Installation and Deployment

HOPEX Aquila 6.2

MEGA

a Bizzdesign company

Information in this document is subject to change and does not represent a commitment on the part of MEGA International.

No part of this document may be reproduced, translated or transmitted in any form or by any means without the express written permission of MEGA International.

HOPEX Application Server (HAS) Architecture Overview

1. Foreword

The document describes the Logical Architecture and Infrastructure Architecture for the HOPEX Platform.

This document applies to HOPEX Application Server (HAS) Architecture deployment from HOPEX V5 onward. Check if a more recent version of this document is available via the online MEGA Community.

Other related documentations are available, see Other Technical Documentation.

The physical infrastructures provided in this document may be subjected to adjustments based on specific contexts. A specific study from MEGA R&D teams might be required.

1.1. What is HAS?

HAS stands for: **HOPEX Application Server**. HAS is the web platform that **runs**, **administrates** and **deploy** all solutions of MEGA, including **HOPEX**.

HAS is the Architecture deployment mode for HOPEX V5 onward.

1.2. What is HOPEX Store?

MEGA HOPEX Store is the online website that allows to download all the required components to install and deploy the HOPEX solutions.

The store is available here: https://store.mega.com

An **installation key** is required to proceed with the installation process. Please refer to your sales representative to get your installation key.

2. Logical Application Architecture

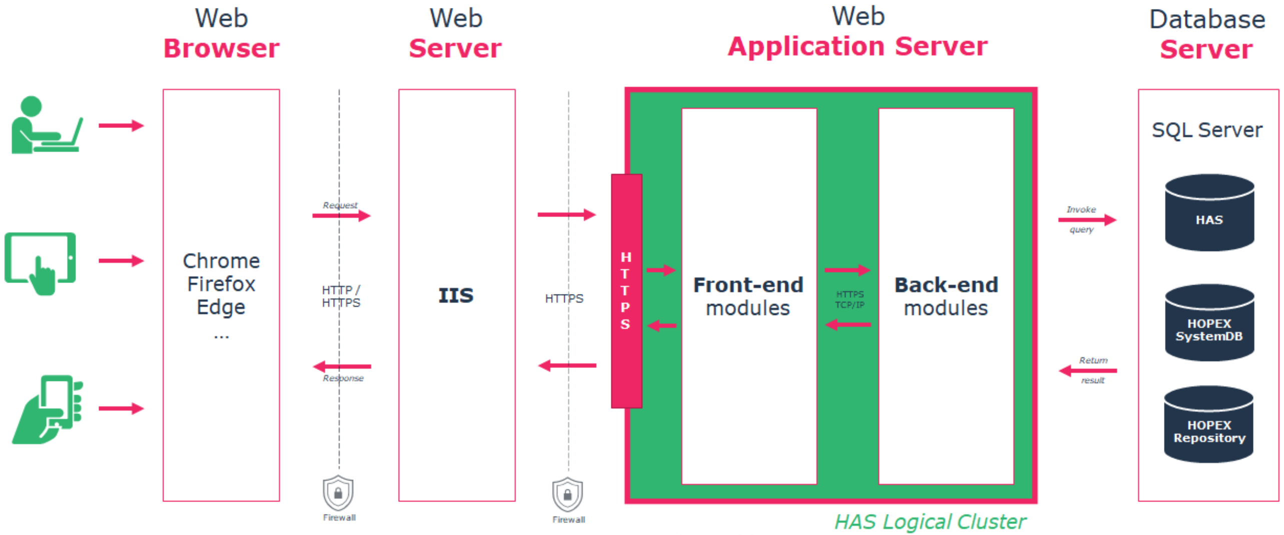
2.1. HAS Server

HOPEX Application Server, shortly named “HAS”, is based on a 3-tier web architecture principle including:

- a presentation tier: representing the web user interface. This layer is packaged as a **Front-end** module of web type. There might be several web front-end modules depending on the use case.
- an application tier: representing the business logic of the HOPEX platform. This layer is packaged as a **Back-end** module. The main module for the platform is called **HOPEX Core**.
- a Data tier: representing the persistence mechanisms of the data. This layer is provided by a market RDBMS.

As web application, the HOPEX solutions can be navigated using modern web browsers. The device used to browse the solutions depends on the Front-End module used and its compatibility with laptops, tablets, and mobiles.

The overall architecture of HAS is described in the following architecture view:



- Gateway
- SSL Certificate
- Load Balancer
- Cluster list
- Cluster Node list

- Various module type
- Several nodes in a cluster
- Enable smart allocation based on usage

Figure 1 HAS Architecture Overview

The Web HOPEX Application Server provides its own web server based on **Kestrel ASP.NET Core**

The technical name of HAS as a Windows process is **HAS.server.exe**.

2.2. HAS Modules

2.2.1. Module overview

The embedded application web server is organized to work with a group of modules that deliver technical or business services.

Technical Classification	Purposes
System	These modules are the required system modules for the service to be up and running. They include authentication, clustering, monitoring…
Back-end	These are the modules that perform all the business logics and interact with the database to store information. These modules are called by the front-end modules.
Front-end	These are the modules that expose web front-end part. After identification, these modules can be accessed by the user web interface or by API.

HAS embeds all the modules in its web architecture. It will manage:

- Start/Stop: to Start or Stop the required modules and ensure the application is up and running.
- Restart: to avoid failover HAS manages the restart of the appropriate modules.

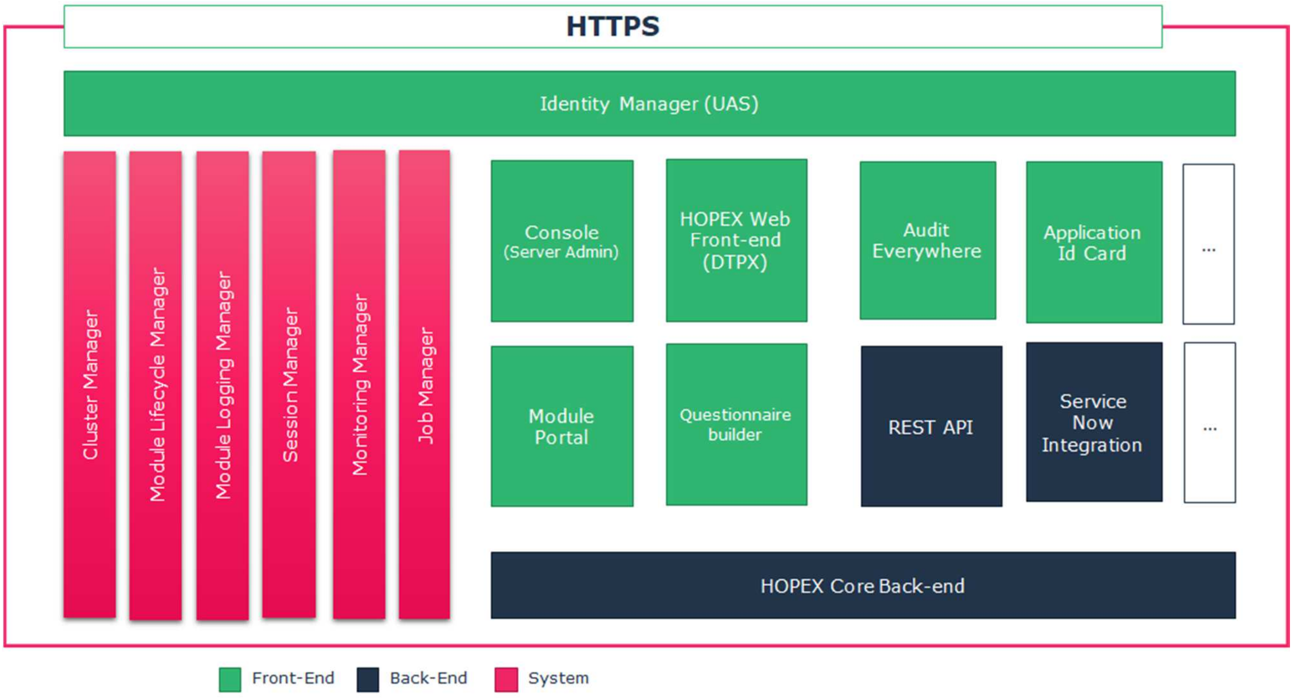


Figure 2 HAS Modules Overview

2.2.2. System modules

These modules are technical and are a prerequisite for the application to run. They can appear as dedicated modules or as part of HAS Server.

Module	Process Name	Purposes
Identity Manager	HAS.Modules.UAS.exe	This module manages the authentication workflow. This module can be configured to support various SSO configurations.
Console	HAS.Modules.Console.exe	It allows to manage the server installation from a web portal.
Cluster Manager	HAS.Server.exe	Ensures the synchronization of the physical installation across the logical cluster.
Job Manager	HAS.Server.exe	Ensures the treatment of the scheduled jobs and their execution in the appropriate node of the cluster.
Lifecycle Manager	HAS.Server.exe	Enables updates of the modules based on available version from the HOPEX Store.
Session Manager	HAS.Server.exe	Ensures the opening and closing of the session when people request an HOPEX connection.
Monitoring Manager	HAS.Server.exe	Exposes supervision metrics to diagnostic health of the deployment.
Logging Manager	HAS.Server.exe	Provides the appropriate logs for each module with consistent naming convention and content.

2.2.3. Back-end modules

These modules expose the core treatment of the platform and can access a database to store data.

Module	Process Name	Purposes
HOPEX Core	HAS.Hopex.BackEnd.exe	This is the main process to run all the business logic of HOPEX.
…	…	…

All the other Back-end modules are available online on the HOPEX Store.

2.2.4. Front-end modules

These modules expose a web front-end and can be called by the user to access the platform.

Module	Process Name	Purposes
HOPEX Web	HAS.Modules.Dtpx.exe	This is the main process to expose the web front-end of HOPEX.
…	…	…

Other Front-End modules like Application ID Card, Audit Everywhere… are available online on the store and can be installed on an HAS Instance.

2.3. HAS Instance Manager

When deploying the solution, a Windows service named "**HAS Instance Manager**" is created. It handles:

- Fail-over: HAS Instance Manager start/restart HAS instance.
- Remote control: to request **start**, **stop**, **restart**, and even **update** from a web or through REST API.

The HAS Instance Manager embeds its own web server to expose a web front and REST API to perform the mentioned actions.

Moreover, with HOPEX Application Server it is possible to manage multiple instances on the same physical infrastructure. In that case the HAS Instance Manager ensures that all the HAS instances are up and running.

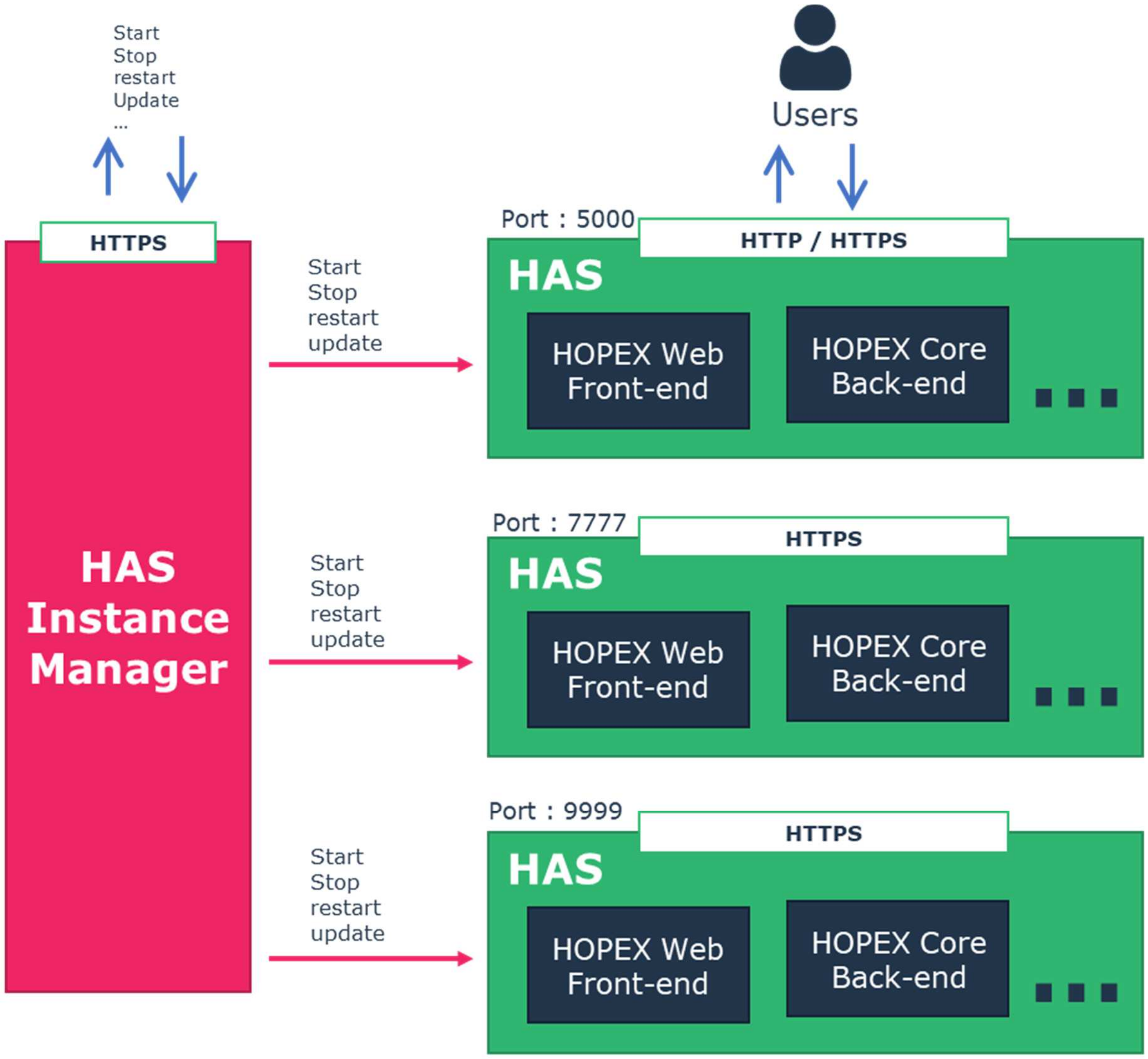


Figure 3 HAS Instance Manager Overview

2.3.1. Use case of Multiple HAS instance

In some situations, you may want to have multiple instances of HOPEX Application Server on the same server. The major use cases are:

- Multiple HOPEX environments: to manage in a different way the lifecycle of the database environments (SystemDb) and HOPEX customizations.
- Development, Pre-production, Production on the same server for small deployments to reduce infrastructure cost.
- SaaS multi-tenant deployment proposed by MEGA International.

Each instance is launched by HAS Instance Manager and is executed with the same user account.

2.3.2. Security

HAS Instance Manager must not be available from the web. It must be used in local host mode only.

2.4. HAS Bundle

A **HAS Bundle** is a collection of modules that represent a given version. For instance, you can find the following bundles: V5, V6, V7…

Each bundle contains:

- a version of the HAS Server
- a version of the HAS Instance Manager
- a collection of system Back-end and Front-end modules: HOPEX Core, HOPEX Web…

After the bundle installation, the modules can be updated individually regardless of the initial bundle.

2.5. HAS Installer

The installer is an **executable** program that eases the installation and deployment of the different components.

The component is built in **.NET Framework 4.8** which is by default installed in recent Windows server operating systems without prerequisites. This executable embeds an **MSI** setup built with **WIX**.

The installation process can be scripted with PowerShell script to ease deployment across several servers. The installer can be downloaded from the HOPEX Store. The installer supports 2 modes for different use cases:

- Online installation

  When going through the installation steps, the installer will download from the online store the needed modules.

- Offline installation

  At some point in the installation process, the installer will create an offline package to continue the installation in a server that does not have access to the Internet.

2.5.1. Limited internet access?

To benefit from the best experience, when using HAS, we recommend you to allow access from the server to the https://store.mega.com.

We understand that in some context HAS might be installed in a secured network area where internet is not available.

In that situation you will need to use the offline installation procedure and download required modules and update prior to install them on the server.

3. Software Technology Stack

3.1. Overview

For each layer of the architecture to operate, a set of technologies and software are required.

Layer	Technology Stack
Web Client	• Web Browser: Google Chrome, Mozilla Firefox ESR, MS Edge Chromium • PDF Reader (optional) • Microsoft Word *(optional)*: https://www.microsoft.com/en-us/microsoft-365/microsoft-office • Microsoft Excel *(optional)*: https://www.microsoft.com/en-us/microsoft-365/microsoft-office
IIS Web Server	• Windows Server 2016, 2019, 2022 *(recommended)*, 2025[2] • Microsoft Internet Information Service (IIS) 10 • Application Request Routing (ARR): https://www.iis.net/downloads/microsoft/application-request-routing • URL Rewrite 2.1 https://www.iis.net/downloads/microsoft/url-rewrite • SSL Certificate
HAS Web Application Server	• Web Browser (Chrome, Firefox, Edge) • Windows Server 2016, 2019, 2022 *(recommended)*, 2025[2] • .NET 8 Hosting Bundle: https://dotnet.microsoft.com/fr-fr/download/dotnet/8.0 • .NET Framework 4.8: https://dotnet.microsoft.com/download/dotnet-framework • Visual C++ Redistributable 2015 – 2022 vc_redist.x64.exe https://aka.ms/vs/17/release/vc_redist.x64.exe • Windows File System • ODBC Driver for SQL Server X64[1]: https://docs.microsoft.com/en-us/sql/connect/odbc/download-odbc-driver-for-sql-server?view=sql-server-ver15
Database SQL Server	• SQL Server 2019 or SQL Server 2022 • https://www.microsoft.com/en-us/sql-server

[1] If SQL server is installed on the same server as HAS the client may be already installed.

[2] Starting from HOPEX Aquila V6.1 SP2 onward.

3.2. Web Client

A **minimum 1360 x 768 laptop/screen resolution** is recommended for optimal rendering of HOPEX Web Front-End.

For the web browser the requirements are:

- HTML5 support
- JavaScript enabled
- Cookies enabled
- Download of files enabled
- Pop-up blocker disabled
- Web storage enabled

3.3. IIS Web Server

We use the Web server to behave as a **public Website face** to increase security and increase flexibility. Moreover, we use IIS with ARR as a **load balancer** across the HAS Logical cluster.

The IIS components: HTTP errors, Static Content Compression, HTTP Logging, Tracing and URL Rewrite are required on this server with complementary ARR component.

You must create your own HTTPS / SSL Certificate for the "public" DNS domain.

3.4. HAS Web Application Server

The mentioned software technologies above, must be installed on each HAS Server. HAS Servers work with a **self-signed certificate** for **internal communication**. Please refer to chapter 8 Security for more details.

3.5. Database SQL Server

Ensure that the database Collation is set to SQL_Latin1_General_CP1_CI_AS.

4. Communications and Protocols

4.1. Overview

The elements that compose the architecture interact with each other using:

- HTTP(S) for all web interaction and across server's interaction.
- Socket IP across the modules **within the same server**

The High-level communication stack is summarized by the following schema:

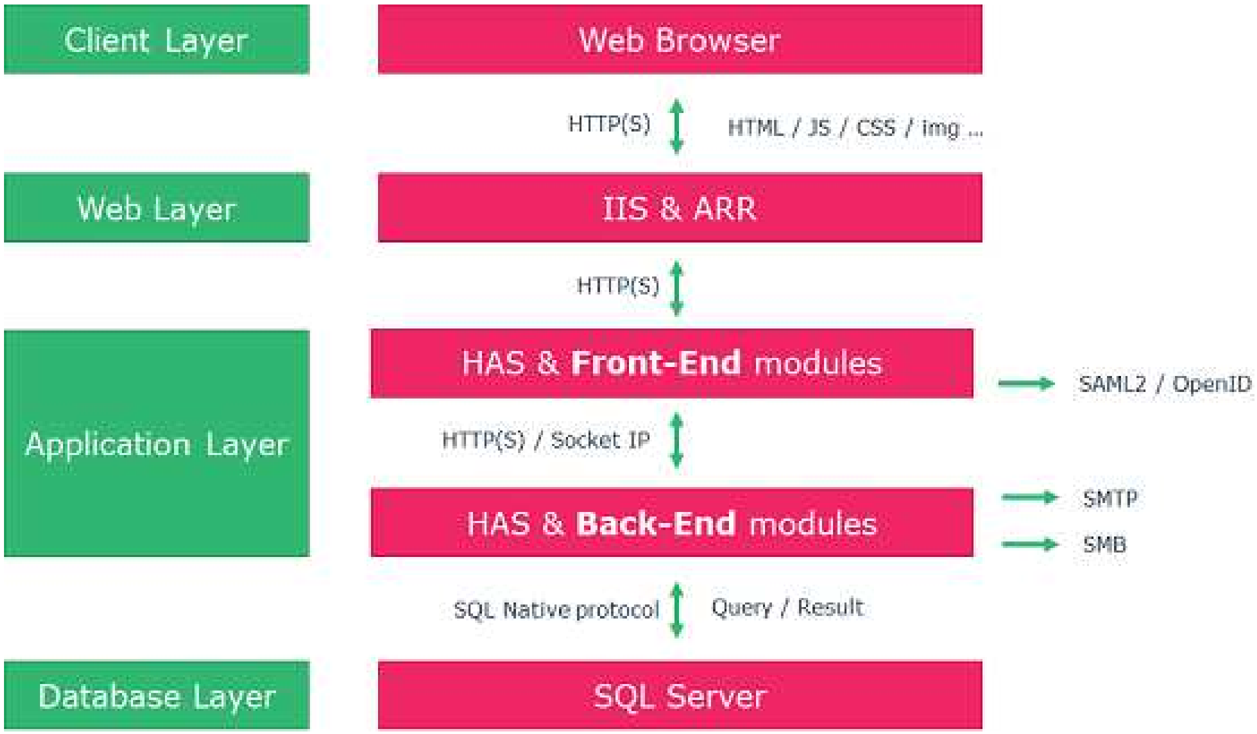
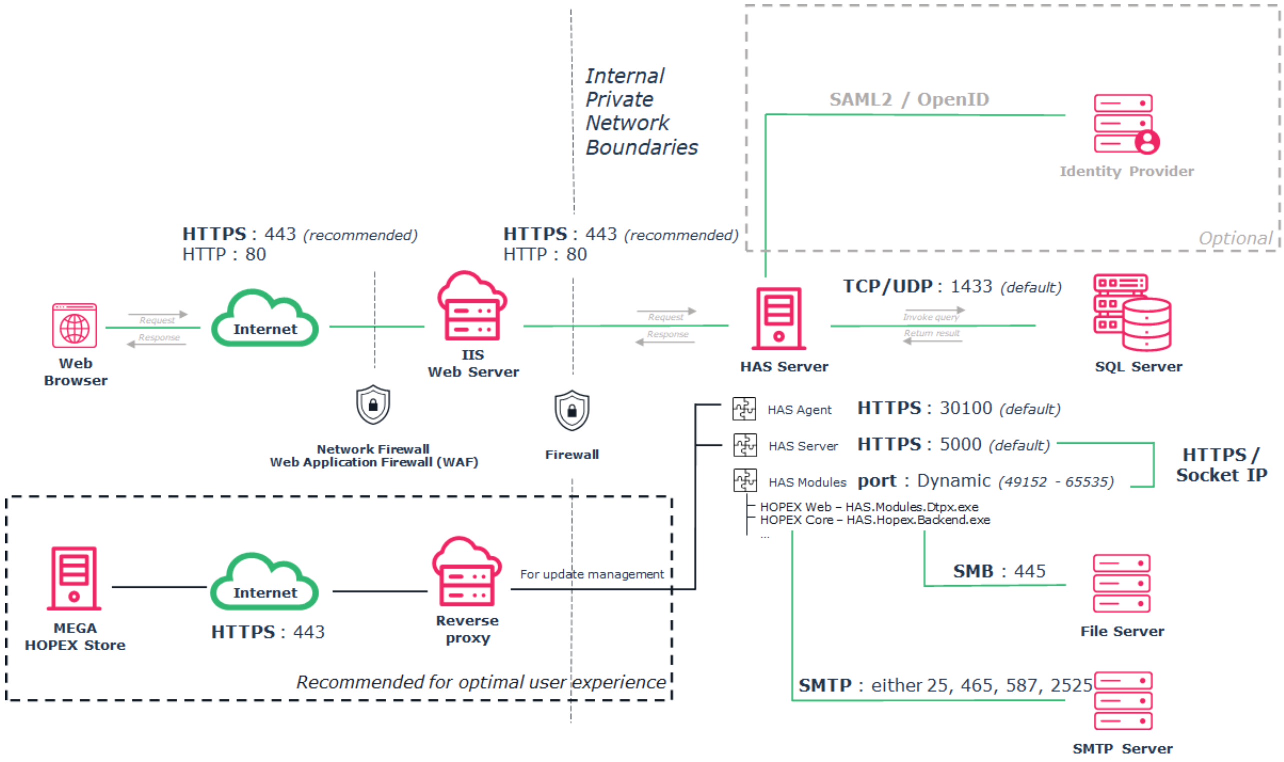


Figure 4 HAS Communication Stack

The full schema of communications and protocols used is shown below:



4.2. Detailed protocols and ports needed

4.2.1. List of ports

	Protocol	Port(1)	Network Bandwidth(2)	Latency(2)
Web browser	HTTP HTTPS	80 443 (recommended)	60 kbits/s average 512 kbits/s peak	100Ms
IIS Web Server	HTTP HTTPS	80 443 (recommended)	1 Gbit/s	
HAS Instance Manager	HTTPS	30100 *(To be opened in cluster deployment)*	1 Gbit/s	
HAS Server	HTTPS	5000 *(to be opened* *if IIS is on another server* *or If cluster deployment)*	1 Gbit/s	
HAS Modules(3)	HTTPS	49152 – 65535 *(Internal port - not to be opened)*	1 Gbit/s	

	Protocol	Port[1]	Network Bandwidth[2]	Latency[2]
HOPEX Module HOPEX Back-End[3]	Socket IP	49152 – 65535 *(Internal port - not to be opened)*	1 Gbit/s	1 Ms
File Server	SMB	445	1 Gbit/s	1 Ms
SQL Server **(Native client)**	TCP/UDP	1433	1 Gbit/s	1 Ms
SMTP Server	SMTP	25, 465, 587, 2525	1 Gbit/s	1 Ms
HOPEX Store **https://Store.mega.com**	HTTPS	443	1 Gbit/s	

[1] Port number may vary depending on IT policies. Given values are the default one.

[2] Recommended values for optimal performance

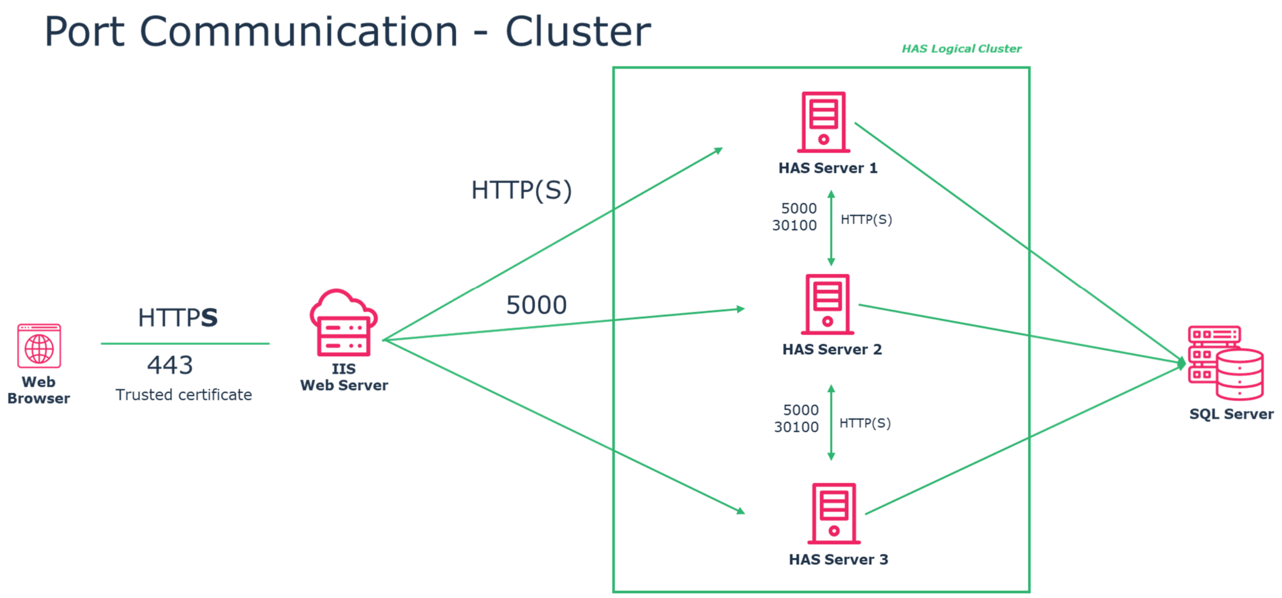
[3] The **Dynamic port range** used between HAS Server and the module is used only ***within the Server*** (localhost). No communication across servers is done with this port range. For more information: *https://support.microsoft.com/en-us/help/929851/the-default-dynamic-port-range-for-tcp-ip-has-changed-in-windows-vista*

4.2.2. Communication flow for each port

Here is the port used between servers:

Server source	Port	Server target
Web Browser	80 or 443	IIS
IIS	5000	HAS Server
HAS Server (internal calls)	49152 – 65535 (Windows Dynamic port range)	HAS Server (internal calls)
HAS Server 1 (Cluster node)	30100 5000	HAS Server 2 (Cluster node)
HAS Server … (Cluster node)	30100 5000	HAS Server … (Cluster node)
HAS Server	1433	SQL Server
HAS Server	445	File Server
HAS Server	25	SMTP Server
HAS Server	443	HOPEX Store
HAS Server	443	IIS

For cluster deployment apply the rule for each node of the cluster:



5. Logical Infrastructure

5.1. Deployment overview

The elements of the application architecture can be deployed in various ways. The appropriate infrastructure depends on:

- Pre-existing infrastructure: IIS servers or Databases servers
  1. Security constraints
  2. Business continuity and disaster recovery plan, based on application business criticality.
  3. Production, Pre-production, Training, or Developments environments requirements.
  4. Number of concurrent users.

The required infrastructure can go from a single server to a farm of servers.

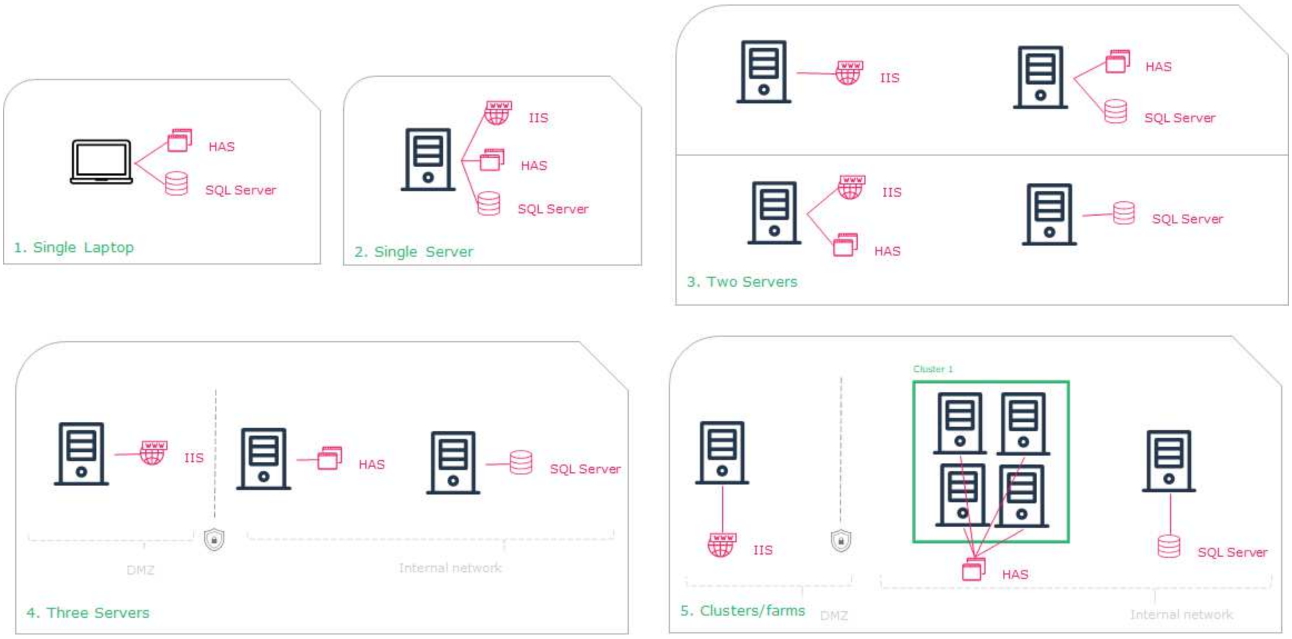


Figure 5 HAS Infrastructure deployment overview

	Type	Recommend for	Comment
1	Single Laptop	For single user or developer	For local usage
2	Single Server	Small deployment	For limited concurrent users with no specific IT policy constraints
3.1	Two Server	Medium deployment	To leverage existing IIS server
3.2	Two Server	Medium deployment	To leverage existing SQL server
4	Three Servers	Medium deployment	Most commonly seen deployment
5	Clusters/farms	Large Deployment	To meet the most demanding constraints

The “Recommend for” is driven by the **number of concurrent users**.

Depending on customer constraints, you may need to go to number 4 or 5 deployment types to meet BCP/DRP or security constraints.

5.2. Deployment type: decision tree

Depending on your context, you may choose one or the other deployment type. This decision tree can help you decide the best option to select:

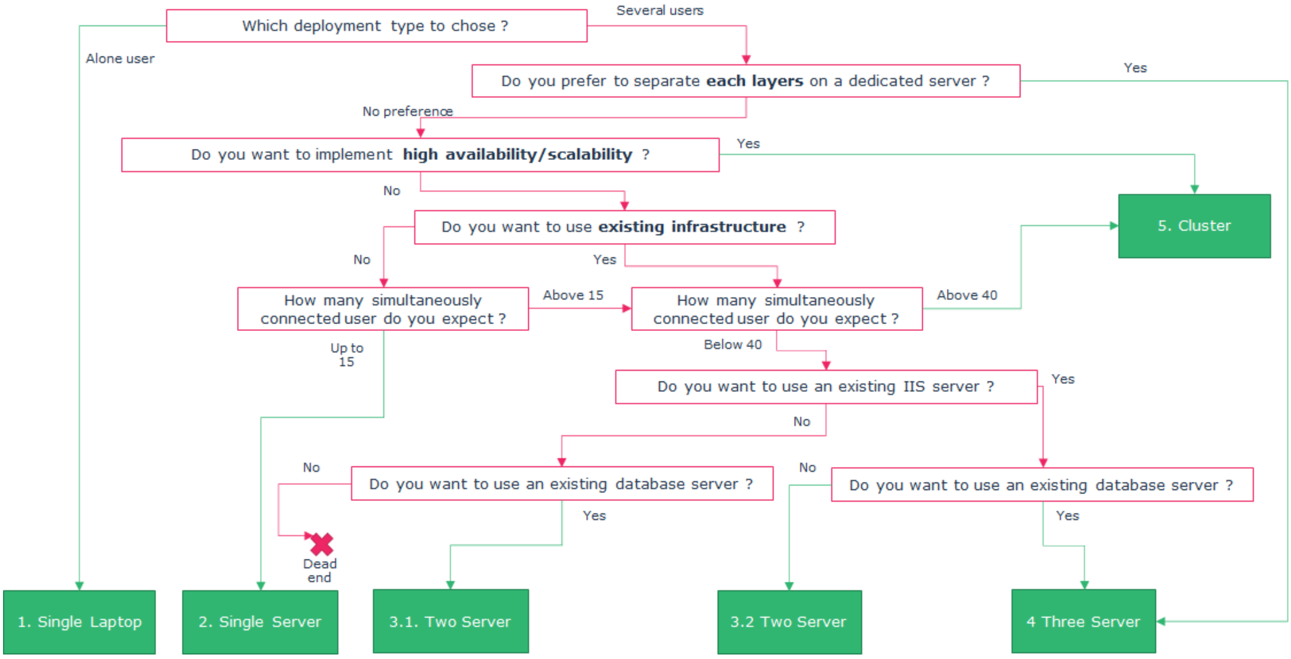

Which deployment type to chose ?
Several users
Alone user
Do you prefer to separate each layers on a dedicated server ?
Yes
No preference
Do you want to implement high availability/scalability ?
Yes
No
Do you want to use existing infrastructure ?
5. Cluster
No
Yes
How many simultaneously connected user do you expect ?
Above 15
How many simultaneously connected user do you expect ?
Above 40
Up to 15
Below 40
Do you want to use an existing IIS server ?
Yes
No
No
Do you want to use an existing database server ?
No
Do you want to use an existing database server ?
Yes
Dead end
Yes
1. Single Laptop
2. Single Server
3.1. Two Server
3.2 Two Server
4 Three Server

Figure 6 Deployment type Decision T...

For your information, the most seen deployment, regardless of the decision tree, is the one including 3 servers. In this context customers:

- Leverage existing IIS servers to address the routing of the HTTP request
- Leverage existing SQL server to create the needed database.
- Create a dedicated server for HAS

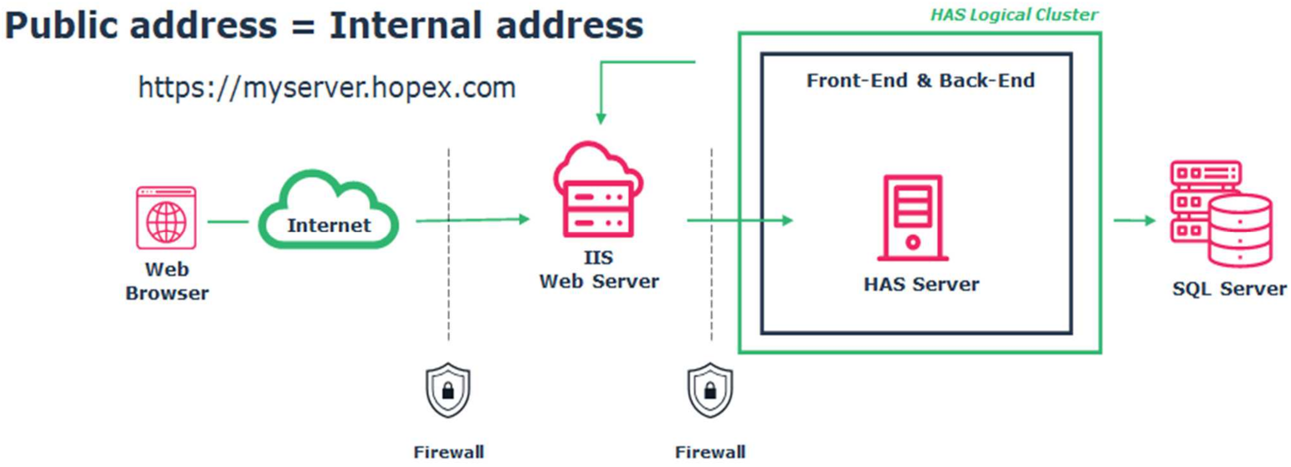


Figure 7 Most commonly seen deployment

5.3. Scaling the infrastructure

When demand for HOPEX application is increasing and you need to expand its accessibility, storage, and availability levels, you can scale vertically and horizontally.

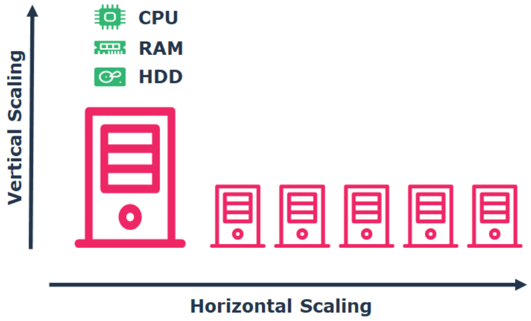


Figure 8 HAS Scaling principle

- Scaling Vertically: to improve performance, you improve existing servers by adding more CPU, RAM and disk space.
- Scaling Horizontally: to manage fail over, manage loads of concurrent users, or improve performance, you add additional servers.

The decision to scale horizontally vs. vertically depends on several factors.

If you have followed the sizing instructions for each server (CPU+RAM) described below, the Vertical scaling will have limited impact and we recommend you scale Horizontally.

Scaling Horizontally is called **Cluster deployment:** please refer to the dedicated chapter “Cluster deployment” for further information.

5.4. Cluster deployment

Clustering is used for **availability**, **scalability,** and **load balancing** at HOPEX Application server deployment. This technique consists in using multiple servers of similar type. The HAS Servers of the cluster can be managed by the **HAS console**.

Servers can be added at three levels:

- For the web server: for multiple IIS instances placed behind a load balancer.
- For HAS Server: for multiple servers to manage front and back-end roles.
- For Database Server: in an active/passive mode.

5.4.1. HAS server - Node role

When creating a logical cluster, each node must define its role. The same node can **implement several roles**:

- Front-End: All modules of type Front-End will be run on this server.
- Back-End: All modules of type Back-End will be run on this server.
- Job: Back-End Jobs will run on this server. Particularly useful to separate heavy treatment to avoid interacting with user currently connected.

5.4.2. Scaling HAS Server

The first step is to scale the HAS Server to gain:

- Availably: ensure that there is always a server up and running
- Scalability: ensure there is enough physical resource to meet concurrent users' demand.

In this scenario you can add one, two, three… servers dedicated to HAS Server. Each server must have a set of node roles. Servers can be exclusively defined on a role or share multiple roles.

We recommend in scalability context:

- One server dedicated for Jobs
- All other servers to play both Front-End and Back-End roles

The high-level overview of such deployment can be represented by the following schema:

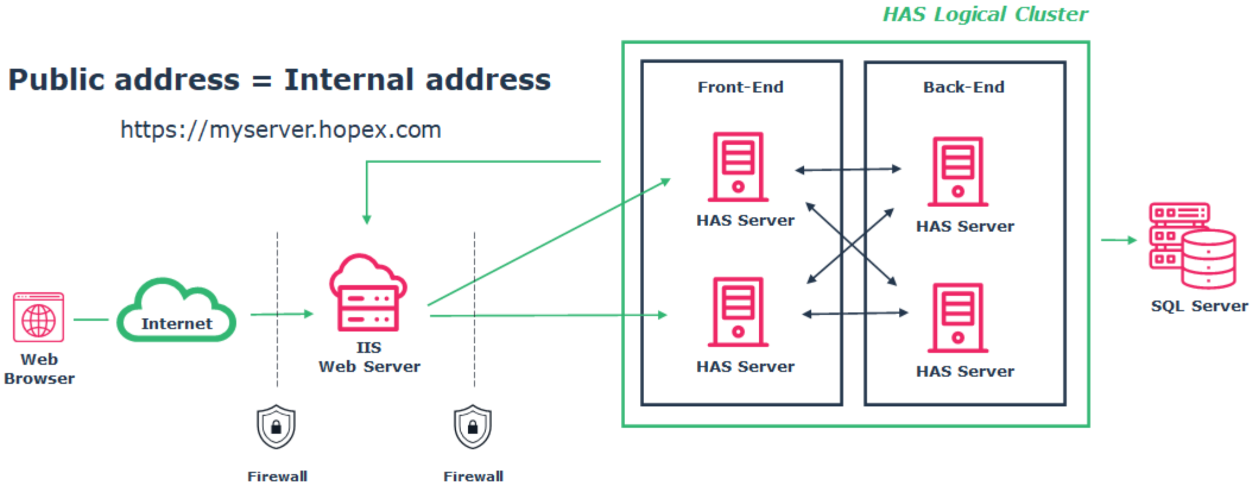


Figure 9 HAS Server Availability and Scaling with 4 servers

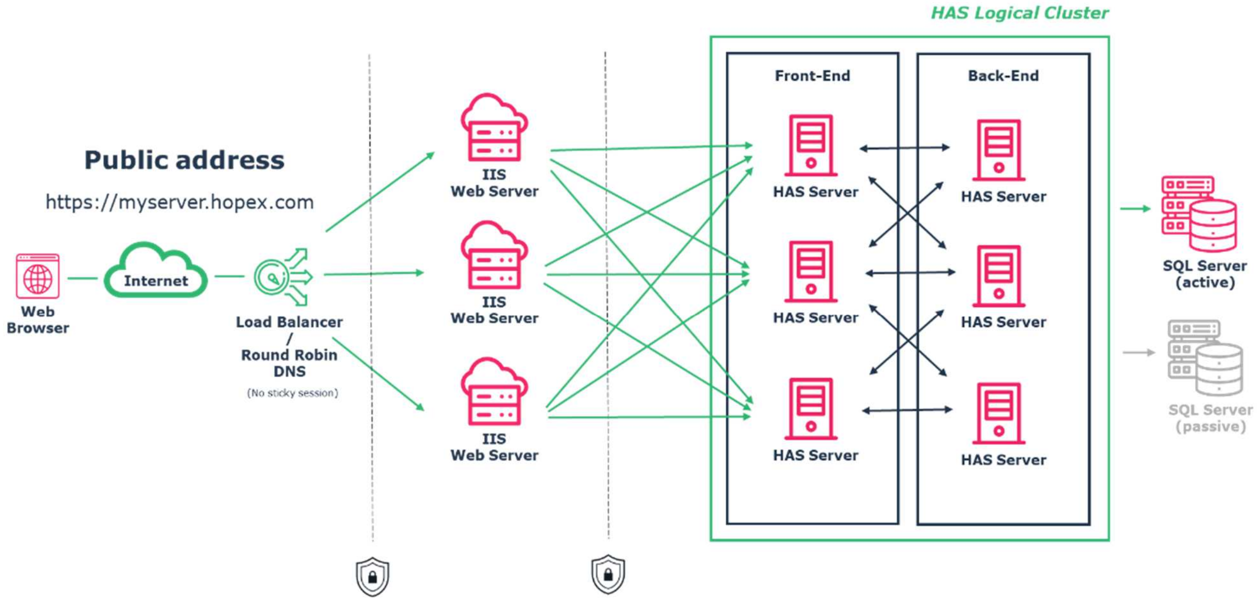
In cluster deployment HAS behaves as a logical cluster where:

- An "HAS" database contains configuration settings across nodes of the cluster.
- An internal load balancing mechanism ensures proper use of Back-End or Jobs Node.
- A cluster manager synchronizes modules versions across nodes.

5.4.3. Advanced availability cluster architecture

If you want to ensure each layer has **high availability,** then you need to duplicate all servers.

The overall architecture of such advanced scaling is described below. This schema is applicable regardless the number of chosen servers:



6. Sizing Physical Infrastructure

6.1. Disclaimer

The following sizing is based on our regular benchmark and load testing performed by the R&D. It is made based on the following assumptions:

- Smallest sizing: Possible for few concurrent users
- Small deployment: Up to 15 concurrent users
- Medium deployment: Up to 40 concurrent users
- Large deployment: Count one HAS Server for each 40 concurrent users' group.

This infrastructure can be:

- Physical server
- Virtual server: In this context the physical underlying infrastructure must be sized enough to support all running virtual servers.

We recommend a dedicated server for the HAS Server layer.

MEGA has made reasonable efforts to ensure the quality, accuracy, and validity of the performance benchmarking resulting in this sizing. Changes in any of the server's parameters might cause a positive or negative effect on the user experience and performances.

6.2. Hardware sizing

6.2.1. Server configuration

This sizing is based on the following hardware configurations. All HDD are of **SSD** type in these configurations.

Sizing	CPU Core	RAM	HDD
S1	2	8	100 Gb
S2	4	16	128 Gb
S3	8	32	128 Gb
S4	16	64	128 Gb

6.2.2. For Production

- Users mentioned in this table are maximum number of **simultaneously connected users**. *(see below for calculation rule)*
- In the cell the "S+number" represents the server configuration to choose.
- In bold are the preferred choices

	Configuration	Max simultaneous users:	<2	<7	<16	<41	>40
1	Single Laptop	HAS Application Server SQL Server	S2				
2	Single Server Smallest sizing	IIS Web Server HAS Application Server SQL Server		S2	S3		
3.1	Two servers Medium Deployment	IIS Web Server HAS Application Server		**S2**	S2	S3	
		SQL Server		**S1**	S2	S2	
3.2	Two servers Medium Deployment	IIS Web Server		S1	S1	S1	
		HAS Application Server SQL Server		S2	S3	S4	
4	Three servers Medium Deployment	IIS Web Server			S1	S1	
		HAS Application Server			S2	S3	
		SQL Server			S2	S3	

	Configuration	Max simultaneous users:	<2	<7	<16	<41	>40
5	Cluster/Farms Large Deployment	IIS Web Servers			S1	S1	S1
		HAS Application Servers*			S2	S3	S3
		SQL Server			S2	S3	S3

* Add one server for each additional group of users 40 users.

