MailStore SPE 13

Documentation

15. July 2020

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners.
The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Inhalt

1

Kapitel

Before You Start

1.1 Overview

Architecture

MailStore Service Provider Edition's architecture consists of the following three components:

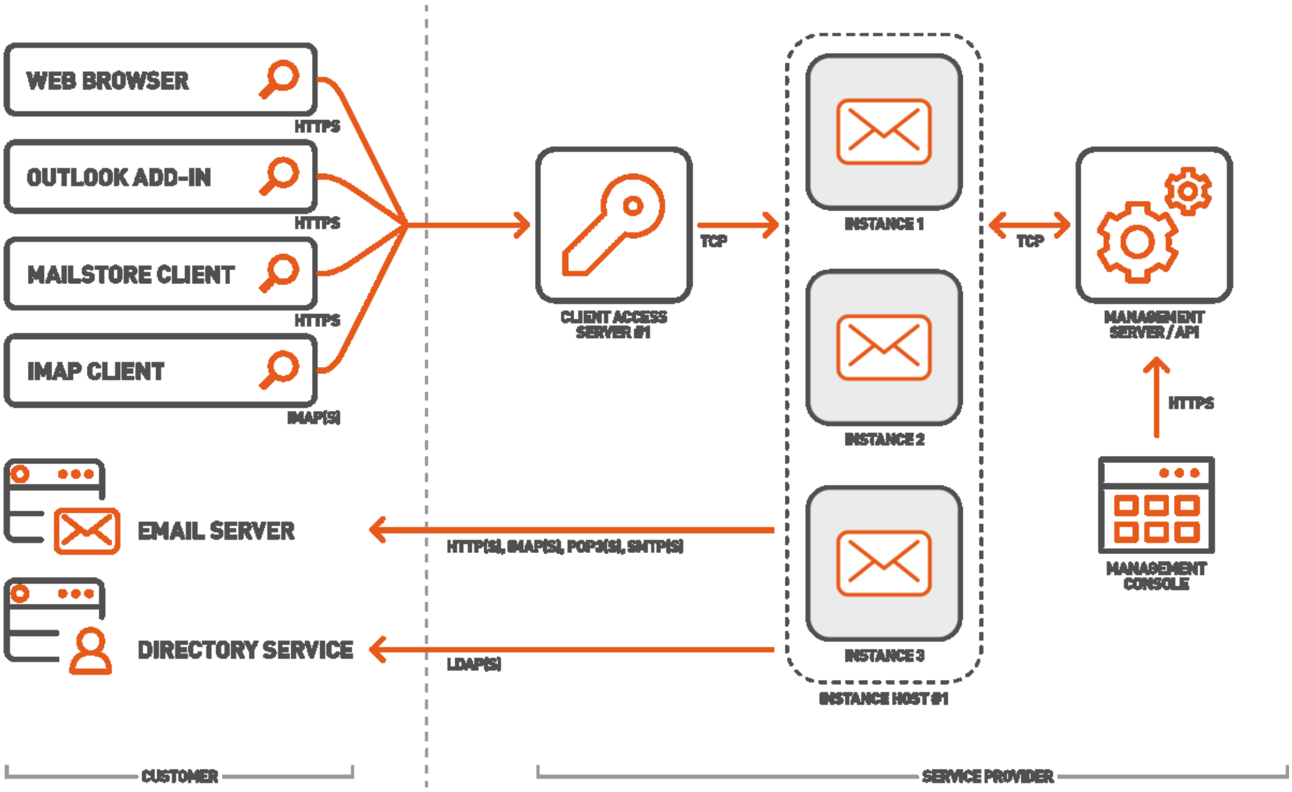
- Management Server
- Instance Host
- Client Access Server

As the name already points out the Management Server is used to manage and monitor all components of the MailStore Service Provider Edition centrally.

Instance Hosts are responsible for operation of the archive instances, whereby the number of possible instances is practically unlimited if there are enough Instance Hosts. Instances directly access email server for archiving and directory services for synchronizing and authenticating users.

End customers can access their own archive instances through a Client Access Server. By using multiple client access servers load-balancing as well as security concepts can be implemented effectively.

The graphic below provides an overview of the whole MailStore Service Provider Edition architecture with all its components and communication channels.



Scenarios

Due to its modular design MailStore Service Provider Edition is suitable for implementing virtually any imaginable scenario.

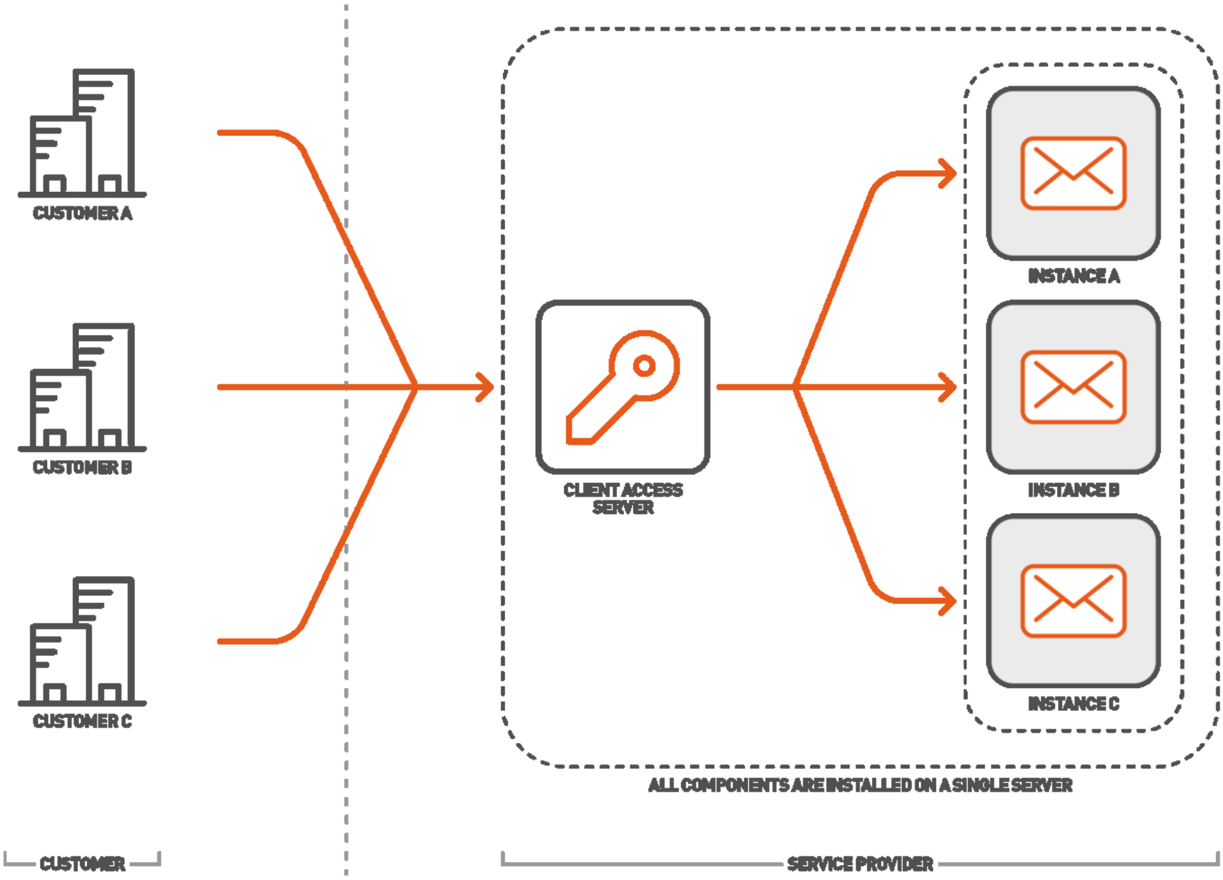
Smaller service provider with a limited number of customers are able to provide hosted email archiving on just one physical or virtual server by setting up MailStore Service Provider Edition in single server mode, whereas service providers with a large number of customers will find a scalable solution by setting up MailStore Service Provider Edition in multi server mode.

No matter how MailStore Service Provider Edition was initially set up, it is always possible to change modes by adding or removing Instance Hosts and Client Access Servers.

Find further information about three typical setups in the following.

Single Server Mode

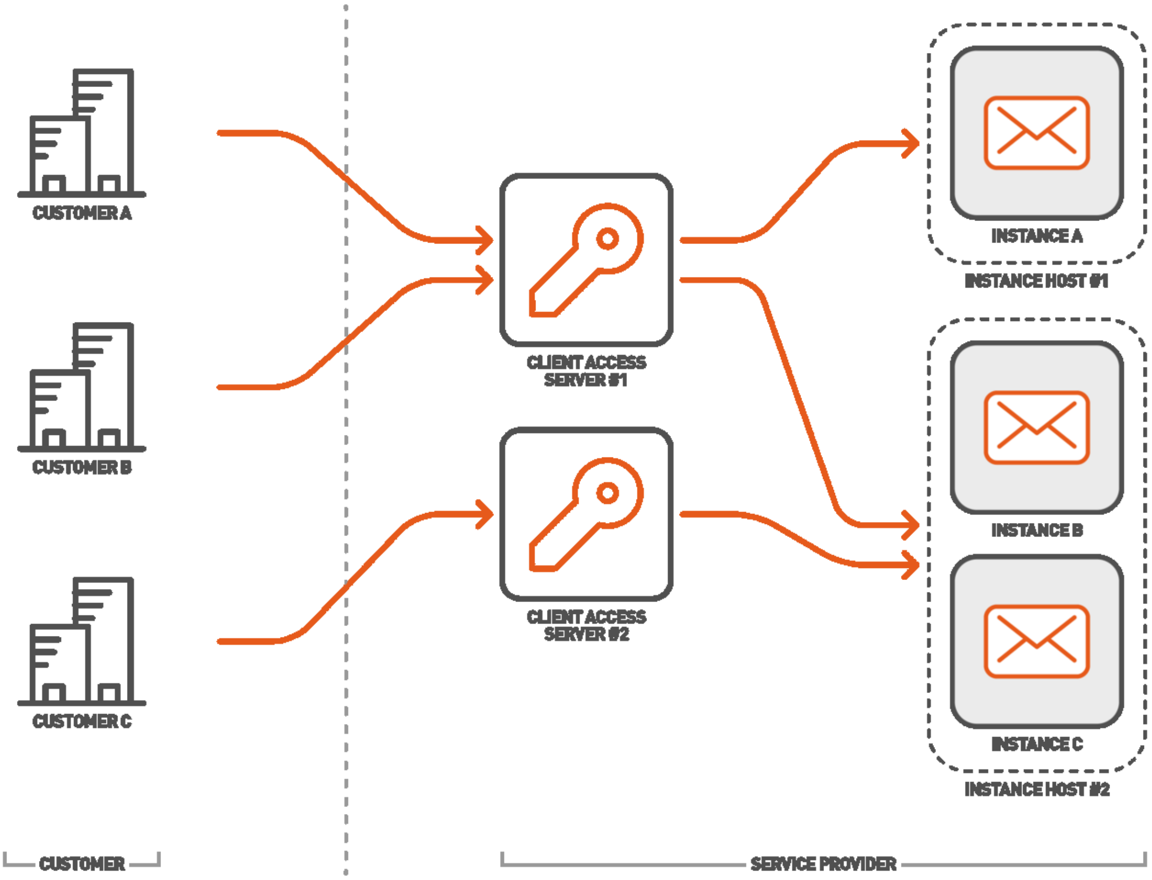
The simplest way to setup MailStore Service Provider Edition is a single server mode setup. In that type of setup the Management Server, Instance Host and Client Access Server roles are installed on a single virtual or physical server as shown in the graphic below.



This setup is suitable for smaller service providers with a limited number of customers and end users. If the number of customers increases or the server no longer has enough available resources, further Instance Host and Client Access Server can be added at any time, which will change the setup over to a typical multi server mode setup as described below.

Multi Server Mode

In opposite to a single server mode setup the different roles are distributed among several servers. This allows to achieve a scalable and highly available setup of MailStore Service Provider Edition.



For accessing instances it does not matter to which Client Access Server a user connects. Upon each new incoming connection the Client Access Server requests information about the Instance Host on which the user's instance is running from the the Management Server.

Virtual Private Clouds

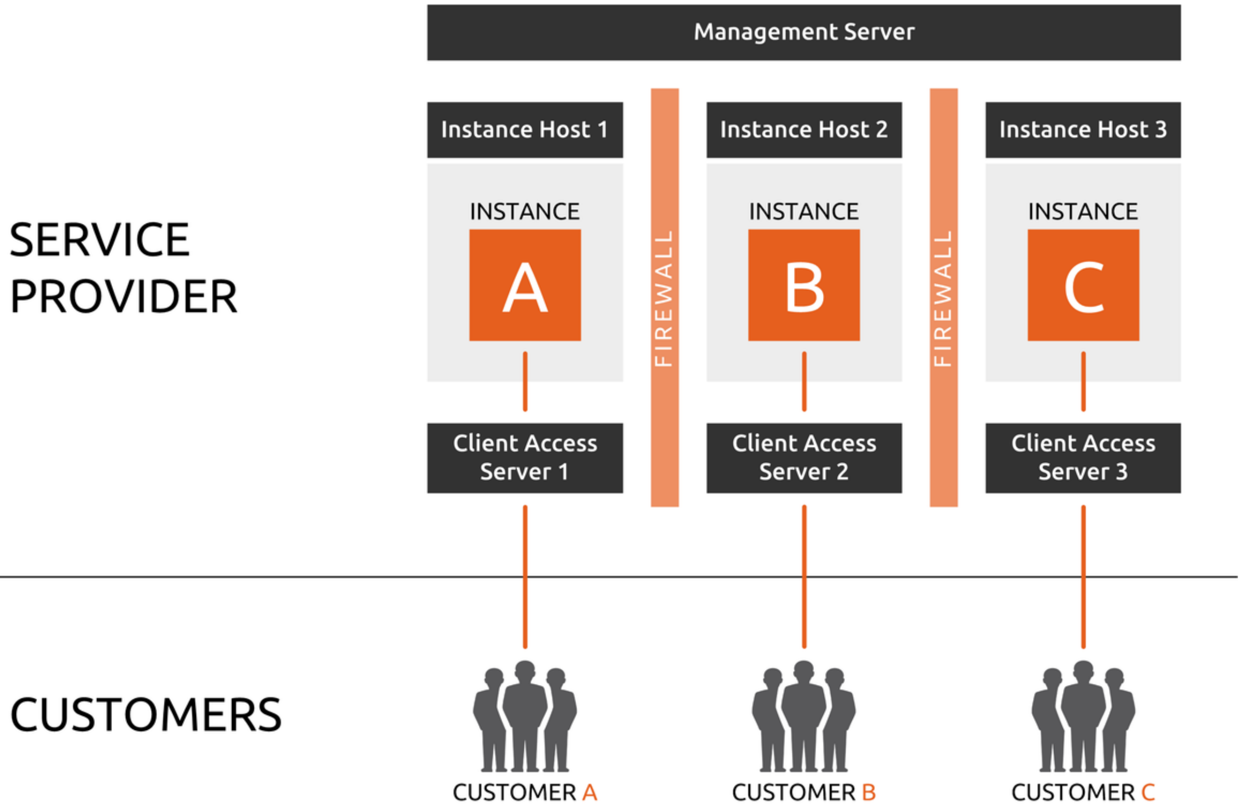
In environments where each customer is provided a protected private network and servers (often referred to as *virtual private cloud*), MailStore Service Provider Edition copes well with the higher security requirements.

Due to the fact that each MailStore component is fully trusted once it is paired with the Management Server, it is important to keep in mind that the security of the whole MailStore infrastructure also depends on who has administrative rights on the servers' operating system.

The following two options provide solutions for both scenarios where the service provider is solely the administrator (Central Management Server) and where customers have full administrative access to the servers' operating system in their virtual private cloud (Dedicated Management Servers).

Central Management Server

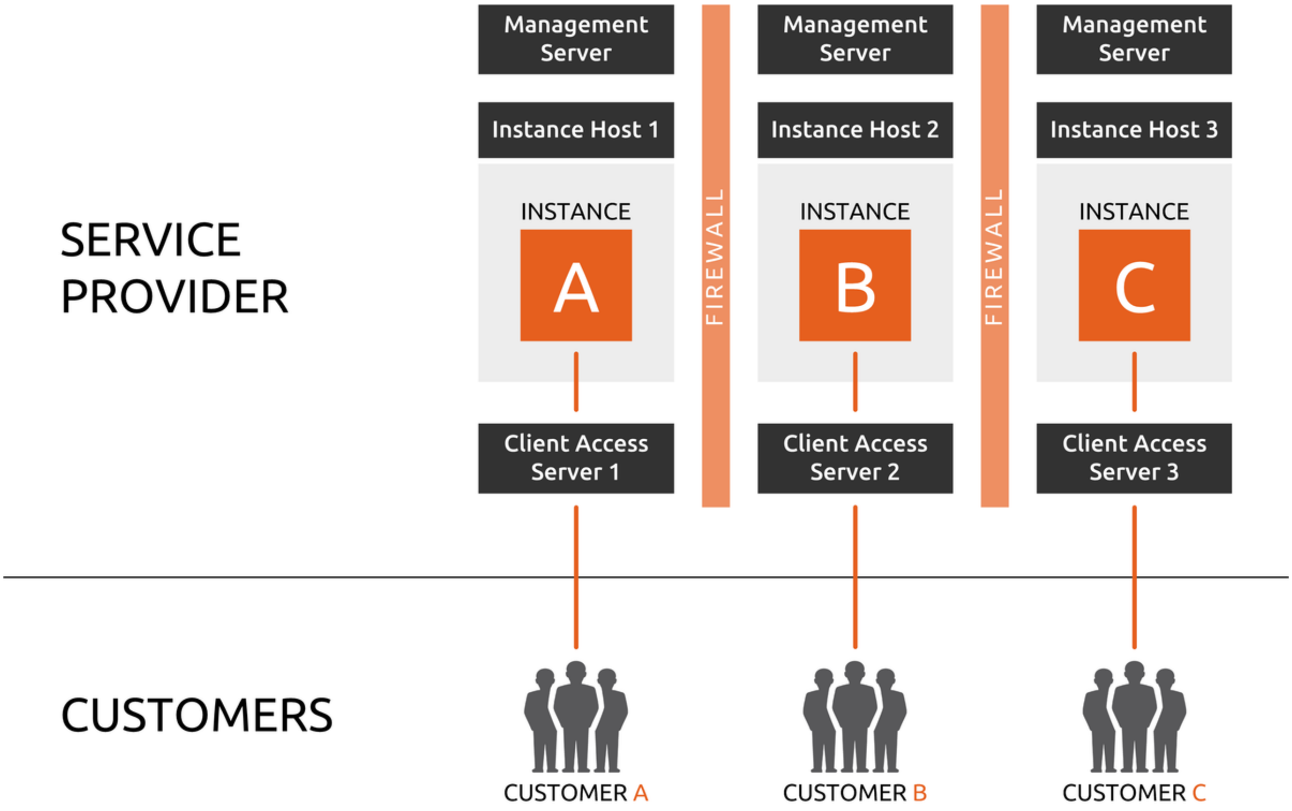
If the service provider is the only one who has administrative access, a central management server can be used to centrally administrate the Instance Hosts and Client Access Servers.



