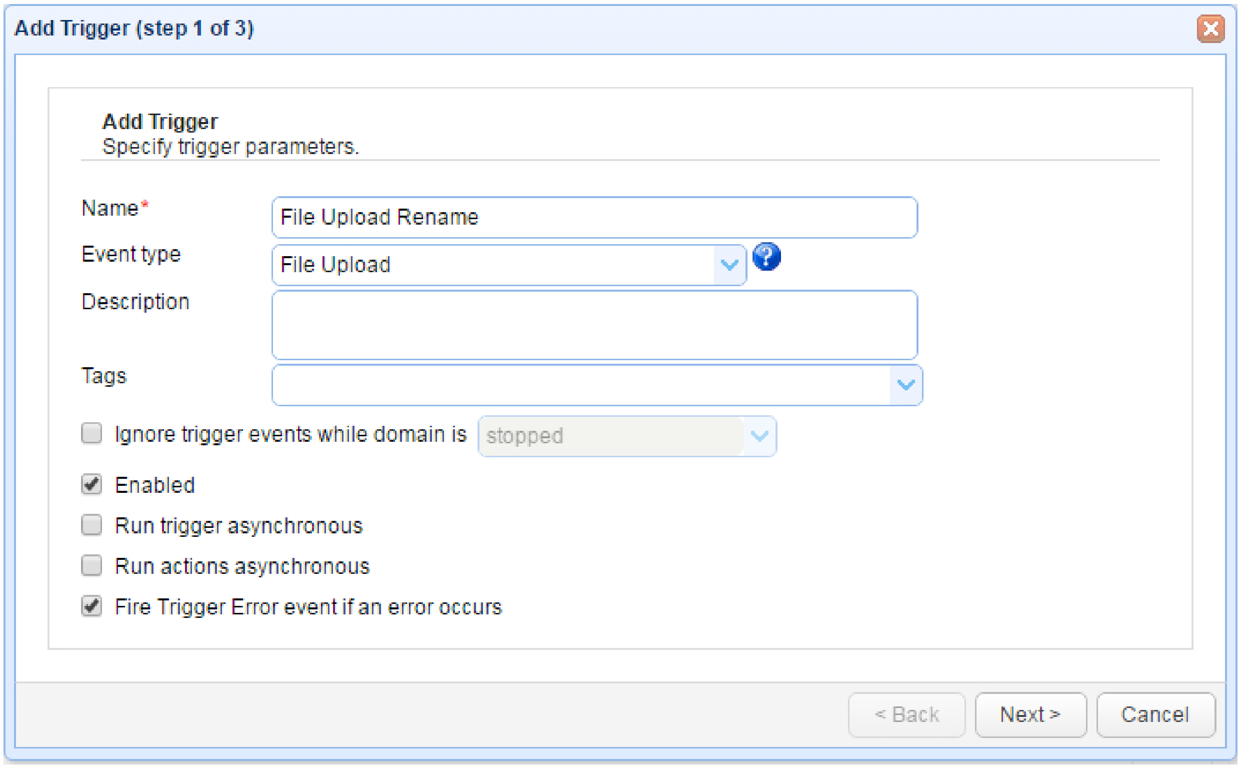
Name	Event Type	Enabled	Condition	Actions	Tags
File Upload Rename	File Upload	true		Rename File	

Displaying 1 to 1 of 1 items

To add a trigger click on the `Add` button in the lower right corner. The `Add Trigger` wizard will be displayed.

Figure 35

Trigger management 6



Add Trigger (step 1 of 3)

Add Trigger
Specify trigger parameters.

Name*	File Upload Rename
Event type	File Upload
Description	
Tags	

☐ Ignore trigger events while domain is stopped

☑ Enabled

☐ Run trigger asynchronous

☐ Run actions asynchronous

☑ Fire Trigger Error event if an error occurs

Name - A unique name identifying this trigger.

Event Type - The type of event you want to listen for.

Description - Description of this trigger.

Tags - If used, this trigger will only be visible to administrators with a system administrator flag or who have been assigned a role with specified tag.

Ignore trigger events while domain is - If checked, events will not be processed when domain is in specified state.

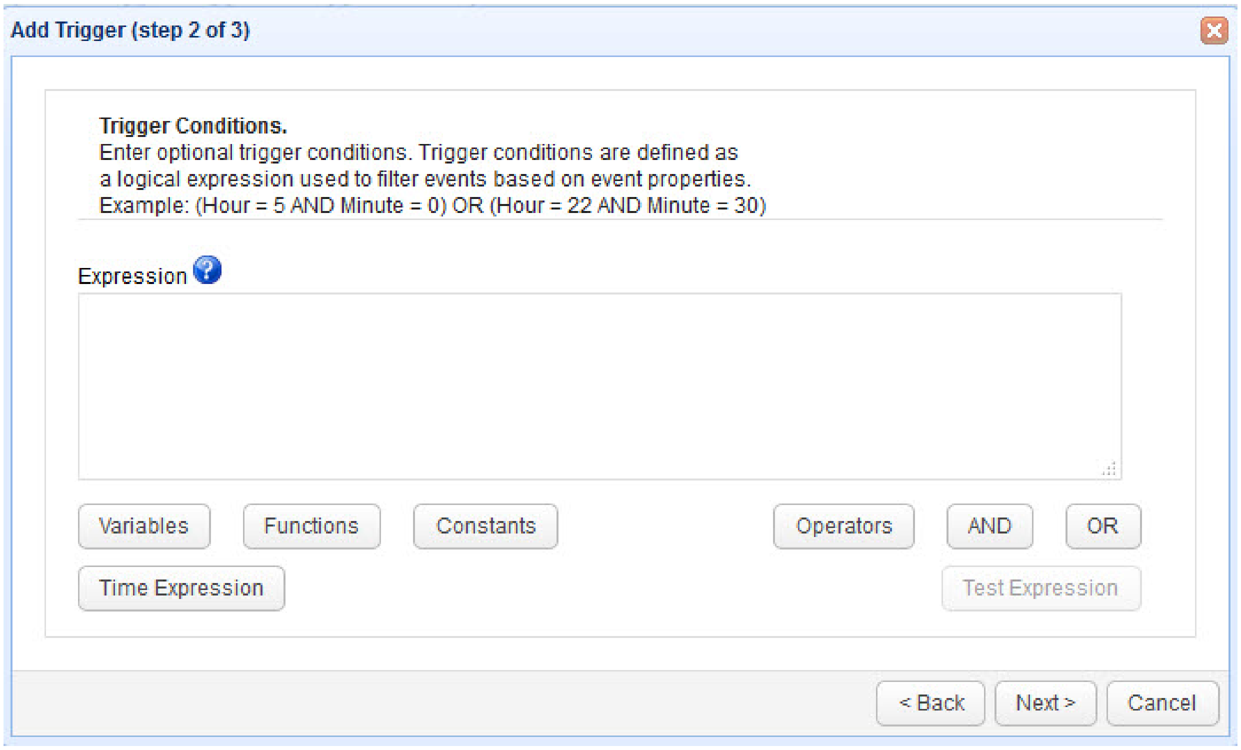
Enabled - Enables/disables trigger.

Run trigger asynchronous - If checked, trigger will be processed asynchronously.

Run actions asynchronous - If checked, trigger actions will be processed asynchronously.

Fire Trigger Error event if error occurs - If an error occurs while executing any of the actions associated with this trigger, a `Trigger Error` event will be raised. You may capture this event using a trigger that listens for the `Trigger Error` event and respond appropriately.

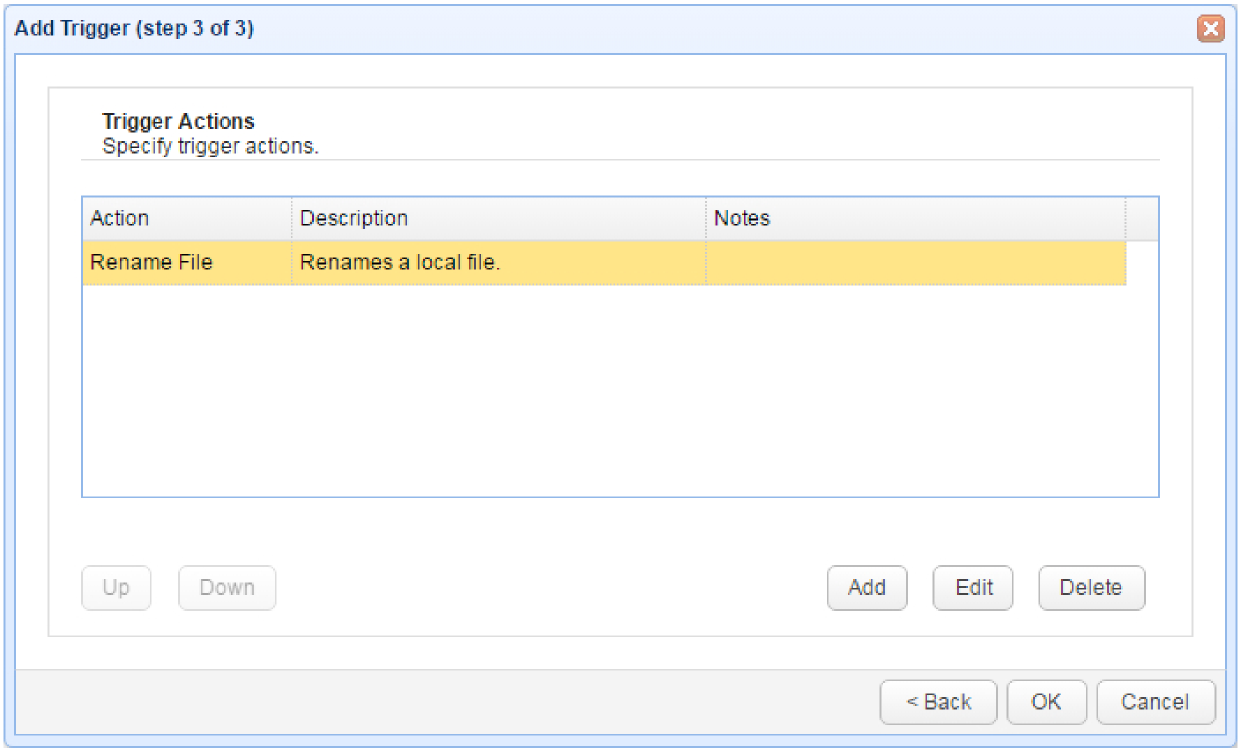
Figure 36



Add Trigger (step 2 of 3)

Trigger Conditions.
Enter optional trigger conditions. Trigger conditions are defined as a logical expression used to filter events based on event properties.
Example: (Hour = 5 AND Minute = 0) OR (Hour = 22 AND Minute = 30)

Figure 37



Add Trigger (step 3 of 3)

Trigger Actions
Specify trigger actions.

Action	Description	Notes
Rename File	Renames a local file.	

Notes - This would typically contain a description of the trigger action, which would allow the administrator to distinguish it from the rest. Descriptions may be entered in the Notes field found in the Advanced tab of each trigger action.

Trigger management 6

See also

[Event types](#)
[Action types](#)
[Function types](#)
[Defining custom action types](#)

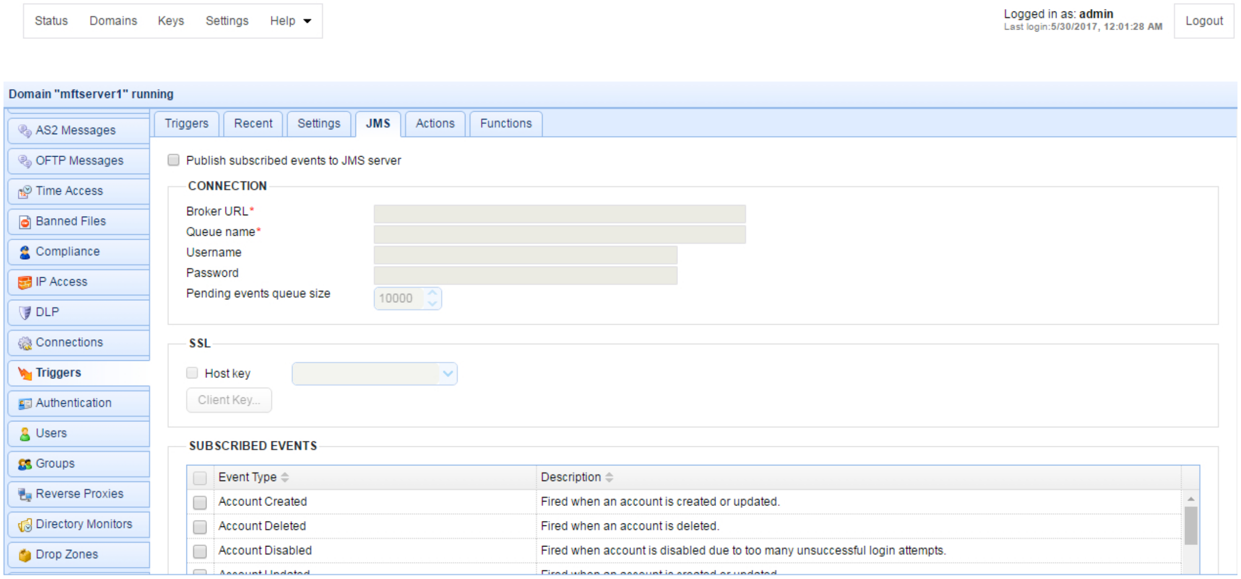
JMS

JMS (Java Message Service) may be used to publish subscribed JSCAPE MFT Server events to an external JMS message queue. This is particularly useful in cases where you want to capture an event on JSCAPE MFT Server but require that it be processed by another service.

You may choose which events you want to be published to a JMS message queue. This allows you to handle some event types locally while others may be processed by a remote JMS message queue. Note, events that are published to JMS message queue WILL NOT be processed by domain level Triggers for your instance of JSCAPE MFT Server.

To configure those events to be published to a JMS message queue select the `Triggers > JMS` pane for the desired domain.

Figure 209



Logged in as: admin
Last login:5/30/2017, 12:01:28 AM

Domain "mftserver1" running

□ Publish subscribed events to JMS server

CONNECTION

Broker URL*
Queue name*
Username
Password
Pending events queue size 10000

SSL

□ Host key

SUBSCRIBED EVENTS

□	Event Type	Description
□	Account Created	Fired when an account is created or updated.
□	Account Deleted	Fired when an account is deleted.
□	Account Disabled	Fired when account is disabled due to too many unsuccessful login attempts.
□	Account Updated	Fired when an account is created or updated.

Publish subscribed events to JMS server - If checked, subscribed events will be published to JMS server.

Connection

Broker URL - The JMS broker URL.

Queue name - The JMS queue name.

Username - The JMS service username.

Password - The JMS service password.

Pending events queue size - The maximum number of events to hold in queue for sending to JMS service.

SSL

Host key -The host key to use when verifying certificate of remote JMS service.

Subscribed events

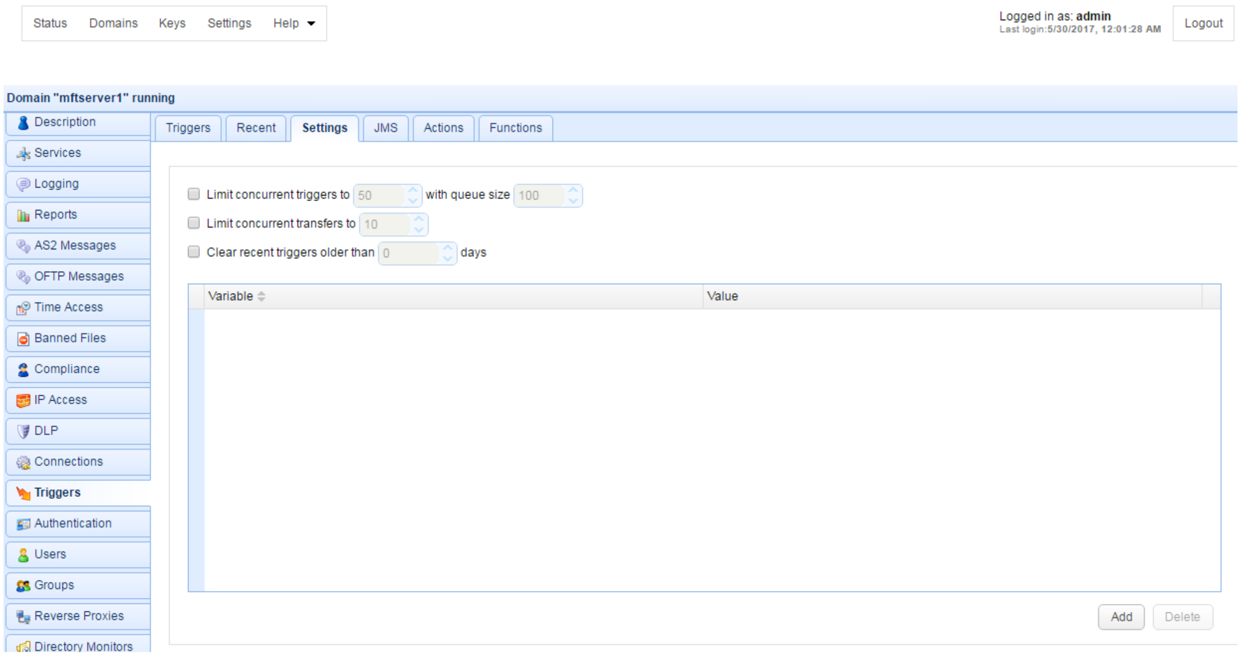
Check those event types that you would like to be published to JMS queue.

Settings

There are various settings that control how triggers are executed. These are defined in the `Triggers > Settings` panel in JSCAPE MFT Server Manager.

Limiting number of concurrent triggers
Limiting number of concurrent transfers
Automatically clearing recent trigger history
Defining global variables

Figure 139



□ Limit concurrent triggers to 50 with queue size 100
□ Limit concurrent transfers to 10
□ Clear recent triggers older than 0 days

Limiting number of concurrent triggers

You may wish to limit the number of concurrent triggers that are running in JSCAPE MFT Server. Since each trigger and it's associated actions take up a portion of memory and CPU this is useful in cases where many triggers could be running simultaneously causing your server to be overloaded. To prevent this you can optionally set the maximum number of concurrent triggers. If the maximum number of concurrent triggers is reached then triggers will be placed in a queue for later execution. If the size of the queue is exceeded then an error message will be written to the server activity log.

Limiting number of concurrent transfers

You may wish to limit the number of concurrent file transfer related trigger actions that are running in JSCAPE MFT Server. Since each file transfer related trigger action takes up a portion of bandwidth and disk I/O this is useful in cases where many file transfer triggers could be running simultaneously causing your server to be overloaded. To prevent this you can optionally set the maximum number of concurrent file transfers. If the maximum number of concurrent file transfers is reached then file transfer triggers actions will be placed in a queue for later execution, or depending on the trigger action priority they may interrupt an existing file transfer action and be given execution priority. Interrupted file transfer actions will automatically resume upon completion of higher priority file transfer actions. If the size of the queue is exceeded then an error message will be written to the server activity log.

Automatically clearing trigger history

Over time the history of executed triggers can grow and become quite large, in particular in systems that execute a large number of triggers on a regular basis. You may optionally automatically clear the history of trigger execution using the `Clear recent triggers older than N days` option. If enabled, the recent trigger history will be cleared of those executed triggers older than the specified value on a scheduled basis.

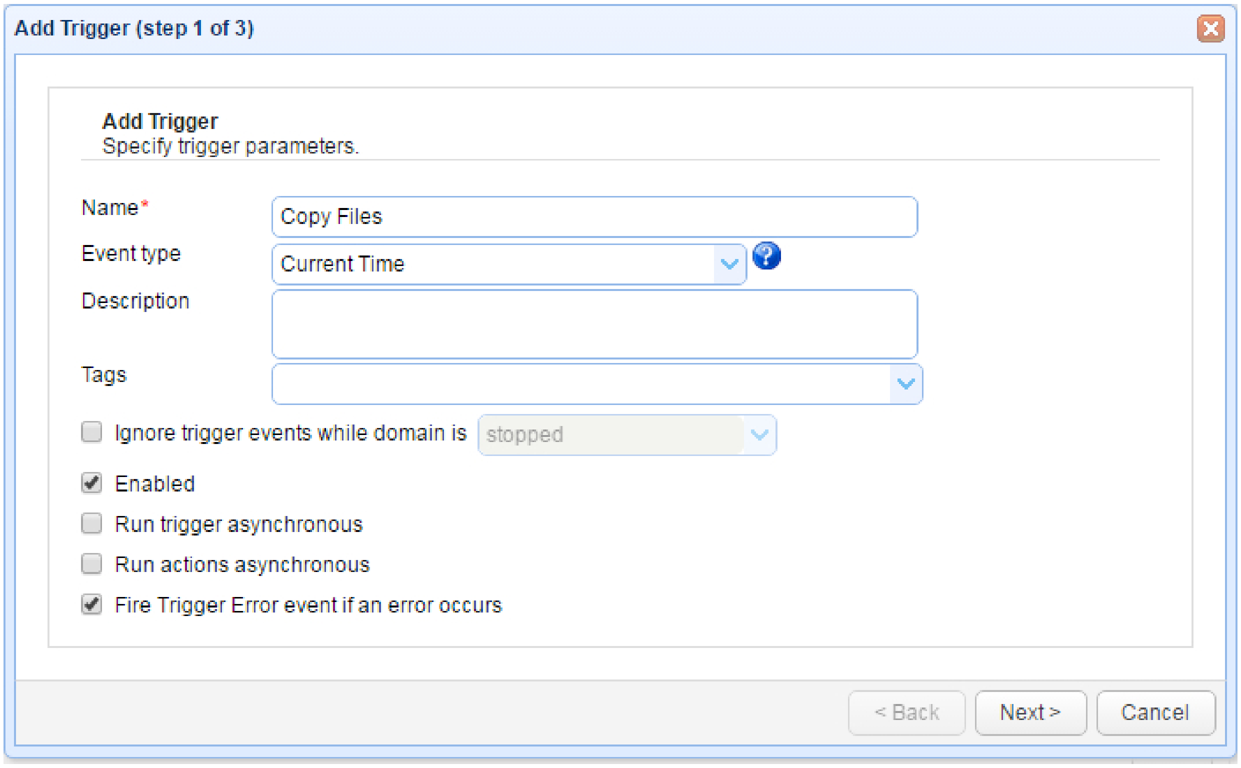
Defining global variables

You may wish to define global event variables that can be used by all of your triggers. Once created these global variables can be accessed from any of your trigger actions using the `Add` button.

Using time based triggers

JSCAPE MFT Server includes a powerful scheduler which allows you to schedule actions for execution on a one-time-only or recurring basis. To setup a time based trigger create a new Trigger with an `Event type` of `Current Time`. The `Current Time` event is fired every one (1) minute while the server is running. Using one or more `Trigger Condition(s)` you can specify when the actions associated with a trigger should be executed. The example condition below in *Figure 77* would be valid for 5:00 AM.

Figure 57



Add Trigger (step 1 of 3)

Add Trigger
Specify trigger parameters.

Name*	Copy Files
Event type	Current Time
Description	
Tags	

□ Ignore trigger events while domain is stopped

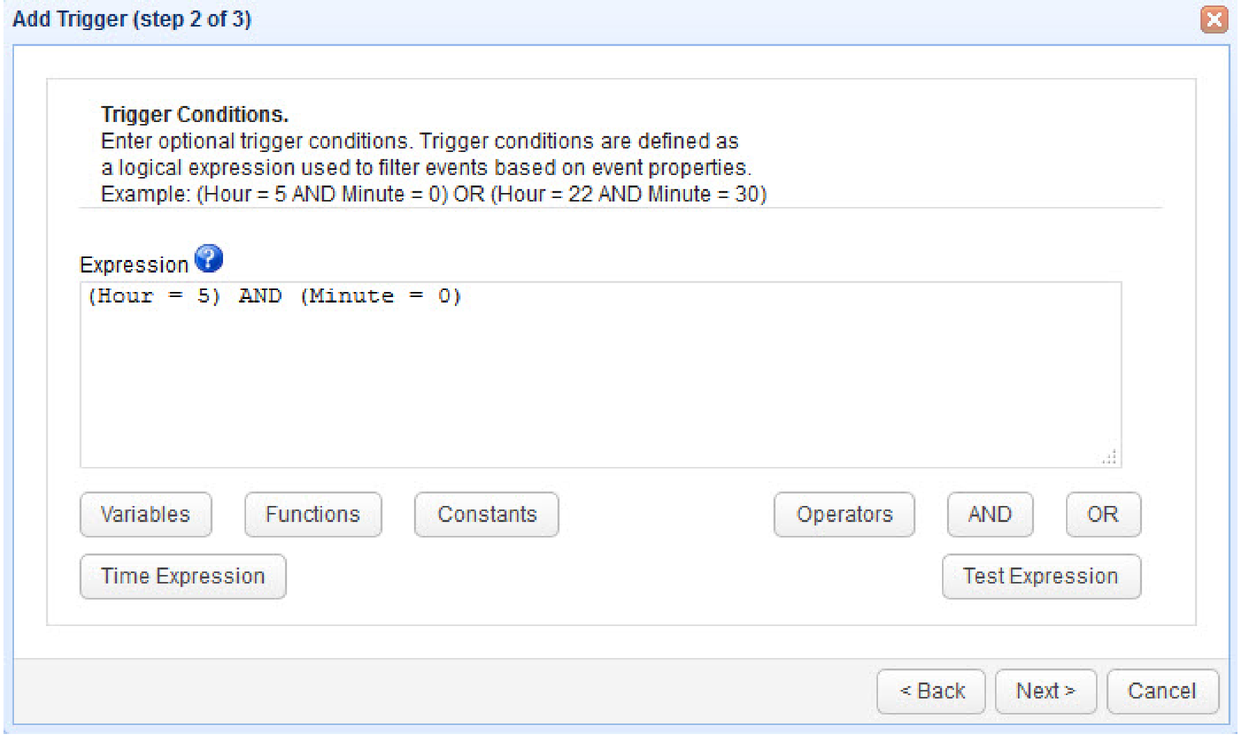
☑ Enabled

□ Run trigger asynchronous

□ Run actions asynchronous

☑ Fire Trigger Error event if an error occurs

Figure 77



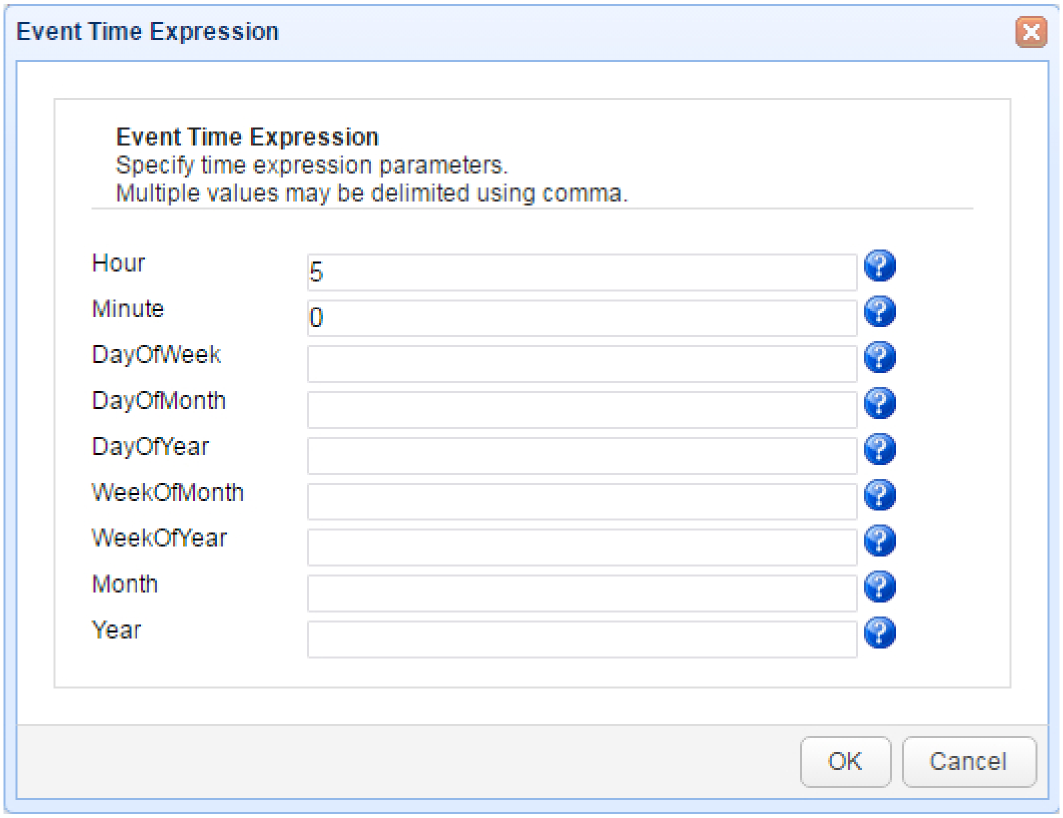
Add Trigger (step 2 of 3)

Trigger Conditions.
Enter optional trigger conditions. Trigger conditions are defined as a logical expression used to filter events based on event properties.
Example: (Hour = 5 AND Minute = 0) OR (Hour = 22 AND Minute = 30)

Expression

```
(Hour = 5) AND (Minute = 0)
```

You may click the `Time Expression` button for a more convenient way of specifying time expression parameters.



Event Time Expression

Event Time Expression
Specify time expression parameters.
Multiple values may be delimited using comma.

Hour	5
Minute	0
DayOfWeek	
DayOfMonth	
DayOfYear	
WeekOfMonth	
WeekOfYear	
Month	
Year	

See also

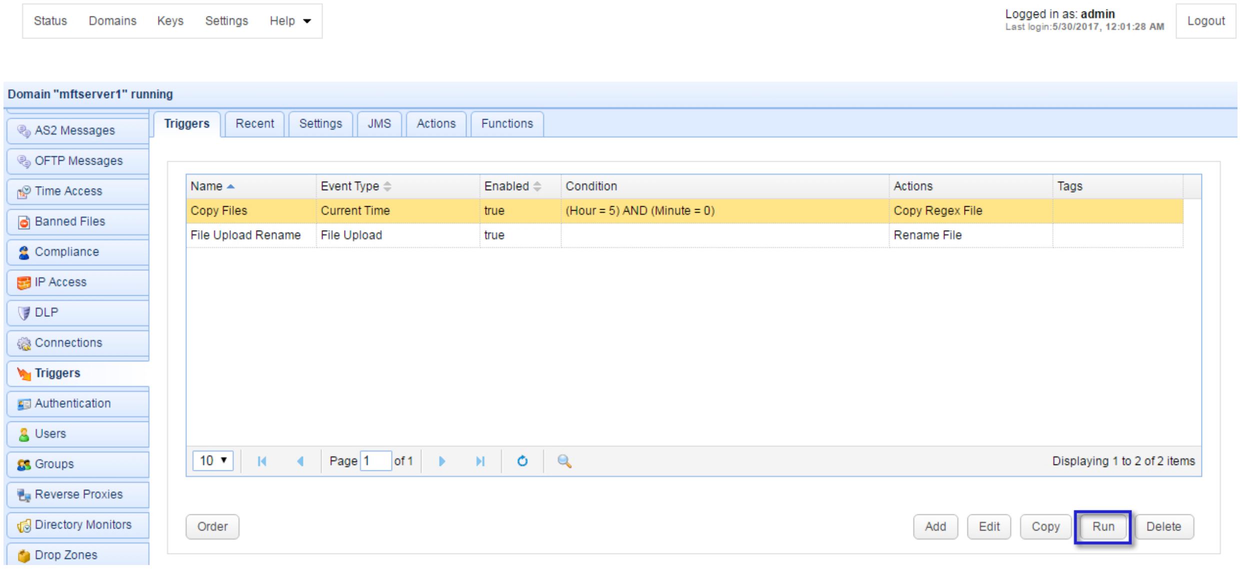
- Event types
- Adding triggers
- Writing conditions

Manually executing time based triggers

Triggers that use the `Current Time` event may be executed manually. To manually execute a `Current Time` trigger select the trigger in the `Triggers` panel and click the `Run` button. The trigger will be immediately executed ignoring any `Current Time` event conditions.

Figure 130

Trigger management 6



Domain "mftserver1" running

Name	Event Type	Enabled	Condition	Actions	Tags
Copy Files	Current Time	true	(Hour = 5) AND (Minute = 0)	Copy Regex File	
File Upload Rename	File Upload	true		Rename File	

Writing conditions

Trigger conditions are defined as a logical expression used to filter events based on event properties. An expression consists of zero (0) or more statements with each statement having a variable, operator and constant. Multiple statements may be joined together using `AND` or `OR` clauses to form complex expressions. Parenthesis may be used to set statement precedence. If the condition is left blank then the trigger actions will be executed anytime the trigger event is fired.

Example

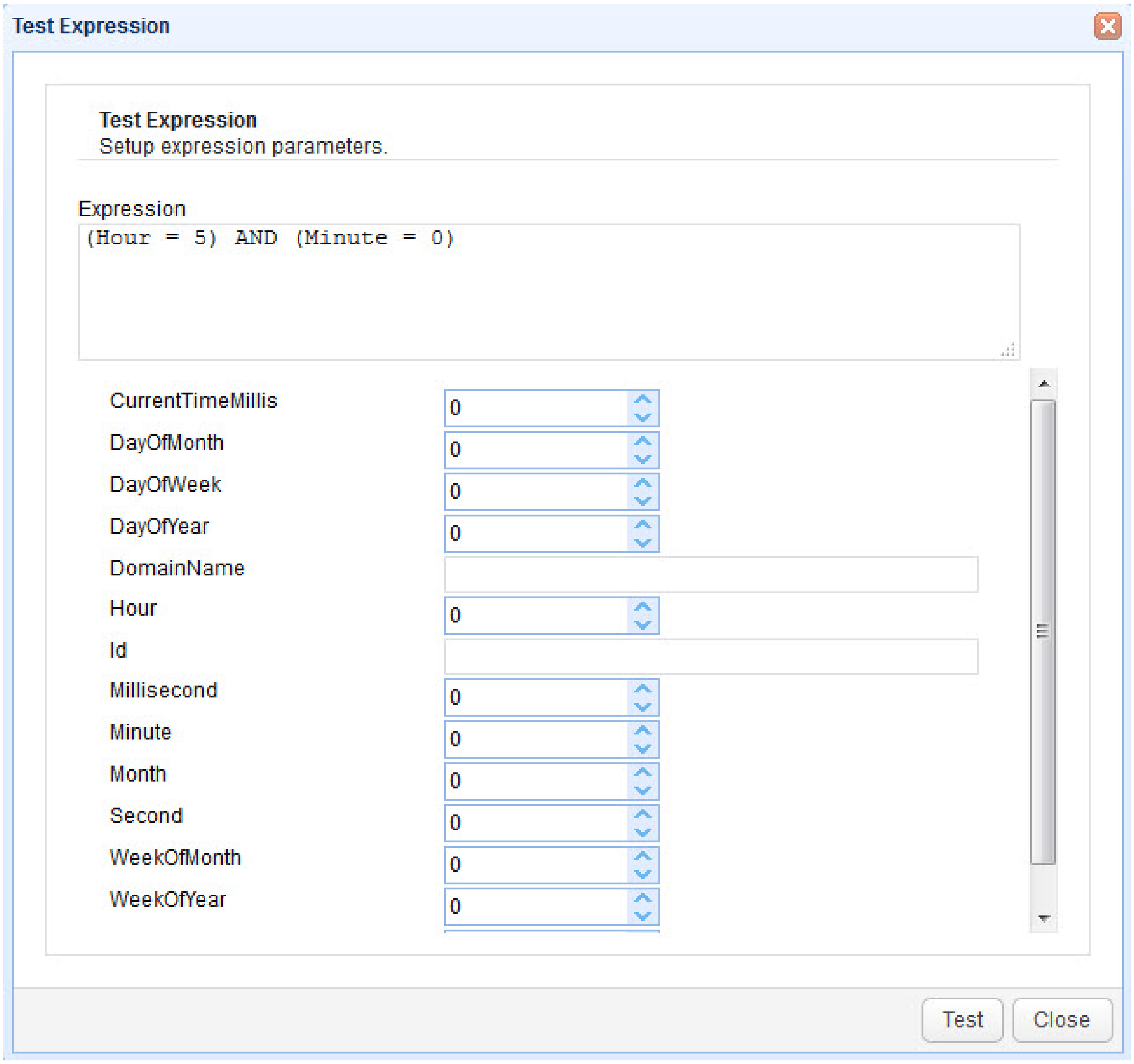
```
(Hour = 5 AND Minute = 0) OR (Hour = 22 AND Minute = 30)
```

The above expression is true at 5:00 AM or 10:30 PM.

Testing conditions

Prior to deploying a trigger you may wish to test your conditions against sample data to see if the condition logic functions as expected. To test a condition go to *Step 2* of adding or editing a trigger and click on the `Test Expression` button. At this point you may enter sample data to test against the condition. Upon clicking `Test` a dialog will be displayed indicating the success or failure of the test.

Figure 56



Test Expression

Test Expression

Setup expression parameters.

Expression

```
(Hour = 5) AND (Minute = 0)
```

CurrentTimeMillis	0
DayOfMonth	0
DayOfWeek	0
DayOfYear	0
DomainName	
Hour	0
Id	
Millisecond	0
Minute	0
Month	0
Second	0
WeekOfMonth	0
WeekOfYear	0

Event types

There are several event types that you may listen for when defining triggers. For a list of event types please see the context sensitive help available in JSCAPE MFT Server Manager when creating a trigger.

See also

Adding triggers
Action types
Defining custom action types

Action types

There are several built-in action types that you may use when defining triggers. For a list of available actions please see the context sensitive help available in JSCAPE MFT Server Manager when creating a trigger.

See also

Adding triggers

Trigger management 6

Function types

There are several built in functions that you can use within trigger action fields. These functions are particularly useful in cases where you want to format or parse a trigger event variable. For a list of available functions please see the context sensitive help available in JSCAPE MFT Server Manager when creating a trigger.

Rules for function arguments

1. Function parameters are separated by the comma character `,`. Leading or trailing spaces are considered as the part of parameter.
2. Function parameter string data **may** be surrounded with quotes. If the function parameter is not surrounded by quotes then any leading or trailing spaces **will** be included as part of the parameter.
3. If the function parameter contains a comma then you **must** surround the parameter with quotes to prevent it from being misinterpreted as a parameter separator.
4. If you are nesting a function or variable within a function then you should omit the leading and trailing `%` symbols. e.g. `%LocalDir%\%ToUpperCase(Name)%.RENAMED` In this case the leading and trailing `%` symbol from the `Name` variable is removed.

Using event variables within functions

Each trigger listens for a server event which in turn has several event variables that you can use in your trigger actions when executed. These event variables may be used in functions as well. For example, let's assume you are listening for the `File Upload` event and you want to rename the file to an upper case version of it's filename with a `.RENAMED` file extension. To achieve this you would create a trigger that listens for `File Upload` event and executes a `Rename File` action. The `Rename File` action has two required fields, `File` and `Destination File`, which would be as follows:

File: `%LocalPath%`
Destination File: `%LocalDir%\%ToUpperCase(Name)%.RENAMED`

In this case the `ToUpperCase` function is used, it's argument being the name of the file uploaded as represented by the `Name` event variable.

Using patterns in Format function

The `Format` function is very powerful in that it allows you to format data in a language neutral way. The most common use is in the formatting of dates. For example, assume that you need to get numeric month and day of month values in the format MM-DD. To achieve this you could use the `Month` and `DayOfMonth` event variables. The problem however is that the `Month` and `DayOfMonth` event variables return integer values, not strings, returning the incorrect format for months and days whose values fall between 1 and 9. To resolve this issue you must use the `Format` function to format the `Month` and `DayOfMonth` values in the desired format. The example below demonstrates how a MM-DD format could be achieved.

```
%Format("{0,number,00}-{1,number,00}",Month,DayOfMonth)%
```

The `Format` function uses the `java.text.MessageFormat` class that is provided as part of the JDK. For more information on how patterns may be used, please consult the JavaDoc documentation for this class available at:

http://docs.oracle.com/javase/6/docs/api/java/text/MessageFormat.html

Defining custom action types

You may define your own custom actions using the JSCAPE MFT Server Java Management API classes. To write your own action class extend the `com.jscape.inet.mft.workflow.AbstractAction` class and implement the abstract `execute()` method to perform the work of your action. Below is an example implementation of the `AbstractAction` class. This example prints a message to `System.out` and the log datastore.

JSCAPE MFT Server Manager uses Java reflection to build the GUI dialogs used to collect action properties. Therefore, all properties of your action should have corresponding getter/setter methods using Java naming conventions and an empty argument constructor for constructing the action. Using the `PropertyDescriptor[]` property you can define the order of properties and whether they are required. The `resultMessage` property is the message that will be written to the log file upon executing the action.

Note

Action properties may consist only of Java primitive values e.g. `String`, `int`, `boolean` etc.

For actions to be made available you must create a JAR archive e.g. `myactions.jar`, that contains your actions and place it in the `libs/actions` directory of your JSCAPE MFT Server installation. Any third party libraries that your action depends on should be placed in the `libs` directory of your JSCAPE MFT Server installation. For your action to be recognized by JSCAPE MFT Server restart the JSCAPE MFT Server Service.

Example

For a tutorial and complete source code example please see the following:

http://blog.jscape.com/jscape/2008/11/jscape-secure-f.html

See also

Adding triggers
Event types
Action types
Function types

File Transfer Script Language

The File Transfer Script Language is a very basic scripting language that allows you to automate routine file transfer processes. This language may be used when defining a File Transfer Script action as part of trigger.

Trigger management 6

The following commands may be used in a script file when invoking File Transfer Command Line.

append
cd
connect
del
deldir
disconnect
exec
get
getdir
lcd
lcopy
ldel
ldeldir
lmkdir
lmove
lrename
mget
mkdir
mode
mput
msg
prompt
promptmask
put
putdir
rename
set
set aftpcompression
set aftpcompressionfilesize
set aftpcompressionexclude
set aftpcongestioncontrol
set aftpdownloadrate
set aftpsecurity
set aftpuploadrate
set debug
set hostname
set logfile
set passive
set password
set protocol
set port
set privatekey
set secure
set timeout
set username
set wireencoding
wait

The above commands are reserved words in the FTCL language and may not be used as variable names when using the set or prompt commands.

Example

Bad

```
prompt dir "Enter directory name: "
```

The variable named "dir" may not be used as this is a reserved word for use by the "dir" command used to get a directory listing.

Good

```
prompt mydir "Enter directory name: "
```

The variable named "mydir" is not a reserved word so may be used.

append "<file>" ["<destination>"]	Appends contents of local file to remote file with same name. <file> a quoted relative filename or absolute path <destination> optional quoted remote filename to append to **Example** append "log.txt" "mylog.txt" **Example** append "log.txt"
cd "<directory>"	Sets directory on remote server. <directory> a quoted relative directory name or absolute path **Example** cd "jsmith" **Example** cd "/home/users/jsmith"
connect	Establishes connection with remote server.
del "<file>"	Deletes remote filename. <file> a quoted relative filename or absolute path **Example** del "logs.txt" **Example**

	del "/home/user/logs.txt"
deldir "<directory>"	Deletes remote directory recursively <directory> a quoted relative directory name or absolute path **Example** deldir "logs" **Example** deldir "/home/users/jsmith/logs"
disconnect	Disconnects from remote server.
exec "<command> "	Executes command on local machine. <command> valid command to be interpreted by the local operating system. **Example** exec "dir c:/tmp > c:/tmp/dirout.txt" **See also** Escape sequences
get "<file>"	Downloads file from remote server. <file> a quoted relative filename or absolute path **Example** get "logs.txt"
getdir "<directory>"	Downloads directory recursively from remote server. <directory> a quoted relative directory name or absolute path **Example** getdir "logs" **Example** getdir "/var/logs"
lcd "<directory>"	Sets current working directory on local machine. This directory is used when uploading files using relative paths and when downloading files. <directory>

	a quoted absolute path **Example** `lcd "c:/tmp"` **See also** Escape sequences

lcopy "<path>" "<destination>"	Copies a local file to a local destination.
	<path>
	a quoted relative or absolute file or directory path
	<destination>
	a quoted relative or absolute file or directory path
	Example
	`lcopy "logs.txt" "logs.txt.old"`
	Example
	`lcopy "c:/tmp/logs.txt" "c:/tmp/logs.txt.old"`
	See also
	Escape sequences

ldel "<file>"	Deletes local filename.
	<file>
	a quoted relative filename or absolute path
	Example
	`ldel "logs.txt"`
	Example
	`ldel "c:/tmp/logs.txt"`
	See also
	Escape sequences

ldeldir "<directory>"	Deletes local directory recursively <directory> a quoted relative directory name or absolute path **Example**

	ldeldir "tmp" **Example** ldeldir "c:/tmp" **See also** Escape sequences
lmkdir "<directory>"	Creates local directory recursively <directory> a quoted relative directory name or absolute path **Example** lmkdir "tmp" **Example** lmkdir "c:/tmp" **See also** Escape sequences
lmove "<path>" "<destination>"	Moves a local file to a local destination. <path> a quoted relative or absolute file or directory path <destination> a quoted relative or absolute file or directory path **Example** move "logs.txt" "archive/logs.txt" **Example** move "c:/tmp/logs.txt" "c:/tmp/archive/logs.txt" **See also** Escape sequences
lrename "<path>" "<destination>"	Renames file on local machine. <path> a quoted relative or absolute file or directory path <destination> a quoted relative or absolute file or directory path

	Example lrename "logs.txt" "logs.txt.old" **Example** lrename "c:/tmp/logs.txt" "c:/tmp/logs.txt.old" **See also** Escape sequences
mget "<filter>"	Downloads files from current remote directory matching filter. <filter> a quoted regular expression **Example** mget ".*\\.txt"
mkdir "<directory>"	Creates directory on remote server. <directory> a quoted relative directory name or absolute path **Example** cd "jsmith" **Example** cd "/home/users/jsmith"
mode "<mode>"	Sets transfer mode to ASCII or binary. <mode> a quoted transfer mode of "ascii" or "binary" **Example** mode "ascii"
mput "<filter>"	Uploads local files in current working directory matching filter to remote server. <filter> a quoted regular expression **Example** mput ".*\\.txt"
msg "<message> "	Sends message to current debugging stream. By default the console is the current debug stream and

	debugging is enabled. **Example** msg "connecting to FTP server"
prompt <variablename> "<prompt>"	Prompts user to enter a value to be read from the command line and stores this value in the variable name used in the first argument. The value stored in this variable is then available for use later in the script. **Example** prompt username "Enter username: "
promptmask <variablename> "<prompt>"	Prompts user to enter a value to be read from the command line and stores this value in the variable name used in the first argument. The value stored in this variable is then available for use later in the script. Value entered is masked to user. **Example** promptmask password "Enter password: "
put "<file>" ["<destination>"]	Uploads local file to remote server. <file> a quoted relative filename or absolute path <destination> optional quoted remote filename or absolute path to store file as **Example** put "c:/tmp/logs.txt" **Example** put "c:/tmp/logs.txt" "mylogs.txt" **See also** Escape sequences
putdir "<directory>"	Uploads local directory recursively to remote server. <directory> a quoted relative directory name or absolute path **Example** putdir "logs" **Example**

	`put dir "c:/tmp/logs"` **See also** Escape sequences

`rename` `"<path>" "<destination>"`	Renames file on remote server.
	`<path>`
	a quoted relative or absolute file or directory path
	`<destination>`
	a quoted relative or absolute file or directory path
	Example
	`rename "logs.txt" "logs.txt.old"`
	Example
	`rename "/var/logs/logs.txt" "/var/logs/logs.txt.old"`

`set` `<variablename> <value>`	Creates a user defined variable for use within a script.
	`<variablename>`
	A variable name used to reference the variable. Must begin with a letter, and may be followed by 0 or more letters or digits.
	`<value>`
	The value the variable name represents. Valid values include boolean values of true or false, any valid integer or any quoted string.
	Example
	`set myNumberVariable 12`
	Example
	`set myBooleanVariable true`
	Example
	`set myStringVariable "testing 1.2.3"`
	Variables created may later be referenced using the ${<variablename>} notation.
	Example
	`set myNumberVariable 12`

	msg "value of myNumberVariable is: {myNumberVariable}"
set aftpcompression <boolean>	Specifies whether streaming compression is enabled or disabled in AFTP connections. By default compression is enabled. <boolean> true, false **Example** set aftpcompression false
set aftpcompressionfilesize <filesize>	Specifies the minimum filesize in bytes for compress connections. The default minimum filesize is 1048576 <filesize> A valid integer between 1-2,147,483,647 **Example** set aftpcompressionfilesize 100000
set aftpcompressionexclude "<filter>"	Specifies a case-insensitive, comma-delimited list of file extensions to exclude when using compression in AFTP connections. Default value is: ".bz2,.F,.gz,.lz,.lzma,.lzo,.rz,.sfark,.xz,.z,.Z,.infl,.7z, .s7z,.ace,.afa,.alz,.apk,.arc,.arj,.ba,.bh,.cab,.cfs, .cpt,.dar,.dd,.dgc,.dmg,.gca,.ha,.hki,.ice,.j,.kgb,.lzh, .lha,.lzx,.pak,.partimg,.paq6,.paq7,.paq8,.pea,.pim, .pit,.qda,.rar,.rk,.sda,.sea,.sen,.sfx,.sit,.sitx,.sqx, .tgz,.tbz2,.tlz,.uc,.uc0,.uc2,.ucn,.ur2,.ue2,.uca,.uha, .wim,.xar,.xp3,.yz1,.zip,.zipx,.zoo,.zz," <filter> a comma-delimited list of file extensions. **Example** set aftpcompressionexclude ".zip,.gz"
set aftpcongestioncontrol <boolean>	Specifies whether congestion control is enabled or disabled when connecting using AFTP protocol. By default congestion control is enabled. <boolean> true, false **Example** set aftpcongestioncontrol false
set aftpdownloadrate <bitrate>	Specifies the download rate in Kbits per second. The default rate is 45000 Kbps.

	<bitrate> A valid integer between 1-2,147,483,647 **Example** set aftpdownloadrate 100000
set aftpsecurity "<mode>"	Specifies whether credentials and/or data are protected during an AFTP session. Default value is "none" providing no protection. <mode> a valid security mode. Valid values are "none", "credentials & data", "credentials only". **Example** set aftpsecurity "credentials only"
set aftpuploadrate <bitrate>	Specifies the upload rate in Kbits per second. The default rate is 45000 Kbps. <bitrate> A valid integer between 1-2,147,483,647 **Example** set aftpdownloadrate 100000
set debug <boolean>	Specifies whether debugging is enabled or disabled. By default debugging is enabled and all debugging information is sent to the console. <boolean> true, false **Example** set debug false
set hostname "<hostname>"	Specified the hostname of the remote server. <hostname> a valid quoted hostname or IP address **Example** set hostname "192.168.10.2"
set logfile "<file>"	Specifies the path of the log file to write debug data to. By default all output is sent to the console. <file> a valid relative or absolute file path on local machine

	Example set logfile "c:/tmp/log.txt" **See also** Escape sequences
set passive <boolean>	Specifies whether passive or active mode should be used in FTP/S protocols. Default is true. <boolean> true, false **Example** set passive true
set password "<password>"	Specifies the password to use when logging into the remote server. <password> a valid quoted password for specified username on remote server **Example** set password "secret"
set protocol <protocol>	Specifies the protocol to use when establishing a connection. <protocol> the protocol to use. Valid options are "ftp", "ftps", "ftps-auth-tls", "ftps-auth-ssl", "ftps-implicit", "sftp" and "aftp" for the protocols FTP, FTP over SSL (AUTH SSL), FTP over SSL (Implicit SSL), SFTP (FTP over SSH) and AFTP respectively. Default protocol is "ftp" **Note** When using "ftps-implicit" setting you must set the port to the server port responsible for handling implicit SSL connections. This is typically handled on port 990. **Example** set protocol "ftps-auth-tls" **See also** set port
set port <port>	Specifies the port of the remote server. The default

	ports for FTP and SFTP protocols are 21 and 22 respectively.
	`<port>`
	A valid integer between 1-65535
	Example
	`set port 2021`

set privatekey "<file>"	Specifies the path of private key file to use when authenticating with SFTP server. Valid for use in SFTP protocol only.
	`<file>`
	a valid relative or absolute file path on local machine
	Example
	`set privatekey "c:/ssh/keys/id_dsa"`

set secure <boolean>	Specifies that the secure SFTP protocol be used. FTP protocol is used by default. Requires that SSH version 2.0 or above be installed on remote server and SFTP be enabled.
	`<boolean>`
	true, false
	Example
	`set secure true`

set timeout <seconds>	Sets the maximum timeout used when establishing a connection, sending data or receiving data. If timeout is exceeded script will abort. Default value is 60 seconds.
	`<seconds>`
	the maximum number of seconds to wait
	Example
	`set timeout 30`

set username "<username>"	Specifies the username to use when logging into the remote server.
	`<username>`
	a valid quoted username for remote server
	Example
	`set username "jsmith"`

set wireencoding "<encoding>"	Specifies the wire encoding to use on command

	channel for FTP/S protocols.
	`<encoding>`
	a valid quoted character encoding
	Example
	`set wireencoding "UTF-8"`

wait `<seconds>`	Pauses execution of script for specified number of seconds.
	`<seconds>`
	the number of seconds to wait
	Example
	`wait 5`

Escape sequences

The FTCL language allows for the use of escape characters when defining strings in the same way that the Java programming language does. The `\` character is treated specially inside of strings indicating that the next character is to be escaped.