6.2.3. Other server environments

- For development: use Single Server with **Sizing 2**
- For training: 10 concurrent users, use **Single Server** with **Sizing 3**
- For pre-production: same infrastructure pattern as production with **Sizing 2**

6.2.4. How to calculate maximum simultaneous users

The maximum number of simultaneous users depends on the type of users:

- Main users: these are users using the tool on a regular basis. They have tasks to perform that can take several hours.
- Contributors/Viewers users: these are users that consume information and have limited production contribution. Their usage is punctual over the weeks with limited time spent when they connect.

Complete the following table to find your number of maximum simultaneous users.

License users	Number	Formula	Total
Mains users		RoundUp (Nb / 4)	
Contributors/Viewers		RoundUp (Nb / 100)	
Maximum simultaneous users:			

Example:

You have 5 process modelers, 10 portfolio managers, 40 application owners, 100 viewers. I will then have:

License users	Number	Formula	Total
Mains users	15	RoundUp (Nb / 4)	4
Contributors/Viewers	140	RoundUp (Nb / 100)	2
Maximum simultaneous users:			6

You can choose a single server or two server deployment type. In that context the preferred deployment type is the one highlighted in bold.

6.2.5. Multiple instances

The sizing proposed here is done for only 1 HAS Instance on the server. Should you be in a multi-instance scenario you need to adjust RAM consumption accordingly.

Count minimum 5 Go additional RAM for each new Instance. The needed RAM also depend on maximum concurrent users.

6.2.6. Public vs Private Workspace

In most of the desktops, HOPEX users work in public workspaces, i.e. their actions are automatically saved (within 5 min).

	Multi-Session (MS)	Single Session (SS)
Public Workspace	**Default – recommended**	*Not supported /* *Not Available*
Private Workspace	*Not supported /* *Not Available*	V3/V4: behavior V5: possible

Changing the behavior from public workspace to private workspace has a direct impact on sizing.

You must adjust RAM consumption: count **1Go of RAM** for each additional concurrent user.

Example: You change 10 BPA Modeler into private workspace (SS)

With the new behavior you need to add 10Go of RAM to the server.

6.2.7. Making the right choice

Refer to the decision tree to choose the deployment type.

Select the preferred configuration sizing among the deployment type.

7. SQL Server Databases

All connections to the database are done with ODBC Driver for SQL Server x64.

7.1. How many databases

For any installation there is a minimum of 3 databases for each HAS instance:

- one database to store the technical configuration of HAS

  Default naming convention: HAS_"Port Number" or "HAS Cluster name"
- one database to store the business configuration and customization (SystemDb)

  Default naming convention: "Database environment name"_"SystemDb"
- At least one database to store repository information

  Default naming convention: "Database environment name"_"Repository name"

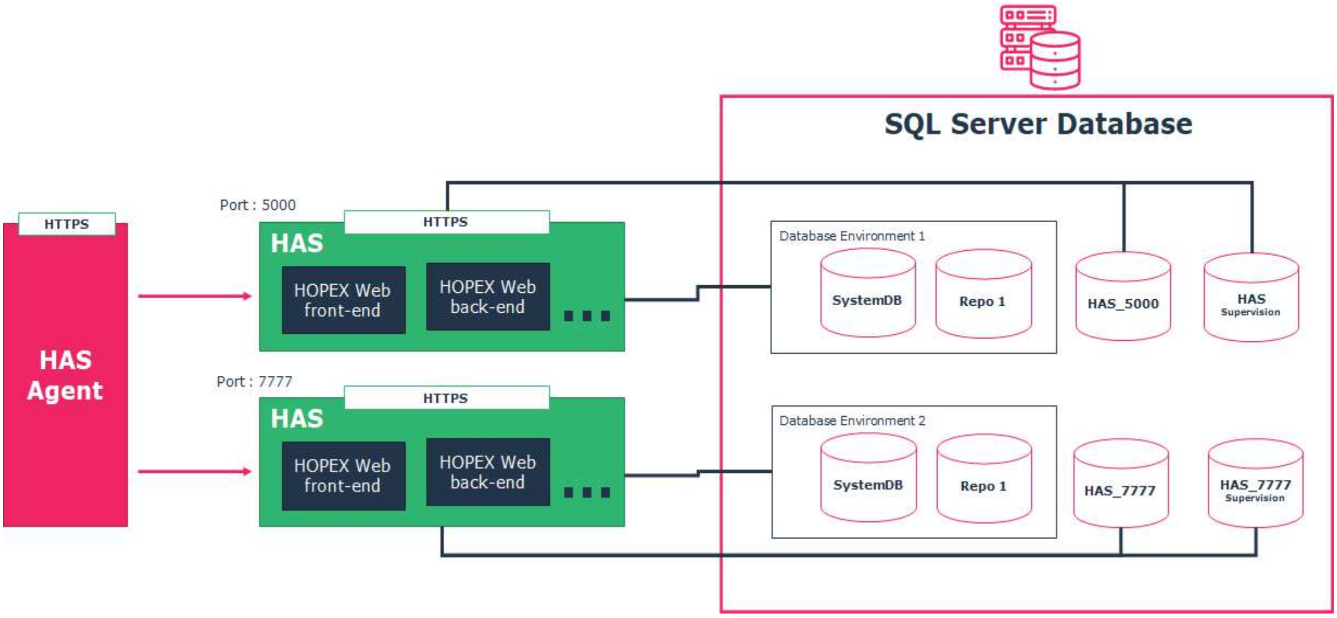


Figure 10 Database Overview

An additional Database might exist to store the data in case of the utilization of the Datamart feature.

7.2. Database size

For HAS main configuration database count 1Gb.

For each SystemDb count 5Gb to start, increase by 5Gb.

For each repository count 5Gb to start, increase by 5Gb.

Commonly seen size:

- After 5 years of usage the SystemDb repository cap up to 15Gb.

- After 5 years of usage, with 15 concurrent users, the repository goes up to 30Gb.

7.3. Database options

The two following settings are required to ensure the usage of the platform.

- Ensure that the database Collation is set to SQL_Latin1_General_CP1_CI_AS
- We recommend the database is created with **auto extend** property

7.4. User account and privileges

You can either set the connection string to the database with:

- a Native SQL account *(preferred choice)*
- a Windows account: all users that will connect to the database must be authorized.

HAS and HOPEX will manage:

- database creation
- tables, columns, index, stored procedure
- data insertion and modification.

It is possible to limit database creation access rights with advanced settings.

7.4.1. Native Account

- **Standard security policy (preferred choice):** the user account is enabled to manage databases.

User type	Comment	Server roles	Database roles	Server permissions
User with maximum privileges	• Create/delete database • Create/update/delete tables • Create/update/delete columns • Create/update/delete index • Create/update/delete stored procedures • Data read/write access	dbcreator	Db_owner (default role)	View server state Sys.dm_exec_sessions

- **Constrained security policy:** the user is not allowed to create the database and thus the database must be created by the DBA.

User type	Comment	Server roles	Database roles	Server permissions
User with limited privileges	• Create/delete database • Create/update/delete tables • Create/update/delete columns • Create/update/delete index • Create/update/delete stored procedures • Data read/write access	public	Db_owner (assigned manually by DBA)	View server state Sys.dm_exec_sessions

7.4.2. Windows Account

- **Constrained security policy:** the user is not allowed to create the database and thus the database must be created by the DBA.

User type	Comment	Server roles	Database roles	Server permissions
User with limited privileges	- Create/delete database - Create/update/delete tables - Create/update/delete columns - Create/update/delete index - Create/update/delete stored procedures - Data read/write access	public	Db_ddladmin Db_datawriter Db_datareader (assigned manually by DBA)	View server state Sys.dm_exec_sessions

For more information on this Windows Account, refer to the detailed documentation.

7.5. Physical backup

We recommend you perform **physical backups** of the databases. Cold or Warm back-ups are supported.

- Frequency: Daily
- Retention: 30 days

You should also **back-up all files** located in the file server at the same time of the databases backup.

7.6. Administrative tasks

To ensure database optimal performance, of HOPEX Core, you should run (monthly or weekly) **batches** of the following stored procedures:

- Conservation of repository performance
- Deletion of historical data
- Deletion of private workspace temporary data
- Database de-fragmentation and statistics
- SQL Server storage maintenance plan *(service need to be stopped)*

8. Security

8.1. Windows Users and Groups

When you install **HAS Instance Manager**, at least one user is necessary to manage the process authentication. By default, the process that launches HAS Instance Manager is defined as a "**Local System account**".

It is recommended to create a dedicated additional user, preferably in the Domain. In case it is not possible to have a domain user, it is still possible to have a local user.

Beware, the domain user or local user must have **read/write/execute** rights:

- On the shared folder for the licenses and HOPEX environments folders
- On the "default" installation following folder.

C:\Program Files\MEGA

C:\ProgramData\MEGA\

No active directory groups are required for this user.

If you have decided to configure the database with a Windows Account please ensure that the user as sufficient privilege.

8.2. HAS Self-signed certificate

The server works with a **self-signed certificate** for **internal communication**. It is possible to change this certificate manually after the first installation.

By default, this certificate is located in:

- C:\ProgramData\MEGA\Hopex Application Server\5000\.certificates

Caution: this certificate cannot be changed without also reinitializing the HAS configuration options.

8.3. Running processes

At runtime, the following processes must be allowed. There can be multiple processes of the same kind running in parallel, depending on the deployment options.

Process name	Comment
HAS.Instance Manager.exe	The main process for the Instance Manager.
HAS.server.exe	The main HOPEX server process
HAS.Modules.UAS.exe	The identity manager
HAS.Modules.Dtpx.exe	The web front end of HOPEX
HAS.Modules.Console.exe	The web console for the administrator
HAS.Modules.Portal.exe	The web portal of modules

Process name	Comment
HAS.Hopex.BackEnd.exe	The core back-end of HOPEX.

Complementary exe files can be launched, depending on modules deployed. Their naming convention follows the pattern **"HAS.*"**

8.4. Antivirus

To maintain good performances, it is recommended to exclude certain folders and files extensions from the antivirus real-time scanning (on access scanning). These folders and files are in the HAS Server.

Default folders, sub-folders and files to exclude:

- C:\Program Files\MEGA
- C:\ProgramData\MEGA

All files within this servers *.* should be excluded for maximum performance.

For environment and must license some extensions must be exclude:

- *.MZL, *.MOL, *.MGL, *.MGR
- *.MGS
- *.haspkg

8.5. Firewall

The firewall and proxy must be configured to allow communications by the different protocols on the ports mentioned above, across all the servers of the deployment.

The firewall and proxy need to allow downloading of the *.haspkg files.

8.6. User Authentication

After installation, the default HOPEX authentication is available. Other authentication models need to be configured in the HAS console. An authentication workflow provides:

- secure authentication requests.
- leverage standard identity providers.

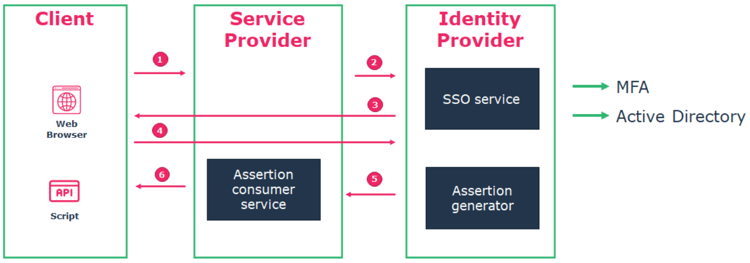


Figure 11 Authentication Workflow

In all cases, the service provider is managed by the HAS and the Identity Provider (IP) can be HOPEX or external.

Several authentication models can be implemented (one or several at the same time):

Authentication model		Comment	IP	SSO
Default HOPEX	HOPEX	Users and passwords are stored, hashed, within the HOPEX SystemDb database. The full workflow of login is managed by HOPEX (SP+IP)	HOPEX	No
	Windows	Passwords are managed by Windows	HOPEX	No
Windows Authentication		The identity provider is based on Windows Identity Foundation.	ADFS	Yes
SAML2		The identity provider is external and manages the user credentials	ADFS, Okta…	Yes
OpenID		The identity provider is external and manages the user credentials	Microsoft, Google, Salesforce…	Yes

For HOPEX Identity Provider the passwords are encrypted in AES256.

8.7. Data Access

Access to data is controlled using profiles:

- repository access,
- CRUD data permissions,
- CRUD GUI permissions.

Complementary features enable:

- writing access management: control of updates on existing objects.
- reading access management: control of visibility regarding existing objects.
- data access rules: computed control of visibility regarding existing objects.

8.8. Cookie security policy

Before performing any audit on the application and checking cookie settings, make sure you are in full HTTPS (IIS and internal communication).

The following table lists the cookies the web page might use or generate.

The table shows default values for a full HTTPS deployment. Values may vary in HTTP.

Cluster name: is the name of the cluster when you created the instance.

Cookie name	Domain	Expires	Http only	Secure	Same site
.oidc.nonce."clustername"	Public URL	10 min	True	True	None
.oidc.correlationId."clustername"	Public URL	10 min	True	True	Lax
.antiforgery."clustername"	Public URL	Session	True	True	Strict
idsrv.session	Public URL	Session	**False**	True	None
.token."clustername"	Public URL	20 min	True	True	Lax
.token."clustername"C1	Public URL	Session	True	True	Lax
.token."clustername"C2	Public URL	Session	True	True	Lax

8.8.1. Why Idsrv is always http only = false

As per specification of open id the idsrv session cookie will always be in Http only = false.

For more details, see the official documentation:

https://openid.net/specs/openid-connect-session-1_0.html#ChangeNotification

> *"… If a cookie is used to maintain the OP User Agent state, the HttpOnly flag likely cannot be set for this cookie because it needs to be accessed from JavaScript. Therefore, information that can be used for identifying the user should not be put into the cookie, as it could be read by unrelated JavaScript…"*

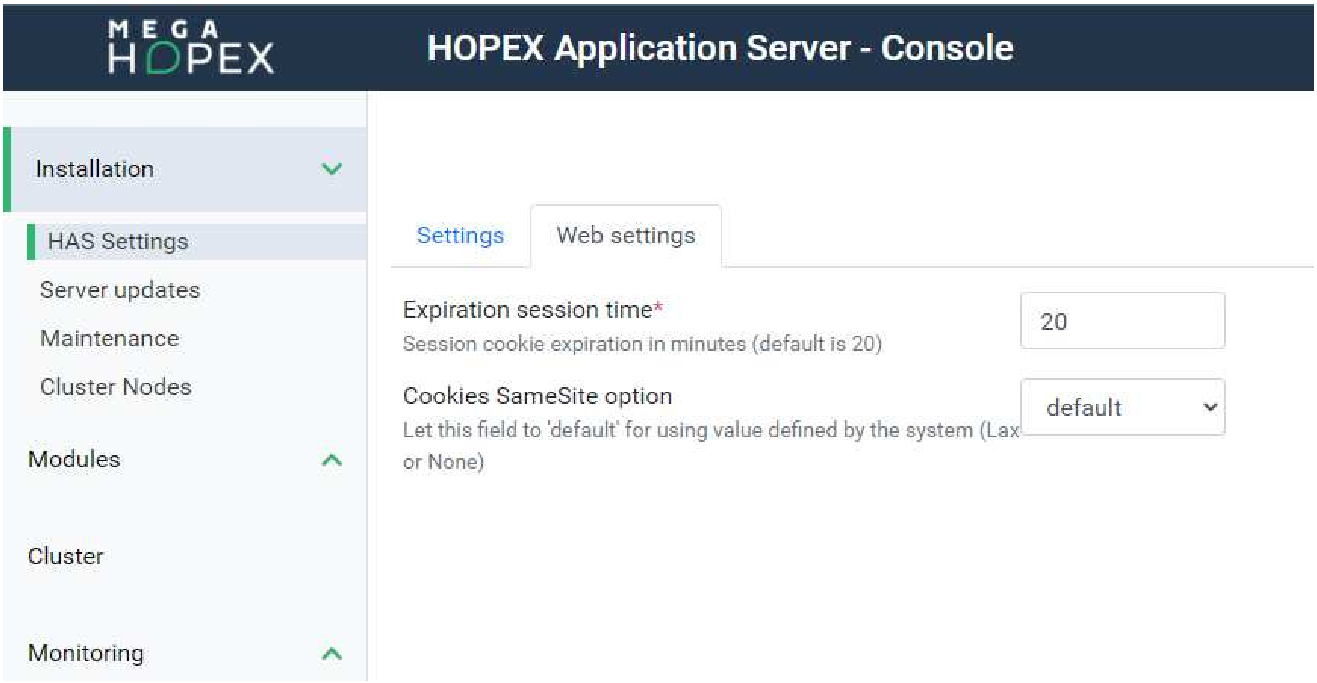
8.8.2. How to enforce Same site Strict or Lax

Should you want to enforce cookies "Same site" to be:

- None
- Strict
- Lax ➔ default

You can edit the value in the HAS Console.

Limiting to Strict may limit module and feature enablement.



Expiration session time*
Session cookie expiration in minutes (default is 20)
20

Cookies SameSite option
Let this field to 'default' for using value defined by the system (Lax or None)
default

9. File Server

The file server is used to share files across the HAS servers. The main data is:

- Database environment files: connection string, temporary files
    - *.MZL, *.MOL, *.MGL, *.MGR, *.XMG
    - *.IX, *.LOG, *.DAT
- Must License: to manage connected users and related tokens
    - *.MUST
    - *.INI, *.TNK*, *.USR*

The files contained in this folders will be accessed by the tool. To enhance usage, you need to make sure policy on proxy, firewall, and antivirus are configured properly to avoid blocking, scanning this files.

10. Supervision and monitoring

The HAS server enables platform supervision and monitoring. Supervision events update the logs or trigger events to be sent to external tools.

The HAS Server can be configured with:

- Logs: with an external tool using HTTP protocol and Compact Log Event Format (CLEF). Supported tool SEQ https://datalust.co/seq
- Tracing: with an external tool using HTTP and Open Tracing. Supported tool Zipkin https://zipkin.io/

11. Error and trace log files

No logs are generated on the client side. All errors are displayed using popup windows or via the HTML browser. An option enables to control the display of errors to end users (GUI). For advanced diagnostic, a verbose mode can be enabled to generate more detailed logfiles.

Different files can be created on server side. There are 2 mains **default locations** for the logs:

- C:\ProgramData\MEGA\Hopex Application Server\logs

  For the logs of the HAS Instance Manager.
- C:\ProgramData\MEGA\Hopex Application Server**5000**\Logs

  For the logs of the **HAS Instance**: HAS server and all the modules.

  Where "**5000**" is the port number of the instance

General naming convention of log files:

"cluster name"-["Module name"-"Module version"]-YYYYMMDD.txt

Where:

- Cluster name: is the name of the cluster or the port number
- Module name: is the name of the module defined in the manifest
- Module version: the full build version of the module as defined in the manifest
- YYYYMMDD: represents the year, month and day

Example:

5000-[HAS.CONSOLE-1.0.301]-20201104.txt

5000-[HAS.UAS-1.0.301]-20201104.txt

Log name	Content
5000-[HAS-X.X.X]-YYYYMMDD.txt	Main HAS Server log
megaerrYYYYMMDD.txt	Main logs of HOPEX
5000-[HAS.CONSOLE-X.X.X]-YYYY.txt	For logs on the HAS console
5000-[HAS.PORTAL-X.X.X]-YYYYMMDD.txt	For logs on the portal that expose all web modules
5000-[HAS.UAS-X.X.X]-YYYYMMDD.txt	For logs about identity manager
5000-[HOPEX WEB DESKTOP-X.X.X]-YYYYDDMM.txt	For logs of the web part of HOPEX
sspsprvsYYYYMMDD.txt	Supervision error logs

Log name	Content
ssperrYYYYMMDD.txt	Errors generated by the SSP when assigning a user to an environment
redis_server_log.txt	Redis logs in case of cache issues.
HopexHealthDigestReportYYYY-MM-DD_XX-XX-XX.html	Report to diagnose HOPEX usages and performance
HopexHealthFullReportYYYY-MM-DD_XX-XX-XX.html	Report to diagnose HOPEX usages and performance
RepositoryHealth-YYYY-MM-DD-MyEnvironment_MyRepository	Report to diagnose HOPEX usages and performance

12. Miscellaneous

12.1. Licensing

Products and solutions of HOPEX platform are protected by Must licenses. Must licenses can be shared between multiple users.

Must licensing is not server-based (there is no Windows process for a license server). At runtime with HOPEX Web Front-end, a set of files are generated dynamically by service account.

However, a domain user (Active directory) is required for:

- HAS Instance Manager.
- User running the Desktop Administration Console: system administrator, functional administrator.
- User running the Desktop Windows Front-end: developer, functional administrator, user associated to a scheduled task.

To obtain a license, contact your sales representative. A UNC will be requested and a .must license file (locked on this UNC) will be sent with installation instructions.

12.2. Full search and indexing

Solutions of HOPEX platform can use full search. A parameter at data repository and/or system repository level enables to activate indexing. There are 2 levels of indexing:

- Full indexing: the data repository/system repository is scanned, and index files are created in a subfolder of the data repository/system repository.
- Incremental indexing: the log (internal) of the data repository/system repository is scanned and index files are updated in a subfolder of the data repository/system repository.

12.3. Mail system

A mail server needs to be configured so that mail notifications can be used within workflows.

SMTP parameters (server, port, proxy...) can be configured for the installation using the Administration console.

12.4. Multi-language

The HOPEX Platform supports multilingualism for:

- User interface language: controls the display of the menus, pages, etc. **Six languages** are provided: English, French, German, Italian, Spanish, Portuguese.
- Input Data language: enables data entry in several languages for the objects (name, comment, …). **Up to 30 languages are supported.**

12.5. Reporting

There are several report capabilities:

Category	Format	Export	Comment
Report	HTML	RTF, XLS, PDF	Generate a report based on a HTML template
MS Word	RTF	RTF	Generate a report based on a Word template
Instant Report	HTML	RTF, XLS, PDF	From a list or dataset generate various charts (pie, histogram…) or tables

You need to have a software that can read the defined **export format**. For instance:

- Microsoft Office or Open Office for RTF, XLS
- Adobe Reader for PDF

12.6. Preventing destabilization due to memory saturation

By default, the "Prevent logging when low memory" option is activated: **additional user connections are blocked** when the system approaches memory saturation. Users trying to connect receive a notification that access is unavailable and that they should contact their administrator.

This helps prevent **unexpected HOPEX shutdowns** due to insufficient memory.

12.6.1. Calculation rules

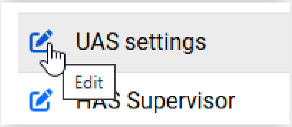
- **Single server**: if the available commit memory drops below **3 GB**, new user connections are blocked.
- **Cluster**: if the active instance has less than **3 GB** of available commit memory, other servers in the cluster are checked. If no server has more than **3 GB** available, new connections are blocked.

12.6.2. How to disable the memory saturation option

If needed, the memory saturation option can be disabled to allow user connections even as memory nears saturation.

To disable the memory saturation option:

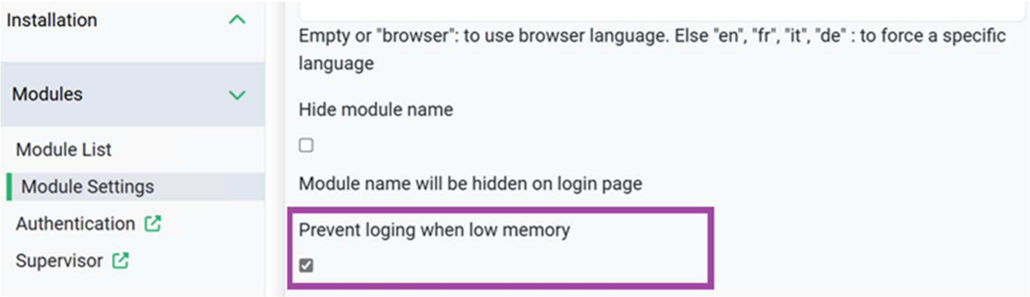
1. Open the HAS Console.
2. Select **Modules > Module Settings**.
3. Click **Edit UAS settings**.



UAS settings

HAS Supervisor

4. Clear **Prevent logging when low memory**.



Empty or "browser": to use browser language. Else "en", "fr", "it", "de" : to force a specific language

Hide module name

☐

Module name will be hidden on login page

Prevent loging when low memory

☑

5. Click **Save**.

13. Other Technical Documentation

For more information, see the following **online documentation**:

- Installation procedures
- RDBMS Repository Installation guide
- HOPEX Administration documentation to manage installation and users
- Must licenses management
- HOPEX Administration Authentication
- Technical articles
- REST API & Server API (Java)
- Functional usage and features see user manuals

14. Frequently Asked Questions (FAQ)

14.1.1. What about other HTML browsers?

MEGA has decided to focus on Chrome, Edge Chromium, Firefox. This does not mean that solutions do not run on other HTML browsers. It means that these HTML browsers are not tested.

14.1.2. Are both 64-bit and 32-bit versions of HTML browsers supported?

MEGA has decided to focus on 64-bit versions of HTML browsers. 32-bit versions of HTML browsers are less qualified. This does not mean that the solutions do not run on such HTML browsers.

14.1.3. Is Edge Classic/Legacy supported?

Edge classic (Legacy version not Edge Chromium) is not supported. MEGA has decided to focus on Edge Chromium.

14.1.4. What is HOPEX Classic deployment?

Classic deployment is the former way to deploy HOPEX from first version (V2, V3, V4). It mainly relies on IIS and HOPEX SSP component. This document is the new HAS Architecture from V5.

14.1.5. Are Windows Server 2012 and Windows Server 2012 R2 still supported?

No. It will not work.

14.1.6. Is SQL Server 2014 or 2017 still supported?

SQL Server 2014 and 2017 are not recommended, use it at your own risks. Support starts from SQL Server 2019 and SQL Server 2022.

14.1.7. What is web storage for HTML browsers?

This is a capability of HTML browsers to store data (local storage mode)

This capability is supported by all recent browsers (Edge, Firefox, Chrome...)

14.1.8. What is supported for Azure?

Not all azure services are compatible with HOPEX

Here are the main options qualified by MEGA so far and used to provide MEGA SaaS:

- VM DS11_V2
- Premium storage Managed disk (SSD disk)

- Backup (backup of VM)
- WAF (Web Application Firewall) tuning required
- Deployment script (deployment by script)
- Image (deployment by image)
- Monitoring

If you consider using other services, contact MEGA Technical Support.

14.1.9. What is Mozilla Firefox ESR?

As Firefox versions change very rapidly, MEGA has decided to focus on ESR versions.

Extended Support Release (ESR) based on an official release of Firefox for desktop is used by organizations that need extended support for mass deployments.

See also http://www.mozilla.org/en-US/firefox/organizations/faq/

14.1.10. Are IE 9/10/11 still supported?

Internet Explorer 9, 10, 11 are no longer supported.

MEGA recommends using a more recent HTML Browser such as Edge Chromium or Chrome. See also https://support.microsoft.com/en-en/lifecycle

14.1.11. How to configure HTTPS?

By default the HAS server is in HTTPS. Note that a certificate for IIS is required to configure HOPEX in HTTPS end to end: see your IIS administrator.

14.1.12. It is possible to use a Must license that is not located on the HAS Server?

This is possible. The Share folder must accessible from the user that launch the process.

14.1.13. Is it possible to use another web server than IIS?

We use IIS for load balancing. MEGA does not provide any documentation to support Nginx or Apache.

14.1.14. Can HOPEX solutions and products run on a mobile platform?

Most HOPEX products and solutions are designed for a web client running on a desktop or laptop. Viewer users can use tablets running Android. Viewer users can consult data usually though a simplified desktop.

In addition to the HOPEX platform, MEGA proposes various web application that are natively designed for smartphones and tablets. See HOPEX Store.

14.1.15. What are the web technologies used by HOPEX Platform?

For HOPEX Web Front-end, the HOPEX platform uses HTML5 and various JavaScript related technologies mainly: Ajax., Extjs., Dojo.

A detailed list of third-party components is available on MEGA Community:

Open Source Components Used in HOPEX V6 | MEGA

14.1.16. What about other database servers?

MEGA has decided to focus on widespread and recent versions of SQL Server 2019 and above.

HOPEX Application Server (HAS) Installation Guide

1. Foreword

The document describes the installation procedure for HOPEX Application Server (HAS). This document applies to HAS installation from Hopex V5 onward.

The option given for IIS and SQL Server may vary depending on your existing situation. A specific study from Bizzdesign professional services might be required.

1.1. Installation & Architecture

Prerequisite: read the *HAS Architecture Overview* documentation prior to start the installation.

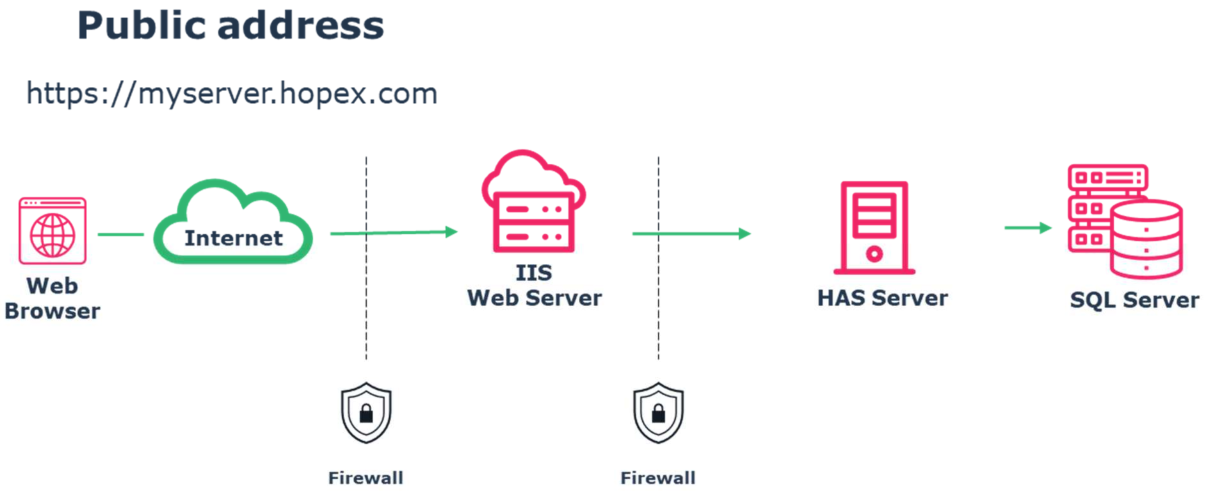
This installation describes installation and configuration of each layer:

1. SQL Server → actions are **manual**, see chapter 5: "SQL Server configuration"
2. IIS Web Server → actions are **manual**, see chapter "2 IIS Web Server"
3. HAS Server → actions are performed with a "**setup**" , see chapter 3 "HOPEX Application Server (HAS) installation"

Each layer can be installed on one or several servers depending on the chosen infrastructure deployment pattern.

This document describes installation with Windows Server and SQL Server. Adjust accordingly should you be in another version. Always check prerequisite.

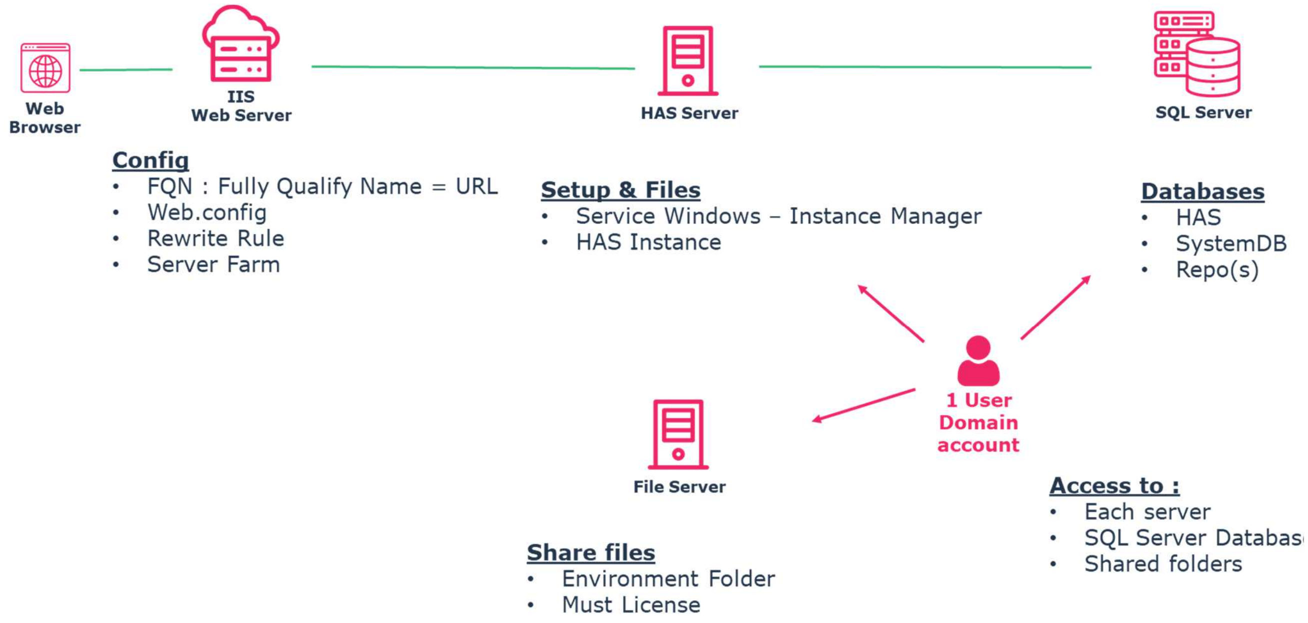
Each main chapter of this documentation describes the following architecture pattern:



Three layer installation

1.2. Step Overview

1.2.1. Major actions



Config

- FQN : Fully Qualify Name = URL
- Web.config
- Rewrite Rule
- Server Farm

Setup & Files

- Service Windows – Instance Manager
- HAS Instance

Databases

- HAS
- SystemDB
- Repo(s)

Access to :

- Each server
- SQL Server Databas
- Shared folders

Share files

- Environment Folder
- Must License

1.2.2. Database installation

As this step is performed by the customer database administrator, its description is not detailed in this documentation.

This documentation describes the database creation and backup restore or specific settings required.

See chapter 5: SQL Server configuration.

In case of cluster deployment: there is no difference for database creation/restore.

1.2.3. IIS Web Server installation

This step is **mandatory** for all deployment except for developer laptop scenario.

See chapter 2: IIS Web Server.

In case of cluster deployment: repeat the process for each IIS server. Configure your load balancer accordingly. Read the cluster deployment for more details.

1.2.4. HAS Application Server installation

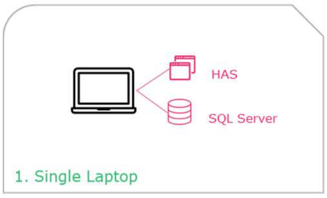
This step is **mandatory** for all deployment.

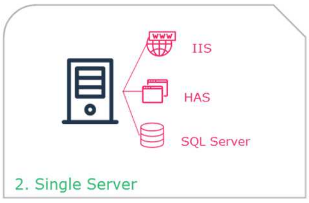
See chapter 3: HOPEX Application Server (HAS) installation.

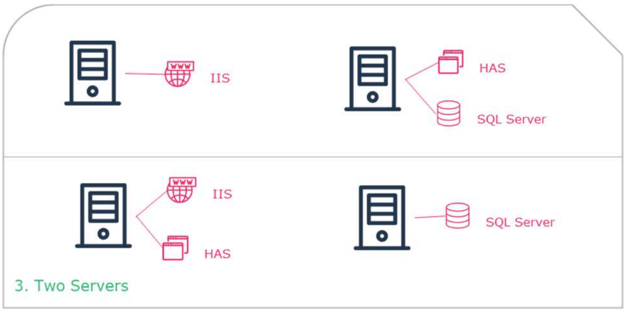
In case of cluster deployment: apply this step for **the first server** of the cluster farm. **Ensure your installation is working** then read the section about cluster deployment for more details.

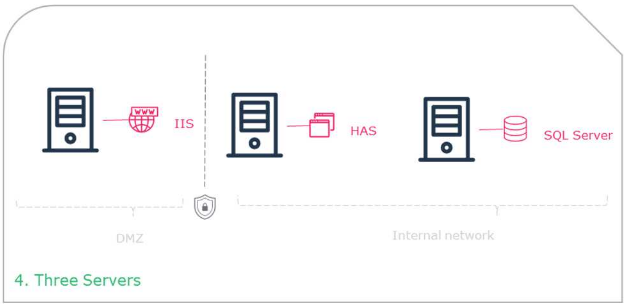
1.3. Different architecture installation scenario

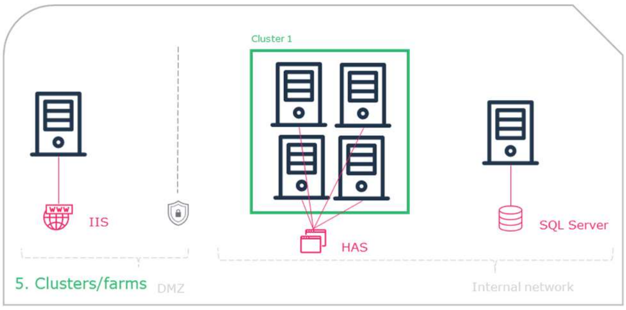
Depending on the installation architecture pattern you choose, you need to repeat the installation steps described in the coming chapters.







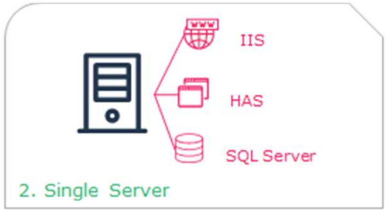




		Perform installation steps described in chapter
1	Single Laptop	• 3 HOPEX Application Server (HAS) installation
2	Single Server	• 2 IIS Web Server • 3 HOPEX Application Server (HAS) installation • 5 SQL Server configuration
3.1	Two Servers	• 2 IIS Web Server • 3 HOPEX Application Server (HAS) installation • 4 SSL Certificates configuration • 5 SQL Server configuration
3.2	Two Servers	• 2 IIS Web Server • 3 HOPEX Application Server (HAS) installation • 5 SQL Server configuration
4	Three Servers	• 2 IIS Web Server • 3 HOPEX Application Server (HAS) installation • 4 SSL Certificates configuration • 5 SQL Server configuration
5	Cluster	• 2 IIS Web Server • 3 HOPEX Application Server (HAS) installation • 4 SSL Certificates configuration • 5 SQL Server configuration • 6 Cluster installation

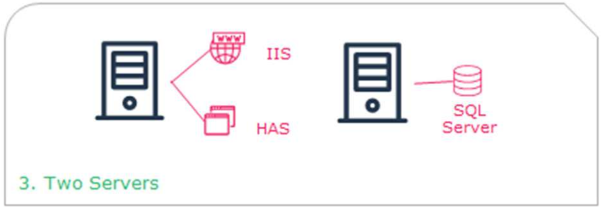
1.4. Summary of my Installation

Complete/Print this architecture diagram and use it to ease your installation process for each environment.



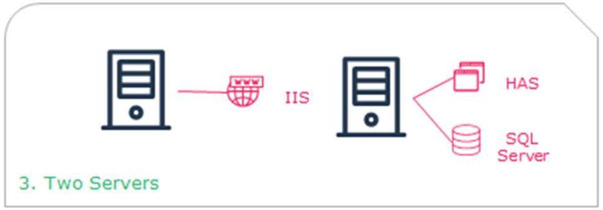
□ Chosen deployment

server name
IP address



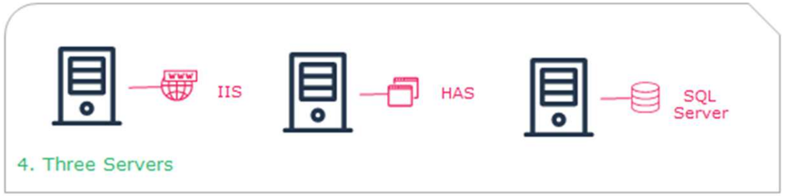
□ Chosen deployment

server name	server name
IP address	IP address



□ Chosen deployment

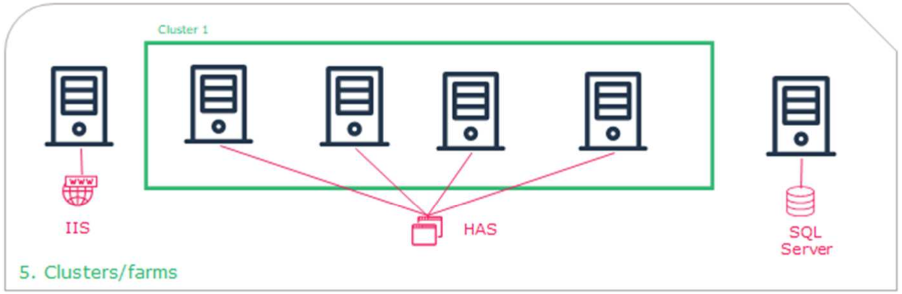
server name	server name
IP address	IP address



□ Chosen deployment

server name	server name	server name
IP address	IP address	IP address

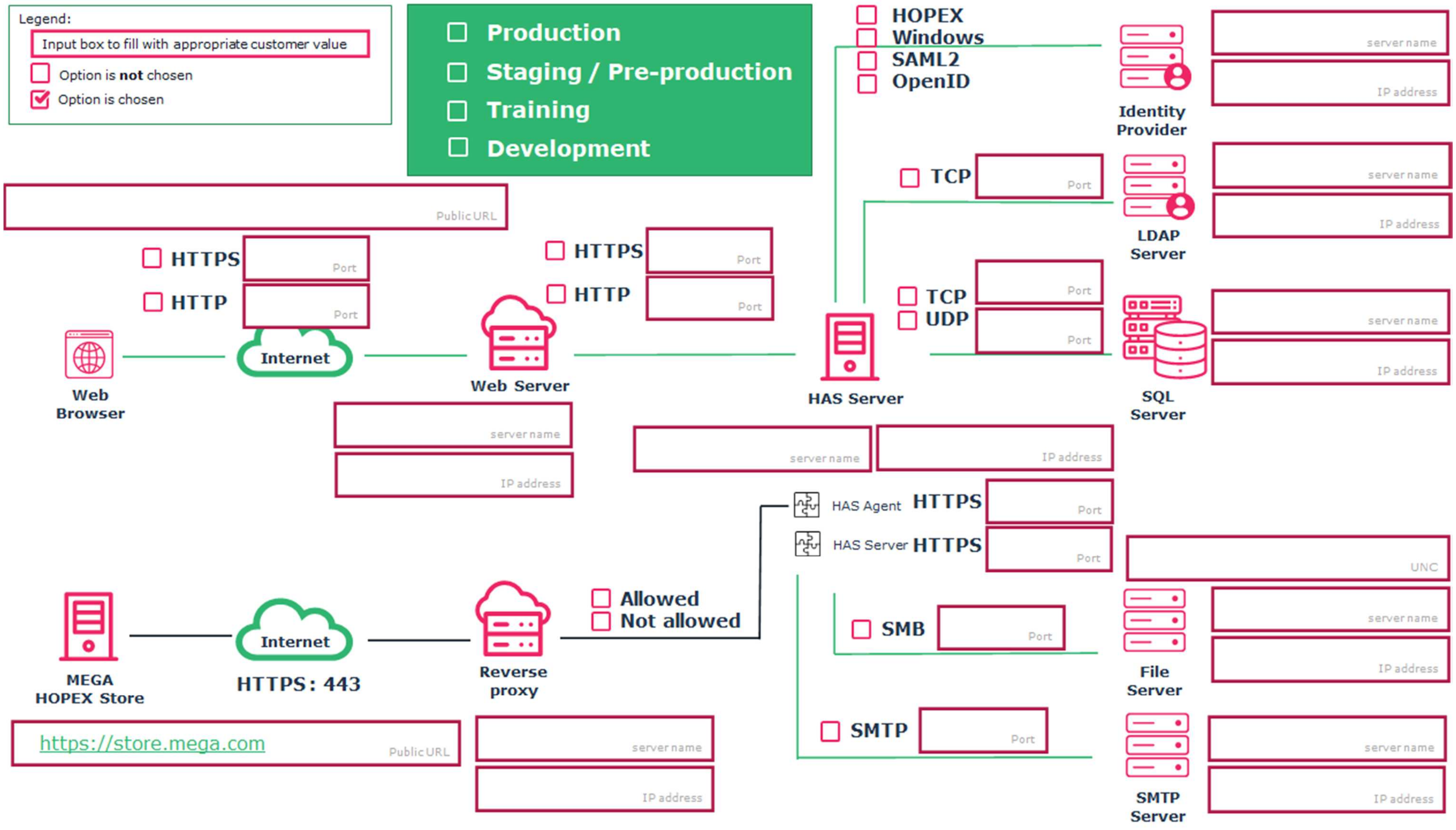
- □ **Production**
- □ **Staging / Pre-production**
- □ **Training**
- □ **Development**



□ Chosen deployment

			HAS Agent	HAS
HAS Server 1	server name	IP address	Port	Port
HAS Server 2	server name	IP address	Port	Port
HAS Server 3	server name	IP address	Port	Port
HAS Server 4	server name	IP address	Port	Port

Complete/Print this architecture diagram and use it to ease your installation process.



2. IIS Web Server

The following installation instructions are to be applied on each server that will behave as an “IIS Web Server”. The following instructions apply to Windows Server 2019. For other Windows versions adjust accordingly.

Should you have several IIS, you need to add a load balancer (no sticky session) in front.

For information:

- one IIS Web server is suitable for most deployments.
- IIS is **not required for single laptop** deployment (consultant, developer, partners), in that case skip this chapter.

2.1. Adding SSL Certificate

To ensure data protection, it is highly recommended to use SSL/TLS. If you want to activate this feature, it is then mandatory, as a prerequisite, to configure your IIS platform to activate the SSL/TLS.

You will need to have a **signed certificate**. You can bind the HTTPS protocol to any wanted port, in the installation process you will choose the port.

For official Microsoft documentation on IIS, see https://docs.microsoft.com/en-us/iis/manage/configuring-security/configuring-ssl-in-iis-manager.

2.1.1. Adding certificate on IIS Web Server

Make sure the SSL certificate has been properly imported in windows certificate store, see the instructions section 4.3 Adding certificate on the server.

In that example the public url of the installation is https://vp-iis1-v5.fr.mega.com Adjust naming based on your own policy and naming convention. Ensure this is a **signed certificated**.

2.1.2. Adding certificate on IIS

The certificate will be automatically visible when you edit the binding of your website. If it does not appear it means the certificate is not valid or you missed a step in previous section.

The instructions are explained in the following steps.