By setting up a dedicated Instance Host and Client Access Server in each customer's virtual private cloud and preventing communication with Instance Hosts and Client Access Server of other virtual private clouds, it is not possible to access instances running on others than the customer's own Instance Host.

Dedicated Management Servers

In case customers have administrative access to the operating system of servers where MailStore Service Provider Edition components are installed on, it is highly recommended to not interconnect these components through a central management server for security reasons. Instead each customer is provided his own, fully independent MailStore Service Provider Edition environment as shown below.



Please contact us for multiple activation keys for the management servers.

1.2 System Requirements

Before beginning the installation of MailStore Service Provider Edition it needs to be ensured that all system requirements are met.

Hardware

Single Server Mode or Individual Instance Hosts

The calculator below helps to specify the hardware needs in a single server mode setup or for an individual instance host in a multi-server mode setup subject to the number of users, instances, stored email, and the archiving strategy.

System Requirements Calculator

Calculations are based on the following base values:

- Email Volume (User/Year): 10000
- Email Size: 75Kb
- Compression Ratio: 60%

<system_requirements />

Management Server

This information only applies to an individual Management Server in a multi-server setup.

Processor	Any x64 compatible CPU
Main Memory	2 GB
Hard Disk	150 MB available disk space
Network Bandwidth	100 MBit/s

Client Access Server

This information only applies to an individual Client Access Server in a multi-server setup.

Processor	Any x64 compatible CPU
Main Memory	2 GB
Hard Disk	150 MB available disk space
Network Bandwidth	100 MBit/s

Software Requirements

The below system requirements only apply to MailStore Service Provider Edition and its components. Client applications such as the E-mail Archive Client and E-mail Archive Add-in for Outlook have their own system requirements. As both applications are identical to MailStore Client and MailStore Outlook Add-in, their system requirements can be found in the MailStore Server help.

- Following operating systems are supported
  - Windows Server 2008 R2 SP1 Standard, Enterprise or Datacenter (Server Core Installation)
  - Windows Server 2008 R2 SP1 Standard, Enterprise or Datacenter (Server with a GUI)
  - Windows Server 2012 Standard or Datacenter (Server Core Installation)
  - Windows Server 2012 Standard or Datacenter (Server with a GUI)
  - Windows Server 2012 R2 Standard or Datacenter (Server Core Installation)
  - Windows Server 2012 R2 Standard or Datacenter (Server with a GUI)
  - Windows Server 2016 Standard or Datacenter (Server Core Installation)
  - Windows Server 2016 Standard or Datacenter (Server with a GUI)
  - Windows Server 2019 Standard or Datacenter (Server without Desktop Experience)
  - Windows Server 2019 Standard or Datacenter (Server with Desktop Experience)
- Following web browsers are supported by the Management Console:
  - Microsoft Edge
  - Microsoft Internet Explorer 10 or higher
  - Google Chrome 18 or higher
  - Mozilla Firefox 18 or higher
  - Apple Safari 6 or higher
- **.NET Framework 4.5.1**
  The appropriate Windows Server feature will be enabled automatically by the MailStore Service Provider Edition installer. In environments with centrally managed Windows updates the automatic installation may not succeed. In such cases the installation of the .NET Framework 4.5.1 feature must be done manually before executing the MailStore Service Provider Edition setup file.

Important Notice: On Windows Server 2008 R2 Core, the features *NetFx2-ServerCore* and *NetFx2-ServerCore-WOW64* must be installed prior to executing the setup. Otherwise the .NET Framework 4.5.1 installer fails silently.

- **IFilter drivers** *(optional)*
  For indexing email attachments other than TXT and HTML files, additional IFilter drivers are required. Please refer to Search Index for further details about attachment indexing.
- It is not recommended to install MailStore Service Provider Edition on servers that already provide other network services. Especially with email or web servers TCP port conflicts are likely to occur. Specifically, Microsoft's Internet Information Server (IIS) MUST NOT be installed on any server that hosts the Client Access Server role.

Network Requirements

- Verify that the DNS name of the MailStore Service Provider Edition servers match their actual computer name and that all servers have a proper forward and reverse DNS resolution configured.
- Do not intercept connections from or to MailStore Service Provider Edition servers with web or email proxies. Read Notes on Antivirus Software in the MailStore Server help for further details.
- To guarantee a decent user experience, the available bandwidth of the network connectivity should be at least 100 MBit/s (symmetric).
- The Management Server Role must be able to access *my.mailstore.com* permanently on port 443.
- For communication between MailStore Service Provider Edition services, access to the MailStore Management Console and end user access to instances, the following TCP ports are opened by the MailStore Service Provider Edition services and must therefore not be used by any other service.

Port	Role	Description
143	Client Access Server	The standard IMAP port is used to provide read-only access to archived emails via IMAP protocol. The IMAP server on this port supports unencrypted as well as TLS secured connections (recommended) that have been initiated by the email client via STARTTLS command.
443	Client Access Server	The standard HTTPS port is used to provide SSL encrypted access to MailStore Instances via MailStore Client, MailStore Outlook Add-in, MailStore Web Access and MailStore Mobile Web Access.
993	Client Access Server	The standard IMAPS port is used to provide read-only access to archived emails via IMAP protocol. The IMAP server on this port support SSL/TLS encrypted connections only.
8470	Management Server	This port is used to provide administrators access to the Management Console via web browser. The HTTP server on this port support SSL/TLS encrypted connections only, also known as HTTPS.
8471	Management Server	Instance Hosts and Client Access Servers connect to the Management Server through this port.
8472	Instance Host	Client Access Servers and the Management Server connect to the Instance Hosts through this port.
8473	Client Access Server	Management Server connects to Client Access Servers through this port.

1.3 Frequently Asked Questions

System Requirements

- **What are the system requirements of MailStore Service Provider Edition?**
  A comprehensive overview of all system requirements can be found on the System Requirements page.
- **Is running MailStore Service Provider Edition on virtual machines supported?**
  The single server mode as well as an individual Instance Hosts in a multi-server setup requires all resources specified in the System Requirements to be allocated exclusively to the machine where the software has been installed to ensure a decent user experience under all circumstances. Therefore, using virtualization requires good planning and proper resource allocation.
  In a multi-server setup, the Management Server and Client Access Server can run on a virtual machine as long as the operating system is supported.
- **Can MailStore Service Provider Edition run on Amazon AWS, Microsoft Azure or similar infrastructure?**
  As long as the system requirements are met, MailStore Service Provider Edition can be used on IaaS platforms such as Amazon AWS or Microsoft Azure. Due to the storage requirements and the required disk I/O throughput, it often requires the use of high end instances.
- **Will there be a Linux version?**
  Due to being fully dependent on Microsoft’s .NET Framework, it is unlikely that a Linux version will exist in the future.

Use Scenarios

- **How can I switch from single server to multi server mode?**
  Any single server mode setup where Management Server, Instance Host and Client Access Server roles are installed on the same server, can be turned easily into a multi server mode setup by adding additional Instance Hosts or Client Access Servers. Further information can be found in the Multi Server Mode Setup chapter.
- **As a large organization (end customer), can I run MailStore Service Provider Edition in my own Private Cloud?**
  Generally, the MailStore Service Provider Edition can be used in Private Clouds. Please contact us [1] for further details.
- **As a Service Provider, can I use MailStore Service Provider Edition in Virtual Private Clouds that I am hosting for my end customers?**
  Using MailStore Service Provider Edition in Virtual Private Clouds is absolutely possible. Please refer to the Overview to learn more about the different supported scenarios.

Quellennachweise

[1] https://cs.mailstore.com

2

Kapitel

Installation and Setup

2.1 Installing MailStore Service Provider Edition

This setup file of MailStore Service Provider Edition includes all necessary data to deploy an arbitrary MailStore Service Provider Edition role. After the installation of the program files has been finished, the roles of the server are to be specified in the initial setup process. There is no difference in the actual installation process for a single server or multi server mode setup. Furthermore the same setup file is used to install MailStore Service Provider Edition on a normal Windows Server or Windows Server Core without graphical user interface.

Installation Procedure

- Use the credentials you have received upon registration to log in to the partner portal [1].
- Navigate to *Download Partner Resources for MailStore Service Provider Edition* and download the setup file of the latest version.
- Start the installation process by double-clicking on the downloaded setup file or, when installing on a Windows Server Core, use the command line prompt to navigate to the location of the setup file and execute it.
- Read the license agreement.
- Select *Accept the agreement* and click *Next*.
- Specify the target directory for the program files (default: `C:\Program Files\MailStore Infrastructure`) and click *Next*.
- The setup program now extracts all program files into the given target directory.
- Leave the option *Launch MailStore Service Provider Edition Configuration* checked and click *Next* to start the configuration program.

  Hint: If *Launch MailStore Service Provider Edition Configuration* was deselected in the previous step, the MailStore Service Provider Edition Configuration can be launched at any time by using the corresponding link on the desktop or from the Windows start menu.

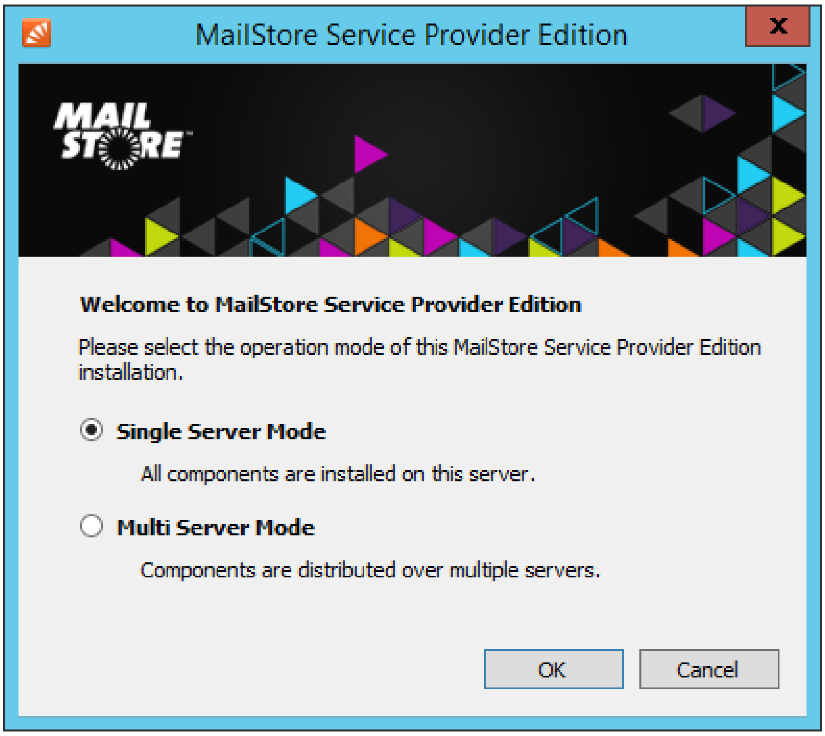
Quellennachweise

[1] https://my.mailstore.com/Partner/

2.2 Single Server Mode Setup

Set Up Single Server Mode

- If not executed automatically by the installation program, start the MailStore Service Provider Edition Configuration tool by double-clicking its desktop icon. On a Windows Server Core use the command line prompt to start the executable (default: `%PROGRAMFILES%\MailStore Infrastructure\MailStoreInfrastructureConfig.exe`.
- If no configuration files and services are found, the MailStore Service Provider Edition Configuration tool will ask for the desired mode. Select *Single Server Mode* and click *OK*.



MailStore Service Provider Edition

Welcome to MailStore Service Provider Edition

Please select the operation mode of this MailStore Service Provider Edition installation.

● Single Server Mode

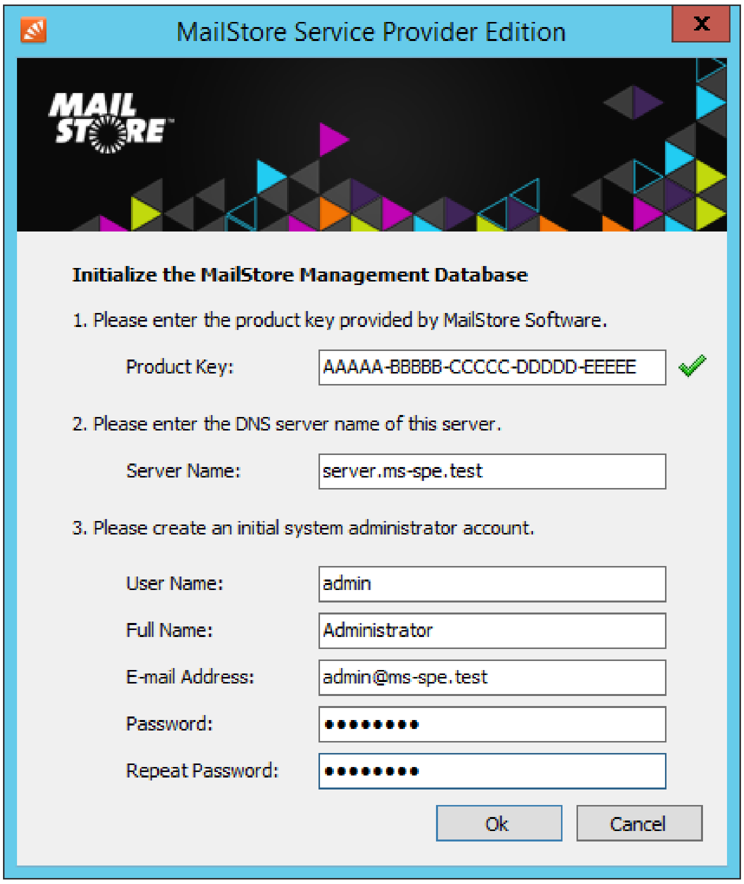
All components are installed on this server.

○ Multi Server Mode

Components are distributed over multiple servers.

- Enter your product key into the *Product Key* field and change *Server Name* to the fully qualified host name of the server (e.g. `server.ms-spe.test`). Enter the user name , the full name (optional), the email address and the password of the initial administrator account that will be used to log on to the Management Console.

Important notice: Changing the host name after MailStore SPE has been configured requires additional, mostly manual actions such as transferring the license, recreation of roles and making changes to the configuration database. Therefore it is recommend to not change the host name afterwards.



Initialize the MailStore Management Database

1. Please enter the product key provided by MailStore Software.

Product Key: AAAAA-BBBBB-CCCCC-DDDDD-EEEEE ✓

2. Please enter the DNS server name of this server.

Server Name: server.ms-spe.test

3. Please create an initial system administrator account.

User Name: admin

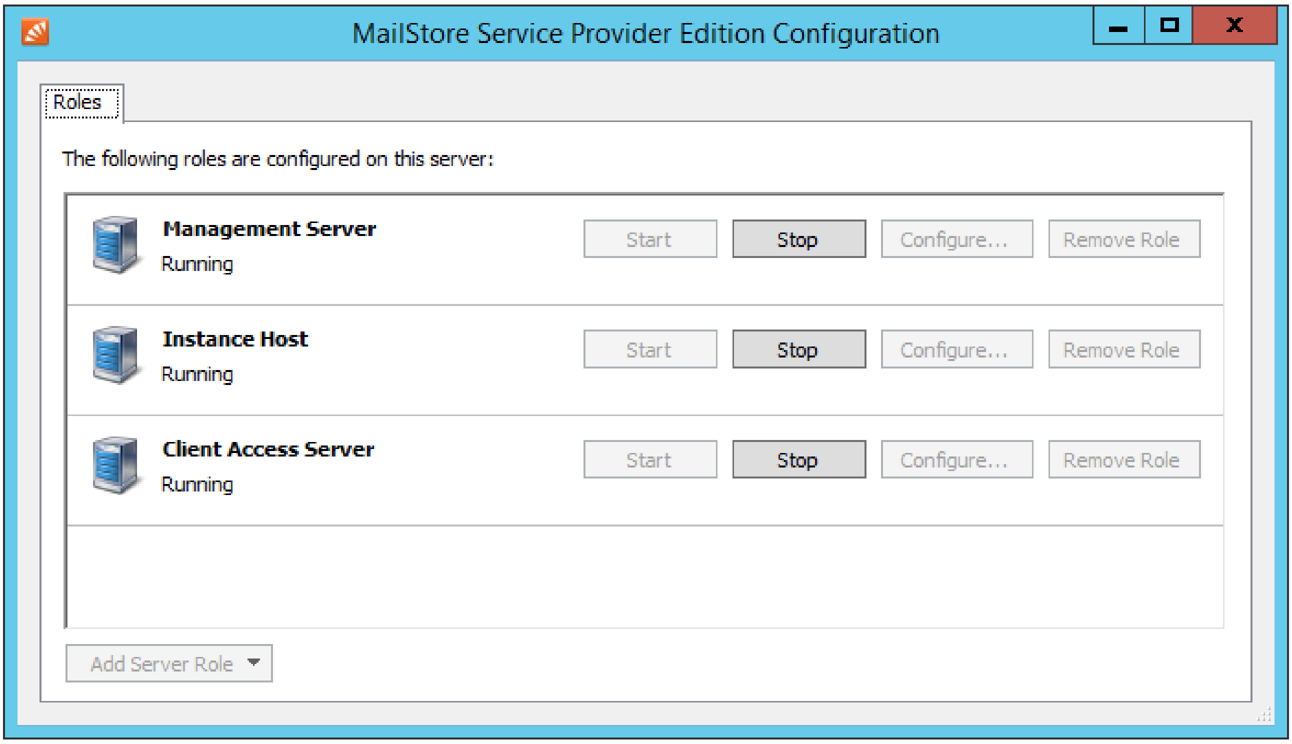
Full Name: Administrator

E-mail Address: admin@ms-spe.test

Password: ••••••••

Repeat Password: ••••••••

- Click *OK*.
- The MailStore Service Provider Edition Configuration tool will now create the configuration files for the *Management Server*, *Instance Host* and *Client Access Server* roles. After the configuration has been successfully created, a Windows service is registered and started for each role. It takes about 10-15 seconds until the roles show up in the MailStore Service Provider Edition Configuration tool.
  Important notice: Unless a different target directory was specified during installation, the configuration files are stored in `%PROGRAMFILES%\MailStore Infrastructure\config`. Although these files are in text format (JSON), please do not attempt to modify any of these files without using the MailStore Service Provider Edition Configuration tool.