Escape sequences

Escape sequence	**Description**
`\t`	Tab
`\r`	Carriage return
`\n`	Line feed
`\\`	Backslash
`\"`	Quote

Note

This is especially important to consider when defining local paths on the Windows operating system. The local path `c:\tmp` must be defined as `c:/tmp` **or** `c:\\tmp` when using FTCL commands that use local path information.

Example

Incorrect

```
lcd "c:\tmp\home"
```

Correct

```
lcd "c:/tmp/home"
```

The first example is incorrect as the `"\t"` in `"c:\tmp\home"` would be interpreted by FTCL as a tab character instead of a literal `\t`. The second example corrects this issue by using a forward slash instead of a backslash.

Web based file transfers 7

Overview

JSCAPE MFT Server Web Client is a web based file transfer client. It has many of the functions of traditional FTP/SFTP clients providing the ability to manage, upload and download files from a remote server. However, unlike traditional FTP/SFTP clients, as a browser based platform-independent application there is no software to install or maintain drastically reducing the total cost of ownership. Additionally, since JSCAPE MFT Server Web Client runs over HTTP/S it bypasses many firewall restrictions while still maintaining the highest level of security.

See also

Enabling web based file transfers
Web user interface
Customizing the web interface

Enabling web based file transfers

JSCAPE MFT Server includes JSCAPE MFT Server Web Client, a browser based file transfer client for performing file transfer sessions with JSCAPE MFT Server.

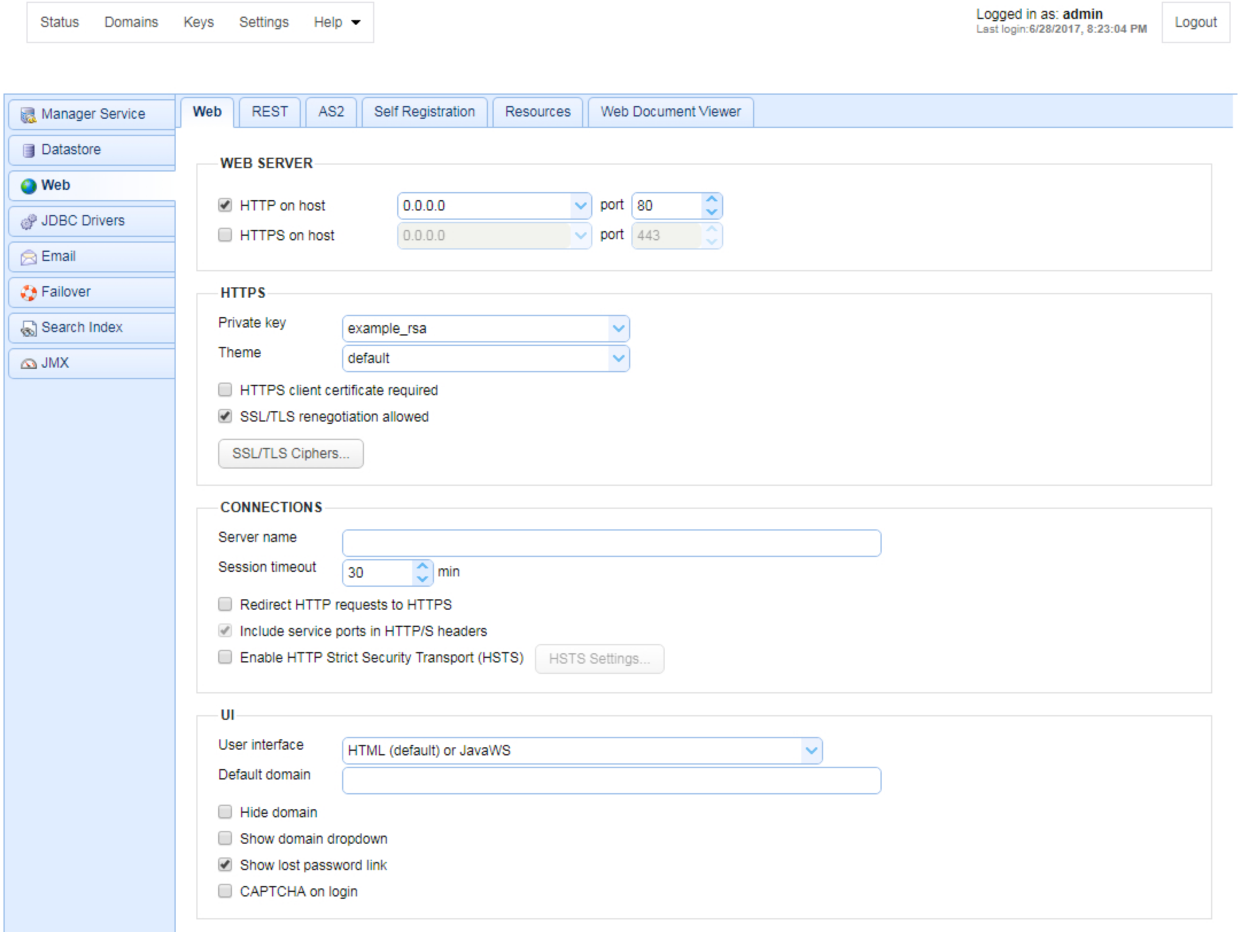
JSCAPE MFT Server Web Client has all the common functions of a file transfer client without having to go through the trouble and expense of installing file transfer client software on your end-users computers. Additionally, since JSCAPE MFT Server Web Client communicates via HTTP/S, you can easily give your users secure file transfer capabilities without having to deal with complex customer firewall issues often associated with FTP/SFTP protocols.

Step 1. - Enable HTTP/S services

Go to the `Settings > Web` node . Here you will find a set of options for enabling HTTP/S services.

Figure 19

Web based file transfers 7



WEB SERVER

☑ HTTP on host 0.0.0.0 port 80

☐ HTTPS on host 0.0.0.0 port 443

HTTPS

Private key: example_rsa

Theme: default

☐ HTTPS client certificate required

☑ SSL/TLS renegotiation allowed

CONNECTIONS

Server name:

Session timeout: 30 min

☐ Redirect HTTP requests to HTTPS

☑ Include service ports in HTTP/S headers

☐ Enable HTTP Strict Security Transport (HSTS)

UI

User interface: HTML (default) or JavaWS

Default domain:

☐ Hide domain

☐ Show domain dropdown

☑ Show lost password link

☐ CAPTCHA on login

Web Server

HTTP on host - The host and port you want to enable HTTP service on. This will also be used for client REST services.

HTTPS on host - The host and port you want to enable HTTPS service on. This will also be used for client REST services.

HTTPS

Private key - The SSL encryption key to be used for HTTPS services.

Theme - The color theme used for the buttons, menus, tabs, and other GUI elements.

HTTPS client certificate required - Requires that client browser successfully identify itself with a client certificate found in "Client keys" section of Key Manager.

SSL/TLS negotiation allowed - If enabled clients will be allowed to renegotiate SSL/TLS sessions.

SSL/TLS Ciphers - List of enabled SSL/TLS ciphers for HTTPS communications.

Connections

Server name - Optional value if entered will replace any HTTP headers that contain hostname data with specified hostname. This is useful in cases where server operates behind a NAT enabled firewall and you do not want to leak internal hostname or IP address information.

Session timeout - The amount of time after which to close inactive HTTP/S sessions.

Redirect HTTP requests to HTTPS - Redirect incoming HTTP requests to secure HTTPS service.

Include service ports in HTTP/S headers - If checked (default), service ports will be included in HTTP/S headers.

Enable HTTP Strict Security Transport (HSTS) - If enabled, HSTS will be enabled.

UI

User interface - Sets what user interface options are available from login page.

Default domain - Defaults domain field to specified value when logging in via web interface.

Hide domain - Hides domain field when logging in via web interface. If this option is checked then a default domain MUST be provided.

Show domain dropdown - If enabled a drop-down of all available domains is displayed for the Domain field when logging in via the web interface, otherwise a text field is displayed requiring user to type in domain.

Show lost password link - If enabled the `Lost password` link will be displayed on web interface login page allowing user to reset their password via email.

CAPTCHA on login - If checked, user will be required to enter a CAPTCHA on login.

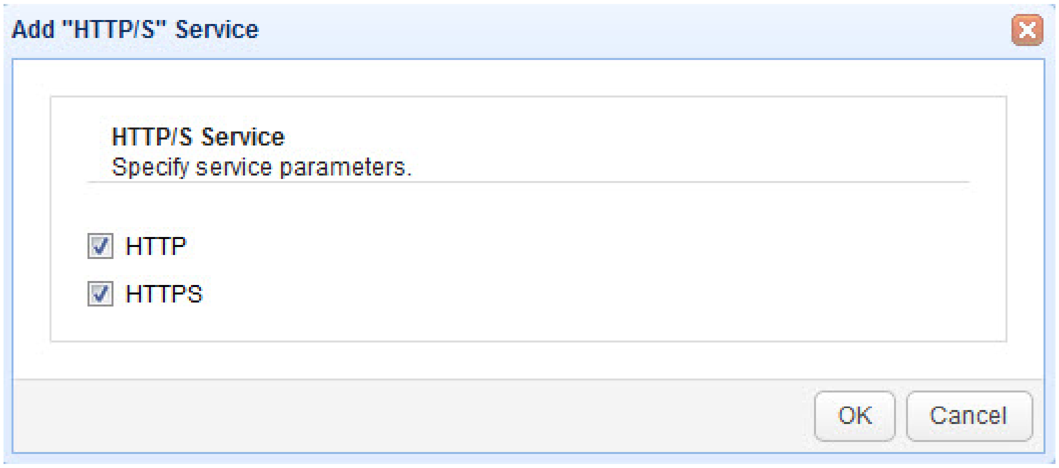
See also

Obtaining a trusted certificate

Step 2. - Add HTTP/S services to your Domain.

For the desired domain go to the `Services` module and click the `Add` button. When prompted set the `Protocol` to `HTTP/S` and select the desired protocols you wish to accept file transfers for.

Figure 33



Add "HTTP/S" Service

HTTP/S Service
Specify service parameters.

☑ HTTP

☑ HTTPS

See also

[Obtaining a trusted certificate]

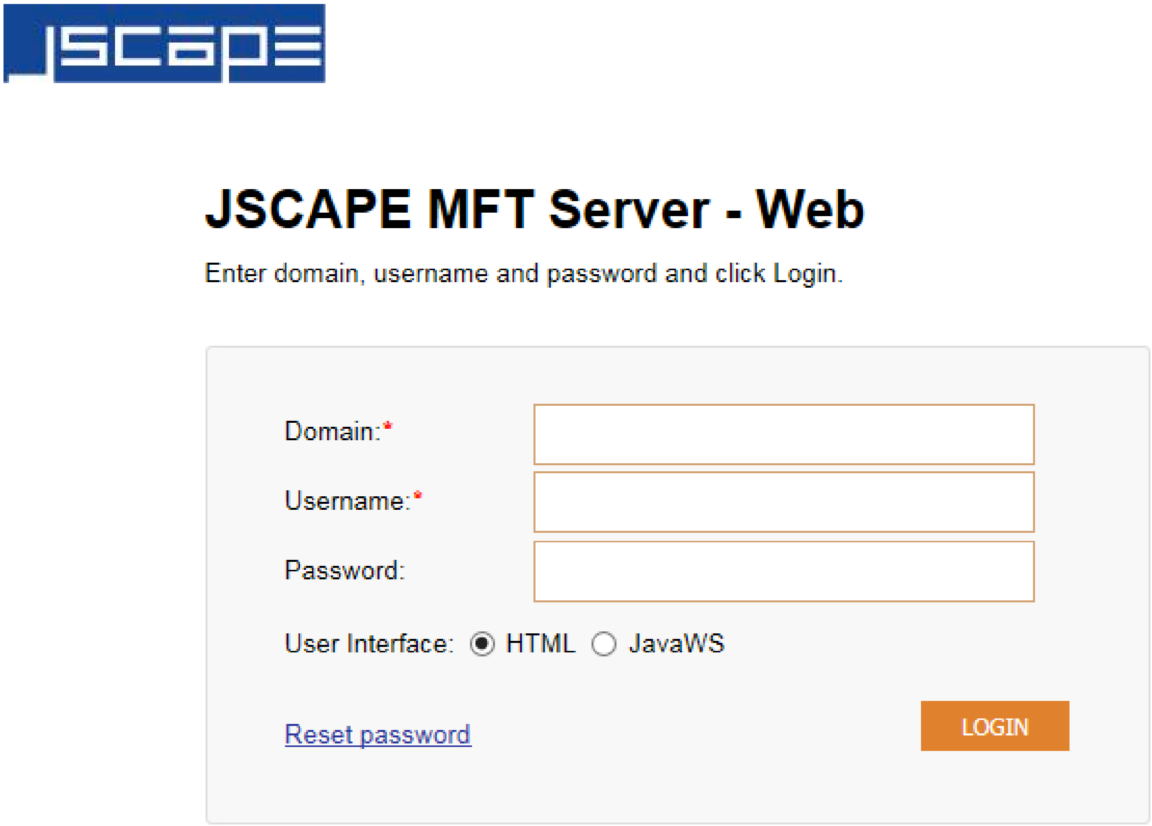
Web user interface

JSCAPE MFT Server Web Client has all the common functions of a file transfer client without having to install file transfer client software on your end-users computers. All user permissions and virtual paths are observed when using JSCAPE MFT Server Web Client.

Figure 25

Web based file transfers

7



JSCAPE MFT Server - Web

Enter domain, username and password and click Login.

Domain:*

Username:*

Password:

User Interface: ● HTML ○ JavaWS

Reset password

LOGIN

Domain - The name of the domain to connect to. This is the name of the domain as identified Domain Name column of JSCAPE MFT Server Manager, not the IP address or hostname although these may be the same.

Username - The account username.

Password - The account password.

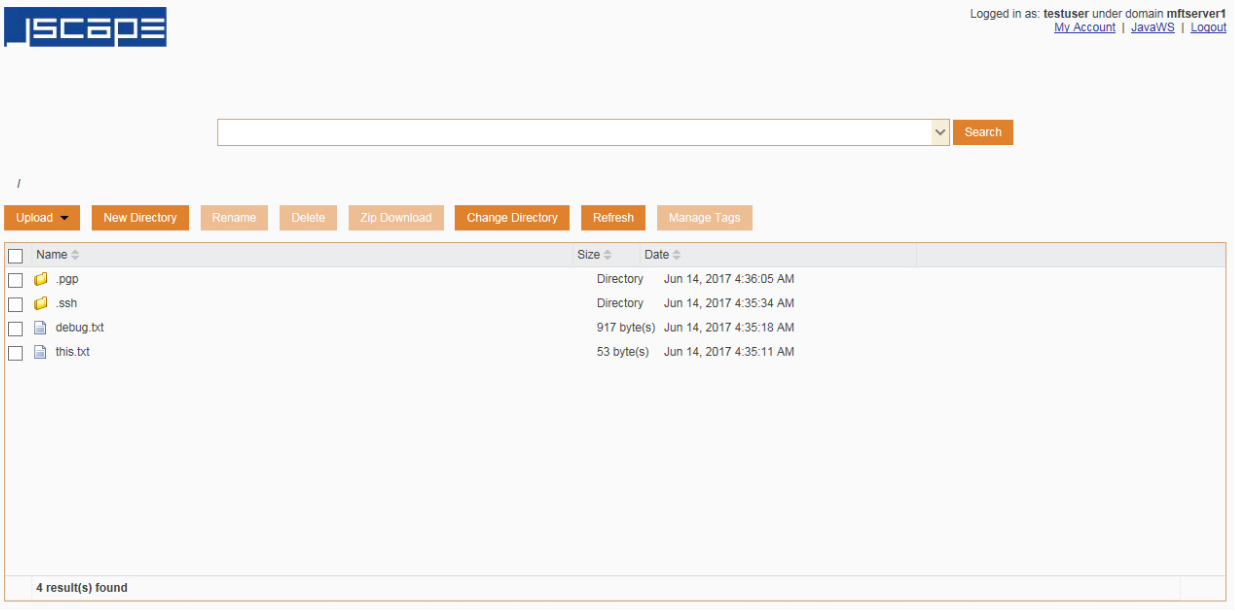
User Interface - The user interface to show upon login. JavaWS user interface is only supported in Enterprise version of JSCAPE MFT Server.

Reset password - Allows user to reset lost password.

Figure 32

Web based file transfers

7



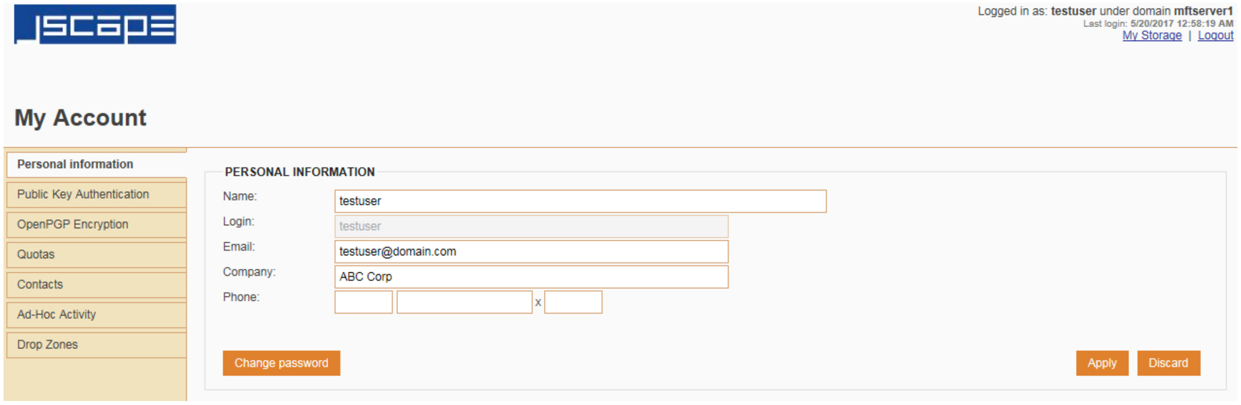
Logged in as: **testuser** under domain **mftserver1**
My Account | JavaWS | Logout

/

□	Name	Size	Date
□	.pgp	Directory	Jun 14, 2017 4:36:05 AM
□	.ssh	Directory	Jun 14, 2017 4:35:34 AM
□	debug.txt	917 byte(s)	Jun 14, 2017 4:35:18 AM
□	this.txt	53 byte(s)	Jun 14, 2017 4:35:11 AM

4 result(s) found

Figure 115



Logged in as: **testuser** under domain **mftserver1**
Last login: 5/20/2017 12:58:19 AM
My Storage | Logout

My Account

PERSONAL INFORMATION

Name:	testuser
Login:	testuser
Email:	testuser@domain.com
Company:	ABC Corp
Phone:	x

Personal Information

This section is available to all users and may be used to update the name, email address, company name, phone number, and password for a user account.

Public Key Authentication

This section can be used to generate a key pair for use in public key authentication (SFTP). When generating a key pair or importing a public key the public key is automatically placed in the `.ssh/key.pub` file relative to the users root login directory on the server. When generating a key pair the user is prompted to store the private key on their system. Note, private keys should **never** be stored on the server, except for purposes of connecting to other remote servers.

OpenPGP Encryption

This section can be used to generate an OpenPGP key pair for use in encrypting files uploaded to virtual directories.

Domain Administration

This section is only available to domain administrators and may be used to manage users.

Quotas

This section displays any bandwidth quota or directory monitor quota information for the user.

Contacts

This section can be used to manage contacts for use in ad-hoc file transfers.

Ad-Hoc Activity

This section can be used to manage ad-hoc emails sent by the user.

Drop Zones

This section shows drop zone information for the user.

See also

Assigning domain administrators

Customizing the web interface

The JSCAPE MFT Server Web Client user interface may be easily customized to match the language and look and feel of your organization.

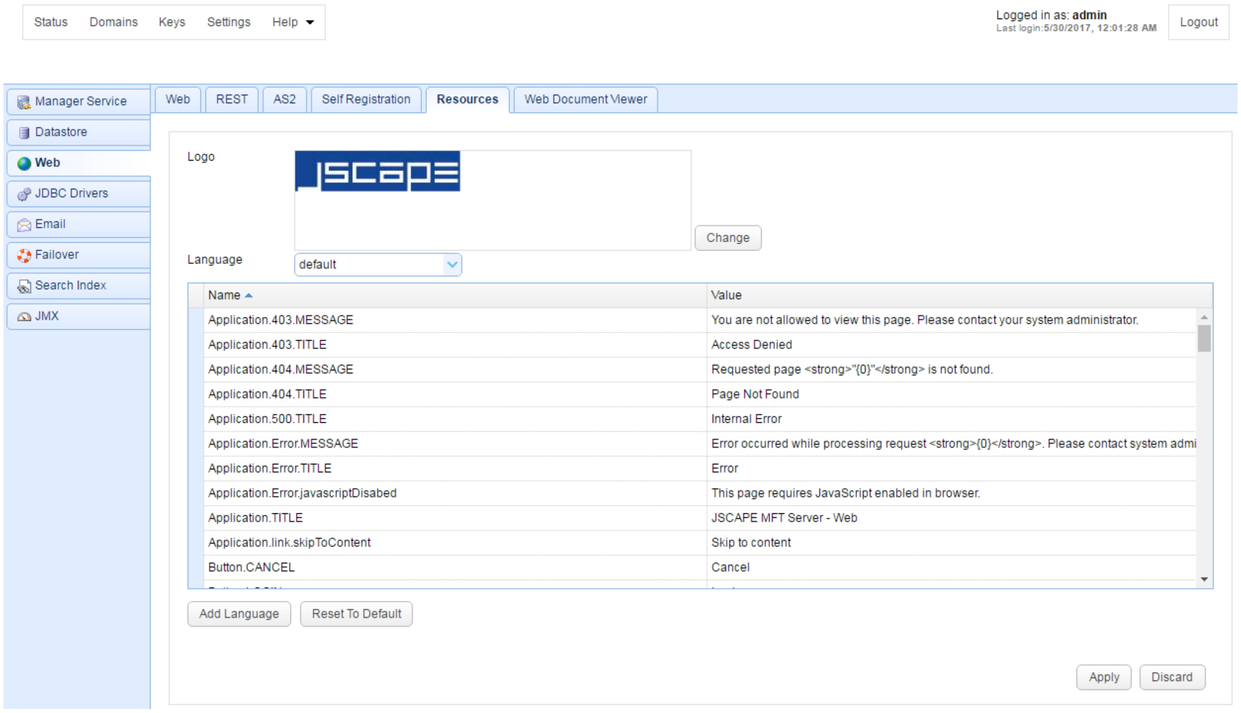
Setting login page properties

When connecting to the JSCAPE MFT Server Web Client the server automatically detects the clients browser language settings and loads the appropriate language file. If a matching language file **cannot** be found then the `default` language file is used. The logo and text for the login page may be changed by going to `Settings > Web` and clicking on the `Resources` tab.

Figure 47

Web based file transfers

7



Logged in as: admin
Last login:5/30/2017, 12:01:28 AM

Logo

Language: default

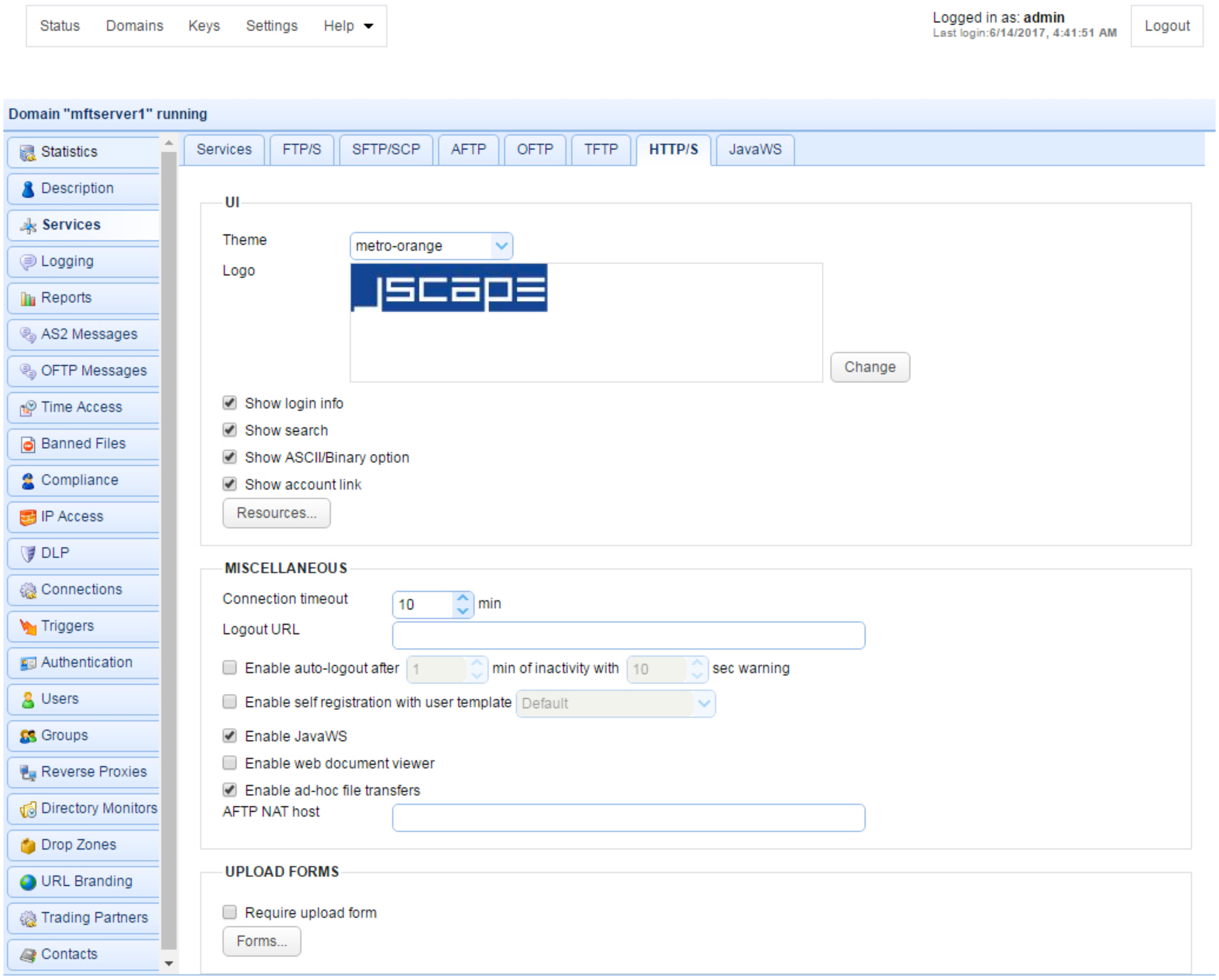
Name	Value
Application.403.MESSAGE	You are not allowed to view this page. Please contact your system administrator.
Application.403.TITLE	Access Denied
Application.404.MESSAGE	Requested page <strong>"{0}"</strong> is not found.
Application.404.TITLE	Page Not Found
Application.500.TITLE	Internal Error
Application.Error.MESSAGE	Error occurred while processing request <strong>{0}</strong>. Please contact system admi
Application.Error.TITLE	Error
Application.Error.javascriptDisabed	This page requires JavaScript enabled in browser.
Application.TITLE	JSCAPE MFT Server - Web
Application.link.skipToContent	Skip to content
Button.CANCEL	Cancel

Setting HTTP domain level properties

When connecting to the JSCAPE MFT Server Web Client the server automatically detects the clients browser language settings and loads the appropriate language file. If a matching language file **cannot** be found then the `default` language file is used. The logo and text for the HTTP/S user interface may be changed at the domain level by going to the `Services > HTTP/S` panel.

Figure 89

Web based file transfers 7



UI

Theme: metro-orange

Logo: JSCAPE [Change]

☑ Show login info

☑ Show search

☑ Show ASCII/Binary option

☑ Show account link

[Resources...]

MISCELLANEOUS

Connection timeout: 10 min

Logout URL:

☐ Enable auto-logout after 1 min of inactivity with 10 sec warning

☐ Enable self registration with user template: Default

☑ Enable JavaWS

☐ Enable web document viewer

☑ Enable ad-hoc file transfers

AFTP NAT host:

UPLOAD FORMS

☐ Require upload form

[Forms...]

UI

Theme - The color theme used for the buttons, menus, tabs, and other GUI elements.

Logo - The logo displayed in upper left corner when using HTML user interface.

Show login info - If checked, the current username and domain is displayed in upper right.

Show search - If checked searches on indexed documents may be performed.

Show ASCII/Binary option - If checked, user has option of uploading files in both ASCII and binary modes. If unchecked only binary is allowed by default and user does not have ability to change this setting.

Show account link - If checked the My Account link is displayed in upper right allowing users to change their account contact information.

Resources… - The current language resource file. Language resource files are used for specifying alternative user interface labels based on client browser default language.

MISCELLANEOUS

Connection timeout - The connection timeout for HTTP requests in minutes.

Logout URL - The URL to redirect user to upon clicking Logout link.

Enable auto-logout - If checked, user will be automatically logged out after X minutes of inactivity with grace period of Y seconds.

Enable self-registration with user template - Enables new users to self-register. The properties of the newly created user account will depend on the template chosen from the drop-down list.

Enable JavaWS - If checked, JavaWS interface is enabled.

Enable web document viewer - If checked web document viewer is enabled.

Enable ad-hoc file transfers - If checked ad-hoc file transfers will be enabled for the domain.

AFTP NAT Host - The host to use when connecting to AFTP service using JavaWS.

UPLOAD FORMS

Require upload form - Requires users to use the upload form when performing file uploads via the web UI

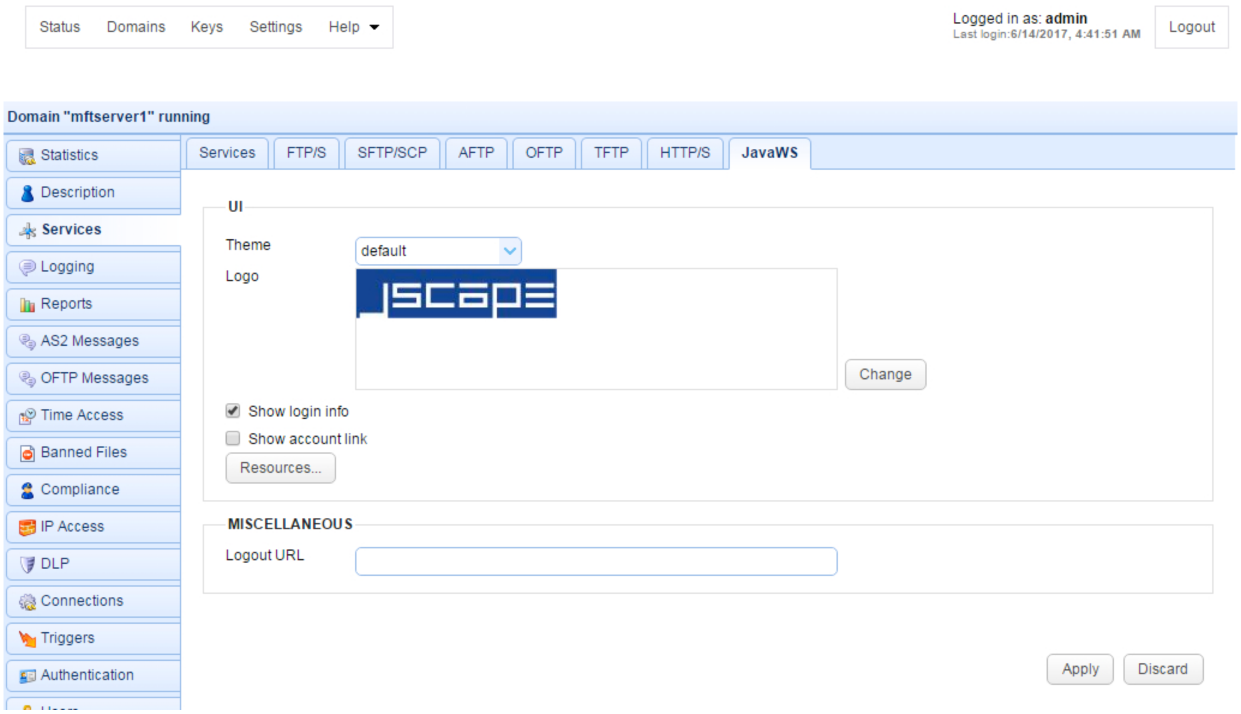
Forms… - Forms available during file upload when using HTML user interface.

Setting JavaWS domain level properties

When connecting to the JSCAPE MFT Server Web Client the server automatically detects the clients browser language settings and loads the appropriate language file. If a matching language file cannot be found then the `default` language file is used. The logo and text for the JavaWS user interface may be changed at the domain level by going to the `Services > JavaWS` panel.

Figure 90

Web based file transfers 7



Logged in as: admin
Last login:6/14/2017, 4:41:51 AM

Domain "mftserver1" running

Theme: default

Logo

☑ Show login info

☐ Show account link

Logout URL:

Theme - The color theme used for the buttons, menus, tabs, and other GUI elements.

Logo - The logo displayed in upper left corner when using WebDAV user interface.

Show login info - If checked, the current username and domain is displayed in upper right.

Show account link - If checked the My Account link is displayed in upper right allowing users to change their account contact information.

Resources… - The current language resource file. Language resource files are used for specifying alternative user interface labels based on client browser default language.

Logout URL - The URL to redirect user to upon clicking Logout link.

Performing automatic login

If you are integrating JSCAPE MFT Server Web Client into an existing web based application you may already have the needed user login credentials. To prevent users from being required to enter login credentials again, you may embed all login credentials as URL parameters. Upon successful login user will be automatically logged into the JSCAPE MFT Server Web Client. SSO (single-sign-on) may also be used.

Example

```
http://hostname:port/action/login?
domain=localhost&username=jsmith&password=secret&continue=/action/cwd?
filename=/path/to/dir
```

URL Parameters

`hostname` - The hostname or IP of the web server.
`port` - The port of the web server.
`domain` - The domain to login to.
`username` - The username to login as.
`password` - The password to login with.
`continue` - The relative URL to redirect user to after login. In the example above the `continue` argument is used to redirect user to a specified directory upon login.

See also

Web SSO

Specifying logout URL

By default when clicking the `Logout` link in JSCAPE MFT Server Web Client the user will be logged out and presented with the login page for JSCAPE MFT Server Web Client. In the event you want the end-user to be redirected to another URL you may specify this in the `Logout URL` field found in the panels for `Services > HTTP/S` and `Services > WebDAV/S`. SSO may also be used for defining login and logout URL.

Note, the `Logout URL` does not apply to session timeouts. If the HTTP/S session experiences a timeout then user will be redirected to the login page.

See also

Web SSO

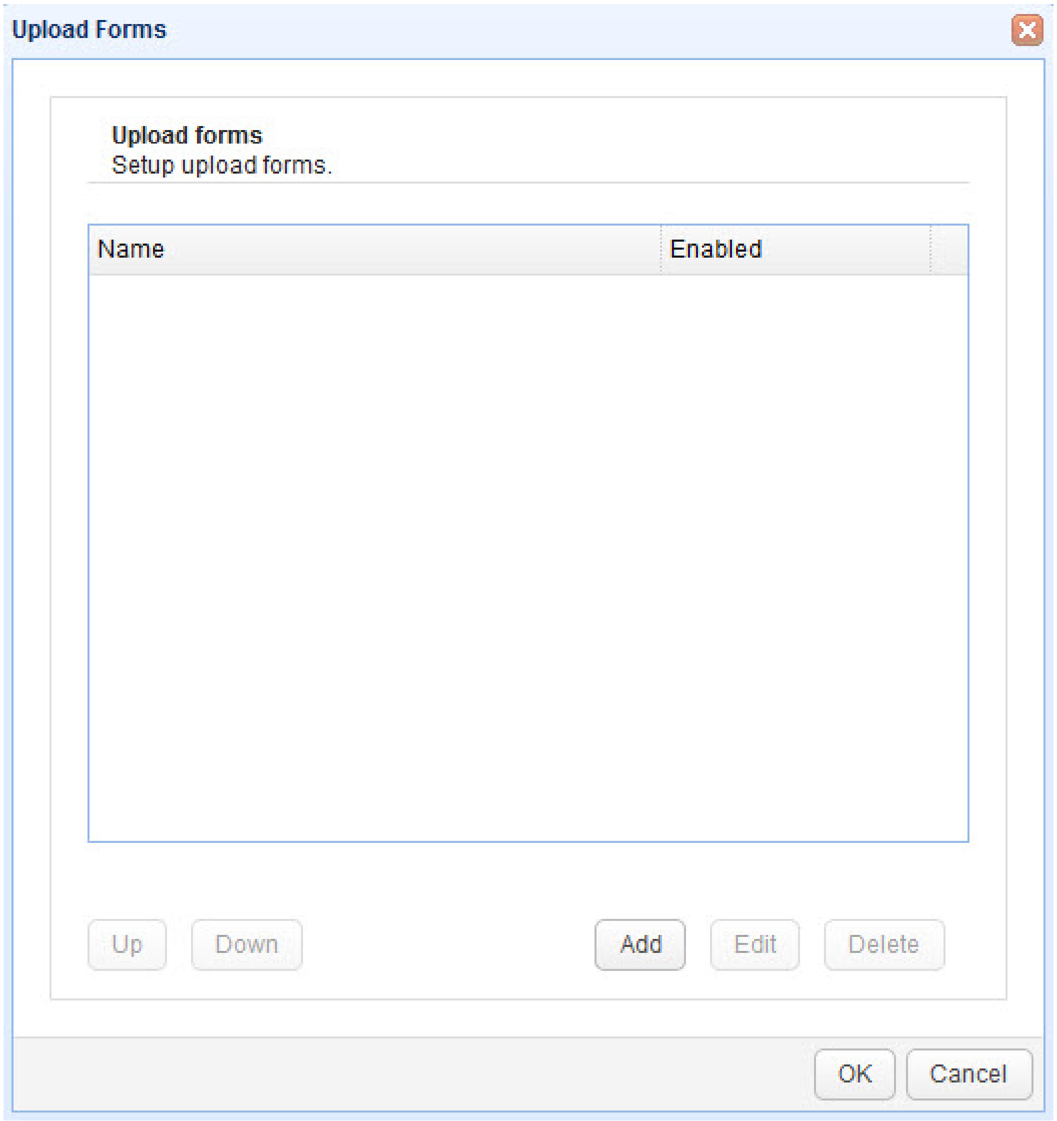
Adding custom forms on file upload

When uploading files using the web based HTML user interface you can optionally request additional information from users to be included with the file upload. This information can be included on a per file basis or in batch mode and captured as part of the `File Upload` event in a trigger.

Creating an upload form

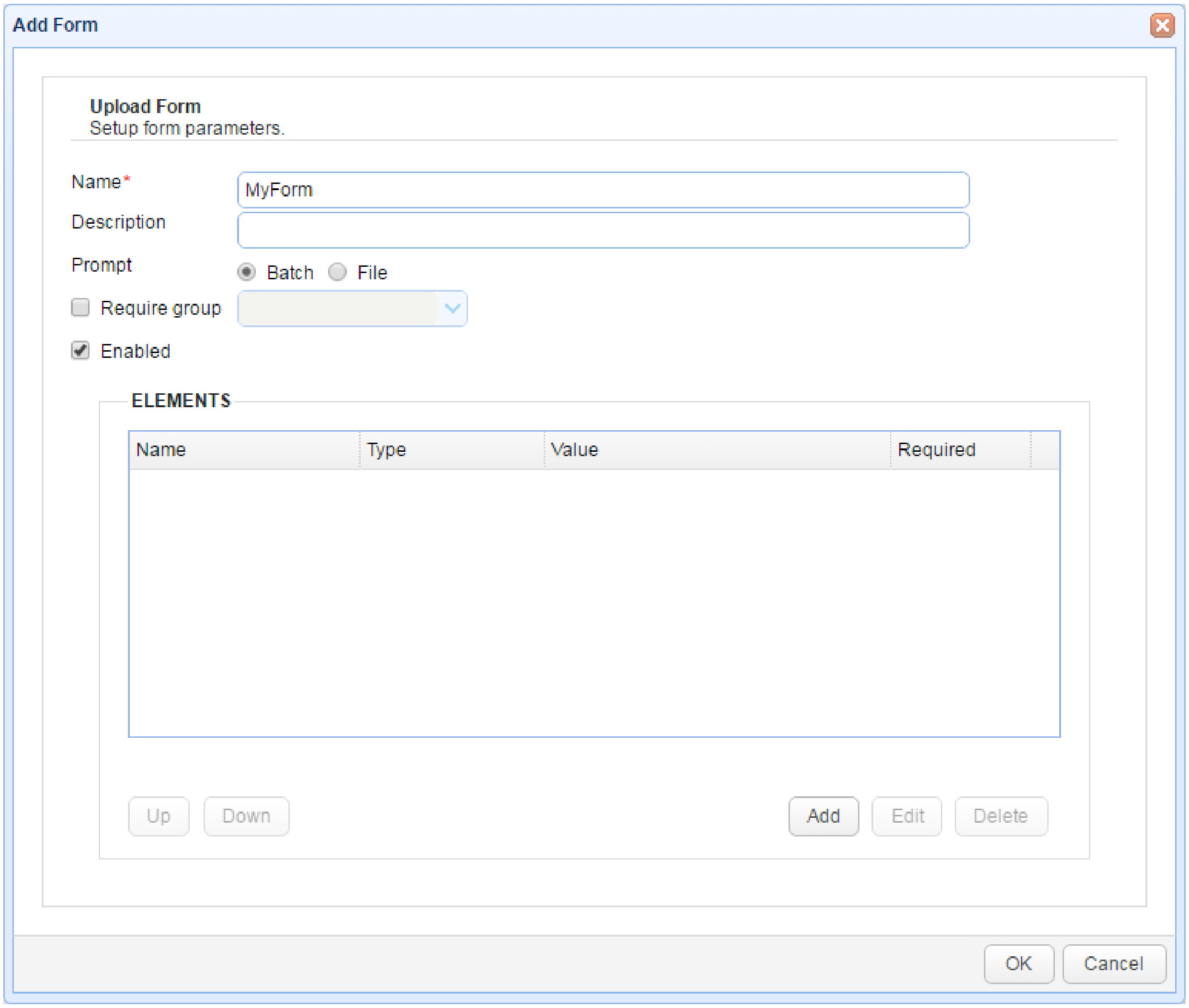
To create an upload form go to the `Services > HTTP/S` panel in JSCAPE MFT Server Manager and click on the `Forms` button. The `Upload Forms` dialog is displayed showing a list of current forms.

Figure 121



To add a form, click on the `Add` button. The `Add Form` dialog is displayed.

Figure 122



Add Form

Upload Form
Setup form parameters.

Name* MyForm

Description

Prompt ● Batch ○ File

□ Require group

☑ Enabled

ELEMENTS

Name	Type	Value	Required

Name - The Name of this form.

Description - A brief description of this form.

Prompt - Sets the prompt method for this form. Batch mode shows the form once for a batch of files to be uploaded. File mode shows the form for each file to be uploaded.

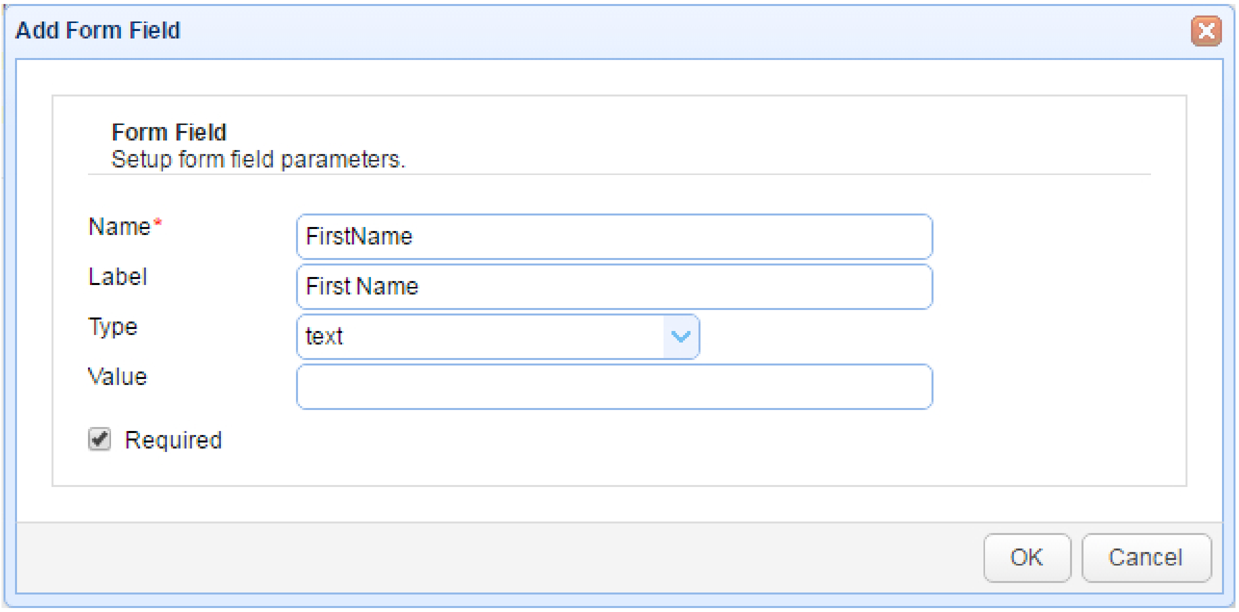
Require group - Requires that user be a member of specified group for form to be available.

Enabled - Sets whether the form is enabled.

Creating upload form fields

To add a form field click on the Add button.

Figure 123



Add Form Field

Form Field
Setup form field parameters.

Name*	FirstName
Label	First Name
Type	text
Value	

☑ Required

Forms may include one or more of the following field types:

Text - A single line text field.

Memo - A multi-line text field.

Dropdown - A single select drop-down list. Available choices must be specified in Value field in comma delimited format. e.g. value1,value2,value3

Multiselect - A multi-select drop-down list. Available choices must be specified in Value field in comma delimited format. e.g. value1,value2,value3

Radio - A single select radio button option. Available choices must be specified in Value field in comma delimited format. e.g. value1,value2,value3

Capturing upload form data

Upload form data can be captured by listening for the File Upload event in a trigger. There are two event properties in each `File Upload` event that you can use to detect whether form data was submitted and the form used.

`FormDataFound` - Whether or not form data was included as part of file upload.

`UploadFormName` - The name of the upload form used if form data is found.

Form field information can be captured using the event property `UploadForm.UploadFormName.UploadFormFieldName`. For example, if you have a form named `Comments` with a field named `Feedback` then the event property to get this field would be `UploadForm.Comments.Feedback`.

Web based file transfers

7

Enabling web document viewer

JSCAPE Web Document Viewer is available as part of the Enterprise Edition of JSCAPE MFT Server product. JSCAPE Web Document Viewer simplifies content distribution by embedding a document viewer in the JSCAPE MFT Server web interface allowing users to view documents on the server without having to download files locally or have supporting software installed.

* Note, JSCAPE Web Document Viewer may only be used to view files that physically reside on the server. Files that are located on another server and are accessible via a reverse proxy are not visible when using JSCAPE Web Document Viewer.

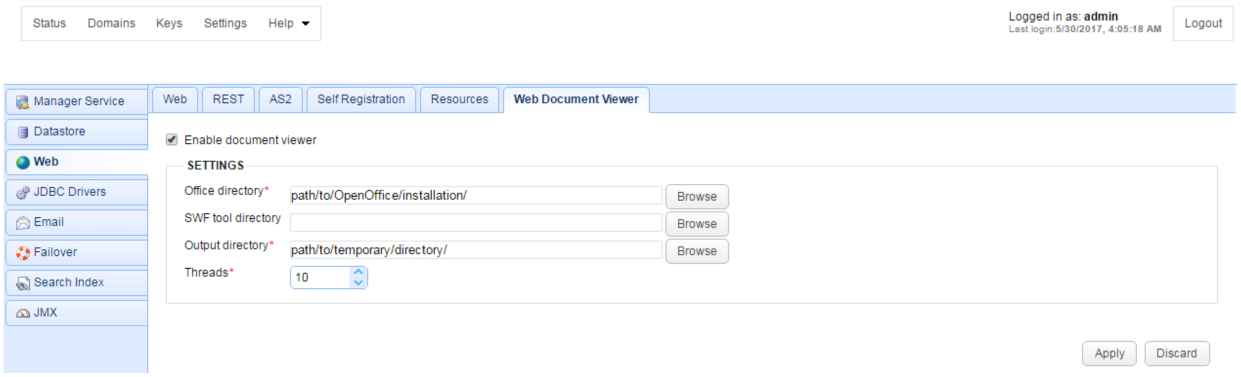
Installation and Configuration
Usage
Supported Document Formats

Installation and Configuration

The steps for installation and configuration of JSCAPE Web Document Viewer are as follows:

1. Download and install the latest version of OpenOffice or LibreOffice for your platform.
2. Download and install the latest version of SWFTools for your platform.
3. Go to `Settings > Web > Web Document Viewer` panel in JSCAPE MFT Server Manager.
4. Check the `Enable document viewer` option and set the installation directories of OpenOffice/LibreOffice and SWFTools. Additionally, set a temporary directory to be used for file conversion purposes.
5. Click the `Apply` button to save settings.

Figure 124



☑ Enable document viewer

SETTINGS

Office directory* path/to/OpenOffice/installation/
SWF tool directory
Output directory* path/to/temporary/directory/
Threads* 10

Enable document viewer - Enables/disables JSCAPE Web Document Viewer service.

Settings

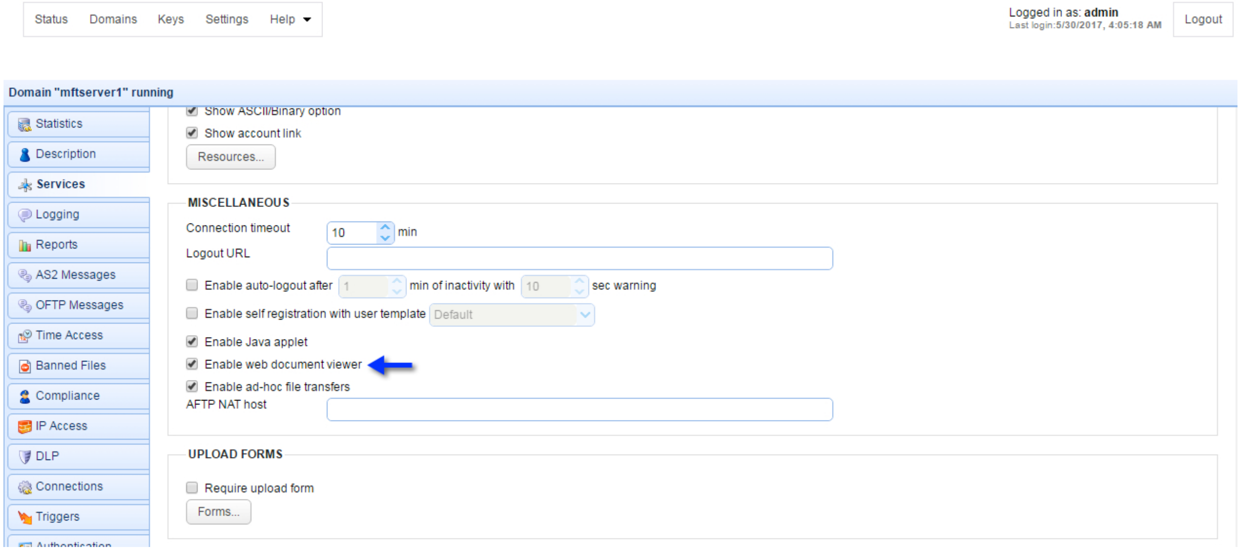
Office directory - The installation directory of OpenOffice/LibreOffice.

SWF tool directory - The installation directory of SWFTools.

Output directory - Temporary directory to be used for document conversion.