2.2. Installing IIS

If IIS is already installed, please check that all required features are enabled

To install IIS:

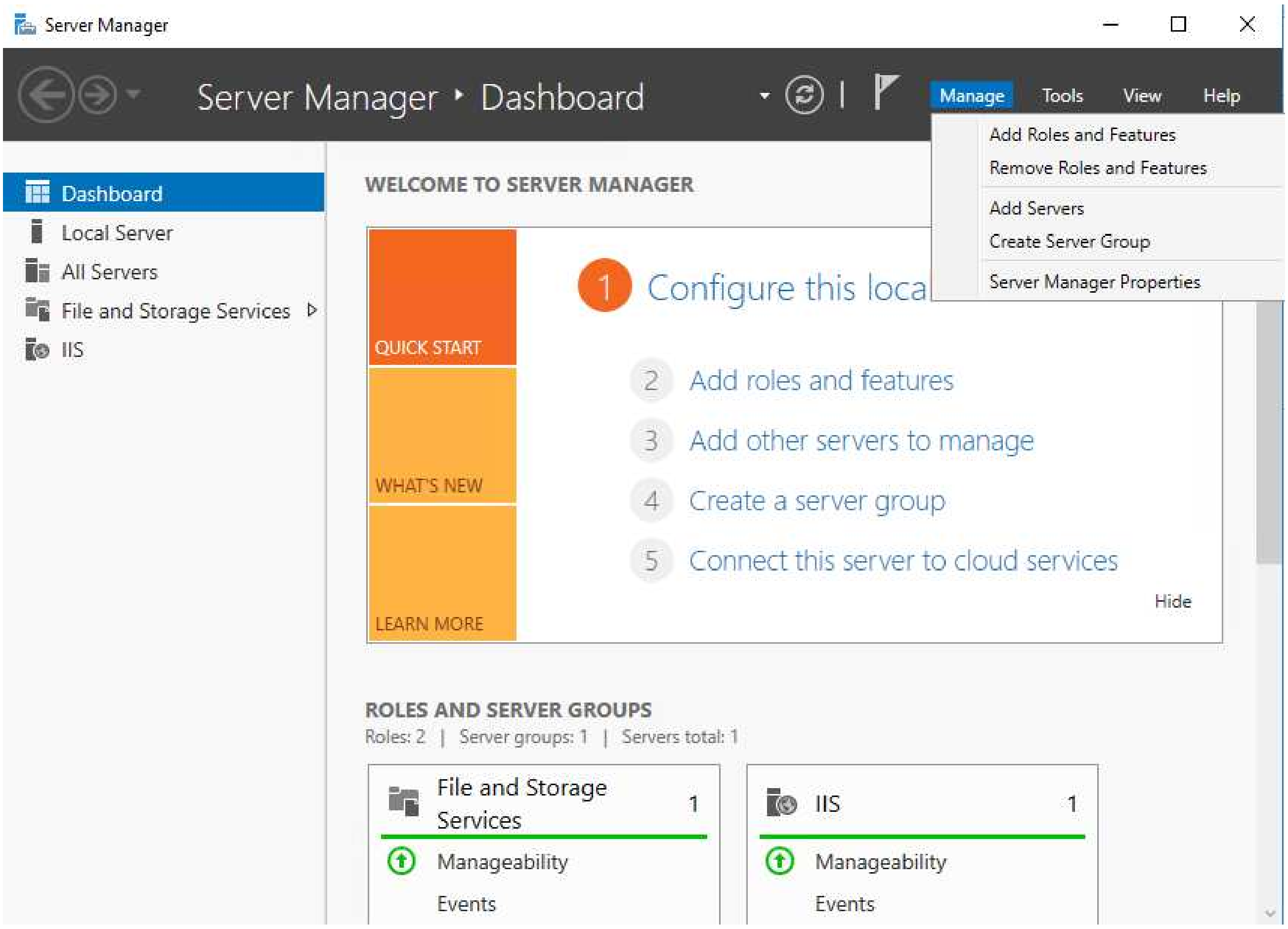
1. In Windows Operating System turn on IIS and its features:

   From Control Panel: "Turn Windows features on or off"

   Or

   From Server Manager: Add Roles and features (https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager#start-server-manager)

2. Click **Manage** > **Add Roles and features**.



3. In the pop-up Wizard, click **Next.**
   The **Server Roles** page is displayed.

4. Select: **Web Server (IIS).**

5. If prompted click **Add Features**.

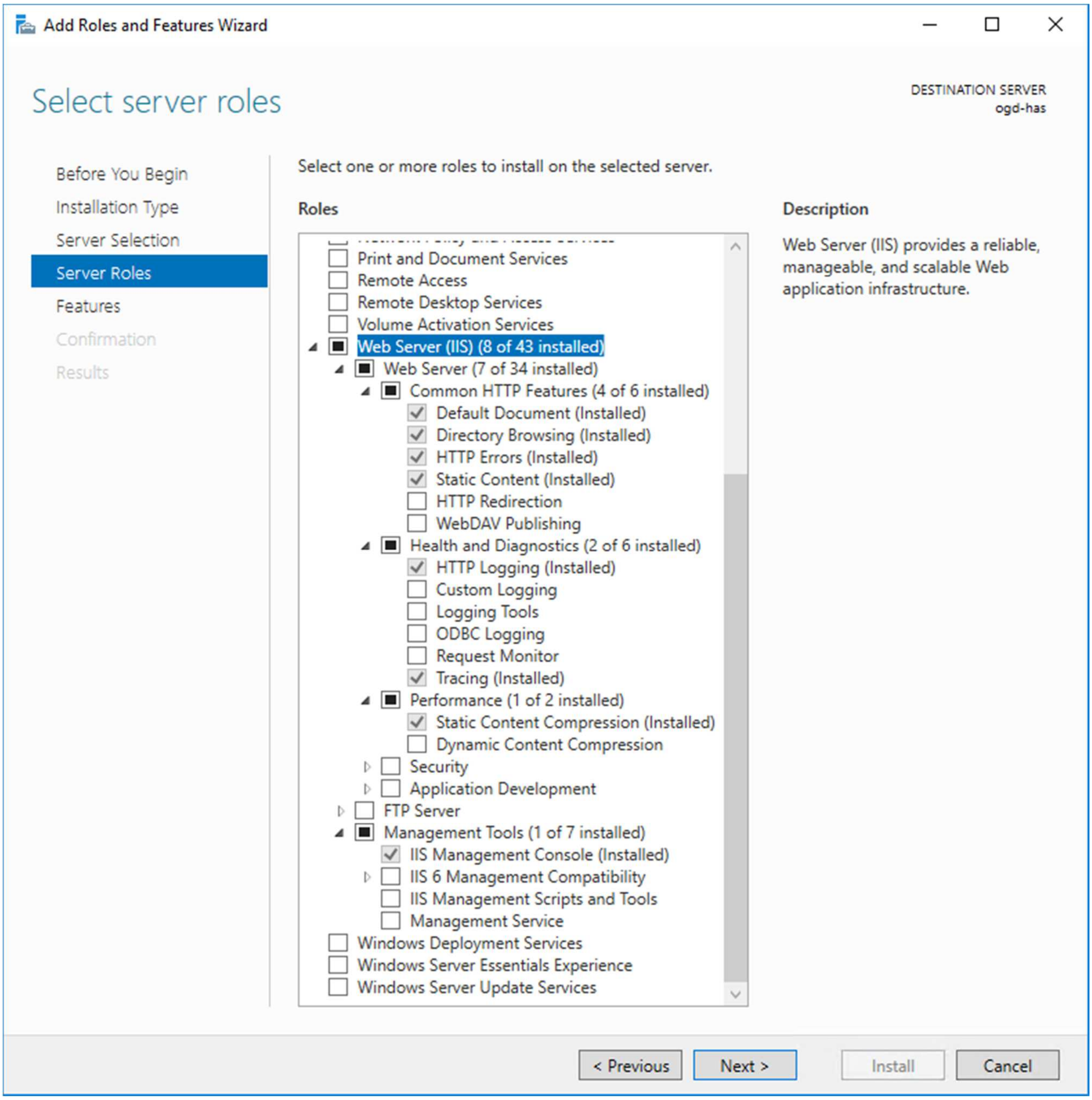
6. Ensure the following options are selected:

Web Server:

- Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - Static Content
- Health and Diagnostics
  - HTTP Logging
  - Tracing
- Performance
  - Static Content Compression

Management Tools:

- IIS Management Console



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
ogd-has

Select one or more roles to install on the selected server.

Roles

- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (8 of 43 installed)
  - ■ Web Server (7 of 34 installed)
    - ■ Common HTTP Features (4 of 6 installed)
      - ☑ Default Document (Installed)
      - ☑ Directory Browsing (Installed)
      - ☑ HTTP Errors (Installed)
      - ☑ Static Content (Installed)
      - □ HTTP Redirection
      - □ WebDAV Publishing
    - ■ Health and Diagnostics (2 of 6 installed)
      - ☑ HTTP Logging (Installed)
      - □ Custom Logging
      - □ Logging Tools
      - □ ODBC Logging
      - □ Request Monitor
      - ☑ Tracing (Installed)
    - ■ Performance (1 of 2 installed)
      - ☑ Static Content Compression (Installed)
      - □ Dynamic Content Compression
    - □ Security
    - □ Application Development
  - □ FTP Server
  - ■ Management Tools (1 of 7 installed)
    - ☑ IIS Management Console (Installed)
    - □ IIS 6 Management Compatibility
    - □ IIS Management Scripts and Tools
    - □ Management Service
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

7. Click **Next** to **Install IIS** and its related features.

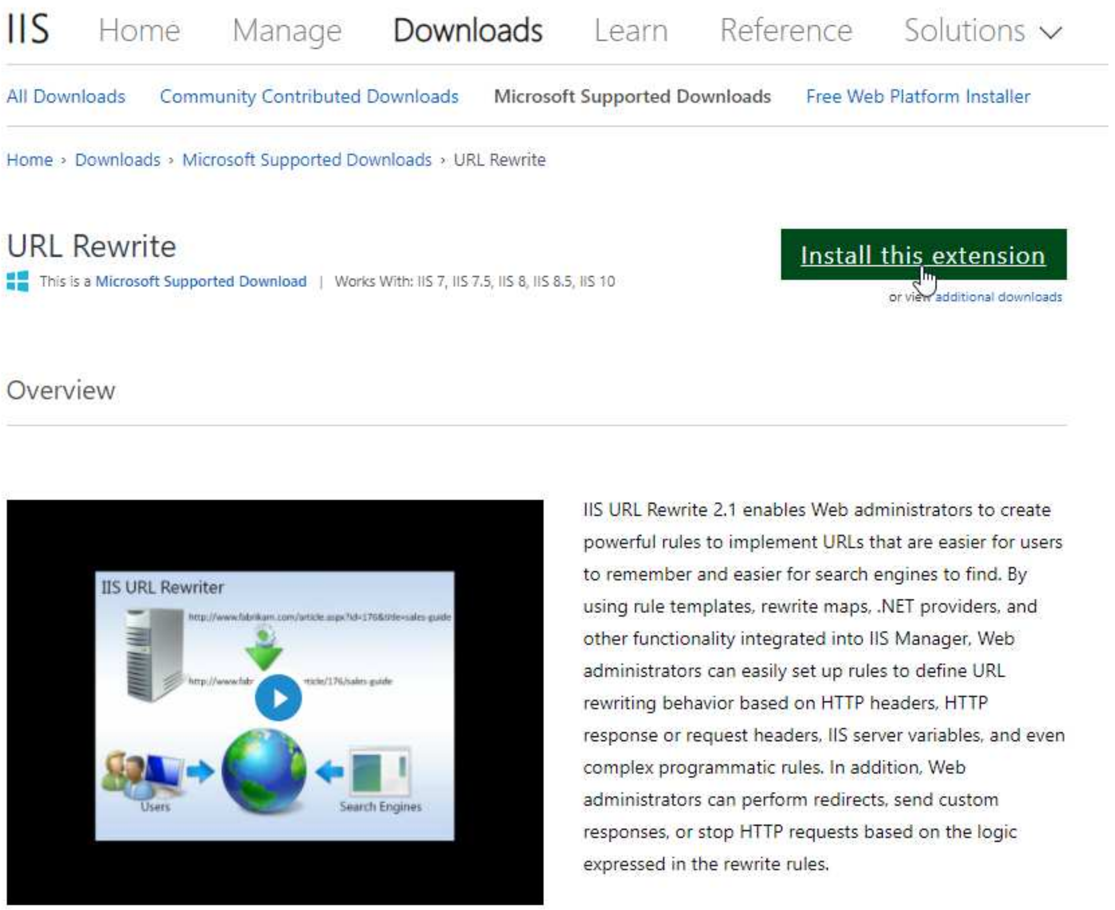
2.3. Installing URL Rewrite

URL Rewrite is tightly integrated with IIS Manager and is a prerequisite for ARR to work as expected.

To install URL Rewrite:

1. Download "**rewrite_amd64_en-US.msi**" URL Rewrite from official IIS website: https://www.iis.net/downloads/microsoft/url-rewrite.

2. Click **Install this extension** to get the **Web installer**.


IIS
Home
Manage
Downloads
Learn
Reference
Solutions
All Downloads
Community Contributed Downloads
Microsoft Supported Downloads
Free Web Platform Installer
Home › Downloads › Microsoft Supported Downloads › URL Rewrite
Install this extension
or view additional downloads
IIS URL Rewriter
Users
Search Engines

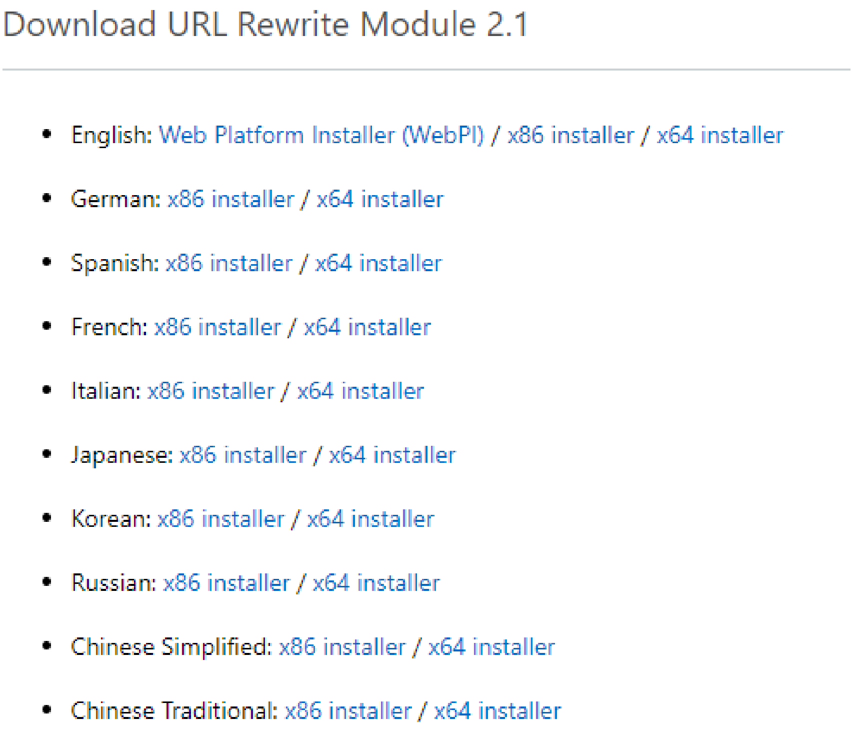
URL Rewrite

This is a Microsoft Supported Download | Works With: IIS 7, IIS 7.5, IIS 8, IIS 8.5, IIS 10

Overview

IIS URL Rewrite 2.1 enables Web administrators to create powerful rules to implement URLs that are easier for users to remember and easier for search engines to find. By using rule templates, rewrite maps, .NET providers, and other functionality integrated into IIS Manager, Web administrators can easily set up rules to define URL rewriting behavior based on HTTP headers, HTTP response or request headers, IIS server variables, and even complex programmatic rules. In addition, Web administrators can perform redirects, send custom responses, or stop HTTP requests based on the logic expressed in the rewrite rules.

3. Scroll down to **Download URL Rewrite Module** section to select an **offline installer.**



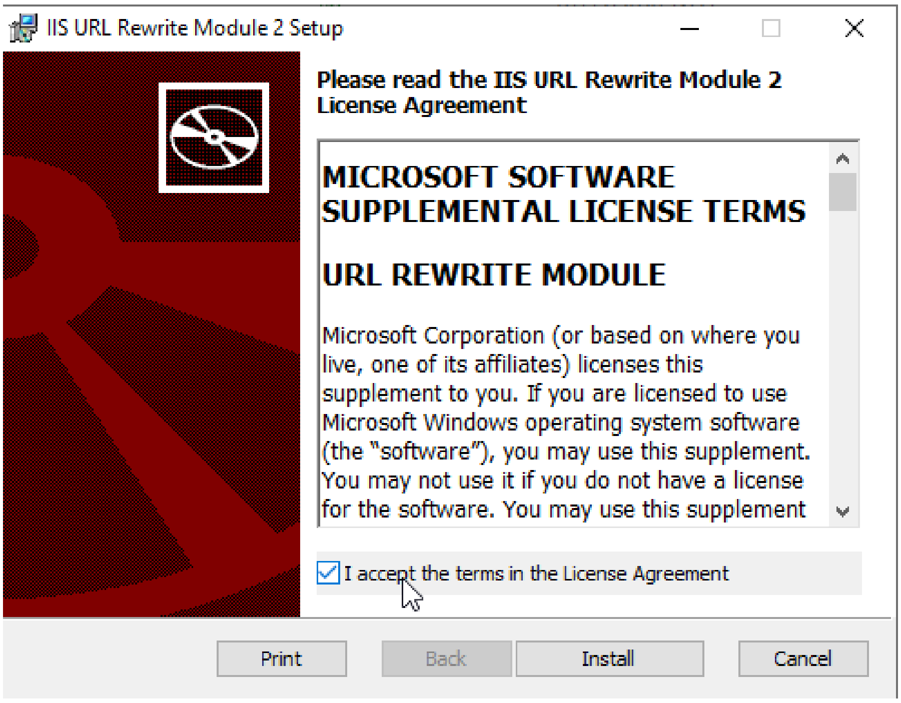
Download URL Rewrite Module 2.1

- English: Web Platform Installer (WebPI) / x86 installer / x64 installer
- German: x86 installer / x64 installer
- Spanish: x86 installer / x64 installer
- French: x86 installer / x64 installer
- Italian: x86 installer / x64 installer
- Japanese: x86 installer / x64 installer
- Korean: x86 installer / x64 installer
- Russian: x86 installer / x64 installer
- Chinese Simplified: x86 installer / x64 installer
- Chinese Traditional: x86 installer / x64 installer

4. Choose:
   - **Web Platform Installer** if the server has **internet access** connection.
   - **x64 installer** if the server does not have internet access.

5. Launch the installer:

   a) Select **Accept the terms in the License Agreement**, then click **Install**.



Please read the IIS URL Rewrite Module 2 License Agreement

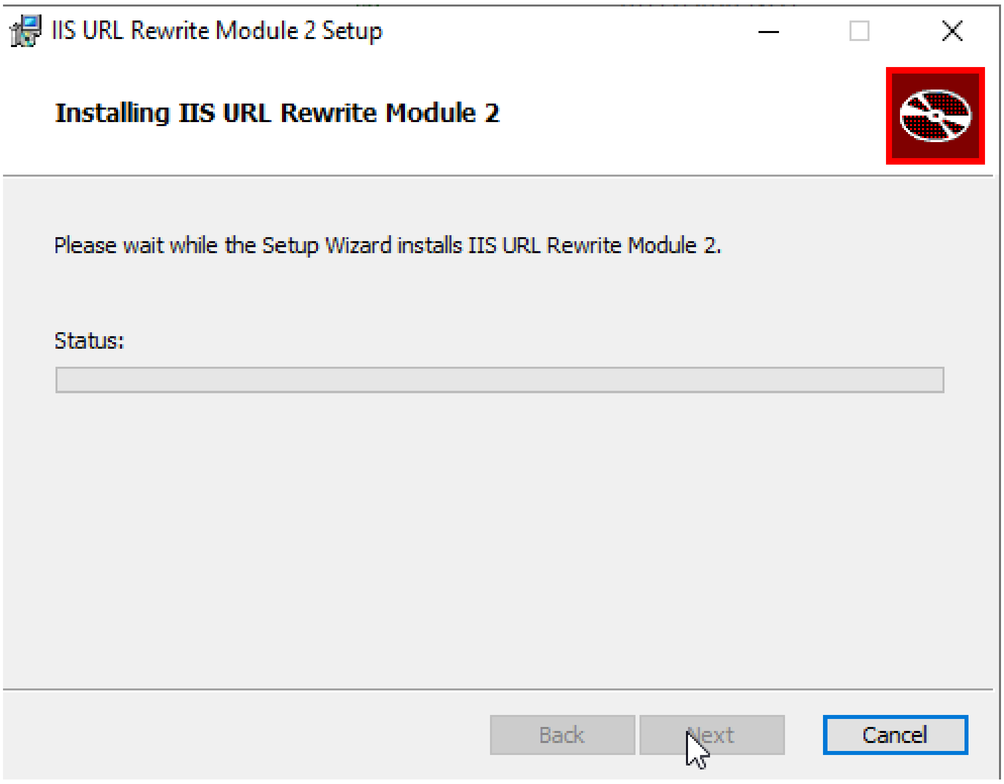
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

URL REWRITE MODULE

Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows operating system software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use this supplement

☑ I accept the terms in the License Agreement

   b) Click **Next** if needed.



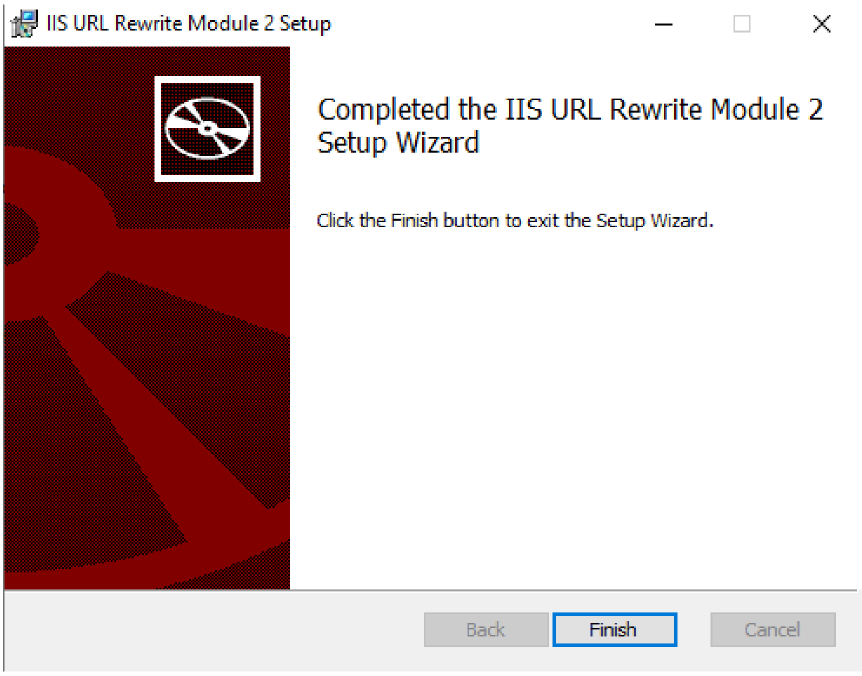
IIS URL Rewrite Module 2 Setup

Installing IIS URL Rewrite Module 2

Please wait while the Setup Wizard installs IIS URL Rewrite Module 2.

Status:

c) Click **Finish**.



IIS URL Rewrite Module 2 Setup

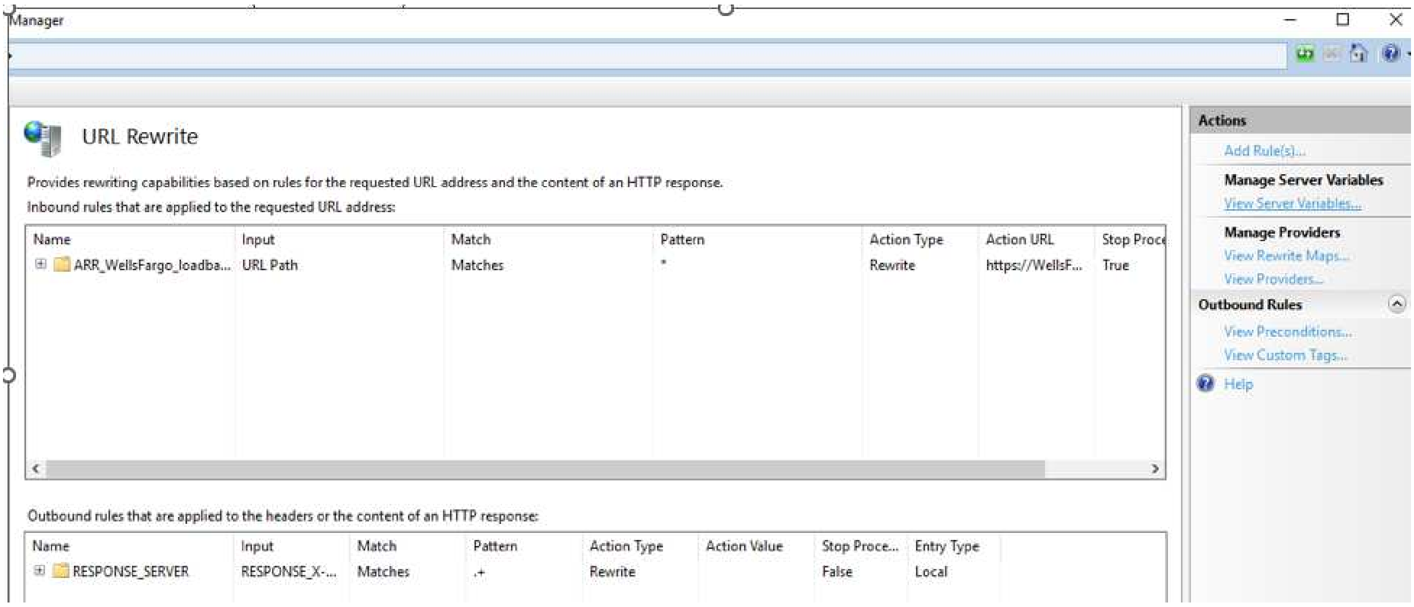
Completed the IIS URL Rewrite Module 2 Setup Wizard

Click the Finish button to exit the Setup Wizard.

2.3.1. Security: removing X-Powered-By header

To remove x-powered-by header:

1. Access **URL Rewrite**.



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	Action URL	Stop Proce
ARR_WellsFargo_loadba...	URL Path	Matches	*	Rewrite	https://WellsF...	True

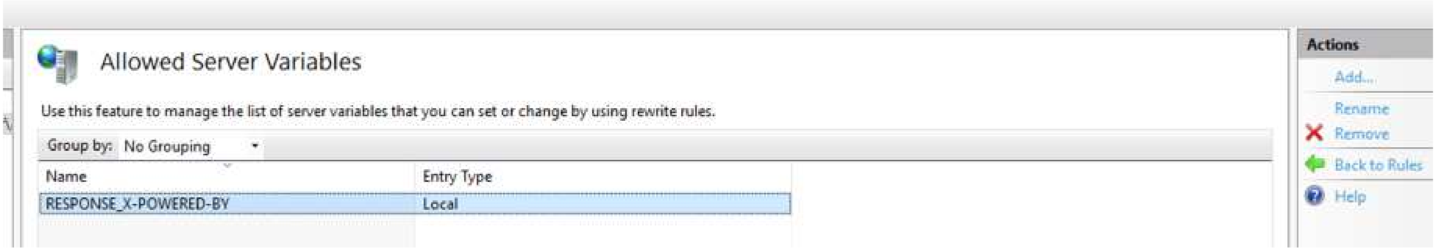
Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type	Action Value	Stop Proce...	Entry Type
RESPONSE_SERVER	RESPONSE_X-...	Matches	.+	Rewrite		False	Local

2. Create a variable:

a) in **Actions > Manage Server Variables**, click **View Server variables**.

b) **Add** the **RESPONDE_X-POWERED-BY** variable.



Allowed Server Variables

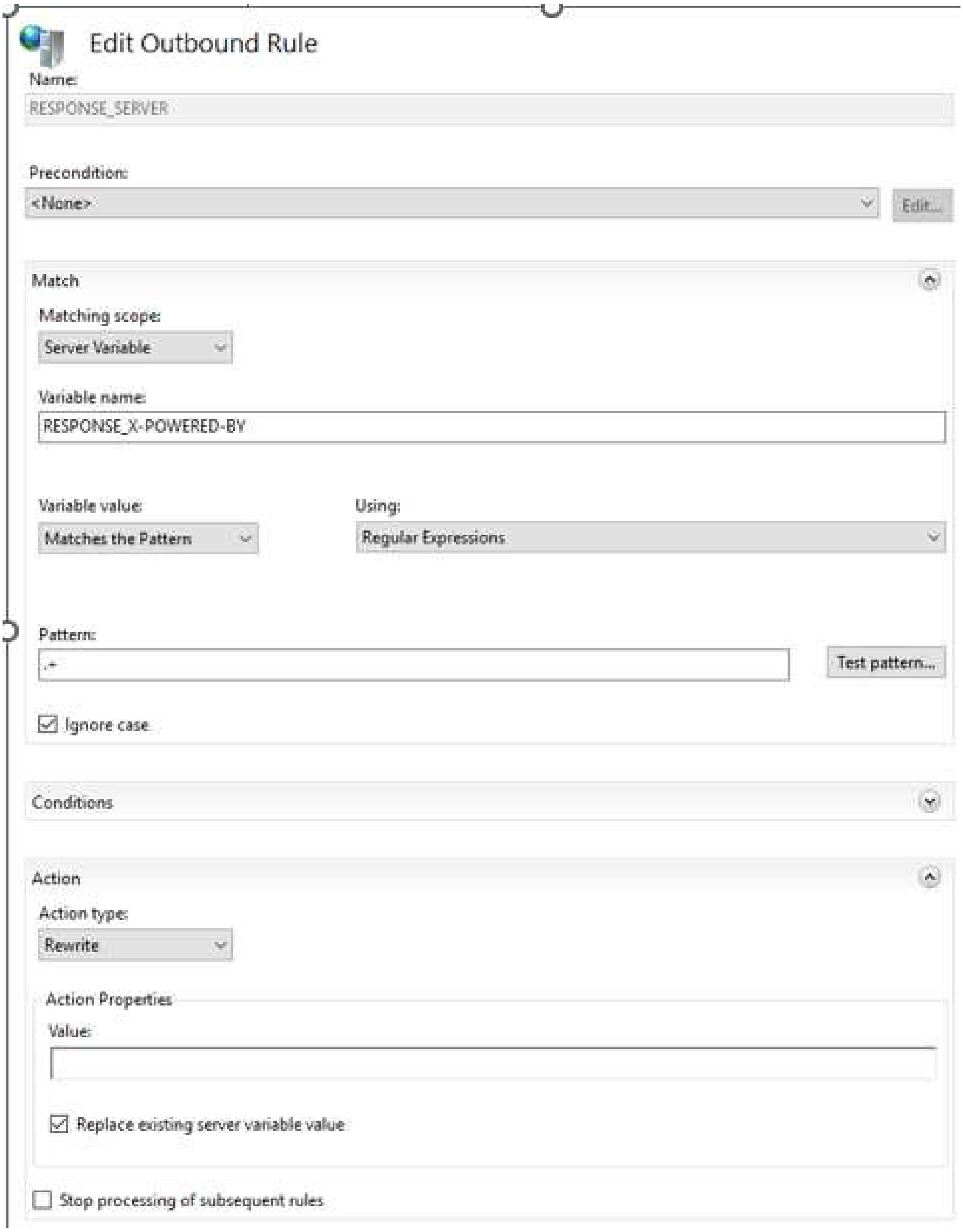
Use this feature to manage the list of server variables that you can set or change by using rewrite rules.

Group by: No Grouping

Name	Entry Type
RESPONSE_X-POWERED-BY	Local

3. At rule level, **Add** an **Outbound Rule**.

For more details see https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710



Edit Outbound Rule

Name:
RESPONSE_SERVER

Precondition:
<None>

Match

Matching scope:
Server Variable

Variable name:
RESPONSE_X-POWERED-BY

Variable value:
Matches the Pattern

Using:
Regular Expressions

Pattern:
.+

☑ Ignore case

Conditions

Action

Action type:
Rewrite

Action Properties

Value:

☑ Replace existing server variable value

□ Stop processing of subsequent rules

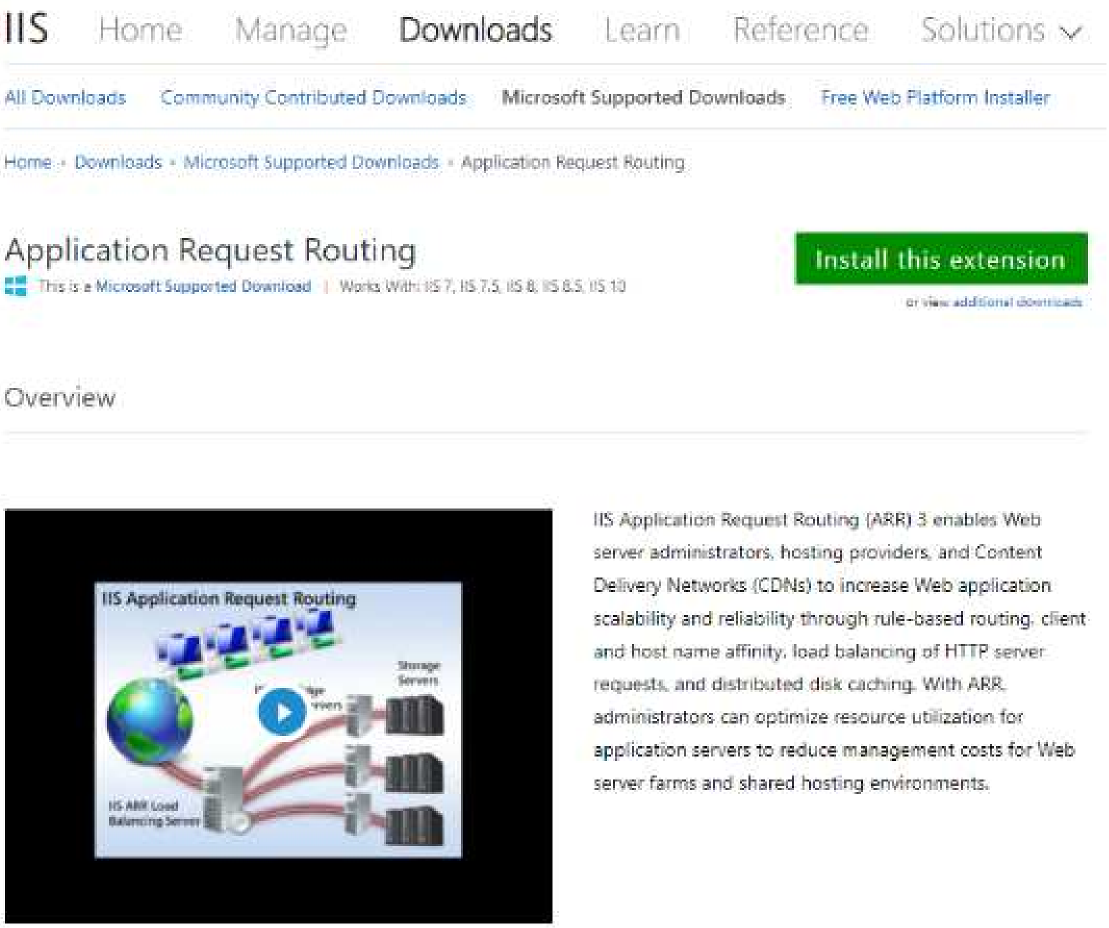
2.4. Installing ARR

IIS Application Request Routing (ARR) is required to map the official "URL DNS" to the HAS server farm that will handle the web request.

To install IIS ARR:

1. Download IIS Application Request Routing (ARR) 3.0 "**requestRouter_amd64.msi**" from the official website: https://www.iis.net/downloads/microsoft/application-request-routing

   ARR depends on URL Rewrite. Make sure URL Rewrite is installed prior to installing ARR. Alternatively, use the Microsoft Web Platform Installer link instead, which installs the ARR and its dependency in the right order.



IIS
Home
Manage
Downloads
Learn
Reference
Solutions
All Downloads
Community Contributed Downloads
Microsoft Supported Downloads
Free Web Platform Installer
Home › Downloads › Microsoft Supported Downloads › Application Request Routing
Install this extension
or view additional downloads
IIS Application Request Routing
Storage Servers
IIS ARR Load Balancing Server

Application Request Routing

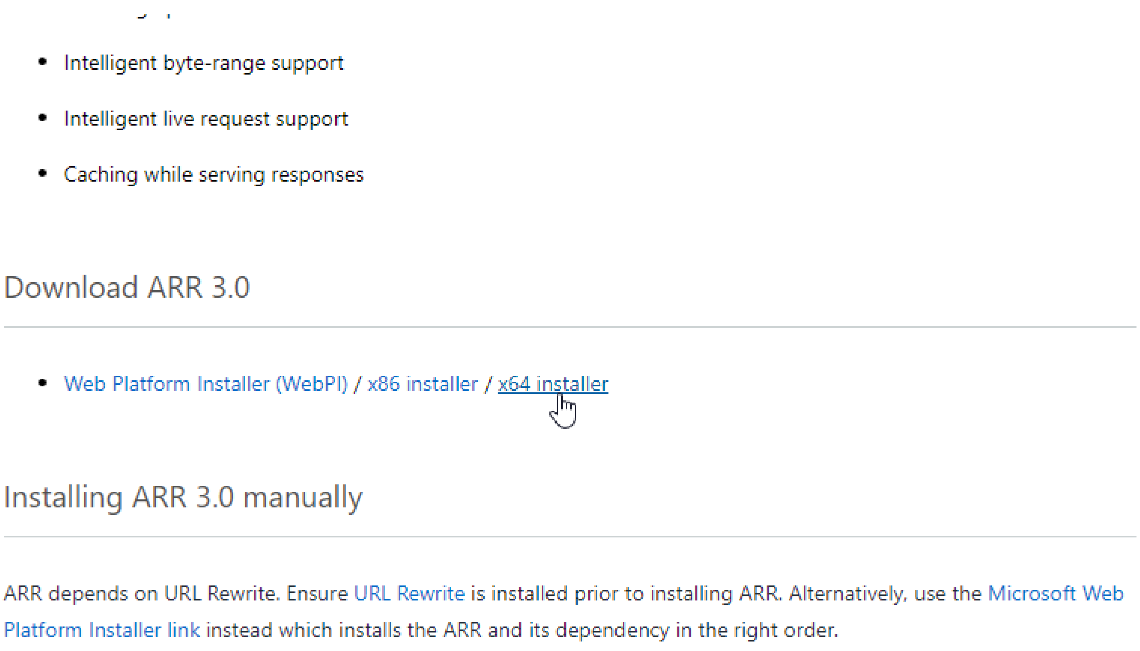
This is a Microsoft Supported Download | Works With: IIS 7, IIS 7.5, IIS 8, IIS 8.5, IIS 10

Overview

IIS Application Request Routing (ARR) 3 enables Web server administrators, hosting providers, and Content Delivery Networks (CDNs) to increase Web application scalability and reliability through rule-based routing, client and host name affinity, load balancing of HTTP server requests, and distributed disk caching. With ARR, administrators can optimize resource utilization for application servers to reduce management costs for Web server farms and shared hosting environments.

2. For online server: click **Install this extension** to get the **Web installer**.

   Or for offline server: scroll down to **Download URL Rewrite Module** section to select an **offline installer**.



- Intelligent byte-range support
- Intelligent live request support
- Caching while serving responses

Download ARR 3.0

- Web Platform Installer (WebPI) / x86 installer / x64 installer

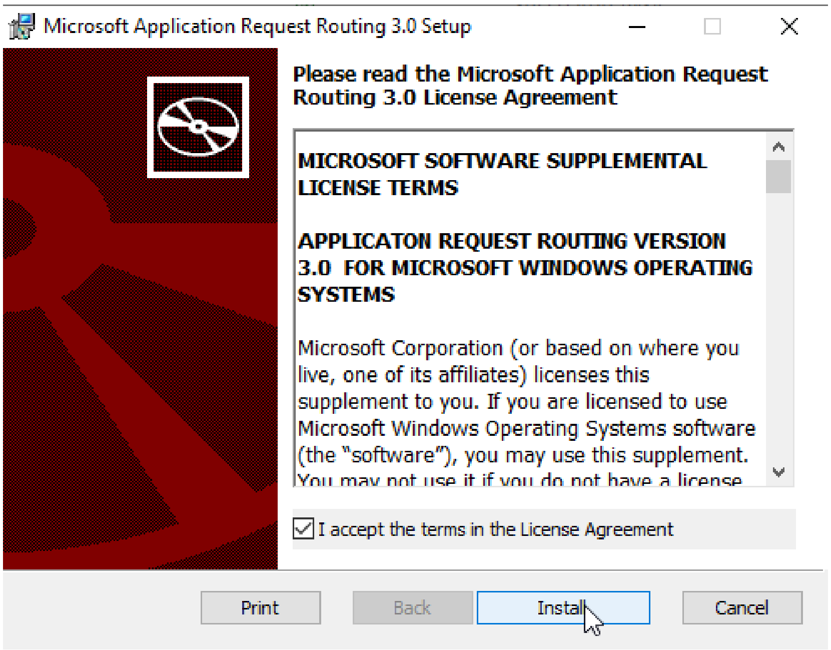
Installing ARR 3.0 manually

ARR depends on URL Rewrite. Ensure URL Rewrite is installed prior to installing ARR. Alternatively, use the Microsoft Web Platform Installer link instead which installs the ARR and its dependency in the right order.

3. Choose:
- **Web Platform Installer** if the server has **internet** access connection
- **x64 installer** if the server does not have internet access

4. Launch the installer:

a) Select **Accept the terms in the License Agreement**, then click **Install**.



Microsoft Application Request Routing 3.0 Setup

Please read the Microsoft Application Request Routing 3.0 License Agreement

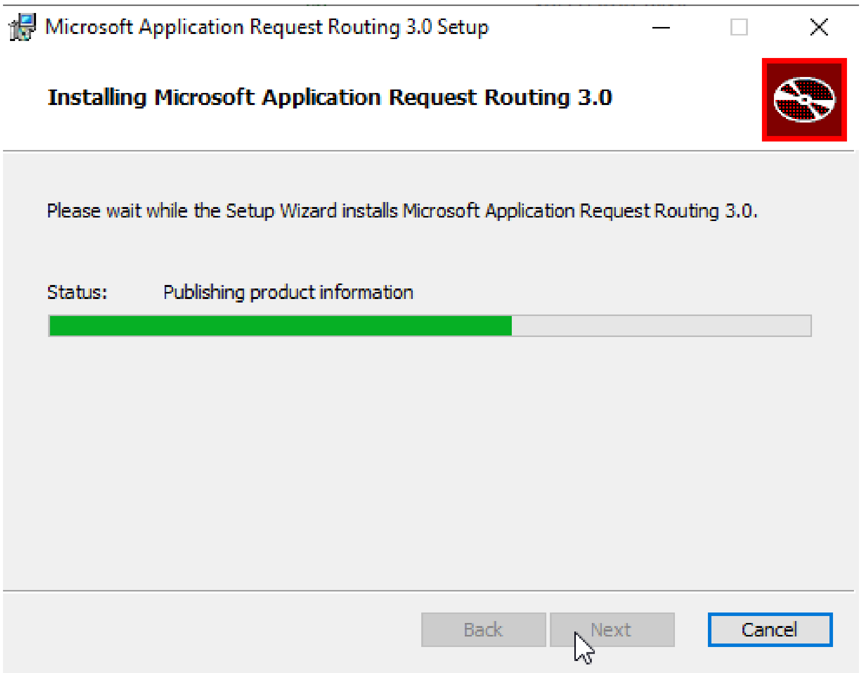
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

APPLICATON REQUEST ROUTING VERSION 3.0 FOR MICROSOFT WINDOWS OPERATING SYSTEMS

Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows Operating Systems software (the "software"), you may use this supplement. You may not use it if you do not have a license

☑ I accept the terms in the License Agreement

b) Click **Next** if needed.

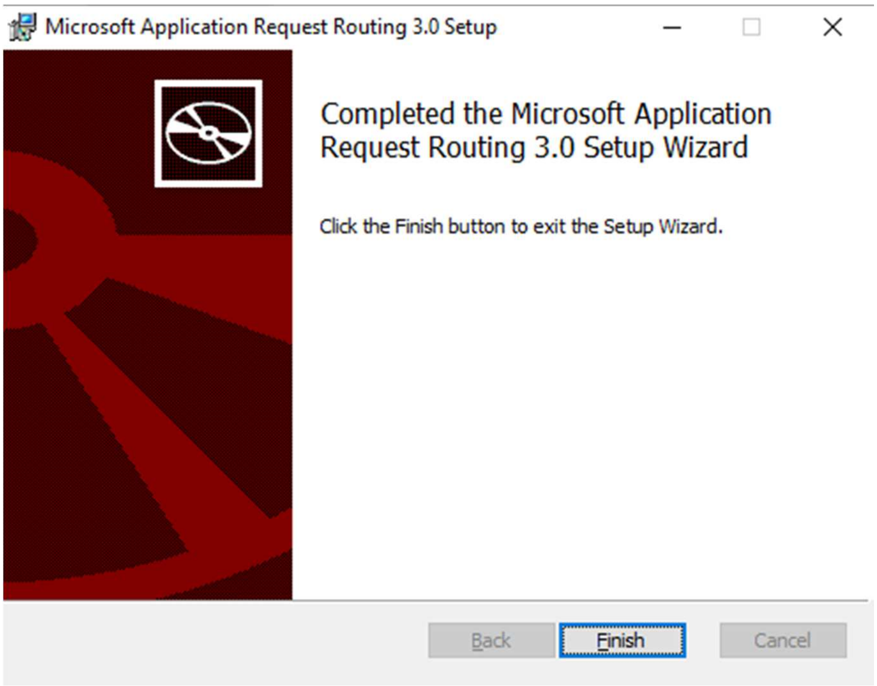

Microsoft Application Request Routing 3.0 Setup

Installing Microsoft Application Request Routing 3.0

Please wait while the Setup Wizard installs Microsoft Application Request Routing 3.0.

Status: Publishing product information

c) Click **Finish**.


Microsoft Application Request Routing 3.0 Setup

Completed the Microsoft Application Request Routing 3.0 Setup Wizard

Click the Finish button to exit the Setup Wizard.

2.5. Configuring Sites

Caution: this configuration may change if you leverage an existing IIS Server

In that configuration the IIS server is dedicated to HOPEX Application Server Deployment.

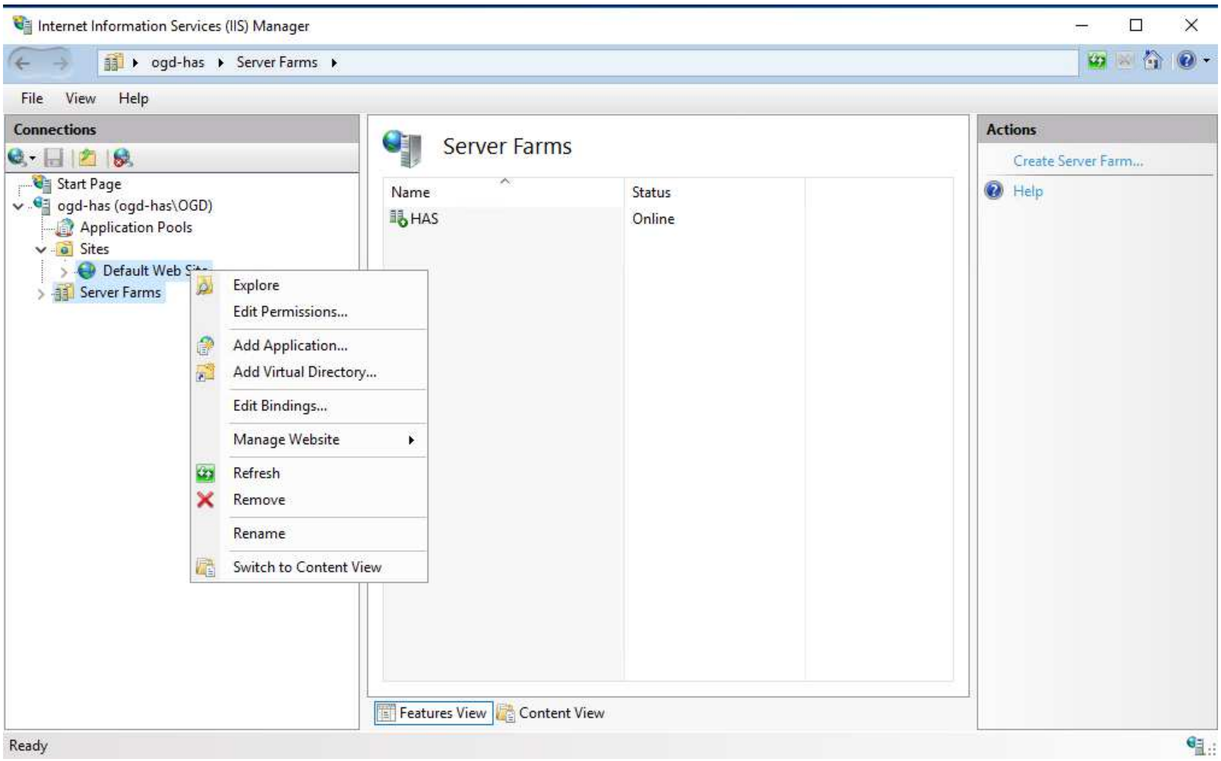
There is no other Website expose by this IIS Server. Should there be other website you will need to adjust URL rewrite rules.