MailStore Service Provider Edition Configuration

The following roles are configured on this server:

Management Server
Running

Instance Host
Running

Client Access Server
Running

- The startup process of the services takes place in the background. Therefore a service shown as *running* may still revert to *stopped* during a period of about 30 seconds in the event of an error.

2.3 Firewall Configuration for Single Server Mode

It is highly recommended to protect any MailStore Service Provider Edition service with appropriate firewall rules. This document should help with setting up the required rules. The firewall rules for running the SPE in Multi Server Mode can be found in this document.

Important Notices:

- The communication channels described below MUST NOT be intercepted by any kind of email or web proxies that are provided as part of antivirus software or unified threat management gateways.
- The Windows Advanced Firewall is activated on any Windows Server installation by default. In order to connect to services (e.g. MailStore Management Console) of the MailStore Service Provider Edition, it is required that the appropriate firewall rules are added (see below).

The table below lists all TCP ports that need to be opened in the firewall when using MailStore Service Provider Edition in single server mode. The following abbreviations are used in the source and target columns of that table:

- ANY = Any computer from private or public networks
- ADM = Computer or network used for administration
- SERVER = Server that hosts MailStore Service Provider Edition

Port	Source	Target	Description
110	SERVER	ANY	Access to email servers for archiving via POP3 (Unencrypted/STARTTLS).
143	SERVER	ANY	Access to email servers for archiving via IMAP (Unencrypted/STARTTLS).
143	ANY	SERVER	IMAP access to archives secured by TLS (STARTTLS) encryption.
389	SERVER	ANY	Access to LDAP servers (including Microsoft Active Directory) using an unencrypted or STARTTLS-encrypted session.
443	SERVER	ANY	Access to Microsoft Exchange servers for archiving via Exchange Web Services (EWS) secured by SSL encryption.
443	SERVER	my.mailstore.com	Usage reporting and license update
443	ANY	SERVER	HTTPS access to instances used by E-mail Archive Client, Outlook Add-in, and Web Access.
636	SERVER	ANY	Access to LDAP servers (including Microsoft Active Directory) using a SSL encrypted connection.
993	SERVER	ANY	Access to email servers for archiving via IMAP (SSL).
993	ANY	SERVER	IMAP access to archives secured by TLS (SSL) encryption.
995	SERVER	ANY	Access to email servers for archiving via POP3 (SSL).
8470	ADM	SERVER	Web-based access to the MailStore Management Console.
8474	ADM	SERVER	Access to the MailStore Management API.

Windows Advanced Firewall

The Windows Advanced Firewall can easily be re-configured for Single Server Mode. By executing the following commands in the Windows PowerShell command prompt, the required TCP ports are opened for inbound connections. Outbound connections to any destination are allowed by default.

```
# Allow access to CAS ports from everwhere
netsh advfirewall firewall add rule name="MailStore Service Provider
Edition (CAS)" `
  action=ALLOW dir=IN protocol=TCP localport="143,443,993" profile=ANY

# Allow access to MailStore Service Provider Management Console from
adminstrator network 192.0.2.0/24
netsh advfirewall firewall add rule name="MailStore Service Provider
Edition (MGMT)" `
  action=ALLOW dir=IN protocol=TCP localport="8470"
remoteip="192.0.2.0/24" profile=ANY

# Allow access to MailStore Management API from adminstrator network
192.0.2.0/24
netsh advfirewall firewall add rule name="MailStore Service Provider
Edition (MGMT)" `
  action=ALLOW dir=IN protocol=TCP localport="8474"
remoteip="192.0.2.0/24" profile=ANY
```

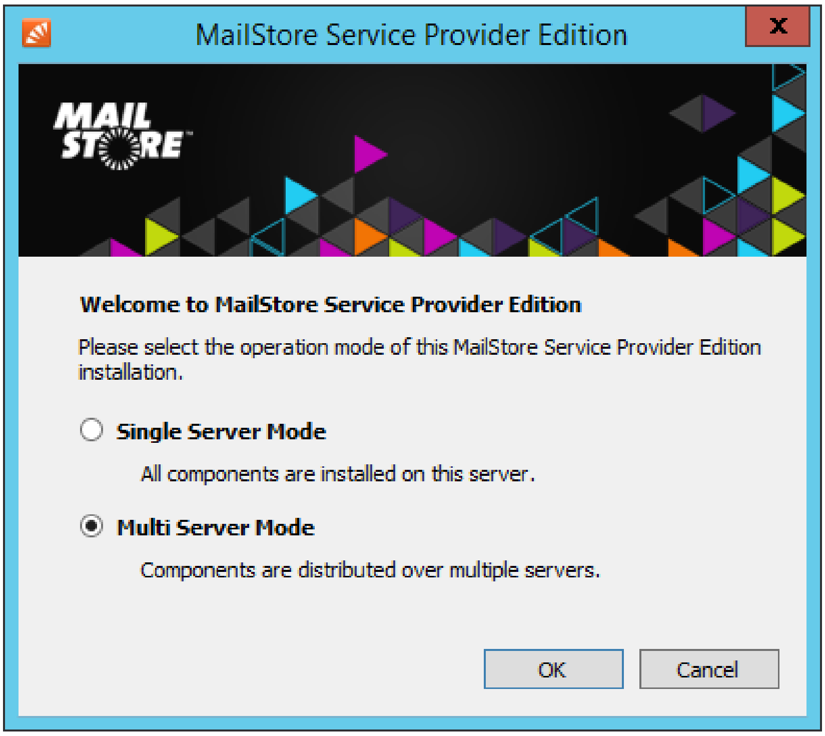
2.4 Multi Server Mode Setup

Multi Server Mode Setup

When setting up MailStore Service Provider Edition in multi server mode, the first role to set up must always be the Management Server role. Afterwards one or multiple Instance Hosts and Client Access Servers can be set up. Each server in a multi server mode setup can host one or multiple roles.

Set Up Management Server

- If not executed automatically by the installation program, start the MailStore Service Provider Edition Configuration tool by double-clicking its desktop icon. On a Windows Server Core use the command line prompt to start the executable (default: `%PROGRAMFILES%\MailStore Infrastructure\MailStoreInfrastructureConfig.exe`.
- If no configuration files and services are found, the *MailStore Service Provider Edition Configuration* will ask for the desired mode. Select *Multi Server Mode* and click *OK*.



MailStore Service Provider Edition

Welcome to MailStore Service Provider Edition

Please select the operation mode of this MailStore Service Provider Edition installation.

○ **Single Server Mode**

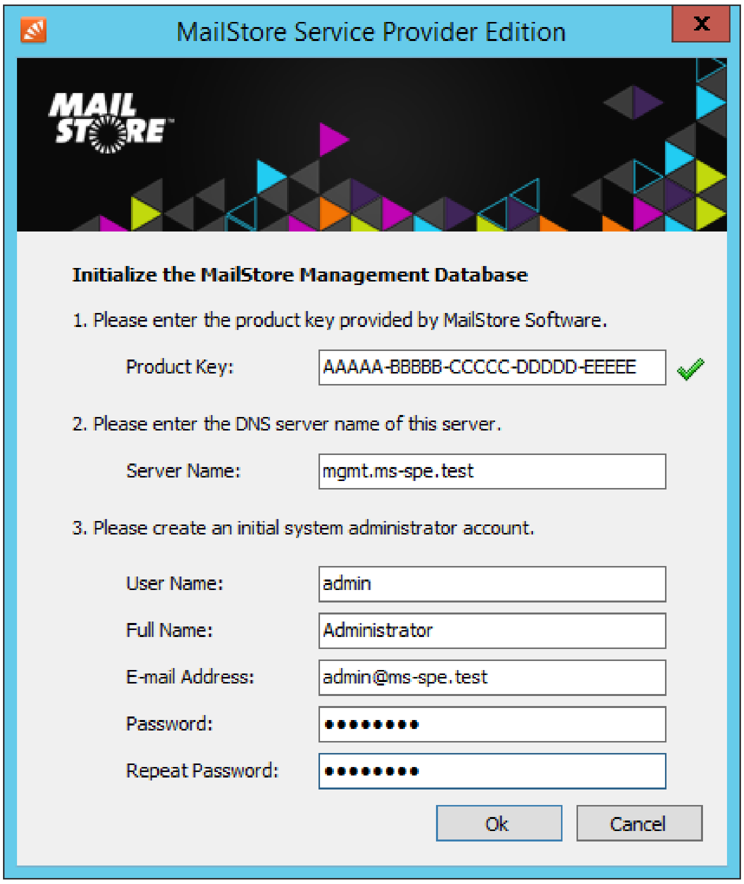
All components are installed on this server.

● **Multi Server Mode**

Components are distributed over multiple servers.

- Click *Add Server Role*
- Select *Management Server*
- Enter your product key into the Product Key field and change Server Name to the fully qualified host name of the server (e.g. mgmt.ms-spe.test). Enter the user name , the full name (optional), the email address and the password of the initial administrator account that will be used to log on to the Management Console.

Important notice: Changing the host name after the Management Server has been configured requires additional, mostly manual actions such as transferring the license, re-pairing Instance Hosts and Client Access Servers and making changes to the configuration database. Therefore it is recommend to not change the host name afterwards.



Initialize the MailStore Management Database

1. Please enter the product key provided by MailStore Software.

Product Key: AAAAA-BBBBB-CCCCC-DDDDD-EEEEE ✓

2. Please enter the DNS server name of this server.

Server Name: mgmt.ms-spe.test

3. Please create an initial system administrator account.

User Name: admin

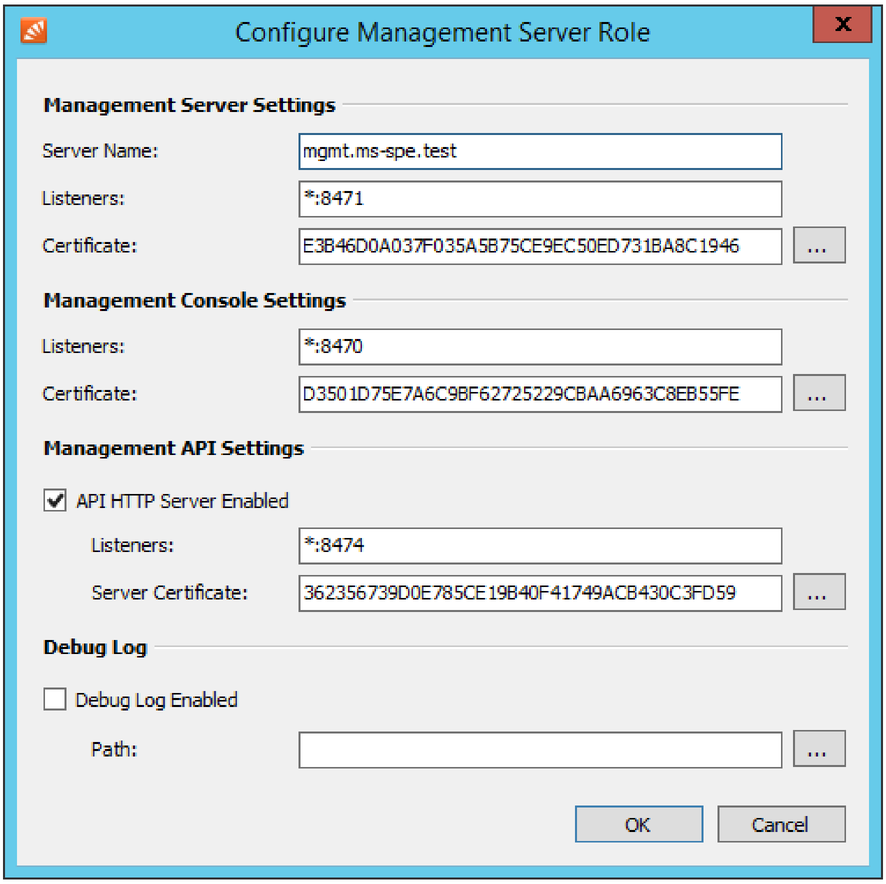
Full Name: Administrator

E-mail Address: admin@ms-spe.test

Password: ●●●●●●●●

Repeat Password: ●●●●●●●●

- Fill out the *Configure Management Server Role* form.



Configure Management Server Role

Management Server Settings

Server Name: mgmt.ms-spe.test

Listeners: *:8471

Certificate: E3B46D0A037F035A5B75CE9EC50ED731BA8C1946

Management Console Settings

Listeners: *:8470

Certificate: D3501D75E7A6C9BF62725229CBAA6963C8EB55FE

Management API Settings

☑ API HTTP Server Enabled

Listeners: *:8474

Server Certificate: 362356739D0E785CE19B40F41749ACB430C3FD59

Debug Log

□ Debug Log Enabled

Path:

Management Server Settings

- **Server Name:** Fully qualified host name (FQHN) of the server
- **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections from Instance Hosts and Client Access Servers (Default: *:8471)
- **Certificate:** Fingerprint of the TLS certificate used by the Management Server to authenticate against Instance Hosts and Client Access Serves. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

Management Console Settings

- **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections to the Management Console (Default: *:8470)
- **Certificate:** Fingerprint of the TLS certificate used by the Management Server's HTTP server. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

Management API Settings

The Management API needs to be active when Instance Hosts or Client Access Servers will be paired with this Management Server.

- **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections to the Management Console and Management API (Default: *:8470)
- **Certificate:** Fingerprint of the TLS certificate used by the Management Server's API server. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

Debug Log

In case of errors the debug log of the Management Server can be enabled here.

- **Path:** Directory on the file system where the debug log files are written into.

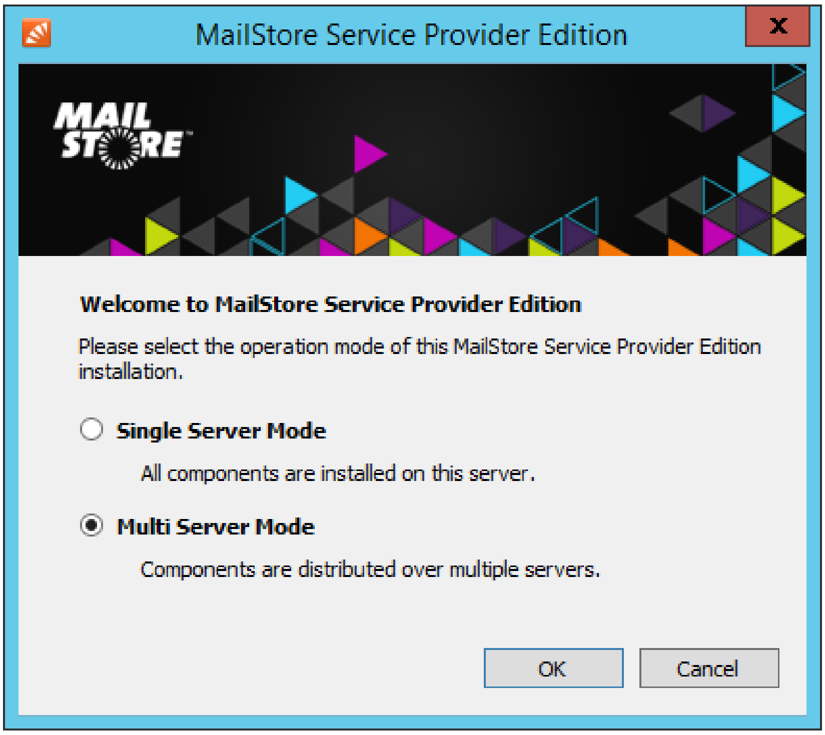
- Click *OK* to add the Management Server role.
- Click *Start* to start the Management Server service.

Please note: As the startup process of the services is asynchronous, please wait up to 30 seconds. A service shown as running may still switch back to stopped during that period if an error occurred.

- It is now safe to close the MailStore Service Provider Edition Configuration tool

Set Up Instance Host

- If not executed automatically by the installation program, start the MailStore Service Provider Edition Configuration tool by double-clicking its desktop icon. On a Windows Server Core use the command line prompt to start the executable (default: `%PROGRAMFILES%\MailStore Infrastructure\MailStoreInfrastructureConfig.exe`.
- If no configuration files and services are found, the *MailStore Service Provider Edition Configuration* will ask for the desired mode. Select *Multi Server Mode* and click *OK*.



Welcome to MailStore Service Provider Edition

Please select the operation mode of this MailStore Service Provider Edition installation.

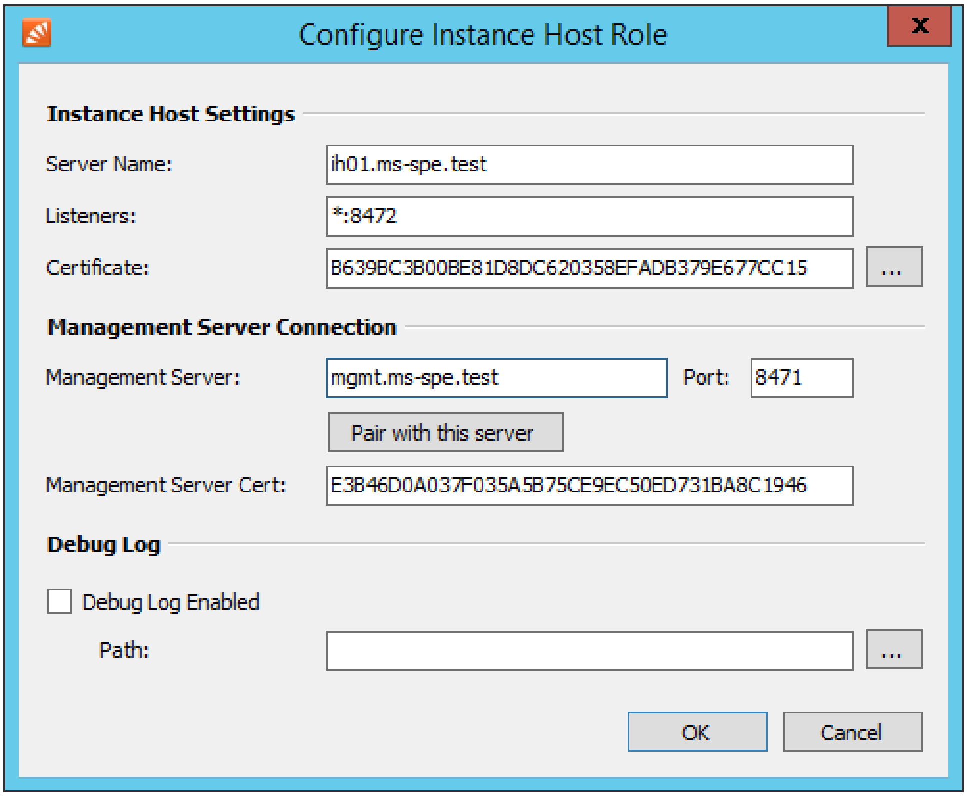
○ **Single Server Mode**

All components are installed on this server.