6. Enable web document viewer for HTTP/S services in the domain level (`Services > HTTP/S panel`). Click `Apply` to save the settings.

Figure 125



Logged in as: **admin**
Last login:5/30/2017, 4:05:18 AM

Domain "mftserver1" running

☑ Show ASCII/Binary option
☑ Show account link

MISCELLANEOUS

Connection timeout 10 min
Logout URL
☐ Enable auto-logout after 1 min of inactivity with 10 sec warning
☐ Enable self registration with user template Default
☑ Enable Java applet
☑ Enable web document viewer
☑ Enable ad-hoc file transfers
AFTP NAT host

UPLOAD FORMS

☐ Require upload form

Usage

To use JSCAPE Web Document Viewer login to the JSCAPE MFT Server Web Client. At this point you should see a `View` button on the main toolbar. To view a document in the HTML user interface, select the checkbox next to the document filename and click the `View` button. For the JavaWS user interface a similar icon is presented in the remote directory toolbar.

Supported Document Formats

```
OpenDocument Text (*.odt)
OpenOffice.org 1.0 Text (*.sxw)
Rich Text Format (*.rtf)
Microsoft Word (*.doc,*.docx)
WordPerfect (*.wpd)
Plain Text (*.txt)
HTML1 (*.html,*.htm)
OpenDocument Spreadsheet (*.ods)
OpenOffice.org 1.0 Spreadsheet (*.sxc)
Microsoft Excel (*.xls,*.xlsx)
Comma-Separated Values (*.csv)
Tab-Separated Values (*.tsv)
```

```
OpenDocument Presentation (*.odp)
OpenOffice.org 1.0 Presentation (*.sxi)
Microsoft PowerPoint (*.ppt,*.pptx)
OpenDocument Drawing (*.odg)
Portable Document Format (*.pdf)
Flash (*.swf)
JPG (*.jpg,*.jpeg)
GIF (*.gif)
PNG (*.png)
```

Drop zones

Drop zones are a way for you to create a space where users can upload files anonymously via their web browser. Users accessing a drop zone are shown an upload form that allows them to upload one or more files. These users cannot see any of the files that they or other users have uploaded to the drop zone.

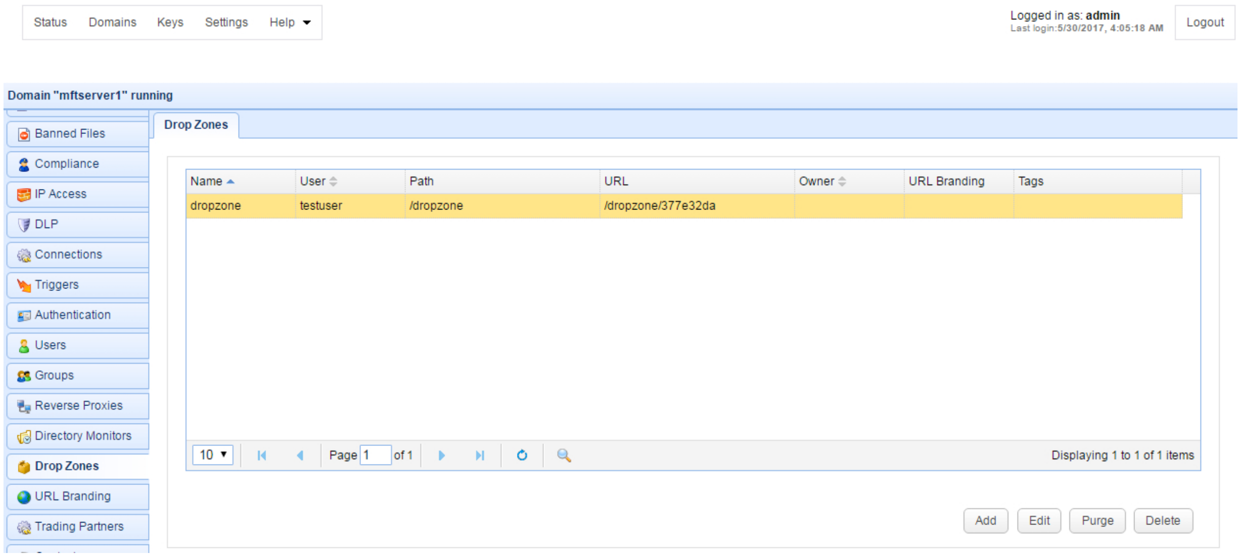
A drop zone is typically used when you want to receive files from one or more people but don't want to create an account for them, allowing them to upload files anonymously.

Creating a drop zone
Purging a drop zone
Detecting files uploaded to a drop zone

Creating a drop zone

To create a drop zone go to the `Drop Zones` module in JSCAPE MFT Server Manager.

Figure 135



Logged in as: **admin**
Last login:5/30/2017, 4:05:18 AM

Domain "mftserver1" running

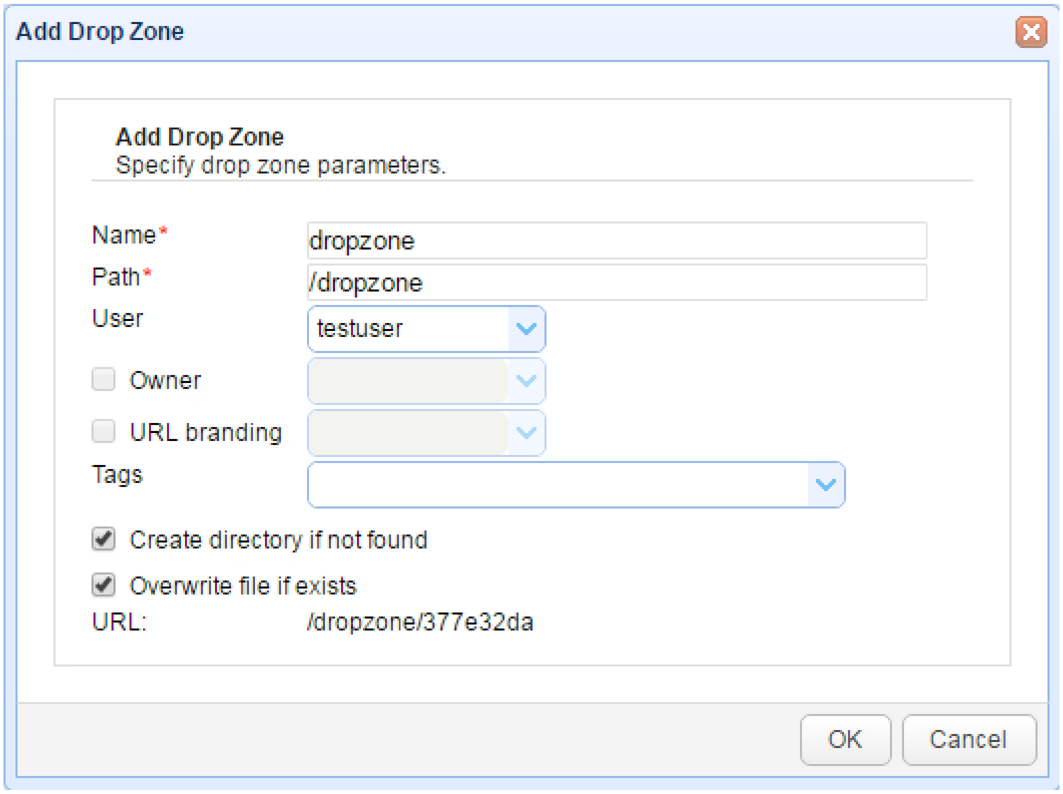
Name	User	Path	URL	Owner	URL Branding	Tags
dropzone	testuser	/dropzone	/dropzone/377e32da			

Page 1 of 1

Displaying 1 to 1 of 1 items

Click the `Add` button. The `Add Drop Zone` dialog is displayed.

Figure 136



Add Drop Zone
Specify drop zone parameters.

Name* dropzone
Path* /dropzone
User testuser
□ Owner
□ URL branding
Tags
☑ Create directory if not found
☑ Overwrite file if exists
URL: /dropzone/377e32da

Name - A unique name to assign to the drop zone.

Path - The virtual path for the account that files uploaded to drop zone will be placed in.

User - The user that this drop zone is mapped to.

Owner - The optional domain administrator who owns this drop zone.

URL branding - The optional URL branding to apply to this drop zone. If set the logo for the URL branding will be used when accessing the drop zone.

Tags - If used, then administrative users who are not flagged as system administrators will be limited to accessing drop zones that are tagged and assigned to their administrative role(s).

Create directory if not found - If virtual path for account is not found then it will be created when drop zone is first accessed.

Overwrite file if exists - If file with same name exists in Path then file will be overwritten, otherwise a unique sequential identifier will be added to filename.

URL - The relative URL that is assigned to the drop zone. This is unique and is automatically generated.

Purging a drop zone

You may purge files from a drop zone as needed. This will effectively delete all files in the drop zone for the mapped account / virtual path. Use this with extreme caution as deleted files may not be recovered.

To purge files from a drop zone go to the `Drop Zones` module in JSCAPE MFT Server Manager, select the drop zone you would like to purge and click the `Purge` button. See *Figure 135* above.

Web based file transfers

7

Detecting files uploaded to a drop zone

Files uploaded to a drop zone will fire a `File Upload` trigger event, similar to the way that files uploaded using the standard web interface or other file transfer services will also fire a `File Upload` event. This event can be captured using a trigger and responded to based on your needs. For example, anytime a file is uploaded to the drop zone you may wish to move the file to another location using `Move File` action, followed by sending out an email notification using the `Send Email` action.

See also

[Trigger management]

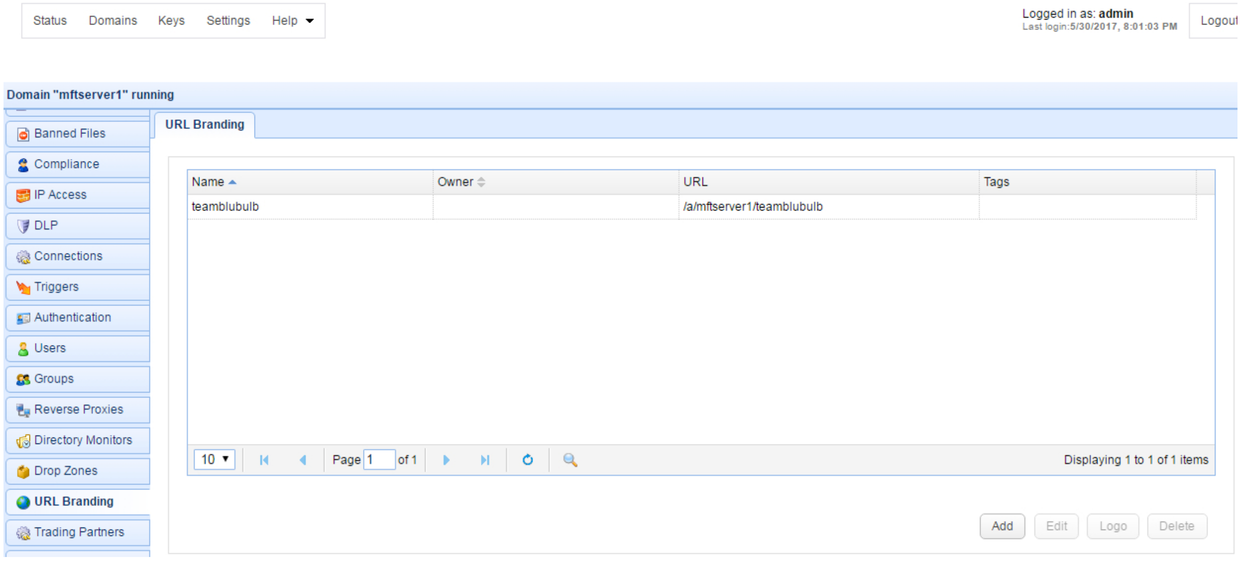
URL branding

URL branding allows you to specify one or more custom login pages when using the web interface. This is useful in shared environments where you have several customers / users accessing a single domain and you want them each to have their own custom logo displayed.

Creating URL branding

To create a URL branding instance go to the `URL Branding` module in JSCAPE MFT Server Manager.

Figure 137



Logged in as: **admin**
Last login:5/30/2017, 8:01:03 PM

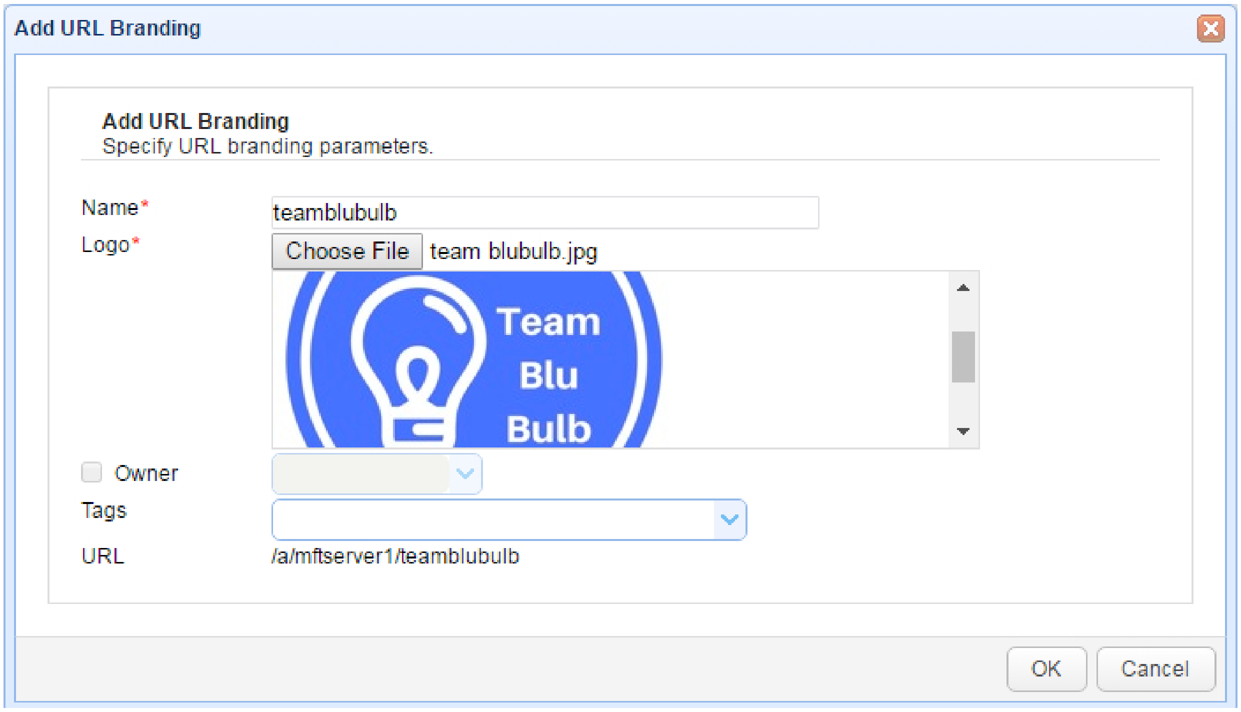
Domain "mftserver1" running

Name	Owner	URL	Tags
teamblubulb		/a/mftserver1/teamblubulb	

Displaying 1 to 1 of 1 items

Click the `Add` button. The `Add URL Branding` dialog is displayed.

Figure 239



Add URL Branding

Add URL Branding
Specify URL branding parameters.

Name* teamblubulb
Logo* Choose File team blubulb.jpg

□ Owner
Tags
URL /a/mftserver1/teamblubulb

Name - A unique alpha-numeric name used to identify this URL branding instance. This name will be used in generating the URL used for accessing the login page.

Logo - The logo to display in login and subsequent pages when accessing and logging in via URL.

Owner - Optional owner field. This may be set to a domain administrator. If the domain administrator has rights to manage URL branding instances then they will be able to manage this URL branding instance from the web interface.

Tags - Use tags to limit the administrators that may have access to this URL branding.

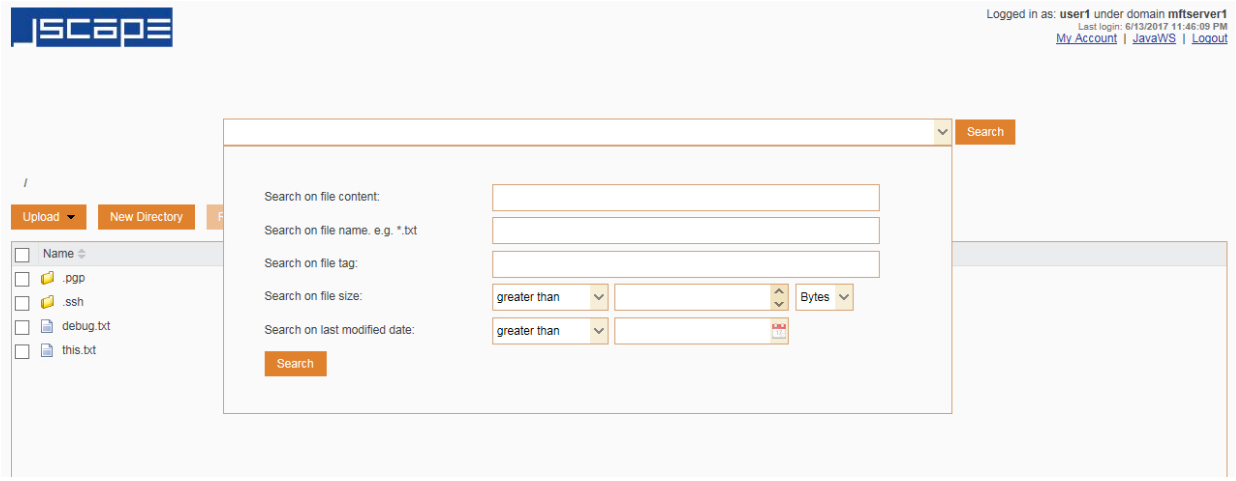
URL - The URL to use to access this URL branded instance.

Searching and tagging documents

Using JSCAPE MFT Server Web Client you can search documents based on their indexed file contents, filename, filesize, last modified date, or keyword tags that you associate with documents.

Searching documents

Figure 140



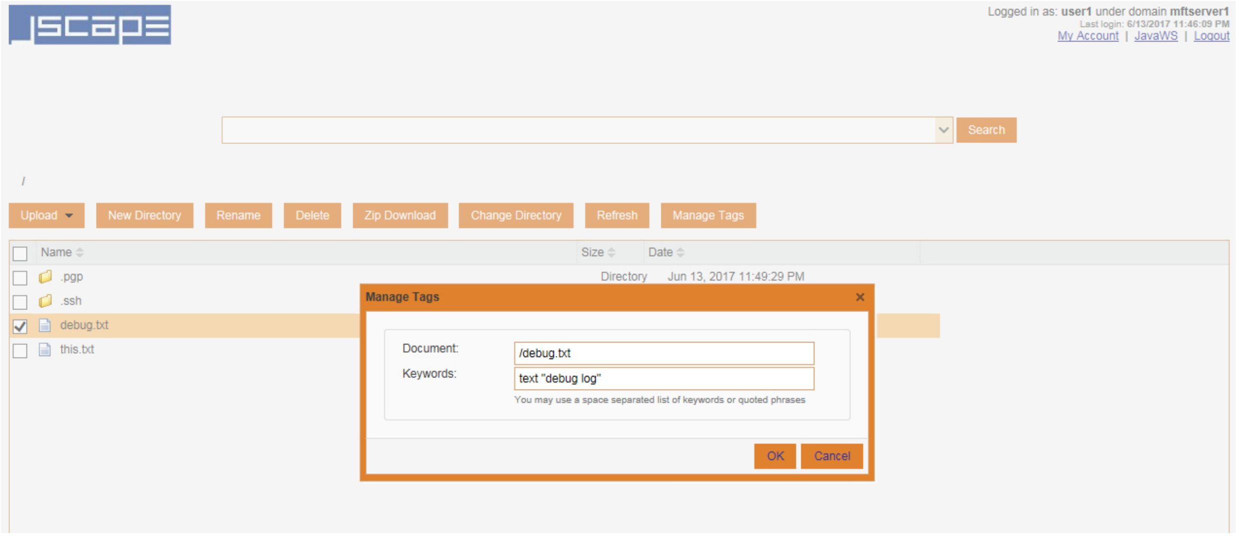
Logged in as: **user1** under domain **mftserver1**
Last login: 6/13/2017 11:46:09 PM

Search on file content:
Search on file name. e.g. *.txt
Search on file tag:
Search on file size: greater than Bytes
Search on last modified date: greater than

Tagging documents

To tag a document select the checkbox next to the filename in the web interface. Next, click the `Manage Tags` button to associate tags with this document and the `Manage Tags` dialog will be displayed prompting you for a space separated list of keywords or phrases to associate with this document. Phrases consisting of multiple words should be quoted. To remove tags for a document click the `Manage Tags` button, remove desired keywords or phrases from the Keywords field and click `OK` to save.

Figure 141



Logged in as: **user1** under domain **mftserver1**
Last login: 6/13/2017 11:46:09 PM

Name	Size	Date
.pgp	Directory	Jun 13, 2017 11:49:29 PM
.ssh		
☑ debug.txt		
this.txt		

Manage Tags

Document: /debug.txt
Keywords: text "debug log"
You may use a space separated list of keywords or quoted phrases

Overview

JSCAPE MFT Server Enterprise Edition supports ad-hoc email transfers. Ad-hoc email transfers offer a method in which users of JSCAPE MFT Server Web Client can email files to any valid email address while avoiding the problems typically associated with emailing files. Unlike a typical email client that attaches files to an email message and sends the email message to the recipient, ad-hoc email transfer send a very small email message to the user with one or more automatically generated web based links embedded in the body of the message. The web based links embedded in the email message provide information on the files sent and allow the recipient to download the files at their own leisure.

Ad-hoc email transfers provide the following benefits:

Email transfers 8

- Avoid bounced emails due to large file attachments or strict firewall rules at the email server.
- Avoid clogging recipients inbox with large file attachments allowing user to download files at their convenience.
- Email multiple files or entire directories with ease.
- Receive optional notification when recipient picks up files.
- Streamline document collaboration both internally and with customers.
- Restrict access to content after a given period of time.
- Email files to users without having to create a user account on the server.

See also

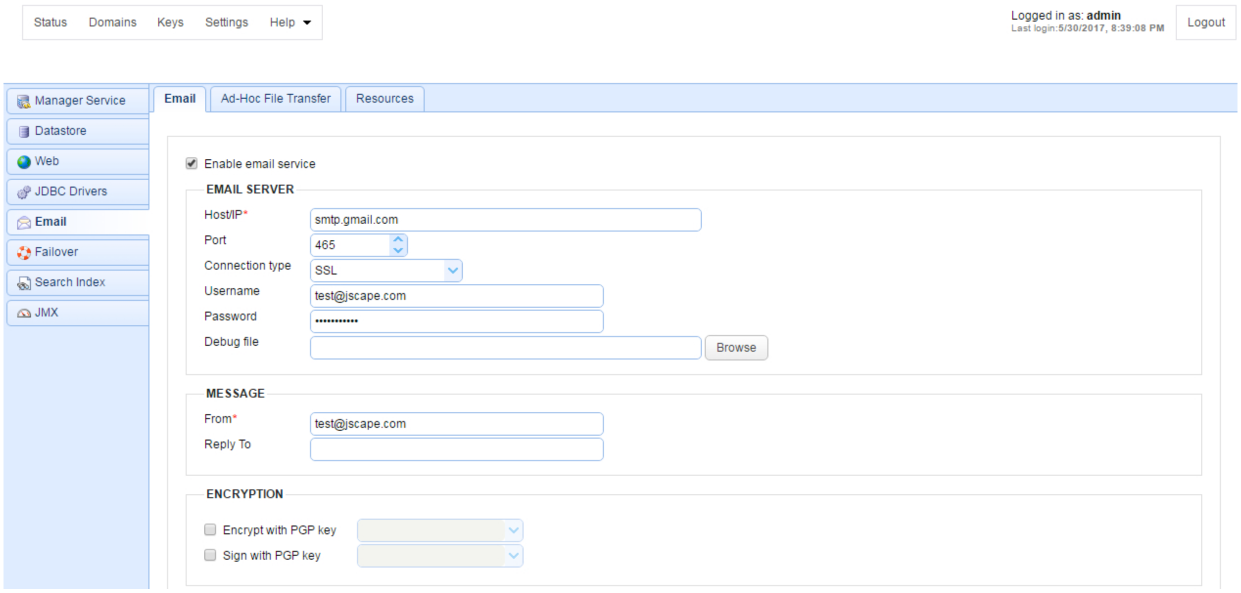
Enabling email transfers
Emailing files
Managing contacts

Enabling email transfers

Email transfers may be enabled in the `Settings > Email` panel. For a user to be able to perform ad-hoc email transfers,

1. The `Enable email service` option must be enabled in the `Settings > Email > Email` panel;
2. The `Enable ad-hoc email transfers` option must be enabled in the `Settings > Email > Ad-Hoc File Transfer` panel; and
3. The `Enable ad-hoc email transfers` option must be enabled for the specified user account in the domain level.

Figure 91



☑ Enable email service

EMAIL SERVER

Host/IP* smtp.gmail.com
Port 465
Connection type SSL
Username test@jscape.com
Password ••••••••••
Debug file

MESSAGE

From* test@jscape.com
Reply To

ENCRYPTION

☐ Encrypt with PGP key
☐ Sign with PGP key

Enable email service - Enables email

Email Server

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

Port - The port of the SMTP server.

Connection type - 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 - Optional From address used when sending emails. This may be overridden by user when performing ad-hoc email transfers.

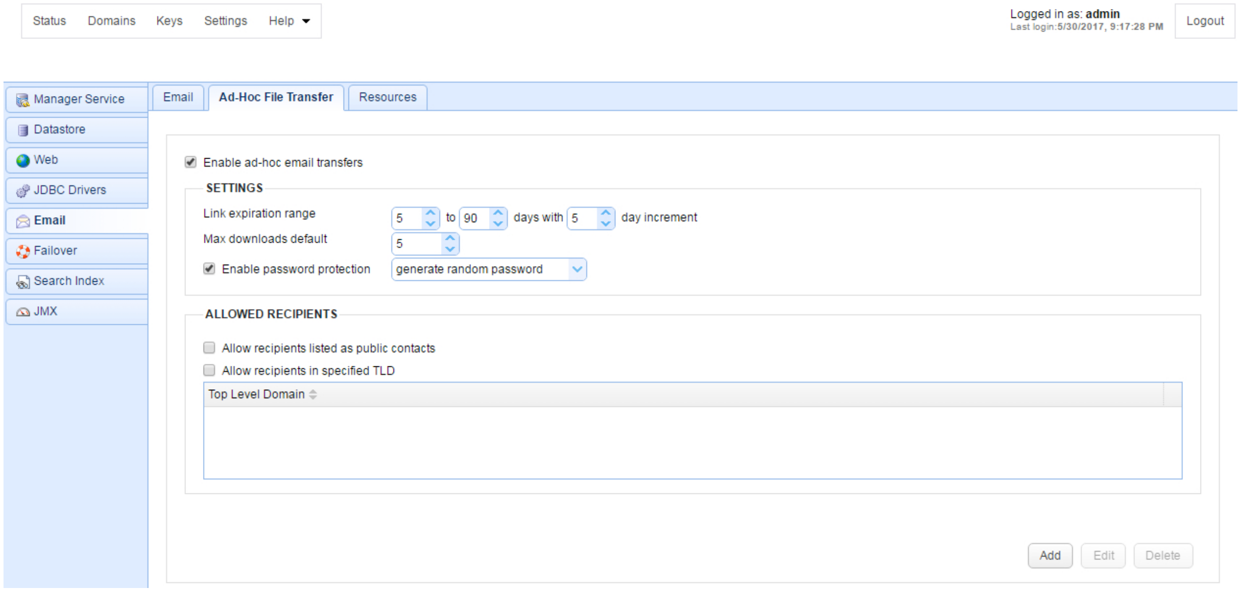
Reply To - Optional Reply-To address used when sending emails. This may be overridden by user when performing ad-hoc email transfers.

Encryption

Encrypt with PGP key - Optional encryption key for use in OpenPGP encrypting outbound email messages.

Sign with PGP key - Optional signing key for use in OpenPGP signing outbound email messages.

Figure 147



☑ Enable ad-hoc email transfers

SETTINGS

Link expiration range 5 to 90 days with 5 day increment

Max downloads default 5

☑ Enable password protection generate random password

ALLOWED RECIPIENTS

□ Allow recipients listed as public contacts

□ Allow recipients in specified TLD

Top Level Domain

Ad-Hoc Email File Transfer Settings

Email transfers 8

Enable ad-hoc email transfer - Check to enable email transfers.

Settings

Link expiration range - The minimum and maximum values that will be displayed to user for setting email link expiration.

Max downloads default - If maximum downloads are enabled then this is the default value supplied in web interface.

Enable password protection - Check to password protect email links.

Datastore Settings - Specify how ad hoc email transfer records are stored.

Allowed Recipients

Allow recipients listed as public contacts - Email addresses for public contacts created in Contacts module will be automatically allowed.

Allow recipients in specified TLD - Email addresses which belong to specified TLD (top level domains) will be allowed.

See also

Adding users

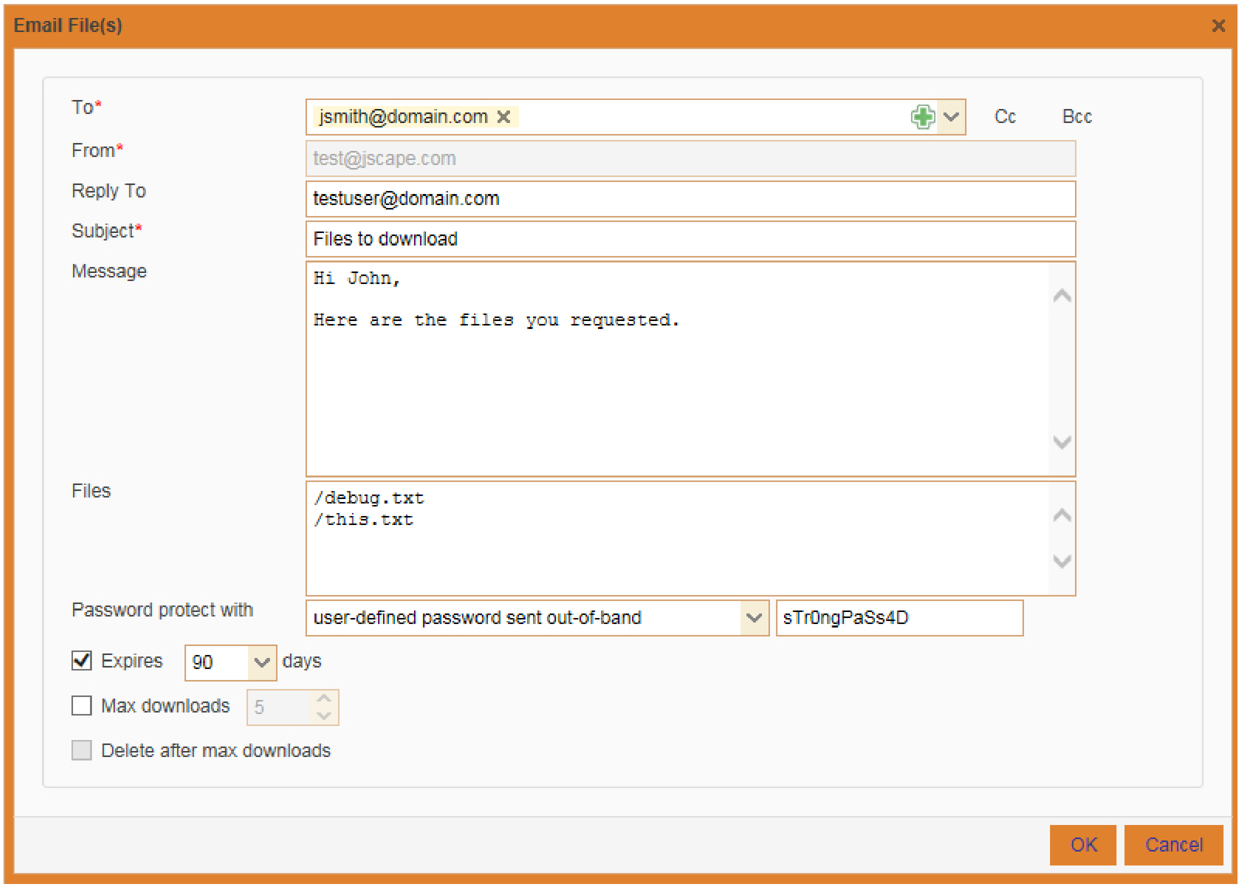
Emailing files

To email files via the JSCAPE MFT Server Web Client select one or more files and/or directories and click the `Email File(s)` button. A dialog will be displayed prompting you for additional information.

Figure 92

Email transfers

8



To*: jsmith@domain.com

From*: test@jscape.com

Reply To: testuser@domain.com

Subject*: Files to download

Message:

```
Hi John,

Here are the files you requested.
```

Files:

```
/debug.txt
/this.txt
```

Password protect with: user-defined password sent out-of-band sTr0ngPaSs4D

☑ Expires 90 days

☐ Max downloads 5

☐ Delete after max downloads

To - The email address to send the email message to. Multiple addresses may be separated using a comma. Existing contacts may be selected by clicking the Contacts icon next to To field.

Cc - Adds Cc (carbon-copy) email addresses.

Bcc - Adds Bcc (blind-carbon-copy) email addresses.

From - The From address to send the email message from. This will default to the email address of the user sending the ad-hoc email. If no email address is found then the From address defined in Settings > Email will be used.

Reply-To - Sets Reply-To header for email message, providing a Reply-To address that may be different than the default From email address.

Subject - The subject of the message.

Message - Custom message to send to recipient.

Files - The files to send.

Password protect with - If password protection is enabled then user may have the option to specify a password. Options available include:

- user-defined password sent out-of-band - Sender specifies a password that is communicated to recipient out-of-band (e.g. over the phone or other method)

- random password sent via email - A random password is generated by the server and included in email message sent to recipient.

Expires - The number of days for which these files may be accessed by the recipient.

Max downloads - The maximum number of times recipient may download files.

Delete after max downloads - Automatically deletes file after maximum number of downloads is reached.

See also

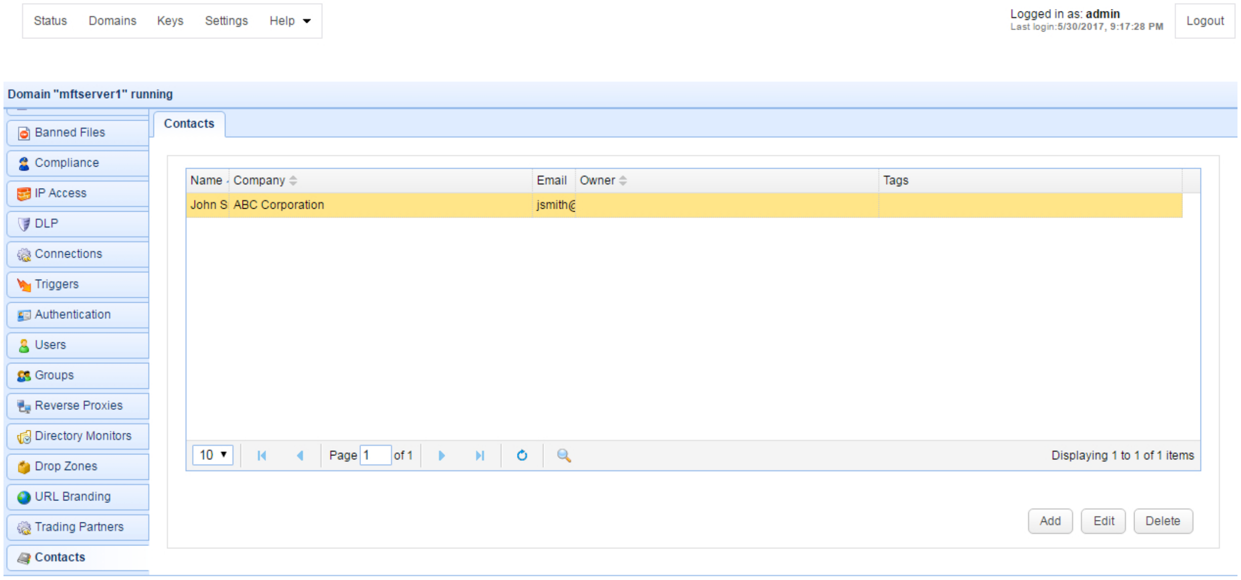
Enabling email transfers

Managing contacts

The `Contacts` module may be used to manage email contacts for use in ad-hoc email transfers. In sending an ad-hoc email transfer recipients may be selected from the Contacts module rather than typing in the email address each time. Contacts may be defined as **private** (visible only to the user that created the contact) or **public** (visible to all users for the domain).

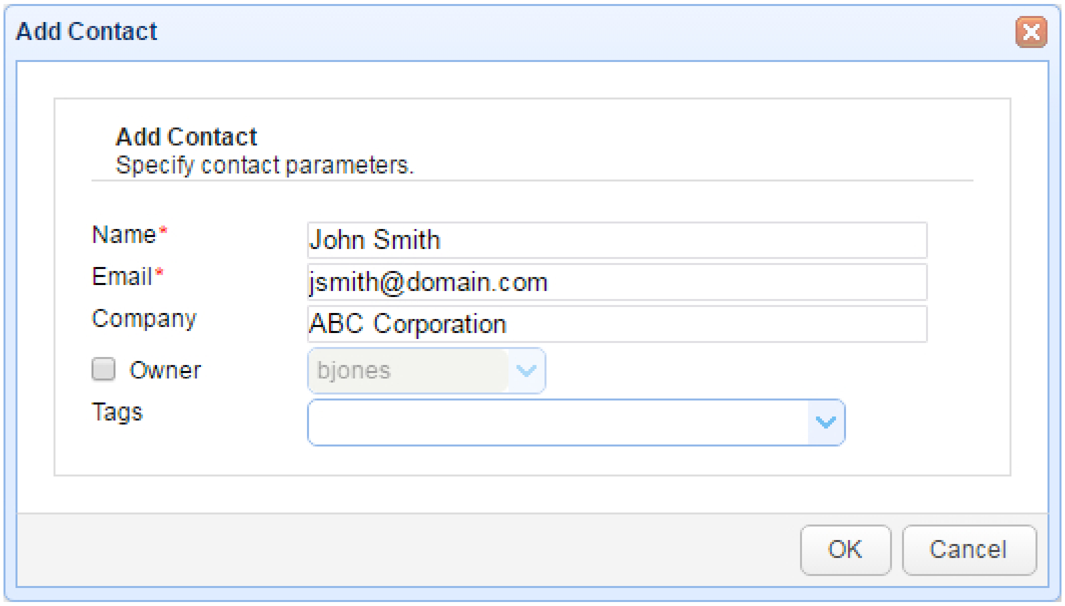
Contacts without an owner are considered private contacts. Contacts may be created/managed from either the `Contacts` module in JSCAPE MFT Server Manager or via the `Contacts` module in the web interface under `My Account`. By default, contacts created in the web interface are private contacts visible only to the user that created them unless user has domain administration rights and the ability to create public contacts.

Figure 144



Name	Company	Email	Owner	Tags
John S	ABC Corporation	jsmith@		

Figure 145



Add Contact
Specify contact parameters.

Name*	John Smith
Email*	jsmith@domain.com
Company	ABC Corporation
□ Owner	bjones
Tags	

Name - The full name of the contact.

Email - The contact email address.

Company - The company name of contact.

Owner - The owner of contact. If an owner is selected then contact will be marked as private and will only be visible to the owner, otherwise contact will be marked as public and will be visible to all users for the domain.

Tags - If used, tags may limit the visibility of this contact for other administrators.

Overview

JSCAPE MFT Server includes support for monitoring local directories for files added, files deleted or files changed. Using a directory monitor you can capture these events and respond to them using a trigger. Generally you should use a directory monitor only when the directory is **not** managed using a service like FTP/S, SFTP or HTTP/S. If the directory is managed using a JSCAPE MFT Server service then you can capture these events more effectively using `File Upload`, `File Renamed` and `File Deleted` event types without using a directory monitor.

See also

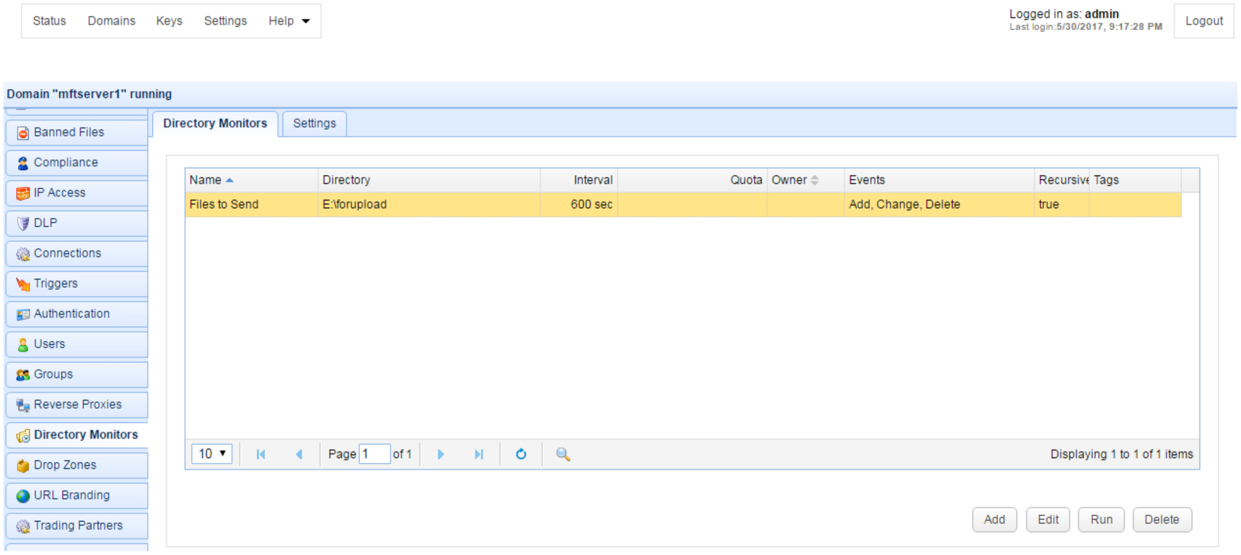
Trigger management
Creating a directory monitor

Creating a directory monitor

To view a list of directory monitors click on the `Directory Monitors` node for the desired domain.

Figure 81

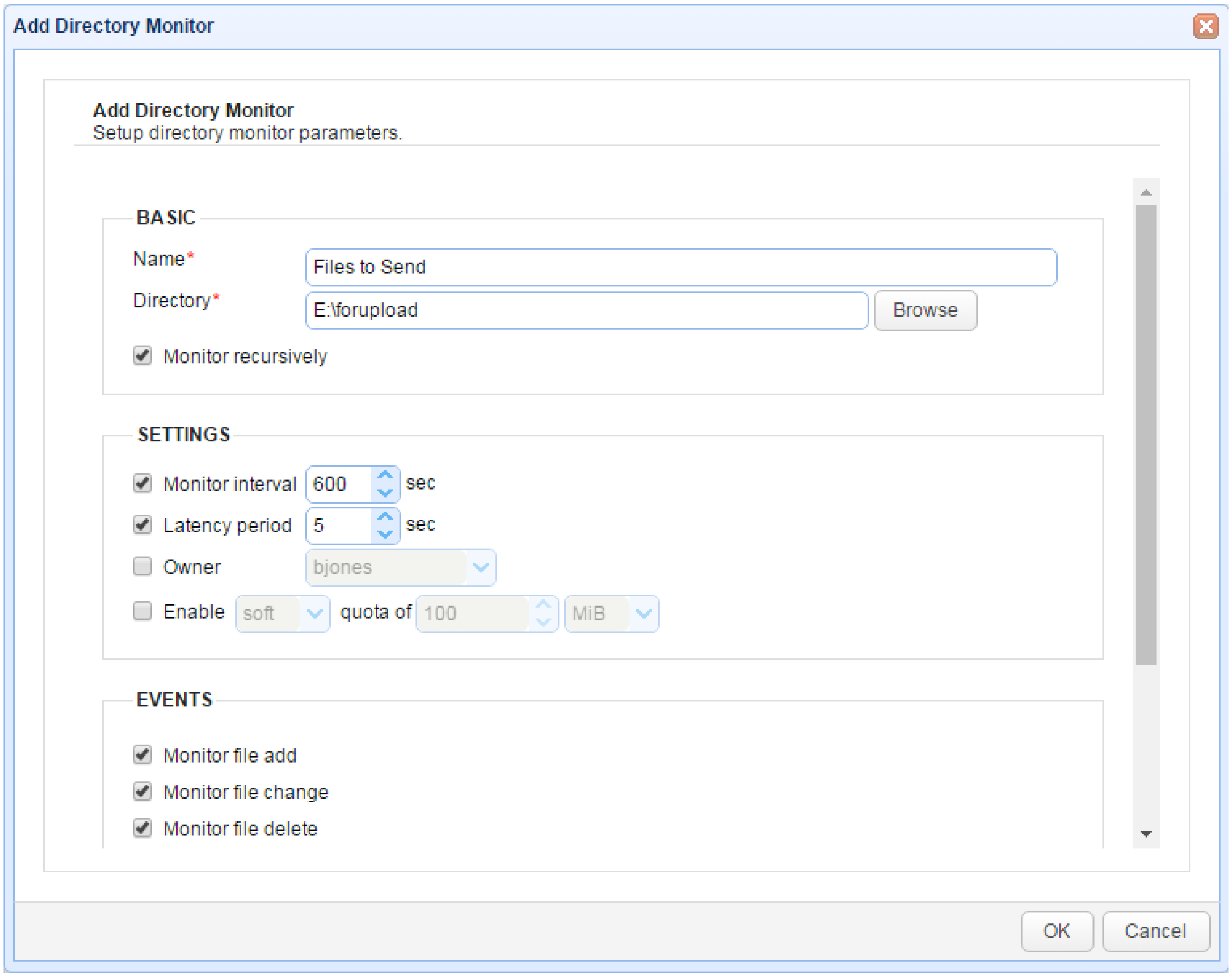
Monitoring directories 9



Name	Directory	Interval	Quota	Owner	Events	Recursive	Tags
Files to Send	E:\forupload	600 sec			Add, Change, Delete	true	

To add a directory monitor click on the `Add` button in the lower right corner. The `Add Directory Monitor` wizard will be displayed.

Figure 82



Add Directory Monitor
Setup directory monitor parameters.

BASIC

Name* Files to Send

Directory* E:\forupload

☑ Monitor recursively

SETTINGS

☑ Monitor interval 600 sec

☑ Latency period 5 sec

☐ Owner bjones

☐ Enable soft quota of 100 MiB

EVENTS

☑ Monitor file add

☑ Monitor file change

☑ Monitor file delete

Monitoring directories 9

Basic

Name - Unique name you wish to assign to this directory monitor.

Directory - The directory you wish to monitor.

Monitor recursively - If checked server will monitor all files in this directory and sub-directories when calculating disk usage against quotas and looking for changes (e.g. new files, deleted files etc.).

Settings

Monitor interval (sec) - The optional frequency in seconds that you wish to check directory for changes. If not enabled then you may run the directory monitor on a scheduled basis using a Current Time event trigger and Run Directory Monitor action or manually from the Directory Monitors module.

Latency period (sec) - If file has been modified within defined latency period then directory monitor event will not be fired. This option may be used to prevent responding to a directory monitor event on a file that is in process of being written.

Owner - Sets the owner for this directory monitor for use in displaying disk quota information via the web interface.

Enable quota (Mb) - The maximum amount of data that may be stored in this directory.

If `soft` quota is selected and that quota is exceeded, file transfers to this directory will still be allowed. However, a Directory Monitor Quota Exceeded event will be fired, which can then be used to notify the administrator of the issue.

If `hard` quota is selected, file transfers to this directory will no longer be allowed once the quota is exceeded.

Events

Monitor file add - Fire a Directory Monitor File Added event whenever a file is added to this directory.

Monitor file change - Fire a Directory Monitor File Changed event whenever a file in this directory is changed.

Monitor file delete - Fire a Directory Monitor File Deleted event whenever a file in this directory is deleted.

File exceeds age of N days - Fire a Directory Monitor File Aged event whenever a file in this directory exceeds age of N days.

Tags

Tags - Use tags to limit the administrators that may have access to this directory monitor.

Once the directory monitor has been created, you can capture any changes made to the directory using triggers and events. The available events for a directory monitor include `Directory Monitor File Added`, `Directory Monitor File Changed`, `Directory Monitor File Deleted, Directory Monitor File Aged, Directory Monitor Updated` and `Directory Monitor Quota Exceeded`. See the user documentation on triggers for more information on how to capture and respond to these events.

Monitoring directories

9

See also

Trigger management
Event types

Overview

What is AFTP?

AFTP (Accelerated File Transfer Protocol) is a file transfer protocol developed by JSCAPE. AFTP is designed to accelerate file transfers over high speed networks that are unable to fully utilize network throughput due to high latency and packet loss. Under these conditions AFTP can accelerate file transfers up to 100 times faster than FTP and other file transfer protocols.

How does it work?

Popular file transfer protocols such as FTP/S, SFTP and HTTP/S depend on an underlying protocol named TCP. The problem with TCP is that as network conditions such as latency and packet loss increase, network throughput is significantly reduced. This is largely to due to the algorithm used to ensure TCP's reliability. TCP uses a sliding window algorithm that reduces throughput as latency and packet loss increase. The result is that file transfer protocols based on TCP are often unable to fully utilize bandwidth available, in effect greatly increasing the amount of time needed to transfer a file. The effects of this are often seen in satellite, transcontinental and transoceanic file transfers.

AFTP solves this problem by changing the way file transfers are performed. Rather than relying exclusively on TCP, AFTP has two communications channels using a combination of TCP and UDP protocols. The first channel, called the control channel, uses TCP and is responsible for tasks such as user authentication, file management and coordinating file transfers. The second channel, called the data channel, uses UDP and is responsible for transferring file data. Unlike TCP, UDP does not suffer the same level of throughput reduction when compared to TCP under similar network conditions. AFTP is able to capitalize on this by transmitting a majority of data over UDP, thus providing optimal throughput. AFTP implementations can achieve reliable file transfers while reducing file transfer times by several orders of magnitude (up to 100x) when compared to TCP based file transfer protocols.

Will AFTP work for me?

AFTP provides the greatest performance gains when used in high bandwidth networks (> 5Mbps) that suffer from high latency (> 50ms). For example, a file transfer between Tokyo and Los Angeles over a 45Mbps connection is likely to have high latency given the geographical distance between these two locations and will benefit from the use of AFTP. Conversely, a file transfer between two hosts on a LAN (Local Area Network) over a 100Mbps connection is unlikely to have high latency or benefit from the use of AFTP.

What is latency?

In a network, latency is a measure of the amount of time it takes for a packet of data to get from one network point to another. Latency can be affected by many variables including distance between points, the number of gateways between points, and the medium used (e.g. wireless, fiber optics). Latency is typically measured in milliseconds (ms). Example: The latency between Host A in Los Angeles and Host B in Tokyo is 200 ms.

What is packet loss?

Packet loss is a network condition when one or more packets of data fail to reach their intended destination. Packet loss is measured as a percentage of packets that do not reach their destination, also known as lost or dropped packets. Example: The packet loss between Host A in Los Angeles and Host B in Tokyo is 1.0%.

What is throughput?

Throughput is the actual rate of data delivery over a network. Throughput is typically measured in bps (bits per second). Throughput is often a fraction of bandwidth due to network conditions such as latency and packet loss. Example: The throughput between Host A in Los Angeles and Host B in Tokyo is 5Mbps.

What is bandwidth?

Bandwidth is the theoretical maximum rate of data delivery over a network. Bandwidth is typically measured in bps (bits per second). Example: The bandwidth between Host A in Los Angeles and Host B in Tokyo is 45Mbps.

What is TCP?

TCP (Transmission Control Protocol) is a reliable IP based network protocol in that all packets are sent in order and if a packet is lost it will automatically attempt to resend that packet. See also TCP on Wikipedia.

What is UDP?

UDP is a sibling to the TCP protocol, both of which are dependent on the underlying IP stack. Unlike TCP, UDP does not require that packets be sent in order and does not automatically attempt to retransmit lost packets. Retransmission and reordering of packets are the responsibility of the higher level protocol, in this instance AFTP. See also UDP on Wikipedia.

Adding AFTP service

The AFTP service may be added using the Services node in JSCAPE MFT Server Manager. The AFTP service is available only in the Enterprise edition of JSCAPE MFT Server.

See also

Adding services

Connecting to AFTP service

In order to connect to the AFTP service you must use an AFTP client. JSCAPE currently offers the following AFTP clients.