The following steps detail how to configure the IIS Server on HTTP (80) or HTTPS (443).

You must choose one or the other. A mix of HTTPS and HTTP **is not allowed**.

To configure Sites:

1. Right-click **Default Web Site** and select **Edit Binding**.



2. For:

   an HTTP configuration, see section 2.5.1 Configuring HTTP port 80.

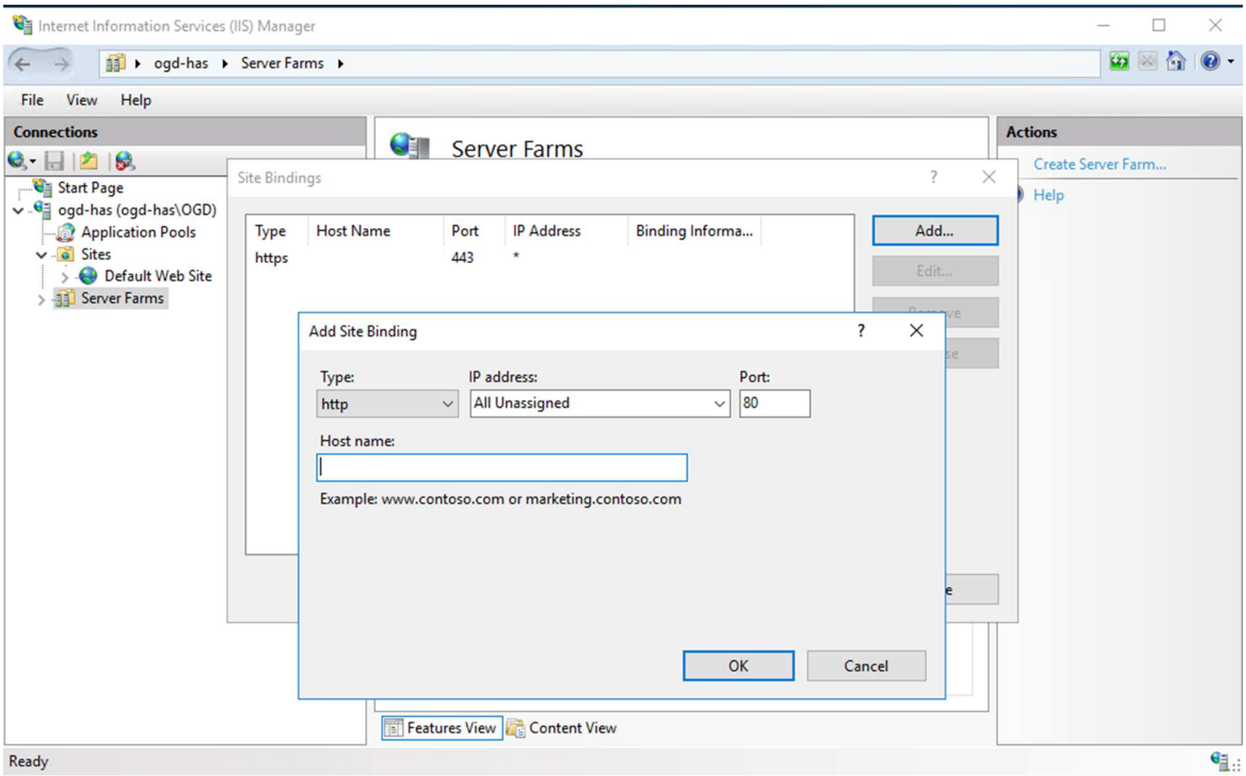
   an HTTPS configuration, see section 2.5.2 Configuring HTTPS port 443.

2.5.1. Configuring HTTP port 80

To perform an HTTP configuration (if not already configured):

1. Click **Add** (or click **Edit** on existing 80).

   - In the **Type** field, select “http”.
   - In the **IP address** field, select “All unassigned”.
   - In the **Port** field, enter: “80”.



Type	Host Name	Port	IP Address	Binding Informa...
https		443	*	

Add Site Binding

Type: http

IP address: All Unassigned

Port: 80

Host name:

Example: www.contoso.com or marketing.contoso.com

2. Click **OK**.

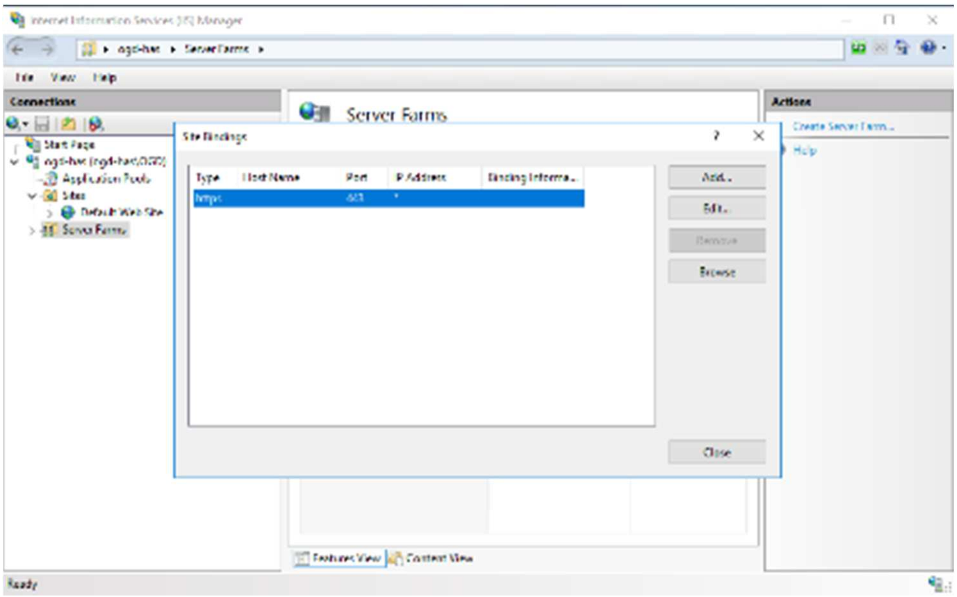
3. Click **Close**.

In that context, remove existing HTTPS.

2.5.2. Configuring HTTPS port 443

To perform an HTTPS configuration (if not already configured):

1. Click **Add** (or click **Edit** on existing 443).



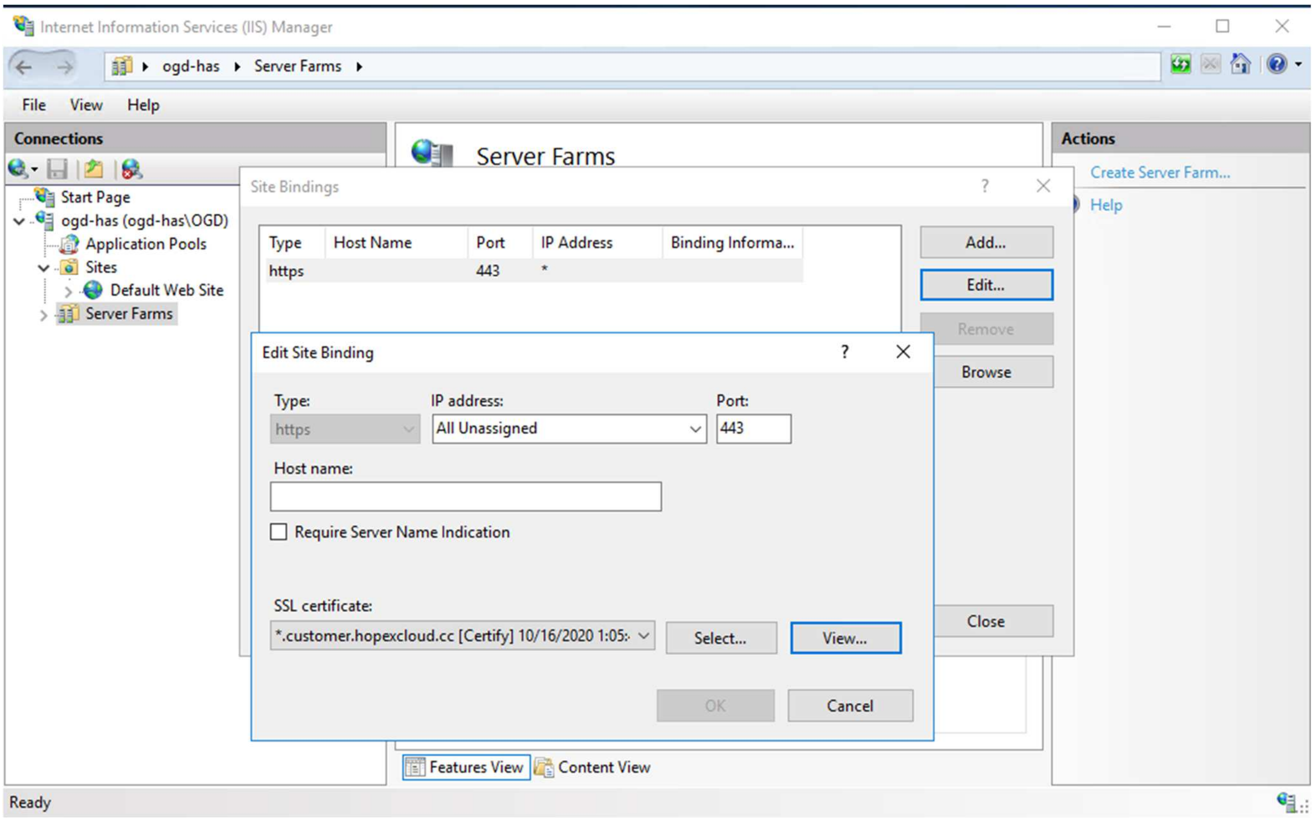
Type	Host Name	Port	IP Address	Binding Informa...
https		443	*	

2. In:

- the **Type** field, select “https”.
- the **IP address** field, select “All unassigned”.
- the **Port** field, enter: 443.

3. Click **OK**.
4. Select appropriate **SSL Certificate** (the one imported from above step 2.1 Adding SSL Certificate).
5. Click **Close**.

➔



Type	Host Name	Port	IP Address	Binding Informa...
https		443	*	

Type: https

IP address: All Unassigned

Port: 443

Host name:

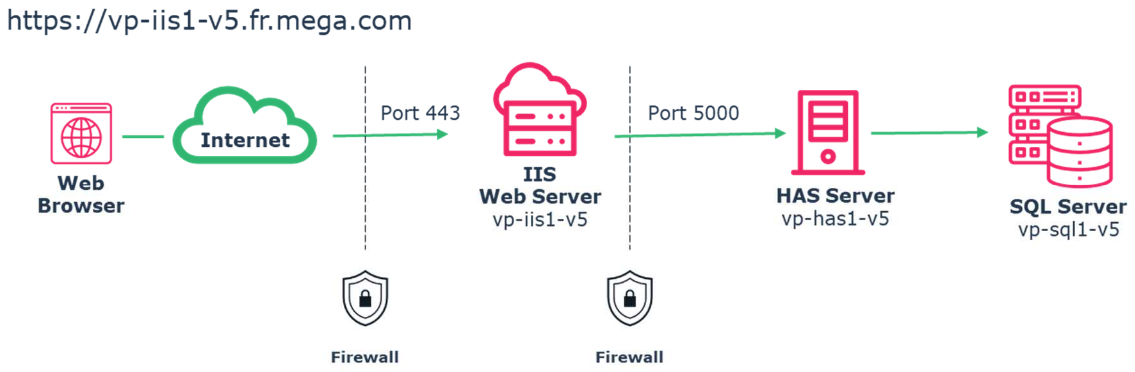
□ Require Server Name Indication

SSL certificate: *.customer.hopexcloud.cc [Certify] 10/16/2020 1:05:

6. In that context, remove existing HTTP.

2.6. Configuring Server Farm - ARR

ARR will allow to redirect the request send to the “IIS Server” to the “HAS Server”.



In that configuration there is:

One public URL DNS that will be https://vp-iis1-v5.fr.mega.com

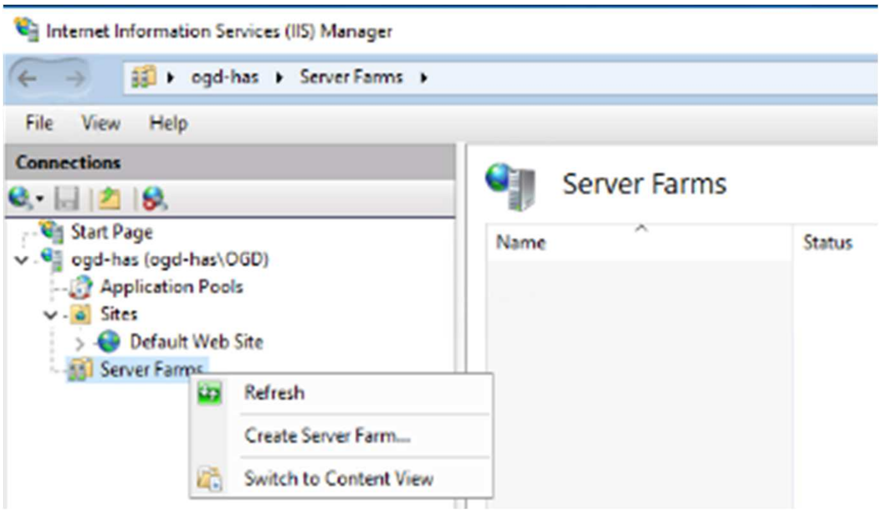
One HAS Server named "vp-has1-V5" installed on port 5000.

You need to adjust the following instruction to your own URL and server name.

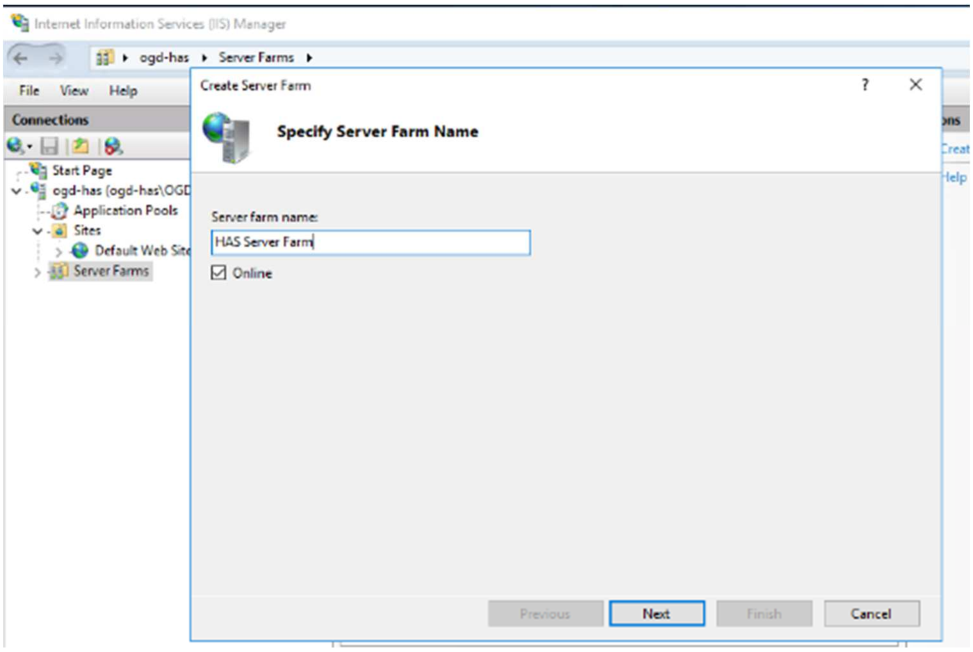
2.6.1. Creating a Server farms

Even if you have a single server, perform the following:

1. Right-click the **Server Farm** root level and select **Create Server Farm**.



2. Enter a name to the server farm: for instance, "HAS Server Farm PROD".



Server farm name: HAS Server Farm

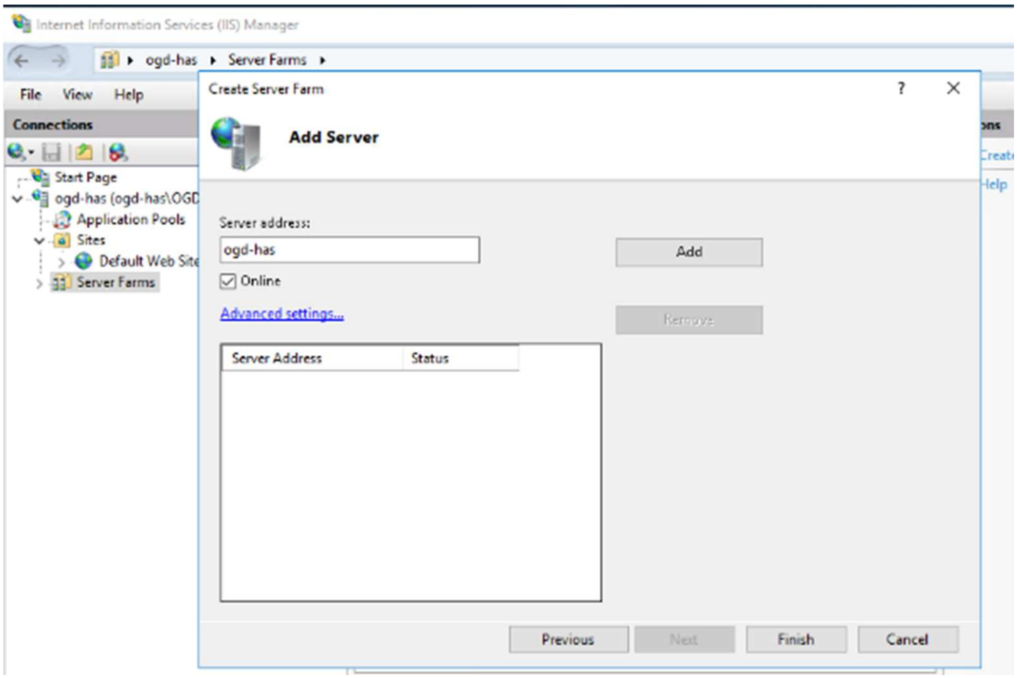
☑ Online

If you have several instances, give an explicit name to the farm
HAS Instance 1 – PROD - 5000
HAS Instance 2 – PRE-PROD 5001

3. Click **Next**.

4. In the server address enter **the name of the server (entering an IP address is not supported)**. In that example: vp-has1-v5

5. Click **Advanced settings**.



Server address: ogd-has

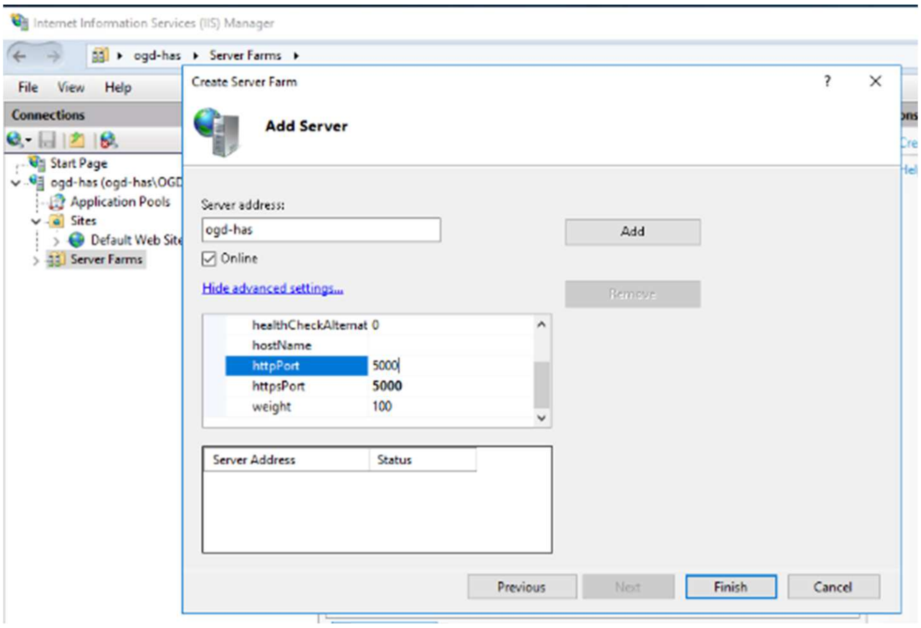
☑ Online

6. . Scroll to **always put both port** (HTTP/HTTPS)

   ○ **HTTP port**, enter 5000

- **HTTPs port**, enter 5000

7. Click **Add.**



Server address: ogd-has

☑ Online

Hide advanced settings...

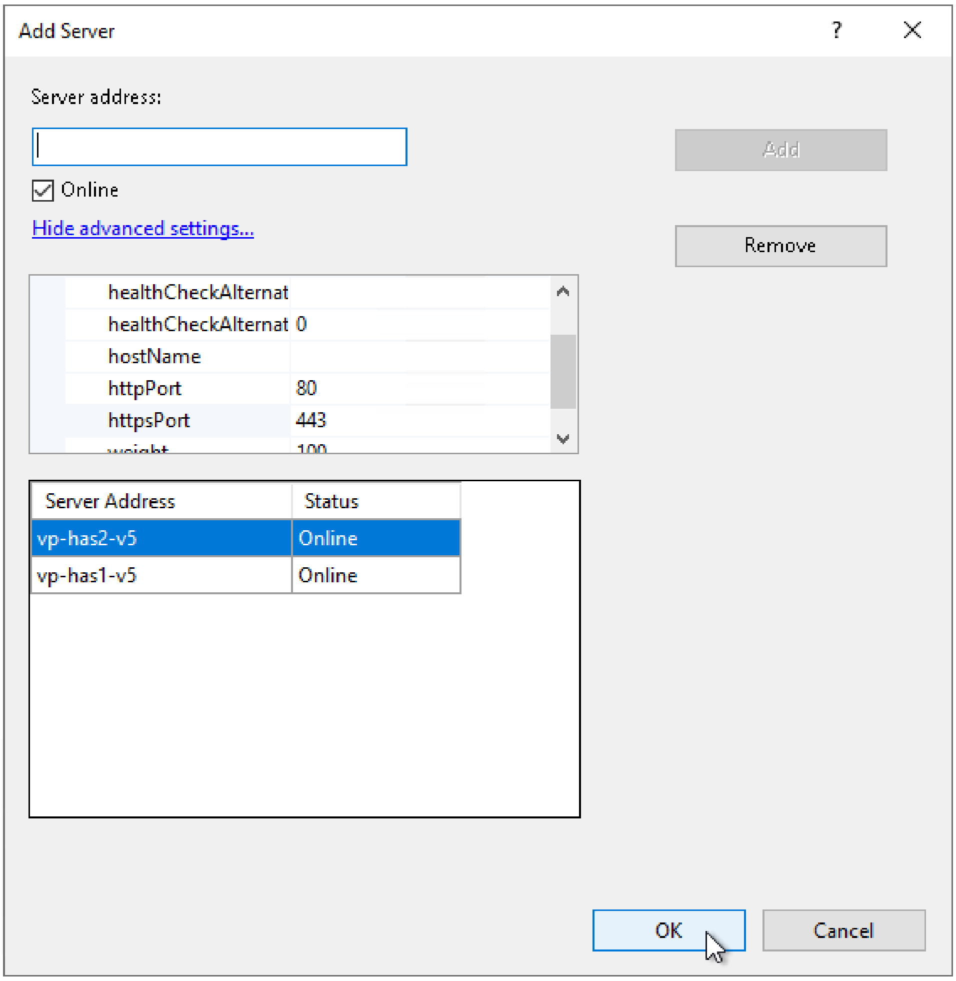
healthCheckAlternat	0
hostName	
httpPort	5000
httpsPort	5000
weight	100

Server Address	Status

8. Repeat this operation **for each HAS Server of the cluster.**

You now need to add each server of the cluster. If you have a single server for HAS then you need to put this server.

Example: with two HAS server names “vp-has1-v5” and “vp-has2-v5”.



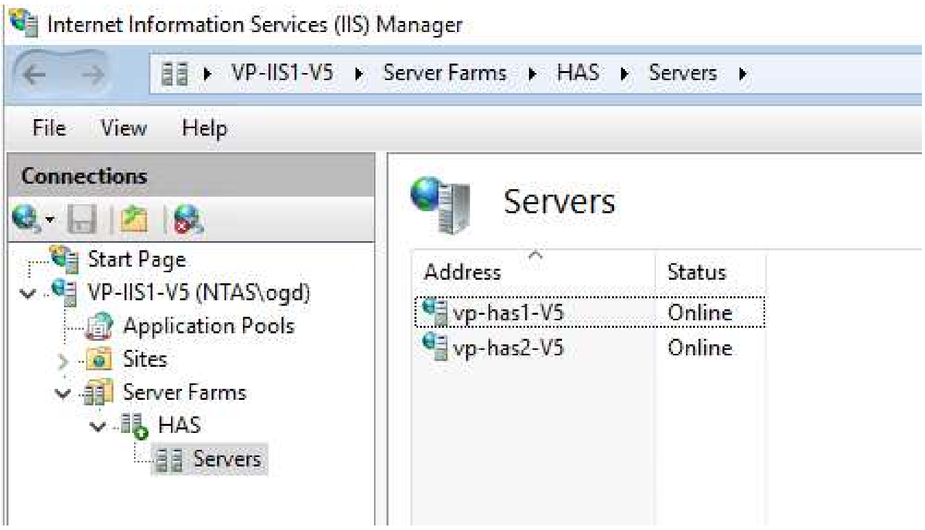
Server address:

☑ Online

healthCheckAlternat	
healthCheckAlternat	0
hostName	
httpPort	80
httpsPort	443
weight	100

Server Address	Status
vp-has2-v5	Online
vp-has1-v5	Online

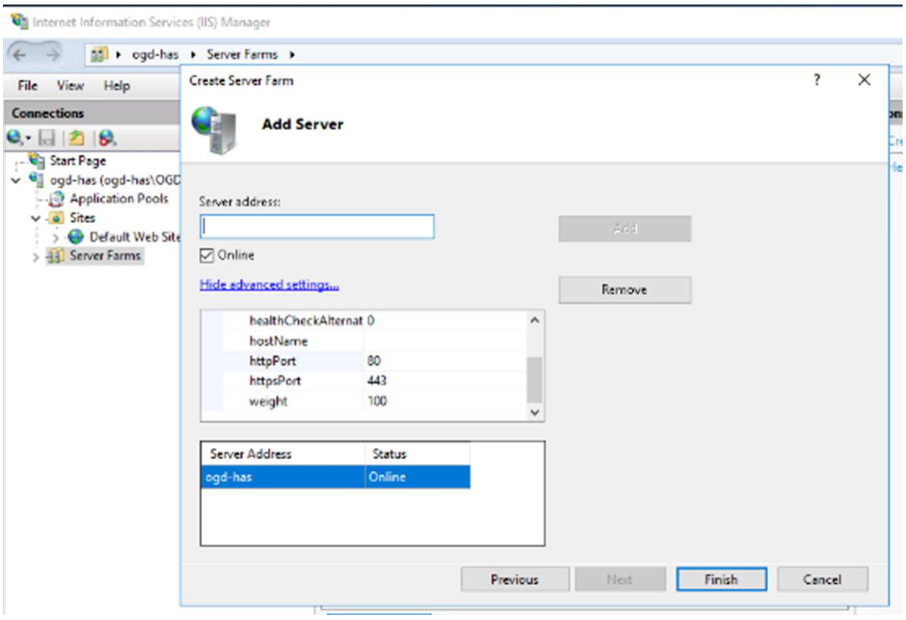
➔



Servers

Address	Status
vp-has1-V5	Online
vp-has2-V5	Online

7. Click **Finish**.



Internet Information Services (IIS) Manager

ogd-has ▸ Server Farms ▸

File View Help

Connections

- Start Page
- ogd-has (ogd-has\OGD
  - Application Pools
  - Sites
    - Default Web Site
  - Server Farms

Create Server Farm

Add Server

Server address:

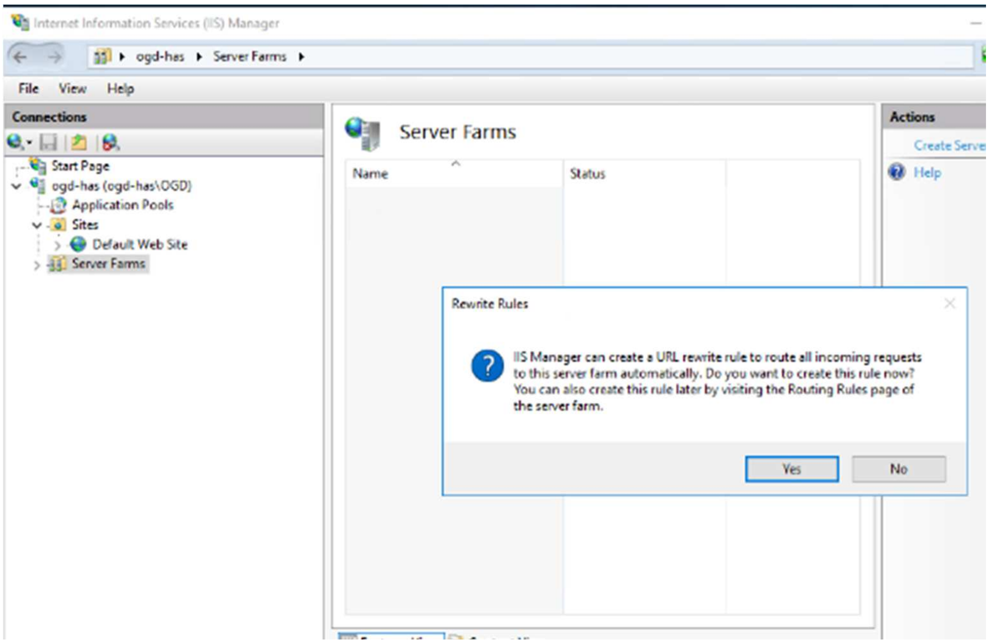
☑ Online

Hide advanced settings...

healthCheckAlternat	0
hostName	
httpPort	80
httpsPort	443
weight	100

Server Address	Status
ogd-has	Online

8. When prompted click **Yes** to create the URL Rewrite rule.



Internet Information Services (IIS) Manager

ogd-has ▸ Server Farms ▸

File View Help

Connections

- Start Page
- ogd-has (ogd-has\OGD)
  - Application Pools
  - Sites
    - Default Web Site
  - Server Farms

Server Farms

Name	Status

Actions

Create Serve

Help

Rewrite Rules

IIS Manager can create a URL rewrite rule to route all incoming requests to this server farm automatically. Do you want to create this rule now? You can also create this rule later by visiting the Routing Rules page of the server farm.

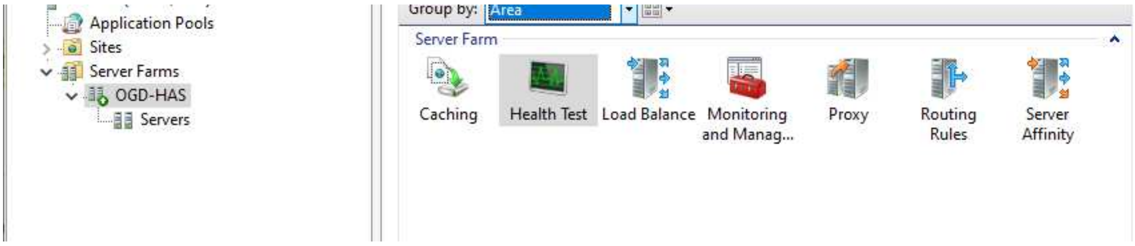
If you do not get prompted to create the URL Rewrite rule it means URL rewrite might not be installed. You must install it and then create the rule manually.

2.6.2. Configuring the Health Test

To configure the Health Test:

1. Select the Server Farms you have just created.

2. Double-click **Health Test**.

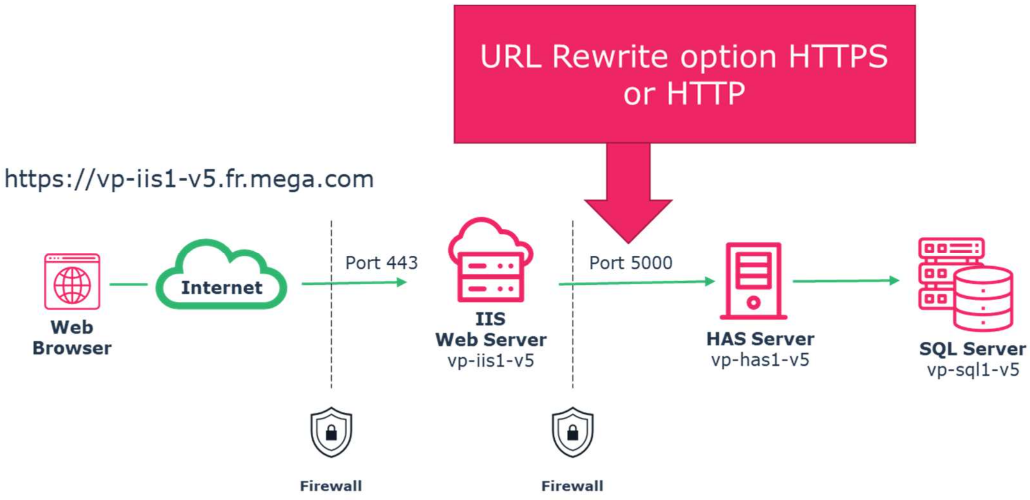


3. In the input URL add the server URL:

Always write "localhost" regardless of your public URL/DNS.

- HTTP: http://localhost/admin/cluster/node/health
- HTTP**S**: http**s**://localhost/admin/cluster/node/health

Choose HTTP or HTTPS depending on how the instance node has been configured. See corresponding chapter for more details "4 SSL Certificates configuration"

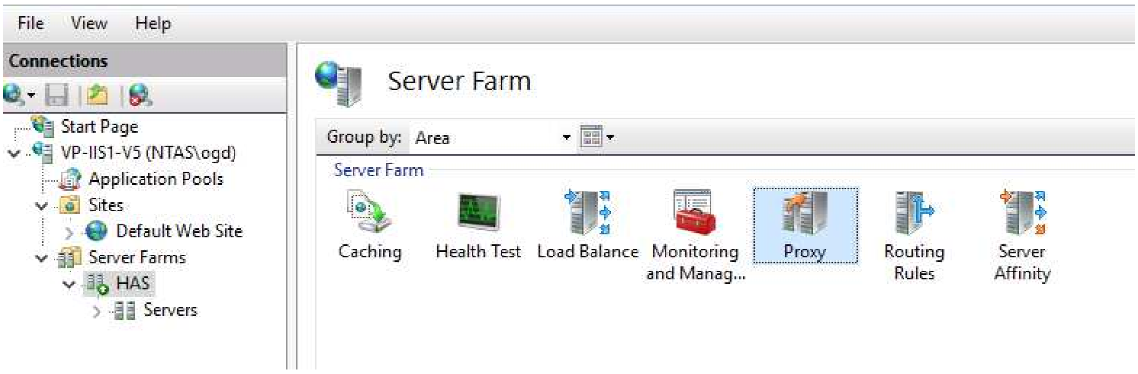


2.6.3. Configuring the proxy timeout

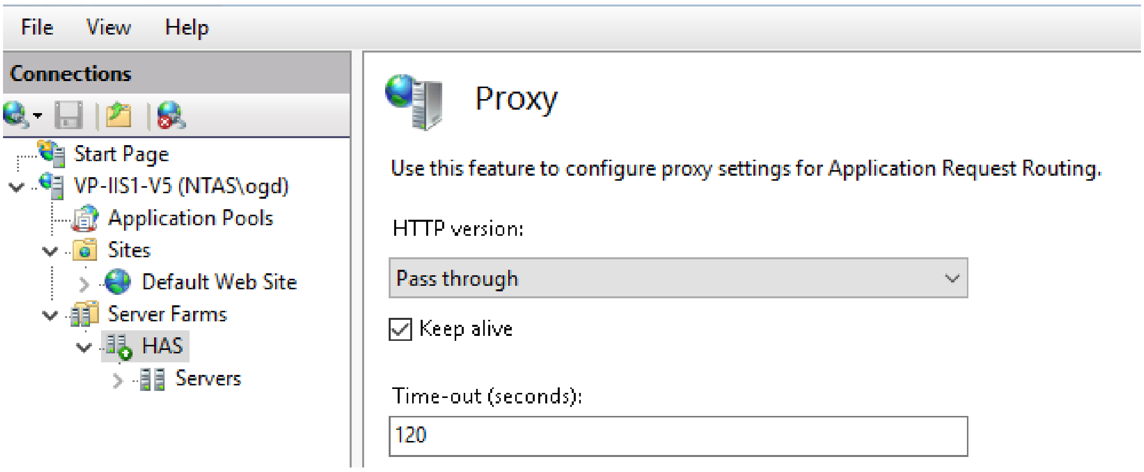
To configure the timeout:

1. Select the Server Farms you have just created.

2. Double-click **Proxy**.



3. In the **Time-out** field, enter **120**, then **Apply**. 120s is the max do not put above.



Proxy

Use this feature to configure proxy settings for Application Request Routing.

HTTP version: Pass through

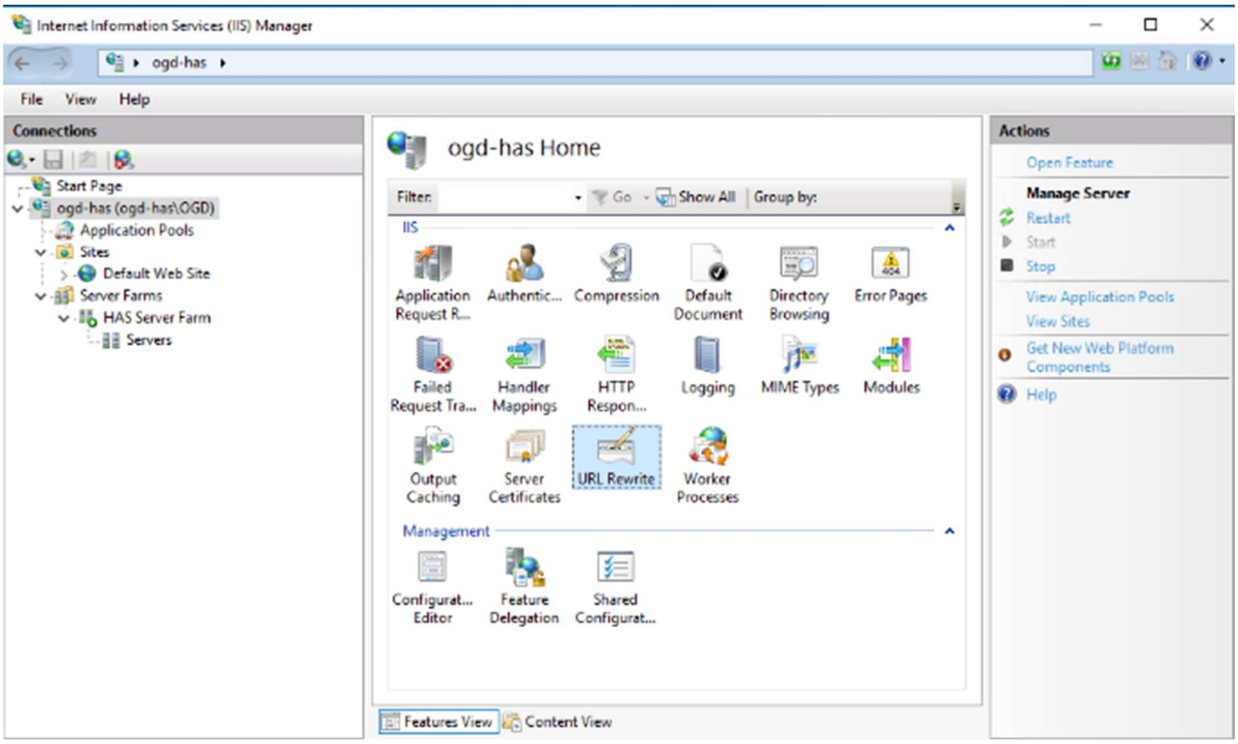
☑ Keep alive

Time-out (seconds): 120

2.6.4. Configuring the URL Rewrite rule

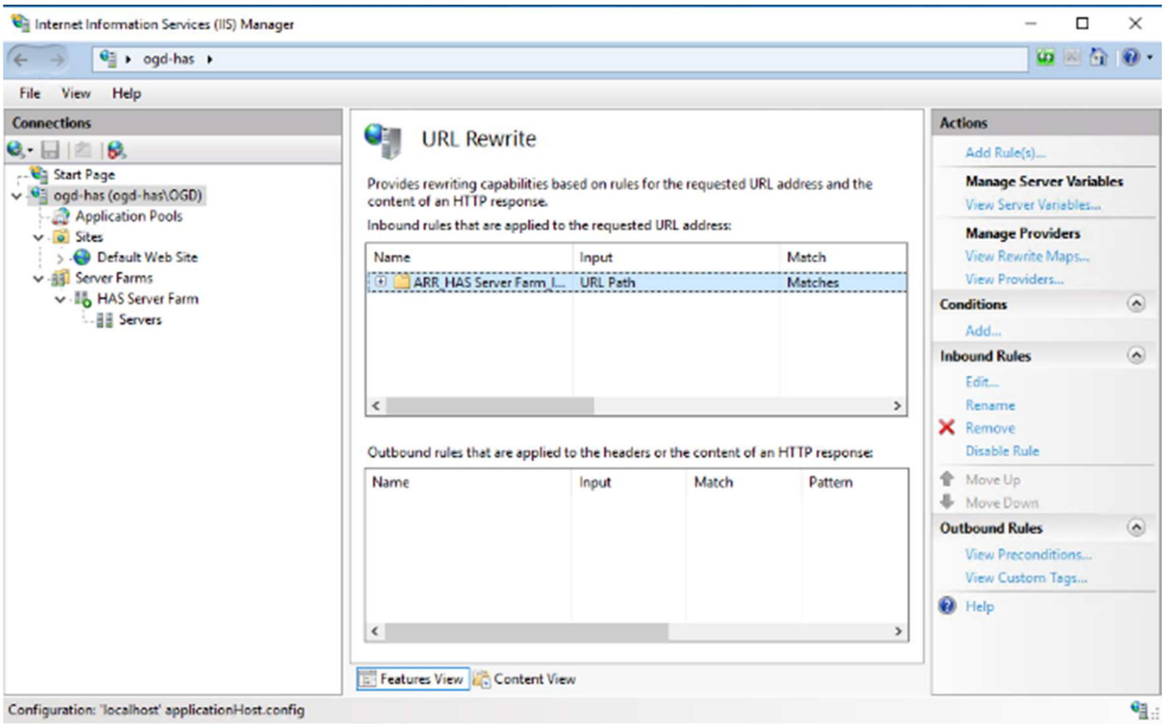
You need to adjust the URL Rewrite rule that was created:

1. Click the IIS root level.



2. Double-click **URL Rewrite**.

The rewrite rule created is named “ARR_ server farm name”.



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match
ARR_HAS Server Farm_l...	URL Path	Matches

Outbound rules that are applied to the headers or the content of an HTTP response:

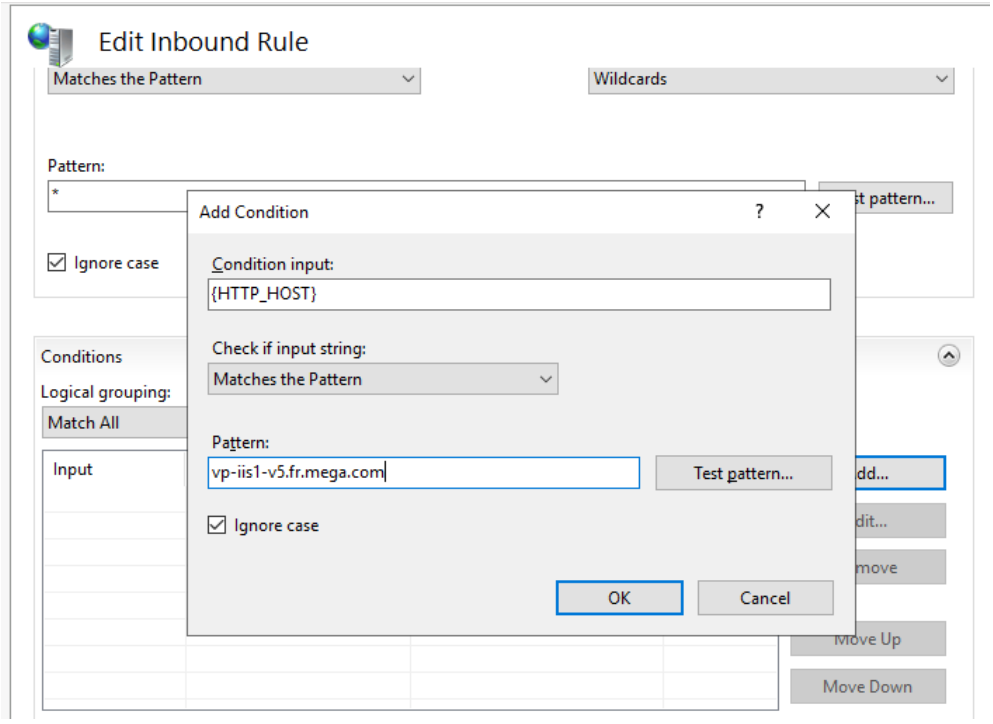
Name	Input	Match	Pattern

Configuration: 'localhost' applicationHost.config

3. Select the rule and double-click it (or click Edit).

4. Expand **Conditions** section to add one:

   - Click **Add**.
   - In the **Condition input** field, enter {HTTP_HOST}
   - Select “Matches the Pattern”
   - In the **Pattern** field, enter the DNS of your URL. Example « vp-iis1-V5.fr.mega.com »



Matches the Pattern

Pattern: *

☑ Ignore case

Logical grouping: Match All

Add Condition

Condition input: {HTTP_HOST}

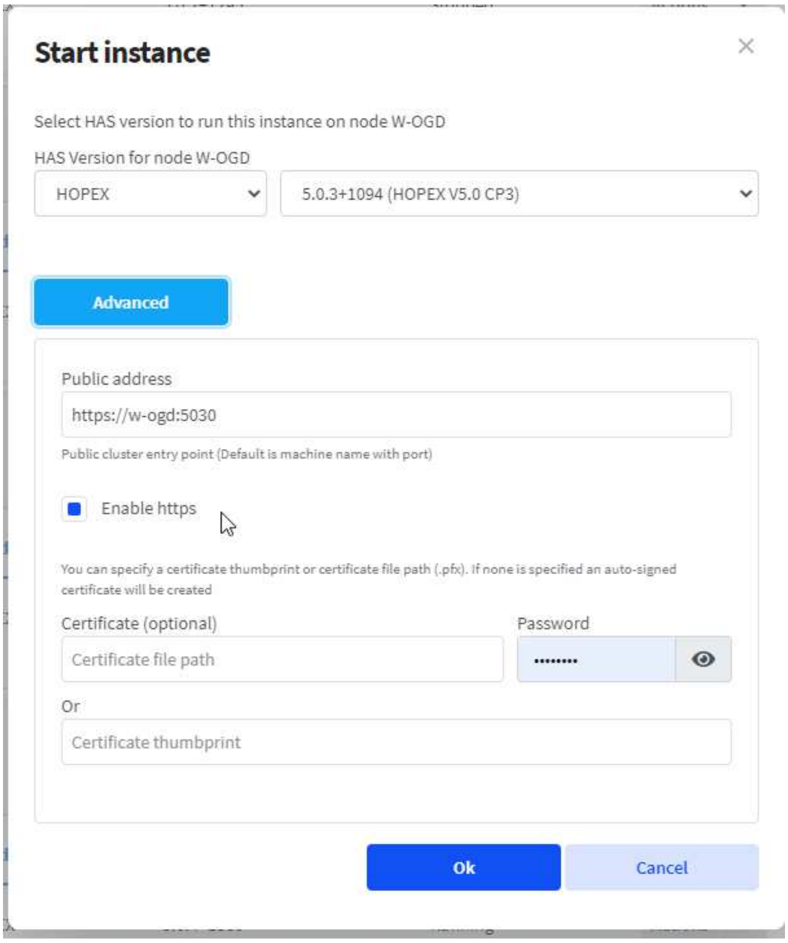
Check if input string: Matches the Pattern

Pattern: vp-iis1-v5.fr.mega.com

☑ Ignore case

5. Scroll down to the **Scheme** drop-down menu:

You will be able to decide this on the Instance Manager in the following chapter. If you have selected “**Enable https**” between cluster then select HTTPS else select HTTP.