● **Multi Server Mode**

Components are distributed over multiple servers.

- Click *Add Server Role*
- Select *Instance Host*
- Fill out the *Configure Instance Host Role* form.



Configure Instance Host Role

Instance Host Settings

Server Name: ih01.ms-spe.test

Listeners: *:8472

Certificate: B639BC3B00BE81D8DC620358EFADB379E677CC15

Management Server Connection

Management Server: mgmt.ms-spe.test Port: 8471

Management Server Cert: E3B46D0A037F035A5B75CE9EC50ED731BA8C1946

Debug Log

□ Debug Log Enabled

Path:

Instance Host Settings

- **Server Name:** Fully qualified host name (FQHN) of the server
- **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections from the Management Server (Default: *:8472)
- **Certificate:** Fingerprint of the TLS certificate used by the Instance Host to authenticate against Management Server. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

Management Server Connection

- **Management Server:** Fully qualified host name (FQHN) of the Management Server to connect to.
- **Port:** TCP port where the above Management Server accepts incoming connections.
- **Management Server Cert:** Fingerprint of the TSL certificate used by the Management Server to authenticate against Instance Host. This value is set automatically when Pairing with Management Server

Debug Log

In case of errors the debug log of the Instance Host can be enabled here.

- **Path:** Directory on the file system where the debug log files are written into.

- Click *OK* to add the Instance Host role.
- Click *Start* to start the Instance Host service.

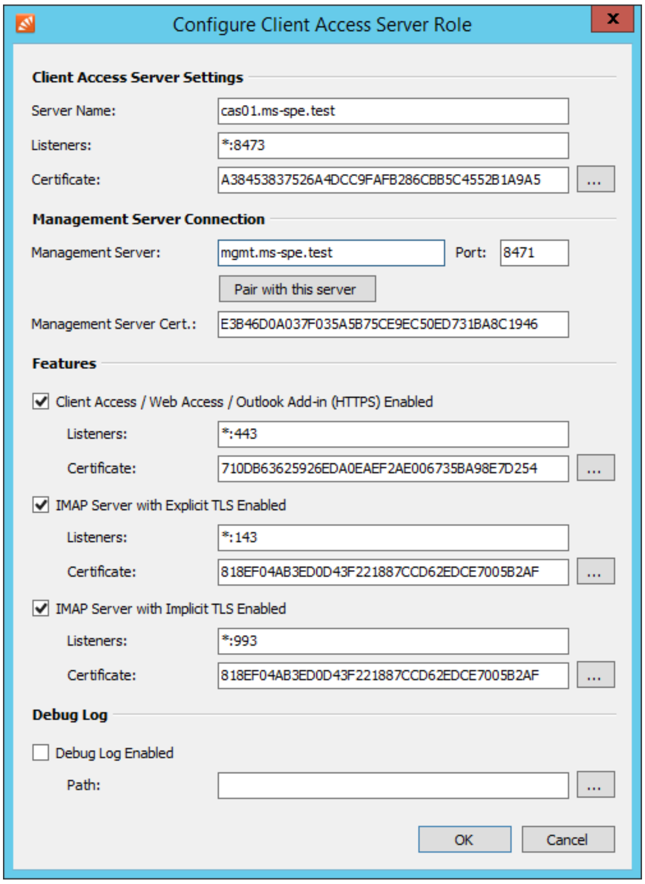
  Please note: As the startup process of the services is asynchronous, please wait up to 30 seconds. A service shown as running may still switch back to stopped during that period if an error occurred.

- It is now safe to close the MailStore Service Provider Edition Configuration tool

Set Up Client Access Server

- If not executed automatically by the installation program, start the MailStore Service Provider Edition Configuration tool by double-clicking its desktop icon. On a Windows Server Core use the command line prompt to start the executable (default: `%PROGRAMFILES%\MailStore Infrastructure\MailStoreInfrastructureConfig.exe`.
- If no configuration files and services are found, the *MailStore Service Provider Edition Configuration* will ask for the desired mode. Select *Multi Server Mode* and click *OK*.

- Click *Add Server Role* .
- Select *Client Access Server*.
- Fill out the *Configure Client Access Server Role* form.



Configure Client Access Server Role

Client Access Server Settings

Server Name: cas01.ms-spe.test

Listeners: *:8473

Certificate: A38453837526A4DCC9FAFB286CBB5C4552B1A9A5

Management Server Connection

Management Server: mgmt.ms-spe.test Port: 8471

Management Server Cert.: E3B46D0A037F035A5B75CE9EC50ED731BA8C1946

Features

☑ Client Access / Web Access / Outlook Add-in (HTTPS) Enabled

Listeners: *:443

Certificate: 710DB63625926EDA0EAEF2AE006735BA98E7D254

☑ IMAP Server with Explicit TLS Enabled

Listeners: *:143

Certificate: 818EF04AB3ED0D43F221887CCD62EDCE7005B2AF

☑ IMAP Server with Implicit TLS Enabled

Listeners: *:993

Certificate: 818EF04AB3ED0D43F221887CCD62EDCE7005B2AF

Debug Log

☐ Debug Log Enabled

Path:

Client Access Server Settings

- **Server Name:** Fully qualified host name (FQHN) of the server
- **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections from the Management Server (Default: *:8473)
- **Certificate:** Fingerprint of the TLS certificate used by the Client Access Server to authenticate against Management Server. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

Management Server Connection

- **Management Server:** Fully qualified host name (FQHN) of the Management Server to connect to.
- **Port:** TCP port where the above Management Server accepts incoming connections.
- **Management Server Cert:** Fingerprint of the TLS certificate used by the Management Server to authenticate against Client Access Server. This value is set automatically when Pairing with Management Server

Features

Client Access / Web Access / Outlook Add-in (HTTPS) Enabled

> **If enabled the Client Access Server provides access to archives via MailStore Client, MailStore Outlook Add-in and MailStore Web Access.**
>
> - **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections (Default: *:443)
> - **Certificate:** Fingerprint of the TLS certificate used by the HTTP Server. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

IMAP Server with explicit TLS Enabled

> **If enabled the Client Access Server provides access to archives via IMAP protocol. Connections must be secured via STARTTLS.**
>
> - **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections (Default: *:143)
> - **Certificate:** Fingerprint of the TLS certificate used by the IMAP Server. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

IMAP Server with implicit TLS Enabled

> **If enabled the Client Access Server provides access to archives via IMAP protocol. Connection is encrypted via SSL/TLS.**
>
> - **Listeners:** If the server is multihomed you can specify on which IP address and TCP port to listen for incoming connections (Default: *:993)
> - **Certificate:** Fingerprint of the TLS certificate used by the IMAP Server. Use the button next to the fingerprint to select a different certificate from the computer's certificate store.

Debug Log

In case of errors the debug log of the Client Access Server can be enabled here.

  - **Path:** Directory on the file system where the debug log files are written into.

- Click *OK* to add the Client Access Server role.
- Click *Start* to start the Client Access Server service.

  Please note: As the startup process of the services is asynchronous, please wait up to 30 seconds. A service shown as running may still switch back to stopped during that period if an error occurred.

- It is now safe to close the MailStore Service Provider Edition Configuration tool

Pairing with Management Server

Before Client Access Servers and Instance Hosts are able to communicate with the Management Server, TLS certificate fingerprints must be exchanged to establish a trust relationship. Additionally the Instance Hosts and Client Access Servers must be registered in the Management Server with its server name and TCP port.

This process can simply be performed by using the pairing function as described in the following:

- Enter the fully qualified host name of the server where the role is added in the *Server Name* field.
- Enter the fully qualified host name of the *Management Server* in the corresponding *Management Server* field while configuring an Instance Host or Client Access Server.
- Click *Pair with this server*.
- Enter the user name and password of a MailStore Service Provider Edition administrator.
- Click *OK* to pair this role with the Management Server.
- The fingerprint of the Management Server's TLS certificate is copied in the *Management Server Cert* field of the role to be installed.
- The fingerprint of the role's TCP server's TLS certificate is transferred to the Management Database of the Management Server. This can be reviewed here.

Please note: Pairing is carried out through the Management API. Therefore the Management API must be enabled on the Management Server and the Instance Hosts and Client Access Servers must be able to establish a connection to the API on the Management Server (Default TCP port: 8474).

If your security policy does not permit establishing such a connection, pairing must be performed manually. Please refer to Add New Instance Host or Add New Client Access Server for further details.

2.5 Firewall Configuration for Multi Server Mode

It is highly recommended to protect any MailStore Service Provider Edition service with appropriate firewall rules. This document should help with setting up the required rules. The firewall rules for running the SPE in Single Server Mode can be found in this document.

Important Notices:

- The communication channels described below MUST NOT be intercepted by any kind of email or web proxies that are provided as part of antivirus software or unified threat management gateways.
- The Windows Advanced Firewall is activated on any Windows Server installation by default. In order to connect to services (e.g. MailStore Management Console) of the MailStore Service Provider Edition, it is required that the appropriate firewall rules are added (see below).

The below table lists all TCP ports that need to be opened in the firewall when using MailStore Service Provider Edition in multi server mode. The following abbreviations are used in the source and target columns:

- ANY = Any computer from private or public networks
- ADM = Computer or network used for administration
- CAS = Server hosting Client Access Server role
- IH = Server hosting Instance Host role
- MGMT = Server hosting Management Server role

Port	Source	Target	Description
110	IH	ANY	Access to email servers for archiving via POP3 (Unencrypted/STARTTLS).
143	IH	ANY	Access to email servers for archiving via IMAP (Unencrypted/STARTTLS).
143	ANY	CAS	IMAP access to archives secured by TLS (STARTTLS) encryption.
389	IH	ANY	Access to LDAP servers (including Microsoft Active Directory) using an unencrypted or STARTTLS-encrypted session.
443	IH	ANY	Access to Microsoft Exchange Server for archiving via Exchange Web Services (EWS) secured by SSL encryption.
443	ANY	CAS	HTTPS access to instances used by E-mail Archive Client, Outlook Add-in, and MailStore Web Access.
443	MGMT	my.mailstore.com	Usage reporting and license update
636	IH	ANY	Access to LDAP servers (including Microsoft Active Directory) using a SSL encrypted connection.
993	ANY	CAS	IMAP access to archives secured by TLS (SSL) encryption.
993	IH	ANY	Access to email servers for archiving via IMAP (SSL).
995	IH	ANY	Access to email servers for archiving via POP3 (SSL).
8470	ADM	MGMT	Web-based access to the MailStore Management Console.
8471	CAS, IH	MGMT	Internal communication with Management Server
8472	MGMT, CAS	IH	Internal communication with Instance Hosts
8473	MGMT	CAS	Internal communication with Client Access Servers
8474	ADM	MGMT	Access to the MailStore Management API.
8474	IH, CAS	MGMT	Optional: Required for initial pairing with Management Server in Multi Server Mode. If not available, manual registration of Instance Hosts and Client Access Servers in Management Server is required.

3

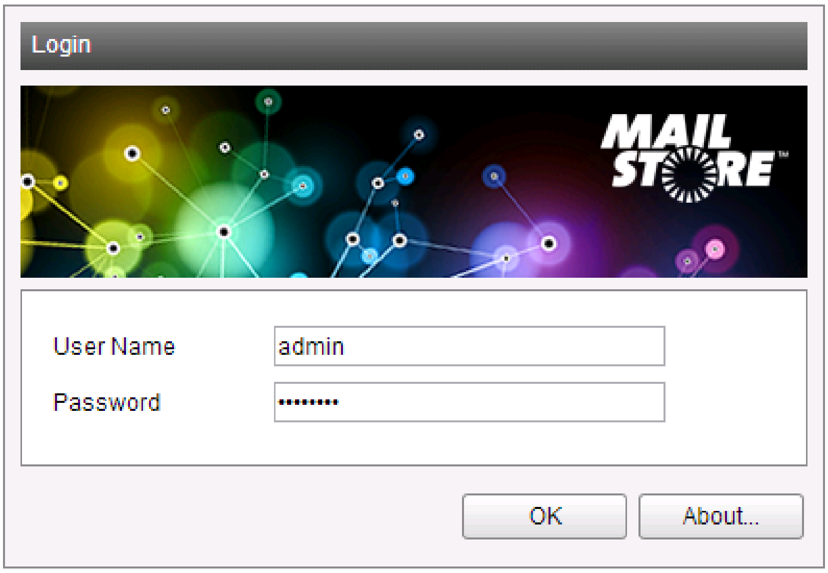
Kapitel

Using MailStore Service Provider Edition

3.1 Management Console - Logging On

In order to log on to the Management Console follow these instructions:

- Open your favorite web browser.
- Navigate to `https://<hostname-or-ip-address-of-management-server>:8470`.
- Accept any security related warning from your browser caused by the self-signed certificate.
- In the *User Name* field enter *admin* or your personal system administrator's user name. Enter the appropriate password into the *Password* field and click *OK*.



User Name: admin

Password: •••••••••

- After authentication succeeded you will see the Management Console's dashboard.

3.2 Management Console - General

Dashboard

The dashboard of the Management Console is divided into the following parts.

Service Health

This sections gives a quick overview of the status of all configured hosts and their roles which are under the control of the Management Server. The root node of the tree always represents the Management Server, the left branch the Instance Hosts and the right branch shows the Client Access Servers. Instance Host nodes also show the number of available and active instances.

Version and License Information

Details about the product version in use and the licensee including their customer number are displayed here.

My Resources

The *My Resources* sections lists all resources created in the MailStore Service Provider Edition. This includes the number of *Management Server*, *Instance Hosts*, *Client Access Server* and the total number of instances available and running.

Messages

System messages that might require further administrative actions are shown in the *Messages* section of the dashboard. Typical message may contain warnings about license update failures or necessary search index rebuilds.

Related Links

This sections contains links to the most valuable online resources including this online help, Customer Service Center, etc.

Instances

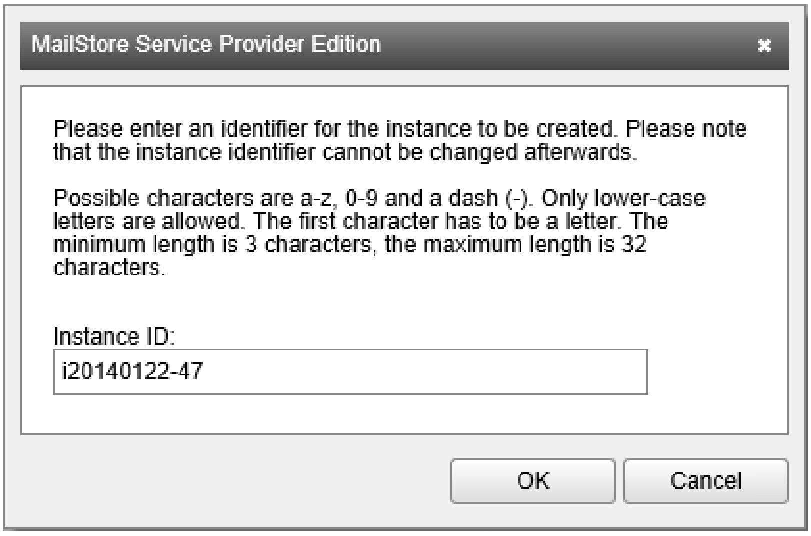
The main task of each MailStore Service Provider Edition administrator will be the management of instances. General administrative tasks such as creating, configuring, stating, stopping and deleting instances is described in the following.

Individual instance tasks like managing archive stores and search indexes, managing users and creating setting up archiving is covered in Instance Management.

Creating Instances

To create new instances for customers follow these steps:

- Log on to the Management Console, if not already logged on.
- Click on *General* > *Instances*.
- Click *Create Instance*.
- Enter a unique *Instance ID*.



MailStore Service Provider Edition

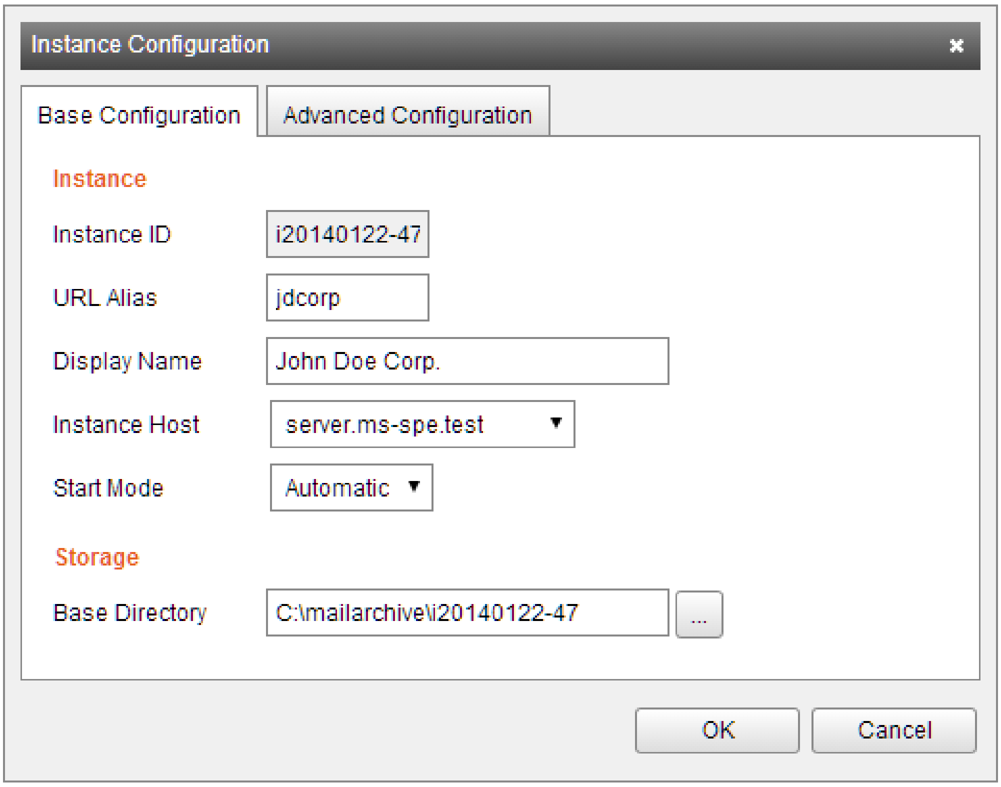
Please enter an identifier for the instance to be created. Please note that the instance identifier cannot be changed afterwards.

Possible characters are a-z, 0-9 and a dash (-). Only lower-case letters are allowed. The first character has to be a letter. The minimum length is 3 characters, the maximum length is 32 characters.

Instance ID: i20140122-47

Hint: It is not necessary to choose a meaningful instance ID, as an alias name can define in the next step. The instance ID could for example be a customer number or any other unique identifier from a CRM system.

- Click *OK*.
- Fill out the *Instance Configuration* form:



Instance Configuration

Instance

Instance ID: i20140122-47

URL Alias: jdcorp

Display Name: John Doe Corp.