AnyClient

AnyClient Enterprise

AnyClient Web

AFTP Java Client Library (*contact JSCAPE for access*)

File Transfer Command Line

Trigger actions

There are also a number of AFTP trigger actions in JSCAPE MFT Server that may be used for automating AFTP file transfer processes.

Accelerated file transfer (AFTP) 10

Overview

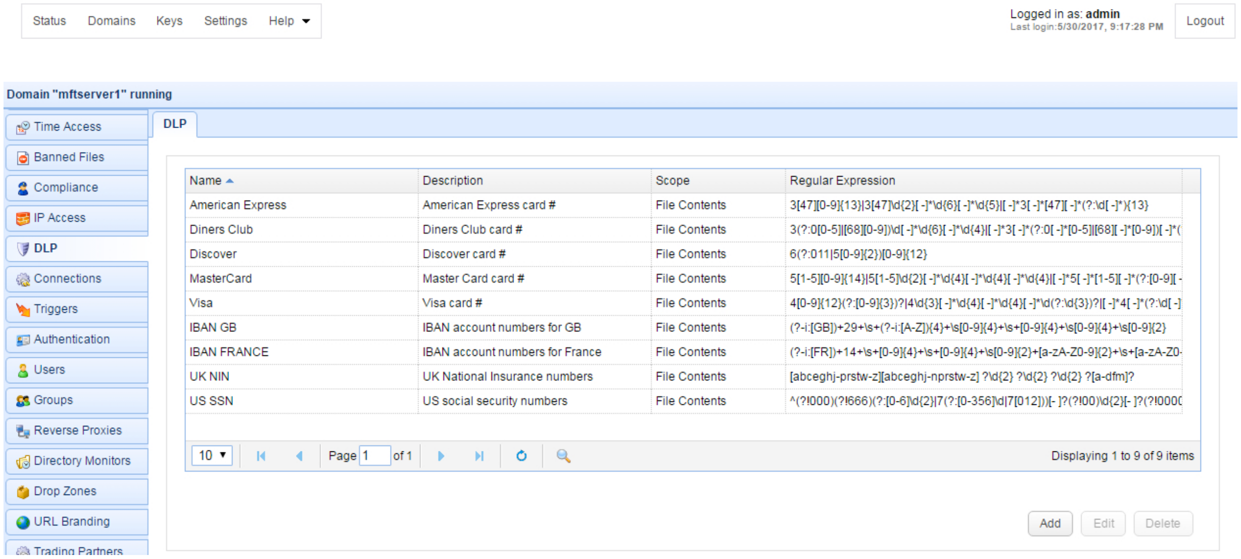
Data Loss Prevention (DLP) are systems that identify and prevent the loss of sensitive data. The DLP module in JSCAPE MFT Server Enterprise Edition can be used to identify sensitive data at rest and prevent it's unauthorized distribution over all file transfer protocols supported by JSCAPE MFT Server.

Creating DLP Rules

DLP rules are regular expressions that are used in identifying sensitive data at rest. JSCAPE MFT Server has a number of built-in rules that may be used to identify sensitive data at rest such as credit card numbers (Visa, MasterCard, Amex, Discover) , U.S. social security numbers, UK national insurance numbers and IBAN account numbers.

To create a DLP rule go to the `DLP` module in JSCAPE MFT Server Manager. Here you will find a list of currently available DLP rules.

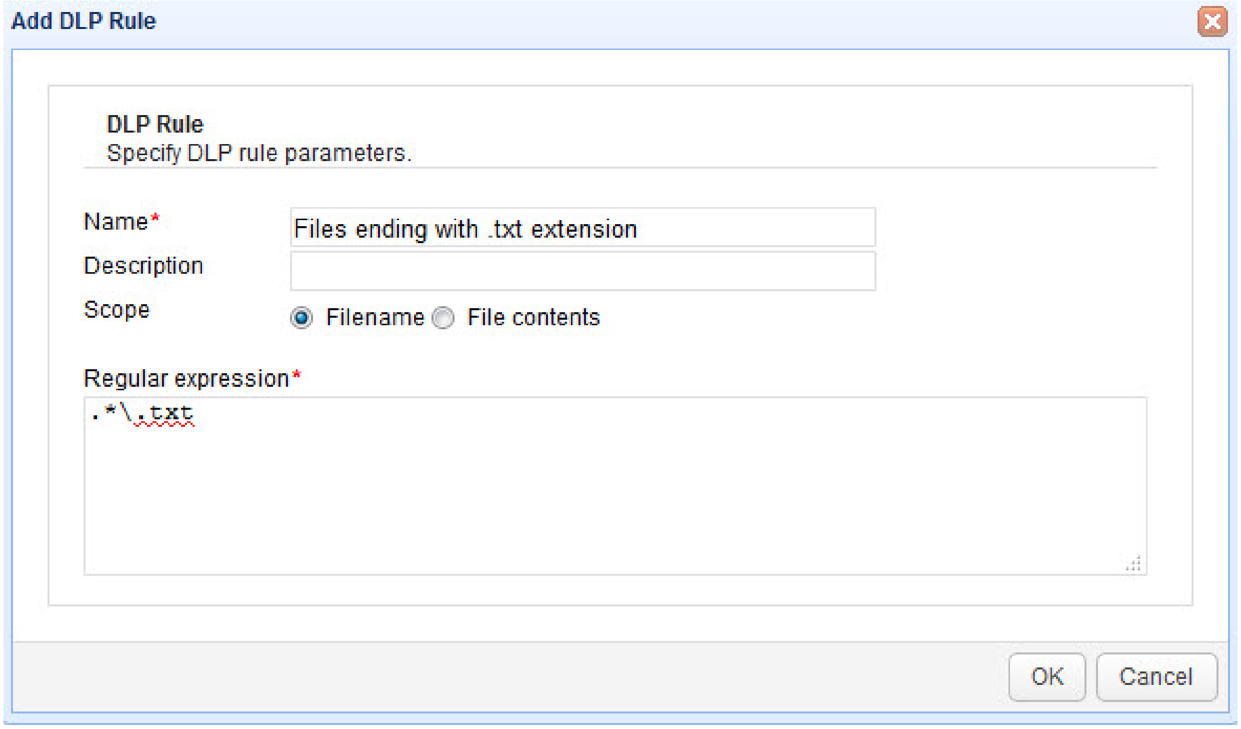
Figure 148



Name ▲	Description	Scope	Regular Expression
American Express	American Express card #	File Contents	3[47][0-9]{13}|3[47]\d{2}[-]*\d{6}[-]*\d{5}|[-]*3[-]*[47][-]*(?:\d[-]*){13}
Diners Club	Diners Club card #	File Contents	3(?:0[0-5]|[68][0-9])\d[-]*\d{6}[-]*\d{4}|[-]*3[-]*(?:0[-]*[0-5]|[68][-]*[0-9])[-]*(
Discover	Discover card #	File Contents	6(?:011|5[0-9]{2})[0-9]{12}
MasterCard	Master Card card #	File Contents	5[1-5][0-9]{14}|5[1-5]\d{2}[-]*\d{4}[-]*\d{4}[-]*\d{4}|[-]*5[-]*[1-5][-]*(?:[0-9][-
Visa	Visa card #	File Contents	4[0-9]{12}(?:[0-9]{3})?|4\d{3}[-]*\d{4}[-]*\d{4}[-]*\d(?:\d{3})?|[-]*4[-]*(?:\d[-]
IBAN GB	IBAN account numbers for GB	File Contents	(?-i:[GB])+29+\s+(?-i:[A-Z]){4}+\s[0-9]{4}+\s+[0-9]{4}+\s[0-9]{4}+\s[0-9]{2}
IBAN FRANCE	IBAN account numbers for France	File Contents	(?-i:[FR])+14+\s+[0-9]{4}+\s+[0-9]{4}+\s[0-9]{2}+[a-zA-Z0-9]{2}+\s+[a-zA-Z0-
UK NIN	UK National Insurance numbers	File Contents	[abceghj-prstw-z][abceghj-nprstw-z] ?\d{2} ?\d{2} ?\d{2} ?[a-dfm]?
US SSN	US social security numbers	File Contents	^(?!000)(?!666)(?:[0-6]\d{2}|7(?:[0-356]\d|7[012]))[-]?(?!00)\d{2}[-]?(?!000(

To create a new rule click on the `Add` button. The `Add DLP Rule` dialog will be displayed.

Figure 149



DLP Rule
Specify DLP rule parameters.

Name*: Files ending with .txt extension
Description:
Scope: ● Filename ○ File contents

Regular expression*
.*\.txt

Name - Unique name for the DLP rule.

Description - Description of DLP rule.

Scope - Scope of rule when applying regular expression. A scope of `File contents` will analyze contents of file for instances of regular expression. A scope of `Filename` will analyze filename for instances of regular expression.

Regular expression - The regular expression to use when performing content analysis.

See also

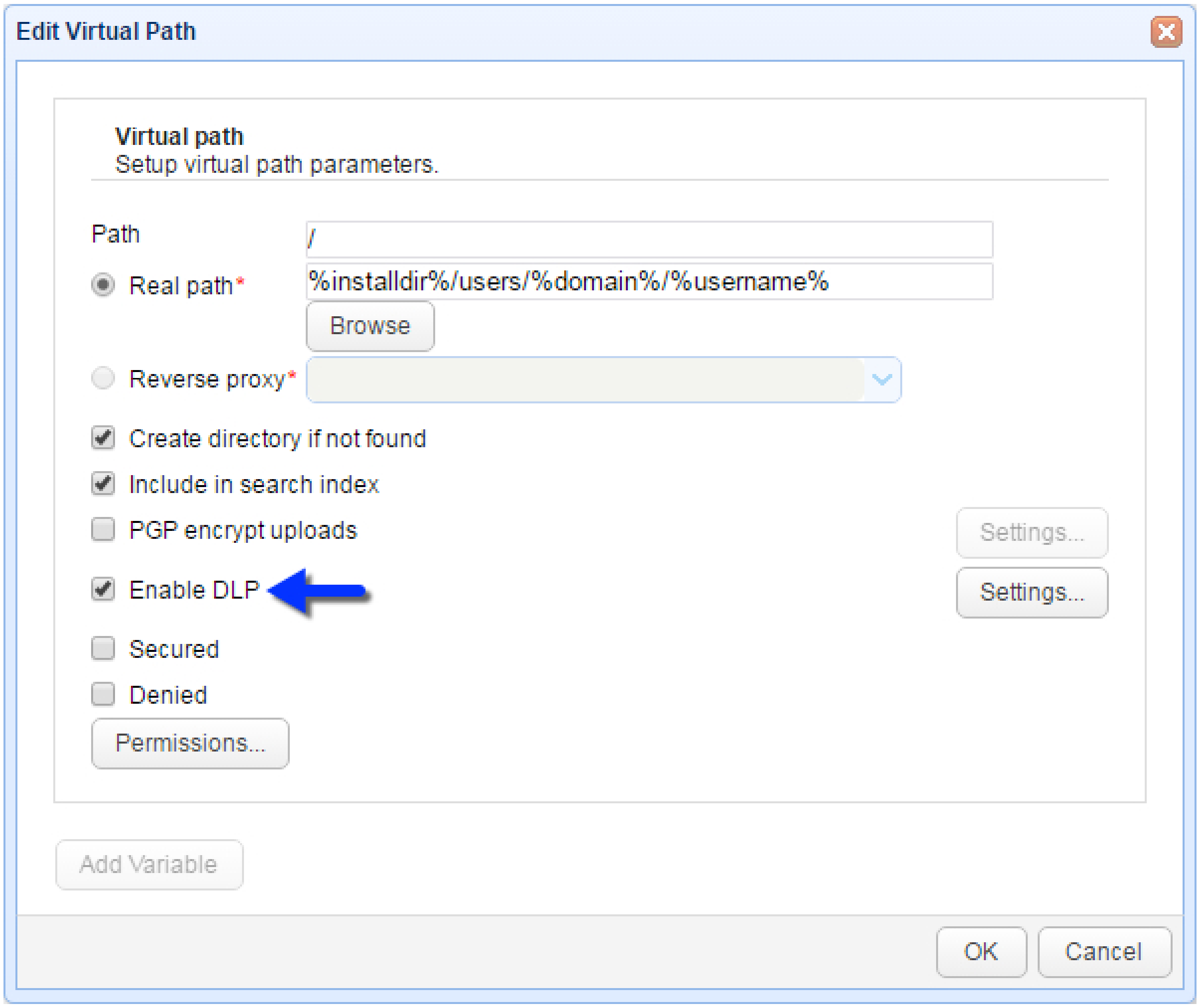
Regular expression reference

Enabling DLP

DLP may be enabled for any virtual path. This gives you the power and flexibility to limit DLP at the directory, user or group level depending on your needs.

To enable DLP for a virtual path, select the virtual path and click `Edit`. Next, click the `Enable DLP` option followed by the `Settings` button to define which DLP rules and actions should be applied to the virtual path.

Figure 150



Edit Virtual Path

Virtual path
Setup virtual path parameters.

Path: /

● Real path*: %installdir%/users/%domain%/%username%

○ Reverse proxy*:

☑ Create directory if not found

☑ Include in search index

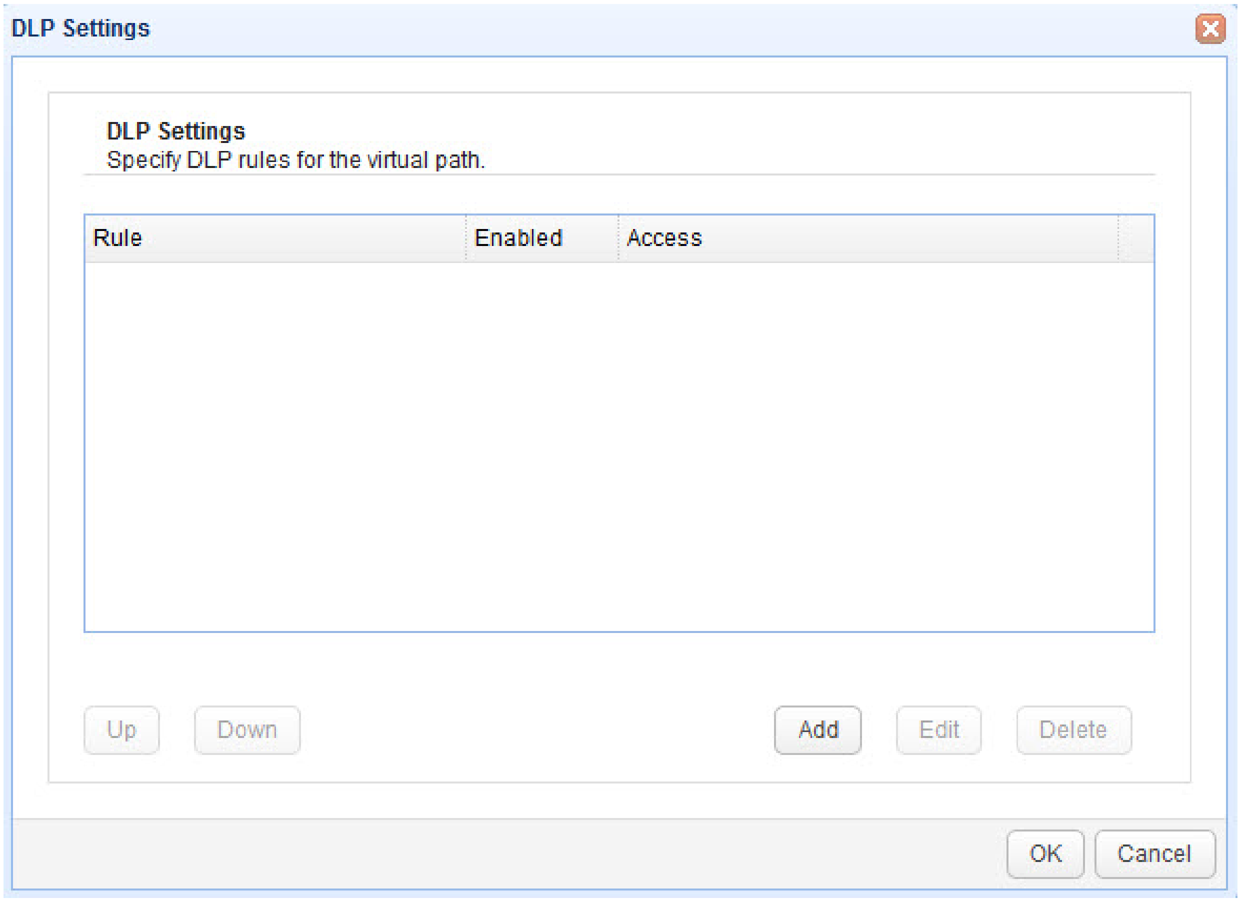
□ PGP encrypt uploads

☑ Enable DLP

□ Secured

□ Denied

Figure 151



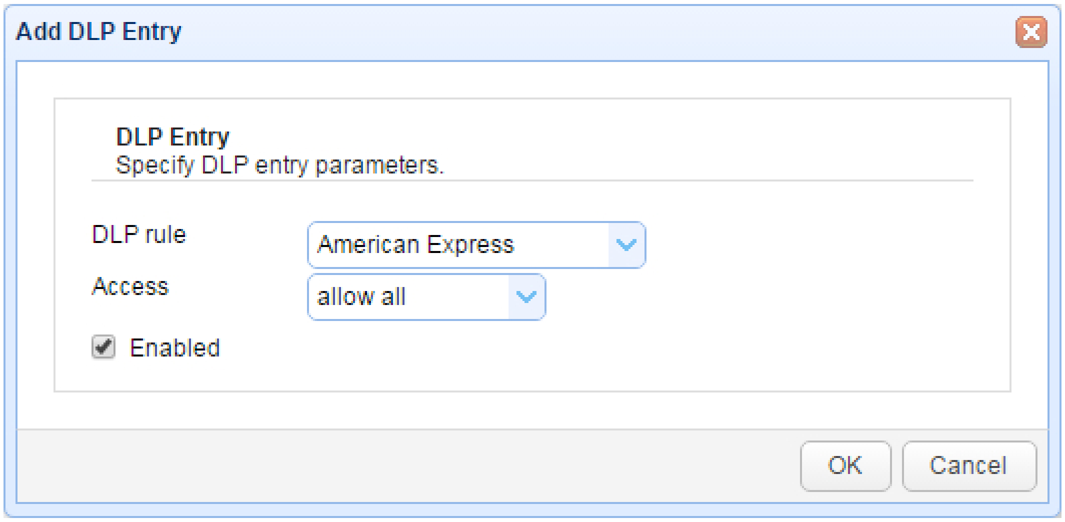
DLP Settings

DLP Settings
Specify DLP rules for the virtual path.

Rule	Enabled	Access

Rules are processed in order. The first rule to match determines access level. Use the "Up" and "Down" buttons to change the order in which rules are processed.

Figure 152



Add DLP Entry

DLP Entry
Specify DLP entry parameters.

DLP rule: American Express
Access: allow all
☑ Enabled

DLP rule - The DLP rule to add.

Access - The level of access to grant when DLP rule regular expression is matched. The `allow all` option allows access and raises a DLP Rule Matched trigger event. The deny all option denies access and raises a DLP Rule Matched trigger event. The deny ad-hoc option denies access to email recipients via ad-hoc file transfer and raises a DLP Rule Matched event.

Enabled - Enables/disables DLP rule.

Capturing DLP events

As part of any DLP implementation you may want to be notified anytime a DLP rule has been triggered. This can be accomplished using a trigger and the DLP Rule Matched event.

See also

Trigger management

Overview

The JSCAPE MFT Server Java Management API is a Java based API for programmatically managing your JSCAPE MFT Server. Using the JSCAPE MFT Server Java Management API you may perform functions like creating domains, adding user accounts, creating groups, stopping and starting domains and various other management functions.

The JavaDoc for the JSCAPE MFT Server Java Management API may be found in the doc/api directory of your JSCAPE MFT Server installation.

See also

Command line utilities
Client REST API
Management REST API

Requirements

The JSCAPE MFT Server Java Management API requires that Oracle or IBM JDK 1.7 or above be used. All classes for the JSCAPE MFT Server Java Management API are part of the ftpserver.jar library which is located in your JSCAPE MFT Server libs directory.

Linux/Solaris/UNIX

The examples provided in the doc/api-examples directory are written to connect to the server using the credentials and server settings stored in the client.cfg configuration file. To run any of the examples you must first configure the client.cfg settings by running the following command.

```
./manager-configuration -host [ip address] -port [port] -rest.host [ip
address] -rest.port [rest.port] -user [username] -password [password]
```

Example

```
./server-configuration -host 127.0.0.1 -port 10880 -rest.host 127.0.0.1 -
rest.port 11880 -user admin -password secret
```

Where [ip address] and [port] are the IP/port that the JSCAPE MFT Server Service is listening on, [rest.port] is the port that the REST web service is listening on, and [username] [password] are the credentials you will use when connecting to the service. Defaults ports for JSCAPE MFT Server

Service and REST web service are `10880` and `11880` respectively.

Creating a domain

Please see the source code example available in the `doc/api-examples/java/create_domain` directory of your JSCAPE MFT Server installation.

Creating an account

Please see the source code example available in the `doc/api-examples/java/create_account` directory of your JSCAPE MFT Server installation.

Creating a group

Please see the source code example available in the `doc/api-examples/java/create_group` directory of your JSCAPE MFT Server installation.

Creating a reverse proxy

Please see the source code example available in the `doc/api-examples/java/create_resource` directory of your JSCAPE MFT Server installation.

Stopping and starting a domain

Please see the source code example available in the `doc/api-examples/java/start_stop_domain` directory of your JSCAPE MFT Server installation.

Client REST API

The client REST API may be used to perform file transfers over HTTP and HTTPS services in JSCAPE MFT Server. To enable client REST services you must enable the HTTP or HTTPS services for JSCAPE MFT Server.

Documentation and Examples

For API documentation on client REST services available visit http://localhost/doc/api where **localhost** is the hostname listening for HTTP requests. Additional REST API examples may be found in the **doc/api-examples/rest** directory relative to your JSCAPE MFT Server installation directory.

See also

Enabling web based file transfers

Management REST API

The management REST API may be used to manage JSCAPE MFT Server over HTTP/S services in JSCAPE MFT Server. To enable management REST services you must enable the REST HTTP and/or REST HTTPS services for JSCAPE MFT Server. To achieve this go to `Settings > Web > REST` from the main menu.

Documentation and Examples

For API documentation on client REST services available visit `http://localhost:11880/` where `localhost` is the hostname and `11880` is the port listening for REST HTTP requests. Next, login using administrative credentials and click the `Help > REST API` link to access the online documentation. Additional REST API examples may be found in the `doc/api-examples/rest` directory relative to your JSCAPE MFT Server installation directory.

REST API 13

See also

Enabling web based file transfers

Overview

Several command line utilities are included as part of JSCAPE MFT Server. Ideal for scripting purposes or for use in a non-GUI environment, these command line utilities allow you to quickly perform common functions without having to use JSCAPE MFT Server Manager.

See also

js-addadmin
js-adddirmonitor
js-adddomain
js-adddropzone
js-addgroup
js-addgroupdir
js-add-server-key
js-addserviceaftp
js-addserviceftp
js-addservicehttp
js-addservicesftp
js-addservicewebdav
js-adduser
js-adduserdir
js-as2purge
js-as2util
js-backuplog
js-client-configuration
js-copyusers
js-database-configuration
js-db-migration
js-deldomain
js-delgroup
js-deluser
js-enablehttp
js-enablehttps
js-importcontacts
js-import-log-searches
js-importusers
js-ipaccess
js-kickuser
js-oftppurge
js-passwd
js-pausedomain
js-resumedomain
js-runtrigger
js-sendmessage
js-server-configuration
js-setdomainquota
js-setuserquota
js-shutdown

Command line utilities 14

Note

Command line argument parameters which contain spaces must be surrounded in quotes to be processed correctly.

```
e.g.

-type "explicit SSL"
```

See also

Management API

js-addadmin

The `js-addadmin` command may be used to add an administrator in JSCAPE MFT Server.

```
Usage: js-addadmin <options>

Options:

[-file <file>] configuration file
-username <username> administrator username
-password <password> administrator password
[-role <name>] administrator role
[-sa] system administrator flag
[-db | -api] database or API access flag; default: -api
-h display this help menu
```

The `-db` option should only be used for emergency recovery purposes (e.g. lost administrative password). When using this option the utility will add an administrator to the database directly without using the API or existing credentials. When using this option it is important that JSCAPE MFT Server be shutdown. Failure to do so may result in potential file locking issues.

js-adddirmonitor

The `js-adddirmonitor` command may be used to add a directory monitor to JSCAPE MFT Server.

```
Usage: js-adddirmonitor -n <value> -r <value> [-options]

Options:

-d the domain name
-n directory monitor name
-r directory path (e.g. c:\home)
-t monitor interval (seconds)
-q directory quota (MB)
```

```
-l latency period
-o directory monitor owner
-a enable monitor file add
-e enable monitor file edit
-de enable monitor file delete
-re enable monitor recursively
-h display this help menu
```

If `js-adddirmonitor` command is run without options then user will be prompted for necessary information.

js-adddomain

The `js-adddomain` command may be used to add a domain to JSCAPE MFT Server.

```
Usage: js-adddomain [-options]

Options:

-d the domain name
-ld log directory
-ds user datastore directory
-h display this help menu
```

If `js-adddomain` command is run without options then user will be prompted for necessary information.

js-adddropzone

The `js-adddropzone` command may be used to add a drop zone to JSCAPE MFT Server.

```
Usage: js-adddropzone [-options]

Options:

[-file <file>] configuration file
-domain <name> domain name
-name <name> zone name
-account <username> account name
-directory <path> virtual directory path in account's file system
[-create-dir] whether directory should be created if it does not exist
[-overwrite-file] whether file should be overwritten if already exist
[-url-branding-name <name>] URL branding to map to the drop zone
[-owner <username>] owner of the drop zone
[-tags <csv list of tags>] zone tags
-h display this help menu
```

If `js-adddropzone` command is run without options then user will be prompted for necessary information.

js-addgroup

The `js-addgroup` command may be used to add a group to JSCAPE MFT Server.

```
Usage: js-addgroup [-options]

Options:

-d the domain name
```

```
-g the groupname
-p the virtual path
-r the real directory path
-a the path access permissions [RWADRLCDLB]
-f force exit success if group already exists
-h display this help menu
```

If `js-addgroup` command is run without options then user will be prompted for necessary information.

See also

Virtual path permissions

js-addgroupdir

The `js-addgroupdir` command may be used to add a directory path to an existing group in JSCAPE MFT Server.

```
Usage: js-addgroupdir [-options]

Options:

-d the domain name
-g the groupname
-p the path
-r the real directory path
-a the path access permissions [RWADRLCDLB]
-h display this help menu
```

If `js-addgroupdir` command is run without options then user will be prompted for necessary information.

See also

Virtual path permissions

js-add-server-key

The `js-add-server-key` command may be used to add a server key to Key Manager in JSCAPE MFT Server.

```
Usage: js-add-server-key [-options]

Options:

[-file <file>] configuration file
-alias <alias> key alias
[-rsa | -dsa] key algorithm; default: -rsa
[-size <bits>] key size in bits; default: 1024
-h display this help menu
```

If `js-add-server-key` command is run without options then user will be prompted for necessary information.

Command line utilities 14

js-addserviceaftp

The `js-addserviceaftp` command may be used to add an AFTP service to JSCAPE MFT Server.

```
Usage: js-addserviceaftp [-options]

Options:

-d <name> the domain name
-host <value> host address
-p <value> port
-k <alias> server key
-s <true|false> secure connection required
-h display this help menu
```

If `js-addserviceaftp` command is run without options then user will be prompted for necessary information.

js-addserviceftp

The `js-addserviceftp` command may be used to add a FTP service to JSCAPE MFT Server.

```
Usage: js-addserviceftp [-options]

Options:

-d <name> the domain name
-host <value> host address
-p <value> port
-t <value> ftp type (regular, explicit SSL, forced explicit SSL, implicit
SSL)
-k <alias> server key
-h display this help menu
```

If `js-addserviceftp` command is run without options then user will be prompted for necessary information.

js-addservicehttp

The `js-addservicehttp` command may be used to add a HTTP and HTTP/S services to JSCAPE MFT Server.

```
Usage: js-addservicehttp [-options]

Options:

-d the domain name
-http enable http (true|false)
-https enable https (true|false)
-h display this help menu
```

If `js-addservicehttp` command is run without options then user will be prompted for necessary information.

Command line utilities 14

js-addservicesftp

The `js-addservicesftp` command may be used to add SFTP service to JSCAPE MFT Server.

```
Usage: js-addservicesftp [-options]

Options:

-d <name> the domain name
-host <value> host address
-p <value> port
-a <value> authentication type (password, publickey, password OR publickey, pass
word AND publickey)
-k <alias> server key
-h display this help menu
```

If `js-addservicesftp` command is run without options then user will be prompted for necessary information.

js-addservicewebdav

The `js-addservicewebdav` command may be used to add WebDAV service to JSCAPE MFT Server.

```
Usage: js-addservicewebdav [-options]

Options:

-d the domain name
-http enable http (true|false)
-https enable https (true|false)
-h display this help menu
```

If `js-addservicewebdav` command is run without options then user will be prompted for necessary information.

js-adduser

The `js-adduser` command may be used to add a user to JSCAPE MFT Server.

```
Usage: js-adduser [-options]

Options:

-d <name> the domain name
-t <name> the template name
-n <name> the user full name
-u <name> the username (login)
-p <password> the account password
-r <path> the user home directory
-a <permissions> the user home directory access permissions [RWADRLCDLB]
-e <email> the email address
-g <name> the group
-c <name> company name
-f force exit success if user already exists
-h display this help
```

If `js-adduser` command is run without options then user will be prompted for necessary information.

See also

Virtual path permissions

js-adduserdir

The `js-adduserdir` command may be used to add a directory path to an existing user in JSCAPE MFT Server.

```
Usage: js-adduserdir [-options]

Options:

-d the domain name
-u the username
-p the path
-r the real directory path
-a the path access permissions [RWADRLCDLB]
-h display this help menu
```

If `js-adduserdir` command is run without options then user will be prompted for necessary information.

See also

Virtual path permissions

js-as2purge

The `js-as2purge` command may be used to manually purge AS2 messages from JSCAPE MFT Server.

```
Usage: js-as2purge [-options]

Options:

[-file <file>] configuration file
-d <name> domain name
-p <days> max message age
[-db | -api] database or API access flag; default: -api
-h display this help menu
```

If `js-as2util` command is run without options then user will be prompted for necessary information.

js-as2util

The `js-as2util` command may be used to get information about AS2 messages in JSCAPE MFT Server.

```
Usage: js2-as2util [-options]

Options:

-id <message id> target message id
[-f <file>] write message to specified filename
[-k <key alias>] decryption key alias
-d decrypt the specified message
-s display certificate alias and serial used in signing message
```

```
-h display this help menu
```

If `js-as2util` command is run without options then user will be prompted for necessary information.

js-backuplog

The `js-backuplog` command may be used to import backup log files to a database that were generated as a result of being unable to communicate with the logging database.

```
Usage: js-backuplog [-options]

Options:

-domain <domain> target domain
-h display this help menu
```

If `js-backupload` command is run without options then user will be prompted for necessary information.

js-client-configuration

The js-`client-configuration` command may be used to configure the client connection settings used by various command line utilities in JSCAPE MFT Server.

```
Usage: js-client-configuration -host <value> -port <value> -user <value> -
password <value>

Options:

-host <host/IP> management host
-port <port> management port
-timeout <seconds> connection timeout
-user <username> access username
-password <password> access password
-h display this help menu
```

js-copyusers

The `js-copyusers` command may be used to copy users for one domain to another domain in JSCAPE MFT Server. This utility is typically used for user migration purposes.

```
Usage: js-copyusers [-d <destination domain>] [-s <source domain>] [-h]

Options:

-s the source domain name
-d the destination domain name
-h display this help menu
```

If `js-copyusers` command is run without options then user will be prompted for necessary information.

js-database-configuration

The js-`database-configuration` command may be used to configure the database used for storing configuration settings in JSCAPE MFT Server.

```
Usage: js-database-configuration [-file <file>] configuration file
-configure | -test | -init | -clear | -delete | -copy
```

```
Options:

[-url <URL>] database JDBC URL
[-user <username>] database username
[-password <password>] database password
[-pool <size>] connection pool size
[-ttl <seconds>] connection TTL seconds
[-destination-url <URL>] destination database JDBC URL
[-destination-user <username>] destination database username
[-destination-password <password>] destination database password
```

js-db-migration

The `js-db-migration` command may be used to migrate data from a previous installation where configuration data was stored in individual files to a later version where configuration data is stored in a relational database.

```
Usage: js-db-migration <options>

Options:

[-file <file>] configuration file
[-dir <directory>] data directory
[-exclude-log-searches] exclude log searches flag
[-d] delete original files flag
-h display this help menu
```

js-deldomain

The `js-deldomain` command may be used to delete a domain in JSCAPE MFT Server.

```
Usage: js-deldomain [-options]

Options:

-d the domain name
-h display this help menu
```

If `js-deldomain` command is run without options then user will be prompted for necessary information.

js-delgroup

The `js-delgroup` command may be used to delete an existing group from JSCAPE MFT Server.

```
Usage: js-delgroup [-options]

Options:

-d the domain name
-g the groupname
-h display this help menu
```

If `js-delgroup` command is run without options then user will be prompted for necessary information.

Command line utilities 14

js-deluser

The `js-deluser` command may be used to delete an existing user from JSCAPE MFT Server.

```
Usage: js-deluser [-options]

Options:

-d the domain name
-u the username
-f force exit success if user does not exist
-h display this help menu
```

If `js-deluser` command is run without options then user will be prompted for necessary information.

js-enablehttp

The `js-enablehttp` command may be used to enable HTTP service in JSCAPE MFT Server.

```
Usage: js-enablehttp [-options]

Options:

-host http host
-p http port
-h display this help menu
```

If `js-enablehttp` command is run without options then user will be prompted for necessary information.

js-enablehttps

The `js-enablehttps` command may be used to enable HTTPS service in JSCAPE MFT Server.

```
Usage: js-enablehttps [-options]

Options:

-host <value> host address
-p <value> port
-k <alias> server key
-h display this help menu
```

If `js-enablehttps` command is run without options then user will be prompted for necessary information.

js-importcontacts

The `js-importcontacts` command may be used to perform bulk import of contacts stored in CSV file format.

```
Usage: js-importcontacts [-options]

Options:

-d the domain name
-f file to import
-h display this help menu
-s skip bad lines
```

If js-importcontacts command is run without options then user will be prompted for necessary information.

File Format

Import file should be plain text with comma separated values and each contact on a new line. Non-required fields may be omitted.

Column #	Column Description	Required	Example
1	The full name of contact.	Yes	John Smith
2	The contact email address.	Yes	jsmith@domain.com
3	The contact company.	No	ABC Corp
4	The login of contact owner.	No	admin

Example

```
John Smith,jsmith@domain,ABC Corp,admin
Henry Jones,hjones@domain,XYZ Corp
```

js-import-log-searches

The js-import-log-searches command may be used to import log searches from a previous instance of JSCAPE MFT Server.

```
Usage: js-import-log-searches [-options]

Options:

[-file <file>] configuration file
[-d] delete database searches flag
-h display this help menu
```

If js-import-log-searches command is run without options then user will be prompted for necessary information.

js-importusers

The js-importusers command may be used to perform bulk import of users stored in CSV file format.

```
Usage: js-importusers [-options]

Options:

-d <name> the domain name
-f <path> file to import
-t <name> an account template
-s skip bad lines
-h display this help menu
```

If js-importusers command is run without options then user will be prompted for necessary information.

File Format

Import file should be plain text with comma separated values and each user on a new line. Non-required fields may be omitted.

Column #	Column Description	Required	Example
1	The full name of user.	Yes	`John Smith`
2	The unique user login.	Yes	`jsmith`
3	The user password.	Yes	`secret`
4	The user root login path.	Yes / No *(not required if template is used)*	`C:\users\jsmith`
5	The user email address.	No	`jsmith@domain.com`
6	The user group name.	No	`Administrators`

Example

```
John Smith,jsmith,secret,C:\users\jsmith,jsmith@domain.tx,Administrators
Henry Jones,hjones,secret,C:\users\hjones,hjones@domain.com
```

js-ipaccess

The `js-ipaccess` command may be used to perform manage the IP access list for a domain.

```
Usage: js-ipaccess [-b|-u] [-d <domain>] [-l] [-i <IP address>] [-h]

Options:

-d the domain name
-i insert rule for specified IP address
-b block specified IP address
-u unblock specified IP address
-l lists current IP access settings
-h display this help menu
```

If `js-ipaccess` command is run without options then user will be prompted for necessary information.

js-kickuser

The `js-kickuser` command may be used to forcibly close all sessions for a specified user in JSCAPE MFT Server.

```
Usage: js-kickuser [-options]

Options:

-d the domain name
-u the user name
-h display this help menu
```

If `js-kickuser` command is run without options then user will be prompted for necessary information.

js-oftppurge

The `js-oftppurge` command may be used to manually purge OFTP2 messages from JSCAPE MFT Server.

```
Usage: js-oftppurge [-options]

[-file <file>] configuration file
-d <name> domain name
-p <days> max message age
[-db | -api] database or API access flag; default: -api
-h display this help menu
```

If `js-oftppurge` command is run without options then user will be prompted for necessary information.

js-passwd

The `js-passwd` command may be used to update a password for an account.

```
Usage: js-passwd [-d <domain>] [-p <password>] [-u <user>] [-h]

Options:

-d the domain name
-u the account login
-p the account password
-h display this help menu
```

If `js-passwd` command is run without options then user will be prompted for necessary information.

js-pausedomain

The `js-pausedomain` command may be used to pause a domain in JSCAPE MFT Server. When pausing a domain existing connections will be allowed to continue however new connections will not be accepted.

```
Usage: js-pausedomain [-options]

Options:

-d the domain name
-h display this help menu
```

If `js-pausedomain` command is run without options then user will be prompted for necessary information.

Command line utilities 14

js-resumedomain

The `js-resumedomain` command may be used to resume a paused domain in JSCAPE MFT Server.

```
Usage: js-resumedomain [-options]

Options:

-d the domain name
-h display this help menu
```

If `js-resumedomain` command is run without options then user will be prompted for necessary information.

js-runtrigger

The `js-runtrigger` command may be used to run a trigger which listens for the Current Time event in JSCAPE MFT Server. When running a trigger using `js-runtrigger` any conditions for the trigger will be ignored.

```
Usage: js-runtrigger [-options]

Options:

-d the domain name
-n the trigger name
-h display this help menu
```

If `js-runtrigger` command is run without options then user will be prompted for necessary information.

js-sendmessage

The `js-sendmessage` command may be used to send an email message to all users for a domain.

```
Usage: js-sendmessage [-options]

Options:

-d domain
-host smtp host
-p smtp port
-t smtp connection type (plain|ssl|start-tls)
-debug enable debug mode (true|false)
-u smtp username
-pass smtp password
-f from address
-s subject
-b body
-h display this help menu
```

If `js-sendmessage` command is run without options then user will be prompted for necessary information.

js-server-configuration

The js-`server-configuration` command may be used to configure the administrative host/IP(s) and ports used for the administrative service in JSCAPE MFT Server. This command is typically run once during initial installation in non-GUI environments (e.g. Linux, UNIX).

```
Usage: js-server-configuration <options>

Options:

-host <host/IP> management host
-port <port> management port
-timeout <seconds> application session timeout
-h display this help menu
```

js-setdomainquota

The `js-setdomainquota` command may be used to set bandwidth quotas at the domain level in JSCAPE MFT Server.

```
Usage: js-setdomainquota [-options]

Options:

-d the domain name
-uq max uploads quota
-ur uploads quota reset period (days)
-dq max downloads quota
-dr downloads quota reset period (days)
-tq max transfers quota
-tr transfers quota reset period (days)
-h display this help menu
```

If `js-setdomainquota` command is run without options then user will be prompted for necessary information.

js-setuserquota

The `js-setuserquota` method may be used to set bandwidth quotas at user level in JSCAPE MFT Server.

```
Usage: js-setuserquota [-options]

Options:

-d the domain name
-u the username
-uq max uploads quota (MB)
-ur uploads quota reset frequency (days)
-dq max downloads quota (MB)
-dr downloads quota reset frequency (days)
-tq max transfers quota (MB)
-tr transfers quota reset frequency (days)
-h display this help menu
```

If `js-setuserquota` command is run without options then user will be prompted for necessary information.

Command line utilities 14

js-shutdown

The `js-shutdown` command may be used to perform an orderly shutdown of all services for all domains in JSCAPE MFT Server. In an orderly shutdown all existing processes are allowed to complete while no new connections are accepted.

```
Usage: js-shutdown [-options]

Options:

-h display this help menu
```

If `js-shutdown` command is run without options then user will be prompted for necessary information.

js-shutdowndomain

The `js-shutdowndomain` command may be used to perform an orderly shutdown of all services for the specified domain in JSCAPE MFT Server. In an orderly shutdown all existing processes are allowed to complete while no new connections are accepted.

```
Usage: js-shutdowndomain [-options]

Options:

-d the domain name
-h display this help menu
```

If `js-shutdowndomain` command is run without options then user will be prompted for necessary information.

js-startdomain

The `js-startdomain` command may be used to start a domain in JSCAPE MFT Server.

```
Usage: js-startdomain [-options]

Options:

-d the domain name
-h display this help menu
```

If `js-startdomain` command is run without options then user will be prompted for necessary information.

js-stopdomain

The `js-stopdomain` command may be used to stop a domain in JSCAPE MFT Server.

```
Usage: js-stopdomain [-options]

Options:

-d the domain name
-h display this help menu
```

If `js-stopdomain` command is run without options then user will be prompted for necessary information.

Command line utilities 14

js-syncstate

The `js-syncstate` command may be used to synchronize server configuration information from this server to a target server in JSCAPE MFT Server.

```
Usage: js-syncstate [-options]

Options:

-ip <host/IP> failover server host/IP
-p <port> failover server port
-u <username> administrator username
-pwd <password> administrator password
-s <IP substitution rules> comma delimited list of semi-colon delimited ip
substitution rules (e.g. 1.2.3.4,1.2.3.5;4.5.6.7,7.8.9.0)
-h display this help menu
```

If `js-syncstate` command is run without options then user will be prompted for necessary information.

js-triggersreport

The `js-triggersreport` command may be used to list all triggers and settings for a domain.

```
Usage: js-triggersreport [-options]

Options:

-d <name> the domain name
-h display this help menu
```

If `js-triggersreport` command is run without options then user will be prompted for necessary information.

js-update-email-resources

The `js-update-email-resources` command may be used to update email resources to latest version of JSCAPE MFT Server.

```
Usage: js-update-email-resources [-options]

Options:

[-file <file>] configuration file
[-d] delete database searches flag
-h display this help menu
```

If `js-update-email-resources` command is run without options then user will be prompted for necessary information.

js-users

The `js-users` command may be used to list, enable or disable users in JSCAPE MFT Server.

```
Usage: js-users [-d <domain>] [-l] [-fe|-fd] [-u <user>] [-h]

Options:

-d domain name
```

```
-l list users
-u user name
-fe enable flag
-fd disable flag
-h display this help menu
```

If `js-users` command is run without options then user will be prompted for necessary information.

js-web-configuration

The js-`web-configuration` command may be used to configure the host/IP(s) and ports used for the web-based administrative service in JSCAPE MFT Server. This command is typically run once during initial installation in non-GUI environments (e.g. Linux, UNIX).

```
Usage: js-web-configuration <options>

Options:

-host <host/IP> application host
-port <port> application port
-timeout <minutes> application session timeout
-h display this help menu
```

Enabling WebDAV service

JSCAPE MFT Server Enterprise Edition offers support for the WebDAV file transfer protocol. To enable WebDAV please perform the following using JSCAPE MFT Server Manager:

1. Go to `Settings > Web` and enable the HTTP/S protocols.

2. In the `Services` node for the desired domain, click on the `Add` button. The `Add Service` dialog is displayed.

3. Under `Protocol` select the `WebDAV/S` option. Select the protocols you wish to enable WebDAV on.

4. Click `OK`.

See also

[Web based file transfers](#)

Establishing a connection

Connect using 3rd party WebDAV client

To connect using a 3rd party WebDAV client you will be prompted for the following information:

URL - The URL (Uniform Resource Locator) that you want to connect to. This generally takes the form of `http://hostname:port/webdav/` or `https://hostname:port/webdav/` for SSL encrypted connections.

Username - The username to connect with. This should be in the format of `username@domain` where `username` is the user you are logging in as and `domain` is the JSCAPE MFT Server domain you wish to login to.

Password - The password to connect with.

See also

WebDAV support 15

Web based file transfers

Overview

In the context of JSCAPE MFT Server, a Reverse Proxy consists of all the necessary properties for connecting to a remote service. The power of reverse proxy lies in it's ability to be mapped to a virtual path for a user or group. This is useful in cases where you want to transparently provide users access to one or more remote services via a single account.

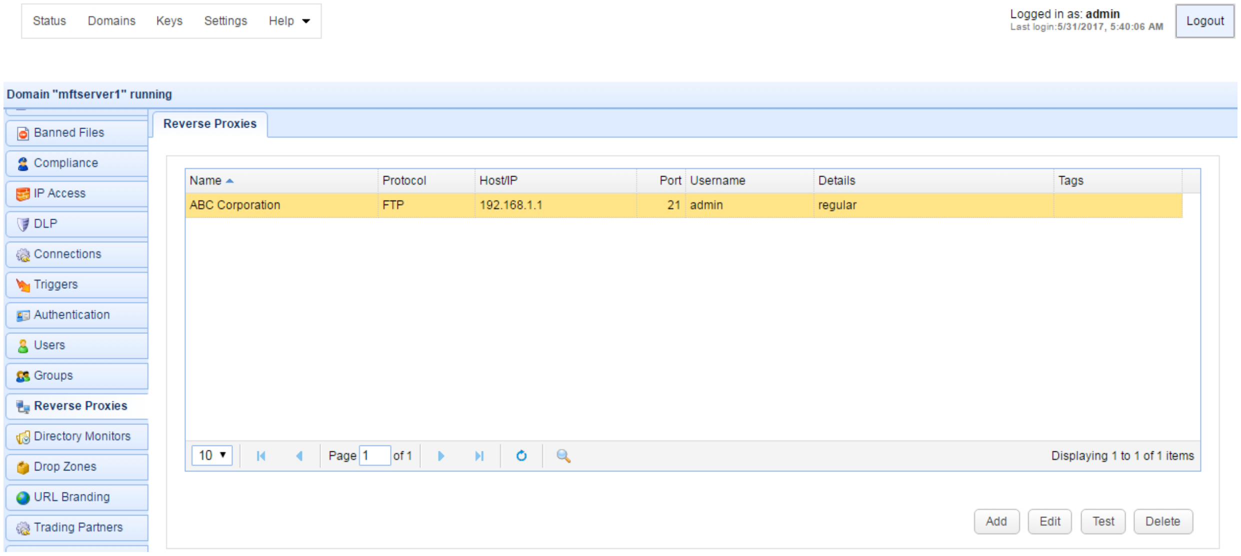
See also

Creating a reverse proxy
Mapping a reverse proxy to a virtual path

Creating a reverse proxy

You may create a reverse proxy using the JSCAPE MFT Server Manager.   To view a list of reverse proxies click on the `Reverse Proxies` node for the desired domain.

Figure 48



Logged in as: admin
Last login:5/31/2017, 5:40:06 AM

Domain "mftserver1" running

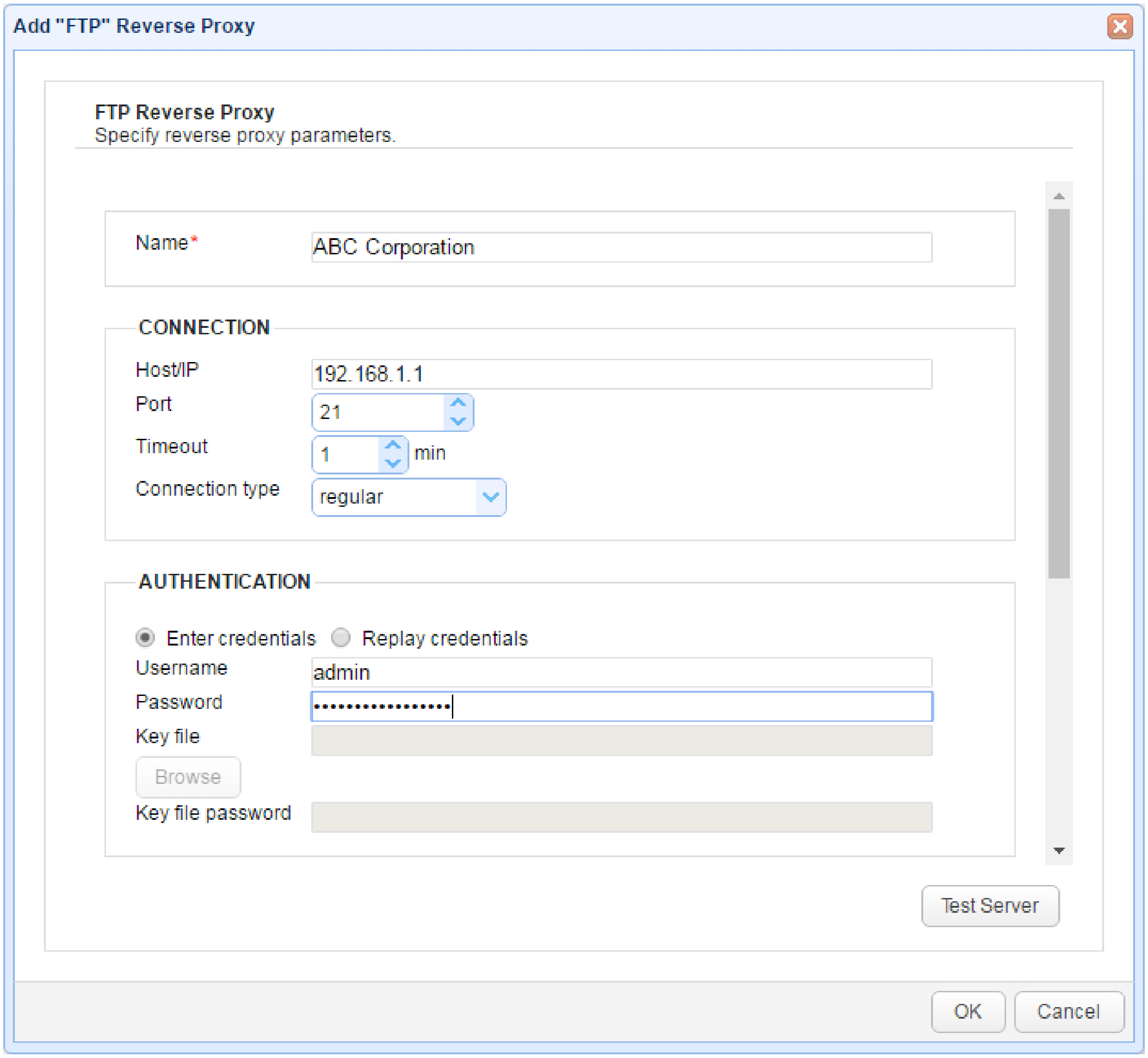
Name	Protocol	Host/IP	Port	Username	Details	Tags
ABC Corporation	FTP	192.168.1.1	21	admin	regular	

Displaying 1 to 1 of 1 items

Add reverse proxy

To add a reverse proxy click on the `Add` button in the lower right corner. Choose a protocol from the drop-down list. The `Add Reverse Proxy` dialog will be displayed.

Figure 49



Add "FTP" Reverse Proxy

FTP Reverse Proxy
Specify reverse proxy parameters.

Name* ABC Corporation

CONNECTION

Host/IP 192.168.1.1
Port 21
Timeout 1 min
Connection type regular

AUTHENTICATION

● Enter credentials ○ Replay credentials
Username admin
Password ••••••••••••••••••
Key file
Key file password

Name - Unique name for this reverse proxy.

Host/IP - The remote IP or host address for this reverse proxy.

Port - The remote port for this reverse proxy.

Timeout - The maximum timeout for establishing a connection to remote server.

Connection type - The connection type for this reverse proxy.

Enter credentials - Enables the administrator to specify a static username and password for all users

Replay credentials - Uses the current user's credentials instead of a static username and password.

Username - The username for connecting to this remote server.

Password - The password for connecting to this remote server.

Key file - The optional client private key to use for this connection. (FTPS/SFTP)

Key file password - The optional client private key password to use for this connection. (FTPS/SFTP)

Remote directory - maps local virtual path to a specific remote virtual path

Map current local directory to remote directory - If enabled, maps local virtual path to remote virtual path having the same name as the local virtual path. For example, if reverse proxy is mapped to virtual path /path then when connecting to reverse proxy it will drop user in /path directory on target server.