Start instance

Select HAS version to run this instance on node W-OGD

HAS Version for node W-OGD

HOPEX | 5.0.3+1094 (HOPEX V5.0 CP3)

Advanced

Public address

https://w-ogd:5030

Public cluster entry point (Default is machine name with port)

☑ Enable https

You can specify a certificate thumbprint or certificate file path (.pfx). If none is specified an auto-signed certificate will be created

Certificate (optional): Certificate file path

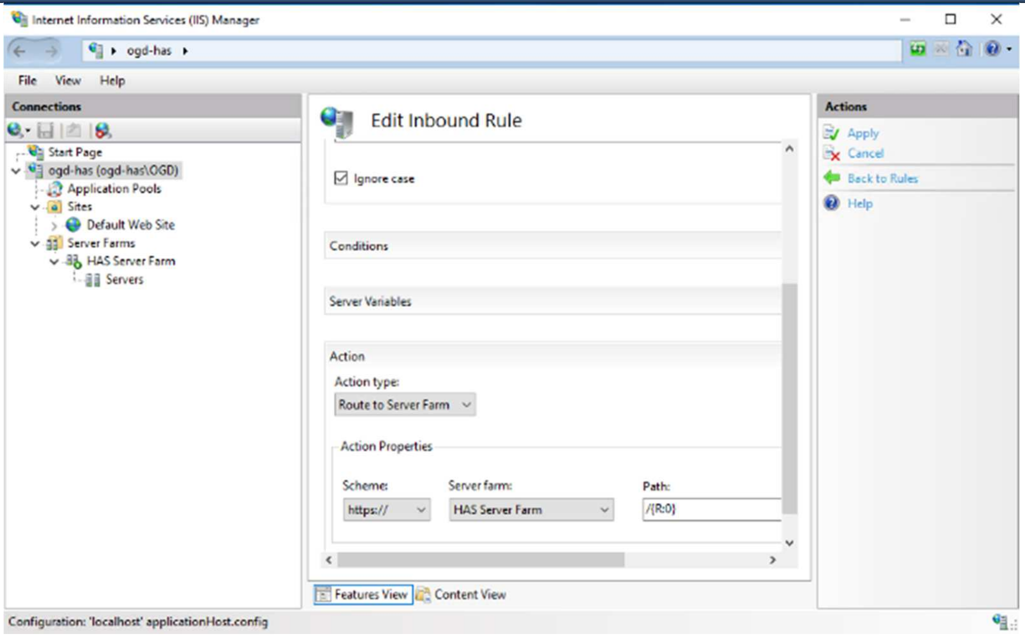
Password: ••••••••

Or

Certificate thumbprint

- Select **HTTPS (443)** if you are securing the URL
- Select **HTTP (80)** if you are not securing the URL

HTTPS (preferred choice)



Edit Inbound Rule

☑ Ignore case

Conditions

Server Variables

Action

Action type: Route to Server Farm

Action Properties

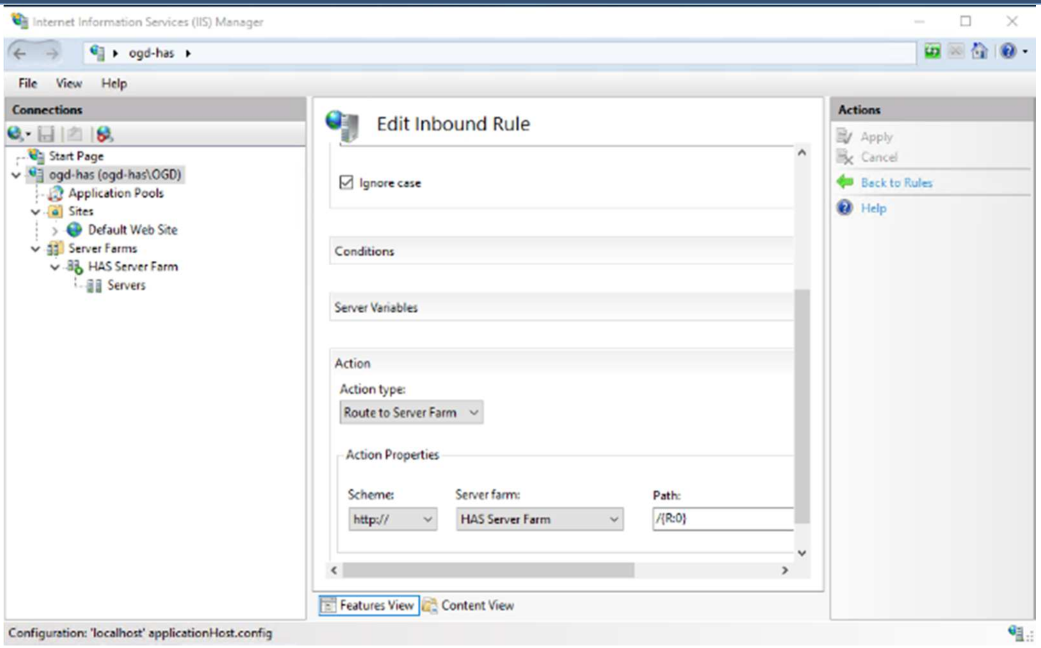
Scheme: https://

Server farm: HAS Server Farm

Path: /{R:0}

Configuration: 'localhost' applicationHost.config

HTTP



Internet Information Services (IIS) Manager

ogd-has

Edit Inbound Rule

☑ Ignore case

Conditions

Server Variables

Action

Action type: Route to Server Farm

Action Properties

Scheme: http://

Server farm: HAS Server Farm

Path: /{R:0}

Configuration: 'localhost' applicationHost.config

6. Click **Apply**.

CAUTION: There are 2 areas where you defined HTTP and HTTPS. This option is the communication between IIS and HAS

2.7. Request Filtering

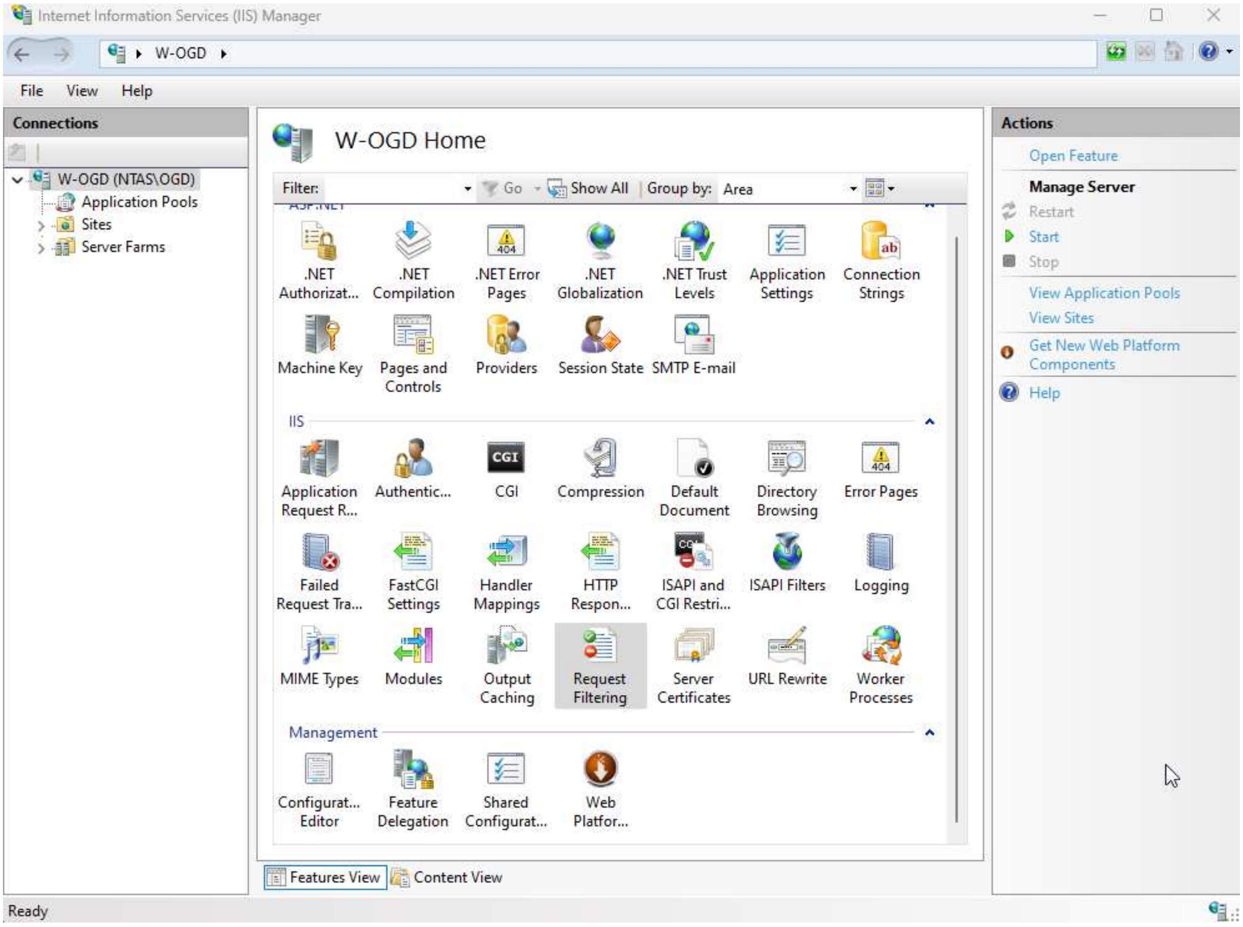
You need to adjust the Request filtering rules in IIS. Make sure that:

- there is no URL request filtering.
- there is no HTTP Verbs request filtering.
- there is no header request filtering.
- there is no query string request filtering.

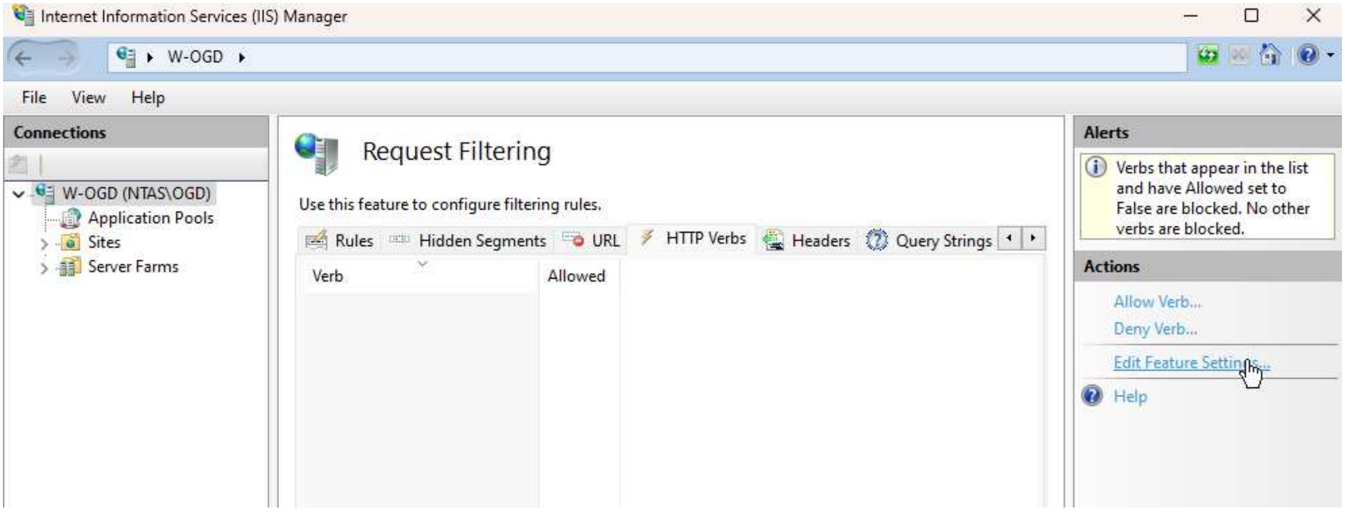
Having value in any of this tab of IIS may interfere with Hopex and prevent it from working properly. All security aspect of this request filtering are already managed by HAS.

You must Edit feature settings:

1. On root level select **Request Filtering**.



2. In the **Actions** pane, click **Edit Feature Settings**.

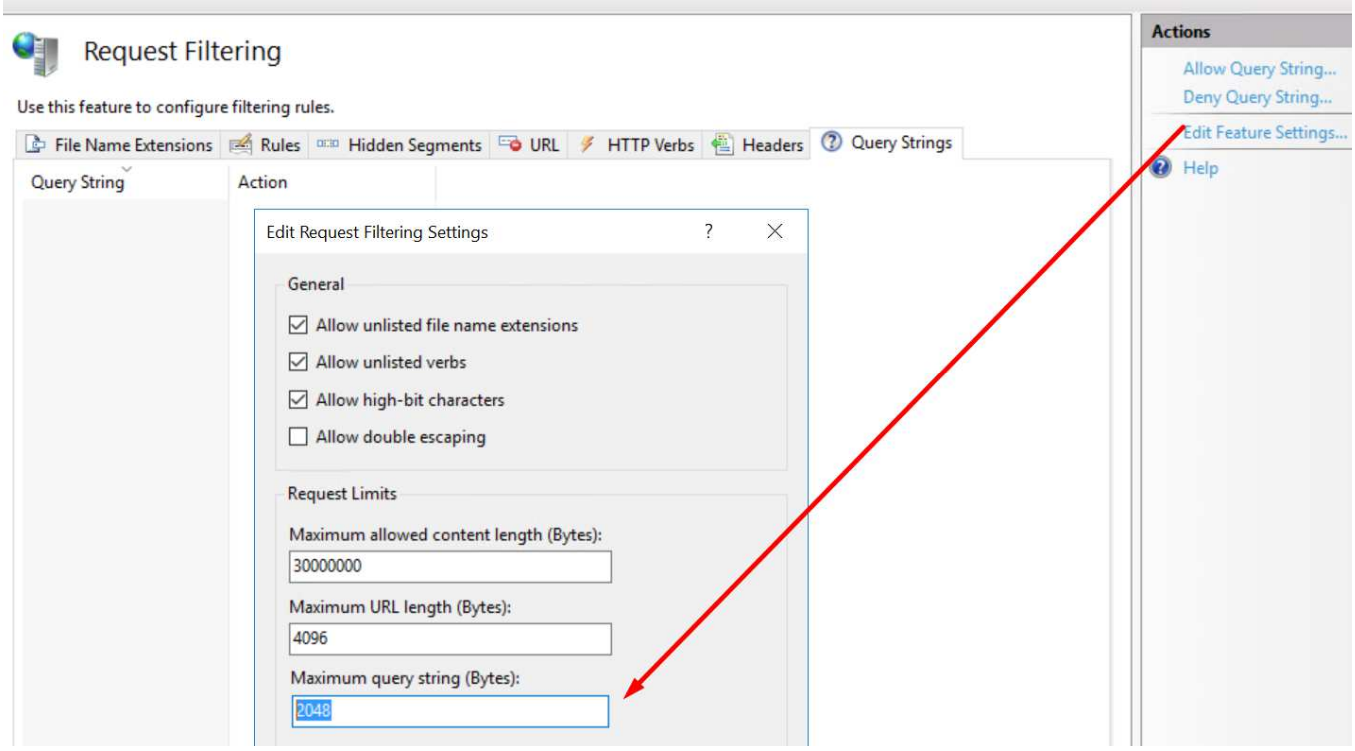


Use this feature to configure filtering rules.

Verbs that appear in the list and have Allowed set to False are blocked. No other verbs are blocked.

3. Increase default value 2048.

- Maximum query string (Bytes): **9012**



Request Filtering

Use this feature to configure filtering rules.

Edit Request Filtering Settings

General

☑ Allow unlisted file name extensions

☑ Allow unlisted verbs

☑ Allow high-bit characters

□ Allow double escaping

Request Limits

Maximum allowed content length (Bytes): 30000000

Maximum URL length (Bytes): 4096

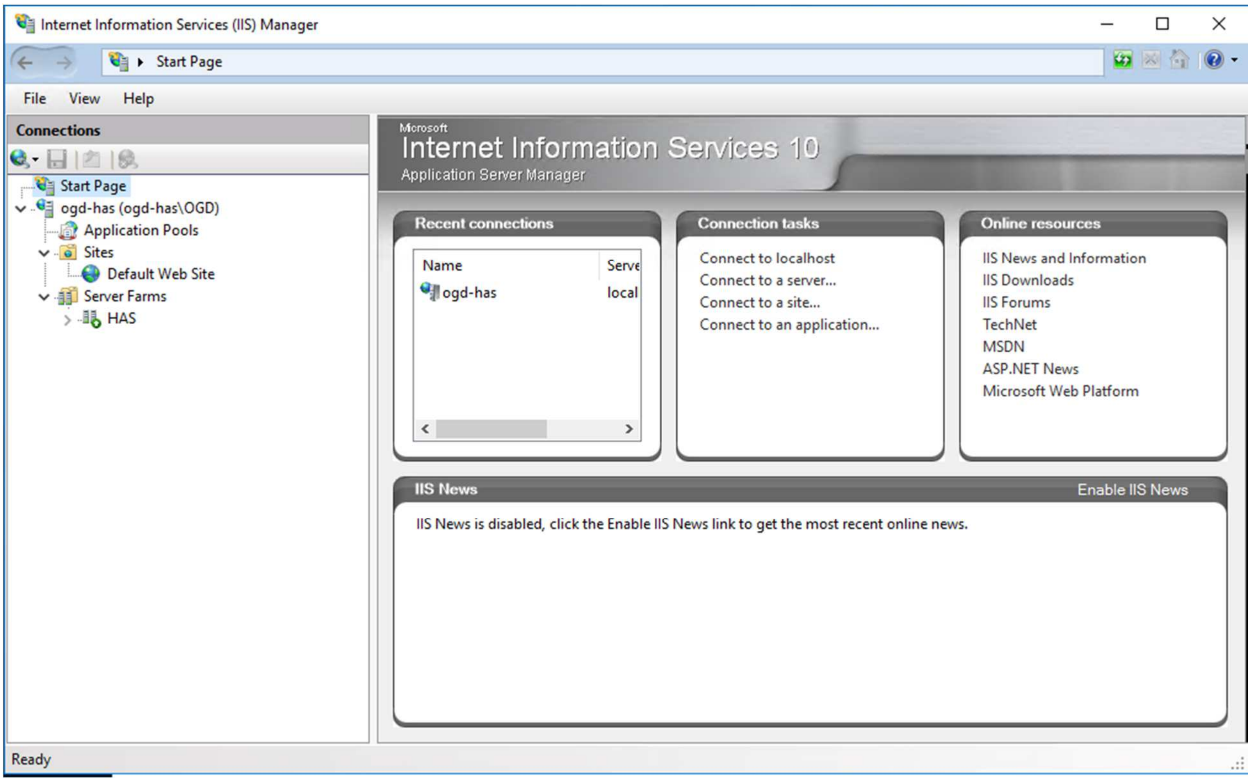
Maximum query string (Bytes): 2048

2.8. Configuring Logs files details and location

The following steps are “**optional**”. They are here to ease:

- diagnosis with complementary logs
- move location of all IIS logs

Launch the IIS Management Console

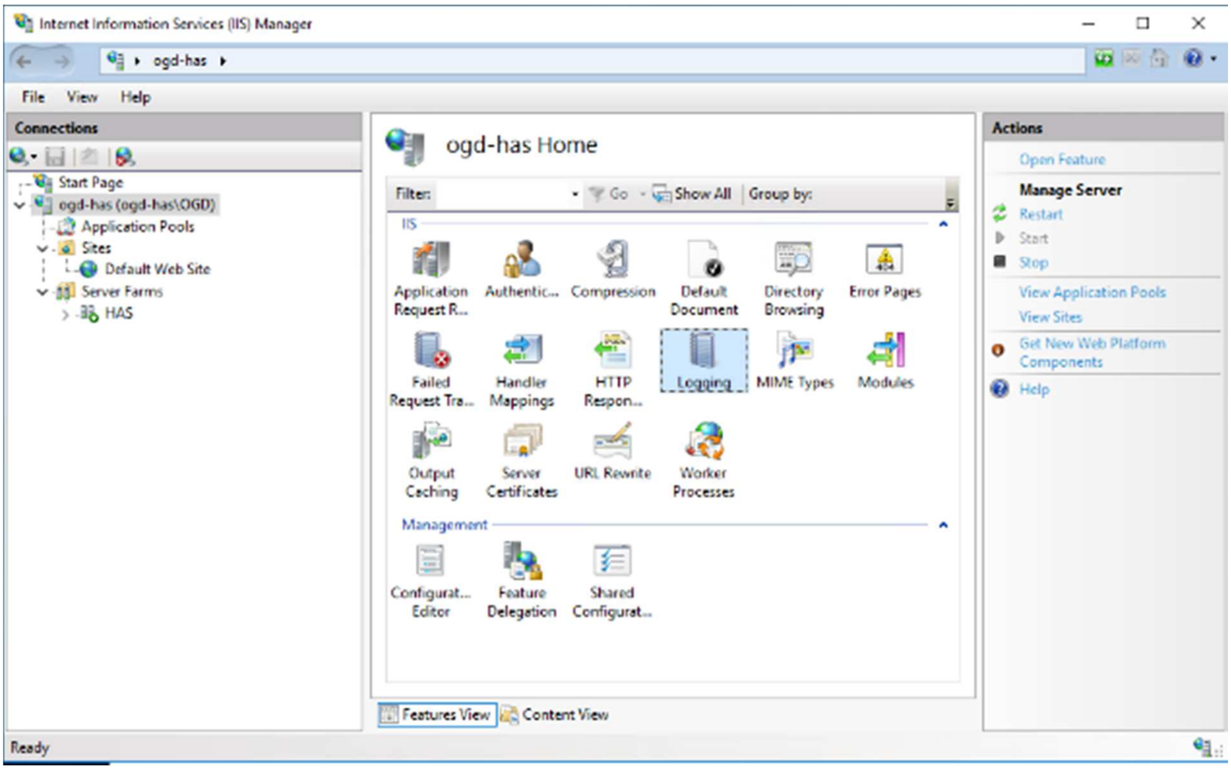


IIS News is disabled, click the Enable IIS News link to get the most recent online news.

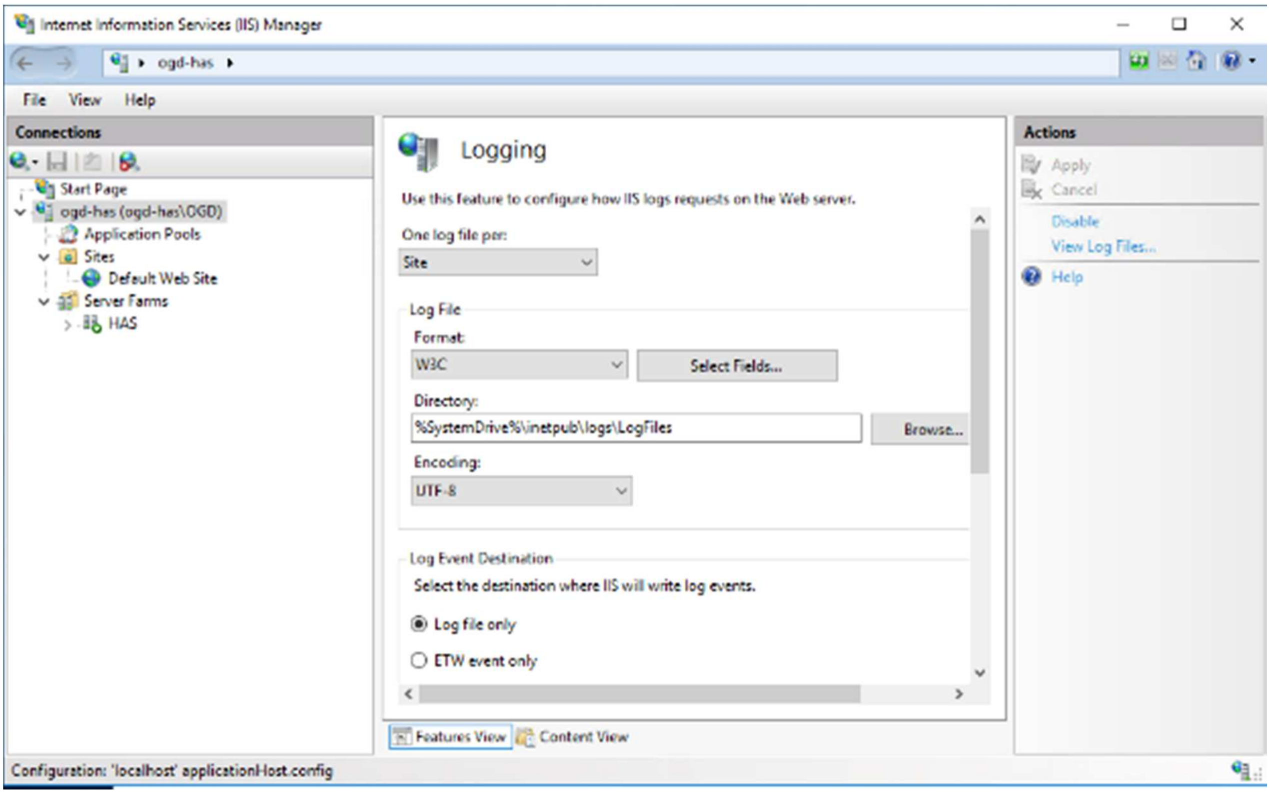
2.8.1. Locating IIS Logs

To locate IIS logs:

1. Select the Root level of the IIS Server.



2. Double-click **Logging**.



Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only

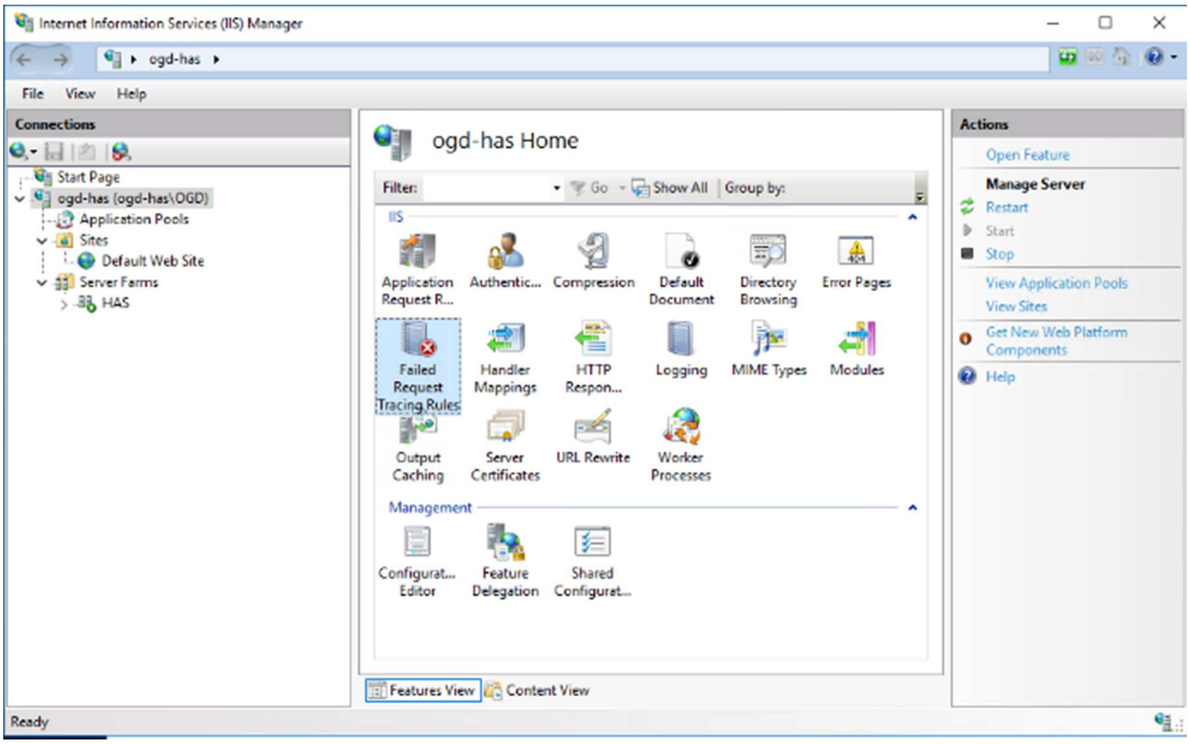
○ ETW event only

3. In the **Logging** pane, adjust **Directory location** of logs.

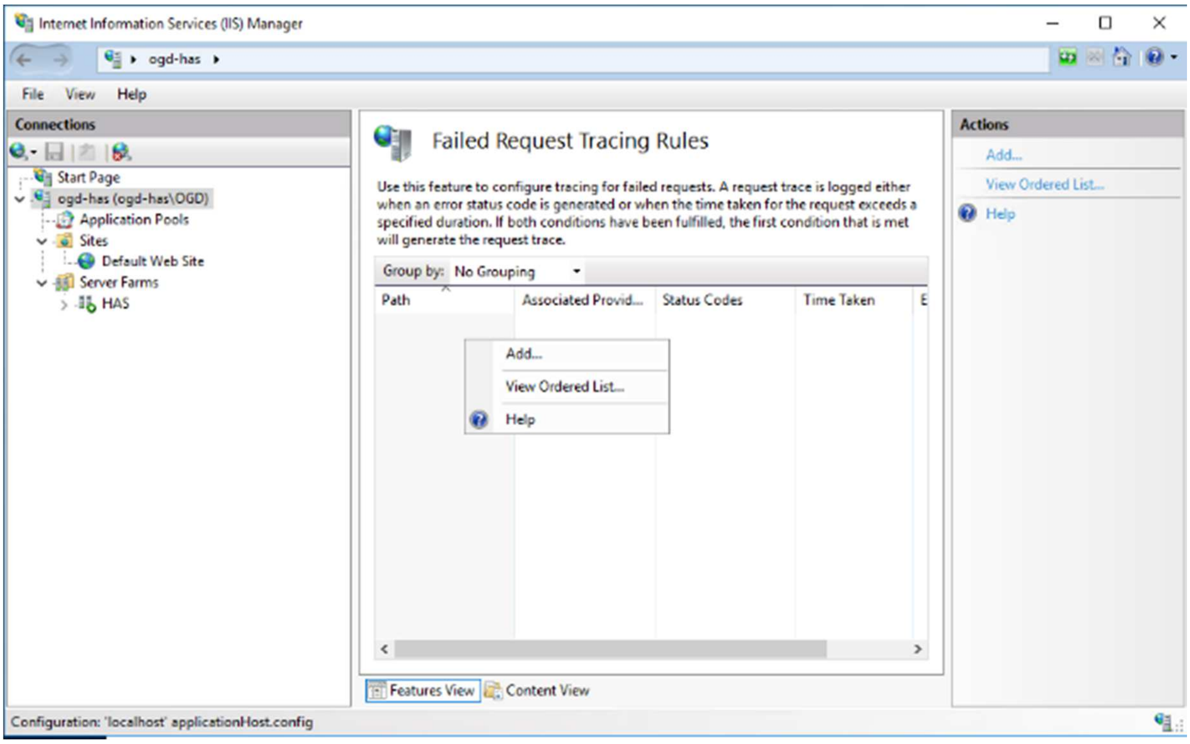
2.8.2. Enabling detailed logs for HTTP status code 502

To enable detailed logs for HTTP status code 502:

1. Go to Root level.

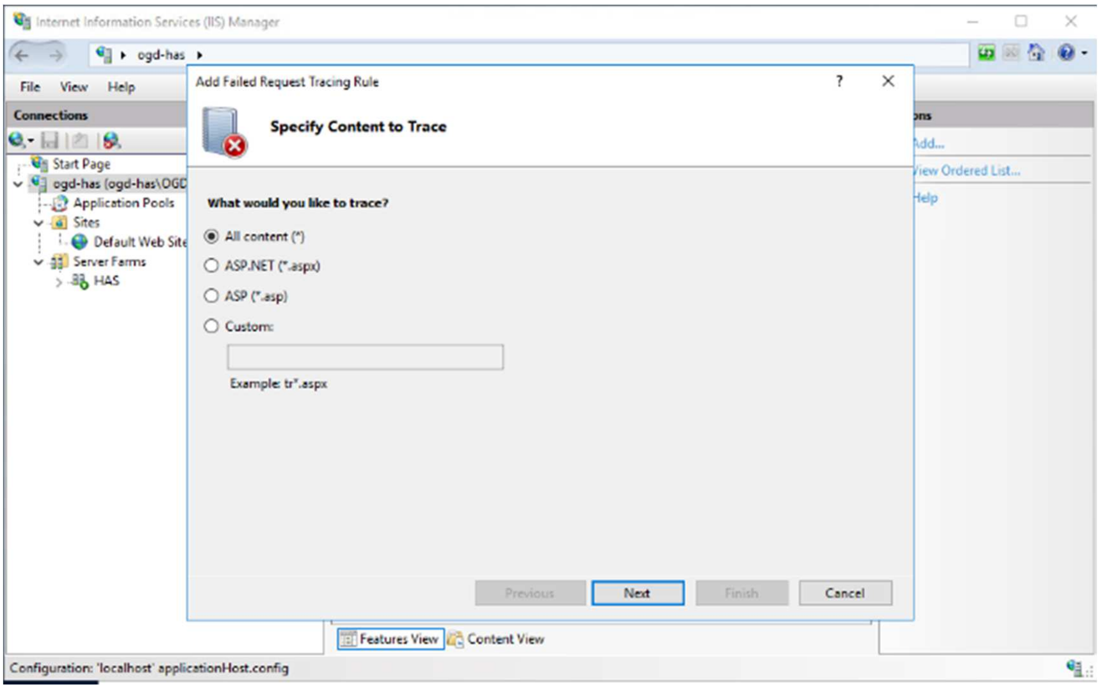


2. Double-click **Failed Request Tracing Rules**.



Use this feature to configure tracing for failed requests. A request trace is logged either when an error status code is generated or when the time taken for the request exceeds a specified duration. If both conditions have been fulfilled, the first condition that is met will generate the request trace.

3. Right-click the list and select **Add**.



Add Failed Request Tracing Rule

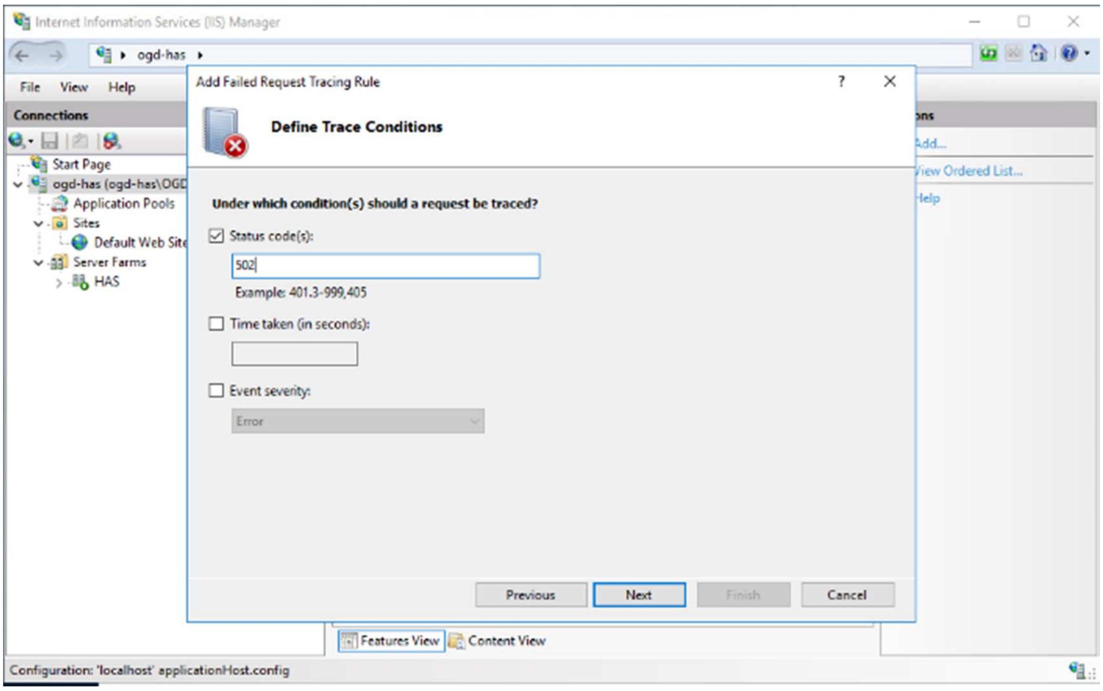
Specify Content to Trace

What would you like to trace?

● All content (*)
○ ASP.NET (*.aspx)
○ ASP (*.asp)
○ Custom:

Example: tr*.aspx

4. In the **Add Failed Request Tracing Rule**, select **All Content** and click **Next**.



Add Failed Request Tracing Rule

Define Trace Conditions

Under which condition(s) should a request be traced?

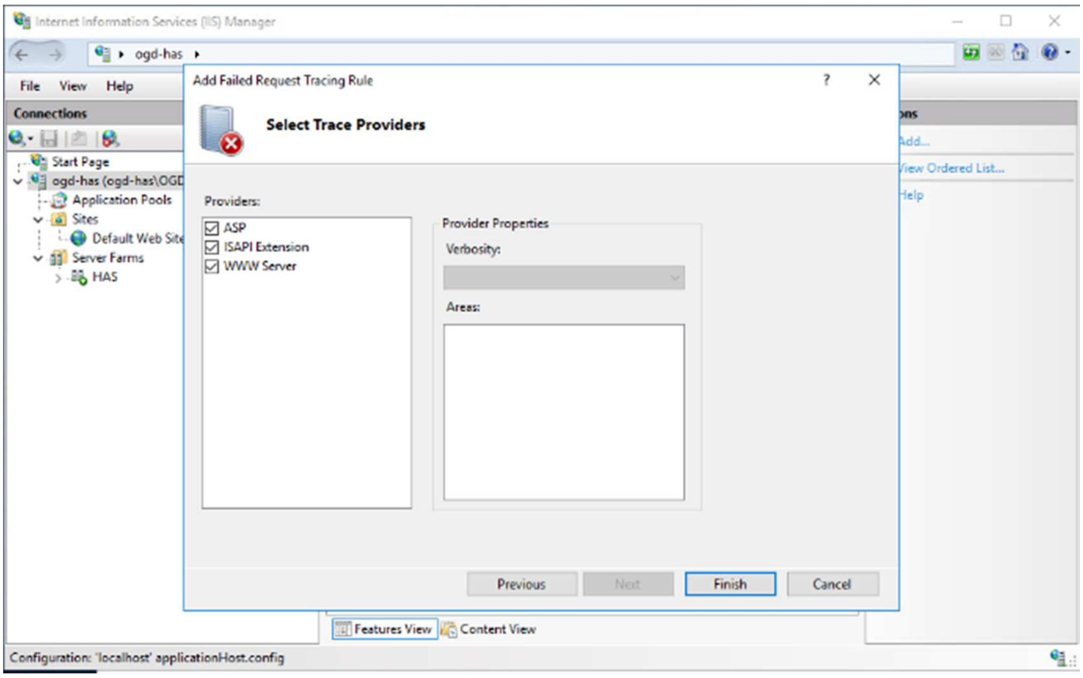
☑ Status code(s): 502

Example: 401.3-999,405

□ Time taken (in seconds):

□ Event severity: Error

5. Select **Status Code** and in the field enter “502” then click **Next**.



Add Failed Request Tracing Rule

Select Trace Providers

Providers:

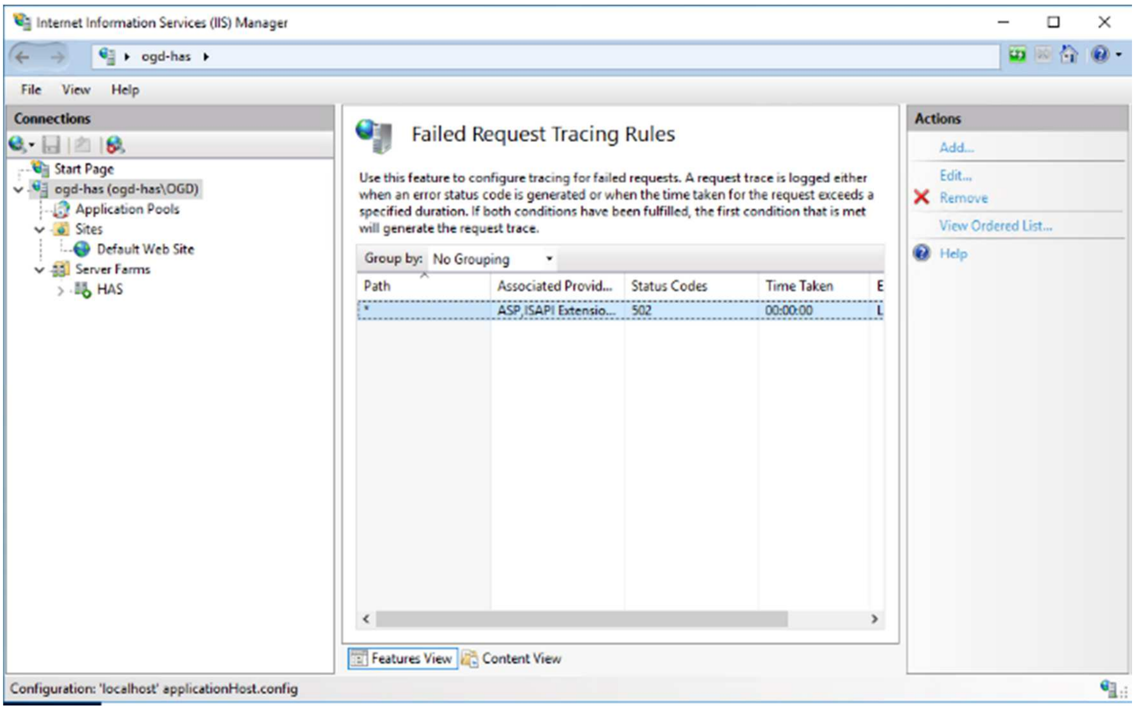
- ☑ ASP
- ☑ ISAPI Extension
- ☑ WWW Server

Provider Properties

Verbosity:

Areas:

6. Click **Finish**.



Failed Request Tracing Rules

Use this feature to configure tracing for failed requests. A request trace is logged either when an error status code is generated or when the time taken for the request exceeds a specified duration. If both conditions have been fulfilled, the first condition that is met will generate the request trace.

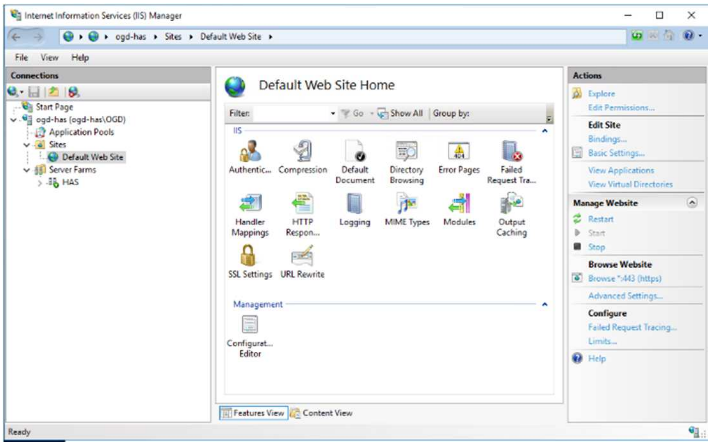
Group by: No Grouping

Path	Associated Provid...	Status Codes	Time Taken	E
*	ASP,ISAPI Extensio...	502	00:00:00	L

The rule for tracing HTTP 502 errors is now added. You must now enable the Tracing logs.

To enable the Tracing logs:

1. Go to **Default Web Site**.



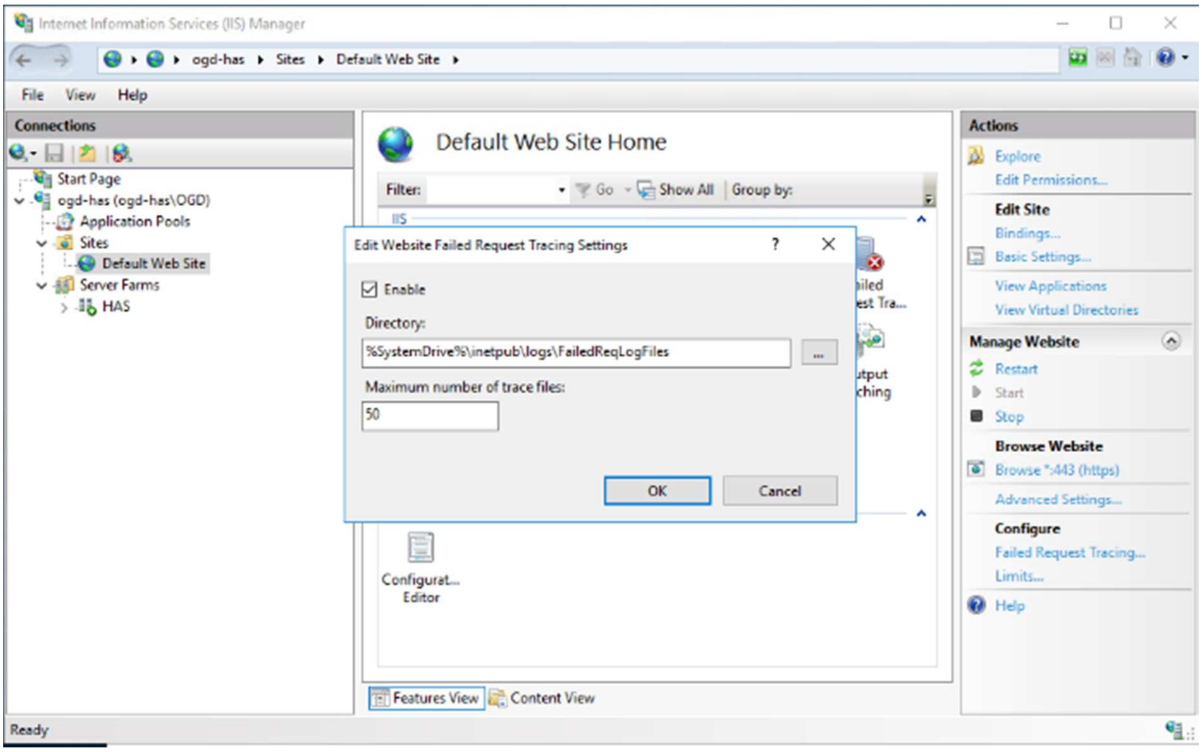
2. In the **Actions** pane, **Manage Website** > **Configure** section, click **Failed Request Tracing**.

3. In the **Edit Website Failed Request Tracing Settings** window, select **Enabled**.

4. (If needed) In the **Directory** field, modify folder location. Default: %SystemDrive%\inetpub\logs\FailedReqLogFiles.

5. Adjust **Maximum number of trace files**. Default 50.

6. Click **OK**.


Edit Website Failed Request Tracing Settings

☑ Enable

Directory: %SystemDrive%\inetpub\logs\FailedReqLogFiles

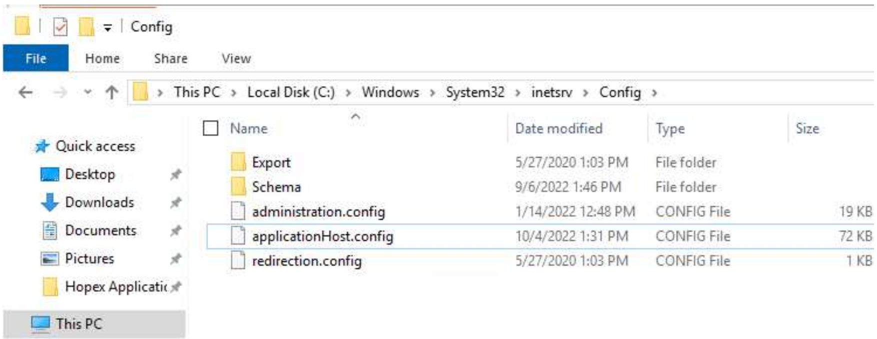
Maximum number of trace files: 50

2.8.3. Checking configuration (optional)

The server farm and healthcheck configuration you did are stored by IIS in an XML file in Microsoft. This file is called **applicationHost.config**.