Instance Host: server.ms-spe.test

Start Mode: Automatic

Storage

Base Directory: C:\mailarchive\i20140122-47

Tab: Base Configuration

URL Alias Meaningful unique alias name that can be used as an alternative to the instance ID.

Display Name: Additional identification information for the instance, e.g. customer name.

Instance Host: Instance Host on which the new instance gets created.

Start Mode: Defines how the instance is started. Choose from the following options (Default: *Automatic*):

Disabled: The instance can neither be started automatically nor manually.

Manual: The instance can only be started manually.

Automatic: The instance will automatically be started with the Instance. Host.

Base Directory: Directory where instance's data will be stored.

Tab: Advanced Configuration

Enable VSS Writer: Enable support for Volume Shadow Service.

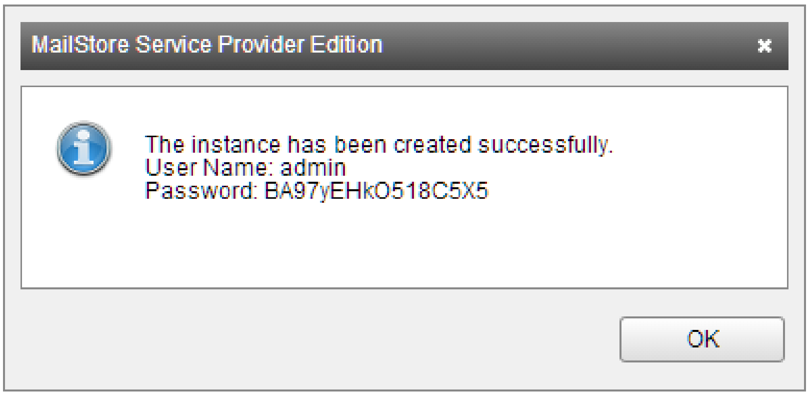
Exclude Indexes from VSS Backup: Excludes the unencrypted search index files from the backup set reported by the VSS writer.

Please note: This option can be set so that administrators which have access to the backup files cannot access the unencrypted search index files. When restoring backups that do not include search index files, the search indexes have to be rebuilt.

Enable Debug Log: Enable debug logging for the instance.

Enable IMAP Server Connection Log: Enable IMAP Server connection logging for the instance.

- Click *OK* to create the instance.
- MailStore Service Provider Edition will now create the new instance and displays the login credential for afterwards.



The instance has been created successfully.
User Name: admin
Password: BA97yEHkO518C5X5

If the end customer should be able to administrate the newly created MailStore Server instance on his own, these credentials must be made available to him. Otherwise it is not necessary to save these credentials.

- Click *OK* to finish.

Irrespective of the configured *Start Mode*, the newly created instance must be started manually before it can be used. Read more about starting, stopping and restarting of instances in the next section.

Controlling Instances

To start, stop or restart instances follow the steps:

- Log on to the Management Console, if not already logged on.
- Click on *General* > *Instances*.
- Select one or multiple instances from the list using the appropriate checkboxes.
- Click either on *Start*, *Safe Mode*, *Stop* or *Restart*.

Please notice that the *Start Mode* of an instance must be set to *Automatic* or *Manual* in order to start an instance.

Safe Mode

An instance can be started in *Safe Mode* to perform maintenance on its configuration.

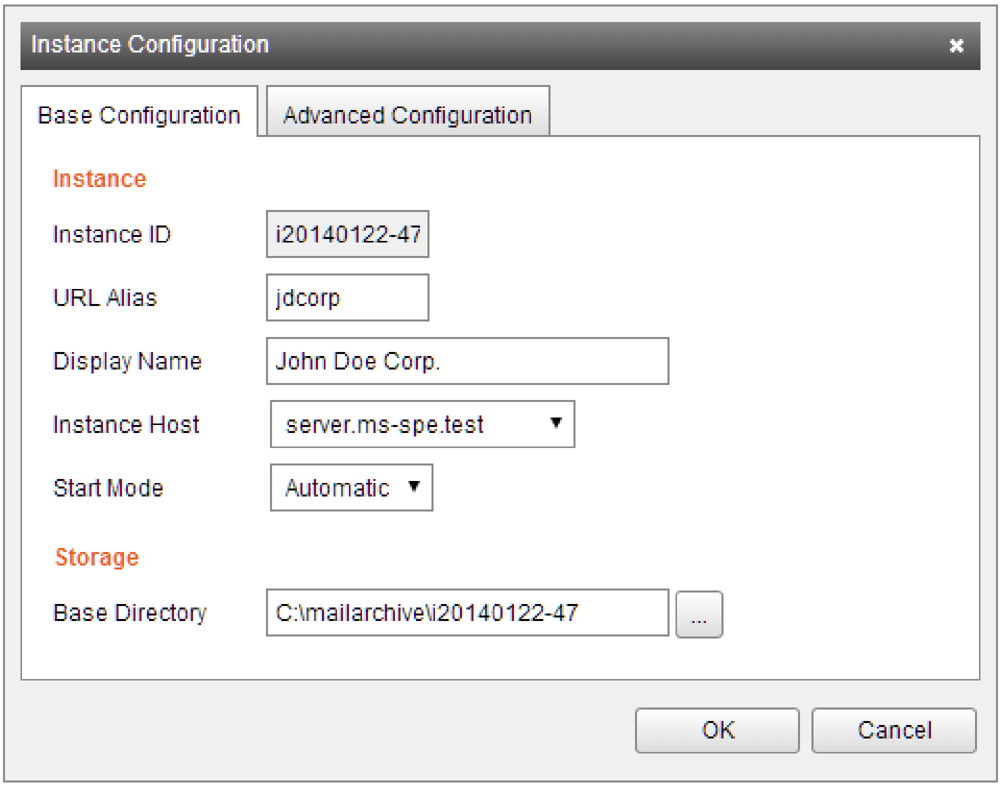
While the *Safe Mode* is active:

- Only administrators can log in to the instance
- Automatic archiving and export profiles are not started
- Jobs are not started automatically
- All internal heartbeats are disabled

Configuring Instances

Most configuration settings of existing instances can be modified. The instance to modify must be stopped before its configuration can be changed. To change the configuration proceed as follows:

- Log on to the Management Console, if not already logged on.
- Click on *General* > *Instances*.
- Select the instances to modify.
- Click on *Configure...*.
- Make the desired configuration changes.



Instance ID: i20140122-47

URL Alias: jdcorp

Display Name: John Doe Corp.

Instance Host: server.ms-spe.test

Start Mode: Automatic

Base Directory: C:\mailarchive\i20140122-47

Tab: Base Configuration

URL Alias Meaningful unique alias name that can be used as an alternative to the instance ID.

Display Name: Additional identification information for the instance, e.g. customer name.

Instance Host: Instance Host on which the new instance gets created.

Start Mode: Defines how the instance is started. Choose from the following options (Default: *Automatic*):

Disabled: The instance can neither be started automatically nor manually.

Manual: The instance can only be started manually.

Automatic: The instance will automatically be started with the Instance. Host.

Base Directory: Directory where instance's data will be stored.

Tab: Advanced Configuration

Enable VSS Writer: Enable support for Volume Shadow Service.

Exclude Indexes from VSS Backup: Excludes the unencrypted search index files from the backup set reported by the VSS writer.

> **Please note:** This option can be set so that administrators which have access to the backup files cannot access the unencrypted search index files. When restoring backups that do not include search index files, the search indexes have to be rebuilt.

Enable Debug Log: Enable debug logging for the instance.

Enable IMAP Server Connection Log: Enable IMAP Server connection logging for the instance.

- Click *OK* to save the changes.

Important notice: Neither changing the *Instance Host* nor the *Base Directory* will move the archive data to the new location. If necessary this must be done manually before starting the instance again.

Deleting Instances

Instances can be deleted at any time as long as they are stopped. Deleting an instance only removes it from the management database of the MailStore Service Provider Edition. All instance data remains on the hard disk and must be removed manually if necessary. To delete an instance follow these instructions:

- Log on to the Management Console, if not already logged on.
- Click on *General* > *Instances*.
- Select the instances to delete.
- Click on *Command* > *Delete*.
- Confirm the security query with *OK* to delete the instance, otherwise click *Cancel* to abort.

License Information

Clicking on the *License Information* menu item opens an overview of all data that is used by the billing process.

Used Licenses per Instance

Displays a list off all instances and their respective amount of used licenses.

Used Resources

This is a statistical overview of used resources.

Raw Licensing Request

The raw licensing request tab shows how the actual licensing request to our accounting servers looks like. The Management Server sends this information once every 24 hours to renew the local licensing information of the MailStore Service Provider Edition.

SMTP Settings

Notifications are send by email in the following situations:

- product updates are available,
- a new Web Access version was installed automatically,
- license renewal requests failed for three consecutive days.

To send emails to administrators of the Service Provider Edition, the following settings have to be defined:

- **Server:** Enter the host name or IP address of the SMTP server.
- **Port:** By default, port 587 is used for email submission. If a different port (i.e. 25) is required by the SMTP server, change it here.
- **Protocol:** Select the protocol required by the SMTP server. Select *SMTP* for an unencrypted connection to the SMTP server. For an encrypted connection, select *SMTP-TLS* (STARTTLS, Explicit SSL) or *SMTP-SSL* (Implicit SSL). If the SMTP server does not use a SSL certificate signed by a trusted Certificate Authority, check *Ignore SSL Warnings*; otherwise, the sending process will fail.

- **Server requires authentication:** If the SMTP server requires authentication prior to sending, check the corresponding checkbox and enter the appropriate credentials into the *User Name* and *Password* fields.
- **Display Name:** Enter a name that helps to identify the origin of the emails send by the Service Provider Edition.
- **Email Address:** Enter the email address of the sender. Some email servers, like Microsoft Exchange, verify that the authenticated users is allowed to use a particular email address.
- **Recipient for Notifications:** Select the system administrators who should receive notifications. When none are listed, verify that at least one system administrator has the email address attribute set.

Once all settings have been specified, the SPE can be instructed to send a test email to the selected system administrators; simply click on *Apply and Test*. If an error message appears or the recipient specified does not receive the email, the following hints for troubleshooting may be helpful.

Troubleshooting

- If no error occurs upon sending but the email does not arrive, please check the spam or junk mail folder of the mailbox.
- If an error message appears because of an invalid certificate ("Server's certificate was rejected by the verifier because of an unknown certificate authority."), check *Ignore SSL Warnings* and try again.
- If an error message appears indicating that *"One or more recipients rejected"*, the SMTP server probably requires authentication. Enter the appropriate credentials as described above.
- If an error message appears because of invalid credentials (e.g. *"Incorrect authentication data"*or *"Authentication failed"*), verify the data entered.
- If further error messages appear or other problems arise, please check your input for possible mistakes.

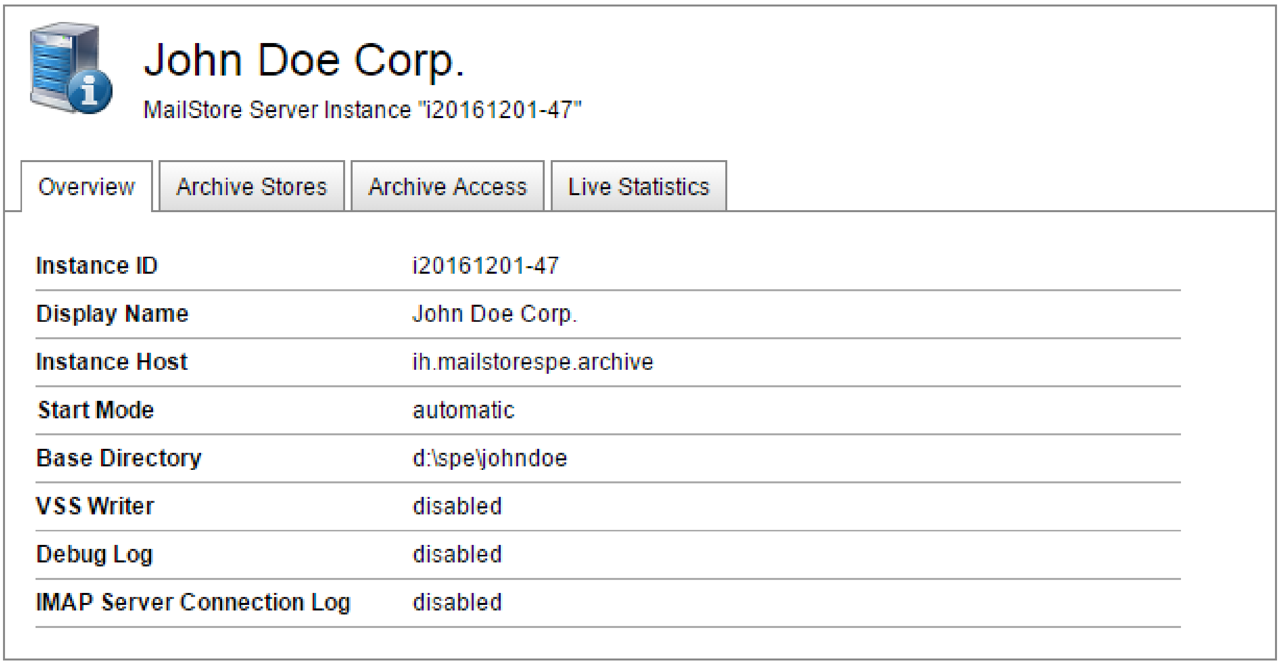
3.3 Instance Management

For each instance further individual administrative functions exist. These functions are accessible through the instance details, which appear in pane below the instance list (*General* > *Instances*) of the Management Console when clicking on a running instance in the list.

All these functions are group by tabs, for which further details are provided below.

Overview

On the *Overview* tab of the instance details a summary of the configuration is shown.



John Doe Corp.

MailStore Server Instance "i20161201-47"

Instance ID	i20161201-47
Display Name	John Doe Corp.
Instance Host	ih.mailstorespe.archive
Start Mode	automatic
Base Directory	d:\spe\johndoe
VSS Writer	disabled
Debug Log	disabled
IMAP Server Connection Log	disabled

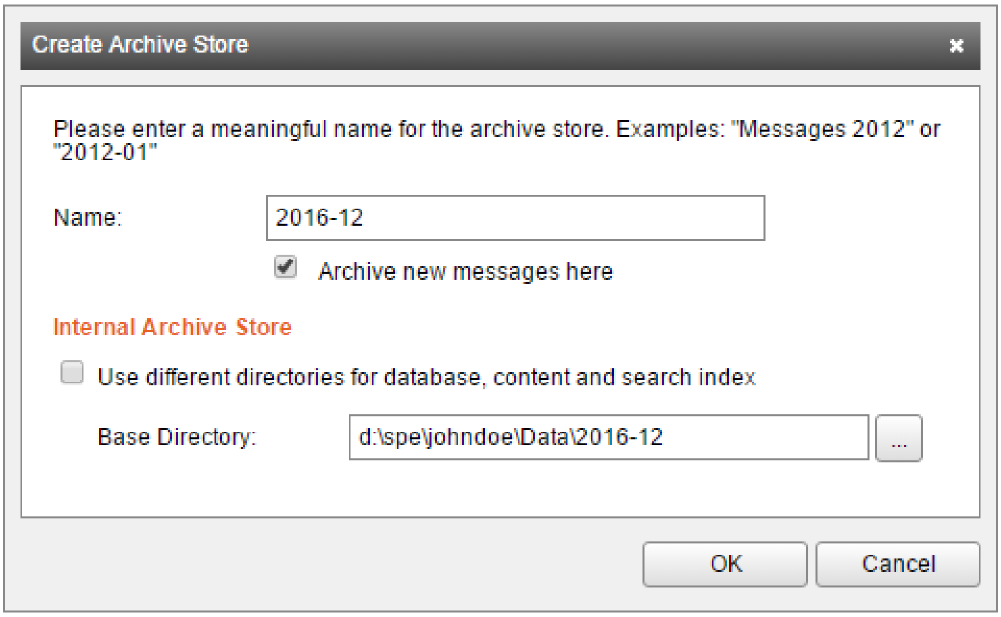
Archive Stores

The *Archive Stores* tab allows the administration of the instance storage as well as the search indexes. New archive stores are automatically created in the base directory of the instance every 5.000.000 messages.

Create Archive Stores

Although MailStore Service Provider Edition creates new archive stores automatically, this can also be done manually as described in the following:

- Log on to the Management Console, if not already logged on.
- Click on *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Stores* tab.
- Click *Create Store*.
- Fill out the *Create Archive Store* form:



Create Archive Store

Please enter a meaningful name for the archive store. Examples: "Messages 2012" or "2012-01"

Name: 2016-12

☑ Archive new messages here

Internal Archive Store

□ Use different directories for database, content and search index

Base Directory: d:\spe\johndoe\Data\2016-12

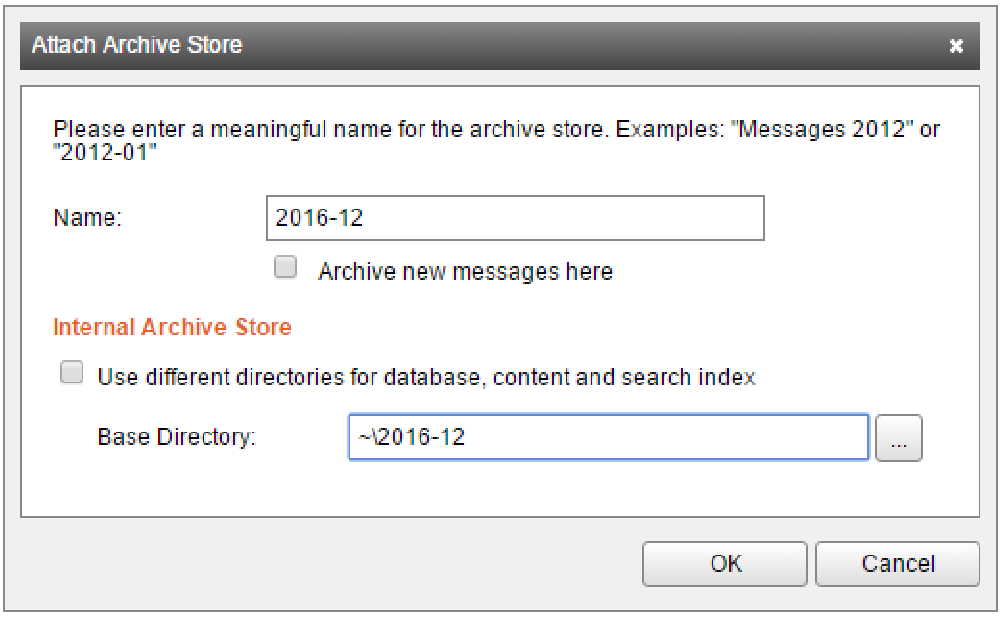
- **Name:** Meaningful name for the archive store.
- **Archive new messages here:** Enabled by default, new message will be archived in the newly created archive store if this option is checked.
- **Use different directories for database, content and search index:** If checked, a non-default directory structure can be used, e.g. the database and index directory may reside on a fast storage while the content resides in on a slower storage.
- **Directory:** Directory in which the new archive store will be created. A proposal is created from the *Name* of the archive store and the base directory of the instance. Use the tilde to point to a directory relative to the base directory of the instance, e.g. `~\Messages-2013-10`

- Click *OK* to create the new archive store.