Debug log directory - Directory in which to store debug logs for this reverse proxy.

Max proxy age - The maximum amount of time to keep this reverse proxy connection in connection pool.

Use passive transfer mode - Flag indicating whether passive mode is used for connecting to this remote server.

Mapping a reverse proxy to a virtual path

Mapping a reverse proxy to a virtual path is a powerful feature that allows users to transparently access one or more remote services via a single client session. In order to map a reverse proxy to a virtual path first create a reverse proxy, then map that reverse proxy to a virtual path for a user or group of users. When users access the virtual path of a reverse proxy they will be connected to the remote server. This is completely transparent to the end user.

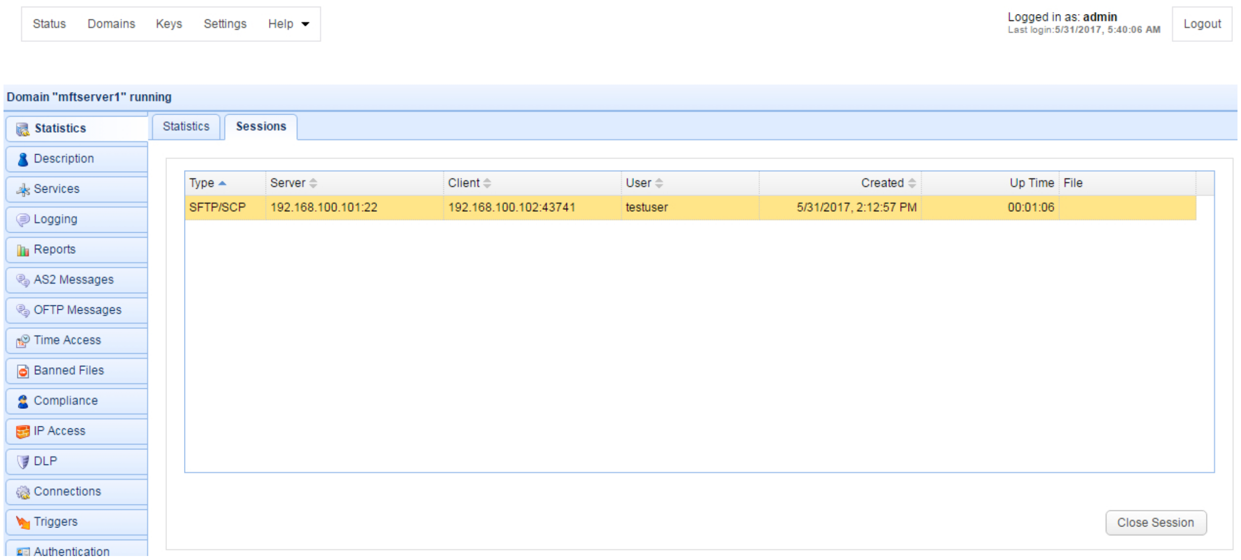
See also

[Creating a reverse proxy](#)
[Defining virtual paths](#)

Overview

A session is defined as a connection with the server. Current sessions may be seen from the `Statistics` module in JSCAPE MFT Server Manager.

Figure 146



Logged in as: **admin**
Last login:5/31/2017, 5:40:06 AM

Domain "mftserver1" running

Type	Server	Client	User	Created	Up Time	File
SFTP/SCP	192.168.100.101:22	192.168.100.102:43741	testuser	5/31/2017, 2:12:57 PM	00:01:06	

Close Session - Forcibly terminates selected session.

Key management

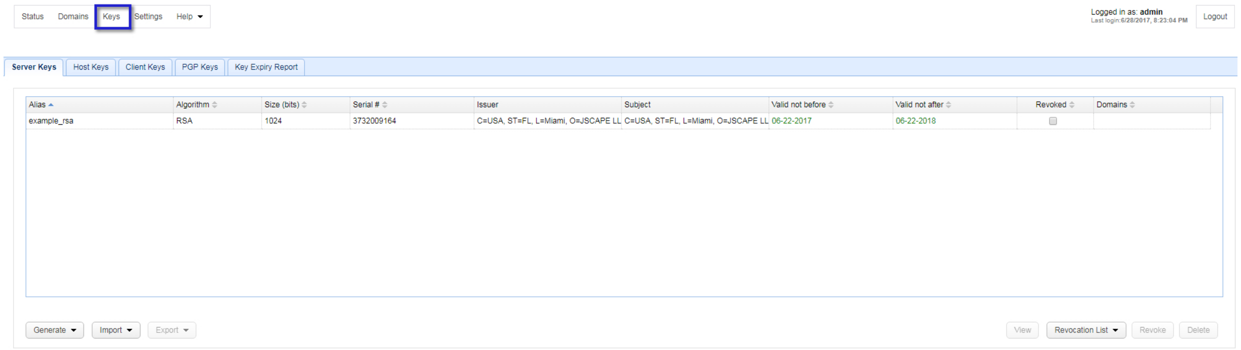
18

Overview

JSCAPE MFT Server includes support for encrypted file transfer protocols as well as OpenPGP encryption. In order to take advantage of encryption services you must create one or more keys that may be used for encrypting your sessions and/or files. Key management is accomplished via the `Key Manager`. To access the Key Manager select `Keys` from the main menu. The `Key Manager` dialog will be displayed.

[Server keys](#)
[Client keys](#)
[OpenPGP keys](#)

Figure 22



Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked	Domains
example_rsa	RSA	1024	3732009164	C=USA, ST=FL, L=Miami, O=JSCAPE LL	C=USA, ST=FL, L=Miami, O=JSCAPE LL	06-22-2017	06-22-2018	□	

Server keys

Overview

Server keys are required for encrypting communications between a client and the server when using secure file transfer protocols such as FTPS, SFTP and HTTPS. Additionally, server keys may be used for the signing and/or decryption of messages in AS2 and OFTP protocols. In the context of the `Key Manager`, a server key consists of a private key, certificate and public key.

Note

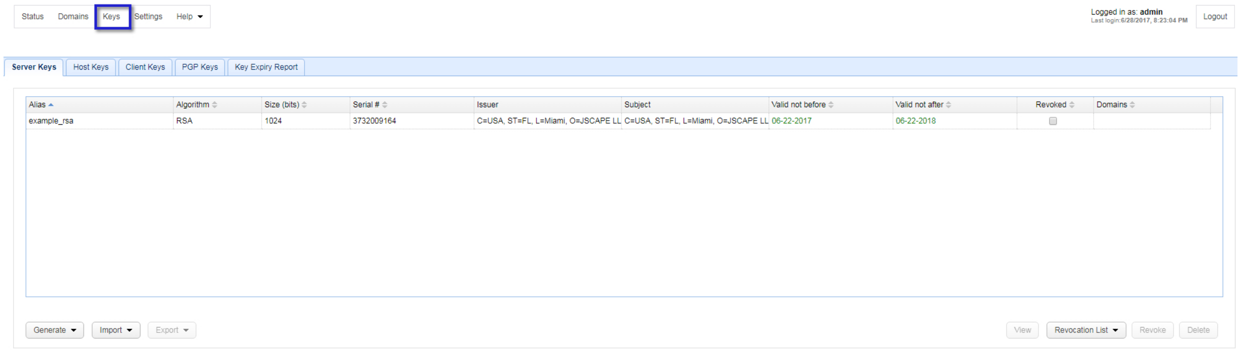
Some server keys are installed by default with JSCAPE MFT Server. These are meant only for testing purposes and should **not** be deployed to a production environment.

Generating a key

To generate a private key open the Key Manager by selecting `Keys` from the main menu. The `Key Manager` dialog will be displayed.

Figure 22

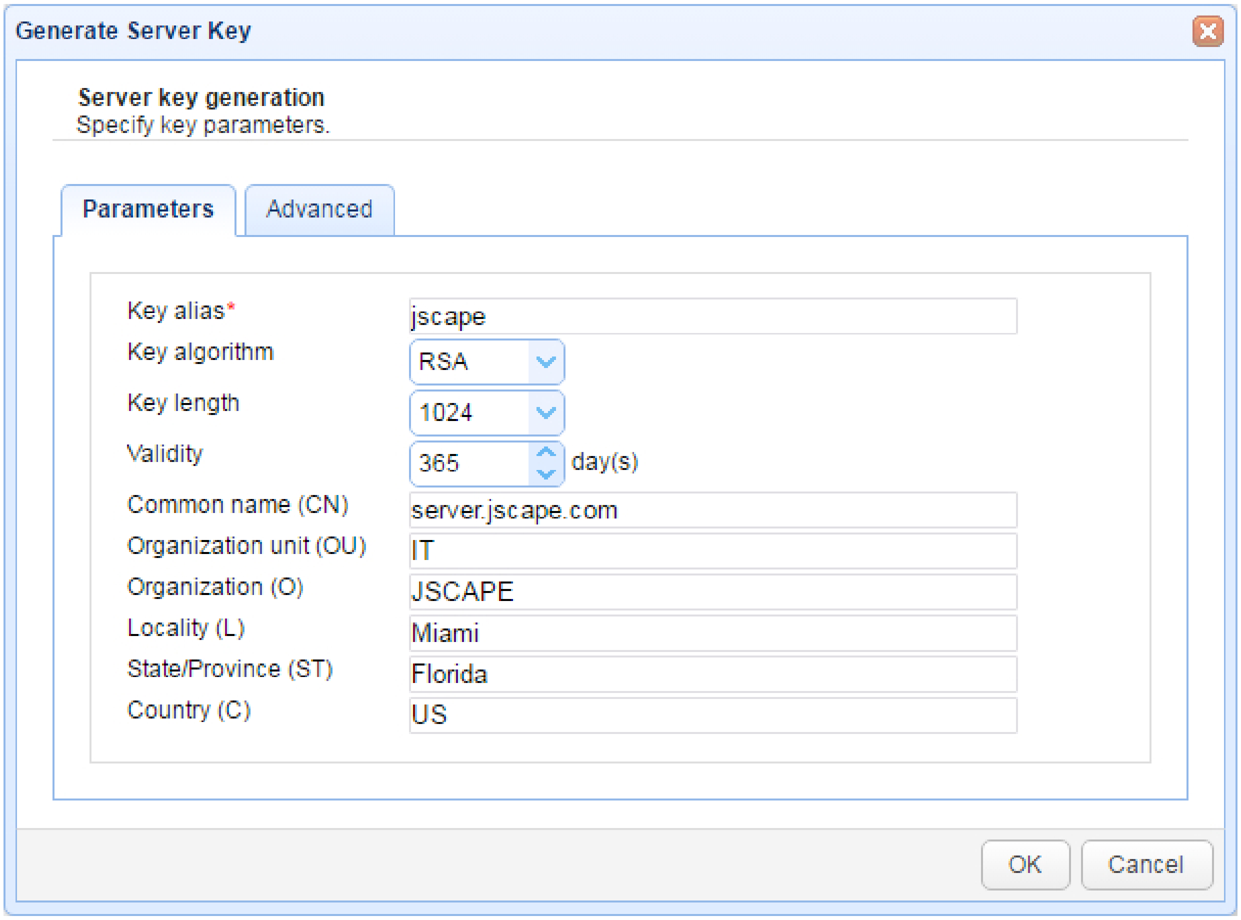
Key management 18



Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked	Domains
example_rsa	RSA	1024	3732009164	C=USA, ST=FL, L=Miami, O=JSCAPE LL	C=USA, ST=FL, L=Miami, O=JSCAPE LL	06-22-2017	06-22-2018	□	

Select the `Server Keys` tab and click on the `Generate` button. The `Generate Server Key` dialog is displayed.

Figure 23



Server key generation
Specify key parameters.

Key alias*	jscape
Key algorithm	RSA
Key length	1024
Validity	365 day(s)
Common name (CN)	server.jscape.com
Organization unit (OU)	IT
Organization (O)	JSCAPE
Locality (L)	Miami
State/Province (ST)	Florida
Country (C)	US

Key alias - Alias you wish to assign to the key.

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

Key length - The length of the key in bytes. Valid options are 1024 and 2048. Note, for key lengths greater than 1024 you must install the [Unlimited Jurisdiction Policy Files](#).

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.mydomain.com

Organizational 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".

Advanced

Key usage -Key usage parameter for certificate associated with server key.

Extended key usage - Extended key usage parameter for certificate associated with server key.

CRL URL - Certificate revocation list URL.

Sign with - Sign certificate with specified key.

Obtaining a trusted certificate

If you decide to use the web interface for performing file transfers you have the option of securing these transfers using HTTPS. The HTTPS protocol requires an SSL certificate to be used. You can either generate your own self-signed certificate using the `Key Manager` found in JSCAPE MFT Server 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 the client web browser 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 and 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 FTPS or HTTPS server. For example, if your HTTPS or FTPS server will be served under the domain `www.mydomain.com` then this is the value you should use in your `Common Name` field when generating your private key.

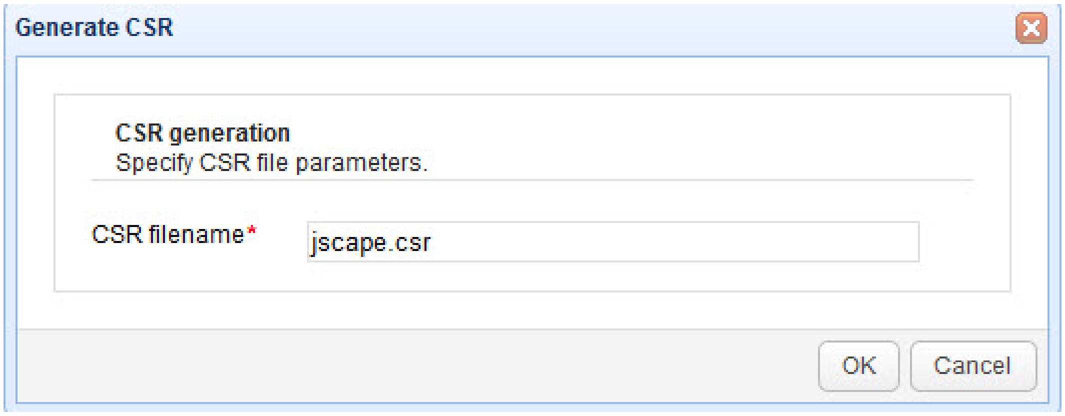
See also

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 `Key Manager` and click the `Generate CSR` button. A dialog will prompt you for the location in which to store the CSR.

Figure 87



Generate CSR

CSR generation

Specify CSR file parameters.

CSR filename*: jscape.csr

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 common format. To request a JSCAPE signed certificate please visit the following:

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

Importing signed certificate

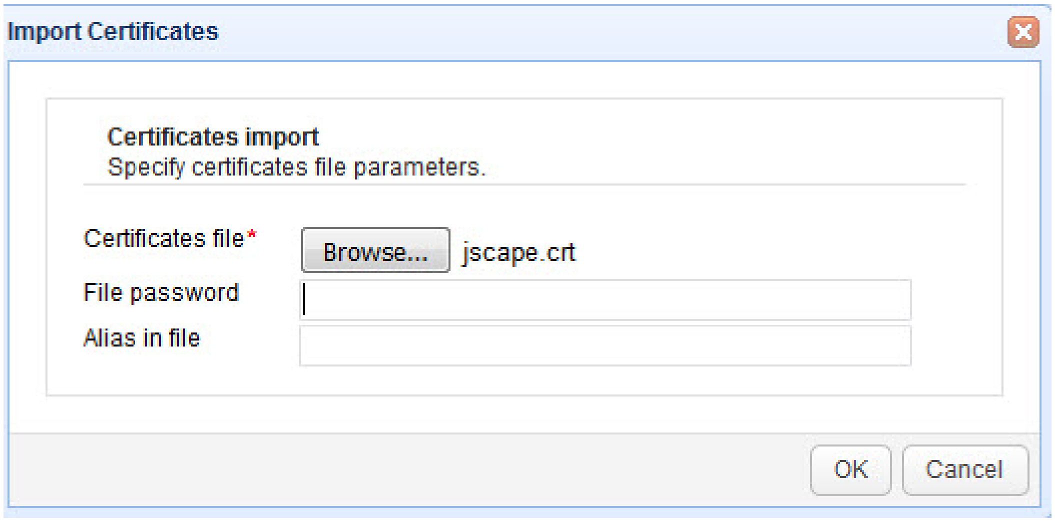
The last step is to import the signed certificate issued to you by your CA. To import the signed certificate select the server key that was used to generate the CSR and click the `Import Certificates` button. You will be prompted for the path of the certificate file issued to you by your CA.

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.

Figure 78



Certificates import
Specify certificates file parameters.

Certificates file* jscape.crt
File password
Alias in file

Certificates 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 HTTPS or FTPS 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 Server server private key signed by a certificate authority (CA) such as Thawte, Verisign or JSCAPE you may import the issued certificate using the `Import Certificates` 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

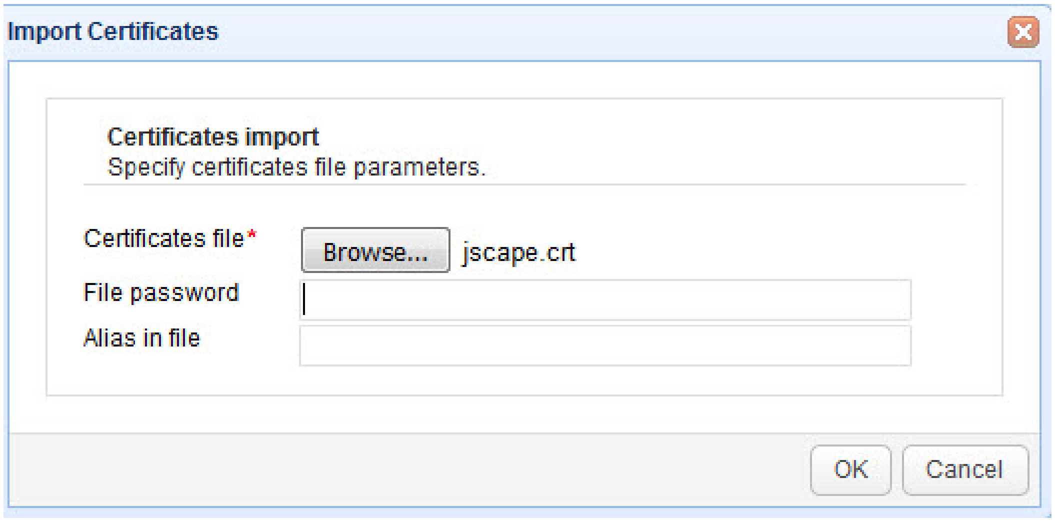
1. Open `Key Manager`.

2. Click on `Server Keys` panel.

3. Select existing key that you wish to import certificates for.

4. Click `Import > Import Certificates` button.

Figure 78



Import Certificates

Certificates import
Specify certificates file parameters.

Certificates file* Browse... jscape.crt

File password

Alias in file

Certificates file - The file containing signed certificate.

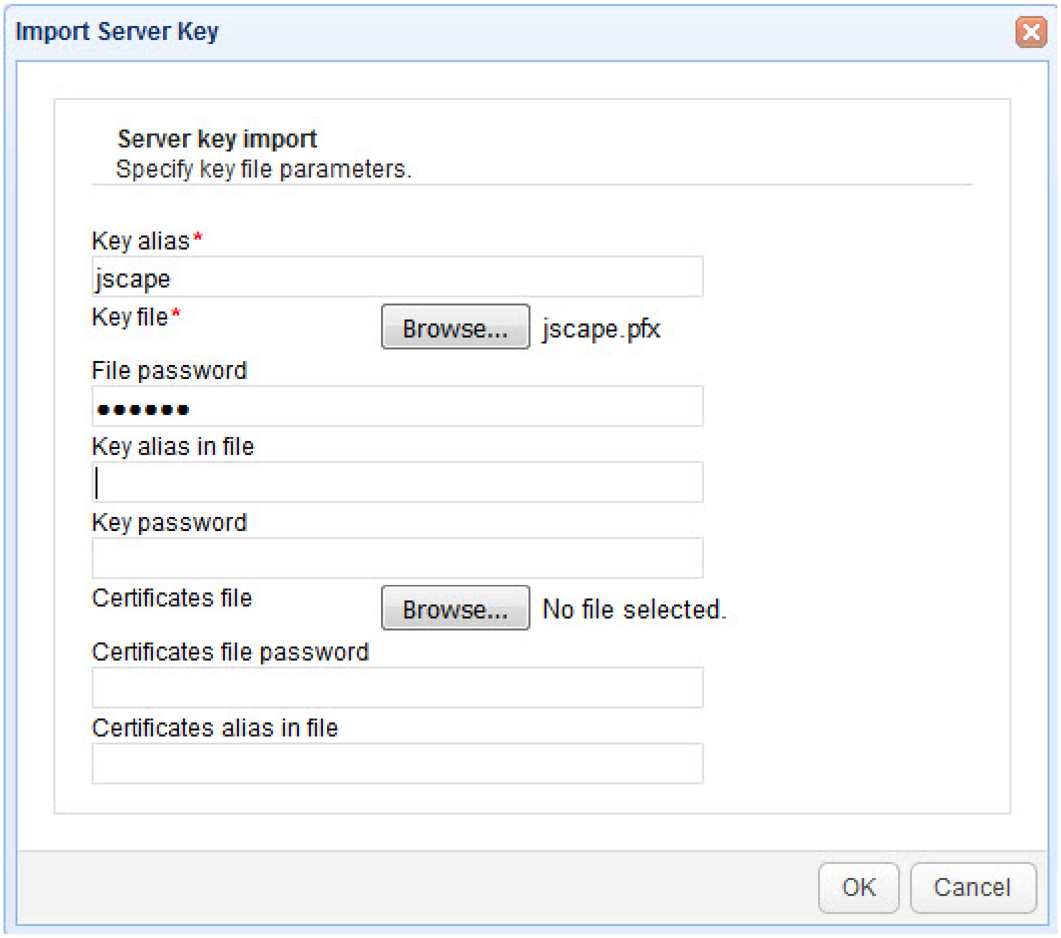
File password - The password protecting certificate. Leave blank if none.

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

Importing a key

You may import existing server keys and certificates for use in encrypting FTPS, SFTP and HTTPS connections. To import an existing key/certificate pair open the Key manager by selecting `Keys` from the main menu. The `Key Manager` will be displayed. Select the `Server Keys` tab and click on the `Import` button. The `Import Server Key` dialog is displayed.

Figure 50



Import Server Key

Server key import
Specify key file parameters.

Key alias*
jscape

Key file* Browse... jscape.pfx

File password
••••••

Key alias in file

Key password

Certificates file Browse... No file selected.

Certificates file password

Certificates alias in file

OK Cancel

Key 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.

Key file - The private key file to import from.

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

Key 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.

Note

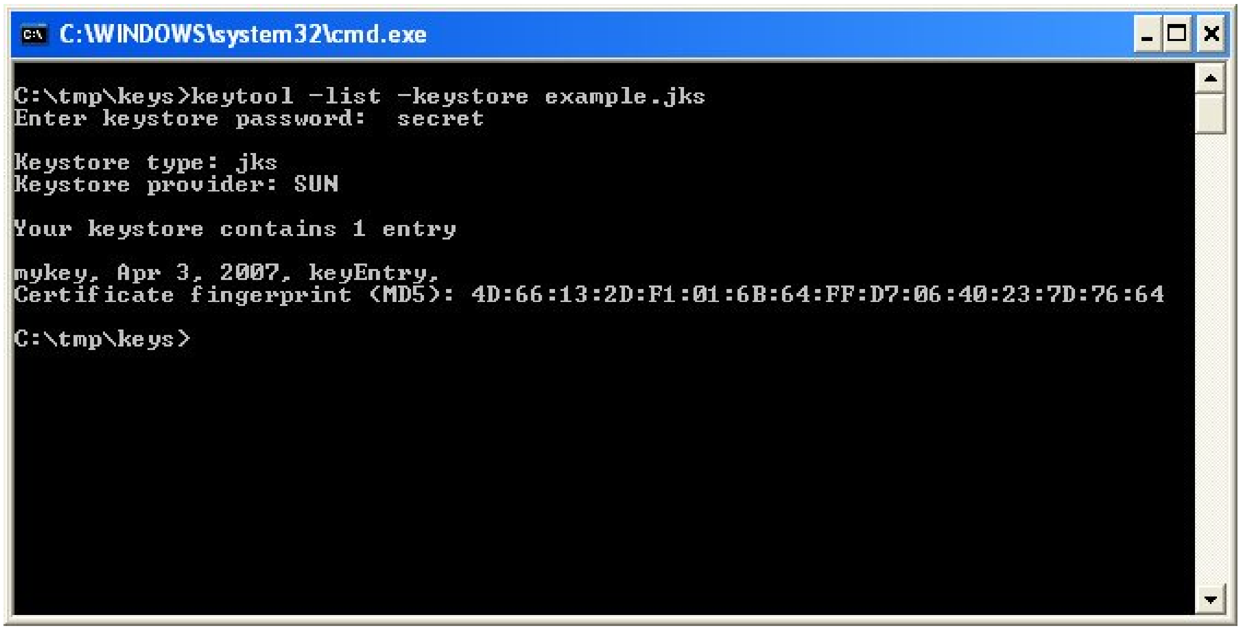
If you are unsure of the alias for the source keystore this may be obtained as follows:

JKS keystore

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

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

Figure 79



```
C:\tmp\keys>keytool -list -keystore example.jks
Enter keystore password:  secret

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

mykey, Apr 3, 2007, keyEntry,
Certificate fingerprint (MD5): 4D:66:13:2D:F1:01:6B:64:FF:D7:06:40:23:7D:76:64

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.

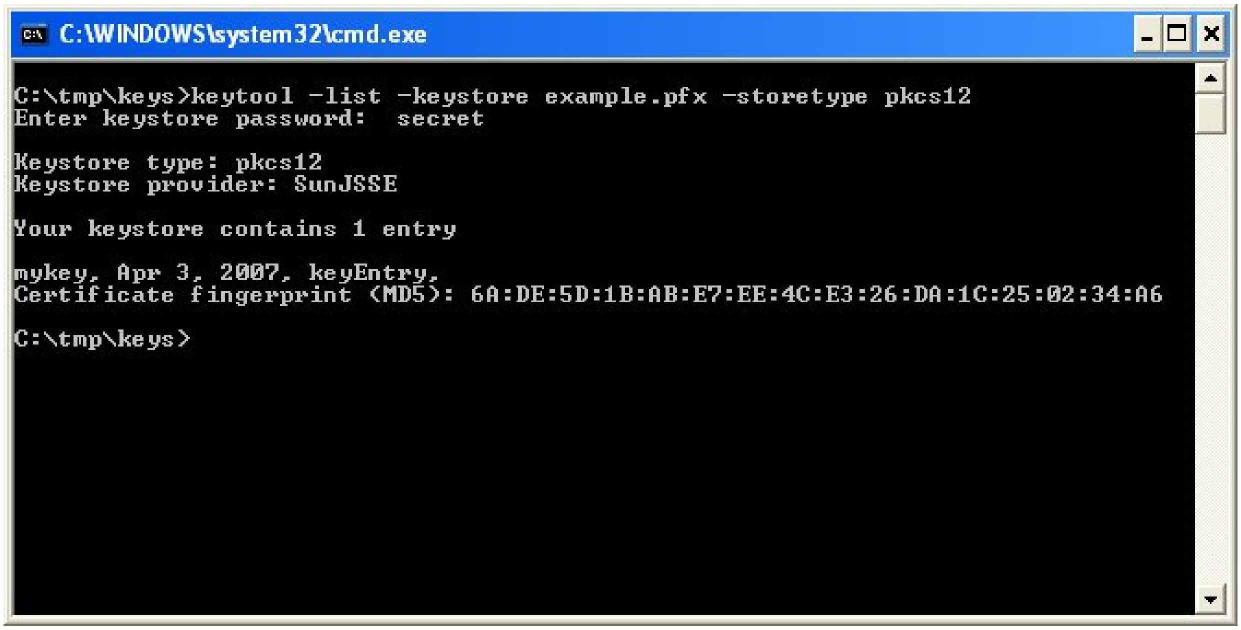
In the above example the key alias is `mykey`.

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 80



```
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`.

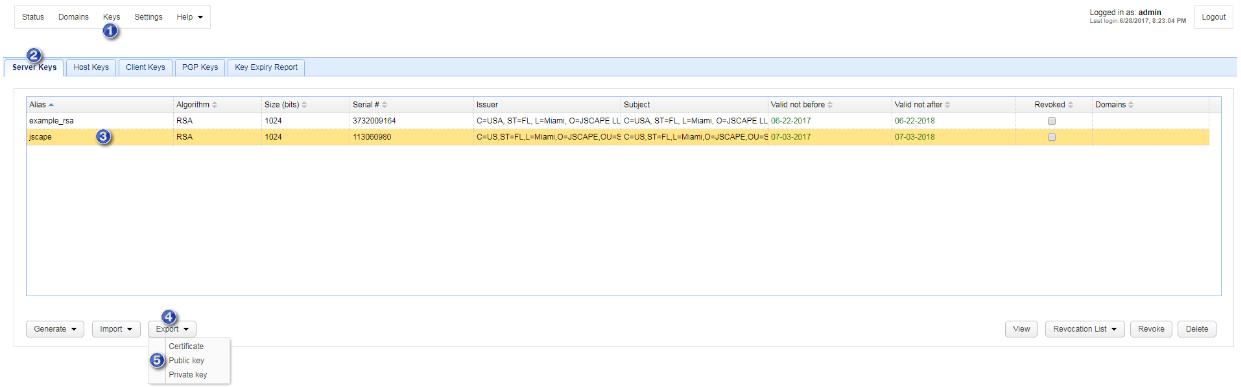
See also

[Generating a key]

Exporting a certificate, public or private key

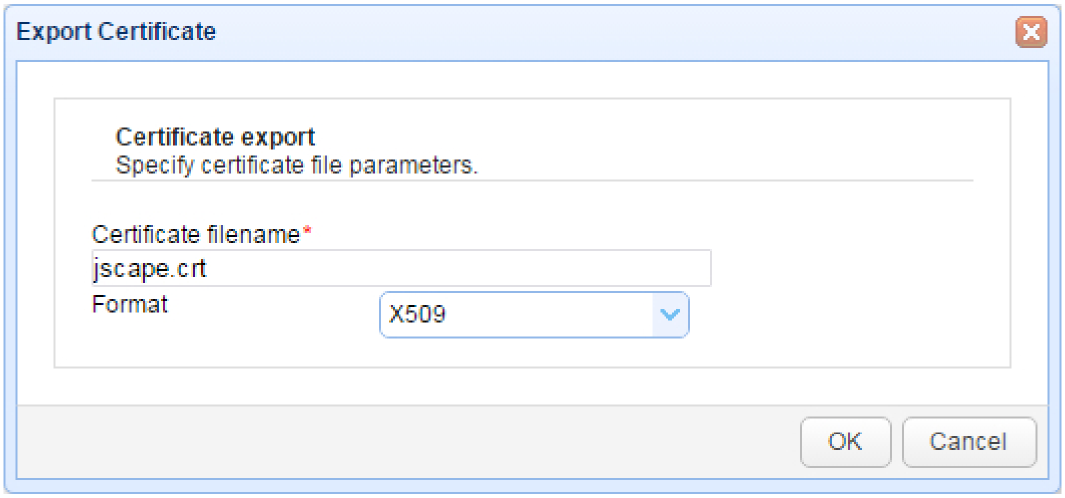
You may export existing server key certificates and/or public keys for use by clients in validating trusted FTPS, SFTP and HTTPS servers or for having a third party certificate authority e.g. Thawte, Verisign or JSCAPE sign your certificate. To export an existing server certificate and/or public key open the Key Manager by selecting `Keys` from the main menu. The `Key Manager` will be displayed. Click on `Server Keys` tab, select a server key and click on the `Export` button. Select which item you want to export, i.e., `Certificate`, `Public key`, or Private key.

Figure 158



Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked	Domains
example_rsa	RSA	1024	3732009164	C=USA, ST=FL, L=Miami, O=JSCAPE LL	C=USA, ST=FL, L=Miami, O=JSCAPE LL	06-22-2017	06-22-2018	□	
jscape	RSA	1024	113060980	C=US,ST=FL,L=Miami,O=JSCAPE,OU=S	C=US,ST=FL,L=Miami,O=JSCAPE,OU=S	07-03-2017	07-03-2018	□	

Figure 64



Certificate export
Specify certificate file parameters.

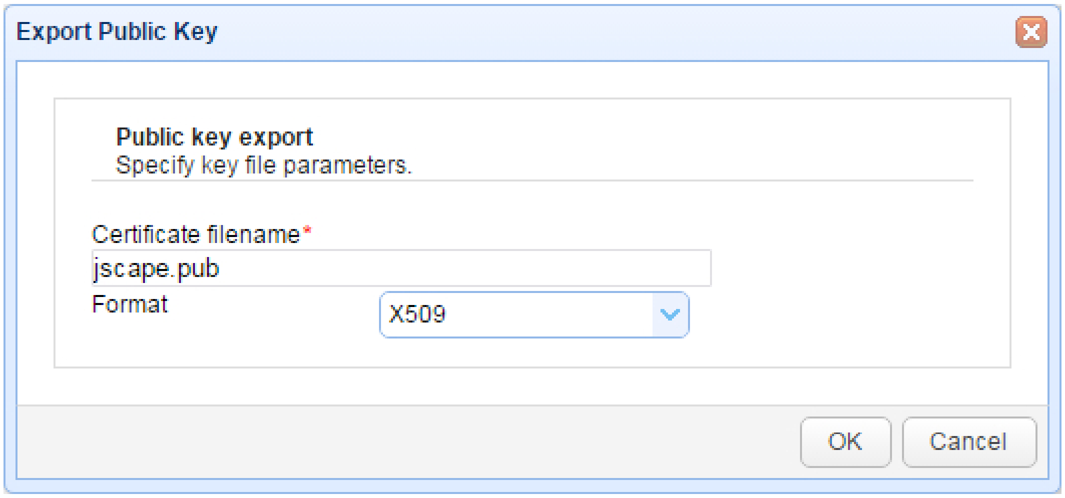
Certificate filename*: jscape.crt

Format: X509

Certificate filename - The filename to export the certificate to.

Format - The format in which to export certificate.

Figure 159



Export Public Key

Public key export
Specify key file parameters.

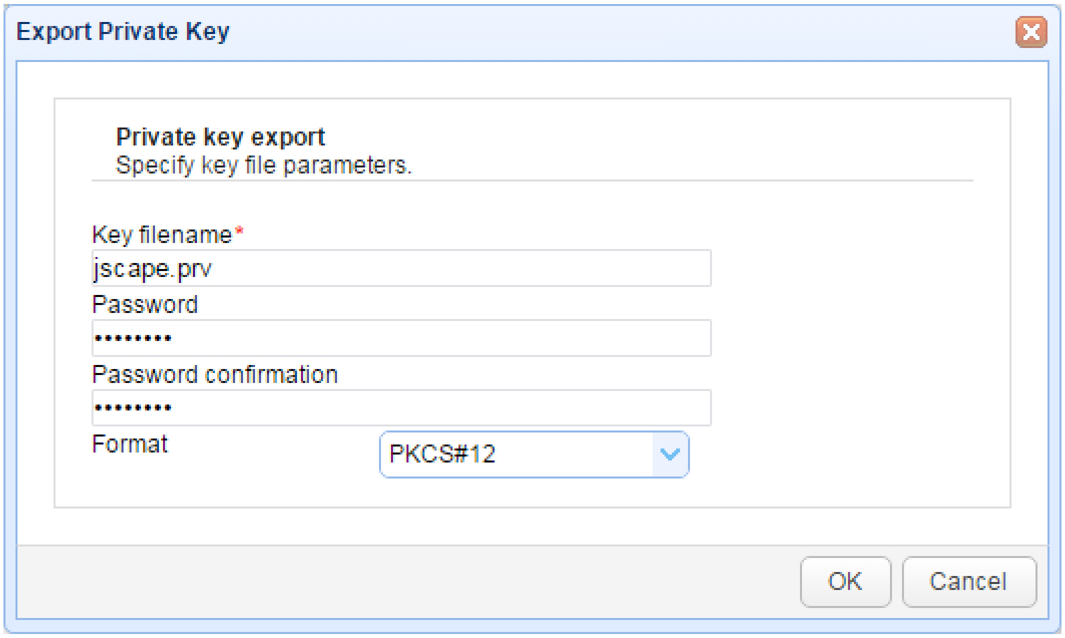
Certificate filename*: jscape.pub

Format: X509

Key filename - The filename to export public key file to.

Format - The format in which to export public key.

Figure 190



Export Private Key

Private key export
Specify key file parameters.

Key filename*: jscape.prv

Password: ••••••••

Password confirmation: ••••••••

Format: PKCS#12

Key filename - The filename to export private key file to.

Password - The password used to protect the private key.

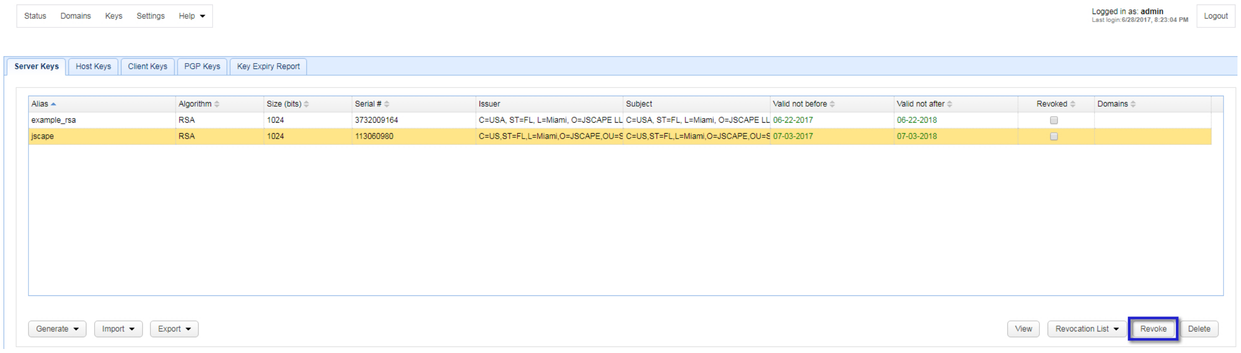
Format - The format in which to export private key.

Key management

Revoking a key

A server key may be revoked from within JSCAPE MFT Server by selecting the desired key from `Server Keys` tab in `Key Manager` and clicking the `Revoke` button. Revoking a server key does not prevent the key from being used, but merely flags the key as revoked in the administrative user interface and in it's underlying certificate properties. Server keys may also be revoked automatically if they are associated with a CRL (Certificate Revocation List) URL. This CRL URL may be defined when creating a server key under the `Advanced` tab. When a CRL URL is defined JSCAPE MFT Server will automatically check the CRL URL for the server key every evening at 11:00 PM local time and update the revocation status as needed.

Figure 227

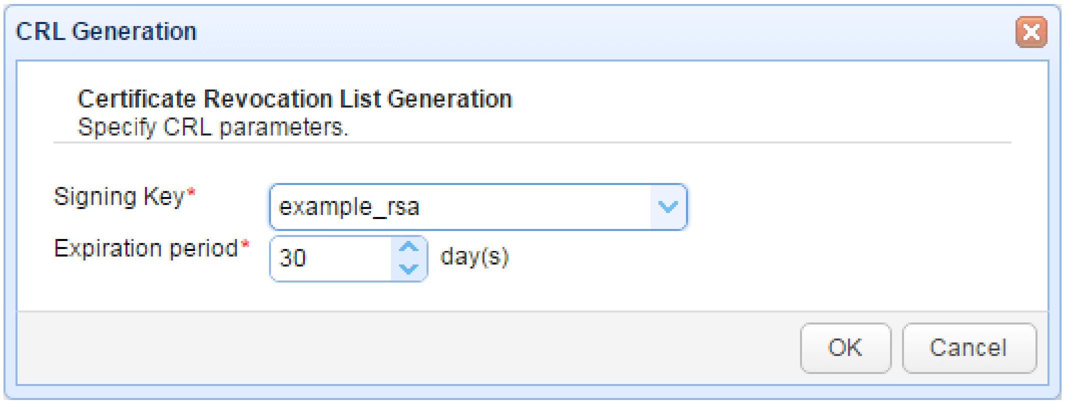


Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked	Domains
example_rsa	RSA	1024	3732009164	C=USA, ST=FL, L=Miami, O=JSCAPE LL	C=USA, ST=FL, L=Miami, O=JSCAPE LL	06-22-2017	06-22-2018	□	
jscape	RSA	1024	113060980	C=US,ST=FL,L=Miami,O=JSCAPE,OU=S	C=US,ST=FL,L=Miami,O=JSCAPE,OU=S	07-03-2017	07-03-2018	□	

Generating a certificate revocation list

A certificate revocation list (CRL) may be used by external applications to identify server keys that have been revoked by JSCAPE MFT Server. To generate a certificate revocation list go to the `Server Keys` panel in `Key Manager` and click the `Revocation List > Generate` button. The resulting CRL will be placed in the file `/webapp/management/mft-server.crl` relative to your installation directory. This file may be accessed as a CRL URL using the following format `http(s)://<server management host>:<server management port>/mft-server.crl`

Figure 228



Certificate Revocation List Generation
Specify CRL parameters.

Signing Key* example_rsa

Expiration period* 30 day(s)

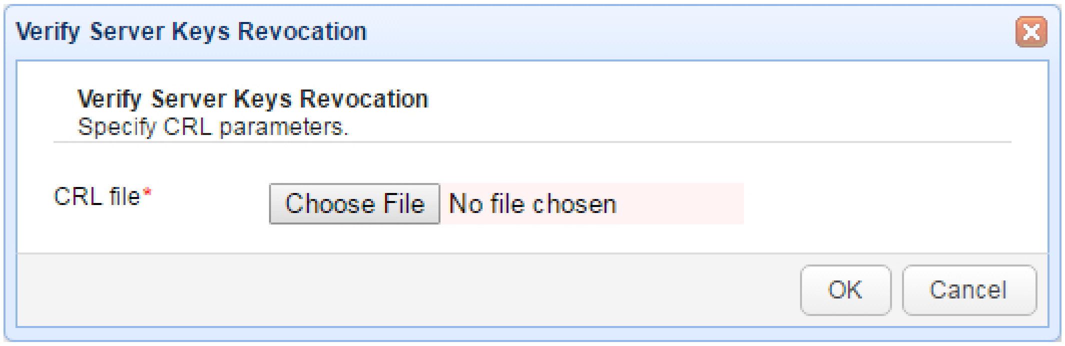
Signing Key - The server key used to sign the CRL.

Expiration period - The number of days from generation that this CRL is valid.

Verifying against a certificate revocation list

A certificate revocation list (CRL) may be used to identify server keys that have been revoked. These CRL may be generated within JSCAPE MFT Server or from external applications. In the event that the CRL is managed in an external application you may wish to periodically verify your server keys against this CRL. This can be performed manually from the `Server Keys` panel in `Key Manager` by clicking the `Revocation List > Verify` button. To automate this process you can associate a CRL URL with the server key during the creation process. See Revoking a key for details.

Figure 229



CRL file - A valid CRL file.

Host keys

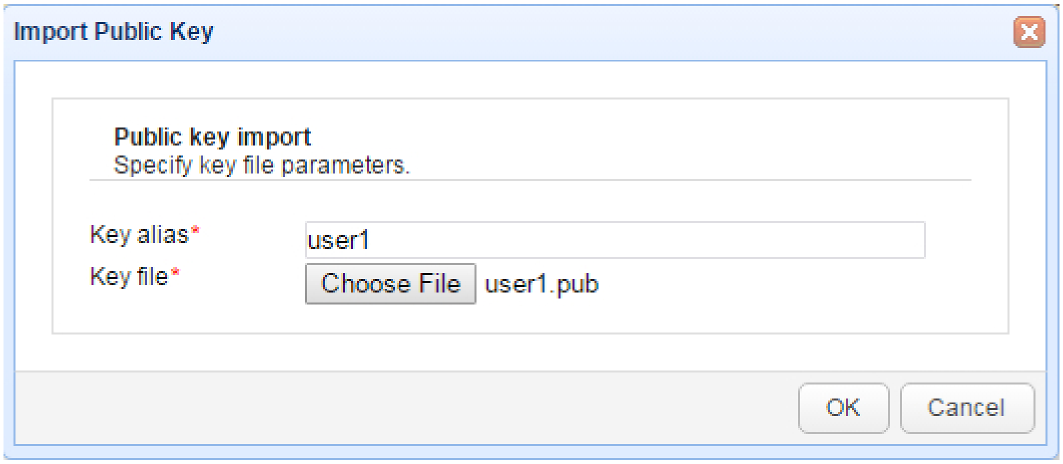
Overview

Host keys are the keys which are used to verify the identity of remote hosts. These may include public keys for SSL certificates used to protect FTPS and HTTPS services as well as public host keys for SSH/SFTP services. Host keys may be associated with trading partners and/or used in certain trigger actions that perform secure file transfers to verify the identity of remote hosts. Host keys may also be used in AS2 trading partners for the purposes of encrypting AS2 messages.

Importing a host key

You may import existing certificates or public key for use in validating the identity of remote hosts in secure client connections. To import an existing certificate or public key open the Key Manager by selecting `Keys` from the main menu. The `Key Manager` will be displayed. Select the `Host Keys` tab and click on the `Import > Import File` button. The `Import` dialog is displayed.

Figure 69



Import Public Key

Public key import
Specify key file parameters.

Key alias*	user1
Key file*	Choose File user1.pub

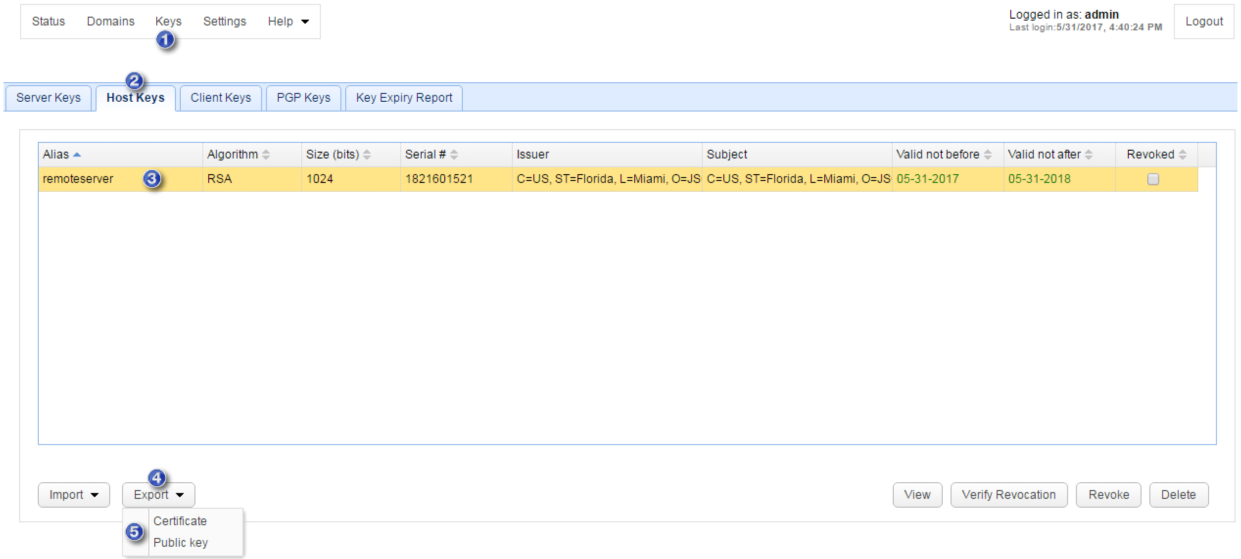
Key alias - The local alias which will be used for storing in the servers local keystore. This may be any value of your choice.

Key file - The source certificate/public key file path to import from.

Exporting a host key

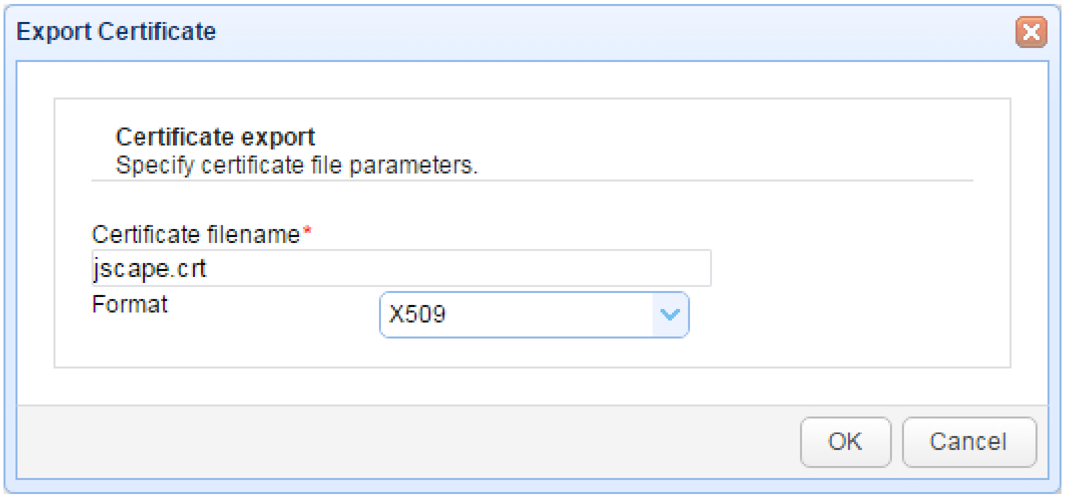
To export an existing host key certificate or public key open the `Key Manager` by selecting the `Server > Key Manager...` option from the main menu. The `Key Manager` will be displayed. Select the `Host Keys` tab, select a key and click on the `Export > Certificate` or `Export > Public key` button. The `Export` dialog is displayed.

Figure 194



Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked
remoteserver	RSA	1024	1821601521	C=US, ST=Florida, L=Miami, O=JS	C=US, ST=Florida, L=Miami, O=JS	05-31-2017	05-31-2018	□

Figure 64



Certificate export
Specify certificate file parameters.

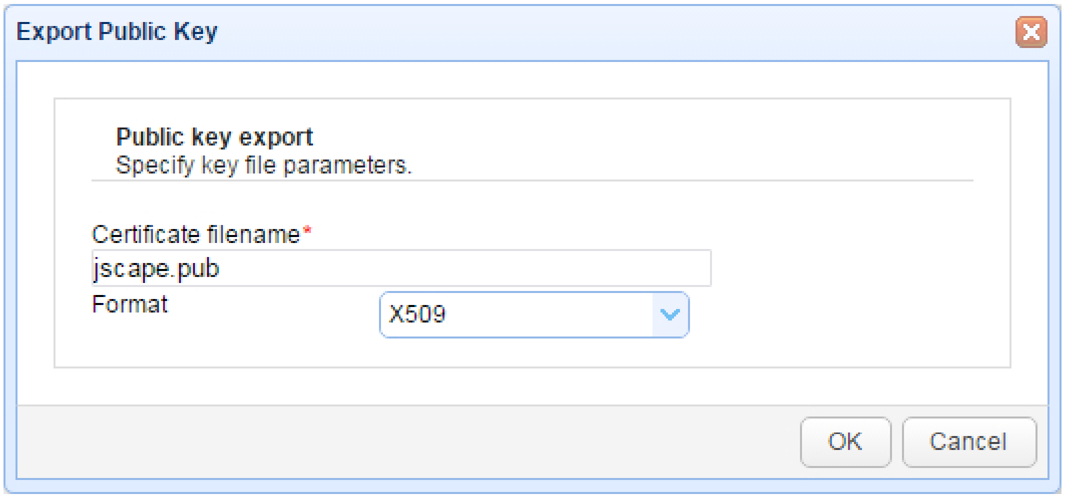
Certificate filename*: jscape.crt

Format: X509

Certificate filename - The name of the file you wish to export the certificate to

Format - The format in which to export certificate.

Figure 159



Public key export
Specify key file parameters.

Certificate filename*: jscape.pub

Format: X509

Certificate filename - The name of the file you wish to export the public key to.

Format - The format in which to export public key.