You can find this file here: %windir%\system32\inetsrv\config

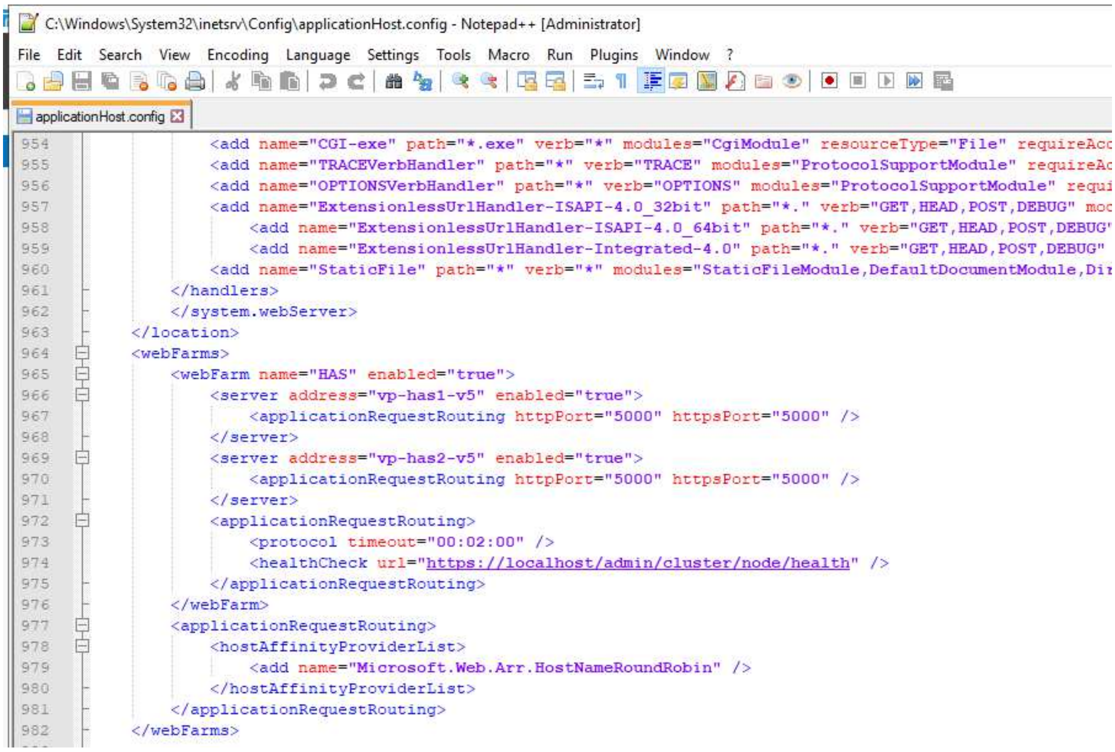
1. Access the applicationHost.config file.



Name	Date modified	Type	Size
Export	5/27/2020 1:03 PM	File folder	
Schema	9/6/2022 1:46 PM	File folder	
administration.config	1/14/2022 12:48 PM	CONFIG File	19 KB
applicationHost.config	10/4/2022 1:31 PM	CONFIG File	72 KB
redirection.config	5/27/2020 1:03 PM	CONFIG File	1 KB

2. Go at the end of the file or search for your server name and port.

3. You can check here the port you have selected and healthcheck url.



```
                <add name="CGI-exe" path="*.exe" verb="*" modules="CgiModule" resourceType="File" requireAcc
                <add name="TRACEVerbHandler" path="*" verb="TRACE" modules="ProtocolSupportModule" requireAc
                <add name="OPTIONSVerbHandler" path="*" verb="OPTIONS" modules="ProtocolSupportModule" requi
                <add name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" path="*." verb="GET,HEAD,POST,DEBUG" moc
                    <add name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" path="*." verb="GET,HEAD,POST,DEBUG"
                    <add name="ExtensionlessUrlHandler-Integrated-4.0" path="*." verb="GET,HEAD,POST,DEBUG"
                <add name="StaticFile" path="*" verb="*" modules="StaticFileModule,DefaultDocumentModule,Dir
            </handlers>
            </system.webServer>
        </location>
        <webFarms>
            <webFarm name="HAS" enabled="true">
                <server address="vp-has1-v5" enabled="true">
                    <applicationRequestRouting httpPort="5000" httpsPort="5000" />
                </server>
                <server address="vp-has2-v5" enabled="true">
                    <applicationRequestRouting httpPort="5000" httpsPort="5000" />
                </server>
                <applicationRequestRouting>
                    <protocol timeout="00:02:00" />
                    <healthCheck url="https://localhost/admin/cluster/node/health" />
                </applicationRequestRouting>
            </webFarm>
            <applicationRequestRouting>
                <hostAffinityProviderList>
                    <add name="Microsoft.Web.Arr.HostNameRoundRobin" />
                </hostAffinityProviderList>
            </applicationRequestRouting>
        </webFarms>
```

For more details read the Microsoft official documentation:

https://learn.microsoft.com/en-us/iis/get-started/planning-your-iis-architecture/introduction-to-applicationhostconfig

3. HOPEX Application Server (HAS) installation

The following installation instructions are to be applied for the First server of the farm that will behave as an "**HAS Server**".

Should you have several "HAS Server" you need to add each additional HAS Server to the cluster. Please read the cluster section.

3.1. Installing the prerequisite software

Download and install this prerequisite software technologies:

A supported web browser: Chrome, Firefox, Edge

.NET 8 Hosting Bundle x64 (latest version as more secure):
https://dotnet.microsoft.com/download/dotnet/8.0

.NET 8 SDK x64 (for Development server only)

.NET Framework 4.8:
https://dotnet.microsoft.com/download/dotnet-framework

Visual C++ Redistributable 2015 – 2022 64 bits

- vc_redist.x64.exe

https://aka.ms/vs/17/release/vc_redist.x64.exe

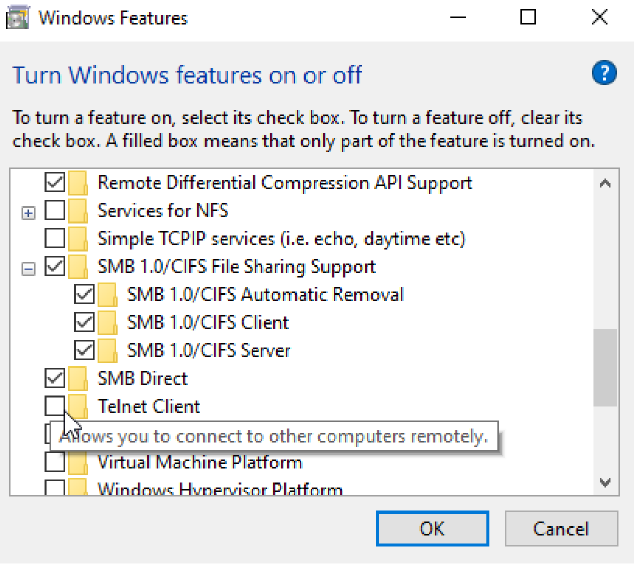
ODBC Driver 17 or 18 for SQL Server X64 too if the SQL Server database is not on the same physical Windows than HAS Server.
https://docs.microsoft.com/fr-fr/sql/connect/odbc/download-odbc-driver-for-sql-server?view=sql-server-ver16

CAUTION: ²ODBC Driver 18 is supported from V5 CP4 onward.

3.2. Configuring the file server

1. In Windows Operating System turn on File Server and SMB:

With Windows 10: from **Control Panel**: "Turn Windows features on or off"



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

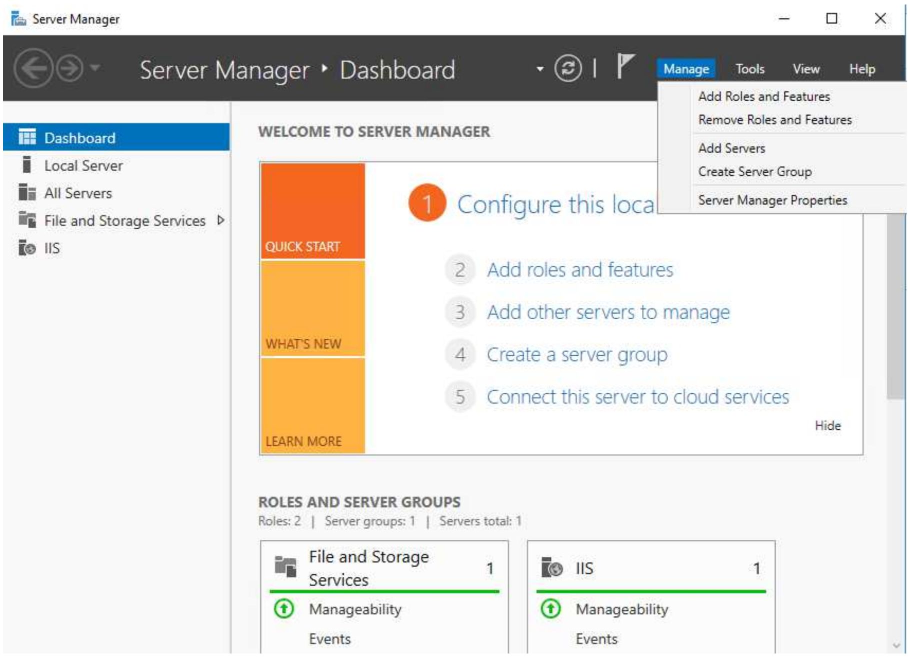
- ☑ Remote Differential Compression API Support
- ☐ Services for NFS
- ☐ Simple TCPIP services (i.e. echo, daytime etc)
- ☑ SMB 1.0/CIFS File Sharing Support
  - ☑ SMB 1.0/CIFS Automatic Removal
  - ☑ SMB 1.0/CIFS Client
  - ☑ SMB 1.0/CIFS Server
- ☑ SMB Direct
- ☐ Telnet Client
- ☐ Virtual Machine Platform
- ☐ Windows Hypervisor Platform

Allows you to connect to other computers remotely.

Or

With Windows Server: from **Server Manager**: Add Roles and features (https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager#start-server-manager)

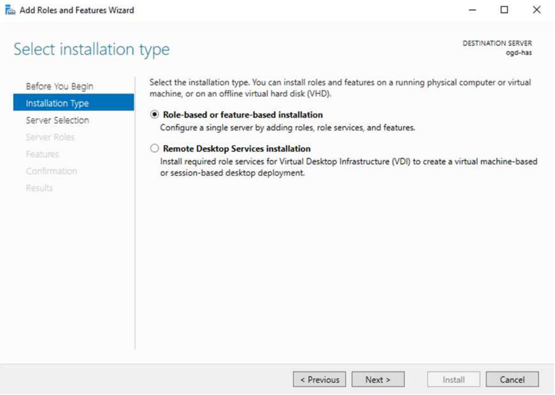
2. Click **Manage** and select **Add Roles and features**.



3. In the pop-up Wizard, click **Next**.
   The **Server Roles** page is displayed.

4. Select: **File Server**.

5. If prompted click **Add Features**.



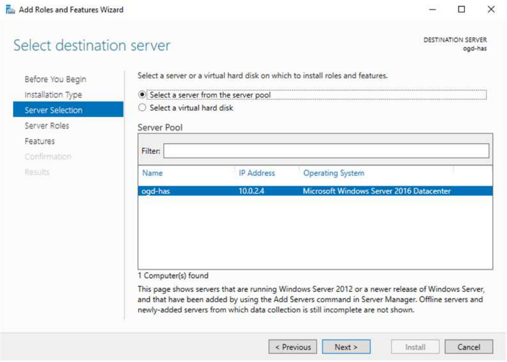
Select installation type

DESTINATION SERVER
ogd-has

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



Select destination server

DESTINATION SERVER
ogd-has

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

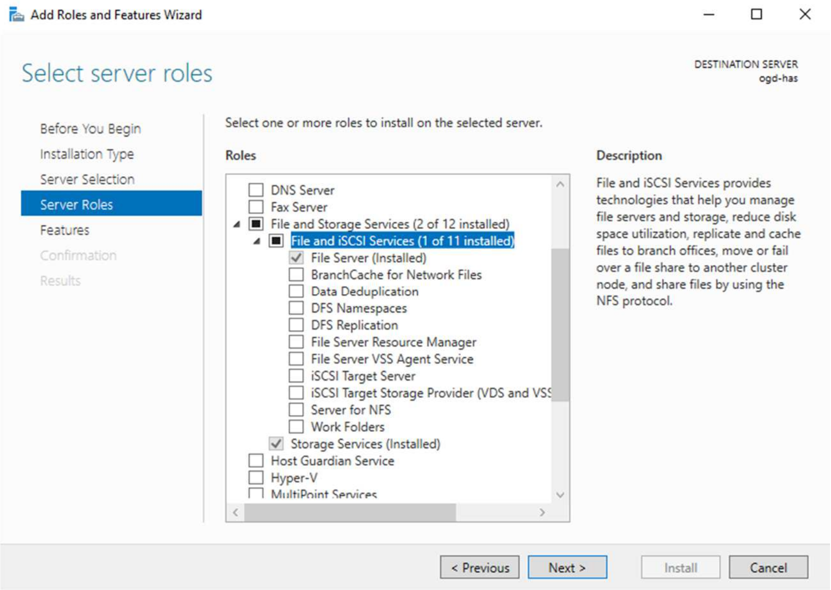
Server Pool

Filter:

Name	IP Address	Operating System
ogd-has	10.0.2.4	Microsoft Windows Server 2016 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.



Select server roles

DESTINATION SERVER
ogd-has

Select one or more roles to install on the selected server.

Roles

- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
  - ■ File and iSCSI Services (1 of 11 installed)
    - ☑ File Server (Installed)
    - □ BranchCache for Network Files
    - □ Data Deduplication
    - □ DFS Namespaces
    - □ DFS Replication
    - □ File Server Resource Manager
    - □ File Server VSS Agent Service
    - □ iSCSI Target Server
    - □ iSCSI Target Storage Provider (VDS and VSS
    - □ Server for NFS
    - □ Work Folders
  - ☑ Storage Services (Installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services

Description

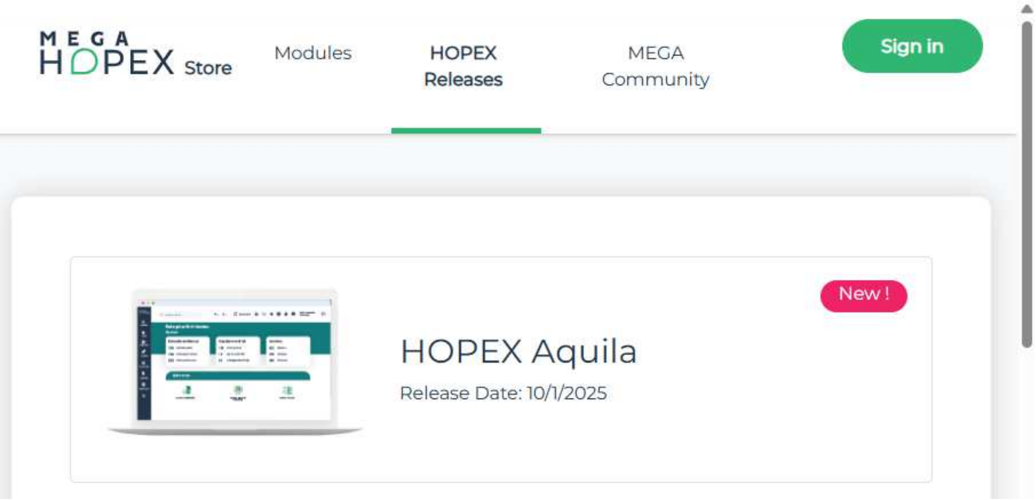
File and iSCSI Services provides technologies that help you manage file servers and storage, reduce disk space utilization, replicate and cache files to branch offices, move or fail over a file share to another cluster node, and share files by using the NFS protocol.

6. Click **Next** up to install.

3.3. Downloading HAS Server installer

To download the latest installer from a server/laptop that has access to internet:

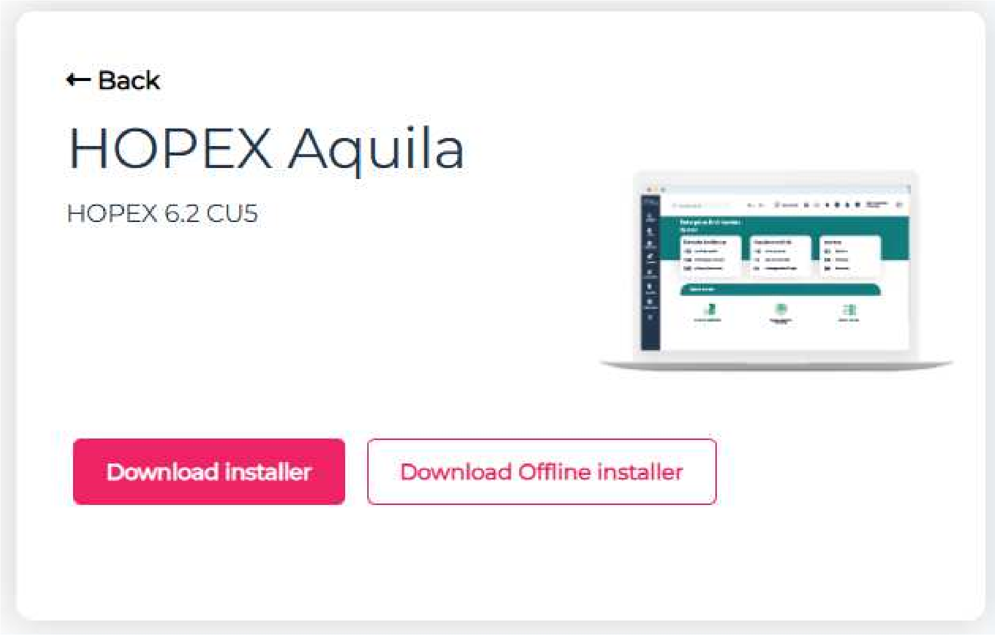
1. Go to https://store.mega.com/.



2. Click **Sign in**.
3. If you have **never connected** to any MEGA website (MEGA Community, MEGA HOPEX Store, MEGA e-learning platform).
   - Click “Don't have an account? **Sign up**”
   - Create an Account.
   - Set a new password.
   - Confirm your account by clicking the email received.

   If you **have already an account** on MEGA website:

   - Connect with your professional e-mail and password.
4. In the **HOPEX Releases** page, click **HOPEX Aquila**.



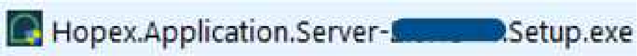
← Back

HOPEX Aquila

HOPEX 6.2 CU5

5. Click **Download installer.**

The Setup file is downloaded.



Hopex.Application.Server-[redacted]Setup.exe

3.4. Getting your installation key

To get your “personal” installation key:

1. Go to https://store.mega.com/.
2. Click **Sign in** and connect with your professional e-mail and password.
3. Click your **Avatar > My Profile** to get your own personal installation key.
4. Copy the **Installation Key**.

   If you fail in this process and encounter an “Access Denied”, contact your sales representative.

DO NOT SHARE this installation key. It is private for your organization.

3.5. Installing HAS Instance Manager with the setup

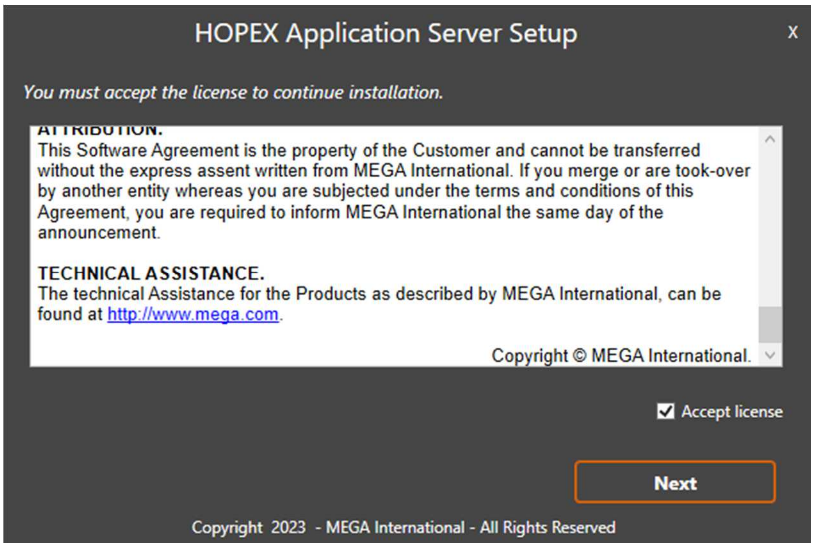
3.5.1. First steps "online"

Caution: you must perform these actions from a server that has online internet access to https://store.mega.com/ You can go offline later.

Step 1
Launch the installer: double-click the "**Hopex.Application.Server-**<Version number>**.Setup.exe"**

Step 2

- Select **Accept license**.
- Click **Next**



HOPEX Application Server Setup

You must accept the license to continue installation.

ATTRIBUTION.
This Software Agreement is the property of the Customer and cannot be transferred without the express assent written from MEGA International. If you merge or are took-over by another entity whereas you are subjected under the terms and conditions of this Agreement, you are required to inform MEGA International the same day of the announcement.

TECHNICAL ASSISTANCE.
The technical Assistance for the Products as described by MEGA International, can be found at http://www.mega.com.

Copyright © MEGA International.

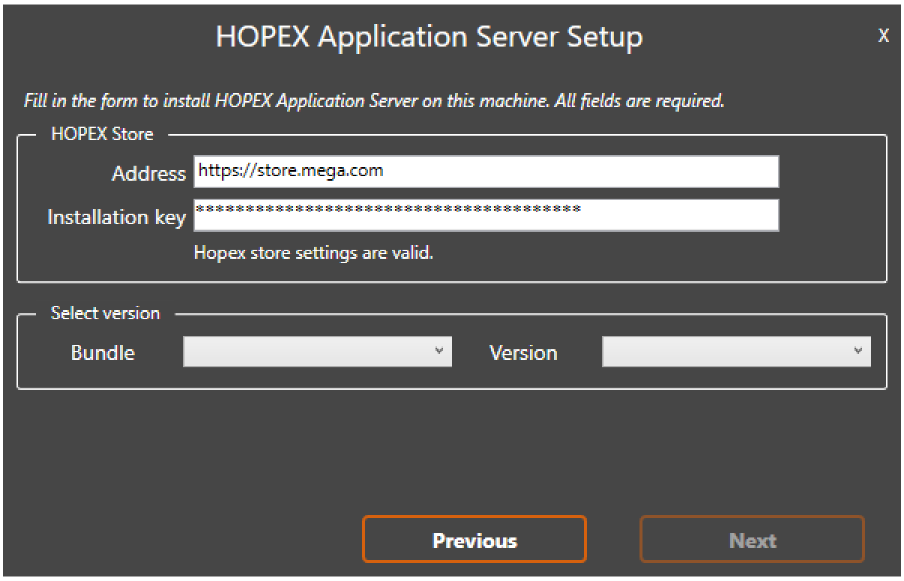
☑ Accept license

Copyright 2023 - MEGA International - All Rights Reserved

Step 3

- Enter your **Installation key** obtained from the MEGA HOPEX Store

  The message “**HOPEX Store settings are valid**” appears if the key is correct.



HOPEX Application Server Setup

Fill in the form to install HOPEX Application Server on this machine. All fields are required.

HOPEX Store

Address: https://store.mega.com

Installation key: **

Hopex store settings are valid.

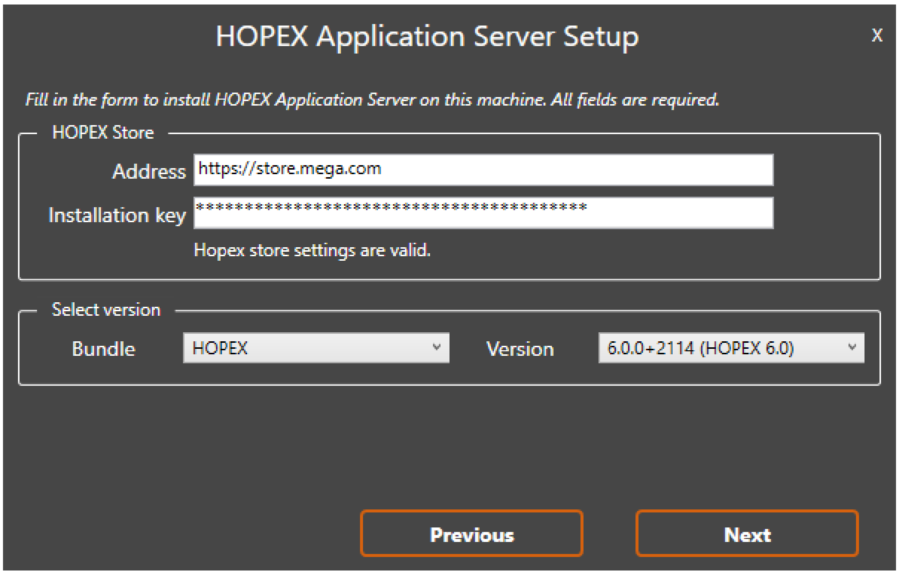
Select version

Bundle:

Version:

Step 4

- Select **Bundle** “HOPEX”
- Select required **Version**: 6.0
- Click **Next**



HOPEX Application Server Setup

Fill in the form to install HOPEX Application Server on this machine. All fields are required.

HOPEX Store

Address: https://store.mega.com

Installation key: ***

Hopex store settings are valid.

Select version

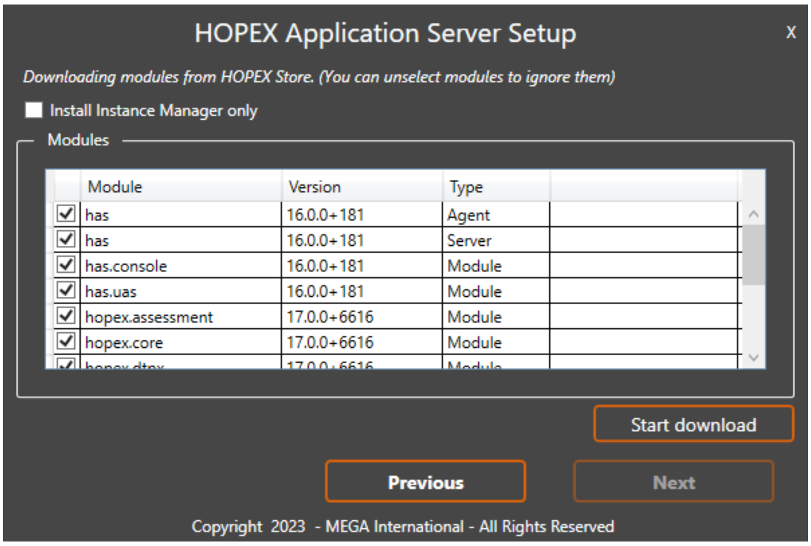
Bundle: HOPEX

Version: 6.0.0+2114 (HOPEX 6.0)

Step 5

- Select the module you want to download. By default, "All"
- Click **Start download**

  This **may take a while**. The total of all modules can go up to 2Gb.



HOPEX Application Server Setup

Downloading modules from HOPEX Store. (You can unselect modules to ignore them)

□ Install Instance Manager only

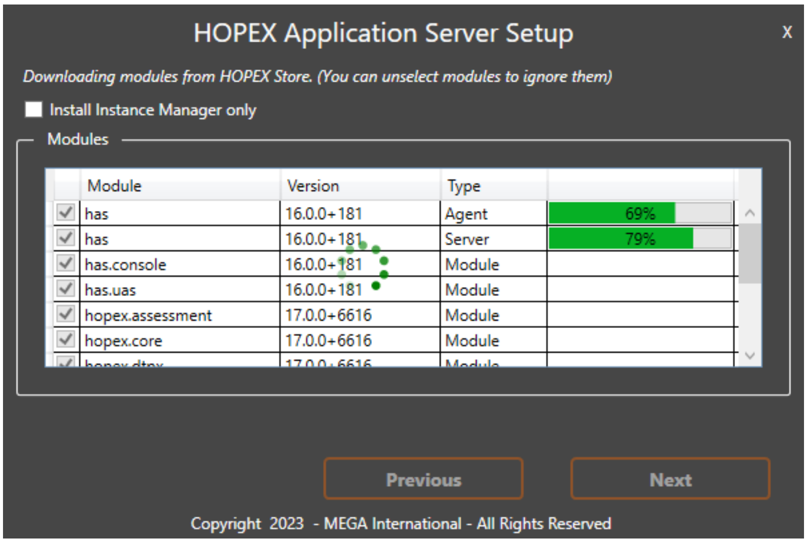
Modules

	Module	Version	Type	
☑	has	16.0.0+181	Agent	
☑	has	16.0.0+181	Server	
☑	has.console	16.0.0+181	Module	
☑	has.uas	16.0.0+181	Module	
☑	hopex.assessment	17.0.0+6616	Module	
☑	hopex.core	17.0.0+6616	Module	
☑	hopex.dtpx	17.0.0+6616	Module	

Copyright 2023 - MEGA International - All Rights Reserved

Step 6

When all downloads are successful click **Next**



HOPEX Application Server Setup

Downloading modules from HOPEX Store. (You can unselect modules to ignore them)

□ Install Instance Manager only

Modules

	Module	Version	Type	
☑	has	16.0.0+181	Agent	69%
☑	has	16.0.0+181	Server	79%
☑	has.console	16.0.0+181	Module	
☑	has.uas	16.0.0+181	Module	
☑	hopex.assessment	17.0.0+6616	Module	
☑	hopex.core	17.0.0+6616	Module	
☑	hopex.dtpx	17.0.0+6616	Module	

Copyright 2023 - MEGA International - All Rights Reserved

At this stage, nothing is installed on the server. Files are only downloaded to start deployment.

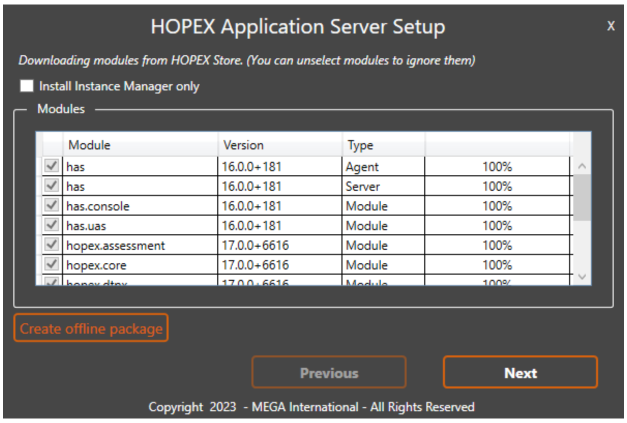
You can decide to:

- go offline (step 7 to 10) if the server you want to install does not have internet access or if you want to keep the package for later use.
- continue the setup (go directly to step 11).

3.5.2. Go “offline”

Step 7

- Click **Create offline package**
- Unfold the folder where you want to put the packages



HOPEX Application Server Setup

Downloading modules from HOPEX Store. (You can unselect modules to ignore them)

□ Install Instance Manager only

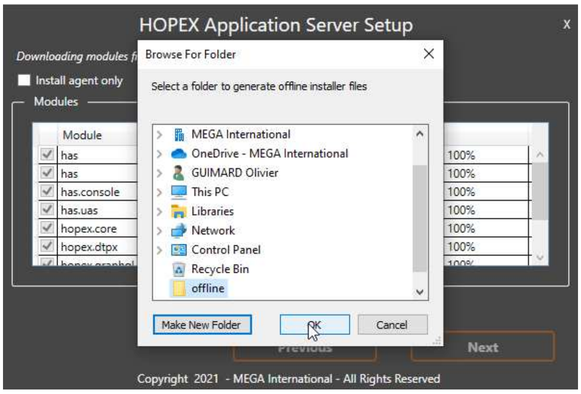
Modules

	Module	Version	Type	
☑	has	16.0.0+181	Agent	100%
☑	has	16.0.0+181	Server	100%
☑	has.console	16.0.0+181	Module	100%
☑	has.uas	16.0.0+181	Module	100%
☑	hopex.assessment	17.0.0+6616	Module	100%
☑	hopex.core	17.0.0+6616	Module	100%
☑	hopex.dtpx	17.0.0+6616	Module	100%

Copyright 2023 - MEGA International - All Rights Reserved

Step 8

- Prefer a C:\ location. You will be able to move the files later.
- Create a new folder or select an existing one for which you have the rights to write.



HOPEX Application Server Setup

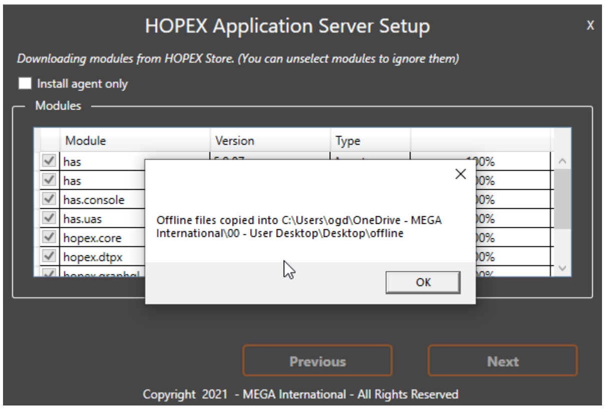
Browse For Folder

Select a folder to generate offline installer files

Copyright 2021 - MEGA International - All Rights Reserved

Step 9

- When successful a pop-up appears Offline files ready
- Click **OK**
- The setup is **closed**



HOPEX Application Server Setup

Downloading modules from HOPEX Store. (You can unselect modules to ignore them)

□ Install agent only

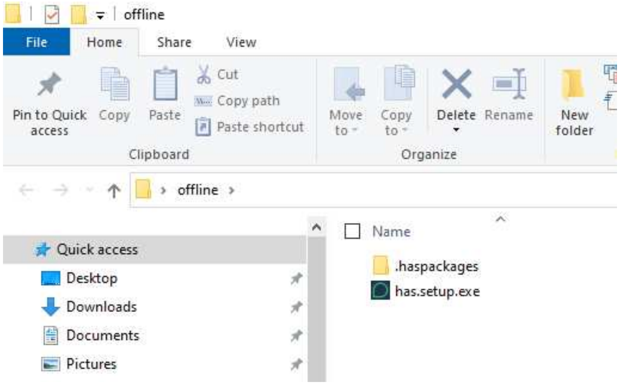
Offline files copied into C:\Users\ogd\OneDrive - MEGA International\00 - User Desktop\Desktop\offline

Copyright 2021 - MEGA International - All Rights Reserved

Step 10

- Search for the folder you have just created

It contains:
- an **has.setup.exe** file
- an **haspackages** folder with *.haspkg file

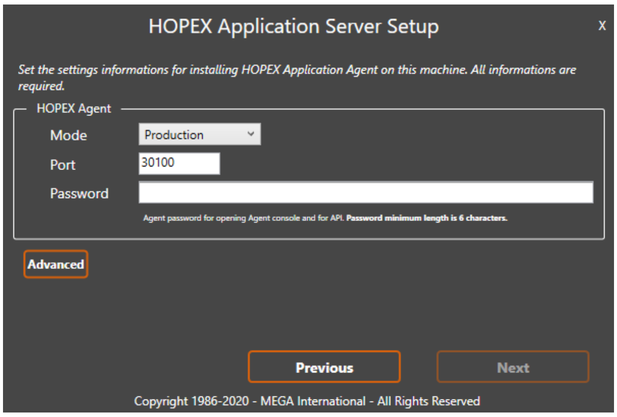
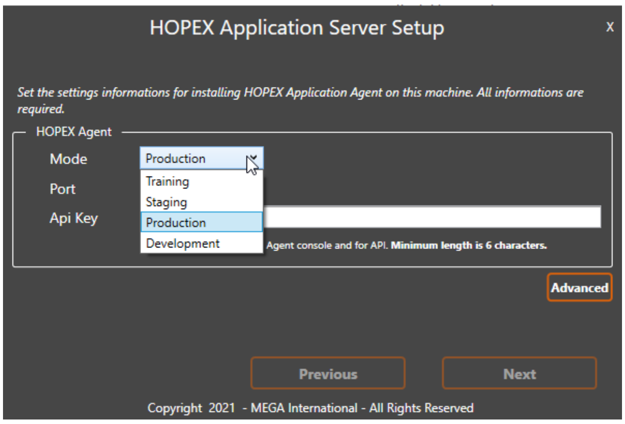


.haspackages
has.setup.exe

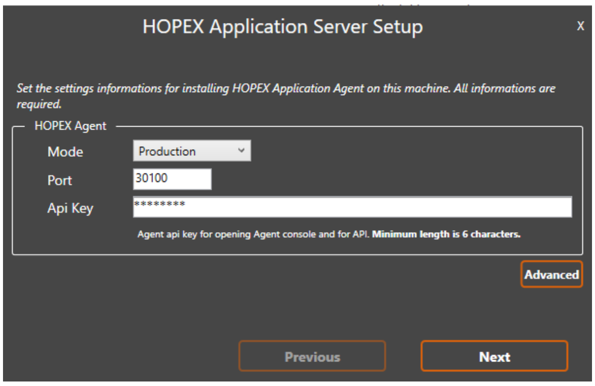
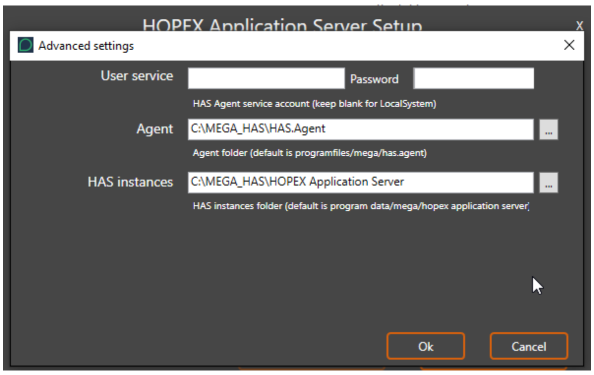
Caution: naming of folders and files should not be changed

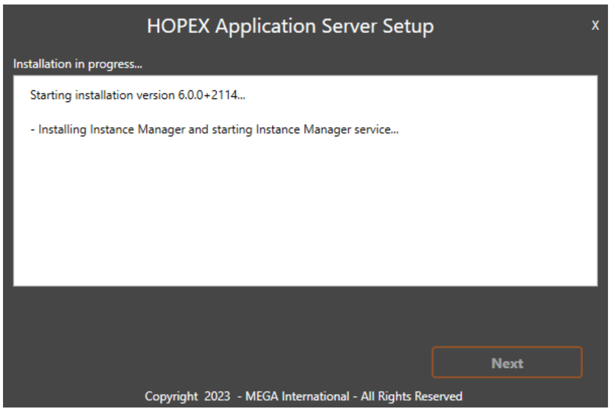
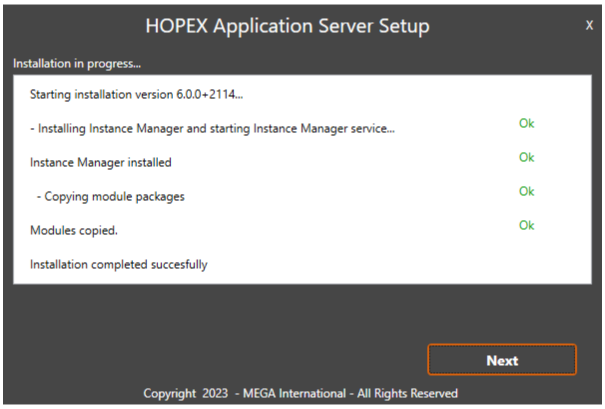
1. Copy this folder on the server where you want to continue the installation.
2. Double-click **has.setup.exe**.
3. Perform **step 1** and **step 2** again. You should arrive directly to **step 11**.

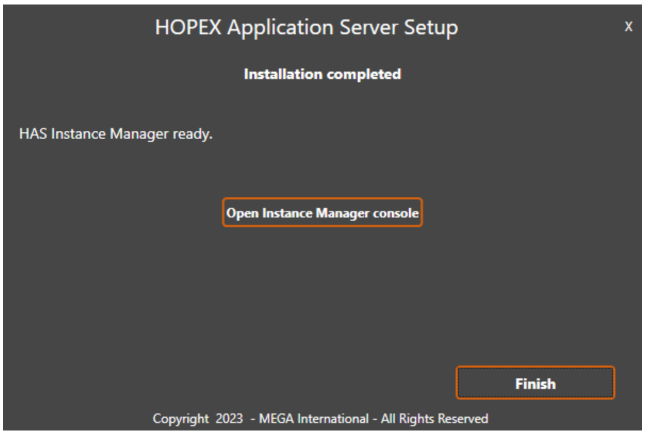
3.5.3. Continue setup

Step 11	Step 12
You need to specify which server you are deploying: - Production: for production server - Staging: for UAT and pre-production - Training: for training only - Development: for customization development  HOPEX Application Server Setup *Set the settings informations for installing HOPEX Application Agent on this machine. All informations are required.* HOPEX Agent Mode: Production Port: 30100 Password: Agent password for opening Agent console and for API. **Password minimum length is 6 characters.** Copyright 1986-2020 - MEGA International - All Rights Reserved	- In the **Mode** drop-down menu select "Production" (or the other choice depending on what you are installing) - In port adjust port number. Default 30100 **Caution:** do not use 80 or 443  HOPEX Application Server Setup *Set the settings informations for installing HOPEX Application Agent on this machine. All informations are required.* HOPEX Agent Mode: Production Port Api Key Agent console and for API. **Minimum length is 6 characters.** x Training Staging Production Development Advanced Previous Next Copyright 2021 - MEGA International - All Rights Reserved

The Mode as an impact on modules you can deploy, features you can enable and default logs details

Step 13	Step 14 (optional)
• Give an **API Key** value for the HAS Instance Manager REST API and Web portal. • This API Key is for server administrator only. **Minimum 6 characters with capital letters and special characters** You can change this API Key later if you forget it.  HOPEX Application Server Setup *Set the settings informations for installing HOPEX Application Agent on this machine. All informations are required.* HOPEX Agent Mode: Production Port: 30100 Api Key: ******** Agent api key for opening Agent console and for API. **Minimum length is 6 characters.** Advanced Previous Next	• Should you want to change: • folder locations *Default:* *"C:\Program Files\MEGA"* for HAS Instance Manager *and* *"C:\ProgramData\MEGA"* HAS for Instance • user to launch the windows service. **Required to access the Must License path or if there is more than 1 HAS Server** See below3.12 Windows User and access rights for more details. In that case: • Click **Advanced** • Adjust **User service** & **Password** (if blank Local System is the default) • Adjust folder locations • Click **OK** then click **Next**  HOPEX Application Server Setup Advanced settings User service: Password: HAS Agent service account (keep blank for LocalSystem) Agent: C:\MEGA_HAS\HAS.Agent Agent folder (default is programfiles/mega/has.agent) HAS instances: C:\MEGA_HAS\HOPEX Application Server HAS instances folder (default is program data/mega/hopex application server) Ok Cancel

Step 15	Step 16
The HAS Instance Manager is being installed and related packaged unzipped.  HOPEX Application Server Setup Installation in progress... Starting installation version 6.0.0+2114... - Installing Instance Manager and starting Instance Manager service... Copyright 2023 - MEGA International - All Rights Reserved	- When all successful (**OK** appears), click **Next**  HOPEX Application Server Setup Installation in progress... Starting installation version 6.0.0+2114... - Installing Instance Manager and starting Instance Manager service... Ok Instance Manager installed Ok - Copying module packages Ok Modules copied. Ok Installation completed succesfully Copyright 2023 - MEGA International - All Rights Reserved

Step 17	Step 18
At that step, the process is being launched by Windows. A process called **HAS.Instance.Manager.exe** should be visible in Windows Task Manager.	- When ready, the **Open Instance Manager console** message appears. - Click it: it will open your web browser.  HOPEX Application Server Setup **Installation completed** HAS Instance Manager ready. Copyright 2023 - MEGA International - All Rights Reserved

The installation process with the setup is finished.

- Click **Finish**.

If you forgot to open the **HAS Instance Manager** console you can access it on: http://localhost:30100/ (adjust port number if you have changed the default value)

Continue, to next step, to create the HAS Instance.

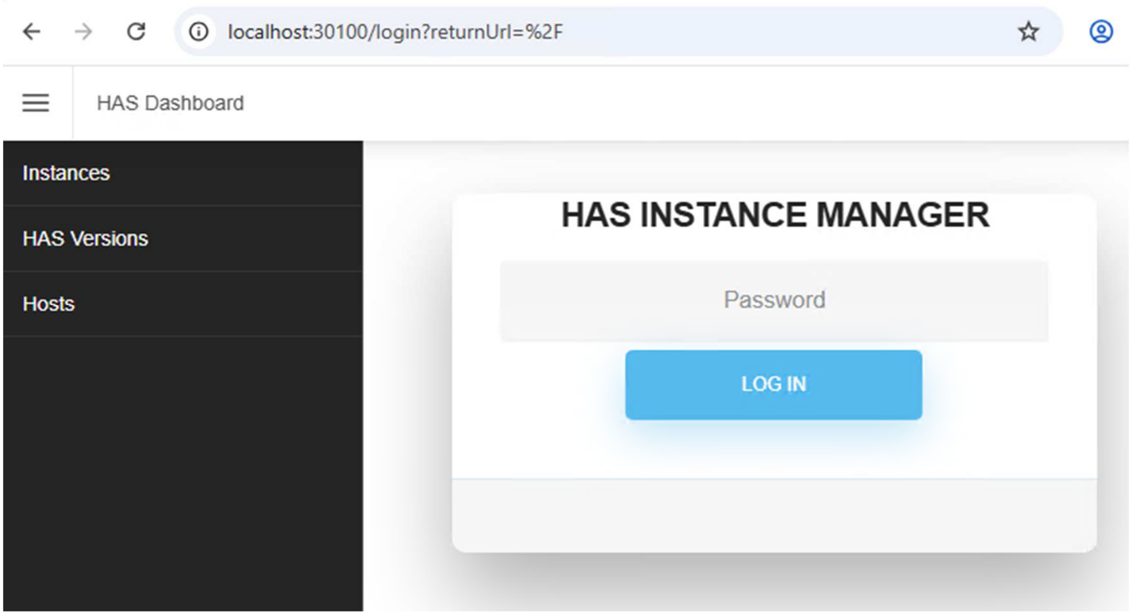
3.6. Creating HAS Instance

The HAS Instance Manager is now running. No HAS Server instance has been created by the setup.

- A minimum of one HAS Instance is required. Start from **Step 20**
- For cluster: see appropriate section.

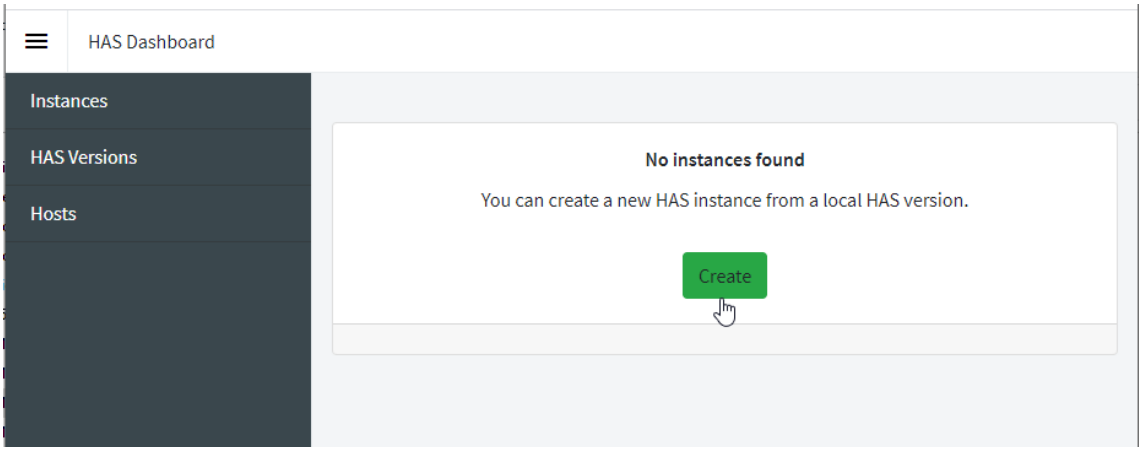
Step 20

- In the login page of the HAS Instance Manager console enter the **API Key** created at installation.



Step 21

- Click **New instance** to create an instance



No instances found

You can create a new HAS instance from a local HAS version.

Step 22

- Give a name to the cluster.