Attach Existing Archive Store

Archive stores from MailStore Service Provider Edition instances or from on-premises MailStore Servers can be attached to an instance as described below:

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Stores* tab.
- Click *Attach Store*.
- Fill out the *Attach Archive Store* form:


Attach Archive Store

Please enter a meaningful name for the archive store. Examples: "Messages 2012" or "2012-01"

Name: 2016-12

□ Archive new messages here

Internal Archive Store

□ Use different directories for database, content and search index

Base Directory: ~\2016-12

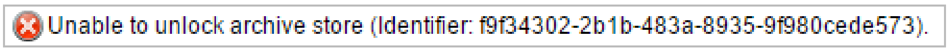
  - **Name:** Meaningful name for the archive store
  - **Archive new messages here:** If checked, new message will be archived in the newly created archive store. (default: unchecked)
  - **Use different directories for database, content and search index:** If checked, a non-default directory structure can be used, e.g. archive stores created before MailStore SPE/Server 10 do have the search index files located in the same directory as the database. So you have to activate this option and remove the \Index directory from the *Index Directory*-field.
  - **Base Directory:** Directory of the archive store to attach. This directory must contain the file "MailStoreFileGroup.fdb". Use the tilde to point to a directory relative to the base directory of the instance, e.g. `~/2016-12`.
- Click *OK* to attach the archive store.

Unlock Archive Stores

In case the archive store was migrated from MailStore Server 10 or newer to MailStore SPE, additional steps are required.

The archive store is protected with a recovery key

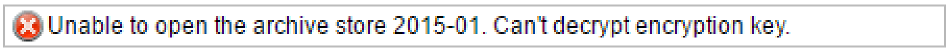
- The archive store cannot be loaded successfully and the note *Unable to unlock archive store (Identifier: <identifier>)* appears.


Unable to unlock archive store (Identifier: f9f34302-2b1b-483a-8935-9f980cede573).

- To finalize the migration of this archive store you need to know the recovery key identified by <identifier>, the instanceID of the instance where the archive store is attached to and the ID of the attached archive store.
- Navigate to *Navigation* > *DEVELOPER* > *Management API*. Select *UnlockStore* from the drop down menu and enter the *instanceID* of the instance, the *ID* of the archive store and the recovery key. The recovery key must be entered in lowercase letters.
- Click *Invoke*, *true* should appear below the text fields.
- Verify that the archive store was attached successfully.

The archive store is protected with a product key

- The archive store cannot be loaded successfully and the note *Unable to open the archive store <name>. Can't decrypt encryption key.* appears.



Unable to open the archive store 2015-01. Can't decrypt encryption key.

- To finalize the migration of this archive store you need to know the product key of the installation where the archive store was attached to last, the instanceID of the instance where the archive store is attached to and the ID of the attached archive store.
- Navigate to *Navigation* > *DEVELOPER* > *Management API*. Select *UnlockStore* from the drop down menu and enter the *instanceID* of the instance, the *ID* of the archive store and the product key. The product key must be entered in uppercase letters.
- Click *Invoke*, *true* should appear.
- Verify that the archive store was attached successfully.

More information about archive security can be found in the MailStore Server Service Configuration article [1].

Maintain FS Databases

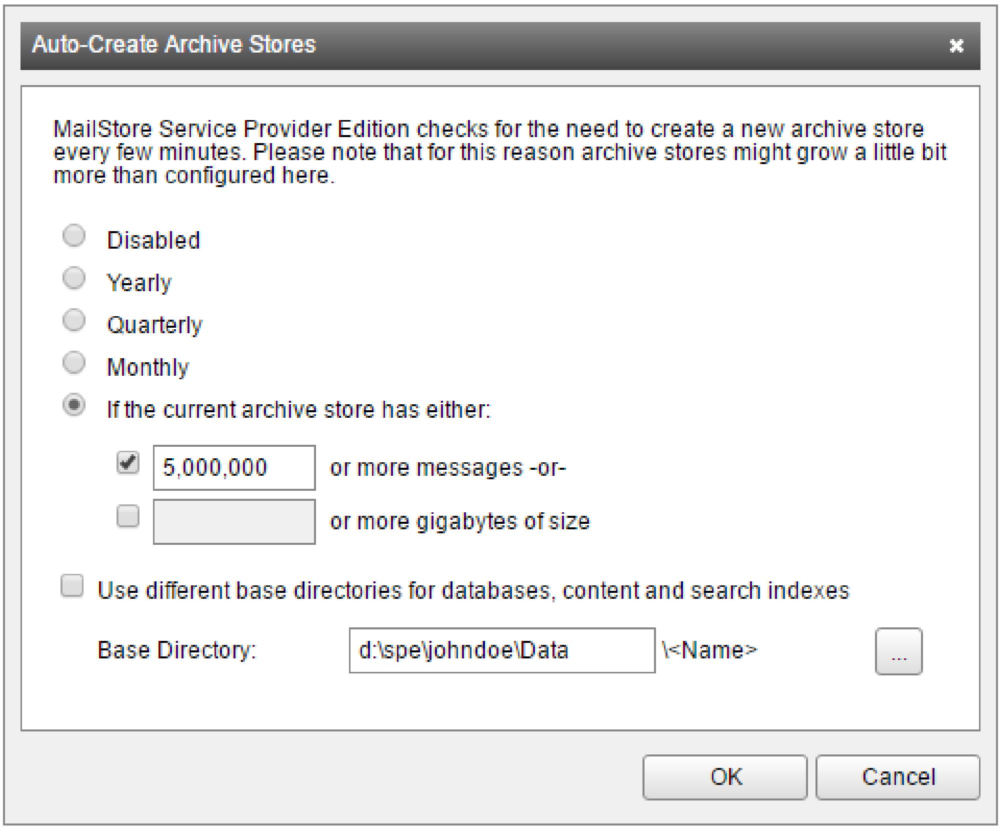
For storing meta data of the archive store's content embedded Firebird databases exist in every archive store. Under certain circumstances (e.g. after a disaster recovery of the server or storage) it might become necessary to perform a maintenance task on those databases. This can easily be done for all archive stores of a particular instance be following the instructions below:

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Stores* tab.
- Click *Maintain FS Databases* to start the maintenance.
- A progress windows will appear.
- Wait until the process is completed successfully and click *OK*. Otherwise click *Cancel* to interrupt maintenance process at any time.

Auto-Create Stores

MailStore Service Provider Edition automatically creates new archive stores every 5.000.000 messages. This setting can be adjusted to your need:

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Stores* tab.
- Click *Auto-create*.
- Adjust the settings in the *Auto-Create Archive Stores* dialog.



MailStore Service Provider Edition checks for the need to create a new archive store every few minutes. Please note that for this reason archive stores might grow a little bit more than configured here.

○ Disabled

○ Yearly

○ Quarterly

○ Monthly

● If the current archive store has either:

☑ 5,000,000 or more messages -or-

□ or more gigabytes of size

□ Use different base directories for databases, content and search indexes

Base Directory: d:\spe\johndoe\Data \<Name>

Important notice: Non-optimal settings can have a negative impact on the overall performance of the instance.

- Click *OK* to save the settings.

Store Commands

Advanced store commands are accessible by following these steps:

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Stores* tab.
- Select an archive store and click on *Store Commands* or right-click on an archive store to open a context menu.

A summary of the available store commands can be found in the tables below:

Requested State

State	Description
Disabled	Disabled archive stores are not in use but the instance still knows about their existence. The content is not available to users or administrators while the archive store is disabled. This state is useful when moving archive stores to a new directory.
Write Protected	The content of write protected archive stores is available to users, but cannot be modified (e.g. delete or move messages, rename or move folders)
Normal	The content of archives store is available to users and can be modified if the user has the appropriate permission.
Current	Same as *Normal* but new messages will be archived in the archive store that is set to *Current*.

Commands

Command	Description
Detach	Detaches the selected archive store. The archive store can be re-attached by using the *Attach* function. Please note that the archive store's name and ID will not be retained when detaching and re-attaching. Therefore, when moving an archive store to a new location, disabling the the archive store and using *Set Path* afterwards is preferred over re-attaching.
Rename	Specify a new name for the archive store.
Set Path	Change the path of the archive store. The archive store must be disabled before changing the path. Please note that the file system directory must be moved manually to the new location before re-enabling the archive store.
Compact	Optimizes the data structures.
Upgrade	If an archive store from a MailStore Server 5 or older was attached to an instance, it is highly recommended to upgrade the archive store to the latest format by using this function. Upgrade process can be interrupted and continued at any time.
Verify	Verification of the data integrity between folder information and meta data as well as email headers, content and recovery records.
Recreate Recovery Records	Recreates broken recovery records of an archive store. Use *Verify* to verify the state of the recovery records.

Search Indexes

Additionally to container files storing the actual email content and the embedded Firebird databases used for storing meta information, a full-text index file is created for each archive that has emails stored in an archive store. By default the full-text index only included email bodies, but virtually any file type is supported (see *Configure*).

To access these functions, follow the instructions below:

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Stores* tab.
- Click *Search Indexes*.

The below functions are available in the search index menu to configure and maintain the full-text indexes of an instance.

Rebuild Broken Indexes

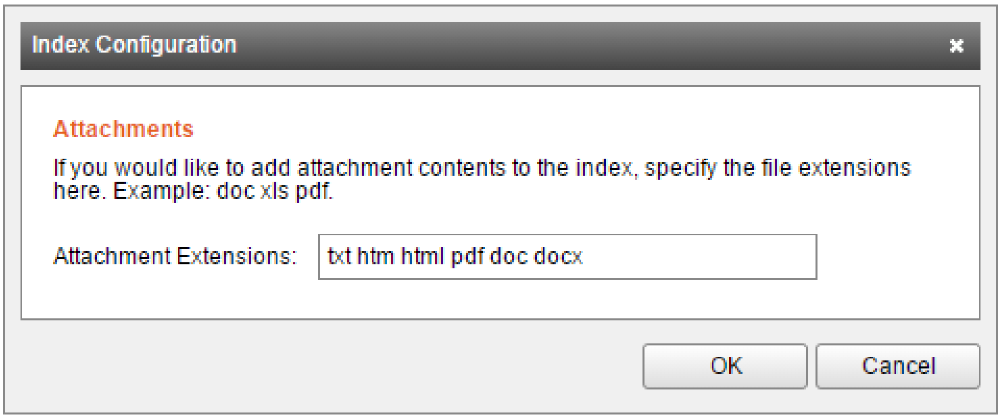
Starts a rebuild of all search indexes across all archive stores that are marked as broken.

Rebuild All Indexes

Starts a rebuild of all search indexes in all archives stores. This is usually only required after making changes to the list of attachment extensions to be included in the full-text index.

Configure

Specify a list of file extensions for attachments to be included in the full-text index. MailStore Service Provider Edition can index all file types for which a so-called IFilter driver is installed on the instance host on which the MailStore instance is running. The list of file extensions has to be separated by space.



Attachments

If you would like to add attachment contents to the index, specify the file extensions here. Example: doc xls pdf.

Attachment Extensions: txt htm html pdf doc docx

Under the name Microsoft Office 2010 Filter Packs [2] Microsoft offers a package that, additionally to all legacy as well as recent Microsoft Office Formats, supports the Open Document Format (OpenOffice/LibreOffice). For indexing PDF files the Adobe Reader or Adobe PDF iFilter [3] must be installed on the instance host. Further background information about the IFilter system itself as well as links to additional IFilter drivers can be found in the corresponding Wikipedia article IFilter.

Important Notices:

- Take note of the installation instructions [3] of the 64bit IFilter. Especially adding the *bin* folder of the IFilter installation folder to the *PATH* system variable increases indexing speed a lot. The *PATH* system variable can be adjusted via an administrative command prompt (cmd) and then rundll32 sysdm.cpl,EditEnvironmentVariables
- Newer versions of Adobe Acrobat Reader do not contain an IFilter. Thus, please deactivate the automatic update function of Adobe Acrobat Reader 11.

For reasons of stability and performance, MailStore Service Provider Edition processes the following file types directly, regardless of the IFilter drivers that are installed:

- Text files (TXT)
- HTML files (HTM and HTML)

Archive Access

The *Archive Access* tab provides access to the service provider archive access as well as download links for the client and Outlook Add-in.

Please note: Details about the logon process for customers and their end users can be found in the article End User Access.

Enable or Disable Service Provider Archive Access

Service provider archive access is only necessary if the administration of the instance is not done by the customers or if the customer requests support from the service provider. To enable or disable service provider access follow these instructions:

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Access* tab.
- Click either *Enable* or *Disable*
- When enabling click *OK* to confirm that the service provider archive access really should be enabled.

  Please notice: Enabling the service provider archive access is logged in the audit log of the instance.

Using Service Provider Archive Access

Before the service provider archive access can be used, this access method must be enabled (see previous section) and the client must be installed on the computer from where you want to connect.

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Access* tab.
- Click *Open Client*
- Depending on your web browser's settings further security related questions may appear.
- Afterwards the client will automatically log on to the instance using the special *$archiveadmin* system account and a one-time password.

Inside the Instance

No matter whether logging on to an instance as the customer's administrator or as service provider via service provider archive access, the available functions of the MailStore Client are nearly the same. Only accessing and or modifying the archive content (e.g. creating folders, deleting messages,..) is prohibited for the *$archiveadmin* user.

Please refer to Instance Administration to get an overview of the functions available inside each individual instance, such as managing users and setting up archiving and how these relate to the on premises solution MailStore Server.

Live Statistics

The *Live Statistics* tab shows real time graphics about the instance activity such as I/O, memory and CPU usage as well as number of Remote Procedure Calls (RPC) and the number of emails verified and archived by the instance's archiving mechanism.

Quellennachweise

[1] https://help.mailstore.com/en/server/MailStore_Server_Service_Configuration#Security_and_Encryption

[2] http://www.microsoft.com/en-us/download/details.aspx?id=17062

[3] http://www.adobe.com/support/downloads/detail.jsp?ftpID=5542

3.4 Instance Administration

The core functionality of an instance is identical to that of an on-premises MailStore Server. Therefore, this article is a collection of links to the corresponding section of the MailStore Server help.

Archive Email

Emails can be archived from the mailboxes of email servers such as Microsoft Exchange as well as from the locally installed email clients of the users. Dependent on its type, archiving tasks can be performed continuously, manually or based on a schedule.

If you are not sure which archiving method best suits your company, please refer to chapter Choosing the Right Archiving Strategy.

In chapter Email Archiving with MailStore Basics you can find out more about working with archiving profiles, archiving specific folders, deleting emails after archiving and automating the archiving process.

Email Servers

A large collection of email servers is supported by MailStore for archiving email. As the actual procedure of setting up archiving depends on the email server you are using, specific instruction for well-known email servers are provided in our Implementation Guides below:

Please note: For various reasons, not all email servers and archiving strategies are fully supported in MailStore SPE (e.g. Gmail, MailStore Proxy). When in doubt, contact our technical support.

- Microsoft Exchange Online / Microsoft 365 (Modern Authentication)
- Microsoft Exchange 2019
- Microsoft Exchange 2016
- Microsoft Exchange 2013
- G Suite
- Gmail
- MDaemon Email Server
- Kerio Connect (Kerio MailServer)
- IceWarp Server
- Archiving Emails Without Your Own Emailserver (e.g. Hosted Exchange or POP3/IMAP-mailbox provided by an ISP)
- Linux-based Email Server
- Intra2net Appliance Pro / Business Server
- hMailServer
- SmarterMail
- Tobit David.fx
- Zimbra Collaboration Suite

Legacy Implementation Guides

The following Implementation Guides should be considered deprecated. They are either referring to email servers that are no longer maintained by the vendor or have not received updates for years, or there have been major changes in MailStore Server that make them obsolete. Though archiving with MailStore Server should still work in most cases, the documentation is no longer updated and providing technical support may be limited.

- Microsoft Exchange Online / Microsoft 365 (Basic Authentication)
- Microsoft Exchange 2010
- Microsoft Exchange 2007
- Microsoft Exchange 2003
- Kolab
- Scalix

For IMAP and POP3 servers, that are not listed above, the following generic instruction might be helpful:

- Archiving Single Mailboxes
- Archiving Multidrop Mailboxes
- Batch-archiving IMAP Mailboxes

Email Clients

Archiving Email from Outlook, Thunderbird and Other E-mail Clients

As opposed to all other archiving features, it is imperative that the E-mail Archive Client software is installed on the user computers when archiving emails from these users' email applications. Once the archiving task is set up, it can be started manually by the user or executed automatically according to a schedule. Additional information about this topic is available in chapter Archiving Email from Outlook, Thunderbird and others.

Email Files

Archiving Outlook PST Files

As administrator, you can archive Microsoft Outlook PST files for other MailStore users. Additional information about these topics is available in chapter Archiving Outlook PST Files Directly.

Archiving EML or MBOX Files

As administrator, you can archive emails from .eml or .msg files for other MailStore users. Additional information about these topics is available in chapter Archiving Emails from External Systems (File Import).

Export Email

MailStore provides several functions regarding the export of archived emails. Emails can be exported directly into server mailboxes, or to the file system as individual email files (EML or MSG format), for example.

Find detailed instruction in the Exporting Email article of the MailStore Server Help.

Please note: Backup strategies (a backup of the entire archive) are discussed separately in the article Backup and Restore.

Administrative Tools

The *Administrative Tools* provides access to the following settings:

Users and Privileges

- Users
- **Directory Services**
  - Active Directory
  - Application Integration
  - Google Apps
  - IceWarp Server
  - Kerio Connect
  - LDAP Generic
  - Office 365
- Privileges
- Archives

Compliance

- Compliance General
- Auditing
- Audit Log

Management API

- Command Prompt
- Jobs
- Job Results

Miscellaneous

- SMTP Settings
- Active Sessions

3.5 Management Console - Infrastructure

Additionally to the Management Server a MailStore Service Provider Edition infrastructure consist of one or more Instance Hosts and Client Access Servers. Management of Instance Hosts and Client Access Server is done in the *Infrastructure* section of the Management Console.