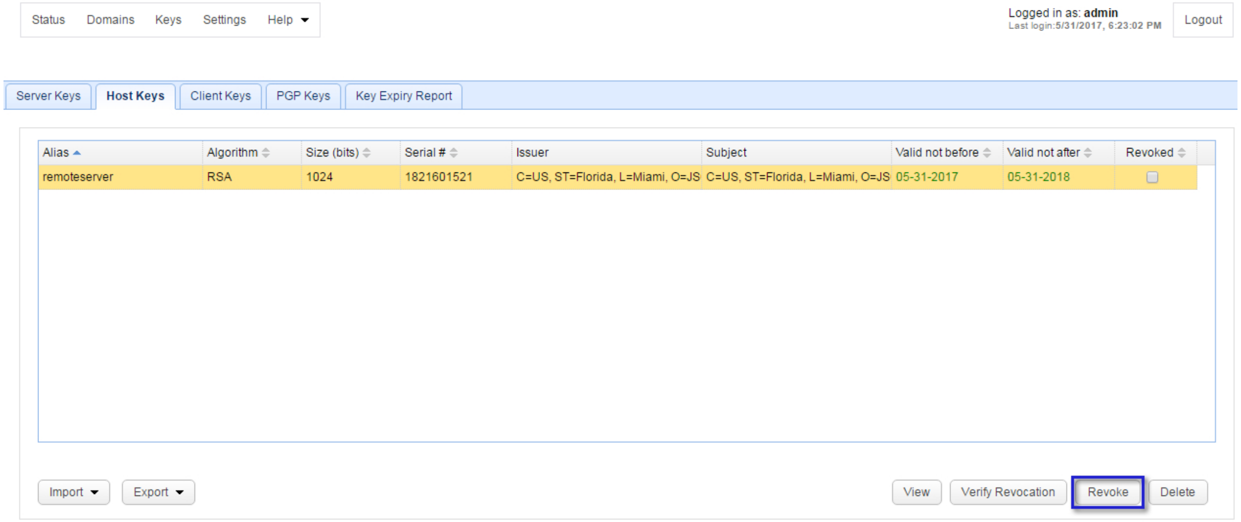
Revoking a key

A host key may be revoked from within JSCAPE MFT Server by selecting the desired key from `Host Keys` tab in `Key Manager` and clicking the `Revoke` button. Revoking a host key prevents the key from being used in both inbound and outbound connections.

Figure 230

Key management

18

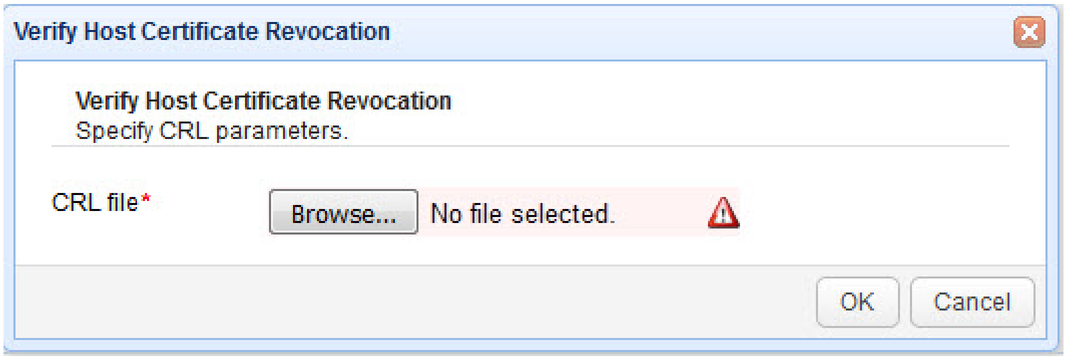


Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked
remoteserver	RSA	1024	1821601521	C=US, ST=Florida, L=Miami, O=JS	C=US, ST=Florida, L=Miami, O=JS	05-31-2017	05-31-2018	□

Verifying against a certificate revocation list

A certificate revocation list (CRL) may be used to identify host keys that have been revoked. These CRL may be generated from external applications. To verify that validity of your host keys navigate to the `Host Keys` panel in `Key Manager` and click the the `Verify Revocation` button.

Figure 231


Verify Host Certificate Revocation
Verify Host Certificate Revocation
Specify CRL parameters.
CRL file*
Browse...
No file selected.
OK
Cancel

CRL file - A valid CRL file.

Client keys

Overview

Client keys are used for enhanced authentication of clients when connecting to JSCAPE MFT Server. For example, you may specify that your service requires that the user provide both a password and private key during the authentication process in order to be granted access. This is more secure form of authentication than simple password authentication as it requires a secondary token (a private key) in addition to the password. Client keys may also be used in the OFTP protocol for the purposes of message encryption and/or signature verification.

See also

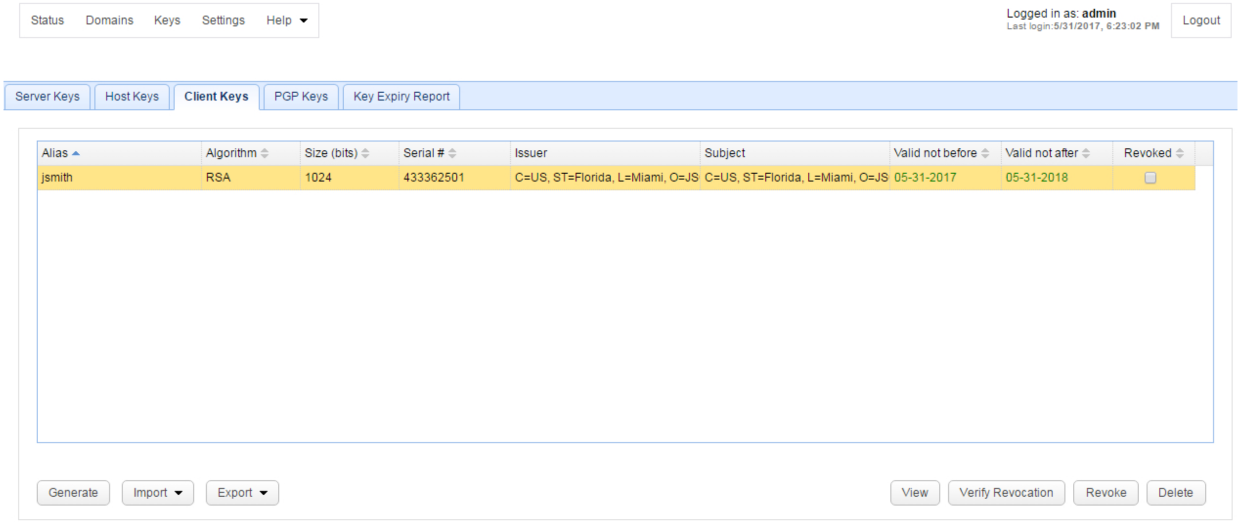
[Generating a key]
[Importing a certificate and/or public key]
[Exporting a certificate and/or public key]

Key management 18

Generating a key

To generate a client key open the `Key Manager` by selecting `Keys` from the main menu. The `Key Manager` will be displayed.

Figure 195

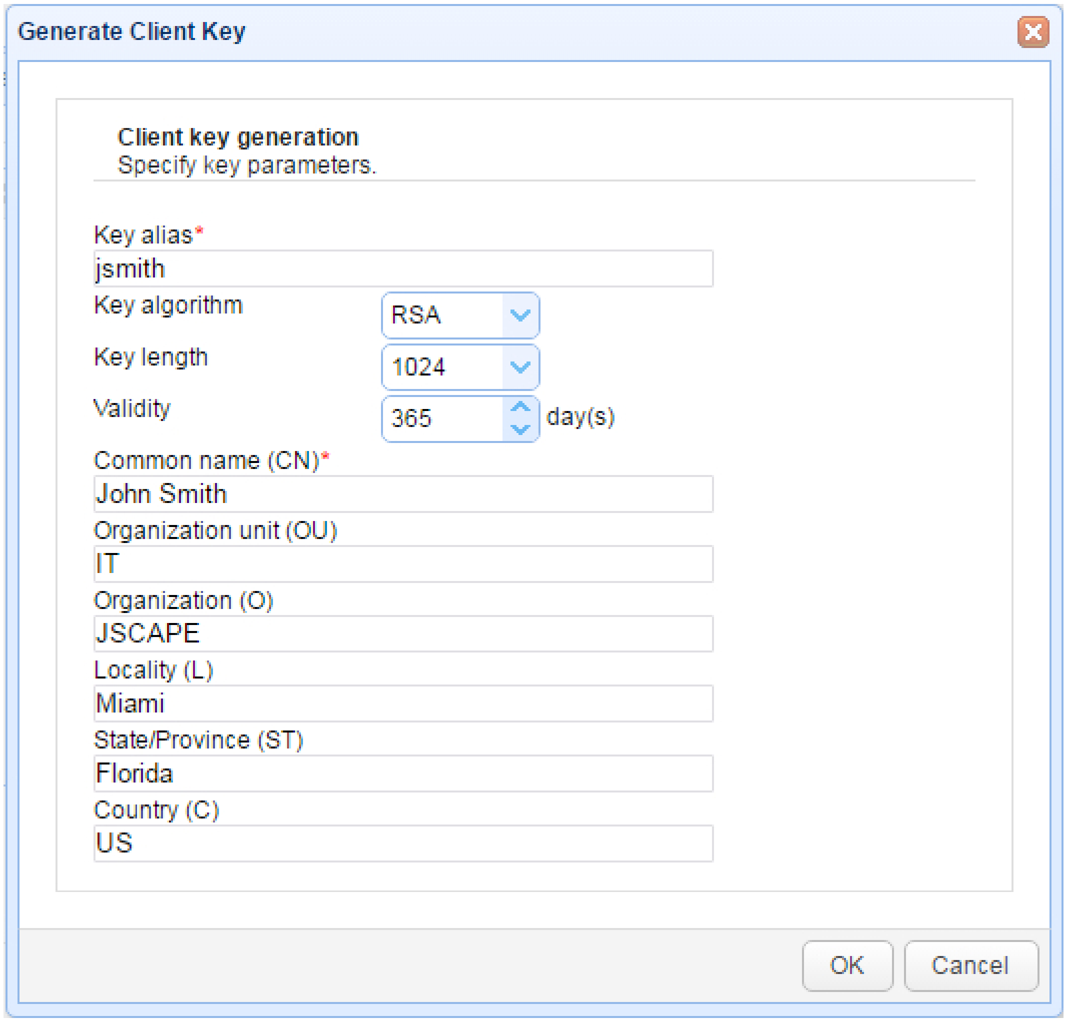


Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked
jsmith	RSA	1024	433362501	C=US, ST=Florida, L=Miami, O=JS	C=US, ST=Florida, L=Miami, O=JS	05-31-2017	05-31-2018	□

Step 1

Select the `Client Keys` tab and click on the `Generate` button. The `Generate Client Key` dialog is displayed.

Figure 66



Generate Client Key

Client key generation
Specify key parameters.

Key alias*: jsmith

Key algorithm: RSA

Key length: 1024

Validity: 365 day(s)

Common name (CN)*: John Smith

Organization unit (OU): IT

Organization (O): JSCAPE

Locality (L): Miami

State/Province (ST): Florida

Country (C): US

Key alias - Alias you wish to assign to the key.

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

Key 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. For a client key this is typically the full name of the user e.g. John Smith.

Organizational unit - The unit within the users organization that this key will be used for e.g. IT.

Organization - The users organization name.

Locality - The users city.

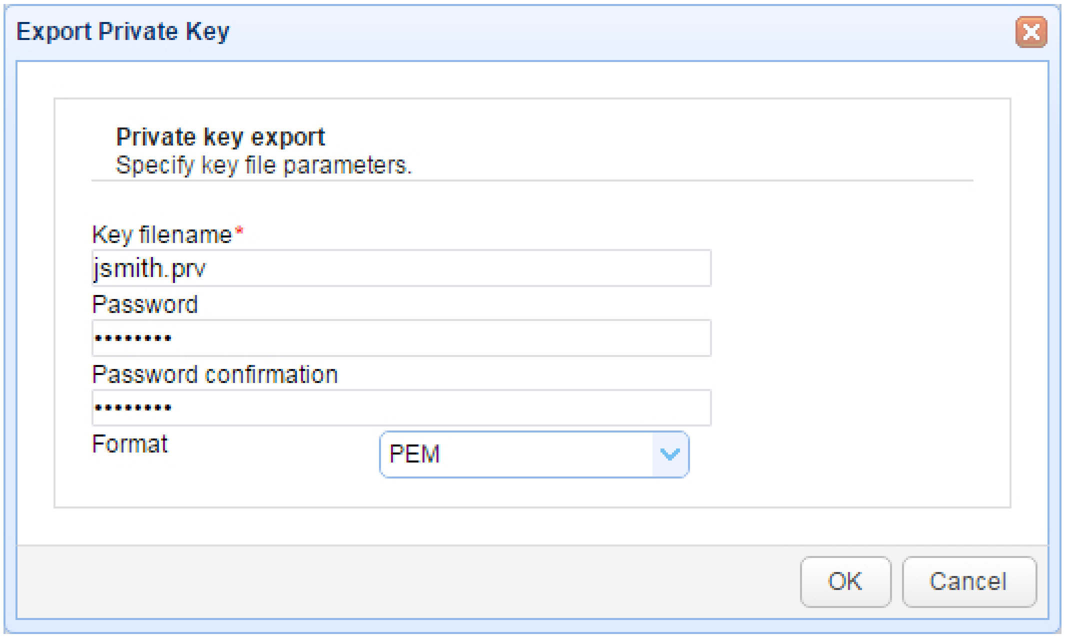
State/Province - The users state or province.

Country - The users 2 character country code e.g. US.

Step 2

Export private key. Exported file may be imported by FTPS and SFTP clients for optional use in client authentication.

Figure 68



Key filename*: jsmith.prv
Password: ••••••••
Password confirmation: ••••••••
Format: PEM

Key filename - The file you wish to export the private key to.

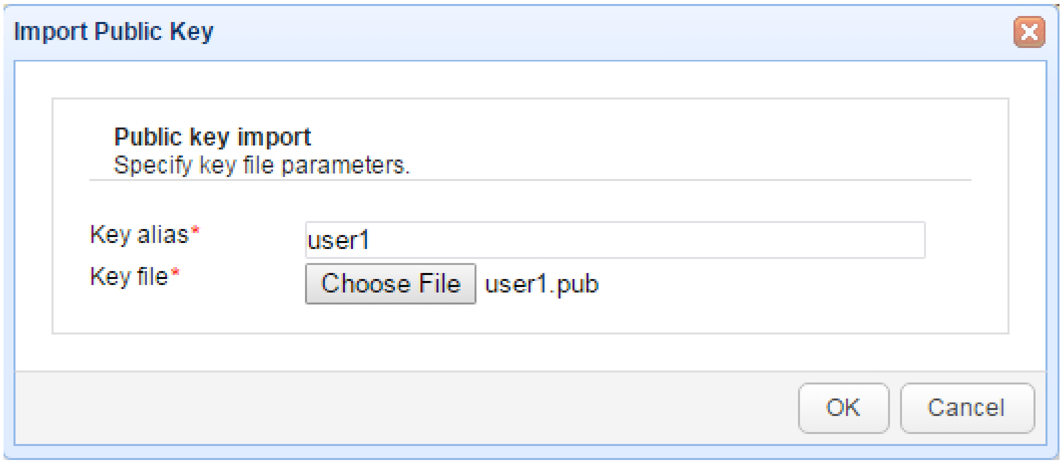
Password - The password used to protect private key. Leave blank for no password.

Format - The format in which you wish to export private key.

Importing a certificate and/or public key

You may import existing certificates or public key for use in authenticating secure client connections using FTPS (FTP over SSL) and SFTP (FTP over SSH) connections or encrypting files using OpenPGP. To import an existing certificate or public key open the `Key Manager` by selecting `Keys` from the main menu. The `Key Manager` will be displayed. Select the `Client Keys` tab and click on the `Import > File` button. The `Import` dialog is displayed.

Figure 69



Public key import
Specify key file parameters.

Key alias* user1

Key file* Choose File user1.pub

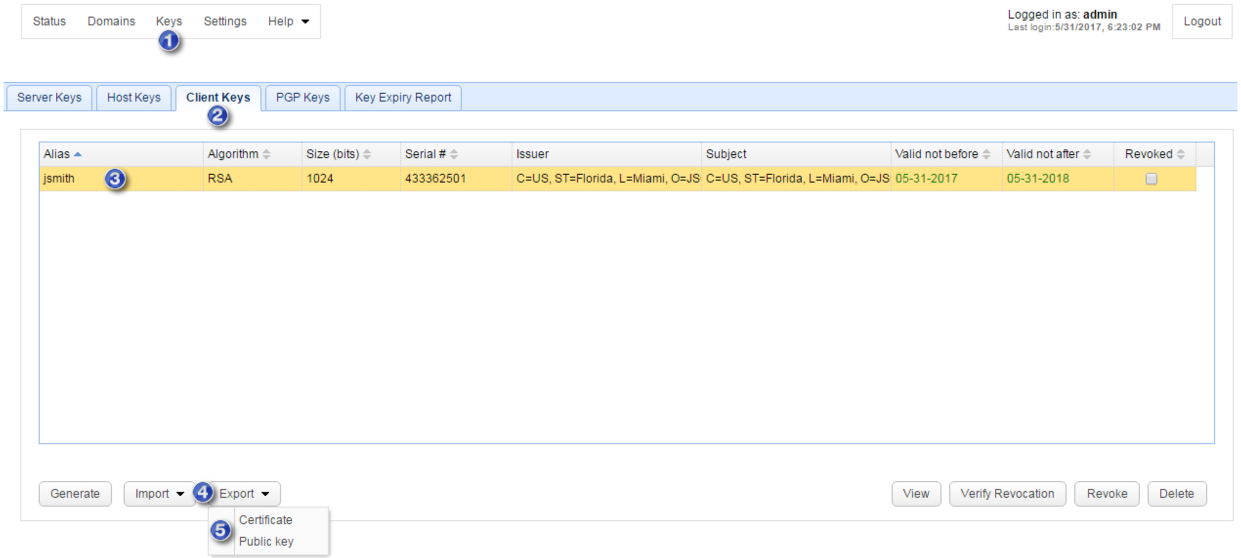
Key alias - The local alias which will be used for storing in the servers local keystore. This may be any value of your choice.

Key file - The source certificate/public key file path to import from.

Exporting a certificate and/or public key

To export an existing client certificate open the `Key Manager` by selecting `Keys` from the main menu. The `Key Manager` will be displayed. Select the `Client Keys` tab, select a certificate and click on the `Export > Certificate` or `Export > Public key` button. The `Export` dialog is displayed.

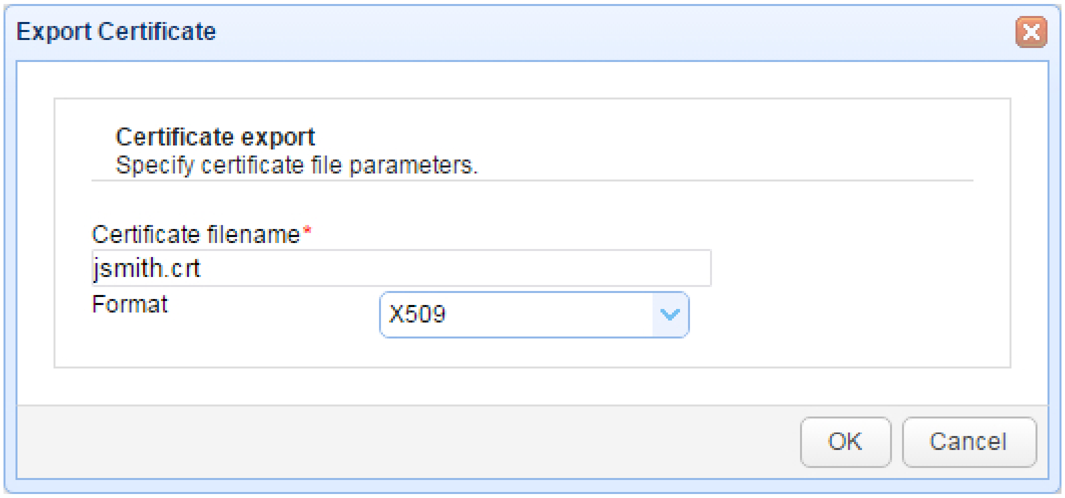
Figure 240



Logged in as: **admin**
Last login:5/31/2017, 6:23:02 PM

Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked
jsmith	RSA	1024	433362501	C=US, ST=Florida, L=Miami, O=JS	C=US, ST=Florida, L=Miami, O=JS	05-31-2017	05-31-2018	□

Figure 188



Export Certificate

Certificate export
Specify certificate file parameters.

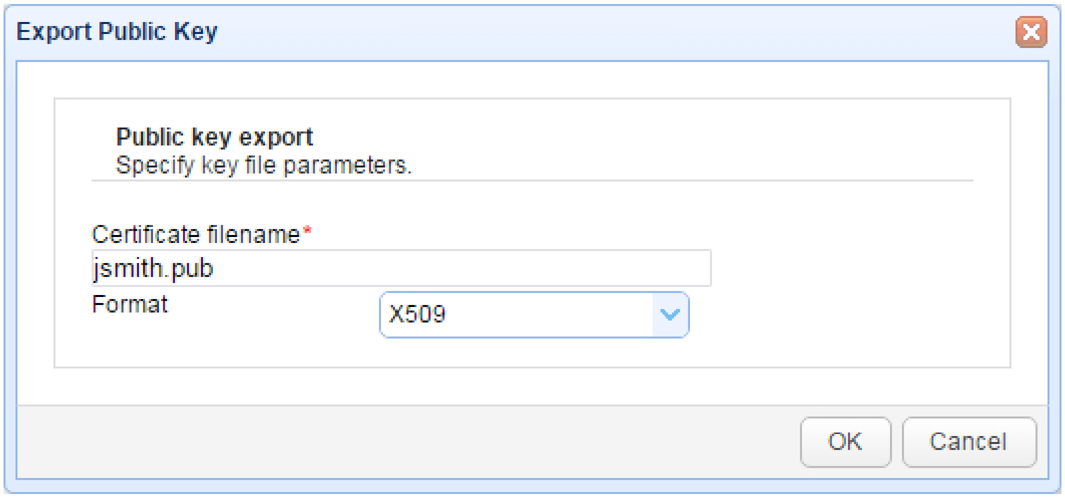
Certificate filename*
jsmith.crt

Format: X509

Certificate filename - The name of the file you wish to export the certificate to.

Format - The format in which to export certificate.

Figure 189



Export Public Key

Public key export
Specify key file parameters.

Certificate filename*
jsmith.pub

Format: X509

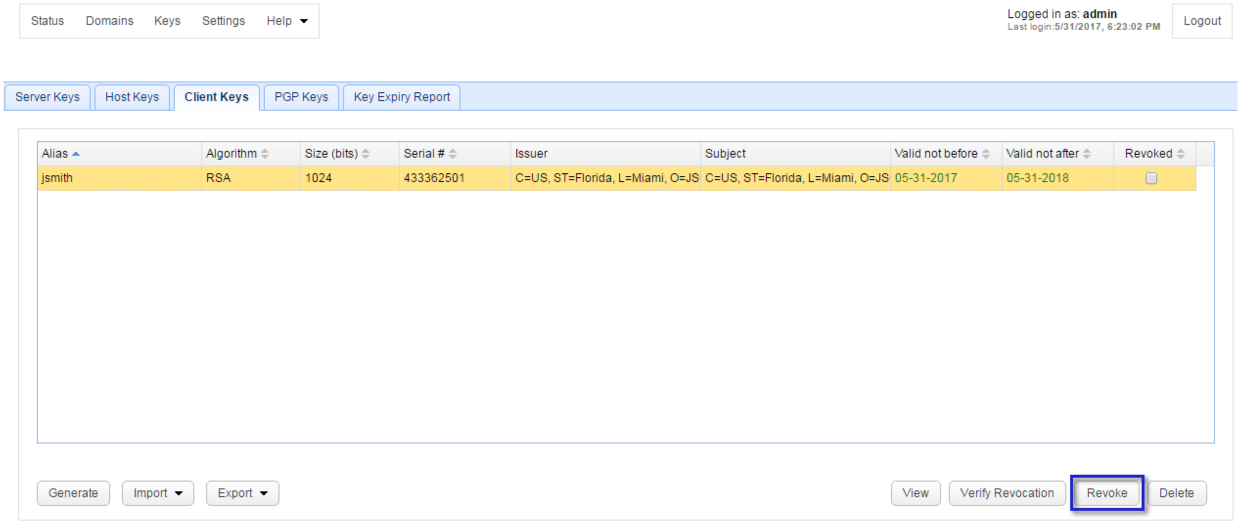
Certificate filename - The name of the file you wish to export the public key file to.

Format - The format in which to export public key.

Revoking a key

A client key may be revoked from within JSCAPE MFT Server by selecting the desired key from `Client Keys` tab in `Key Manager` and clicking the `Revoke` button. Revoking a client key prevents the key from being used in both inbound and outbound connections.

Figure 233

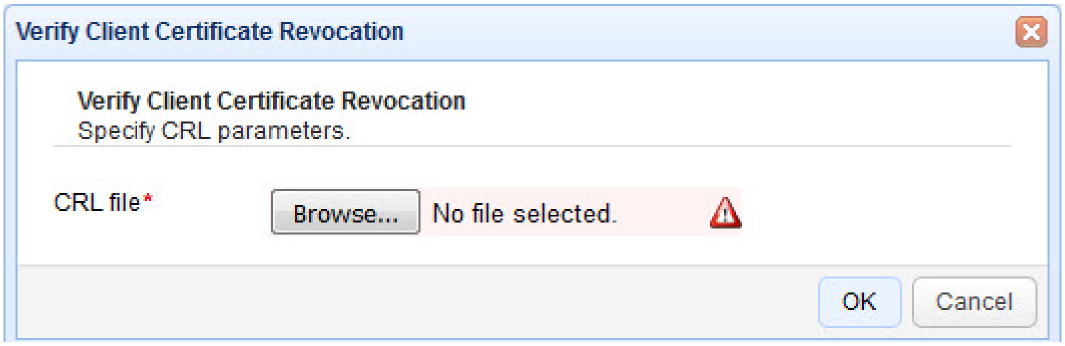


Alias	Algorithm	Size (bits)	Serial #	Issuer	Subject	Valid not before	Valid not after	Revoked
jsmith	RSA	1024	433362501	C=US, ST=Florida, L=Miami, O=JS	C=US, ST=Florida, L=Miami, O=JS	05-31-2017	05-31-2018	□

Verifying against a certificate revocation list

A certificate revocation list (CRL) may be used to identify client keys that have been revoked. These CRL may be generated from external applications. To verify that validity of your client keys navigate to the `Client Keys` panel in `Key Manager` and click the the `Verify Revocation` button.

Figure 232


Verify Client Certificate Revocation
Verify Client Certificate Revocation
Specify CRL parameters.
CRL file*
Browse...
No file selected.
OK
Cancel

CRL file - A valid CRL file.

OpenPGP keys

Overview

JSCAPE MFT Server includes built-in support for PGP and works with many popular PGP clients. PGP is typically used to provide an additional layer of security on top of any network protocol security (e.g. SSL, SSH) that may be used. A common scenario is to PGP encrypt all files automatically upon successful upload to the server. This ensures that in the unlikely event your server is compromised, the attacker would still be unable to view PGP encrypted files without having the secret key needed to decrypt them.

Using PGP to encrypt files at rest is a common way of meeting government compliance standards such as the PCI DSS standard used for protecting credit card information.

Additional libraries needed for OpenPGP
PGP compatibility matrix

Key management 18

PGP encryption primer

PGP is a method of protecting digital content using a pair of PGP keys. PGP encryption makes it nearly impossible for someone to view the contents of an encrypted file without possessing the secret key and key password needed to decrypt the file.

Getting started

To begin, you must create a PGP key pair. This key pair consists of both a private key and public key. This key pair can be created using the tools provided in JSCAPE MFT Server or by using any of the supported third party PGP clients. The private key is yours to keep and may be used for decryption and optional signing of digital documents. The private key should be safely guarded and is typically protected with a password that only you know. The public key is what you distribute to those individuals/ organizations with whom you wish to exchange encrypted content.

To encrypt a document the sender encrypts the document using the recipients public key, then optionally signs the encrypted document with the senders private key. Signing the encrypted document proves to the recipient that the sender is who they say they are. All document encryption/signing in JSCAPE MFT Server is performed via a trigger and the PGP Encrypt File action.

To decrypt a document the recipient decrypts the file using the recipients private key/password and optionally verifies the sender using the public key that was provided to the recipient by the sender. All file decryption in JSCAPE MFT Server is performed via a trigger and the PGP Decrypt File action.

PGP usage

Some typical uses of PGP in JSCAPE MFT Server include:

- Automatically PGP encrypt/sign files upon upload ensuring data is protected while at-rest.
- Automatically PGP decrypt/verify files upon upload.
- Send PGP encrypted email messages to protect sensitive data.

See also

PGP compatibility matrix
Generating a key
Importing a public key
Exporting a public key
Trigger management

PGP compatibility matrix

The following is a PGP client compatibility matrix. The following PGP clients and functions have been tested successfully with JSCAPE MFT Server.

Client	Key Algorithm	Encrypt	Decrypt

PGP Desktop 9.x (and above)	DSA ElGamal	Yes	Yes
PGP Desktop 9.x (and above)	RSA	Yes	Yes
GPG 1.4.x (and above)	DSA ElGamal	Yes	Yes
GPG 1.4.x (and above)	RSA	Yes	Yes

Definitions

Decrypt - Create an OpenPGP key in JSCAPE MFT Server Key Manager or via web interfac. Import resulting public key into PGP client. Encrypt file using PGP client. Decrypt File using JSCAPE MFT Server PGP Decrypt File action.

Encrypt - Create a private key in PGP client. Import corresponding public key into JSCAPE MFT Server Key Manager under OpenPGP keys tab. Encrypt file using JSCAPE MFT Server PGP Encrypt File action. Decrypt file using PGP client.

Note

In order to use PGP successfully with JSCAPE MFT Server you must properly install the Unlimited Jurisdiction Policy Files. For more information on this topic please see the following.

See also

Additional libraries needed for OpenPGP
Trigger management

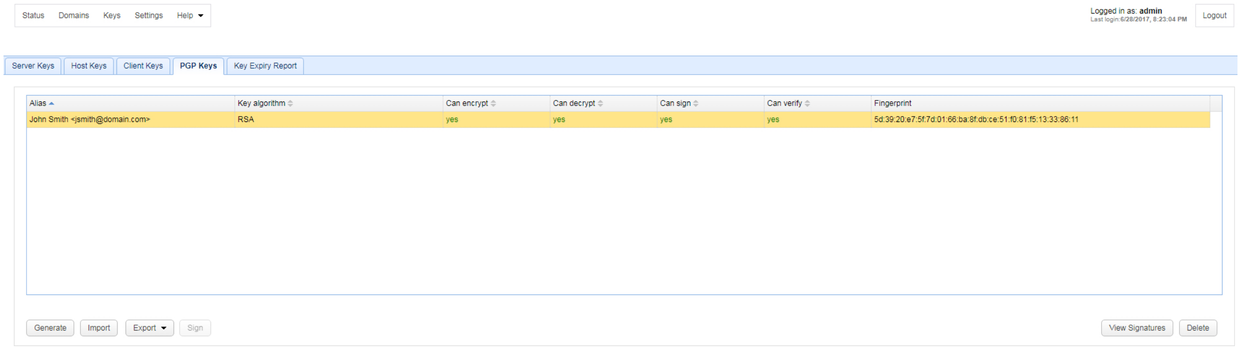
Generating a key pair

PGP key pairs may be generated from either the `Key Manager` available in JSCAPE MFT Server Manager or via the `My Account > OpenPGP Encryption > Generate OpenPGP Key` link in the web interface. Keys imported via the `Key Manager` are system keys that may be used anywhere in the system, whereas keys imported via the web interface are private to the user that imported the key and may be used only to encrypt files uploaded to virtual paths that are accessible to the user and have PGP encryption enabled.

Generating a key pair via Key Manager

To generate a PGP key pair click `Keys` from the main menu in the JSCAPE MFT Server Manager. The `Key Manager` is displayed. Select the `PGP Keys` tab and click the `Generate` button. The `Generate PGP Key` dialog is displayed.

Figure 108



Alias	Key algorithm	Can encrypt	Can decrypt	Can sign	Can verify	Fingerprint
John Smith <jsmith@domain.com>	RSA	yes	yes	yes	yes	5d:39:20:e7:5f:7d:01:66:ba:8f:db:ce:51:f0:81:f5:13:33:86:11

Key algorithm - The type of key used. Valid values are RSA or DSA.

Can encrypt - Indicates whether key can be used for encrypt operations.

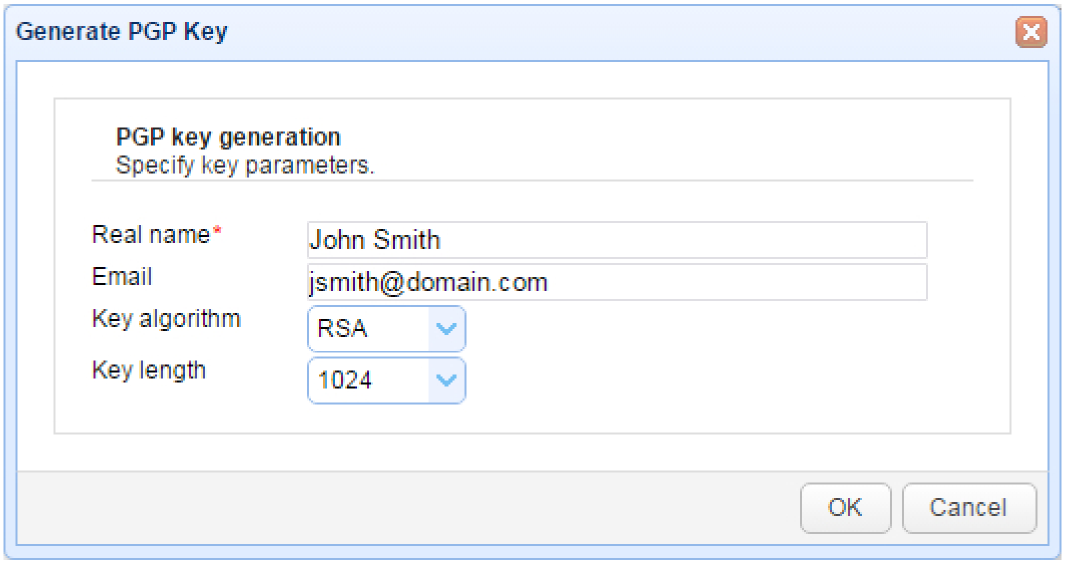
Can decrypt - Indicates whether key can be used for decrypt operations.

Can sign - Indicates whether key can be used for sign operations.

Can verify - Indicates whether key can be used for verify signature operations.

Fingerprint - The unique fingerprint for the key.

Figure 109



Generate PGP Key

PGP key generation
Specify key parameters.

Real name* John Smith
Email jsmith@domain.com
Key algorithm RSA
Key length 1024

Real name - The full name of the key pair owner e.g. John Smith.

Email - The email address for the key pair owner e.g. jsmith@domain.com

Key algorithm - The encryption algorithm used.

Key length - The length of encryption key.

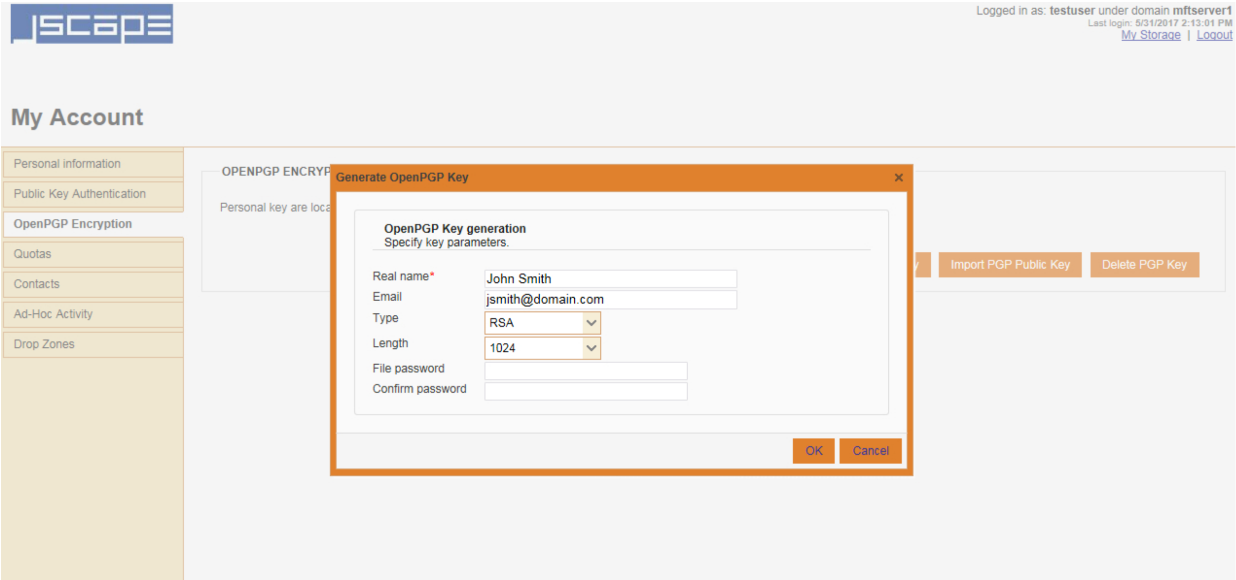
Generating a key pair via client web interface

To generate a key pair login via client web interface and click on the `My Account > OpenPGP Encryption > Generate OpenPGP Key` button. The `Generate OpenPGP Key` dialog is displayed.

Upon clicking the `Generate` button you will be prompted to save the private key on your local system. Make sure to save this key in a safe place as without it you will be unable to decrypt files encrypted using the public key. Furthermore, anyone who obtains your private key may be able to decrypt your PGP encrypted files so it is recommended that you apply a password to your private key.

You will notice that upon generating your PGP key pair that a file named `.pgp/key.pub` will be placed in your home directory. DO NOT DELETE this file as it will be used for encrypting files uploaded to virtual paths that have PGP encryption enabled. Note only one PGP public key may be associated with each account. Generating a new key pair or importing a new public key will overwrite the existing public key file.

Figure 153



Logged in as: **testuser** under domain **mftserver1**
Last login: 5/31/2017 2:13:01 PM

Generate OpenPGP Key

OpenPGP Key generation
Specify key parameters.

Real name* John Smith
Email jsmith@domain.com
Type RSA
Length 1024
File password
Confirm password

Real name - The full name of the key pair owner e.g. John Smith.

Email - The email address for the key pair owner e.g. jsmith@domain.com

Type - The cipher to use when creating key.

Key length - The length of encryption key.

Key algorithm - The encryption algorithm used.

File password - Optional private key password.

Importing public key

Using JSCAPE MFT Server Manager you can import an existing public PGP key. A typical scenario in which you would import a PGP public key would be the case where you want JSCAPE MFT Server to PGP encrypt documents using a PGP public key provided to you by a third party.

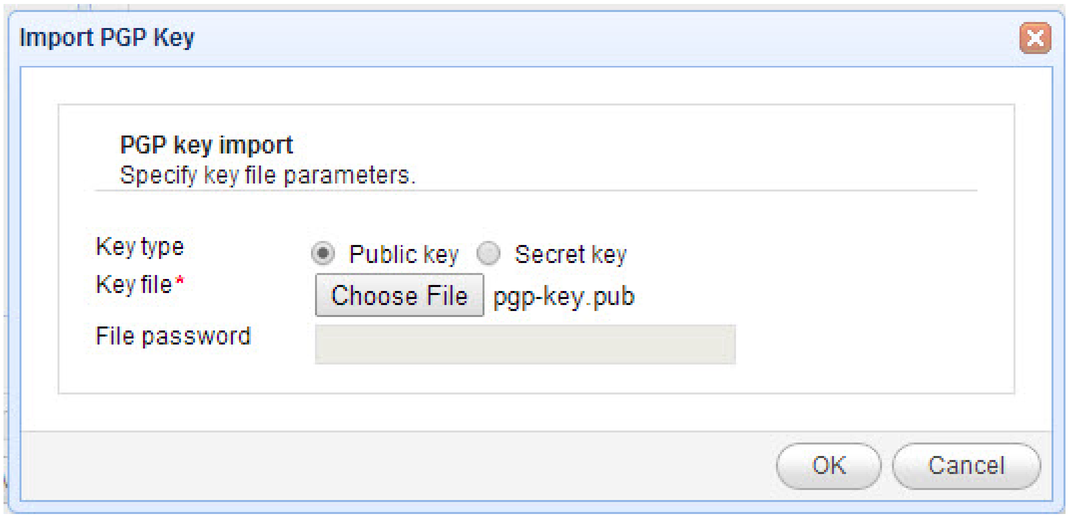
PGP key pairs may be imported from either the *Key Manager* available in JSCAPE MFT Server Manager or via the `My Account > OpenPGP Encryption > Import Public Key` link in the web interface. Keys imported via the `Key Manager` are system keys that may be used anywhere in the system, whereas keys imported via the web interface are private to the user that imported the key and may be used only to encrypt files uploaded to virtual paths that are accessible to the user and have PGP encryption enabled.

Importing public keys via Key Manager

Key management 18

To import a PGP public key click `Keys` from the main menu in JSCAPE MFT Server Manager. The `Key Manager` dialog is displayed. Select the `PGP Keys` tab and click the `Import` button. The `Import PGP Key` dialog is displayed.

Figure 110



Import PGP Key

PGP key import
Specify key file parameters.

Key type ● Public key ○ Secret key

Key file* pgp-key.pub

File password

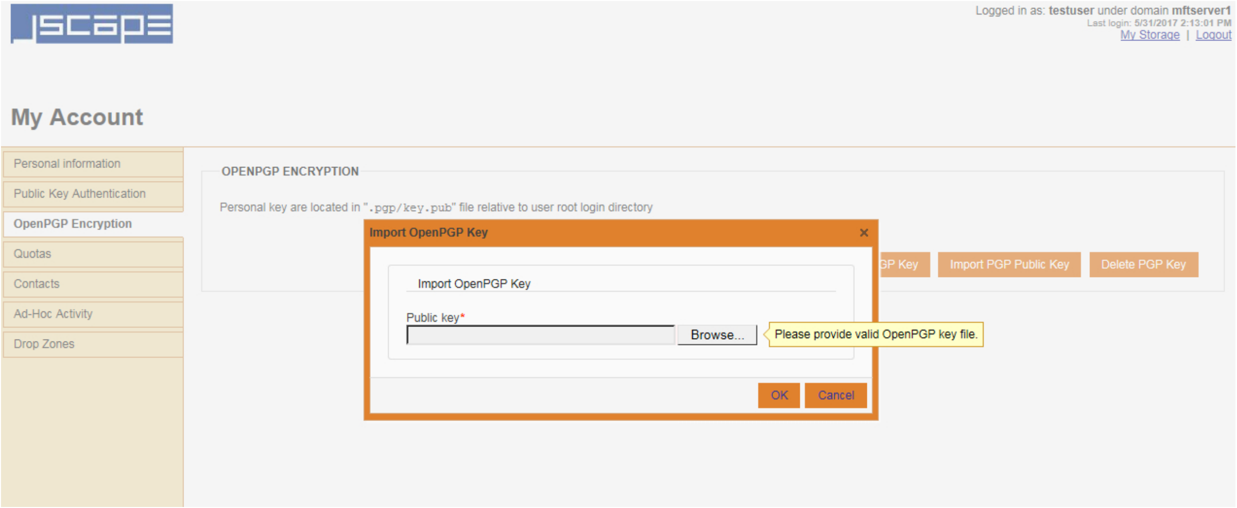
Key file - The PGP public key file.

Importing public keys via web interface

To import a public key login via web interface and click on the `My Account > OpenPGP Encryption > Import PGP Public Key` button. The `Import OpenPGP Key` dialog is displayed.

You will notice that upon importing your PGP key pair that a file named `.pgp/key.pub` will be placed in your home directory. DO NOT DELETE this file as it will be used for encrypting files uploaded to virtual paths that have PGP encryption enabled. NOTE only one PGP public key may be associated with each account. Generating a new key pair or importing a new public key will overwrite the existing public key file.

Figure 154



Logged in as: **testuser** under domain **mftserver1**
Last login: 5/31/2017 2:13:01 PM

My Account

OPENPGP ENCRYPTION

Personal key are located in "`.pgp/key.pub`" file relative to user root login directory

Import OpenPGP Key

Import OpenPGP Key

Public key*

Please provide valid OpenPGP key file.

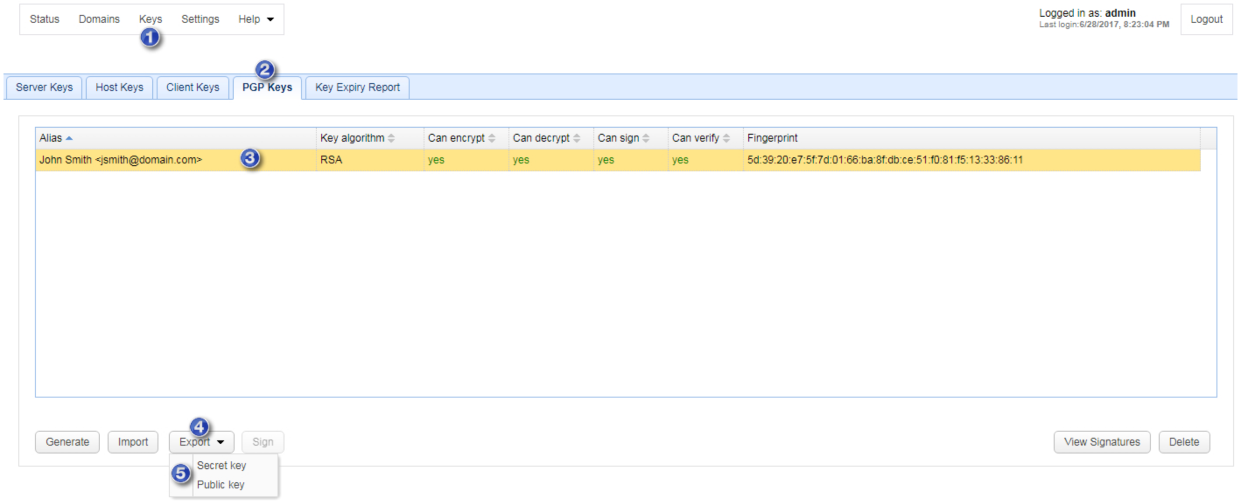
Public key - Location of public key on local system.

Exporting public and private keys

Using JSCAPE MFT Server Manager you can export an existing public PGP key. A typical scenario in which you would export a PGP public key would be the case where you want to distribute your public key to individuals/organizations who will then use your public key for encrypting documents that they then send to you for decryption.

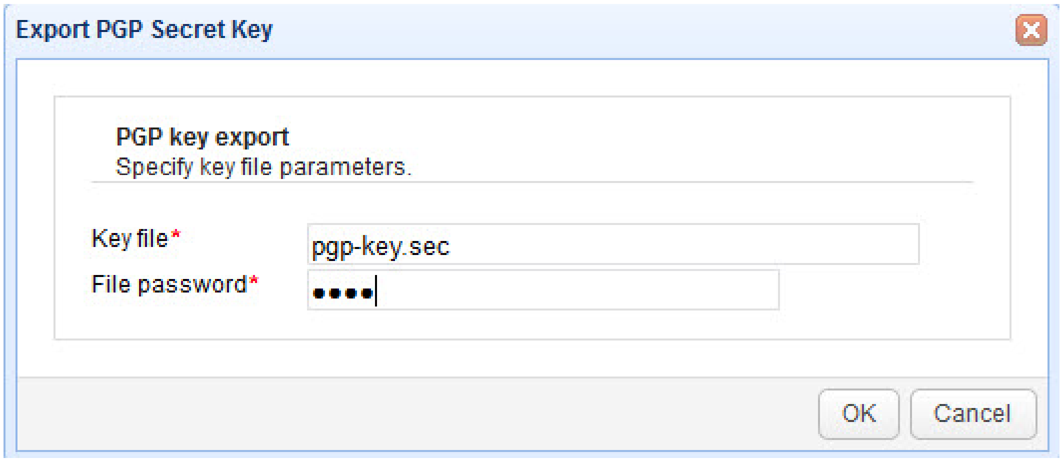
To export a PGP public key click `Keys` from the main menu in JSCAPE MFT Server Manager. The `Key Manager` is displayed. Select the `PGP Keys` tab, select the key alias you wish to export, then click the `Export > Secret key` or `Export > Public key` button. The `Export PGP Key` dialog is displayed.

Figure 241



Alias	Key algorithm	Can encrypt	Can decrypt	Can sign	Can verify	Fingerprint
John Smith <jsmith@domain.com>	RSA	yes	yes	yes	yes	5d:39:20:e7:5f:7d:01:66:ba:8f:db:ce:51:f0:81:f5:13:33:86:11

Figure 161



PGP key export
Specify key file parameters.

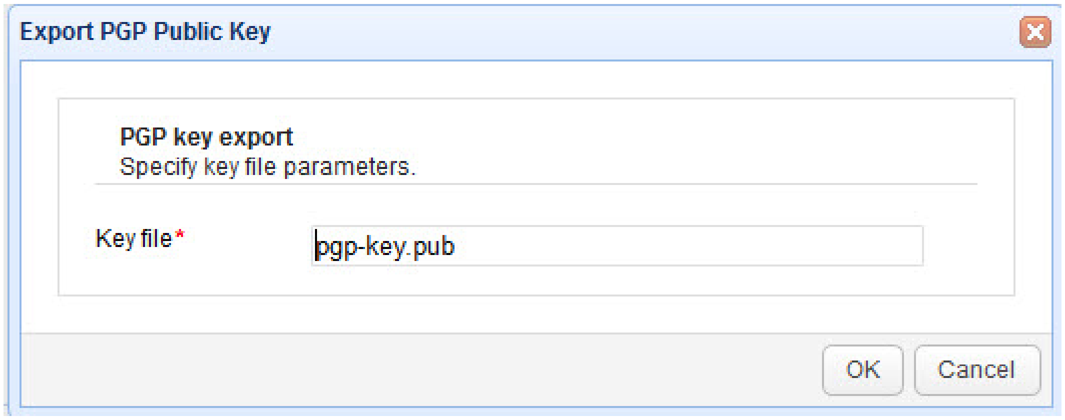
Key file* pgp-key.sec

File password* ••••

Key file - The private key.

File password - Optional password used to protect private key.

Figure 162



Export PGP Public Key

PGP key export
Specify key file parameters.

Key file* pgp-key.pub

Key file - The public key file.

Encrypting files and virtual paths

Files uploaded to JSCAPE MFT Server may be encrypted using a trigger listening for the `File Upload` event and the `PGP Encrypt File` action, or by enabling PGP encryption for a virtual directory. Triggers are recommended when you want to limit encryption of files to certain conditions e.g. filename, file type, etc. Enabling PGP encryption at the virtual path is recommended when you want to encrypt all files uploaded to a certain virtual path.

Encrypting files using triggers

For more information on encrypting files using triggers see the documentation on triggers and the inline help for the `File Upload` event and `PGP Encrypt File` action.