  For instance, "**HAS_PRODUCTION**"

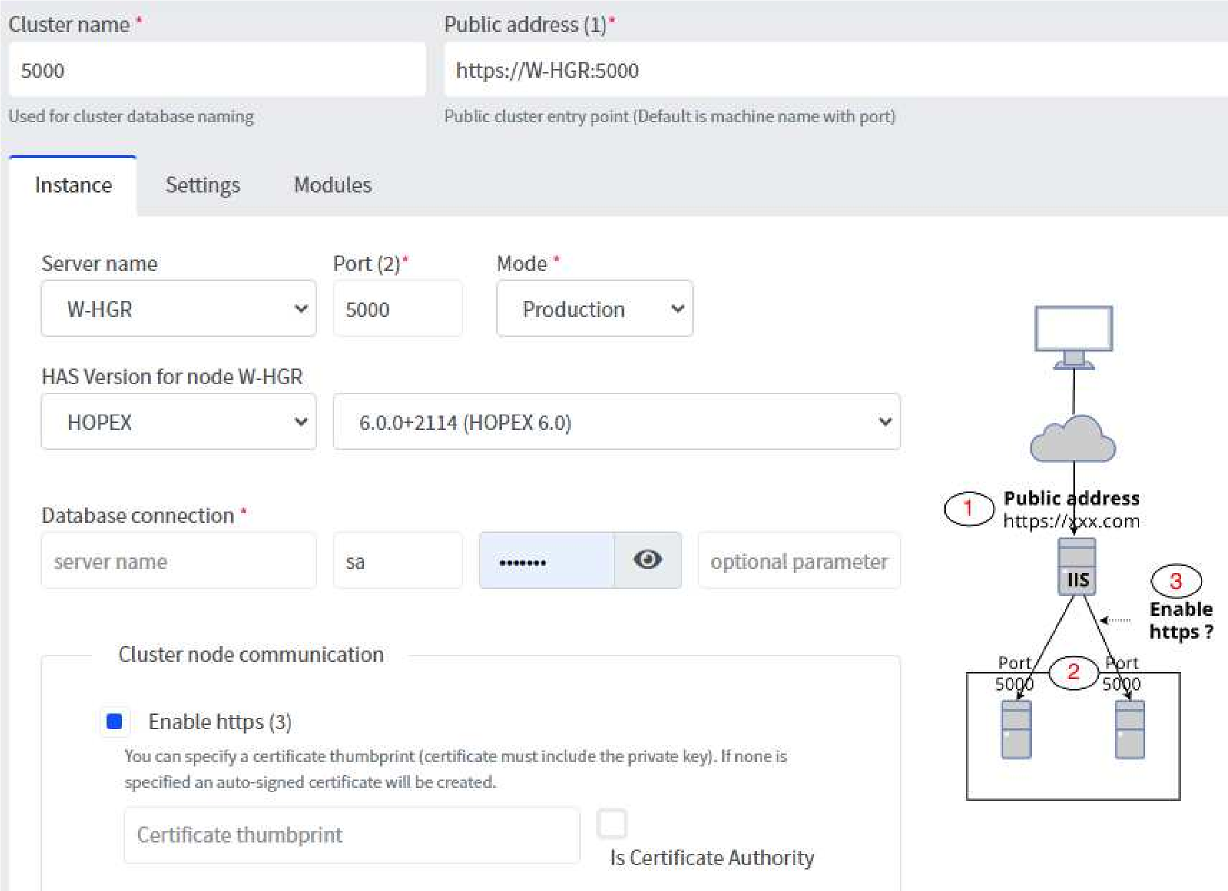
  Caution: If you keep default value ensure there is no existing cluster name with same name.

- Set the public URL. (Enter HTTP or HTTPS according to your case)

  Example: https://vp-iis1-v6.fr.mega.com

- Keep **Enable https** selected.

CAUTION: Do not leave the default value with the server name if you are not installing a standalone laptop.



Cluster name * 5000
Used for cluster database naming

Public address (1)* https://W-HGR:5000
Public cluster entry point (Default is machine name with port)

Instance | Settings | Modules

Server name: W-HGR
Port (2)*: 5000
Mode *: Production

HAS Version for node W-HGR: HOPEX | 6.0.0+2114 (HOPEX 6.0)

Database connection *: server name | sa | ••••••• | optional parameter

Cluster node communication

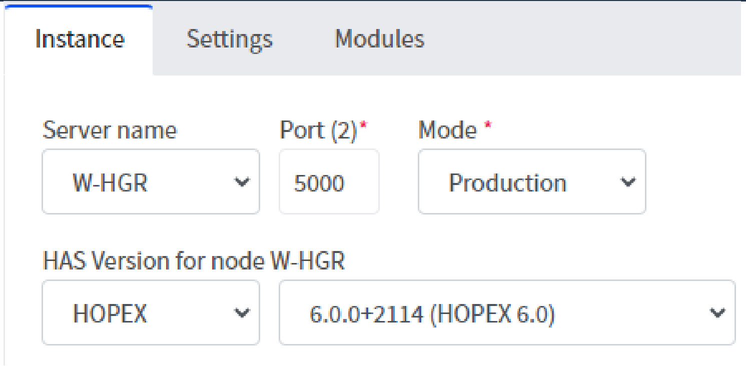
☑ Enable https (3)

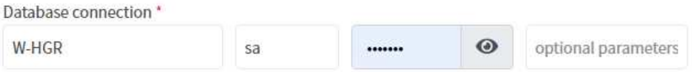
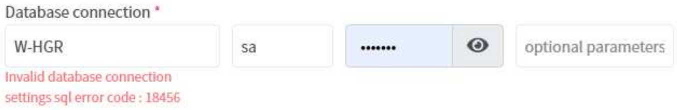
You can specify a certificate thumbprint (certificate must include the private key). If none is specified an auto-signed certificate will be created.

Certificate thumbprint

□ Is Certificate Authority

The name given to the instance will be the name of the database for HAS.

Step 23	
In the tab **Instance** fill in the following information: • Select the **Server Name**. Default: the server on which you are performing the installation. • Set HAS Instance **Port**. Default: 5000 • Select an HAS Bundle. Default: HOPEX • Select an **HAS** Instance **Version**. Default: the one selected at setup	 Instance | Settings | Modules Server name: W-HGR Port (2)*: 5000 Mode *: Production HAS Version for node W-HGR: HOPEX 6.0.0+2114 (HOPEX 6.0)

Step 24	
• Define the Database connection. Should you make an error in database connection an error message appears. • SQL Server instance <<machine network name>>\<<SQL instance name>> • SQL Server User Account User enabled to access/update SQL Server • SQL Server User Password Password of the SQL server user • Optional parameter If you want to use the trusted connection mode put: Trusted_Connection=True In that case login and password should be empty. Make sure you have set the user service for HAS Instance Manager see below 3.12 Windows User and access rights	 Database connection * W-HGR | sa | ••••••• | optional parameters In case of Database connection error:  Database connection * W-HGR | sa | ••••••• | optional parameters Invalid database connection settings sql error code : 18456

Step 25

In the **Settings** tab enter the following information:

- **HOPEX Store** installation Key.

Default: it is prefilled with the information given at setup. Except if you went offline.

<u>Optional actions </u>(that you can perform later if needed):

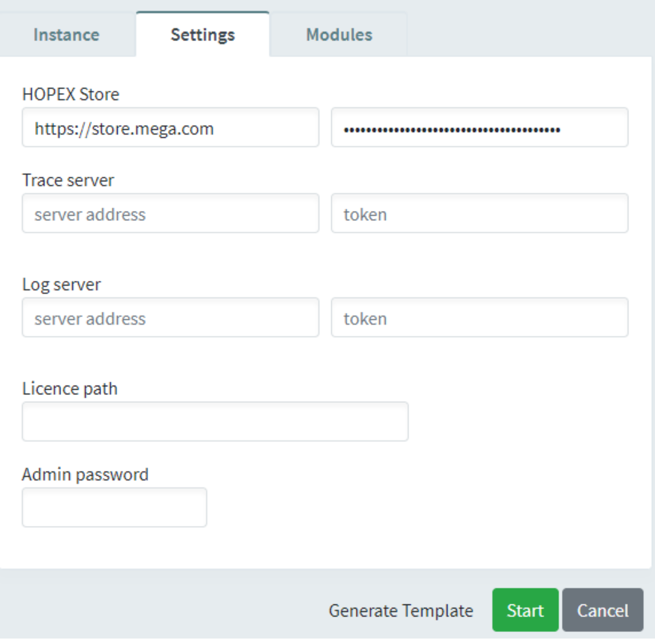
- **Log server**: if you want to use SEQ add the URL and token to connect to the log server.
- **Tracer server**: if you want to use Zipkin add the URL and token to connect to the log server.
- **License path**: path of the UNC for the Must license

<u>Example:</u> \\W-OGD\Must

- **Admin password**: change the default password for admin user on the console.

<u>Example:</u> Has2k21!

Note: password must comply with complexity rules.



HOPEX Store: https://store.mega.com | ••••••••••••••••••••••••••••••••••••••

Trace server: server address | token

Log server: server address | token

Licence path:

Admin password:

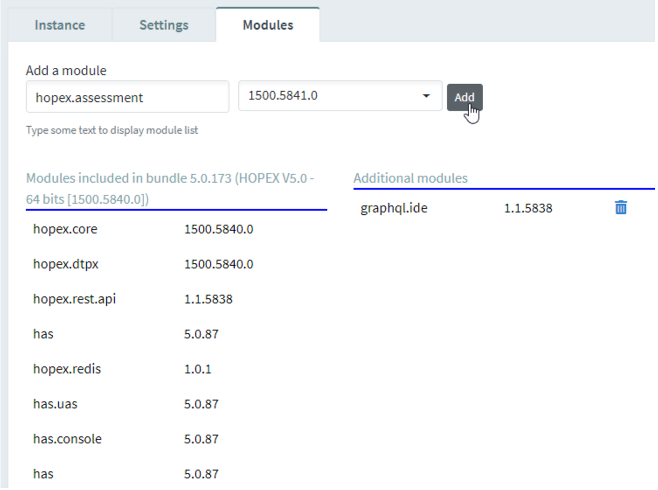
Step 26 (optional)

The **Modules** tab displays the modules available by default in the bundle.

If your server has internet access to the https://store.mega.com you can add complementary module at this step.

Otherwise skip this step.

- Select the module to add. The selection is done by the module ID
- Select the required version.
- Click **Add**.



Add a module: hopex.assessment | 1500.5841.0

Type some text to display module list

Modules included in bundle 5.0.173 (HOPEX V5.0 - 64 bits [1500.5840.0])

hopex.core	1500.5840.0
hopex.dtpx	1500.5840.0
hopex.rest.api	1.1.5838
has	5.0.87
hopex.redis	1.0.1
has.uas	5.0.87
has.console	5.0.87
has	5.0.87

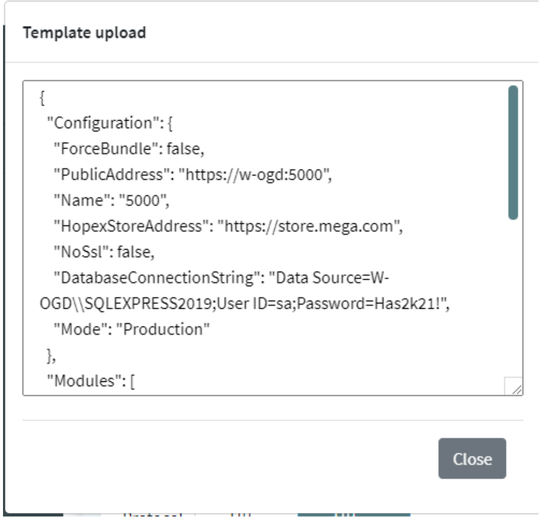
Additional modules

graphql.ide	1.1.5838

Step 27 (optional)

When your settings are correct you can save same as a template for scripting installation purposes.

- click Generate template.
- Copy and save the generate JSON in a text file

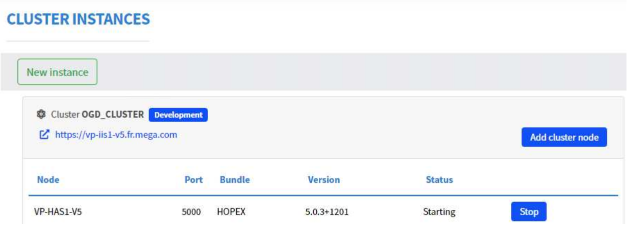


Template upload

```
{
  "Configuration": {
    "ForceBundle": false,
    "PublicAddress": "https://w-ogd:5000",
    "Name": "5000",
    "HopexStoreAddress": "https://store.mega.com",
    "NoSsl": false,
    "DatabaseConnectionString": "Data Source=W-
OGD\\SQLEXPRESS2019;User ID=sa;Password=Has2k21!",
    "Mode": "Production"
  },
  "Modules": [
```

Step 28

- Click **Start**
- When ready the status changes to "**Running**"
- Click the URL Public address to access the HAS Instance created



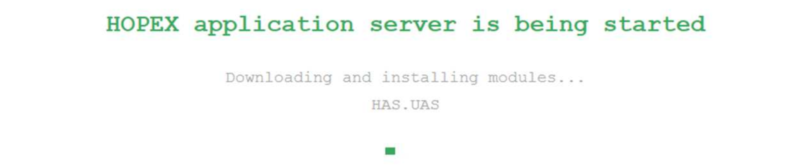
CLUSTER INSTANCES

Node	Port	Bundle	Version	Status	
VP-HAS1-V5	5000	HOPEX	5.0.3+1201	Starting	Stop

The URL visible at that stage should be the public URL. Should you see an URL such as https://localhost:5000 or https://servername:5000 your installation is not correct

Step 29

- While loading you will see a message HAS is starting with the list of modules being deployed



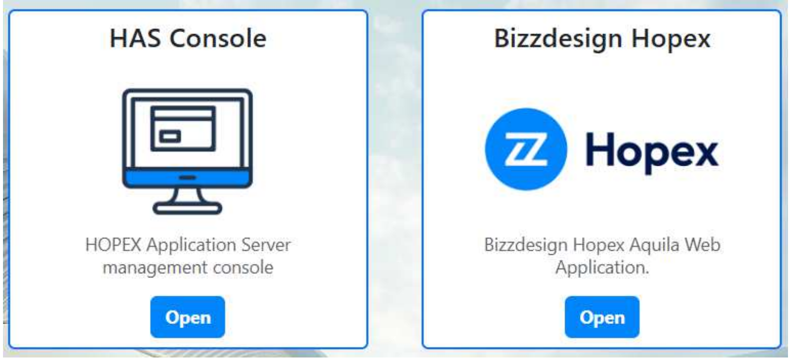
HOPEX application server is being started

Downloading and installing modules...

HAS.UAS

When ready you get redirected to the HAS portal

- Click the **HAS console** tile to enter the console.



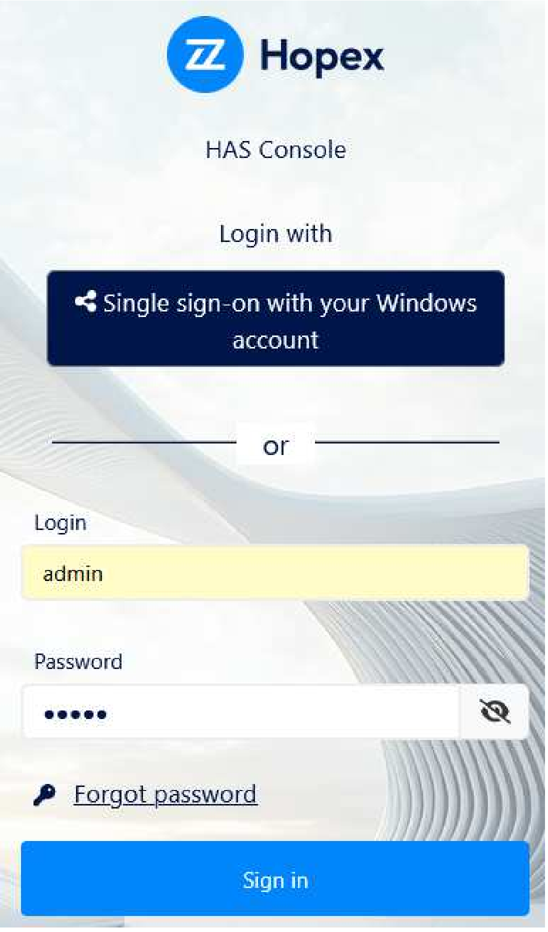
HAS Console

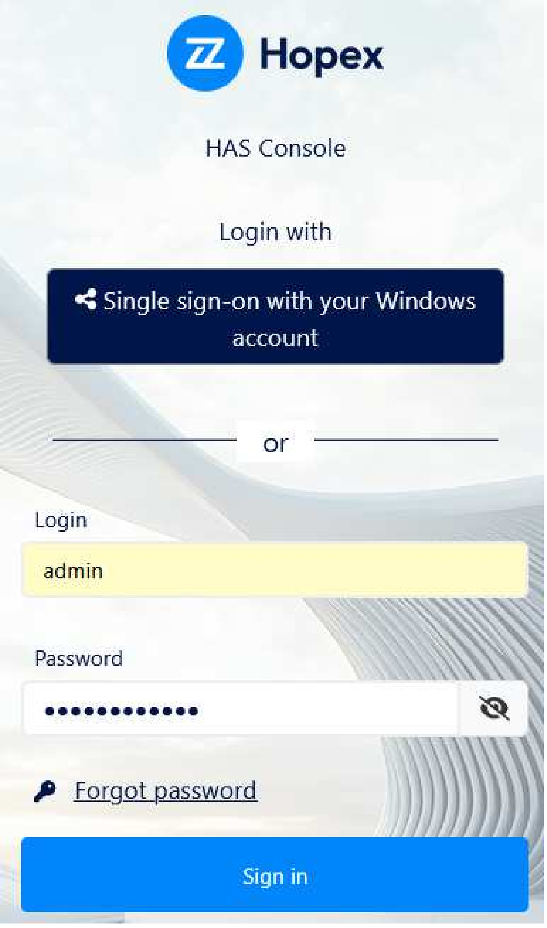
HOPEX Application Server management console

Bizzdesign Hopex

Bizzdesign Hopex Aquila Web Application.

3.7. First connection to HAS Console

Step 30	Step 31 (optional)
- At first login (creation of the HAS database) on the HAS Console the default login and password are: - Login: **admin** - Password: **Hopex** (except if you did set it up on step 25) - Enter the values in the fields - Click **Sign in**.  Login: admin Password: ••••• Hopex HAS Console Login with Single sign-on with your Windows account or Forgot password Sign in	- Change the password as requested. - Click **Change password** The password must: - include at least 8 characters, one uppercase, one lowercase, one digit, and one special character - not use any sequence of characters (e.g.: 12345, qwert) nor contextual words (e.g.: hopex, mega) - be complex enough to meet your enterprise security requirements

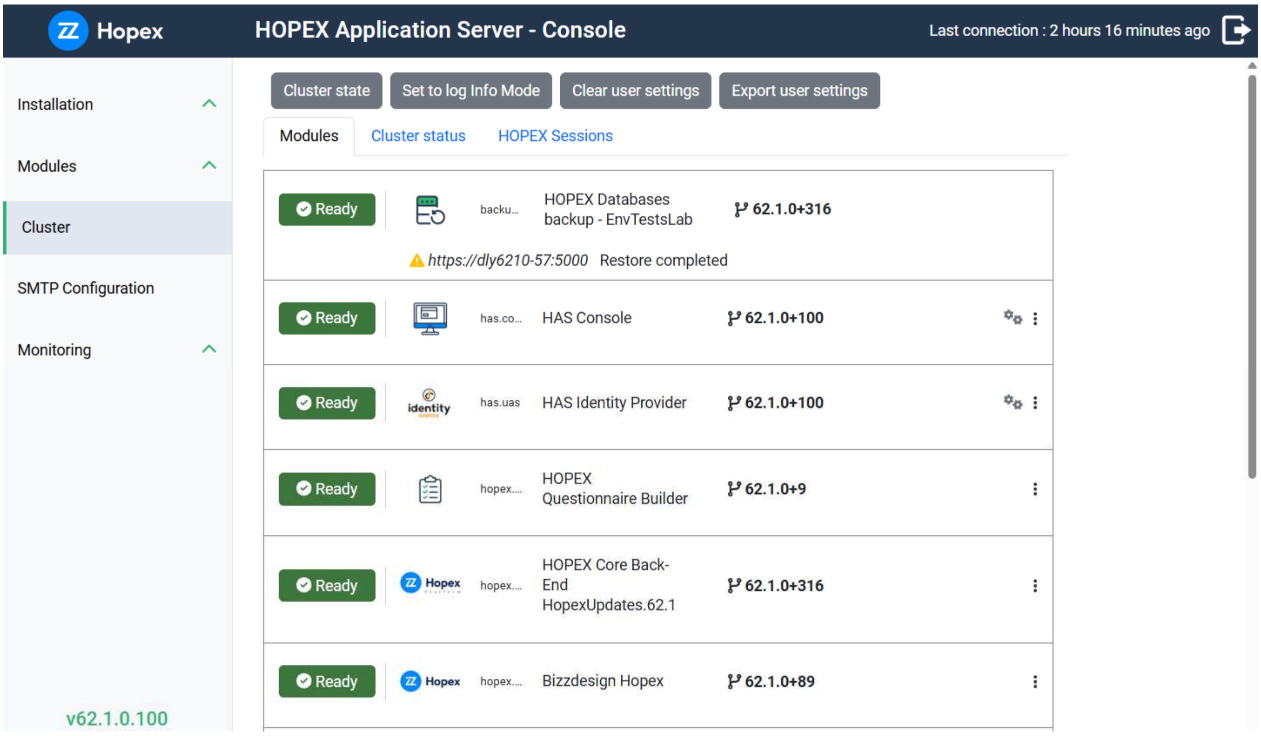
Step 32 (optional)	Step 33 (optional)
• When successful a message informs you that: "**Password has been changed successfully**". • Click **Sign in with new password**.	• Login with the new password with user "**Admin**".  Hopex HAS Console Login with Single sign-on with your Windows account or Login admin Password ••••••••••••• Forgot password Sign in

Step 34

The **Console** shows the modules that are installed and running.

HOPEX Core is not running because it needs:

- the Must license
- One environment (SystemDB)



Ready	backu...	HOPEX Databases backup - EnvTestsLab	62.1.0+316	
		⚠ https://dly6210-57:5000 Restore completed		
Ready	has.co...	HAS Console	62.1.0+100	⋮
Ready	has.uas	HAS Identity Provider	62.1.0+100	⋮
Ready	hopex....	HOPEX Questionnaire Builder	62.1.0+9	⋮
Ready	hopex....	HOPEX Core Back-End HopexUpdates.62.1	62.1.0+316	⋮
Ready	hopex....	Bizzdesign Hopex	62.1.0+89	⋮

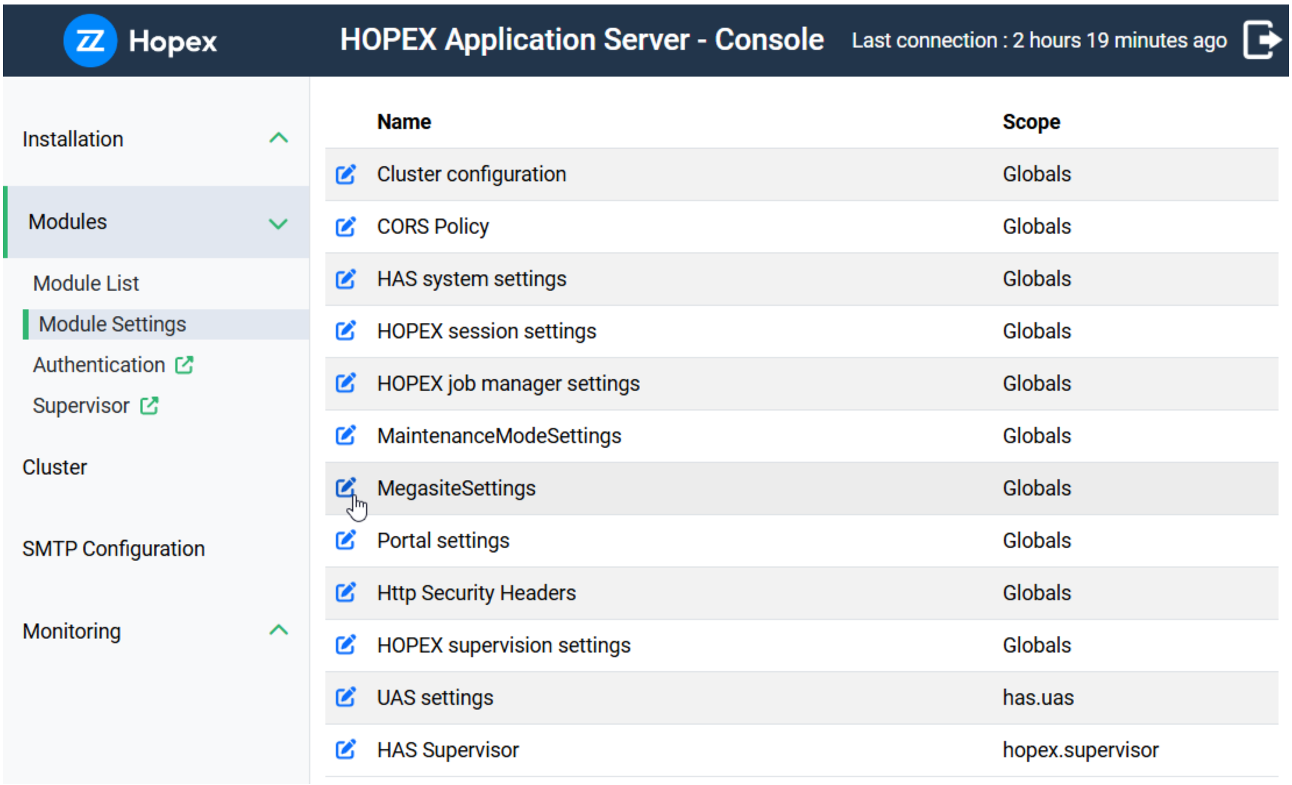
3.8. Adding Must license to MegaSite.ini setting

If you have already set the Must license path with the Instance Manager on **Step 25**, you can skip the following steps and **go to step 50**.

Step 40

Edit **MegaSite.ini**:

- Select **Modules > Module Settings** menu
- In the right pane, click the **MegasiteSettings** icon to edit "Megasite.ini"



Name	Scope
Cluster configuration	Globals
CORS Policy	Globals
HAS system settings	Globals
HOPEX session settings	Globals
HOPEX job manager settings	Globals
MaintenanceModeSettings	Globals
MegasiteSettings	Globals
Portal settings	Globals
Http Security Headers	Globals
HOPEX supervision settings	Globals
UAS settings	has.uas
HAS Supervisor	hopex.supervisor

Step 41

Add Must settings in the text area:

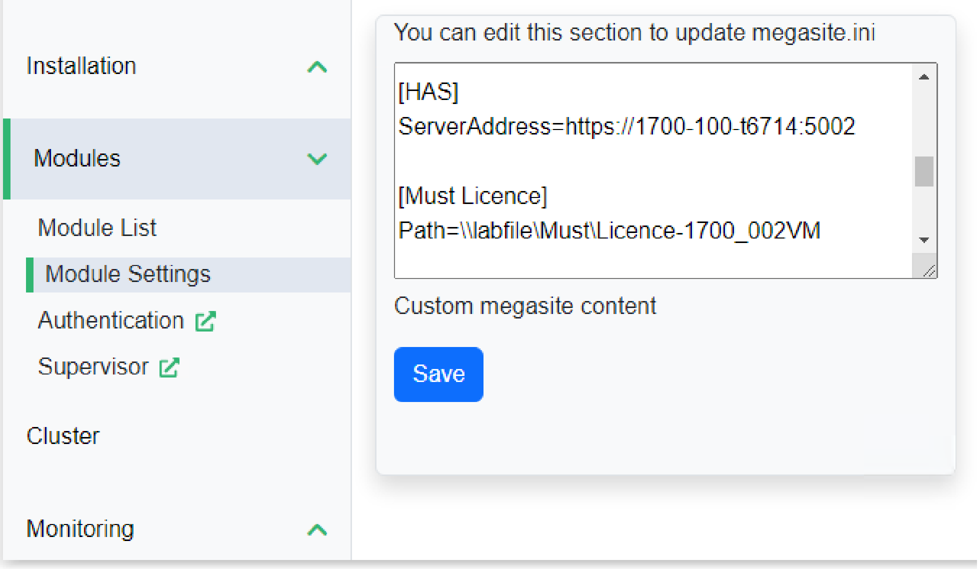
- Add the following section:

  [Must licence]

  Path=<< UNC server>>

  Where <<UNC server>> is the path given to sales administration when you requested your Must license file.

- Click **Save**



You can edit this section to update megasite.ini

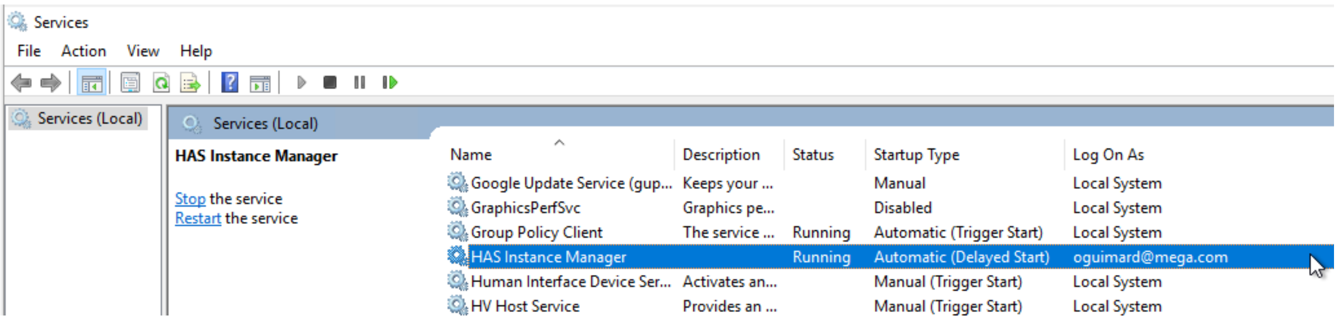
```
[HAS]
ServerAddress=https://1700-100-t6714:5002

[Must Licence]
Path=\\labfile\Must\Licence-1700_002VM
```

Custom megasite content

If the license is not correct all next steps will fail. Moreover, **HOPEX Core** cannot start if there is no environment with a valid **SystemDb**.

If you did not set yet a domain user, HOPEX will not be able to access the shared drive for the license.

To verify the user used to launch HAS Instance manager go to windows services and search for HAS Instance Manager.



HAS Instance Manager

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Google Update Service (gup...	Keeps your ...		Manual	Local System
GraphicsPerfSvc	Graphics pe...		Disabled	Local System
Group Policy Client	The service ...	Running	Automatic (Trigger Start)	Local System
HAS Instance Manager		Running	Automatic (Delayed Start)	oguimard@mega.com
Human Interface Device Ser...	Activates an...		Manual (Trigger Start)	Local System
HV Host Service	Provides an ...		Manual (Trigger Start)	Local System

3.9. Creating or referencing HOPEX environment

Now you have 3 possibilities:

- **Creating** a totally new HOPEX environment: **at first installation** (new SQL Server databases)
- **Restoring** existing HOPEX environments (**recommended choice**)
    - To leverage "backup" provided in the MEGA HOPEX Store **at first installation** (restore)
    - To leverage existing databases (migration)
- **Referencing:** To leverage existing environment when you migrate from previous version.

For:

- Creating: start at step 50
- Restoring: start at step 60 ➔ **recommended choice**
- Referencing start at step 70

3.9.1. Creating a New "HOPEX environment"

This solution may take a while as it creates all the database structure and technical content. The system will:

- create a SystemDB (~2h)
- create a repository (~10min)

For a faster approach go to the recommended choice.

First you must download the HOPEX Environment Installation Package V5.0 from the store and import it in HAS Console module
https://store.mega.com/modules/details/hopex.core.install

Step 50

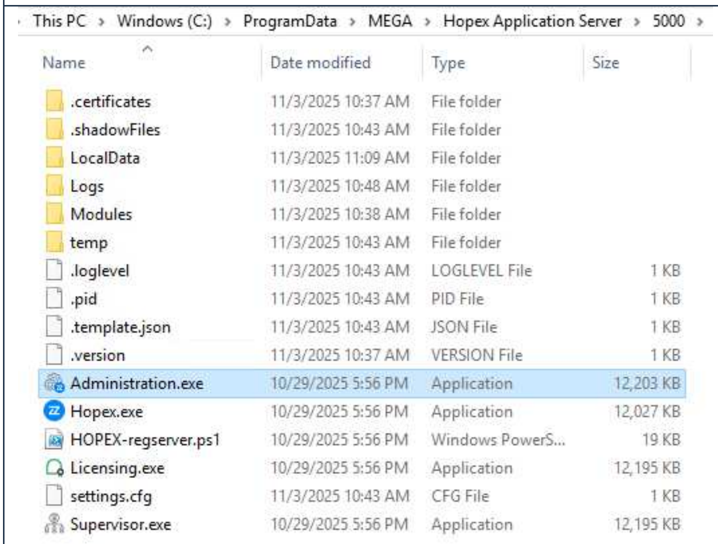
- Go to HOPEX installation folder

Default: C:\ProgramData\MEGA\Hopex Application Server\5000

- Launch Administration.exe

If it doesn't launch, you have:

- a license issues,
- a HAS web access issue.

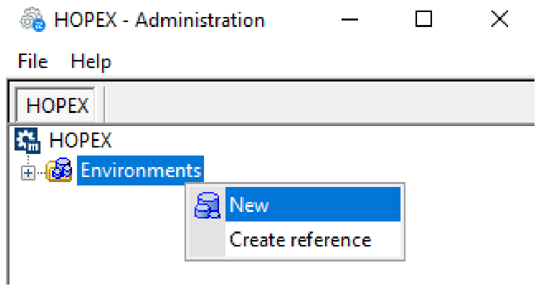


This PC > Windows (C:) > ProgramData > MEGA > Hopex Application Server > 5000 >

Name	Date modified	Type	Size
.certificates	11/3/2025 10:37 AM	File folder	
.shadowFiles	11/3/2025 10:43 AM	File folder	
LocalData	11/3/2025 11:09 AM	File folder	
Logs	11/3/2025 10:48 AM	File folder	
Modules	11/3/2025 10:38 AM	File folder	
temp	11/3/2025 10:43 AM	File folder	
.loglevel	11/3/2025 10:43 AM	LOGLEVEL File	1 KB
.pid	11/3/2025 10:43 AM	PID File	1 KB
.template.json	11/3/2025 10:43 AM	JSON File	1 KB
.version	11/3/2025 10:37 AM	VERSION File	1 KB
Administration.exe	10/29/2025 5:56 PM	Application	12,203 KB
Hopex.exe	10/29/2025 5:56 PM	Application	12,027 KB
HOPEX-regserver.ps1	10/29/2025 5:56 PM	Windows PowerS...	19 KB
Licensing.exe	10/29/2025 5:56 PM	Application	12,195 KB
settings.cfg	11/3/2025 10:43 AM	CFG File	1 KB
Supervisor.exe	10/29/2025 5:56 PM	Application	12,195 KB

Step 51

- Right-click **Environments > New**



Step 52

- Give a name to your environment. It will create a database with the name:

  <<Name>>_SystemDb

- Adjust location of the folder. A set of files will be created. In case of Cluster/Farms deployment the Location should be a shared folder

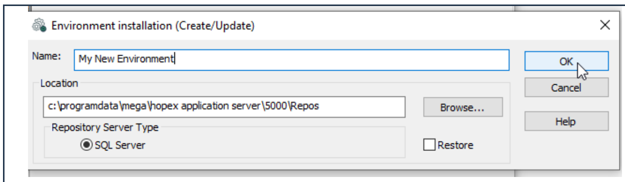
Example: \\Environments\SharedEnvFolder

- Click **OK**.

Step 53

- Enter SQL instance parameter
- Set the SQL user password
- Set the password for the SQL password
- Set the parameter Encrypt=no; or "yes" if you use SSL communication

For other SQL instance connection string please read the appropriate database setting documentation. Used **Trusted Connection** if you rely on domain user to authenticate to SQL Server. Leave login/password blank in that case.



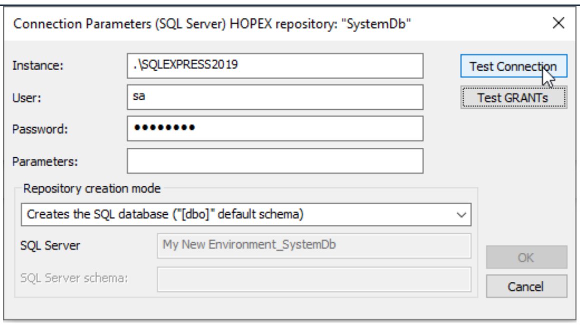
Environment installation (Create/Update)

Name: My New Environment

Location: c:\programdata\mega\hopex application server\5000\Repos

Repository Server Type: ● SQL Server

□ Restore



Connection Parameters (SQL Server) HOPEX repository: "SystemDb"

Instance: .\SQLEXPRESS2019

User: sa

Password: ••••••••

Parameters:

Repository creation mode: Creates the SQL database ("[dbo]" default schema)

SQL Server: My New Environment_SystemDb

SQL Server schema:

CAUTION: for ODBC Driver 18 ensure to put Encrypt=no; in parameter if you do not leverage SSL communication with SQL Server

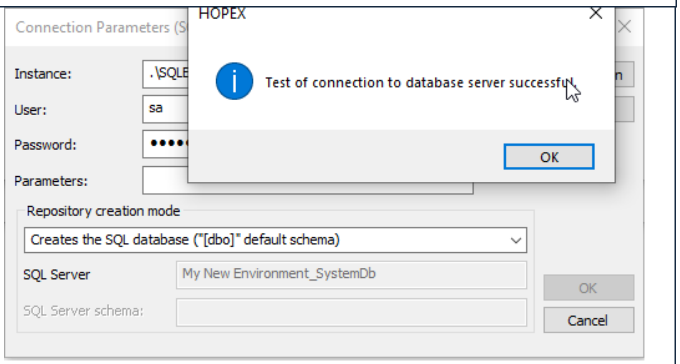
Step 54

- Click **Test Connection**

  Ensure the message says "Successful" else adjust the configuration in previous step

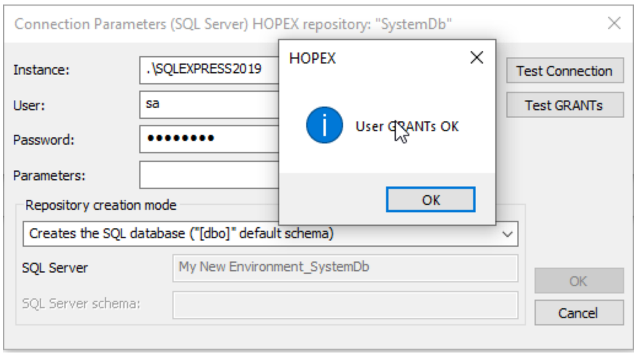
- Click **Test GRANTs**

Ensure the message says "User GRANTs OK" else adjust the configuration in previous step



HOPEX

Test of connection to database server successful



HOPEX

User GRANTs OK

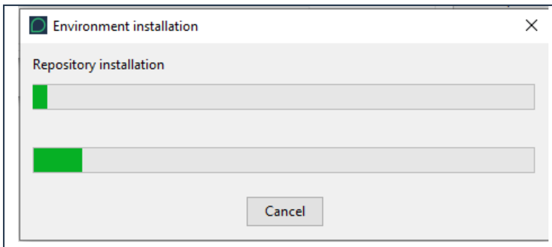
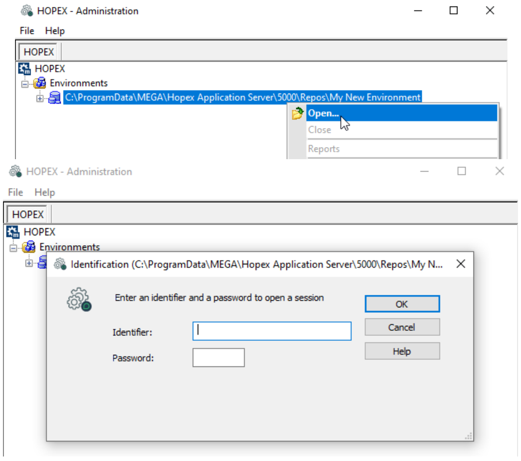
Step 55

- The process is in progress. It may take a while (From 2 to 6 hours)

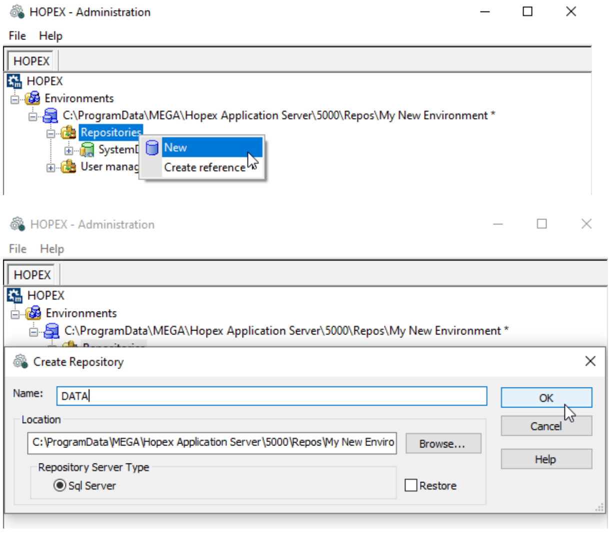
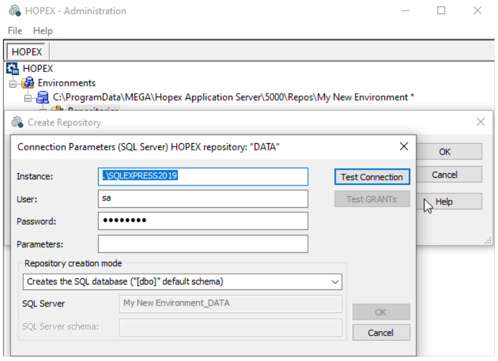
Step 56

Once the environment is created:

- Right-click the environment and select **Open**
- Default Identifier: "System" with Hopex as password (or empty for previous version)
- Click **OK**

 Environment installation Repository installation	 HOPEX - Administration C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\My New Environment Identification (C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\My N... Enter an identifier and a password to open a session

This documentation is done for an English Environment and Repositories. If you want a repository in French/Spanish/German/Italian…Ensure to compile the Metamodel in the appropriate language before creating the repository.

Step 57	Step 58
- Expand the environment - Right-click **Repositories** and select **New** - Give a name to the repository "DATA" - Click **OK**	- If prompted **Test Connection** and **Test Grants** - The creation is in progress. some file will be imported automatically. CAUTION: do not click Cancel or Pause For information: the repository language at creation is the same as the SystemDB one.
 C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\My New Environment * Create Repository Name: DATA Location: C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\My New Enviro Repository Server Type: ● Sql Server □ Restore	 C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\My New Environment * Connection Parameters (SQL Server) HOPEX repository: "DATA" Instance: .\SQLEXPRESS2019 User: sa Password: •••••••• Parameters: Repository creation mode: Creates the SQL database ("[dbo]" default schema) SQL Server: My New Environment_DATA SQL Server schema:

Step 59

Once the repository is created:

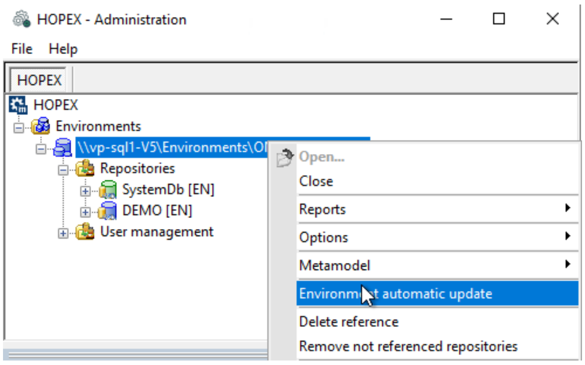
- Right-click the environment and select **Environment automatic update**

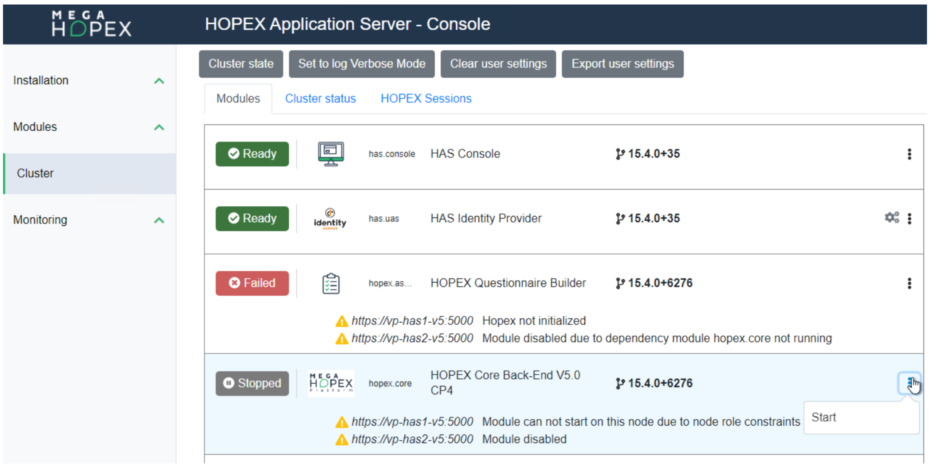
  You may need to stop the module **HOPEX Core Back-End** from **HAS Console** and restart **Administration.exe**

- Follow the step of the wizard by clicking Next up to **Run**.

For **PRODUCTION** environment:

- Select **Permission compilation**





Ready has.console HAS Console 15.4.0+35

Ready has.uas HAS Identity Provider 15.4.0+35

Failed hopex.as... HOPEX Questionnaire Builder 15.4.0+6276

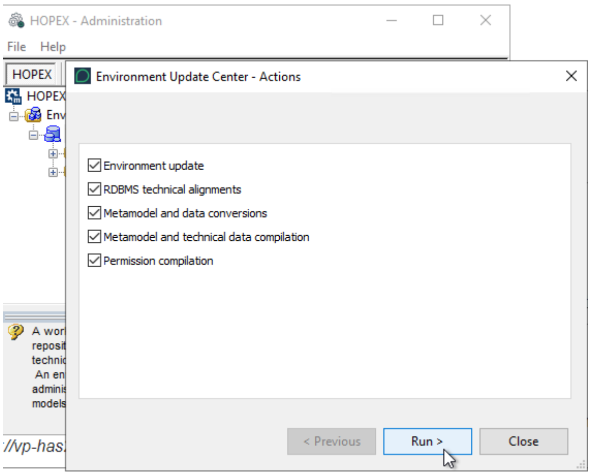
https://vp-has1-v5:5000 Hopex not initialized

https://vp-has2-v5:5000 Module disabled due to dependency module hopex.core not running

Stopped hopex.core HOPEX Core Back-End V5.0 CP4 15.4.0+6276

https://vp-has1-v5:5000 Module can not start on this node due to node role constraints

https://vp-has2-v5:5000 Module disabled



☑ Environment update
☑ RDBMS technical alignments
☑ Metamodel and data conversions
☑ Metamodel and technical data compilation
☑ Permission compilation

3.9.2. Restoring an existing database

Restore an existing database if you did not just create a totally new environment in previous chapter.

Two scenarios:

- You are a totally new customer:

  You can leverage “backup” provided by MEGA HOPEX Store

- You are an existing customer:

  You have existing database (SystemDb and repositories) that you want to add to this new installation. This is common in case of migration to a newer version.