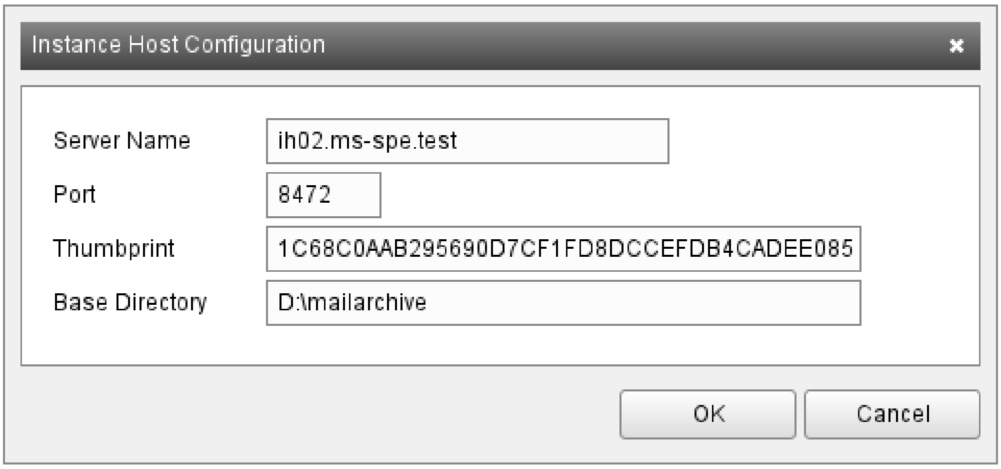
Instance Hosts

The *Instance Hosts* page shows a list of available Instance Hosts that are registered in the Management Server.

Adding New Instance Hosts

New Instance Hosts can be added to the MailStore Service Provider Edition either by pairing via the MailStore Service Provider Edition Configuration tool as described in Multi Server Mode Setup or manually as described in the following:

- Log on to the Management Console.
- Click on *Infrastructure* > *Instance Hosts*.
- Click *Add Instance Host*.
- Fill out the *Instance Host Configuration* form:



Instance Host Configuration

Server Name: ih02.ms-spe.test
Port: 8472
Thumbprint: 1C68C0AAB295690D7CF1FD8DCCEFDB4CADEE085
Base Directory: D:\mailarchive

  - **Server Name:** Must match the fully qualified host name of the Instance Host server.
  - **Port:** The TCP port on which the Instance Host listens for incoming connection from the Management Server and Client Access Servers (default: 8472)
  - **Thumbprint:** The SSL thumbprint of the certificate used by the Instance Host to identify itself. Execute the *Management API* command *GetServiceStatus* and search for the item which has `"serverType" : "managementServer"` set. The thumbprint value can be found in the *serverCertificate* key of the item.
  - **Base Directory:** Default directory for all newly created instances on the Instance Host. Can be overwritten individually for each new instance.
- Click *OK* to add the new Instance Host or *Cancel* to abort.

Configuring Instance Hosts

- Log on to the Management Console.
- Click on *Infrastructure* > *Instance Hosts*.
- Select the Instance Host to be modified from the list.
- Click on *Commands* > *Configure..*
- Change one or more of the following setting in the *Instance Host Configuration* dialog:
    - **Port:** The TCP port on which the Instance Host listens for incoming connection from the Management Server and Client Access Servers (default: 8472)
    - **Thumbprint:** The SSL thumbprint of the certificate used by the Instance Host to identify itself. Execute the *Management API* command *GetServiceStatus* and search for the item which has `"serverType" : "managementServer"` set. The thumbprint value can be found in the *serverCertificate* key of the item.
    - **Base Directory:** Default directory for all newly created instances on the Instance Host. Can be overwritten individually for each new instance.
- Click *OK* to save changes or *Cancel* to discard.

Removing Instance Hosts

In case an Instance Host should be removed from the MailStore Service Provider Edition environment, proceed as follows:

- Log on to the Management Console.
- Click on *Infrastructure* > *Instance Hosts*.
- Select the Instance Host to be removed from the list.
- Click on *Commands* > *Remove*
- Click *OK* to confirm the deletion of Instance Host or *Cancel* to abort.

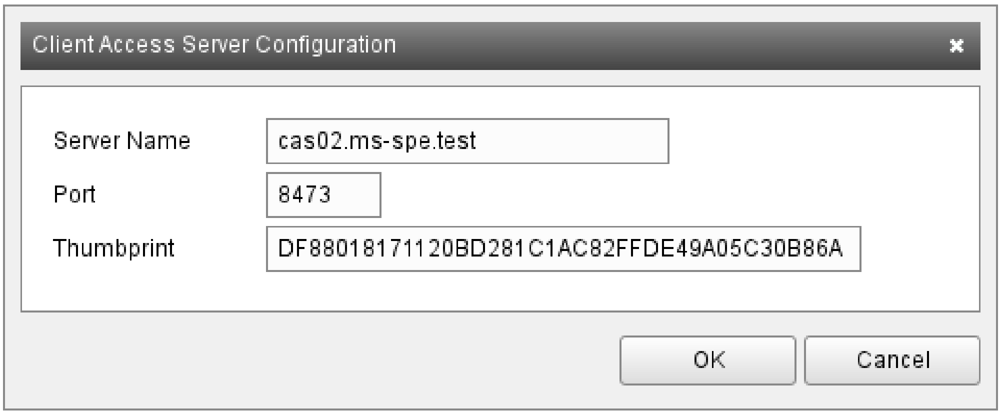
Client Access Servers

The *Client Access Servers* page shows a list of available Client Access Server that are registered in the Management Server. Additionally the current status of the network services provided by the Client Access Servers are shown.

Adding New Client Access Servers

New Client Access Server can be added to the MailStore Service Provider Edition either by pairing via the MailStore Service Provider Edition Configuration tool as described in Multi Server Mode Setup or manually as described in the following:

- Log on to the Management Console.
- Click on *Infrastructure* > *Client Access Servers*.
- Click *Add Client Access Server*.
- Fill out the *Client Access Server Configuration* form


Client Access Server Configuration

Server Name: cas02.ms-spe.test

Port: 8473

Thumbprint: DF88018171120BD281C1AC82FFDE49A05C30B86A

- **Server Name:** Must match the fully qualified host name of the Client Access Server's server.
- **Port:** The TCP port on which the Client Access Server listens for incoming connection from the Management Server (default: 8473)
- **Thumbprint:** The SSL thumbprint of the certificate used by the Client Access Server to identify itself. Use the MailStore Service Provider Edition Configuration tool on the Client Access Server to retrieve the thumbprint from the *TCP Server Certificate* field.

- Click *OK* to add the Client Access Server or *Cancel* to abort.

Configuring Client Access Servers

- Log on to the Management Console.
- Click on *Infrastructure* > *Client Access Servers*.
- Select the Client Access Server to be modified from the list.
- Click on *Commands* > *Configure...*
- Change one or more of the following setting in the *Client Access Server Configuration* dialog:
  - **Port:** The TCP port on which the Client Access Server listens for incoming connection from the Management Server (default: 8473)
  - **Thumbprint:** The SSL thumbprint of the certificate used by the Client Access Server to identify itself. Use the MailStore Service Provider Edition Configuration tool on the Client Access Server to retrieve the thumbprint from the *TCP Server Certificate* field.
- Click *OK* to save changes or *Cancel* to discard.

Removing Client Access Servers

In case a Client Access Server should be removed from the MailStore Service Provider Edition environment, proceed as follows:

- Log on to the Management Console.
- Click on *Infrastructure* > *Client Access Servers*.
- Select the Client Access Server to be removed.
- Click *Commands* > *Remove*.
- Click *OK* to confirm the deletion of the Client Access Server or *Cancel* to abort.

3.6 Management Console - Security

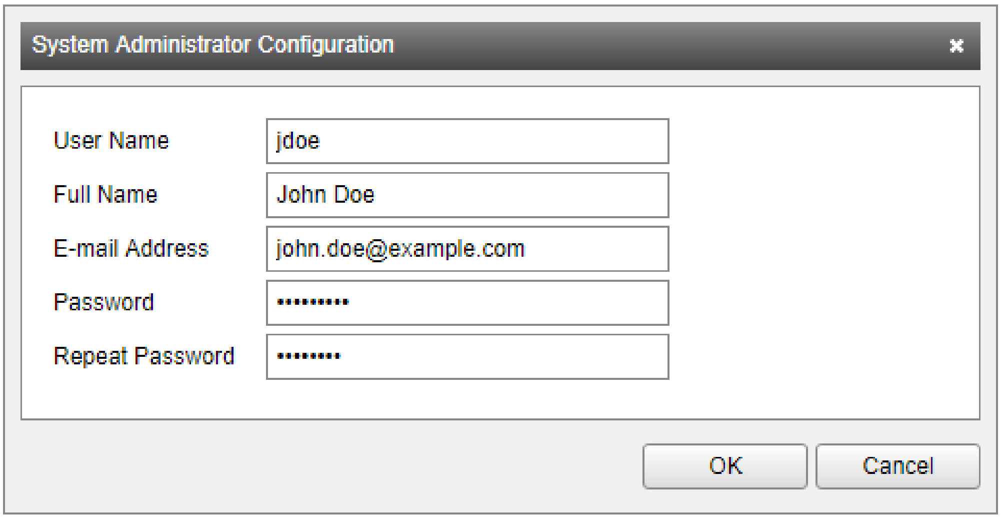
System Administrators

System administrators have the ability to log on to the Management Console and therefore have full administrative privileges.

Creating System Administrators

To create a new system administrator follow these steps:

- Log on to the Management Console.
- Click on *Security* > *System Administrators*.
- Click *Create System Administrator*.
- Fill out the *System Administrator Configuration* form:



System Administrator Configuration

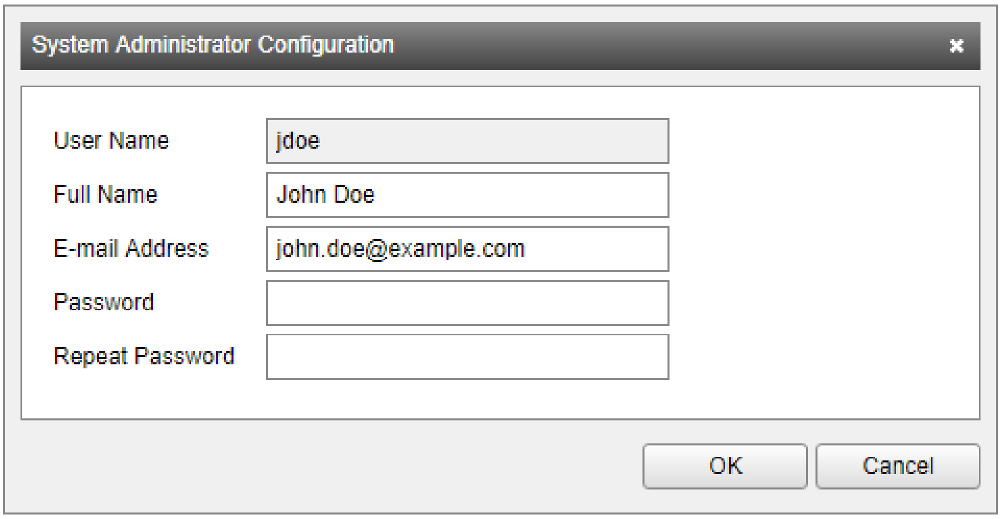
User Name	jdoe
Full Name	John Doe
E-mail Address	john.doe@example.com
Password	•••••••••
Repeat Password	••••••••

  - **User Name:** User name of the system administrator used for logging on to the Management Console.
  - **Full Name:** Full name of the system administrator.
  - **E-mail Address:** E-mail address of the system administrator.
  - **Password:** Password of the system administrator.
  - **Repeat Password** Password confirmation.
- Click *OK* to create the new system administrator.

Configuring System Administrators

To modify an existing system administrator follow these steps:

- Log on to the Management Console.
- Click on *Security* > *System Administrators*.
- Select the system administrator to modify.
- Click on *Commands* and select *Configure...*.
- Fill out the *System Administrator Configuration* form:



User Name	jdoe
Full Name	John Doe
E-mail Address	john.doe@example.com
Password	
Repeat Password	

  - **Full Name:** Full name of the system administrator.
  - **E-mail Address:** E-mail address of the system administrator.
  - **Password:** Password of the system administrator.
  - **Repeat Password** Password confirmation.
- Click *OK* to save changes or *Cancel* to discard.

Deleting System Administrators

To delete an existing system administrator proceed as follows:

- Log on to the Management Console.
- Click on *Security* > *System Administrators*.
- Select the system administrator to delete.
- Click on *Commands* > *Delete*.
- Click *OK* to confirm the deletion of the system administrator or *Cancel* to abort.

3.7 Management Console - Developer

Management API

The *Management API* page of the Management Console provides access to all available API functions. This allows developers to find out which functions exist and what parameters are expected.

For each parameter its name is shown followed by an input field and the expected data type after selecting a function from the drop down list.

Further details about the Management API are available in the Management API chapter.

3.8 Accessing Instances

The *Archive Access* tab provides access to the service provider archive access as well as download links for the client and Outlook Add-in.

Please note: Details about the logon process for customers and their end users can be found in the article End User Access.

Enable or Disable Service Provider Archive Access

Service provider archive access is only necessary if the administration of the instance is not done by the customers or if the customer requests support from the service provider. To enable or disable service provider access follow these instructions:

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Access* tab.
- Click either *Enable* or *Disable*
- When enabling click *OK* to confirm that the service provider archive access really should be enabled.

  Please notice: Enabling the service provider archive access is logged in the audit log of the instance.

Using Service Provider Archive Access

Before the service provider archive access can be used, this access method must be enabled (see previous section) and the client must be installed on the computer from where you want to connect.

- Log on to the Management Console, if not already logged on.
- Click *General* > *Instances*.
- Open the instance details by clicking on a running instance in the list.
- Click on the *Archive Access* tab.
- Click *Open Client*
- Depending on your web browser's settings further security related questions may appear.
- Afterwards the client will automatically log on to the instance using the special *$archiveadmin* system account and a one-time password.

4

Kapitel

Post Installation Tasks

4.1 End User Access

The logon process for customers to administrate their MailStore Instance or to access their archives varies slightly from the logon process of an on-premises MailStore Server.

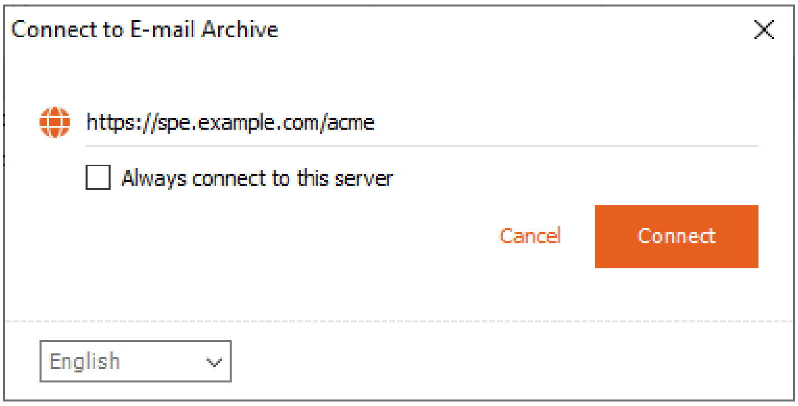
Find detailed information about logging in with E-mail Archive Client and E-mail Archive Add-in for Outlook below. Additionally find information about how to log on to Web Access using a web browser or the integrated IMAP server using any IMAP capable email client.

As both applications are identical to MailStore Client and MailStore Outlook Add-in, their system requirements [1] can be found in the MailStore Server help.

E-mail Archive Client

Customers' administrators can access their own MailStore Instance with the E-mail Archive Client by using the credentials received from their service provider. End users can use the same client to archive or export email or to access their archived email. Follow the instructions below for logging on with E-mail Archive Client:

- Open the E-mail Archive Client by using the link *E-mail Archive* on the desktop.
- Select the preferred language from the *Language* drop down list and enter the URL to connect to in the *Server Name* field. The URL must be in the format `https://<fqdn_of_cas>/<instance_id_or_alias>`.



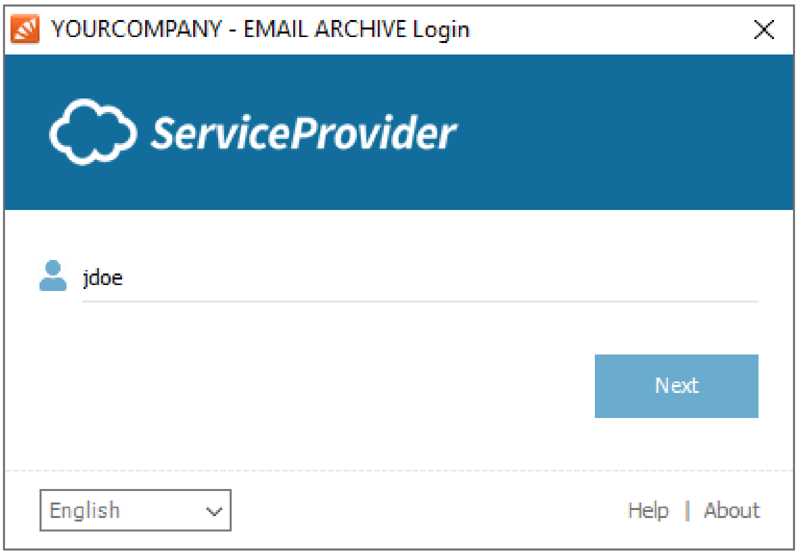
https://spe.example.com/acme

□ Always connect to this server

English

Hint: The language and server name can be saved to skip this step in the future by activating the *Always connect to this server* option. To change the settings again, start E-mail Archive Client while keeping the `SHIFT`-key pressed.

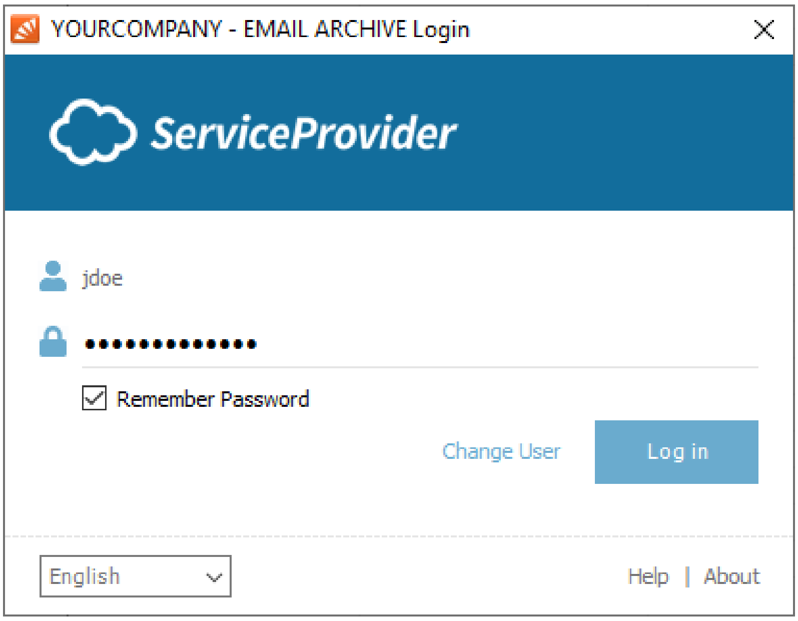
- Click *Connect* to connect.
- The E-mail Archive Client will update itself to become compatible with the provider's version of MailStore Service Provider Edition if necessary.
- Enter your username.