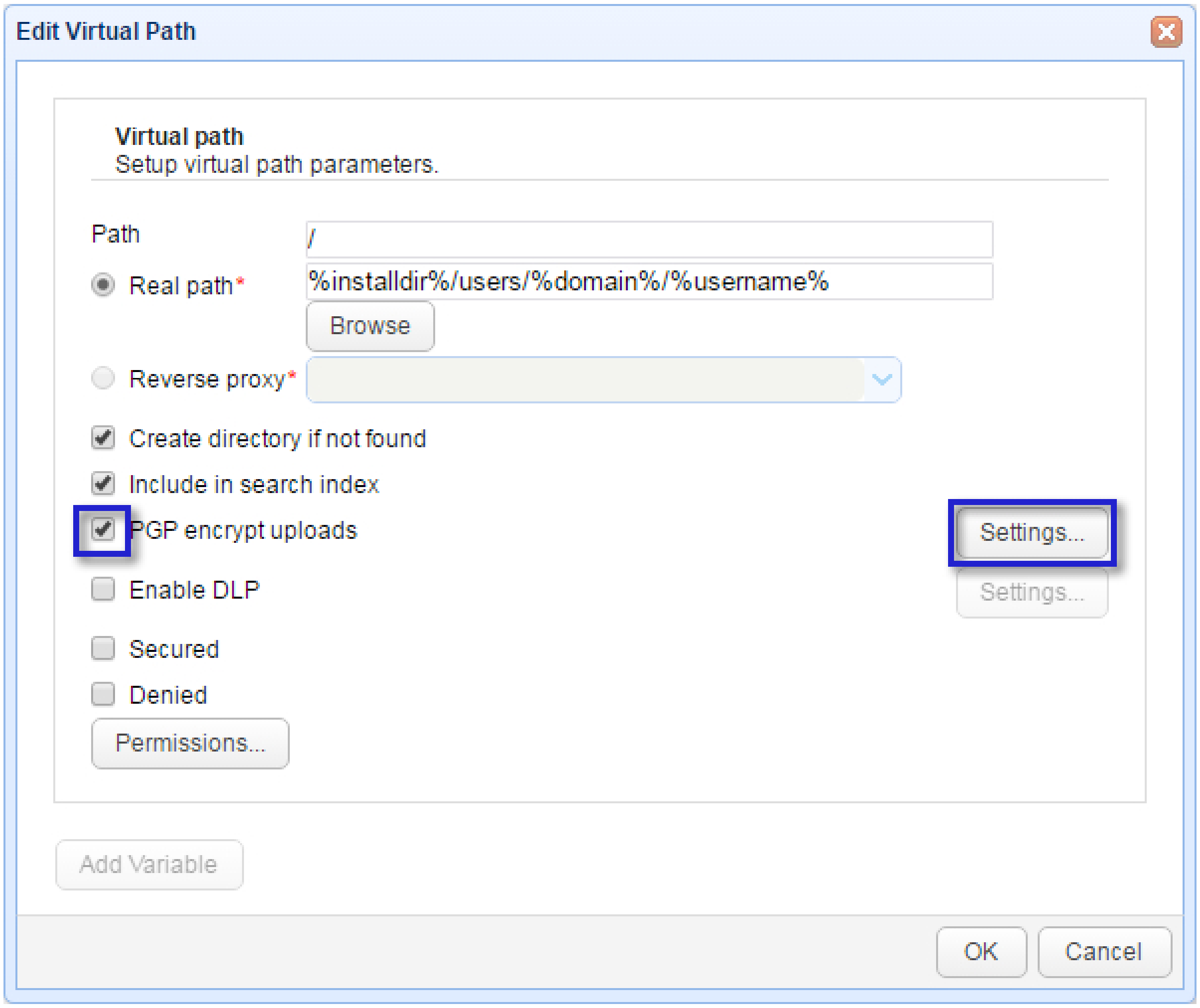
See also

Trigger management

Encrypting files using virtual paths

To PGP encrypt all files uploaded to a virtual path select the virtual path for the user or group and click `Edit`. Next, enable the `PGP encrypt uploads` option and click the `Settings` button. Here you will be prompted for which key to use when encrypting files. You may select either a system key that has been generated via the `Key Manager` in JSCAPE MFT Server Manager or a personal key that was created using the web interface.

Figure 155



Edit Virtual Path

Virtual path
Setup virtual path parameters.

Path: /

● Real path*: %installdir%/users/%domain%/%username%

○ Reverse proxy*

☑ Create directory if not found

☑ Include in search index

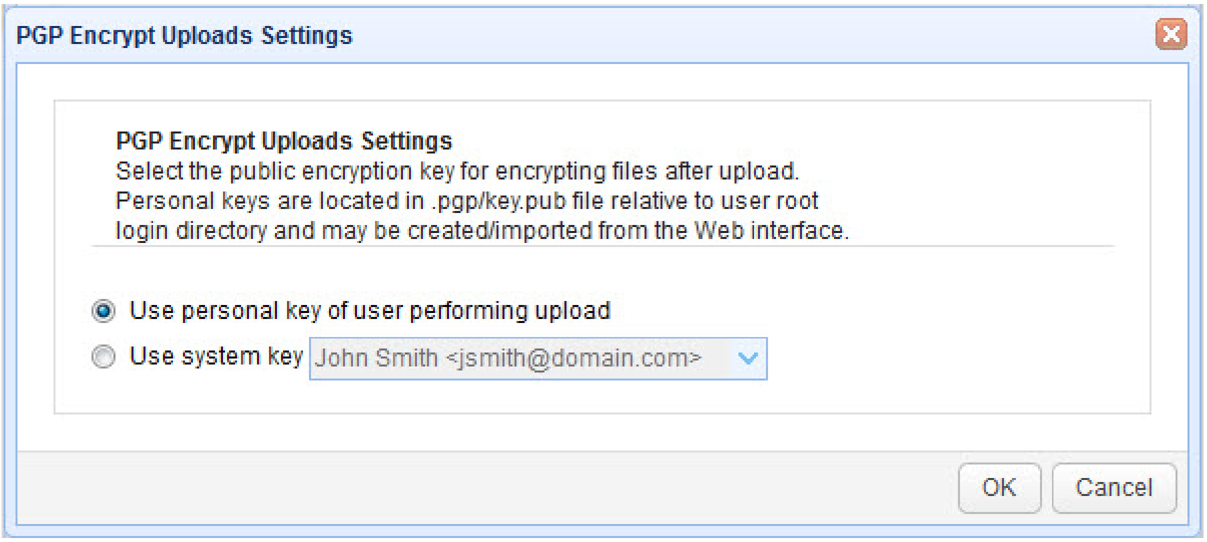
☑ PGP encrypt uploads

□ Enable DLP

□ Secured

□ Denied

Figure 156



PGP Encrypt Uploads Settings

PGP Encrypt Uploads Settings
Select the public encryption key for encrypting files after upload.
Personal keys are located in .pgp/key.pub file relative to user root
login directory and may be created/imported from the Web interface.

● Use personal key of user performing upload

○ Use system key: John Smith <jsmith@domain.com>

Key management 18

Decrypting files

Files uploaded to JSCAPE MFT Server may be decrypted using a trigger listening for the `File Upload` event and the `PGP Decrypt File` action,

For more information on decrypting files using triggers see the documentation on triggers and the inline help for the `File Upload` event and `PGP Decrypt File` action.

See also

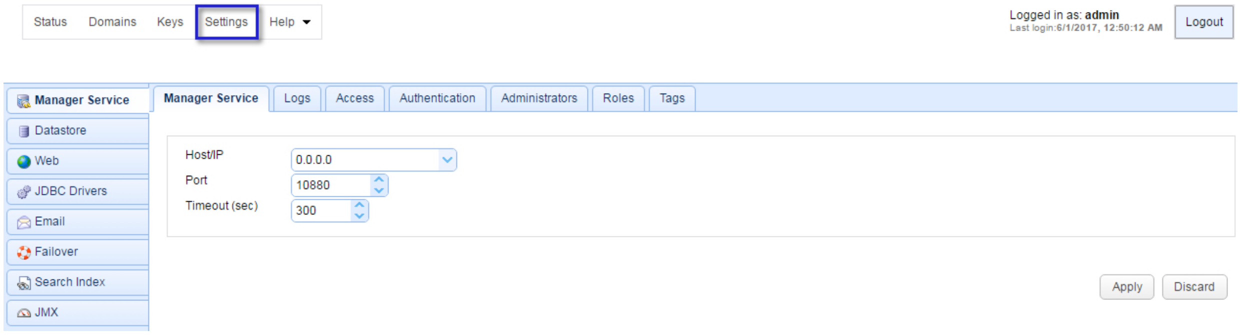
Trigger management

Server Settings

Overview

`Settings` controls various global configuration properties and server side settings for JSCAPE MFT Server Service. To access, select the `Settings` menu item from the main menu.

Figure 164



Host/IP 0.0.0.0
Port 10880
Timeout (sec) 300

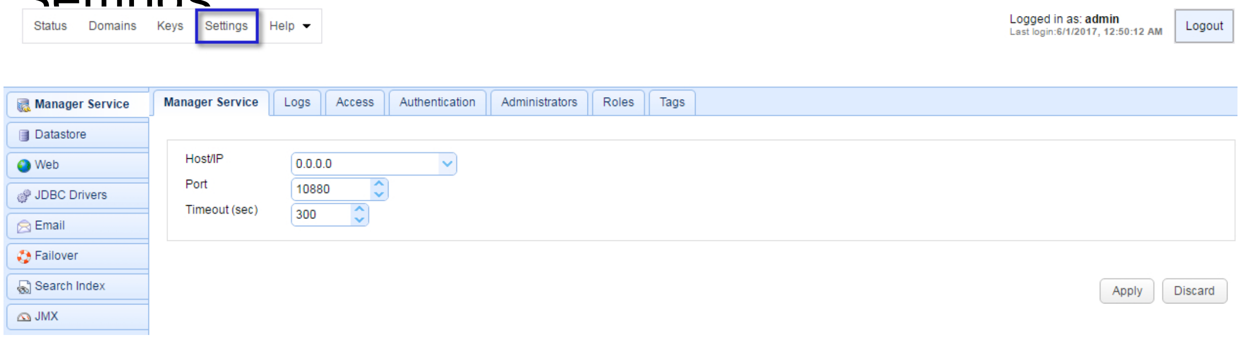
Manager service settings

The `Manager Service` node may be used to change the administrative password for the JSCAPE MFT Server Service as well as other properties.

Viewing administrative logs
Restricting administrative access by IP
Customizing administrator authentication method
Managing administrators
Managing administrative roles
Managing administrative tags

Figure 164

19 JSCAPE MFT Server Manager Settings



Host/IP 0.0.0.0

Port 10880

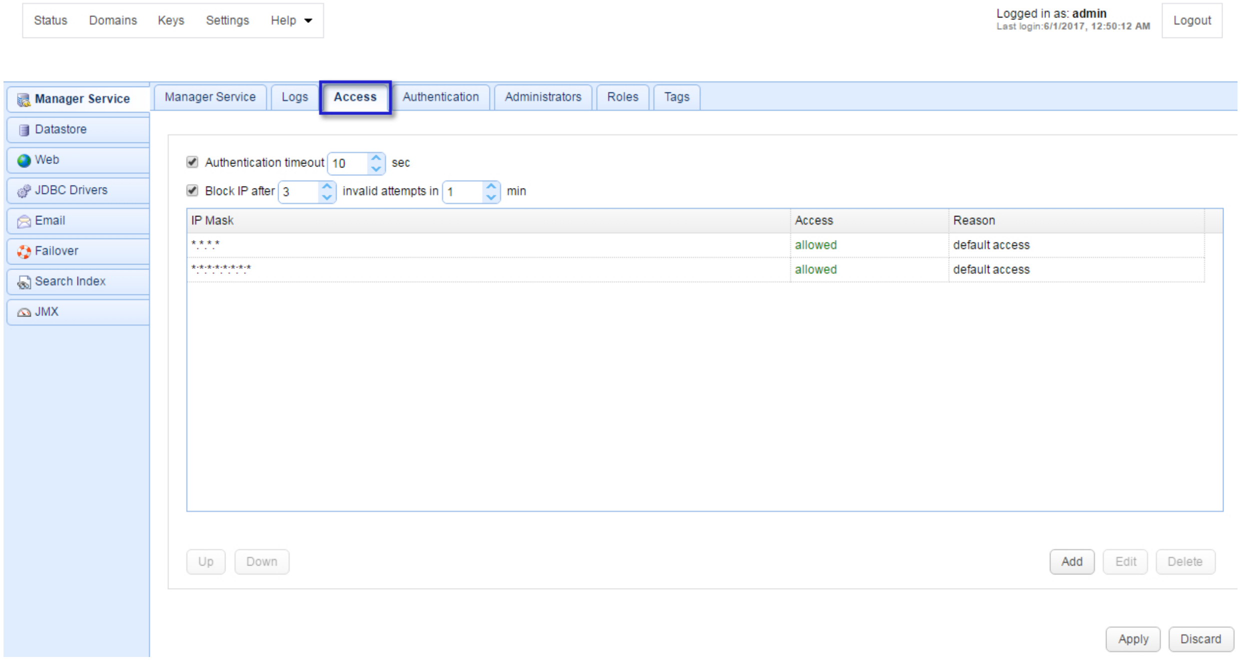
Timeout (sec) 300

Host/IP - The IP address that the JSCAPE MFT Server Service is running on.

Port - The port that the JSCAPE MFT Server Service is running on.

Timeout - Manager timeout in seconds when communicating with JSCAPE MFT Server Service.

Figure 107



☑ Authentication timeout 10 sec

☑ Block IP after 3 invalid attempts in 1 min

IP Mask	Access	Reason
..*.*	allowed	default access
::*:*:*:*:*:*	allowed	default access

Authentication timeout - The amount of time in seconds that administrative service client may remain connected without authenticating.

Block IP after - Blocks a client IP address after X invalid authentication attempts within Y minutes.

As an improved security measure you may define what IP addresses are allowed or disallowed access to access the administrative service.

IP mask examples

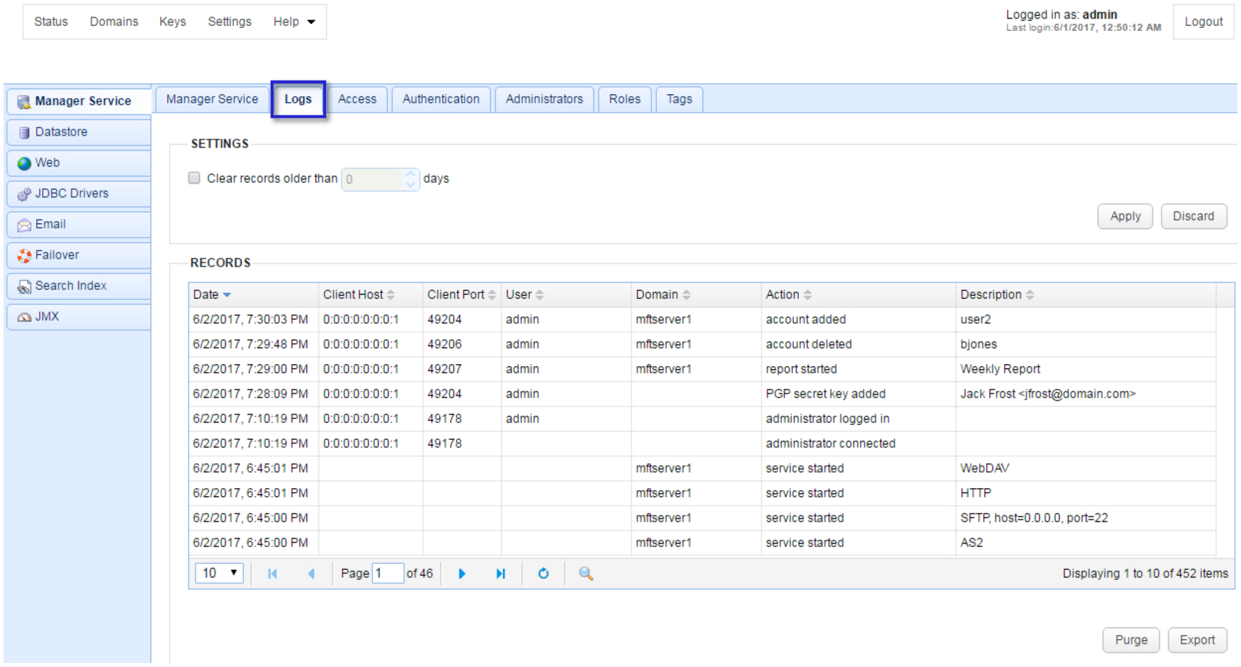
Examples of valid IP masks are as follows:

`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.

Viewing administrative logs

Administrative logs are stored separately from user log data and are used to track all administrative logins and changes to configuration data.

Figure 196



SETTINGS

□ Clear records older than 0 days

RECORDS

Date	Client Host	Client Port	User	Domain	Action	Description
6/2/2017, 7:30:03 PM	0:0:0:0:0:0:0:1	49204	admin	mftserver1	account added	user2
6/2/2017, 7:29:48 PM	0:0:0:0:0:0:0:1	49206	admin	mftserver1	account deleted	bjones
6/2/2017, 7:29:00 PM	0:0:0:0:0:0:0:1	49207	admin	mftserver1	report started	Weekly Report
6/2/2017, 7:28:09 PM	0:0:0:0:0:0:0:1	49204	admin		PGP secret key added	Jack Frost <jfrost@domain.com>
6/2/2017, 7:10:19 PM	0:0:0:0:0:0:0:1	49178	admin		administrator logged in	
6/2/2017, 7:10:19 PM	0:0:0:0:0:0:0:1	49178			administrator connected	
6/2/2017, 6:45:01 PM				mftserver1	service started	WebDAV
6/2/2017, 6:45:01 PM				mftserver1	service started	HTTP
6/2/2017, 6:45:00 PM				mftserver1	service started	SFTP, host=0.0.0.0, port=22
6/2/2017, 6:45:00 PM				mftserver1	service started	AS2

10 Page 1 of 46 Displaying 1 to 10 of 452 items

Settings

Clear records older than N days - If enabled log records older than N days will be automatically purged from database.

Records

Date - The date/time the action occurred.

Client Host - The client IP address of the administrator.

Client Port - The client port of the administrator.

User - The user login of the administrator.

Domain - The domain affected by this change.

Action - The action that occurred.

Description - A description of the action that occurred.

Purge

Performs a purge of all administrative records.

Export

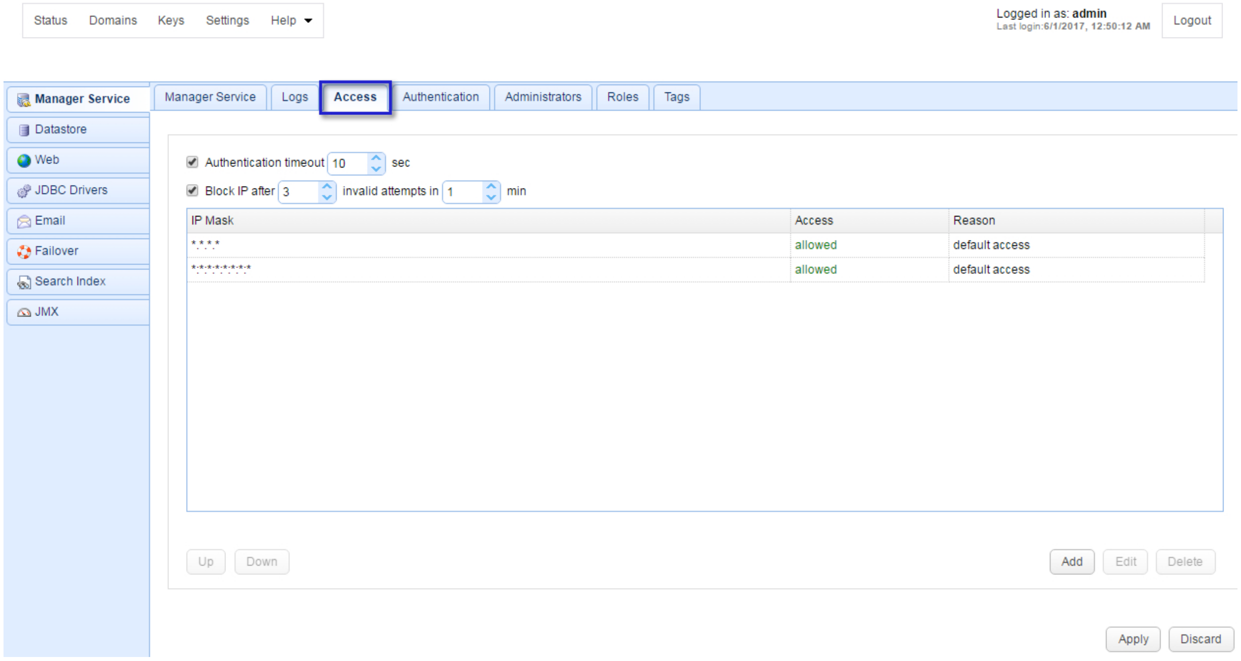
Exports all administrative records to a CSV file.

Restricting administrative access by IP

Administrative access may be restricted by client IP. This is recommended in high security environments where administrators may connect only from known client IP addresses. By default JSCAPE MFT Server allows administrators to connect from ANY client IP address.

[IP mask examples](#)

Figure 107



☑ Authentication timeout 10 sec

☑ Block IP after 3 invalid attempts in 1 min

IP Mask	Access	Reason
..*.*	allowed	default access
::*:*:*:*:*:*	allowed	default access

Authentication timeout - The amount of time in seconds that administrative service client may remain connected without authenticating.

Block IP after - Blocks a client IP address after X invalid authentication attempts within Y minutes.

As an improved security measure you may define what IP addresses are allowed or disallowed access to access the administrative service.

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.

Setting authentication preferences

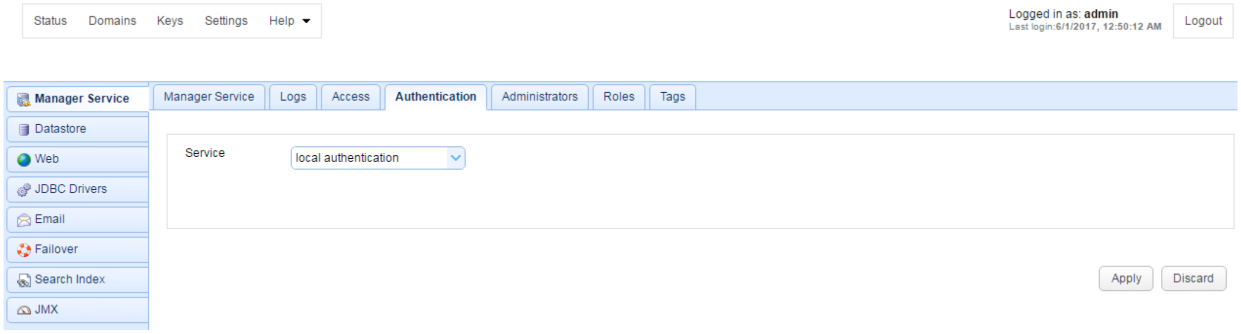
Administrators may authenticate with JSCAPE MFT Server using a variety of different authentication protocols. To view the current authentication method used go to `Settings > Manager Service > Authentication`.

Local Authentication
Database Authentication
Database Query Authentication
LDAP Authentication
LDAP Query Authentication
LDAP Filter Grammar
NTLM Authentication
PAM Authentication
RADIUS Authentication
Custom Authentication

Local Authentication

`Local Authentication` is the most basic form of authentication, authenticating against local administrative accounts created using JSCAPE MFT Server Manager.

Figure 213

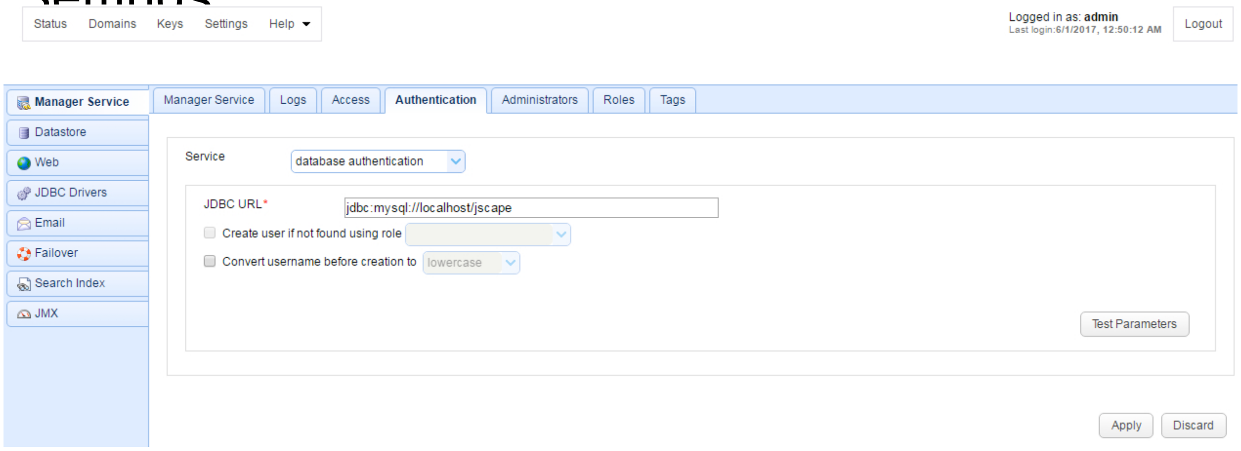


Service: local authentication

Database Authentication

`Database Authentication` allows you to authenticate an administrator based on whether the user has credentials to connect to a database. When connecting to the supplied JDBC URL the username and password provided at time of login are used to login to the JDBC URL. If user authenticates successfully with the JDBC URL then user is considered a valid administrator of the JSCAPE MFT Server service.

Figure 214



Service: database authentication

JDBC URL*: jdbc:mysql://localhost/jscape

□ Create user if not found using role

□ Convert username before creation to: lowercase

JDBC URL - The JDBC URL used to connect to the database. Libraries for JDBC drivers must be placed in the `libs/jdbc` directory of your JSCAPE MFT Server installation, the JSCAPE MFT Server Service restarted and the JDBC driver class registered in `Settings > JDBC Drivers` in order for the database to be accessible to JSCAPE MFT Server.

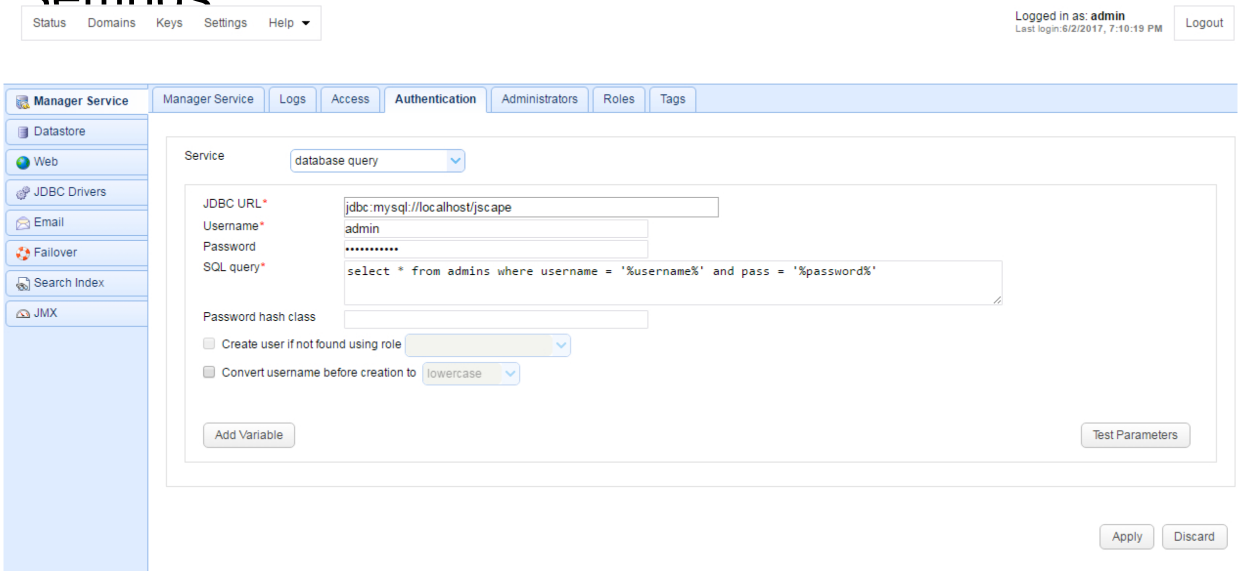
Create user if not found using role - This allows for administrative accounts to be created automatically upon successful authentication. If selected, an administrator will be created automatically (if it does not exist already) using the specified Role.

Convert username before creation to - If enabled, the username supplied will be converted to specified case prior to creation.

Database Query Authentication

`Database Query Authentication` allows you to authenticate an administrator based on the results of a database query. If one or more records are returned from the query then the administrator is successfully authenticated.

Figure 215



Service: database query

JDBC URL*: jdbc:mysql://localhost/jscape

Username*: admin

Password: •••••••••••

SQL query*:

```
select * from admins where username = '%username%' and pass = '%password%'
```

Password hash class:

□ Create user if not found using role

□ Convert username before creation to lowercase

JDBC URL - The JDBC URL used to connect to the database. Libraries for JDBC drivers must be placed in the `libs/jdbc` directory of your JSCAPE MFT Server installation, the JSCAPE MFT Server Service restarted and the JDBC driver class registered in `Settings > JDBC Drivers` in order for the database to be accessible to JSCAPE MFT Server

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

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

SQL query - The query to perform to authenticate the user. There are two special variables that may be used when performing the database query `%username%` and `%password%` which refer the username and password passed in during the authentication process. Note, SQL queries and stored procedures may be used, however stored procedures which make use of output parameters **may not** be used. The variables `%username%` and `%password%` are treated as strings so **must** be enclosed in single quotes.

Password hash class - The Java class to use for hashing password before passing to `SQL query`. If no class is specified then password will be passed to `SQL query` in clear text.

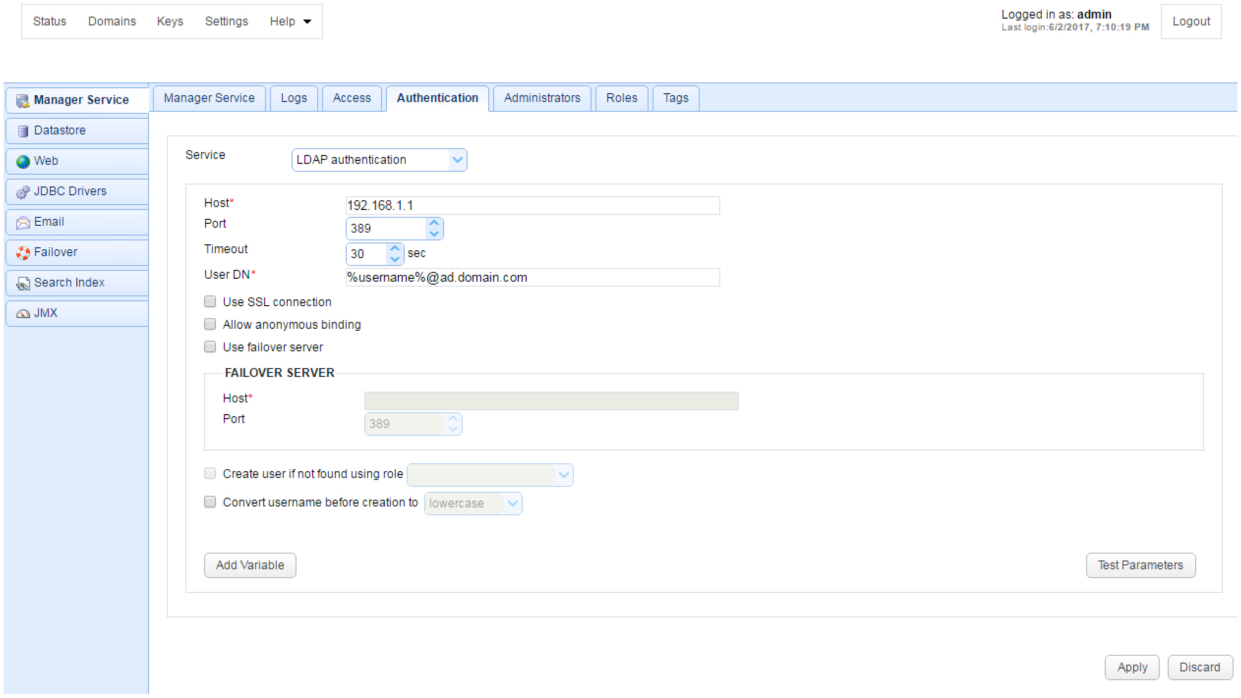
Create user if not found using role - This allows for administrators to be created automatically upon successful authentication. If selected, an administrator will be created automatically (if it does not exist already) using the specified Role.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to SQL query and Role.

LDAP Authentication

`LDAP User Authentication` allows you to authenticate an administrator based on whether the user has the credentials to connect to the LDAP or Active Directory service.

Figure 217



Service: LDAP authentication

Host*: 192.168.1.1

Port: 389

Timeout: 30 sec

User DN*: %username%@ad.domain.com

☐ Use SSL connection

☐ Allow anonymous binding

☐ Use failover server

FAILOVER SERVER

Host*:

Port: 389

☐ Create user if not found using role

☐ Convert username before creation to lowercase

Host - The hostname or IP address of the LDAP service.

Port - The port of the LDAP service.

Timeout - The connection timeout when connecting to LDAP service.

User DN - The users distinguished name for authenticating with the LDAP service. The variable `%username%` may be used which refers to the username passed in during the authentication process.

Use SSL connection - Connect to LDAP server using SSL connection.

Allow anonymous binding - Sets whether user can bind anonymously to LDAP directory.

Use failover server - If enabled and primary LDAP server is inaccessible then authentication will be attempted against failover server.

Create user if not found using role - This allows for administrative accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified Role.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified Role.

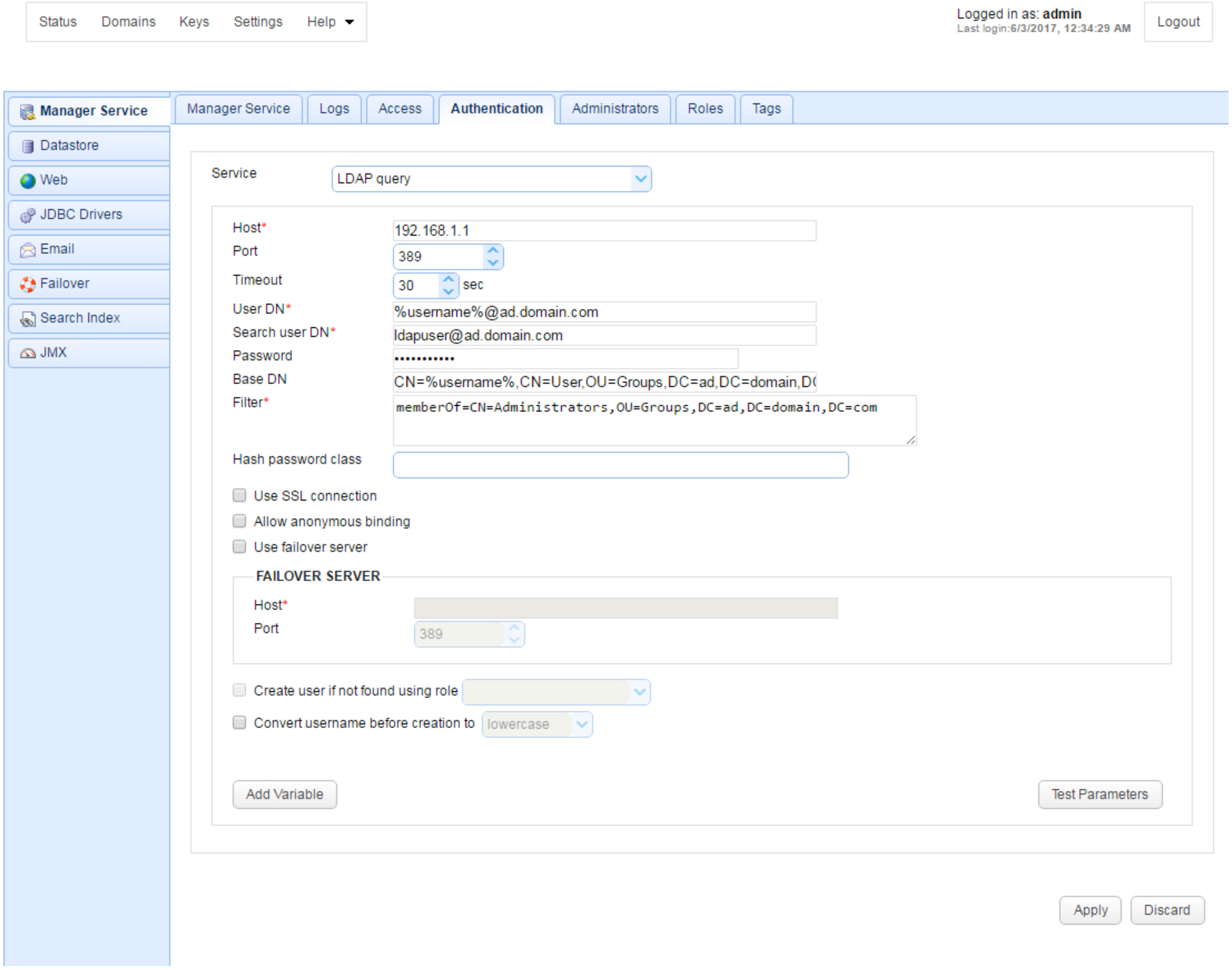
LDAP Query Authentication

`LDAP Query Authentication` allows you to authenticate an administrator user based on the results of a LDAP query and is a two step authentication process.

1. User is authenticated against LDAP server using the `User DN` field and the password supplied by user when authenticating against JSCAPE MFT Server file transfer service.
2. Query is performed using credentials supplied in `Search user DN` and `Password` fields. Note, these credentials **may** be different than the credentials used in Step 1. For example, a case where these might be different is where the `User DN` does not have the needed permissions to perform the query but the `Search User DN` does.

If one or more records are returned from the query then the user is successfully authenticated.

Figure 218



Service: LDAP query

Host*: 192.168.1.1

Port: 389

Timeout: 30 sec

User DN*: %username%@ad.domain.com

Search user DN*: ldapuser@ad.domain.com

Password: ••••••••••

Base DN: CN=%username%,CN=User,OU=Groups,DC=ad,DC=domain,D(

Filter*: `memberOf=CN=Administrators,OU=Groups,DC=ad,DC=domain,DC=com`

Hash password class:

☐ Use SSL connection

☐ Allow anonymous binding

☐ Use failover server

FAILOVER SERVER

Host*:

Port: 389

☐ Create user if not found using role

☐ Convert username before creation to lowercase

Host - The hostname or IP address of the LDAP service.

Port - The port of the LDAP service.

Timeout - The connection timeout when connecting to LDAP service.

User DN - The users distinguished name for authenticating with the LDAP service.

Search user DN - The user distinguished name used for performing LDAP search query.

Password - The user password for performing LDAP search query.

Base DN - The base distinguished name in which to perform the filter.

Filter - The filter to execute using the LDAP filter syntax. There are two special variables that may be used when performing the database query, `%username%` and `%password%` which refer the username and password supplied by the user during the authentication process.

Hash password class - The Java class to use for hashing password before passing to filter. If no class is specified then password will be passed to `Filter` in clear text.

Use SSL connection - Connect to LDAP server using SSL connection.

Use failover server - If enabled and primary LDAP server is inaccessible then authentication will be attempted against failover server.

Create user if not found using role - This allows for administrative users to be created automatically upon successful authentication. If selected, an administrative account will be created automatically (if it does not exist already) using the specified Role.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified Role.

See also

Password Hashing

LDAP Filter Grammar

When using `LDAP Query Authentication` you must define a filter that will be used to identify the record you are searching for. The syntax of LDAP filters are defined in RFC 2254. The table below provides a list of valid expressions and their meanings.

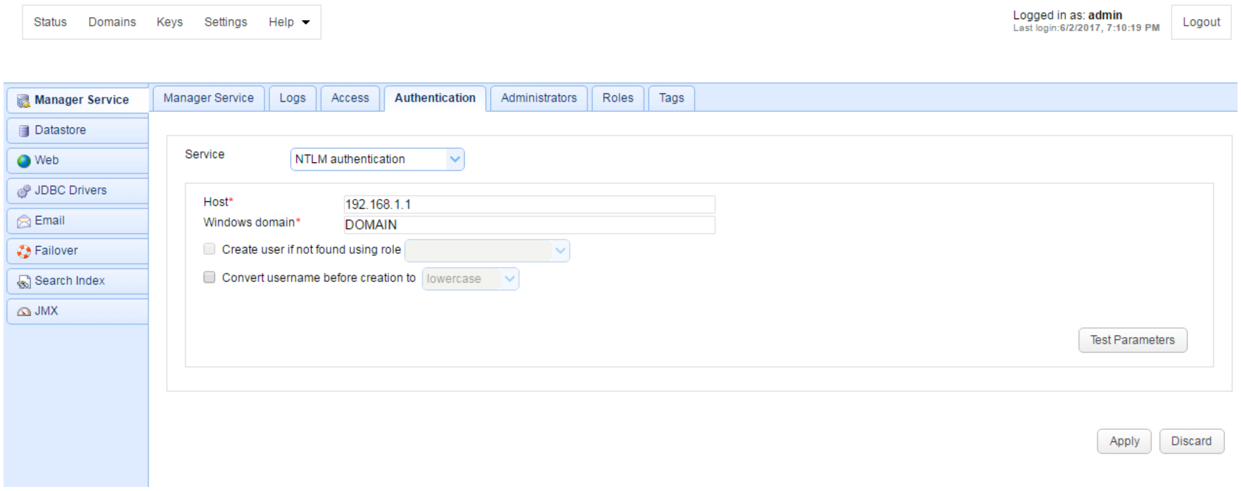
Symbol	Filter	Example	Example matches
=	Equality	(sn=Smith)	Surname of Smith only.
>	Greater than	(sn>Smith)	Any surname that alphabetically follows Smith.
>=	Greater than or equal to	(sn>=Smith)	Any surname that includes or alphabetically follows Smith.
<	Less than	(sn<Smith)	Any surname that alphabetically precedes Smith.
<=	Less than or equal to	(sn<=Smith)	Any surname that includes or alphabetically precedes Smith.
=*	Presence	(sn=*)	All surnames (all entries

			with the sn attribute).
=*	Substring	(sn=Smi*)	Any matching substring of Smith.
&	And	(& (sn=Smith) (cn=John))	Surname of Smith and common name of John.
|	Or	(| (sn=Smith) (sn=Jones))	Surname of Smith or Jones.
!	Not	(! (sn=Smith))	Surname not equal to Smith.

NTLM Authentication

Using `NTLM Authentication` you may authenticate against an existing Windows domain.

Figure 219



Service: NTLM authentication

Host*: 192.168.1.1

Windows domain*: DOMAIN

□ Create user if not found using role

□ Convert username before creation to lowercase

Host - The IP address of Windows domain controller.

Windows domain - The name of the Windows domain to which users belong.

Create user if not found using role - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified Role.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified Role.

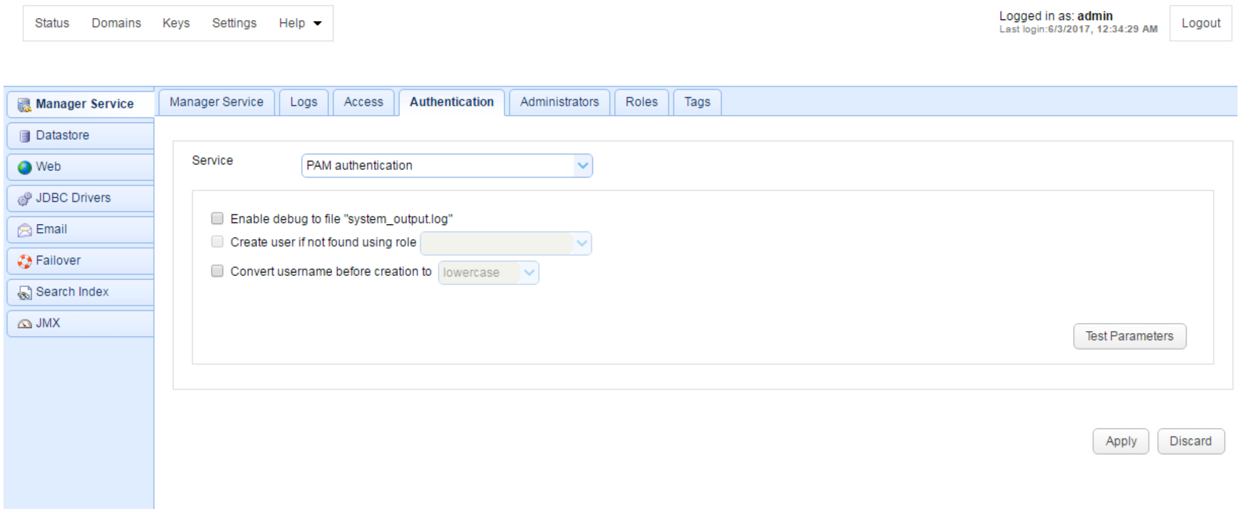
PAM Authentication

Using `PAM Authentication` you may authenticate against an existing UNIX PAM user repository. In order to use the PAM Authentication module you must install some native libraries that allow JSCAPE

MFT Server to communicate with your PAM user repository.

1. Download the JPam library for your operating system.
2. Copy the native library to the Java Native Libary Path. See the Native Library Installation Location table for details.   Note, Step 1 in the JPam instructions should be ignored as the `jpam.jar` file already exists in the `libs` directory of your JSCAPE MFT Server installation. Additionally, JPam instructions state you may optionally place native library in same directory as the `jpam.jar` file instead of the Java Native Library Path. This is incorrect. For JPam to work with JSCAPE MFT Server you **must** place native library in the Java Native Library Path and **not** in the `libs` directory of JSCAPE MFT Server.
3. Configure JPam for use by editing the `net-sf-jpam` file and copying it to to `/etc/pam.d` directory.
4. Restart JSCAPE MFT Server Service.
5. Using JSCAPE MFT Server Manager go to the `Authentication` node and set the `Service type` to `PAM authentication` and enable other options. See Figure 220.
6. Click `Test Parameters` button to test.

Figure 220



Service: PAM authentication

☐ Enable debug to file "system_output.log"

☐ Create user if not found using role

☐ Convert username before creation to lowercase

Enable debug to file system_output.log - Sends debugging information to file `system_output.log` in installation directory.

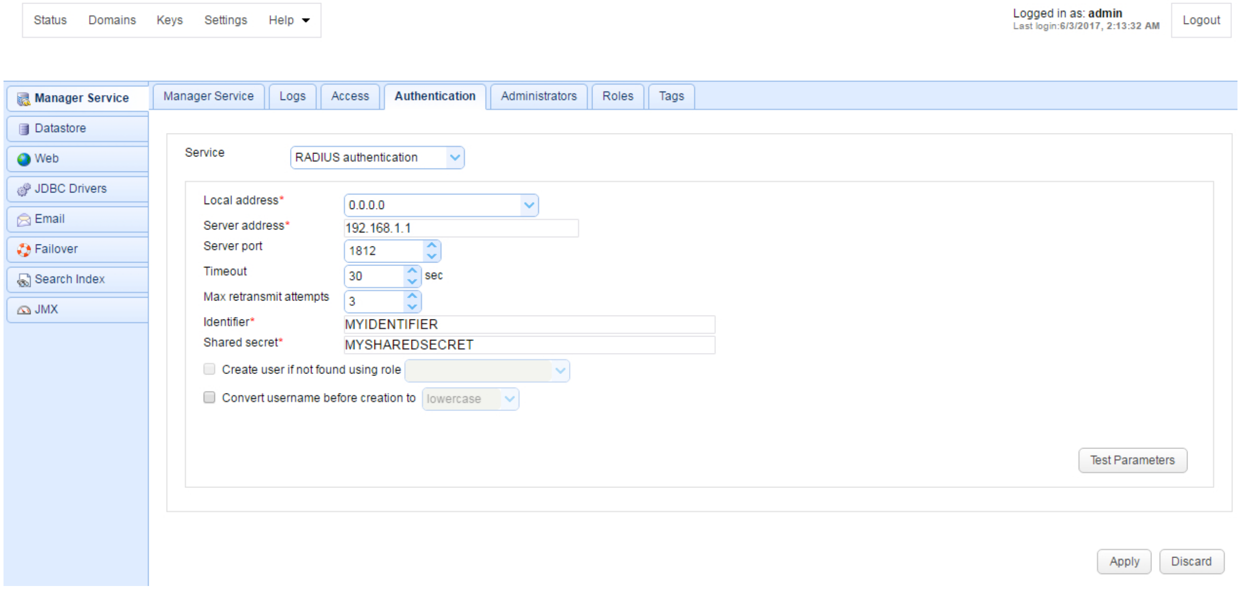
Create user if not found using role - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified Role.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified Role.

RADIUS Authentication

Using `RADIUS authentication` you may authenticate against an existing RADIUS server.

Figure 221



Service: RADIUS authentication

Local address*: 0.0.0.0

Server address*: 192.168.1.1

Server port: 1812

Timeout: 30 sec

Max retransmit attempts: 3

Identifier*: MYIDENTIFIER

Shared secret*: MYSHAREDSECRET

□ Create user if not found using role

□ Convert username before creation to lowercase

Local address - The local UDP address for socket binding.

Server address - The server address of RADIUS server.

Server port - The server port of RADIUS server.

Timeout - The timeout in seconds for connecting to RADIUS server.

Max retransmit attempts - The maximum number of retransmission attempts when there is no response from the RADIUS server

Identifier - The identifier value of the RADIUS server.

Shared secret - The shared secret value of the RADIUS server.

Create account if not found using role - This allows for accounts to be created automatically upon successful authentication. If selected, an account will be created automatically (if it does not exist already) using the specified Role.

Convert username before creation to - If enabled, the username supplied will be converted to specified case before passing username to specified Role.

Custom Authentication

Using `custom authentication` you may define your own custom authentication class. To do so perform the following.

1. Create a class which implements the `com.jscape.inet.mft.subsystems.administrator.authentication.AuthenticationService` class.

2. Overload the `public void authenticate(AuthenticationCredentials creds)` method,

throwing a `com.jscape.inet.mft.subsystems.administrator.authentication.OperationException` exception if authentication fails or returning the username of administrator if authentication passes.

3. Create a JAR file that contains the compiled version of your `com.jscape.inet.mft.subsystems.administrator.authentication.AuthenticationService` implementation. To compile your authentication class you will need to include the `ftpserver.jar` library in your classpath. The `ftpserver.jar` library may be found in the `libs` directory for JSCAPE MFT Server.

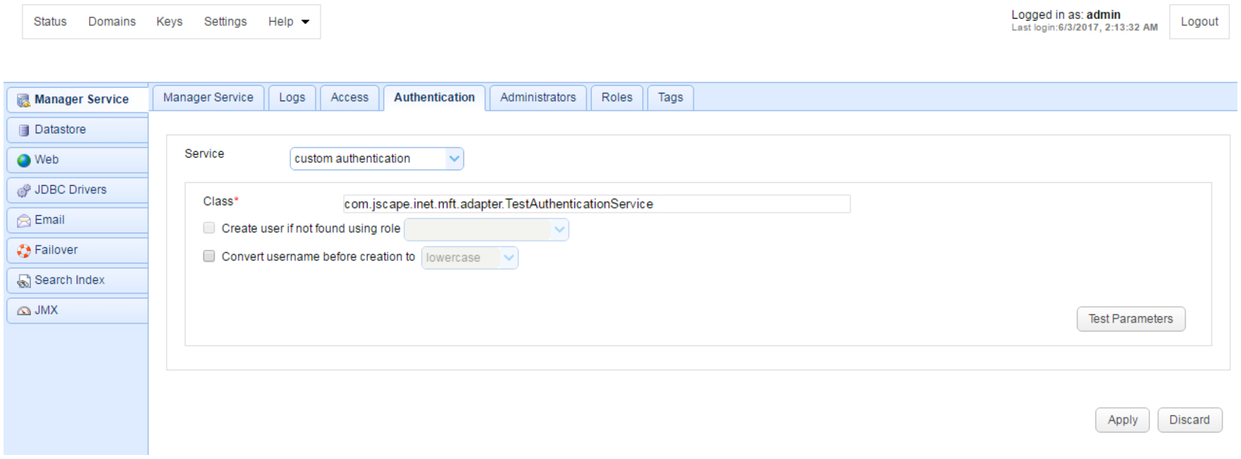
4. Place the JAR file created in Step 3 as well as any needed 3rd party JAR files into the `libs/ext` directory of your JSCAPE MFT Server installation.

5. Restart the JSCAPE MFT Server Service.

6. Open JSCAPE MFT Server Manager and go to `Settings > Manager Service > Authentication` and change the `Service` to `custom authentication` and click `Apply.`

An example implementation `com.jscape.inet.mft.subsystems.administrator.authentication.TestAuthenticationService` is also found in the `ftpserver.jar` file for testing.