YOURCOMPANY - EMAIL ARCHIVE Login

jdoe

- Click *Next* to continue.
- The MailStore Instance now determines how the user is to be authenticated.
  - If the instance is able to verify the user's credentials itself, the password dialog appears. Enter the password into the *Password* field and click on *Log in*



YOURCOMPANY - EMAIL ARCHIVE Login

jdoe

•••••••••••••

☑ Remember Password

  - If the user has been synchronized from Microsoft 365 or Google G Suite, the default web browser will be opened to allow authentication through Microsoft's or Google's authentication service.

E-mail Archive Add-in for Outlook

- Open Microsoft Outlook.
- If the E-mail Archive Add-in for Outlook is not pre-configured, you will be asked to log in to your MailStore Instance as soon as you click any button of the E-mail Archive Add-in for Outlook.
- Enter the URL to connect to in the *Server Name* field. The URL must be in the format `https://<fqdn_of_cas>/<instance_id_or_alias>`.
- Click *Connect* to continue.
- Enter your username in the *User Name* field and click *Next* to continue.
- The MailStore Instance now determines how the user is to be authenticated.
  - If the instance is able to verify the user's credentials itself, the password dialog appears. Enter the password into the *Password* field and click on *Log in*
  - If the user has been synchronized from Microsoft 365 or Google G Suite, the default web browser will be opened to allow authentication through Microsoft's or Google's authentication service.

Web Access

End users can access their archived email easily via any supported web browser, by following the instructions below. Mobile devices are supported.

- Open a web browser.
- Navigate to Web Access. The URL is `https://<fqdn_of_cas>/<instance_id_or_alias>`.
- Enter your username in the *User Name* field and click *Next* to continue.
- The MailStore Instance now determines how the user is to be authenticated.
  - If the instance is able to verify the user's credentials itself, the password dialog as shown below appears. Enter the password into the *Password* field and click on *Log in*
  - If the user has been synchronized from Microsoft 365 or Google G Suite, the web browser will be redirected to allow authentication through Microsoft's or Google's authentication service.

IMAP Client

Archived emails can be accessed via an integrated IMAP server with any IMAP capable email client using the following settings.

When using Microsoft or Google to authenticate users at login, accessing the archive via IMAP is not possible for technical reasons.

- **Incoming Mail Server** - Host name or IP address of a Client Access Server
- **Port** - For STARTTLS-encrypted connections (explicit TLS) standard IMAP port 143 is used. For implicit TLS encrypted connections standard IMAP port 993 is used. Login over unencrypted connections is not supported.
- **User Name** - Name of the MailStore user prepended by his instance id or alias `<instance_id_or_alias>/<username>`, e.g. `jdcorp/jon.doe`.
- **Password** - Password which is required for accessing the MailStore instance.

Please note: In addition to configuring the incoming mail server, email clients often require configuring the outgoing mail server as well. In this case, using the same data as for an existing email account will facilitate further processing emails from the email archive.

Quellennachweise

[1] https://help.mailstore.com/en/server/System_Requirements

4.2 Branding

The appearance of MailStore Client, MailStore Web Access, and MailStore Outlook Add-in can be customized easily to match your corporate design.

Modify and Activate Branding

Follow the instructions below to apply your own branding:

- Open Windows Explorer on the Management Server.
- Navigate to the *config* subdirectory of the MailStore Service Provider Edition installation. (Default: `%PROGRAMFILES%\MailStore Infrastructure\config`).
- Create a new folder named `Branding`.
- Store all files necessary for branding in this newly created folder. Find further details about the branding parameters in Client Branding and Web Branding below.

  Important notices: The dimensions of the images must remain unchanged and no syntax errors must be made when editing JSON files. If necessary, test the JSON files at http://jsonlint.com/.Sample files can be found in the 'Branding.sample' folder located in the *config* subdirectory. The *about.html* file needs to have an UTF-8 BOM (byte order mark) or else it cannot be loaded.
- Log on to the Management Console, if not already logged on.
- Navigate to *Navigation* > *Developer* > *Management API* and select *ReloadBranding* from the drop down menu then press *Invoke* to activate the new branding.

Limitations

Some parts of the Client and Outlook Add-in cannot be branded as they are an integral part of the digitally signed installer packages (e.g. program icons) or are used at an early stage, where no branding information is available yet, like the *Connect to E-mail Archive dialog*.

Client Branding

The following table provides information about the fields available for MailStore Client branding stored in `ClientBranding.json`.

Name	Description
`clientName`	Name of the client application, e.g. "YOURCOMPANY - EMAIL ARCHIVE"
`helpUrl`	URL to be opened when clicking on help in client.
`loginHeaderImage_410x81_png`	Header image for login dialog. Required dimension: width: 410px; height: 81px
`headerBackgroundColor`	Background color of header, e.g. "#126d9c"
`headerLeftImage_autox95_png`	Left header image. Required dimension: width: auto; height: 95px
`headerRightImage_autox95_png`	Right header image. Required dimension: width: auto; height: 95px
`about_html`	HTML file containing the about site.
`watermarkImage_300x150_png`	Watermark image. Required dimension: width: 300px; height: 150px
`gatewayName`	Custom name that the MailStore Gateway archiving profile is listed under.

Web Branding

The following table provides information about the fields available for MailStore Web Access and MailStore Outlook Add-in branding stored in `WebBranding.json`.

Name	Description
`webName`	Name of the web application, e.g. "YOURCOMPANY - EMAIL ARCHIVE WEB ACCESS"
`webAbout_html`	HTML file containing the about site.
`webRoot_html`	HTML file to be used when no in instance was given in the URL.
`webHelpUrl`	URL to be opened when clicking on help in web access.
`webLoginHeaderImage_410x81_png`	Header image for login dialog. Required dimension: width: 410px; height: 81px
`webHeaderBackgroundColor`	Background color of header, e.g. "#126d9c"
`webHeaderBackgroundImage_autox36_png`	Header header image. Required dimension: width: auto; height: 36px
`outlookAddinName`	Name of the Outlook Add-in, e.g. "YOURCOMPANY - EMAIL ARCHIVE ADD-IN".
`outlookAddinHelpUrl`	URL to be opened when clicking on help in Outlook Add-in.
`watermarkImage_300x150_png`	Watermark image. Required dimension: width: 300px; height: 150px
`favicon_ico`	Favicon in 16x16, 32x32, 64x64 pixel.
`favicon_png`	Favicon in 196x196 pixel in PNG format.
`highlightColor`	Color used for section titles, buttons and other controls, e.g. "#6aabce".

4.3 Replace Self-signed SSL Certificates

MailStore Service Provider Edition automatically creates self-signed certificates when adding a new role to a server. While these certificates are suitable for authenticating MailStore Service Provider Edition's own services against each other by storing and verifying the unique fingerprints of the used certificates, self-signed certificates are not suitable for public internet services like email or web servers.

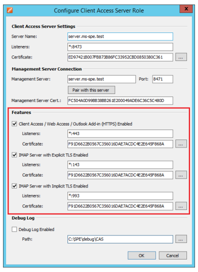
Therefore it is recommended to replace the SSL certificates used by the Client Access Servers for offering IMAP and web based access to the archives with certificates signed by an official certificate authority. Information on requesting, renewing and working with such certificates can be found in this article.

Prerequisites

Before a certificate can be used by the Client Access Server service, the certificate and its private key must be stored in the computer's personal/MY certificate store (**not** Administrator's or any other user's).

Installing New Certificates

- Start the MailStore Service Provider Edition Configuration tool on a server that is a Client Access Server by double-clicking it's desktop icon. On Windows Server Core use the command line prompt to start the executable (default: `%PROGRAMFILES%\MailStore Infrastructure\MailStoreInfrastructureConfig.exe`.
- Stop the *Client Access Server*.
- Click *Configure...*
- For each endpoint in the *Features* section (HTTP, IMAP, IMAPS) click on the button behind the *'Certificate* field to select the new certificate from the Windows certificate store.



Configure Client Access Server Role

Client Access Server Settings

Server Name: server.ms-spe.test

Listeners: *:8473

Certificate: ED97421B007FB873B86FC33952CBD0850380C361

Management Server Connection

Management Server: server.ms-spe.test Port: 8471

Management Server Cert.: FC504A0D99BB38BB261E200049ADE6C36C5C480D

Features

☑ Client Access / Web Access / Outlook Add-in (HTTPS) Enabled

Listeners: *:443

Certificate: F91D6622B0567C356016DAE7ACDC4E2E645F868A

☑ IMAP Server with Explicit TLS Enabled

Listeners: *:143

Certificate: F91D6622B0567C356016DAE7ACDC4E2E645F868A

☑ IMAP Server with Implicit TLS Enabled

Listeners: *:993

Certificate: F91D6622B0567C356016DAE7ACDC4E2E645F868A

Debug Log

□ Debug Log Enabled

Path: C:\SPE\debug\CAS

Please note

> **It is not required to replace the *Certificate* under the *Client Access Server Settings*. If you would change this certificate, you also have to pair your *CAS* with the *Management Server* to gain trust again.**

- Click *OK* to save changes or *Cancel* to discard.
- Start the Client Access Server.

Repeat the above on each Client Access Server in your MailStore Service Provider Edition infrastructure.

4.4 Backup and Restore

Creating Backups

The management database as well as your branding data is stored in the *config* sub directory right below the program files directory of the MailStore Service Provider Edition (default: `C:\Program Files\MailStore Infrastructure`) on the Management Server. To be able to fully restore a MailStore Service Provider Edition installation, it is highly recommended to create regular backups of that *config* directory.

Even more important than the backup of the management database and branding are consistent backups of the MailStore Instances. These instances store their data in at least one directory on the disk, which is the base directory specified during initial creation of the instance. By default, automatically created archive stores are located in sub directories of the base directory, making it sufficient in most cases to only back up the content of the instance's base directory and all sub directories.

When the auto-create settings of archive stores have been modified, additional storage locations must be backed up along with the base directory.

Hint: The base directory contains a link *Debug Log* which points to `%PROGRAMDATA%\MailStore Infrastructure\Debug Log\<instanceID>`. It is usually not necessary to follow that link and backup the debug logs if any.

Depending on the environment, backup capacity, backup locations or the backup software in use, different methods might be available for backing up MailStore Instances. The following provides an overview of the most commonly used backup methods and how they cope with the requirement of creating consistent backups.

File Based Backups

While file based backups solutions are good for backing up independent files, they are usually not suitable for creating consistent backups of MailStore Instances as their data is spread across multiple rapidly changing files.

In order to create consistent backups with file based backup tools, it is required to either freeze and thaw (see #Prepare Instance For Snapshot via API Commands or shutdown and restart each instance that is to be backed up. As the instances must remain shut down for the time of the backup, this typically results in long downtimes during which the instances are neither able to archive new email nor provide end user access to the archived data.

Storage Snapshots

When using Volume Shadow Services (VSS) or other methods of creating snapshots on storage level, it is necessary to ensure that all files used by the instances are closed before the snapshot is created. This can either be achieved by enabling VSS support in the instances themselves or by sending the appropriate API command prior to creating snapshots.

Enabling and Testing VSS Support

Each MailStore Instance provides a so-called Volume Shadow Service Writer (VSS Writer) for external backup software that uses the Microsoft Volume Shadow Service. The external backup software can use it to create consistent backups of the MailStore Instance's database and all archive stores. Whether this method succeeds, however, largely depends on the backup software which is used.

Before MailStore Instances react on VSS events, such support must be enabled in their advanced configuration first. Follow the steps below to enable VSS support for an instance and verify the result.

- Log on to the Management Console.
- Click on *General* > *Instances*.
- Select the instance to modify.
- Click on *Stop* if the instance is running.
- Click on *Configure...*.
- Open the *Advanced Configuration* tab.
- Check the *Enable VSS Writer* option.

- Click *OK* to save the changes.

Now start your VSS based backup and wait until it has finished. To verify that the appropriate VSS events were initiated in MailStore during the backup, open the Windows System Protocol in the event viewer on the Instance Host where the instance was previously backed up and search for the following events:

1. *A backup session has been started.*
2. *The archive has been frozen as a reaction on the OnPrepareSnapshot event.*
3. *The archive has been thawn as a reaction on the OnThaw event.*
4. *The backup session has been shut down.*

If these events cannot be found in the Windows System Protocol, no consistent snapshot using Volume Shadow Service was performed and your backup software obviously does not support the MailStore VSS writer. In that case try the API based method below.

Prepare Instance For Snapshot via API Commands

MailStore Instances can be frozen and thawed similar to using VSS by executing the corresponding API commands FreezeInstances and ThawInstances. Instances also can be stopped and started by executing the API commands StopInstances and StartInstances. The easiest way of executing API commands from other applications such as backup software is by using MailStoreManagementCmd.exe.

To learn how to execute commands before and after performing snapshots, please consult your backup software's documentation.

Full Virtual Machine Backups

Some backup solutions are highly integrated into virtualization solutions and allow to create and backup/replicate full snapshots of virtual machines. These type of snapshots not only contain the current state of the hard disks but also of the current main memory. Thus backups of full virtual machine snapshots can be considered as consistent.

Other Backup or Replication Methods

For questions regarding any other type of backup solutions such as block level replication, continuous backup, etc. please contact the vendor's support to find out whether their software is able to create consistent backups of whole directory structures.

Restoring Backups

Restoring Management Database and Branding

To restore the management database and branding data make sure that none of the MailStore Service Provider Edition roles (Management Server, Instance Host and Client Access Server) are running. Then restore the content of the *config* directory back into its original location (default: `C:\Program Files\MailStore Infrastructure`) and finally start the Management Server role again followed by the Instance Hosts and Client Access Server role.

Restoring Instances

As long as the instance configuration still exists in the management database on the Management Server, the restored data should be placed in the previous location which usually means in the base directory of the instance. Afterwards the instance can be started from the Management Console again.

If the instance configuration has been deleted from the management database, proceed as follows to restore an instance:

1. Create a new instance as described in Creating Instances. Its name does not necessarily need to match the previous name.
2. Open Windows Explorer and navigate to the base directory of the newly created instance.
3. Delete all files and directories from the base directory.
4. Now restore the data into the base directory of the newly created instance.
5. Finally start the instance.

4.5 Monitoring

Monitoring the MailStore Service Provider Edition can be carried our on various levels. While monitoring the underlying infrastructure, which typically includes network components, hardware usage or the status of security updates, is a common task for administrators, setting up further monitoring checks for the MailStore Service Provider Edition is recommended to ensure permanent service availability for end customers.

This article provides generic information about what should be monitored and partly explains how to do it, in order to help administrators setting up additional checks in their monitoring solution.

Management Server

Network Ports	TCP 8470 (Management Console/HTTPS) TCP 8471 (Management Server)
SSL Certificate Lifetime	TCP 8470 (Management Console/HTTPS) TCP 8471 (Management Server)
Windows Service	MailStoreManagementServer
Connectivity	Use Management API command GetServiceStatus to request all data that is used by the Management Console to create the dashboard's service health view, including all messages that are collected from the instances.
Licensing Information	Use Management API command CreateLicenseRequest to request data from which the periodic licensing request is derived.

Client Access Server

Network Ports	TCP 143 (IMAP) TCP 443 (HTTPS) TCP 993 (IMAPS) TCP 8472 (Client Access Server)
SSL Certificate Lifetime	TCP 143 (IMAP) TCP 443 (HTTPS) TCP 993 (IMAPS) TCP 8472 (Client Access Server)
Windows Service	MailStoreClientAccessServer

Instance Host

Network Ports	TCP 8473 (Instance Host)
SSL Certificate Lifetime	TCP 8473
Windows Service	MailStoreInstanceHost

Instances

Instance Status	Use the Management API command GetInstances to receive general information about instances (process ID, status, etc.), which may also be used to identify *MailStoreServer_x64.exe* processes for further monitoring.
Instance Statistics	Use the Management API command GetInstanceStatistics to receive statistics about disk usage and number of archived emails. **Important notice:** Do not run the GetInstanceStatistics command more often than absolutely necessary, as gathering the required data from the file system creates high I/O workload, which might impact the performance of all instance that reside on the same storage.
Service Provider Access	Use the Management API command GetArchiveAdminEnabled to check if the status of the service provider access matches the expected value for the instance.
Recent Results	Use the Management API command GetWorkerResults to get a list of recent results. For the popular Nagios/Icinga monitoring solution you can find further details about monitoring the worker results in MailStore Server's Monitoring Article. A special SPE version of the mentioned check scripts is available in the mentioned Scripting-Package **Please note:** As there can be several non-critical reasons for profiles to fail, it is recommended to define certain thresholds of how many execution per period are allowed to fail before reporting the whole check as failed.
User Archives	Use the Management API command GetFolderStatistics to get a list of all archives, the amount of messages and the size of each archive.

4.6 Enhancing SSL Security

The default configuration of most operating systems allow any set of supported ciphers and hashes to be used by applications when acting as SSL client or server. While this ensures full compatibility with other client and server applications, it does no longer match the expectation in SSL encrypted communication in regards to privacy and trust due to supporting insecure protocols, cipher suites and hash algorithms.

Thus enhancing the security of SSL mainly consists of disabling these insecure protocols, ciphers and hashes as well as prioritize cipher suites that allow the usage of Perfect Forward Secrecy.

As all components of the MailStore Service Provider Edition rely on Windows' security support provider (SSP) called *Secure Channel* (also known as *Schannel*), a number of registry keys have to be created or modified in order to disable insecure protocols, ciphers and hashes. Although Microsoft's article Transport Layer Security (TLS) registry settings [1] describes in detail which registry keys affect the security provider settings, it is not recommended to manually change these keys. A safer way to adjust the *Schannel* settings for server applications is Nartac Software's IIS Crypto [2] tool.

Recommended Settings

Highest level of security can be achieved with the following settings in *IIS Crypto*. In a multi-server setup of MailStore SPE, the changes should be applied to all servers with Management Server or Client Access Server role.

Protocols Enabled	TLS 1.1 TLS 1.2
Ciphers Enabled	AES 128/128 AES 256/256
Hashes Enabled	SHA SHA256 SHA384 SHA512
Key Exchange Enabled	Diffie-Hellman PKCS ECDH
SSL Cipher Suite Order	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

Quellennachweise

[1] https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

[2] https://www.nartac.com/