Figure 207



Service: custom authentication

Class*: com.jscape.inet.mft.adapter.TestAuthenticationService

□ Create user if not found using role

□ Convert username before creation to lowercase

Example

The following example is taken directly from the `TestAuthenticationService` example provided in `ftpserver.jar` library. There are two exception types that MAY be thrown as part of this example `UnsupportedCredentialsTypeException` and `InvalidCredentialsException`. In the event that `UnsupportedCredentialsTypeException` is thrown JSCAPE MFT Server will pass the credentials up and attempt to validate against local credentials stored within JSCAPE MFT Server instead of using the logic provided in custom authentication class. If `InvalidCredentialsException` is thrown then credentials will not be passed up and user will immediately be denied access.

```
package com.jscape.inet.mft.adapter;

import java.util.Scanner;
```

```
public class TestAuthenticationService
        implements AuthenticationService {

    @Override
    public String authenticate(AuthenticationCredentials credentials)
            throws OperationException {
        if (credentials instanceof PasswordCredentials) {
            return authenticate((PasswordCredentials) credentials);
        } else if (credentials instanceof TokenCredentials) {
            return authenticate((TokenCredentials) credentials);
        }
        throw new UnsupportedCredentialsTypeException(credentials);
    }

    private String authenticate(PasswordCredentials credentials)
            throws OperationException {
        assertPasswordValid(credentials.username, credentials.password, credentials);
        return credentials.username;
    }

    private String authenticate(TokenCredentials credentials)
            throws OperationException {
        try {
            Scanner scanner = new Scanner(credentials.token).useDelimiter(":");
            String username = scanner.next();
            String password = scanner.skip(":").nextLine();

            assertPasswordValid(username, password, credentials);
            return username;

        } catch (InvalidCredentialsException e) {

            throw e;

        } catch (Exception e) {

            throw new InvalidCredentialsException(credentials);

        }

    }


    private void assertPasswordValid(String username, String password, AuthenticationCre

            throws InvalidCredentialsException {

        if (!username.equals(password)) {

            throw new InvalidCredentialsException(credentials);

        }

    }

}
```

Managing administrators

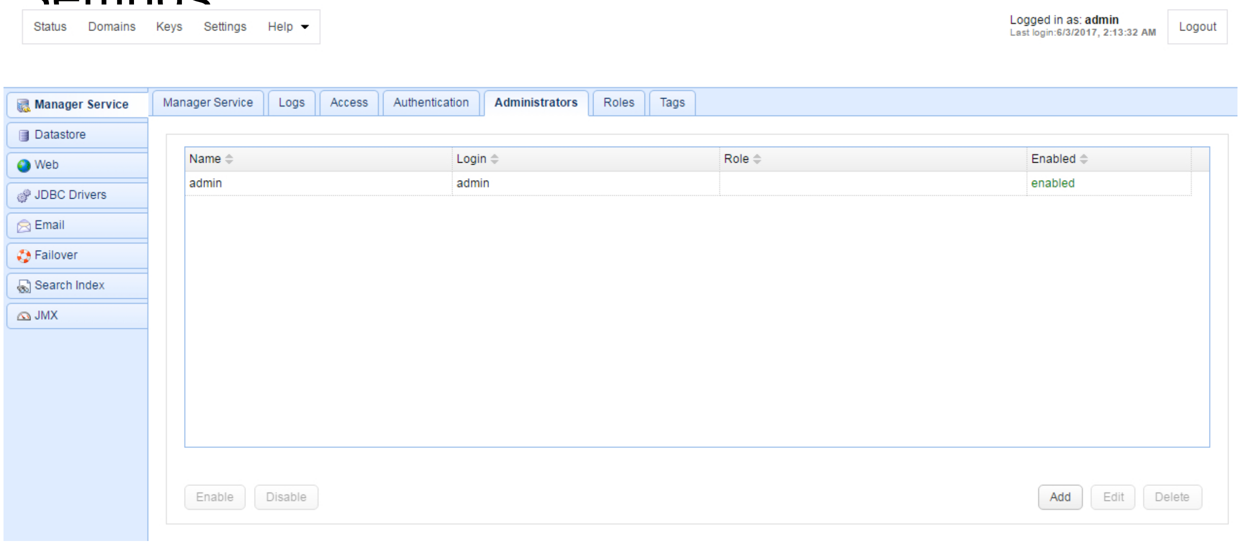
Administrators may be managed from the administrative web interface under the `Administrators` tab.

Adding an administrator

Figure 197

JSCAPE MFT Server Manager Settings

19



Name	Login	Role	Enabled
admin	admin		enabled

Name - The name of this administrator.

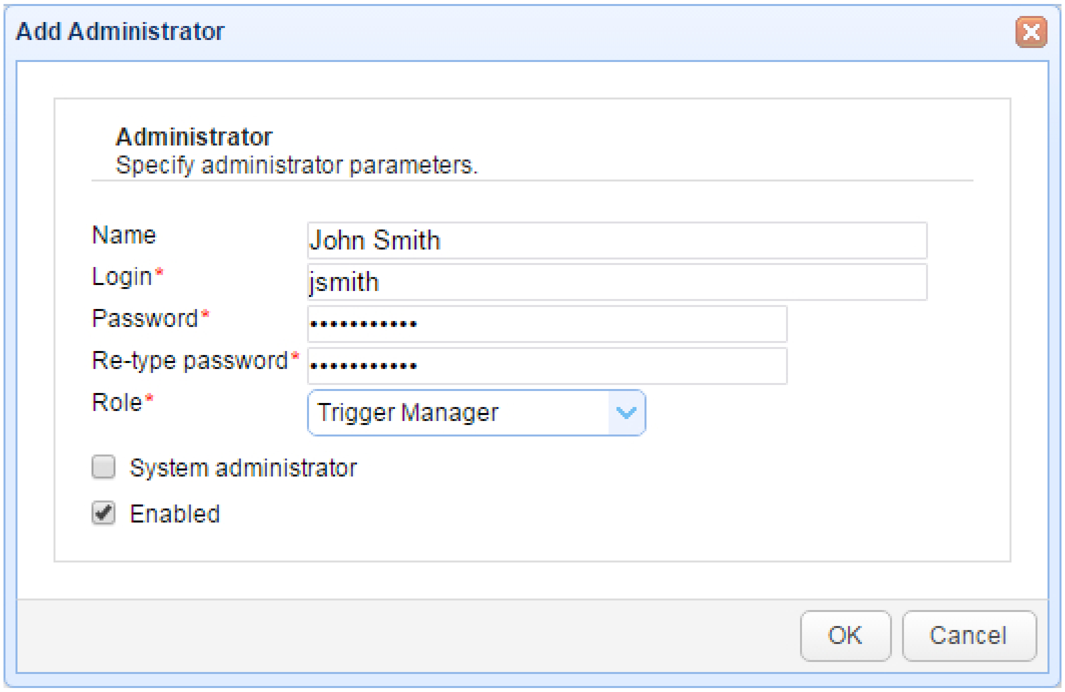
Login - The unique login for this administrator.

Role - The role for this administrator.

Enabled - If this administrator is enabled and may login.

Adding an administrator

Figure 198



Administrator
Specify administrator parameters.

Name: John Smith

Login*: jsmith

Password*: •••••••••••

Re-type password*: •••••••••••

Role*: Trigger Manager

☐ System administrator

☑ Enabled

Name - The name of this administrator.

Login - The unique login for this administrator.

Password - The password for this administrator.

Role - The optional role for this administrator. If no role is selected then user must designated as a `System administrator`.

System administrator - If checked, then administrator will have full unrestricted access.

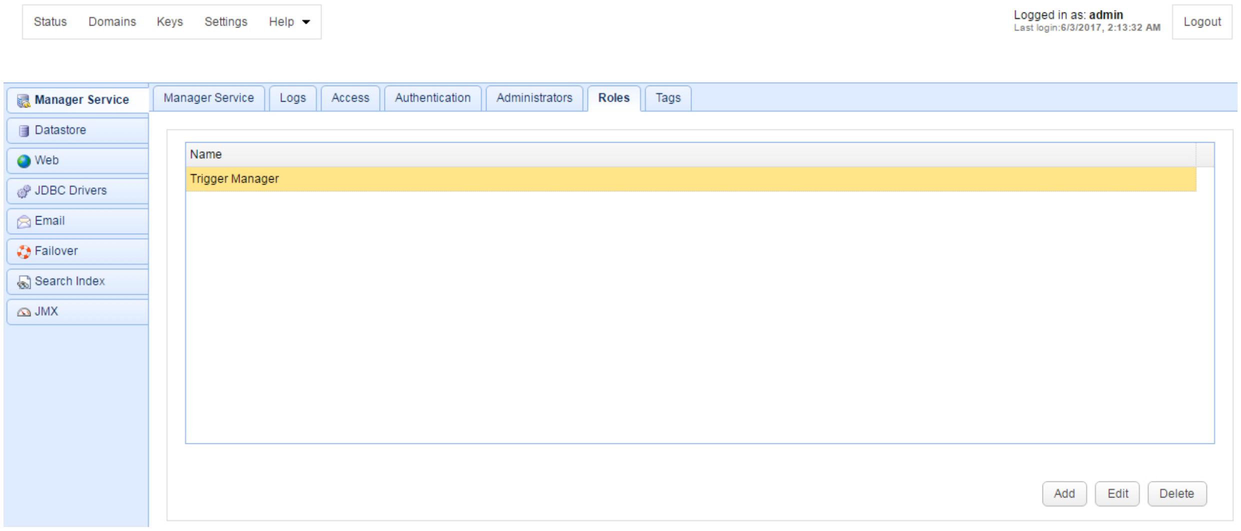
Enabled - If this administrator is enabled and may login.

Managing administrative roles

Administrative roles are a way for you to restrict administrative access to areas of the application using domain, module and tagged data as criteria. For example, you may wish to create an administrative role that allows an administrator to only see Triggers for a specific domain. Another example might be an administrative role that limits the Users that an administrator can see to those tagged users within a specific geographic region. Administrative roles may be managed from the `Roles` tab in the administrative user interface.

Adding administrative roles

Figure 199



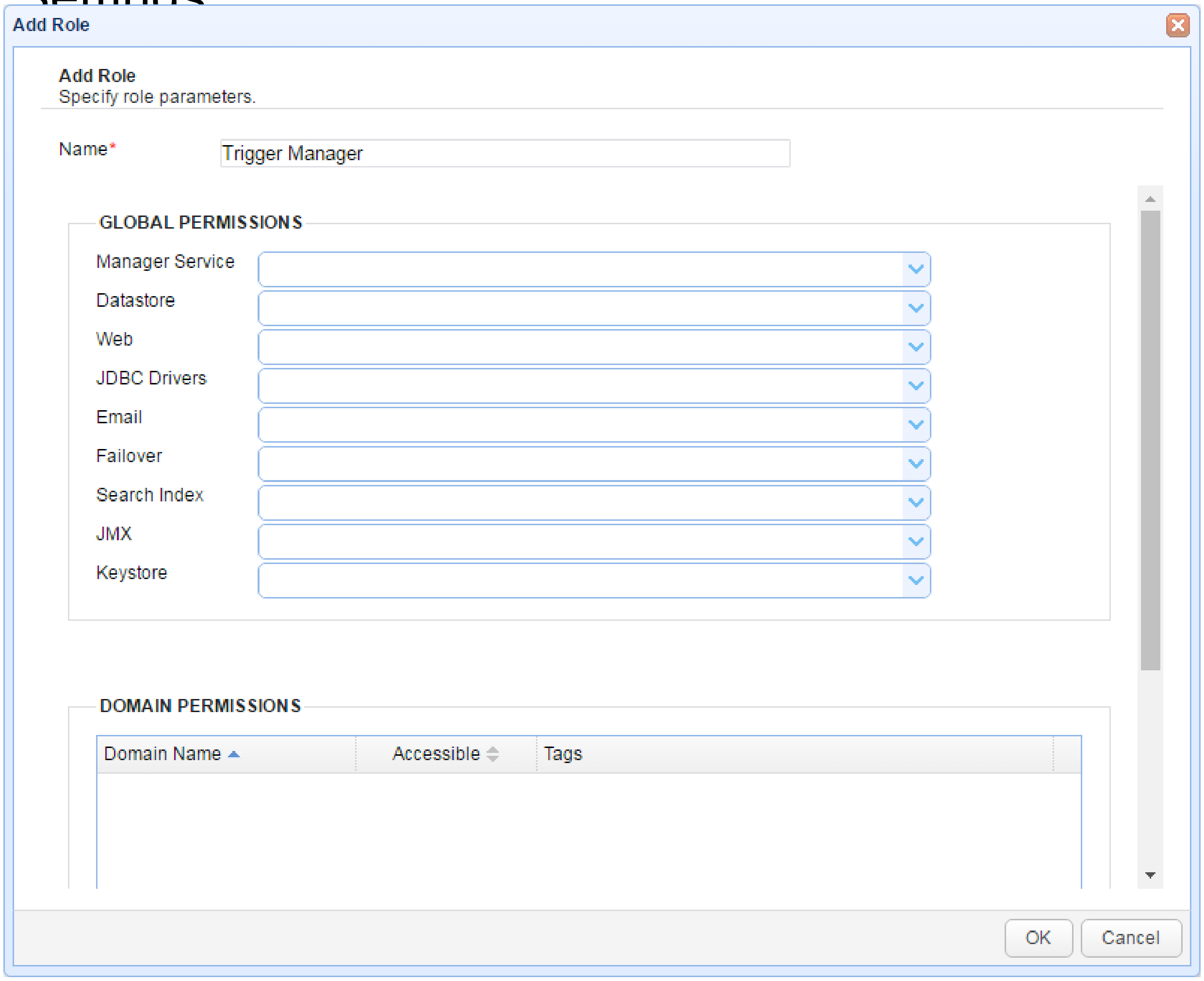
Name
Trigger Manager

Adding administrative roles

To add a Role click on the Add button. The Add Role dialog will be displayed.

Figure 200

19 JSCAPE MFT Server Manager Settings



Add Role

Add Role
Specify role parameters.

Name* Trigger Manager

GLOBAL PERMISSIONS

Manager Service	
Datastore	
Web	
JDBC Drivers	
Email	
Failover	
Search Index	
JMX	
Keystore	

DOMAIN PERMISSIONS

Domain Name	Accessible	Tags

Name - The unique name to assign this role.

Global Permissions

Global permissions are those permissions which are not domain specific.

Manager Service - Defines whether administrators assigned this role can access settings under Settings > Manager Service.

Datastore - Defines whether administrators assigned this role can access settings under Settings > Datastore.

Web - Defines whether administrators assigned this role can access settings under Settings > Web.

JDBC Drivers - Defines whether administrators assigned this role can access settings under Settings > JDBC Drivers.

Email - Defines whether administrators assigned this role can access settings under Settings > Email.

Failover - Defines whether administrators assigned this role can access settings under Settings > Failover.

Search Index - Defines whether administrators assigned this role can access settings under Settings >

Search Index.

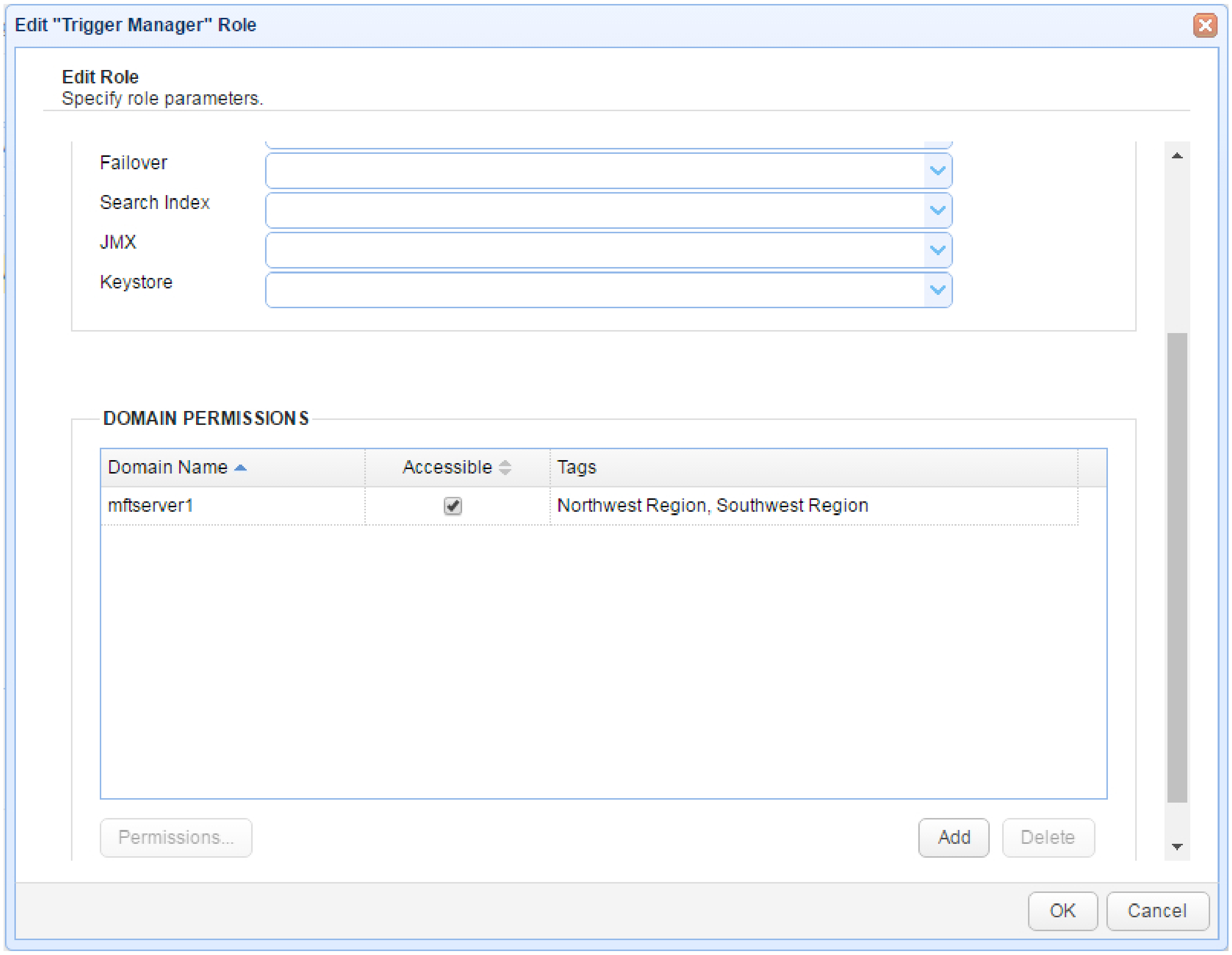
JMX - Defines whether administrators assigned this role can access settings under Settings > JMX.

Keystore - Defines whether administrators assigned this role can access settings under Keys.

Domain Permissions

Domain permissions define those functions that an administrative user can perform for one or more domains. These permissions must be explicitly defined (i.e. if a role is not assigned permissions for a domain then administrative users assigned to that role will not be able to access that domain).

Figure 203



Edit "Trigger Manager" Role

Edit Role
Specify role parameters.

Failover
Search Index
JMX
Keystore

DOMAIN PERMISSIONS

Domain Name ▲	Accessible	Tags
mftserver1	☑	Northwest Region, Southwest Region

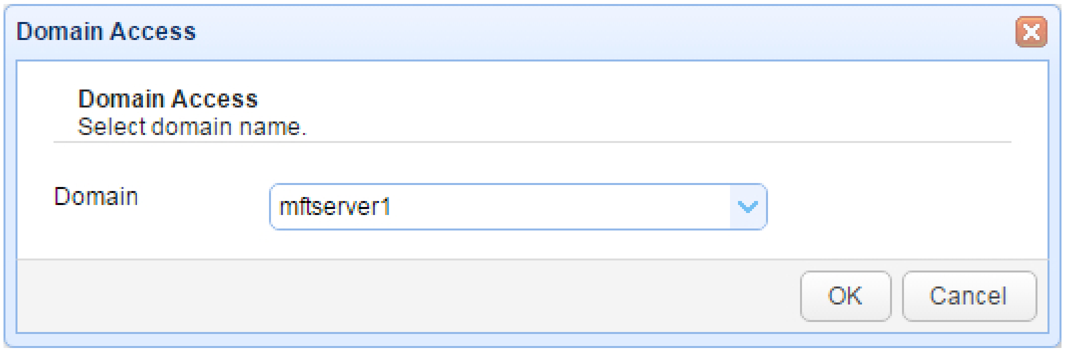
Domain Name - The domain these permissions apply to.

Accessible - Whether or not domain is accessible to role. Default is `false`.

Tags - Optional tags assigned to role. See Managing administrative tags.

To add domain permissions click the `Add` button. The `Domain Access` dialog will then be displayed.

Figure 201



Domain Access

Domain Access
Select domain name.

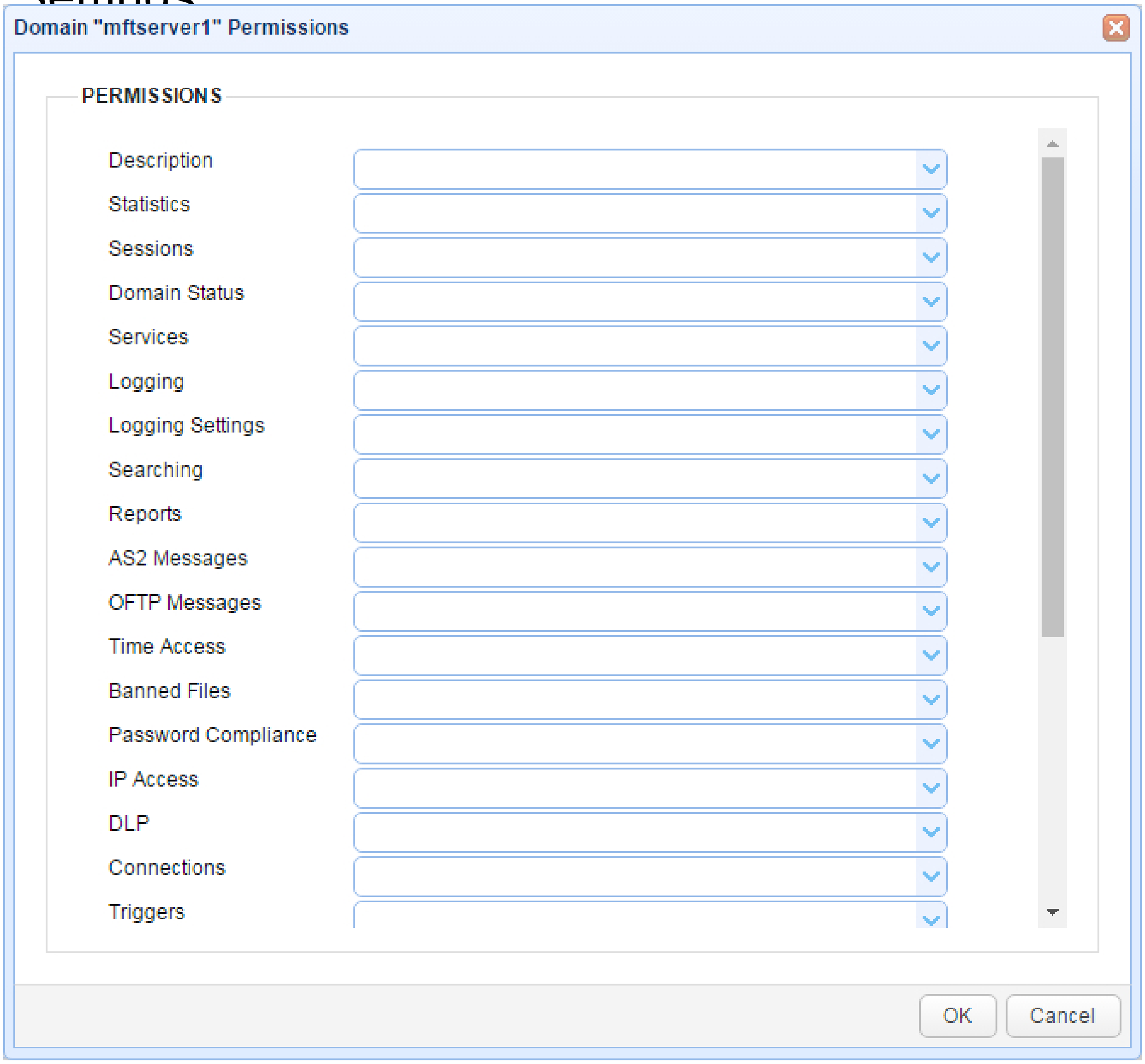
Domain: mftserver1

Domain - The domain to add permissions for.

Once the domain has been added to the role you will then need to define permissions for that domain. To do this select the desired domain and click the `Permissions` button. The `Domain Permissions` dialog will then be displayed.

Figure 202

JSCAPE MFT Server Manager Settings 19



Description - Defines whether role has access to `Description` module for the domain.

Statistics - Defines where role has access to `Statistics` module for the domain.

Sessions - Defines whether role has access to `Sessions` module for the domain.

Domain Status - Defines whether role has ability to change status of the domain (start/stop/pause/resume/restart).

Services - Defines whether role has access to `Services` module for the domain.

Logging - Defines whether role has access to `Logging` module for the domain.

Logging Settings - Defines whether role has access to `Logging > Settings` module for the domain.

Searching - Defines whether role has access to `Logging > Search` module for the domain.

Reports - Defines whether role has access to `Reports` module for the domain.

AS2 Messages - Defines whether role has access to `AS2 Messages` module for the domain.

OFTP Messages - Defines whether role has access to `OFTP Messages` module for the domain.

Time Access - Defines whether role has access to `Time Access` module for the domain.

Banned Files - Defines whether role has access to `Banned Files` module for the domain.

Password Compliance - Defines whether role has access to `Password Compliance` module for the domain.

IP Access - Defines whether role has access to `IP Access` module for the domain.

DLP - Defines whether role has access to `DLP` module for the domain.

Connections - Defines whether role has access to `Connections` module for the domain.

Triggers - Defines whether role has access to `Triggers` module for the domain.

Authentication - Defines whether role has access to `Authentication` module for the domain.

Accounts - Defines whether role has access to `Accounts` module for the domain.

Groups - Defines whether role has access to `Groups` module for the domain.

Reverse Proxies - Defines whether role has access to `Reverse Proxies` module for the domain.

Directory Monitors - Defines whether role has access to `Directory Monitors` module for the domain.

Drop Zones - Defines whether role has access to `Drop Zones` module for the domain.

URL Branding - Defines whether role has access to `URL Branding` module for the domain.

Trading Partners - Defines whether role has access to `Trading Partners` module for the domain.

Contacts - Defines whether role has access to `Contacts` module for the domain.

Managing administrative tags

Administrative tags may be used to restrict the data within a module that an administrative user may have access to. For example, I may need to grant an administrative user access to the Users module but limit their visibility to those users within a specific geographic region. This can be accomplished by creating an administrative Tag, tagging those users in desired region with specified tag, assigning tag to a Role and then assigning role to an administrative user.

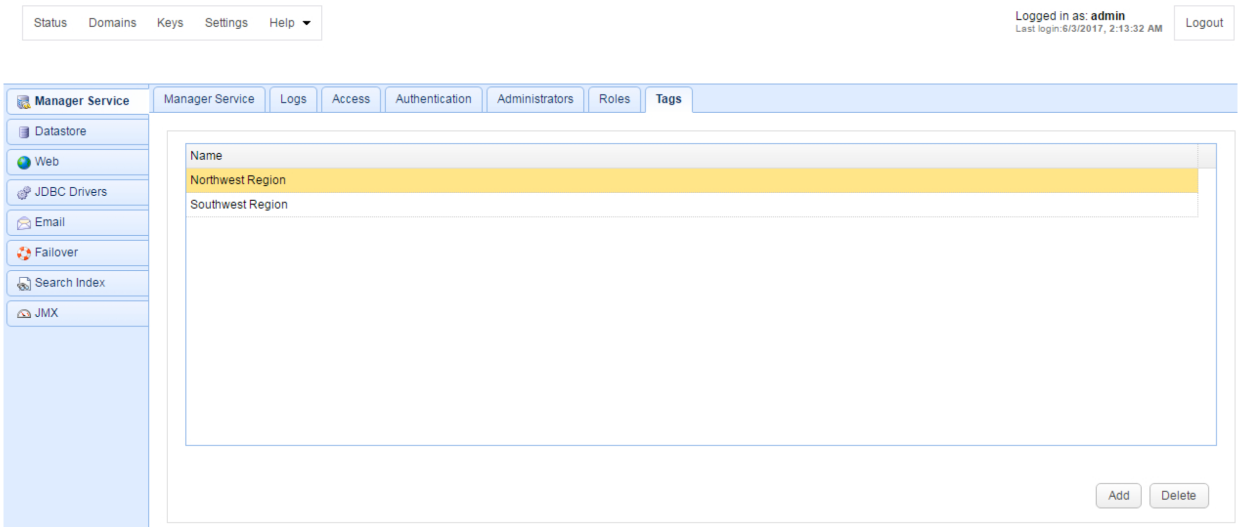
[Creating an administrative tag](#)
[Assigning a tag to a role](#)

Tagging data

Creating an administrative tag

To create an administrative tag go the `Settings > Manager Service > Tags` panel. A list of available tags will be displayed.

Figure 204

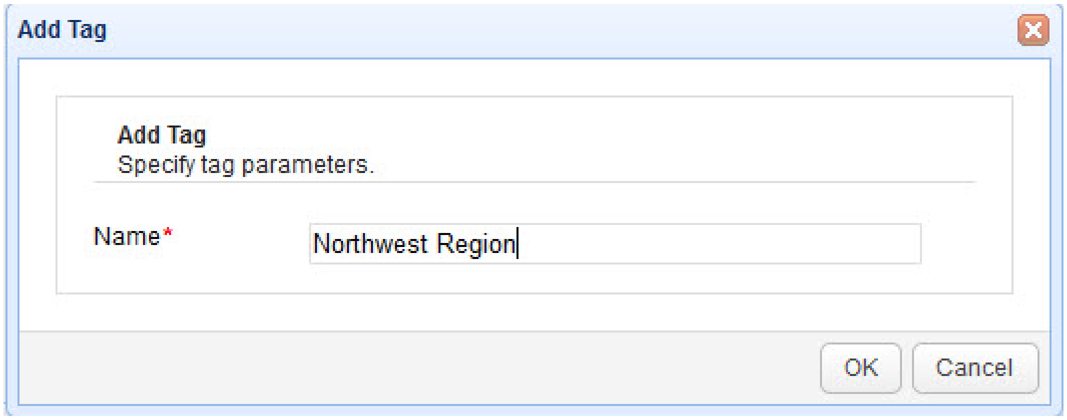


Name
Northwest Region
Southwest Region

Name - The name of the tag.

To create a tag click on the `Add` button. The `Add Tag` dialog will be displayed. Enter a tag name and click `OK`. Once created this tag may be assigned to a Role and used in tagging data.

Figure 205



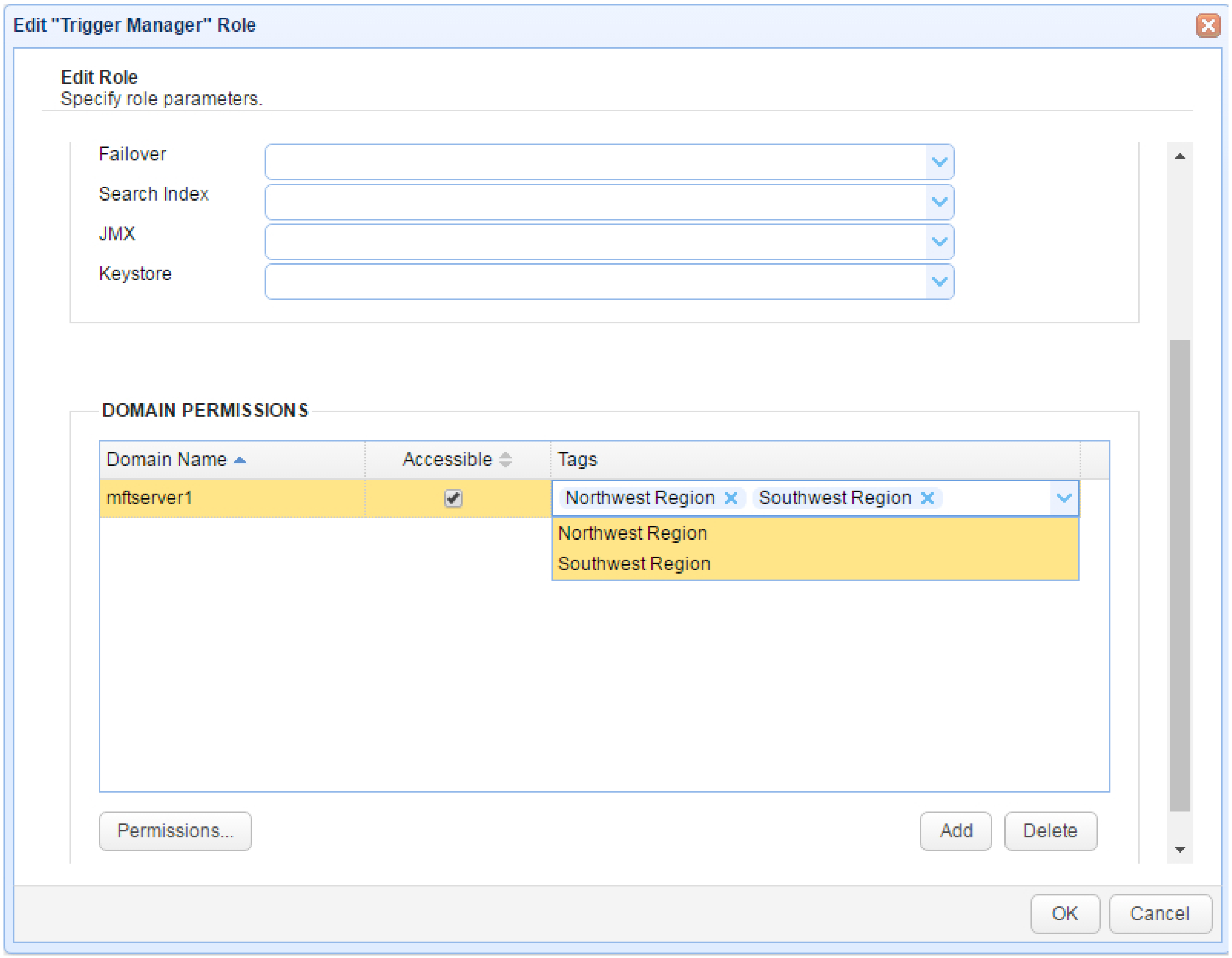
Name* Northwest Region

Name - The unique name to assign this tag.

Assigning a tag to a role

To assign a tag to a role, select the desired role from the `Roles` tab and click the `Edit` button. Scroll to the Domain Permissions section and click on the `Tags` cell for the desired domain. At this point a drop-down of available tags will be displayed. Select the desired tags and click `OK` to save.

Figure 206



Edit "Trigger Manager" Role

Edit Role
Specify role parameters.

Failover
Search Index
JMX
Keystore

DOMAIN PERMISSIONS

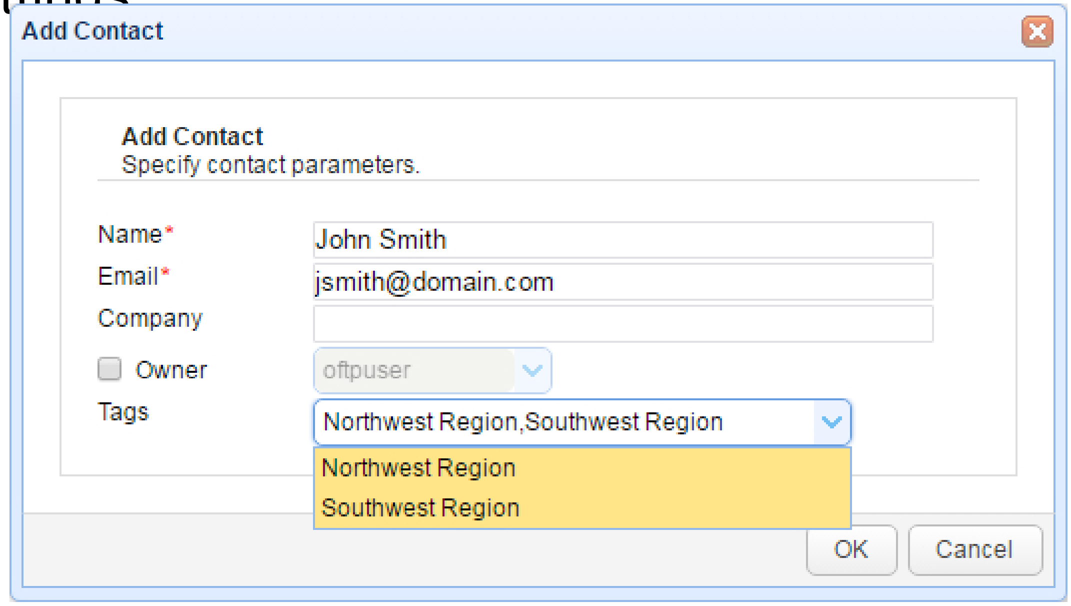
Domain Name	Accessible	Tags
mftserver1	☑	Northwest Region ✕ Southwest Region ✕

Northwest Region
Southwest Region

Tagging data

Many types of data may be tagged. These include Triggers, Users, Groups, Groups, Reverse Proxies, Directory Monitors, Drop Zones, Contacts and more. You may tag an object during creation or while editing an object. The example below demonstrates tagging a Contact with the Tag `Northwest`. This will limit visibility of this Contact to those administrators who are assigned a Role that has a Tag of `Northwest`.

Figure 211



Add Contact

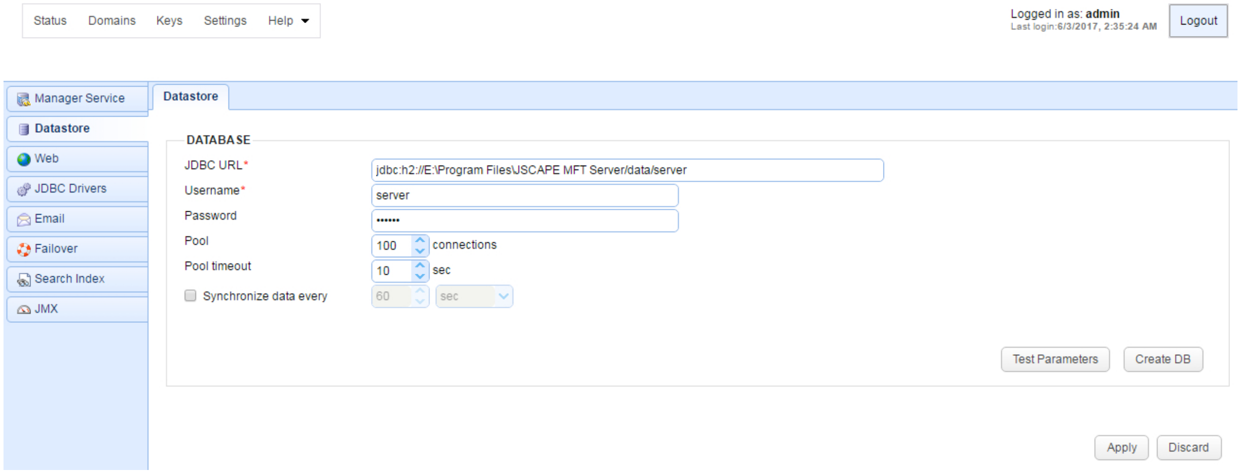
Add Contact
Specify contact parameters.

Name* John Smith
Email* jsmith@domain.com
Company
□ Owner oftpuser
Tags Northwest Region,Southwest Region

Datastore

The Datastore node controls where all configuration settings are stored for JSCAPE MFT Server. All configuration settings are stored in a relational database. By default, a local H2 database is installed with JSCAPE MFT Server for storing this information. You may optionally point this to any ANSI compliant relational database.

Figure 210



Logged in as: **admin**
Last login:6/3/2017, 2:35:24 AM

DATABASE

JDBC URL* jdbc:h2://E:\Program Files\JSCAPE MFT Server/data/server
Username* server
Password ••••••
Pool 100 connections
Pool timeout 10 sec
□ Synchronize data every 60 sec

JDBC URL - The JDBC URL of target database.

Username - The JDBC username of target database.

Password - The JDBC password of target database.

Pool - The number of connections to keep in connection pool for target database.

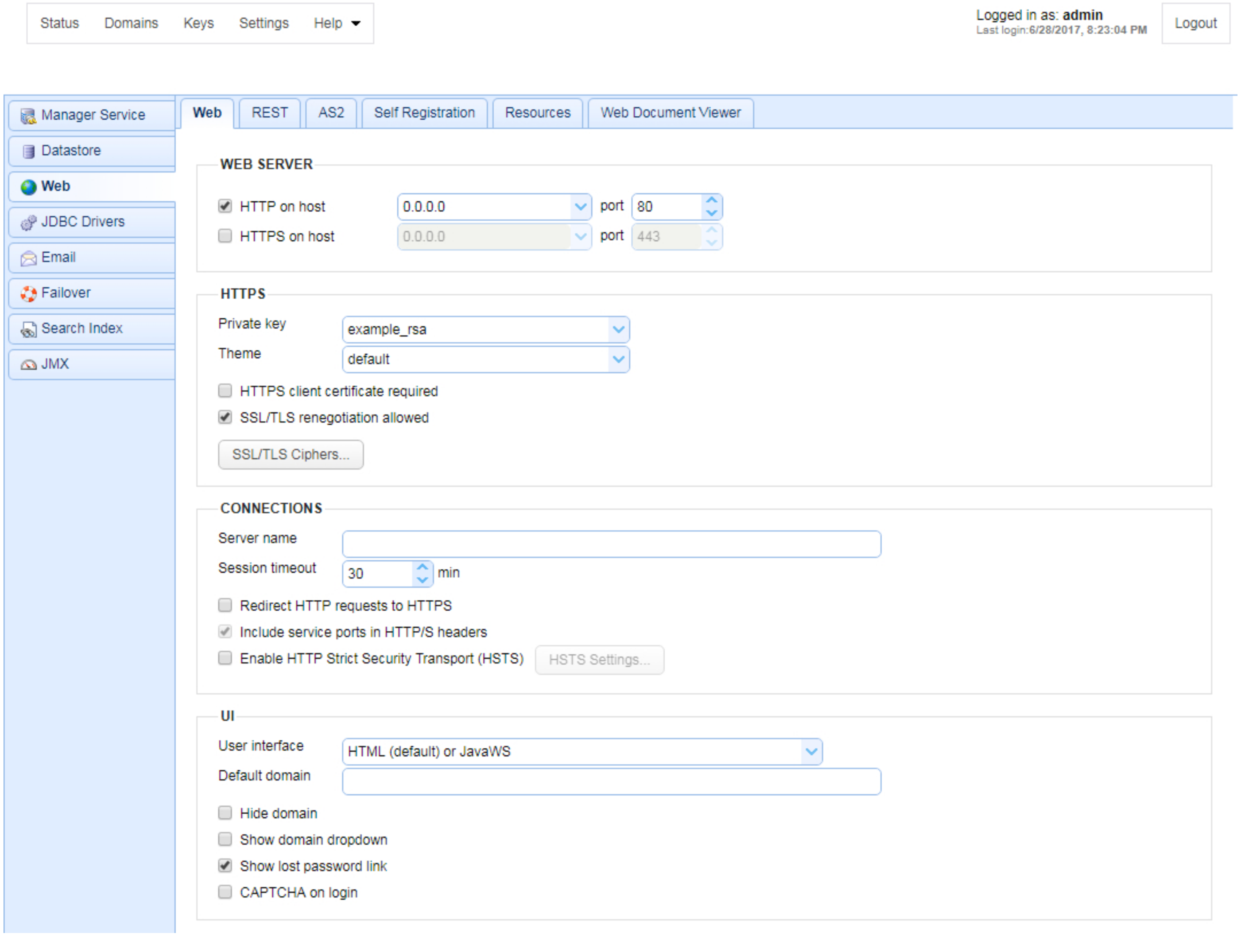
Pool timeout - The amount of inactivity time before expiring a database connection from the pool.

Synchronize data every X (seconds, minutes, hours or days) - Specifies how often GUI data is synchronized with the database. This is normally needed when you have two (2) or more instances of JSCAPE MFT Server connecting to a shared global datastore and you want to specify how often the configuration data on those servers are synchronized.

Web settings

The `Web` node controls whether HTTP/S services are enabled and the ports they are running on. By enabling the HTTP/S service(s) users may use the web based JSCAPE MFT Server Web Client to perform file transfers. All domains share the same HTTP/S service settings.

Figure 19



WEB SERVER

☑ HTTP on host 0.0.0.0 port 80

□ HTTPS on host 0.0.0.0 port 443

HTTPS

Private key: example_rsa

Theme: default

□ HTTPS client certificate required

☑ SSL/TLS renegotiation allowed

CONNECTIONS

Server name:

Session timeout: 30 min

□ Redirect HTTP requests to HTTPS

☑ Include service ports in HTTP/S headers

□ Enable HTTP Strict Security Transport (HSTS)

UI

User interface: HTML (default) or JavaWS

Default domain:

□ Hide domain

□ Show domain dropdown

☑ Show lost password link

□ CAPTCHA on login

Web Server

HTTP on host - The host and port you want to enable HTTP service on. This will also be used for client REST services.

HTTPS on host - The host and port you want to enable HTTPS service on. This will also be used for client REST services.

REST HTTP on host - The host and port you want to enable REST management services on.

REST HTTPS on host - The host and port you want to enable REST management services on.

HTTPS

Private key - The SSL encryption key to be used for HTTPS services.

Theme - The color theme used for the buttons, menus, tabs, and other GUI elements.

HTTPS client certificate required - Requires that client browser successfully identify itself with a client certificate found in "Client keys" section of Key Manager.

SSL/TLS negotiation allowed - If enabled clients will be allowed to renegotiate SSL/TLS sessions.

SSL/TLS Ciphers - List of enabled SSL ciphers for HTTPS communications.

Connections

Server name - Optional value if entered will replace any HTTP headers that contain hostname data with specified hostname. This is useful in cases where server operates behind a NAT enabled firewall and you do not want to leak internal hostname or IP address information.

Session timeout - The amount of time after which to close inactive HTTP/S sessions.

Redirect HTTP requests to HTTPS - Automatically redirects HTTP requests to HTTP.

Include service ports in HTTP/S headers - If enabled, service ports will be included in HTTP/S headers. These may be disabled in cases where HTTP/S services are running on non-standard ports with some sort of port forwarding firewall located in front of server.

Enable HTTP Strict Security Transport (HSTS) - If enabled, HSTS will be enabled.

UI

User interface - Sets what user interface options are available from login page.

Default domain - Defaults domain field to specified value when logging in via web interface.

Hide domain - Hides domain field when logging in via web interface. If this option is checked then a default domain MUST be provided.

Show domain dropdown - If enable a drop-down list of available domains will be shown on login page.

Show lost password link - If enabled the "Lost password" link will be displayed on web interface login page allowing user to reset their password via email.

CAPTCHA on login - If checked, user will be required to enter a CAPTCHA on login.

Self Registration

Show user registration link - If enabled, the user registration link will be displayed on the main login page, allowing users to self-register user accounts.

Use email as login - If enabled, users will not be prompted for a username when self-registering, instead it will use their email address as their login when creating their account.

JSCAPE MFT Server Manager Settings

19

See also

[Web based file transfers]

Email settings

The `Email` node controls whether ad-hoc email transfers are enabled and the SMTP server settings used for sending emails.

See also

[Email transfers]

Failover settings

The `Failover` node controls whether a failover server is defined for this server.

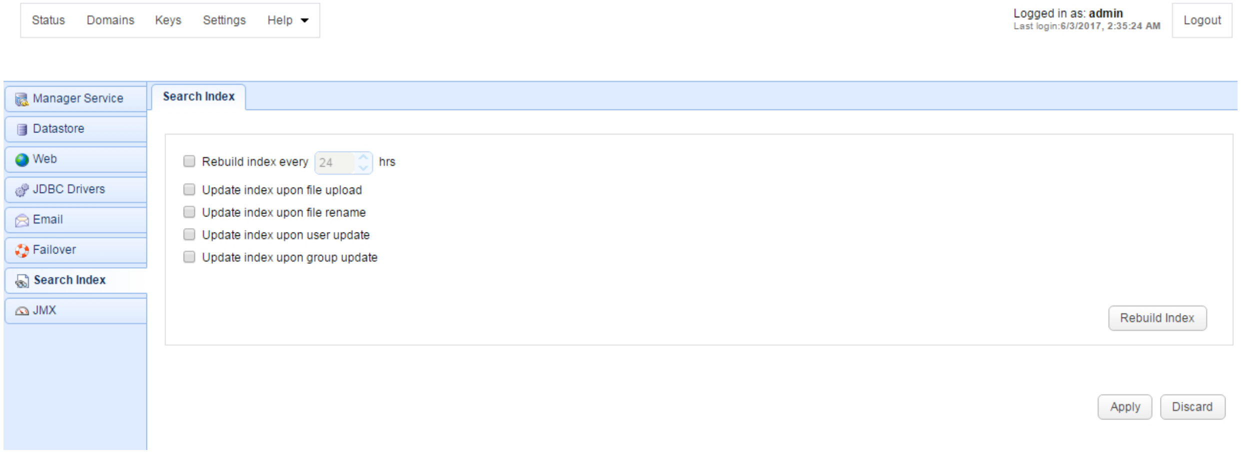
See also

[Defining a failover server]

Search index settings

The `Search Index` node controls whether and how files are indexed for use in performing searches.

Figure 129



□ Rebuild index every 24 hrs
□ Update index upon file upload
□ Update index upon file rename
□ Update index upon user update
□ Update index upon group update

Rebuild index every X hrs - Controls the frequency in which user/group virtual directories flagged for indexing are automatically re-indexed.

Update index upon file upload - If checked, file is automatically indexed upon upload.

Update index upon file rename - If checked, file is automatically re-indexed upon rename or deletion.

Update index upon user update - If checked, virtual directories for account are automatically indexed upon user account update.

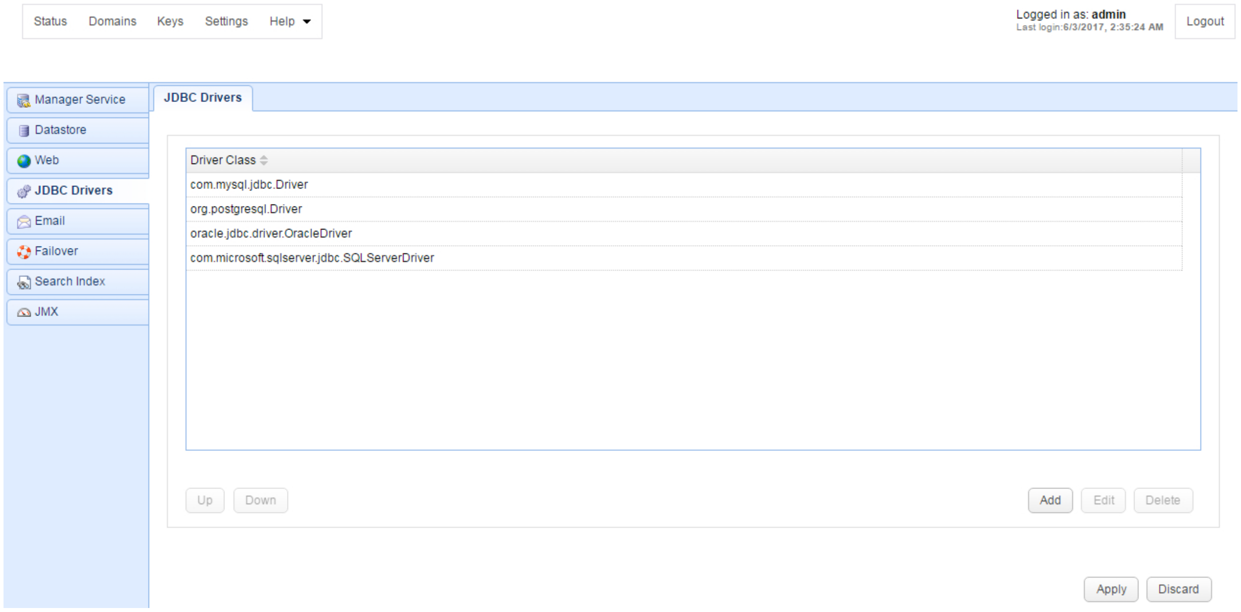
Update index upon group update - If checked, virtual directories for group are automatically indexed upon group update.

JDBC settings

The `JDBC Drivers` node controls what JDBC drivers may be used by JSCAPE MFT Server when storing account and/or log information in a relational database.

JDBC driver downloads
Adding a JDBC driver

Figure 73



Driver Class
com.mysql.jdbc.Driver
org.postgresql.Driver
oracle.jdbc.driver.OracleDriver
com.microsoft.sqlserver.jdbc.SQLServerDriver

JDBC driver downloads

Microsoft SQL Server JDBC Driver
http://msdn.microsoft.com/en-us/sqlserver/aa937724.aspx

Oracle JDBC Driver
http://www.oracle.com/technology/tech/java/sqlj_jdbc/index.html

MySQL JDBC Driver
http://dev.mysql.com/downloads/connector/j/5.1.html

PostgreSQL JDBC Driver

https://jdbc.postgresql.org/

Adding a JDBC driver

Note, drivers for MySQL, Oracle, PostgreSQL, Microsoft SQL Server come pre-installed with JSCAPE MFT Server.

JSCAPE MFT Server Manager Settings

19

1. Place the JDBC driver JAR file in the `libs/jdbc` directory of your JSCAPE MFT Server installation.
2. Shutdown JSCAPE MFT Server Manager and JSCAPE MFT Server Service.
3. Restart JSCAPE MFT Server Manager and JSCAPE MFT Server Service.
4. From JDBC drivers panel click on the `Add` button. When prompted enter the JDBC driver class and press enter.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. The author assumes no responsibility w ith regard to the performance or use of these products. All understandings, agreements, or w arranties, if any, take place directly betw een 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.

This user manual w as created w ith Help & Manual.

Index