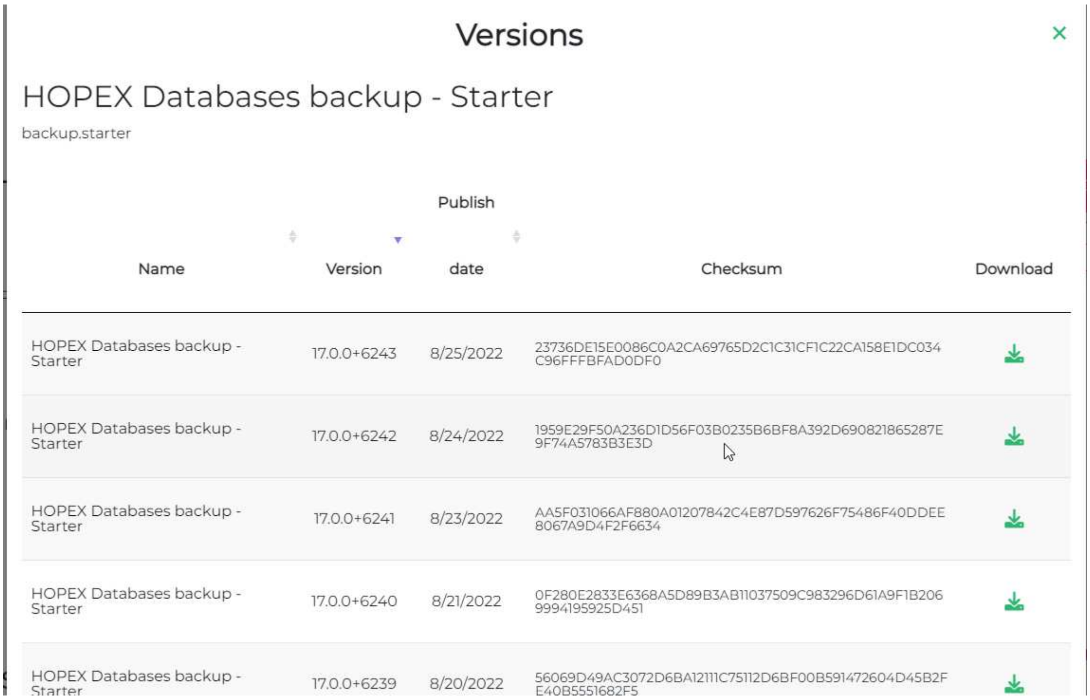
3.9.2.1. Get MEGA HOPEX Store backup

You may skip this part if you already have backup.

Step 60

- Go to MEGA HOPEX Store to get the **HOPEX Databases backup -Starter**

  https://store.mega.com/modules/details/backup.starter
- Download the backup related to your version*. Click "Other version" to access all versions.

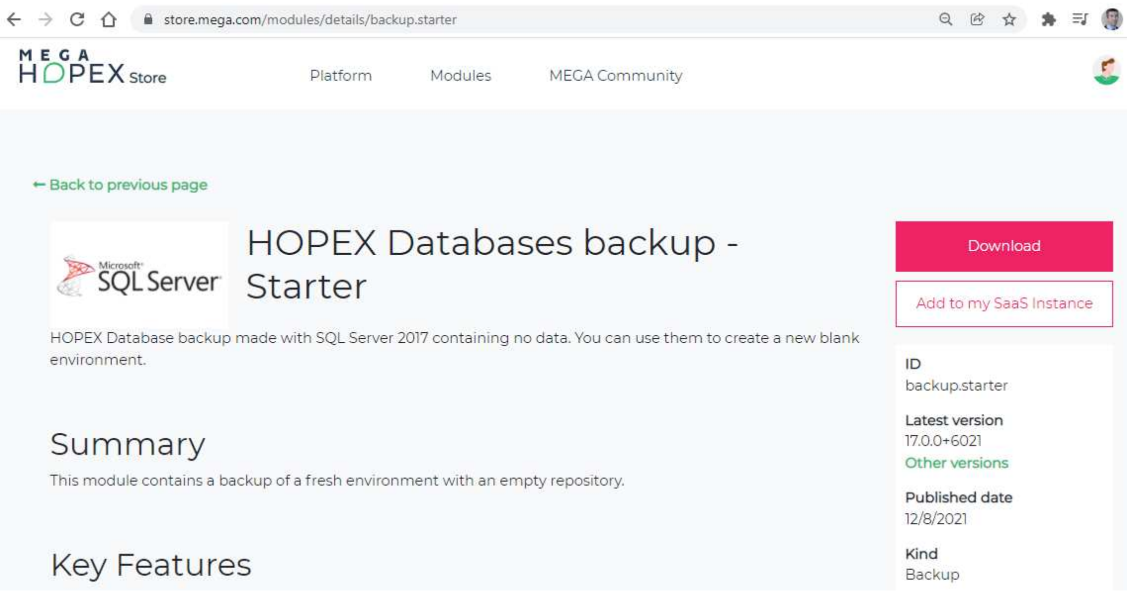


Versions

HOPEX Databases backup - Starter

backup.starter

Name	Version	Publish date	Checksum	Download
HOPEX Databases backup - Starter	17.0.0+6243	8/25/2022	23736DE15E0086C0A2CA69765D2C1C31CF1C22CA158E1DC034C96FFFBFAD0DF0	⤓
HOPEX Databases backup - Starter	17.0.0+6242	8/24/2022	1959E29F50A236D1D56F03B0235B6BF8A392D690821865287E9F74A5783B3E3D	⤓
HOPEX Databases backup - Starter	17.0.0+6241	8/23/2022	AA5F031066AF880A01207842C4E87D597626F75486F40DDEE8067A9D4F2F6634	⤓
HOPEX Databases backup - Starter	17.0.0+6240	8/21/2022	0F280E2833E6368A5D89B3AB11037509C983296D61A9F1B2069994195925D451	⤓
HOPEX Databases backup - Starter	17.0.0+6239	8/20/2022	56069D49AC3072D6BA12111C75112D6BF00B591472604D45B2FE40B5551682F5	⤓



HOPEX Databases backup - Starter

HOPEX Database backup made with SQL Server 2017 containing no data. You can use them to create a new blank environment.

ID
backup.starter

Latest version
17.0.0+6021
Other versions

Published date
12/8/2021

Kind
Backup

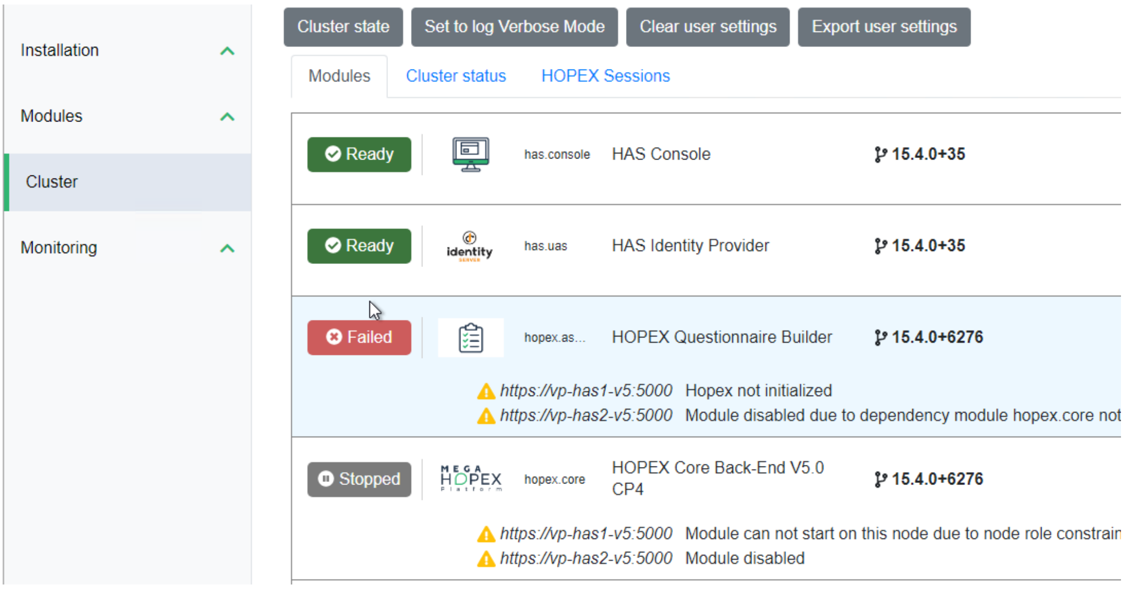
Summary

This module contains a backup of a fresh environment with an empty repository.

Key Features

*To know your version:

- In HAS Console, select **Cluster** menu
- Check the version number for **HOPEX Core Back-end** module
- Take the same version and build x.x.x+xxxx



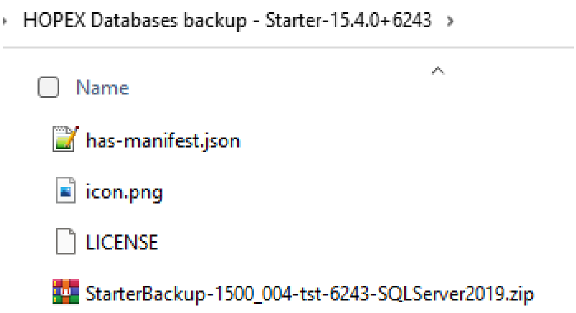
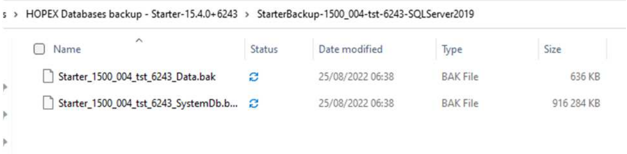
Ready	has.console	HAS Console	15.4.0+35
Ready	has.uas	HAS Identity Provider	15.4.0+35
Failed	hopex.as...	HOPEX Questionnaire Builder	15.4.0+6276
Stopped	hopex.core	HOPEX Core Back-End V5.0 CP4	15.4.0+6276

HOPEX Questionnaire Builder:

⚠ *https://vp-has1-v5:5000* Hopex not initialized
⚠ *https://vp-has2-v5:5000* Module disabled due to dependency module hopex.core not

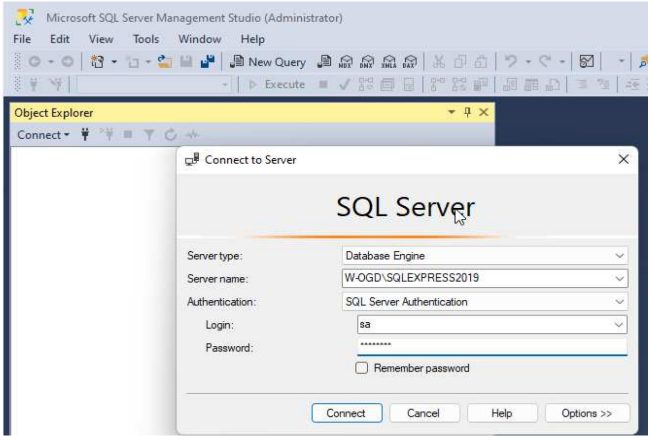
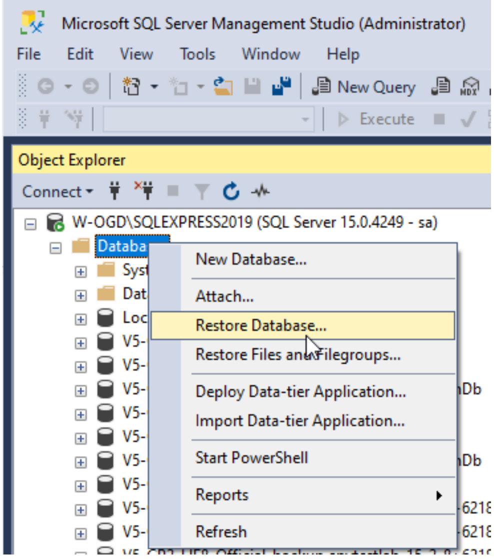
HOPEX Core Back-End V5.0 CP4:

⚠ *https://vp-has1-v5:5000* Module can not start on this node due to node role constrain
⚠ *https://vp-has2-v5:5000* Module disabled

Step 61	Step 62
• Rename extension haspk to zip or open directly with your preferred tool to extract. • Unzip the downloaded file • Unzip the zipped contained inside  HOPEX Databases backup - Starter-15.4.0+6243 › Name has-manifest.json icon.png LICENSE StarterBackup-1500_004-tst-6243-SQLServer2019.zip	• You should have 2 files with the extension ".bak" named: "Starter..._Data.bak" "Starter..._SystemDb.bak"  › HOPEX Databases backup - Starter-15.4.0+6243 › StarterBackup-1500_004-tst-6243-SQLServer2019 Name | Status | Date modified | Type | Size Starter_1500_004_tst_6243_Data.bak | 25/08/2022 06:38 | BAK File | 636 KB Starter_1500_004_tst_6243_SystemDb.b... | 25/08/2022 06:38 | BAK File | 916 284 KB

You now need to import those .bak in SQL Server. Many options are possible and many tools exist to perform this action. **Use your preferred tool**.

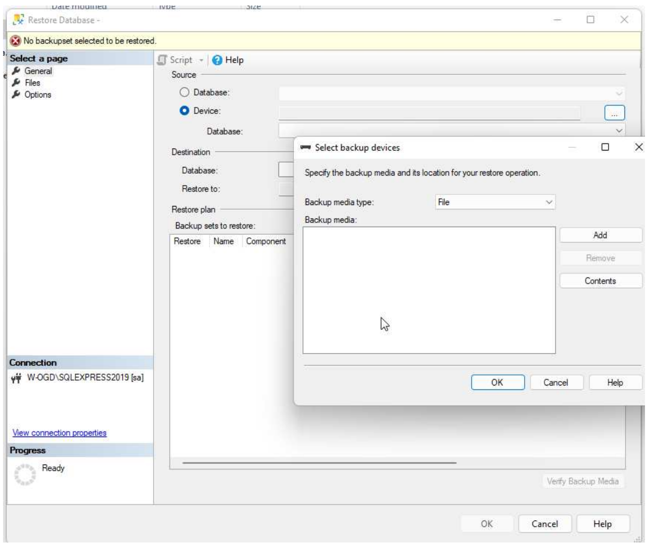
The following step uses **SQL Management Studio** as an example. You can download it here: https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver16

Step 63	Step 64
• Launch SQL Management Studio and connect to your SQL Server • Use the user account that has enough privilege. In that example "sa"  Connect to Server SQL Server Server type: Database Engine Server name: W-OGD\SQLEXPRESS2019 Authentication: SQL Server Authentication Login: sa Password: ******** □ Remember password Connect | Cancel | Help | Options >>	• Right-click **Databases** and select **Restore Database**  W-OGD\SQLEXPRESS2019 (SQL Server 15.0.4249 - sa)

Microsoft SQL Server Management Studio (Administrator)
File Edit View Tools Window Help
New Query
Execute
Object Explorer
Connect
Databa
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Deploy Data-tier Application...
Import Data-tier Application...
Start PowerShell
Reports
Refresh

Step 65

- Select device
- Click **Add**



Restore Database -

No backupset selected to be restored.

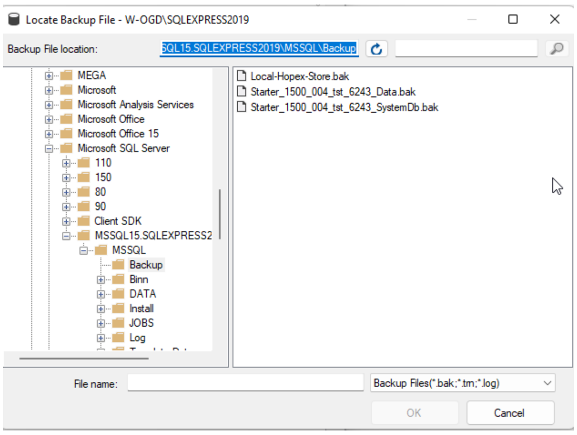
Specify the backup media and its location for your restore operation.

Backup media type: File

Backup media:

Step 66

- Browser for the backup you want to restore

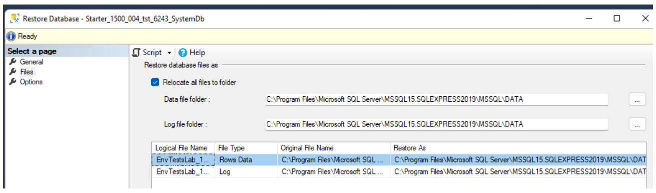


Locate Backup File - W-OGD\SQLEXPRESS2019

Backup File location: SQL15.SQLEXPRESS2019\MSSQL\Backup

Step 67 (optional)

- Click **Files**
- Click Relocate all files to folder
- Adjust file location and name
- Click **OK**



Restore Database - Starter_1500_004_tst_6243_SystemDb

Ready

Restore database files as

☑ Relocate all files to folder

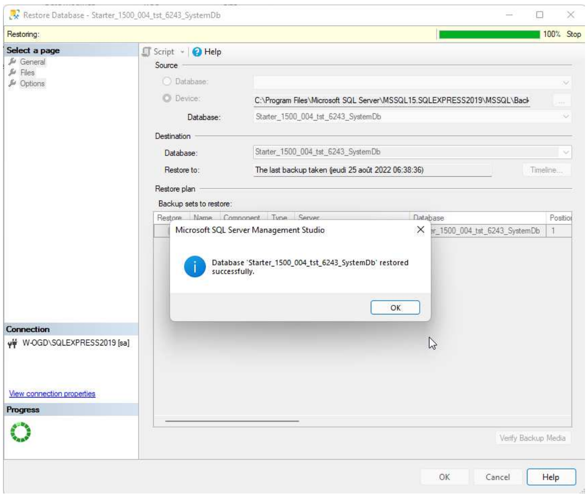
Data file folder : C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS2019\MSSQL\DATA

Log file folder : C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS2019\MSSQL\DATA

Logical File Name	File Type	Original File Name	Restore As
EnvTestsLab_1...	Rows Data	C:\Program Files\Microsoft SQL ...	C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS2019\MSSQL\DAT
EnvTestsLab_1...	Log	C:\Program Files\Microsoft SQL ...	C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS2019\MSSQL\DAT

Step 68

- The import is in progress.
- Click **OK** when done
- Repeat step 64 to 68.



Restore Database - Starter_1500_004_tst_6243_SystemDb

Restoring: 100% Stop

Device: C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS2019\MSSQL\Back

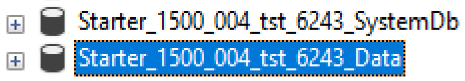
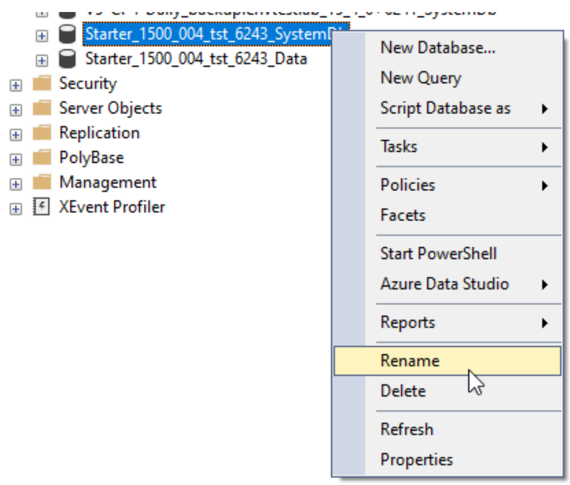
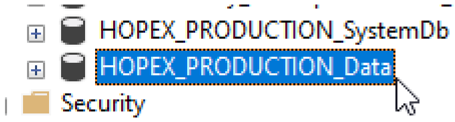
Database: Starter_1500_004_tst_6243_SystemDb

Destination Database: Starter_1500_004_tst_6243_SystemDb

Restore to: The last backup taken (jeudi 25 août 2022 06:38:36)

Microsoft SQL Server Management Studio

Database 'Starter_1500_004_tst_6243_SystemDb' restored successfully.

Step 69
You should now find 2 databases • Rename to your need while keeping naming convention E.g.: replace "Starter***" by "HOPEX_PRODUCTION" _SystemDB cannot be changed. _Data can be changed by "_***" where *** is your new name  Starter_1500_004_tst_6243_SystemDb Starter_1500_004_tst_6243_Data  Starter_1500_004_tst_6243_SystemD Starter_1500_004_tst_6243_Data Security Server Objects Replication PolyBase Management XEvent Profiler New Database... New Query Script Database as Tasks Policies Facets Start PowerShell Azure Data Studio Reports Rename Delete Refresh Properties  HOPEX_PRODUCTION_SystemDb HOPEX_PRODUCTION_Data Security

Go to 3.9.3 Referencing existing environment section.

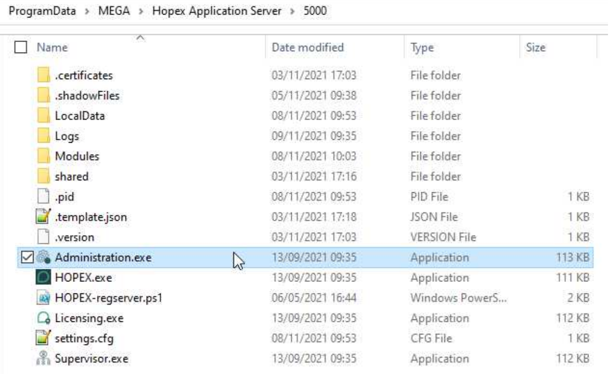
3.9.2.1. Use Customer backup

First you must download the HOPEX Environment Migration Package V5.0 from the store and import it in HAS Console module https://store.mega.com/modules/details/hopex.core.migrate

Perform the same steps with your backup as described in Get MEGA HOPEX Store backup above.

Go to 3.9.3 Referencing existing environment section.

3.9.3. Referencing existing environment

	Step 70
	- Go to HOPEX installation folder Default: C:\ProgramData\MEGA\Hopex Application Server\5000 - Launch Administration.exe If it doesn't launch, you have: - A license issues, - A HAS web access issue.

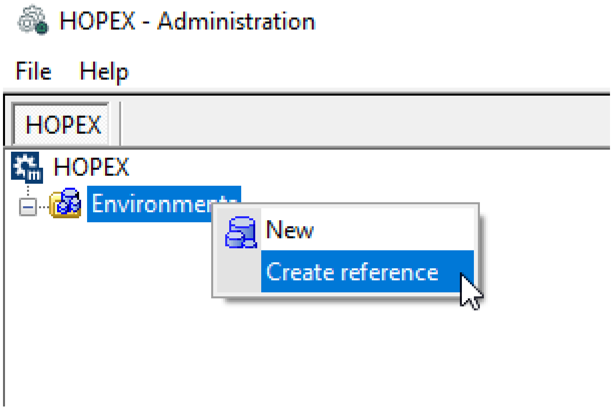
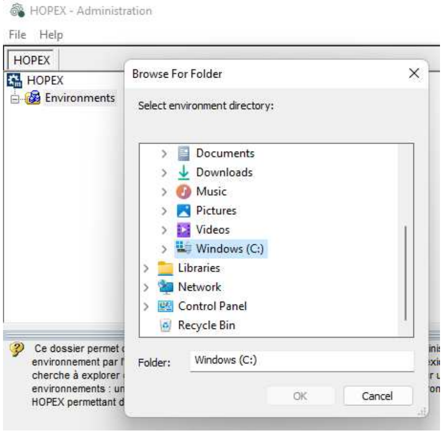
ProgramData › MEGA › Hopex Application Server › 5000

Name	Date modified	Type	Size
.certificates	03/11/2021 17:03	File folder	
.shadowFiles	05/11/2021 09:38	File folder	
LocalData	08/11/2021 09:53	File folder	
Logs	09/11/2021 09:35	File folder	
Modules	08/11/2021 10:03	File folder	
shared	03/11/2021 17:16	File folder	
.pid	08/11/2021 09:53	PID File	1 KB
.template.json	03/11/2021 17:18	JSON File	1 KB
.version	03/11/2021 17:03	VERSION File	1 KB
☑ Administration.exe	13/09/2021 09:35	Application	113 KB
HOPEX.exe	13/09/2021 09:35	Application	111 KB
HOPEX-regserver.ps1	06/05/2021 16:44	Windows PowerS...	2 KB
Licensing.exe	13/09/2021 09:35	Application	112 KB
settings.cfg	08/11/2021 09:53	CFG File	1 KB
Supervisor.exe	13/09/2021 09:35	Application	112 KB

If you are coming from 3.9.2 Restoring an existing database you most likely need to go to Step 73 in chapter "3.9.3.2 From restore step"

3.9.3.1. From existing folder

Follow this step if you have already a folder of environment and a database in SQL. You are in this situation if you are **migrating from previous version**. Otherwise go to the next chapter 3.9.3.2 From restore step

Step 71	Step 72
- Right-click **Environments** and select **Create Reference**	- Select the folder that contains your environment. Once you have selected a valid folder, the **OK** button is enabled
	

Folder: Windows (C:)

Ce dossier permet d
environnement par l
cherche à explorer
environnements : ur
HOPEX permettant d

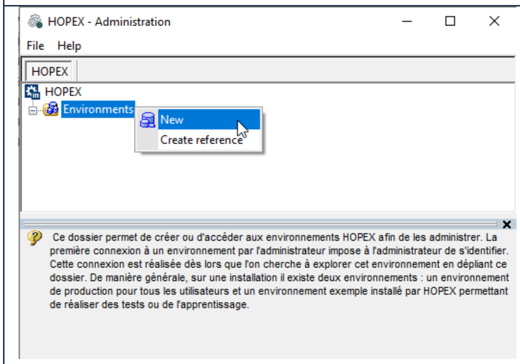
If you succeeded this step, you can now continue to 3.10 Configuring the non-interactive desktop heap

3.9.3.2. From restore step

Perform Step 70 then continue to Step 73

Step 73

- Right-click **Environments** and select **New**



HOPEX - Administration

Ce dossier permet de créer ou d'accéder aux environnements HOPEX afin de les administrer. La première connexion à un environnement par l'administrateur impose à l'administrateur de s'identifier. Cette connexion est réalisée dès lors que l'on cherche à explorer cet environnement en dépliant ce dossier. De manière générale, sur une installation il existe deux environnements : un environnement de production pour tous les utilisateurs et un environnement exemple installé par HOPEX permettant de réaliser des tests ou de l'apprentissage.

Step 74

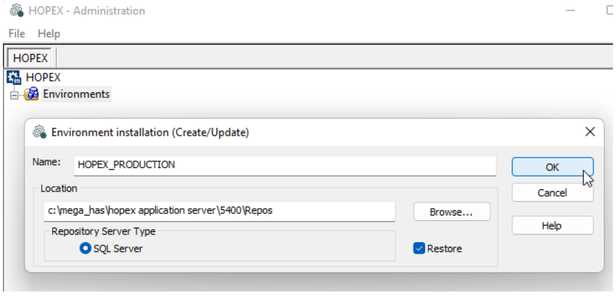
- Enter the name of your environment, the one you chose on "Step 69".

For Example, "HOPEX_PRODUCTION"

- Adjust location of the folder. A set of files will be created. In case of Cluster/Farms deployment the Location should be a shared folder

Example: \\Environments\SharedEnvFolder

- Check **Restore**
- Click **OK**



HOPEX - Administration

Environment installation (Create/Update)

Name: HOPEX_PRODUCTION

Location: c:\mega_has\hopex application server\5400\Repos

Repository Server Type: ● SQL Server

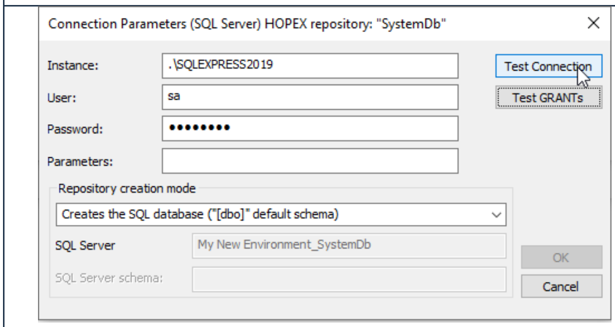
☑ Restore

Step 75

- Enter SQL instance parameter
- Set the SQL user password
- Set the password for the SQL password
- Set the parameter Encrypt=no; or "yes" if you use SSL communication.

For other SQL instance connection string please read the appropriate database setting documentation.

Use Trusted Connection if you rely on domain user to authenticate to SQL Server.



Connection Parameters (SQL Server) HOPEX repository: "SystemDb"

Instance: .\SQLEXPRESS2019

User: sa

Password: ••••••••

Parameters:

Repository creation mode: Creates the SQL database ("[dbo]" default schema)

SQL Server: My New Environment_SystemDb

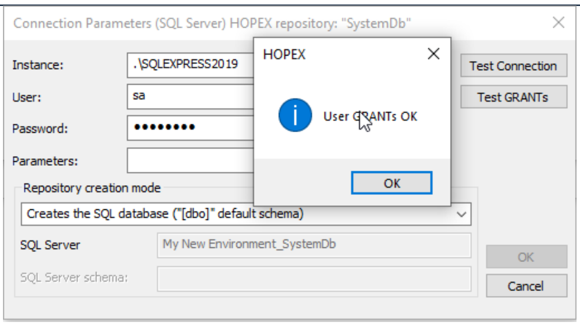
SQL Server schema:

Step 76

- Click **Test Connection**
- Ensure the message says "Successful" else adjust the configuration in previous step
- Click **Test GRANTs**

Ensure the message says "User GRANTs OK" else adjust the configuration in previous step

- Click **OK**



Connection Parameters (SQL Server) HOPEX repository: "SystemDb"

Instance: .\SQLEXPRESS2019

User: sa

Password: ••••••••

Parameters:

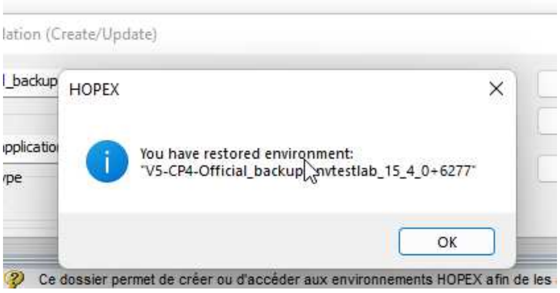
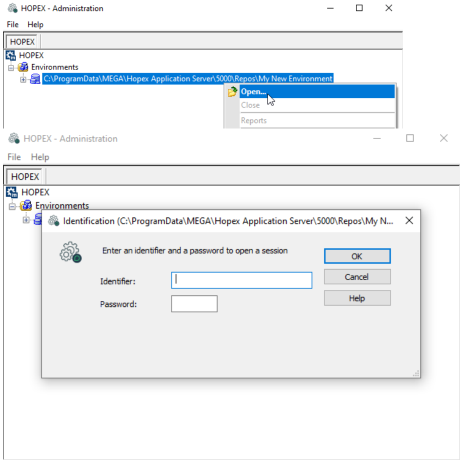
Repository creation mode: Creates the SQL database ("[dbo]" default schema)

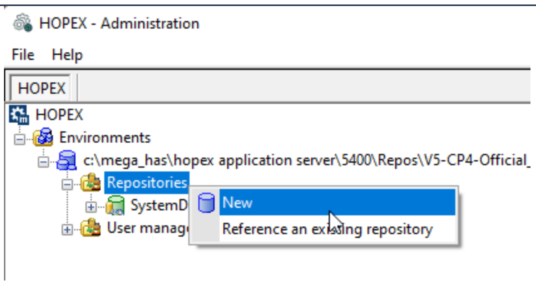
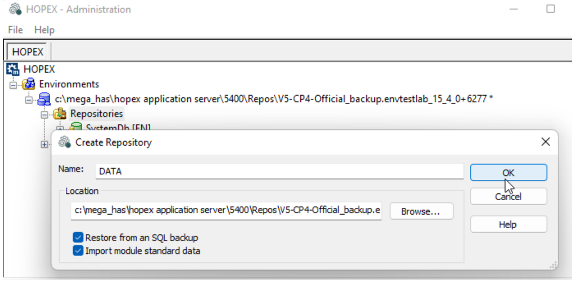
SQL Server: My New Environment_SystemDb

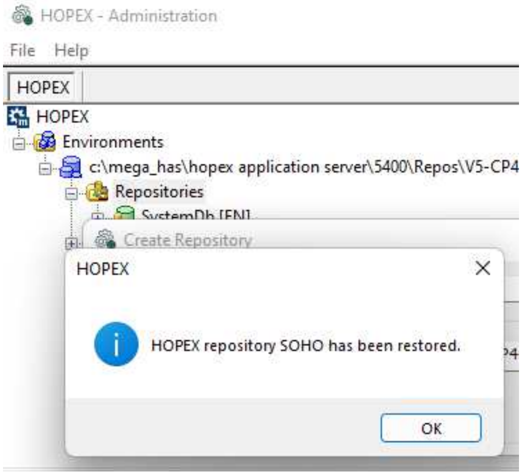
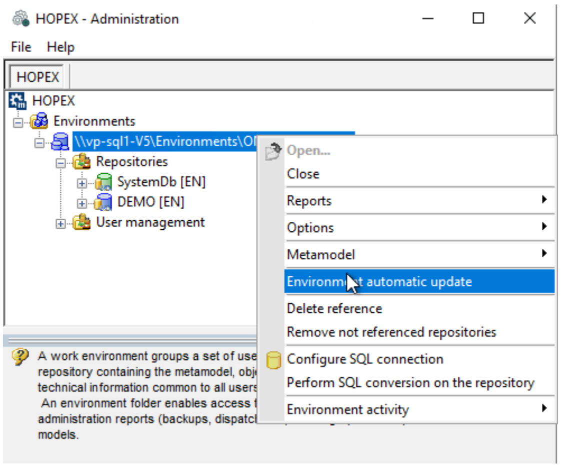
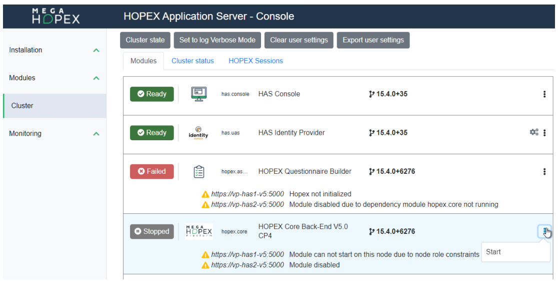
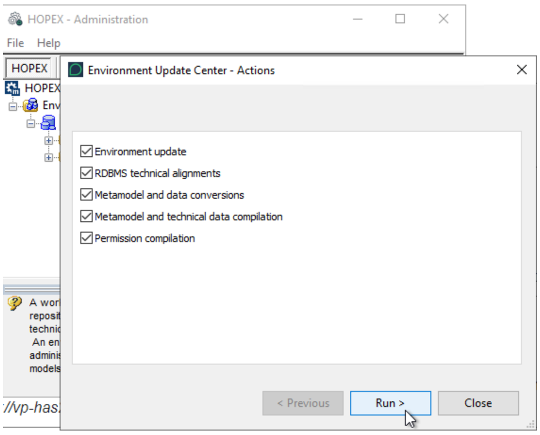
SQL Server schema:

HOPEX

User GRANTs OK

Step 77	Step 78
- When successful you get a message. - Click **OK**	- Once the environment is restored, right-click the environment and select **Open** - Default Identifier: "System" with the appropriate password (default is **Hopex**) - Click **OK**
 HOPEX You have restored environment: "V5-CP4-Official_backup.envtestlab_15_4_0+6277" Ce dossier permet de créer ou d'accéder aux environnements HOPEX afin de les	 C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\My New Environment Identification (C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\My N... Enter an identifier and a password to open a session Identifier: Password:

Step 79	Step 80
- Expand **Environments** - Right-click **Repositories**, and select **New**	- Select **Restore from an SQL Setup** - Enter a **Name** for the repository
 c:\mega_has\hopex application server\5400\Repos\V5-CP4-Official_	 c:\mega_has\hopex application server\5400\Repos\V5-CP4-Official_backup.envtestlab_15_4_0+6277 * Create Repository Name: DATA Location c:\mega_has\hopex application server\5400\Repos\V5-CP4-Official_backup.e ☑ Restore from an SQL backup ☑ Import module standard data

Step 81	Step 82
- Repeat Step 75 and 76 - Click **OK** when successful.	- Once the repository is restored, right-click the environment and select **Environment automatic update** You may need to stop the module **HOPEX Core Back-End** from **HAS Console** and restart **Administration.exe** - Follow the step of the wizard by clicking Next up to **Run**. For **PRODUCTION** environment: - Check “Permission compilation”
 HOPEX - Administration File Help HOPEX HOPEX Environments c:\mega_has\hopex application server\5400\Repos\V5-CP4 Repositories SystemDb [EN] Create Repository HOPEX OK HOPEX repository SOHO has been restored.	 HOPEX - Administration File Help HOPEX HOPEX Environments \\vp-sql1-V5\Environments\O Repositories SystemDb [EN] DEMO [EN] User management Open... Close Reports Options Metamodel Environment automatic update Delete reference Remove not referenced repositories Configure SQL connection Perform SQL conversion on the repository Environment activity A work environment groups a set of use repository containing the metamodel, obj technical information common to all users An environment folder enables access t administration reports (backups, dispatc models.  HOPEX HOPEX Application Server - Console Cluster state Set to log Verbose Mode Clear user settings Export user settings Installation Modules Cluster Monitoring Modules Cluster status HOPEX Sessions Start Ready has.console HAS Console 15.4.0+35 Ready has.uas HAS Identity Provider 15.4.0+35 Failed hopex.as... HOPEX Questionnaire Builder 15.4.0+6276 https://vp-has1-v5:5000 Hopex not initialized https://vp-has2-v5:5000 Module disabled due to dependency module hopex.core not running Stopped hopex.core HOPEX Core Back-End V5.0 CP4 15.4.0+6276 https://vp-has1-v5:5000 Module can not start on this node due to node role constraints https://vp-has2-v5:5000 Module disabled  HOPEX - Administration File Help HOPEX HOPEX Environment Update Center - Actions < Previous Run > Close //vp-has ☑ Environment update ☑ RDBMS technical alignments ☑ Metamodel and data conversions ☑ Metamodel and technical data compilation ☑ Permission compilation

3.10. Configuring the non-interactive desktop heap

The Desktop Heap is an internal memory of Windows. It is used by HOPEX. It is thus mandatory to update this value.

➔ For more information about desktop heap, see official Microsoft documentation: https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/desktop-heap-limitation-out-of-memory.

A minimum value of **8192** is required for optimal usage. This modification is performed in the Windows Registry.

To configure the non-interactive desktop heap:

1. Open Windows registry: "regedit.exe".

2. Search for value name in:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems.

3. Edit the value data: there is a long string for this value that looks similar to:

   %SystemRoot%system32csrss.exe ObjectDirectory=Windows SharedSection=1024,20480,**8192** Windows

   In the **Shared Section** part, the three values are, in order:

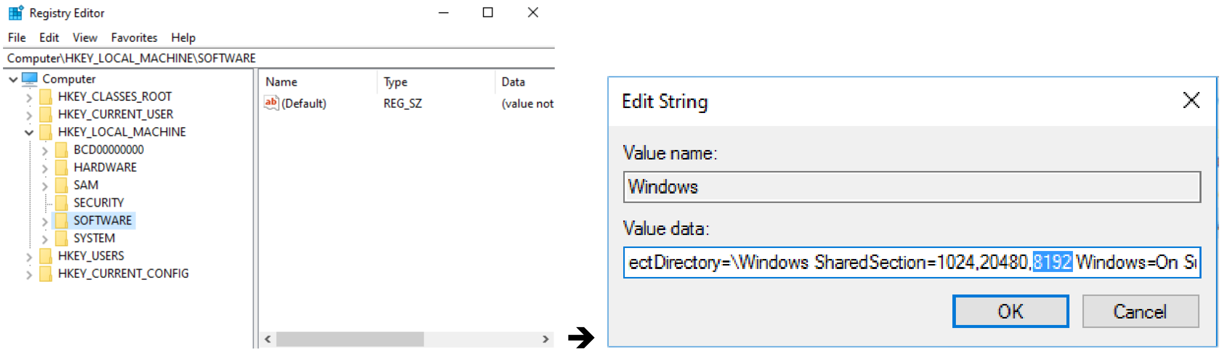
   - the shared heap,
   - the interactive desktop heap, and
   - the non-interactive desktop heap.

   They are expressed in KB. Default values vary significantly between Windows versions.

4. You might need to modify **the non-interactive desktop heap**.

Be careful of not using excessive values, as this could stop you from logging into your server.

It is therefore recommended to change this value using small increments. The recommended value is: **8192**.



Value name: Windows

Value data: ectDirectory=\Windows SharedSection=1024,20480,8192 Windows=On S

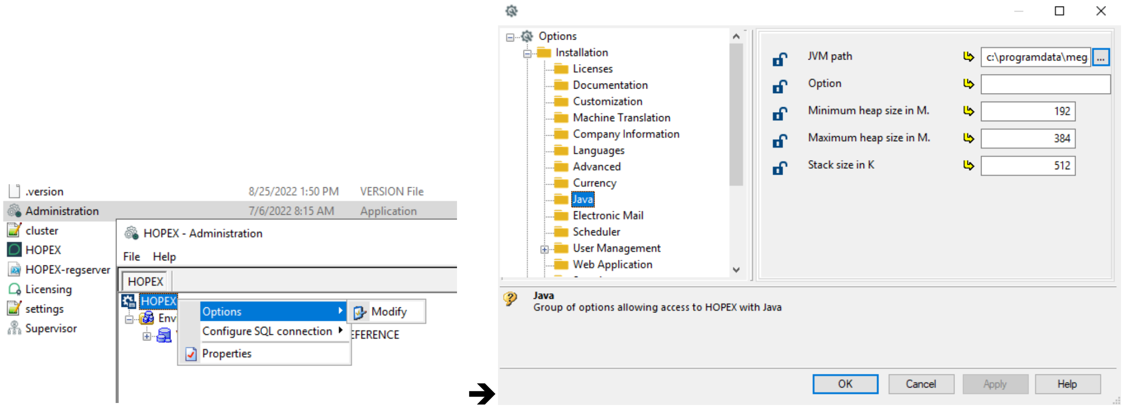
3.11. Configuring Java Heap size (optional)

HOPEX Platform embeds an internal JVM. When running HOPEX some reports might generate huge consumption of JAVA object and therefore consume a lot of memory.

Change this option only if you have hit the limit of memory consumption of JAVA.

1. Launch Administration.exe
2. At the root level, right-click **HOPEX**, and select **Options > Modify**.
3. Select **Installation > Java**.
4. Edit **Maximum heap size** or **Stack size**.

   Recommendation increase by a factor 2: 192, 384, 768… or 512, 1024…



JVM path: c:\programdata\meg

Option:

Minimum heap size in M.: 192

Maximum heap size in M.: 384

Stack size in K: 512

Java
Group of options allowing access to HOPEX with Java

3.12. Windows User and access rights

You can skip this step if you are a developer, consultant or partner doing a standalone.

When installing MEGA HOPEX, a **domain user** is required to manage access to:

- Must license file and folder
- Shared environment UNC

It is recommended not to execute the HAS Instance manager with the default **Local System** account. You will therefore need a domain user with sufficient privilege.

Please note that a **domain user is required for cluster** deployment.

The minimum required privilege of this domain user:

- Read/Write access on the shared folder of the Must license
- Read/Write access on the shared folder of the HOPEX environment folder
- Execute/Read/Write access on all the installation folders

Additional requirements:

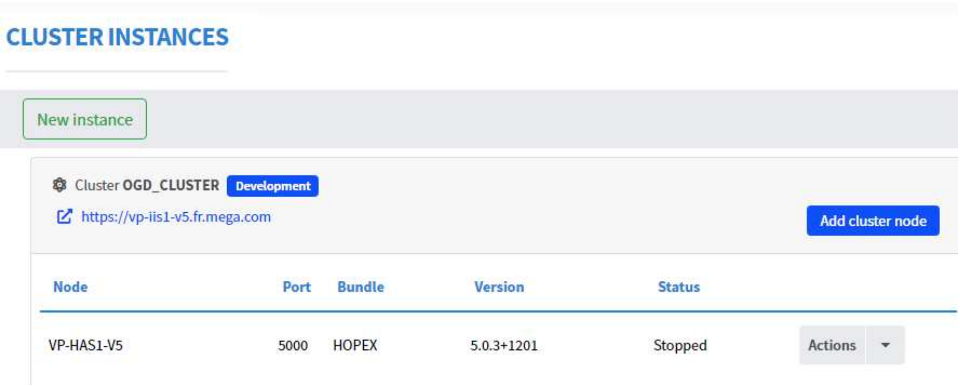
- This domain user can be used to access the database in case you use the connection trusted configuration for SQL Server. It should be properly configured in SQL Server.
- This domain user must have reading access rights on: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
- You should enable Read/Write in the certificate store to import HAS self-signed certificate. If you don't allow it a complementary step to import manually the **root.pfx** located in C:\...\HOPEX Application Server\...\.certificates

Ideally this domain user is Administrator of the server.

3.12.1. Changing the user domain

To change the user please ensure to:

- Stop running instance



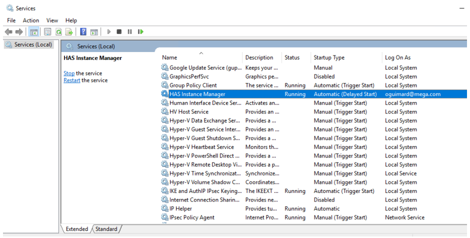
CLUSTER INSTANCES

Cluster OGD_CLUSTER Development
https://vp-iis1-v5.fr.mega.com

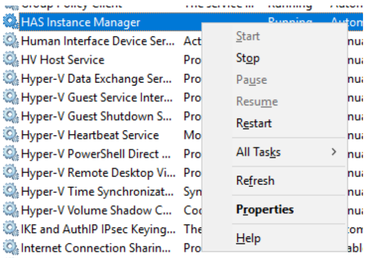
Node	Port	Bundle	Version	Status	
VP-HAS1-V5	5000	HOPEX	5.0.3+1201	Stopped	Actions

- Stop HAS Instance

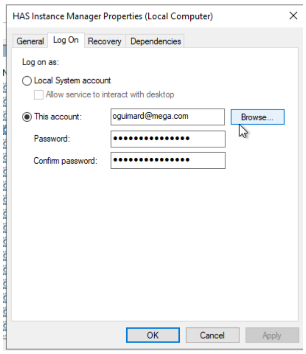
1. Go to windows Services.exe
2. Right-click **HAS Instance Manager** and select **Properties**.
3. Click **Log on** tab.
4. Select **This account** and click **Browse.**
5. Enter the domain user and password.



➔


HAS Instance Manager
Human Interface Device Ser...
HV Host Service
Hyper-V Data Exchange Ser...
Hyper-V Guest Service Inter...
Hyper-V Guest Shutdown S...
Hyper-V Heartbeat Service
Hyper-V PowerShell Direct ...
Hyper-V Remote Desktop Vi...
Hyper-V Time Synchronizat...
Hyper-V Volume Shadow C...
IKE and AuthIP IPsec Keying...
Internet Connection Sharin...
Start
Stop
Pause
Resume
Restart
All Tasks
Refresh
Properties
Help

➔


HAS Instance Manager Properties (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

○ Local System account

☐ Allow service to interact with desktop

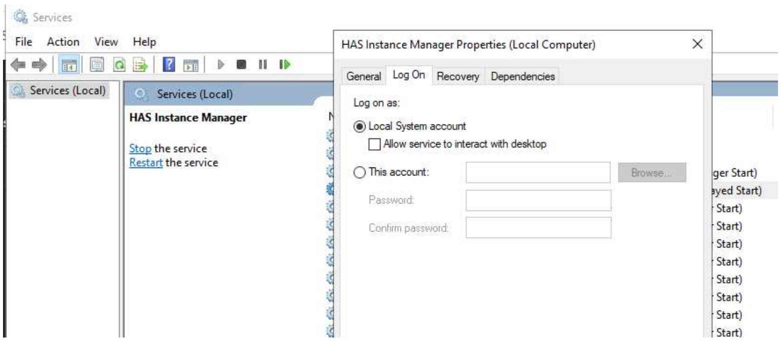
● This account: oguimard@mega.com

Password: •••••••••••••••

Confirm password: •••••••••••••••

3.12.2. Keeping Local system

What is the impact of keeping local system?


HAS Instance Manager Properties (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

● Local System account

☐ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

In that case:

- The Must license shared folder must be shared to “Everyone” with full control
- The environment folder should be on C:\ drive or shared with “Everyone”
- You cannot configure “Trusted Connection” with SQL server
- You cannot **run in cluster**

3.13. Installing a DEV server

When installing a server for “Development” purposes it is mandatory to:

- install .NET 8 SDK
- download “**HOPEX Application Server Customization**” module and import it in HAS Instance
- install HAS nuget package on the server as explained in the module custom. Please README.MD and HOW-TO.MD file the custom module
- ensure you have the right to execute powershell script:

  Set-ExecutionPolicy -ExecutionPolicy RemoteSigne

4. SSL Certificates configuration

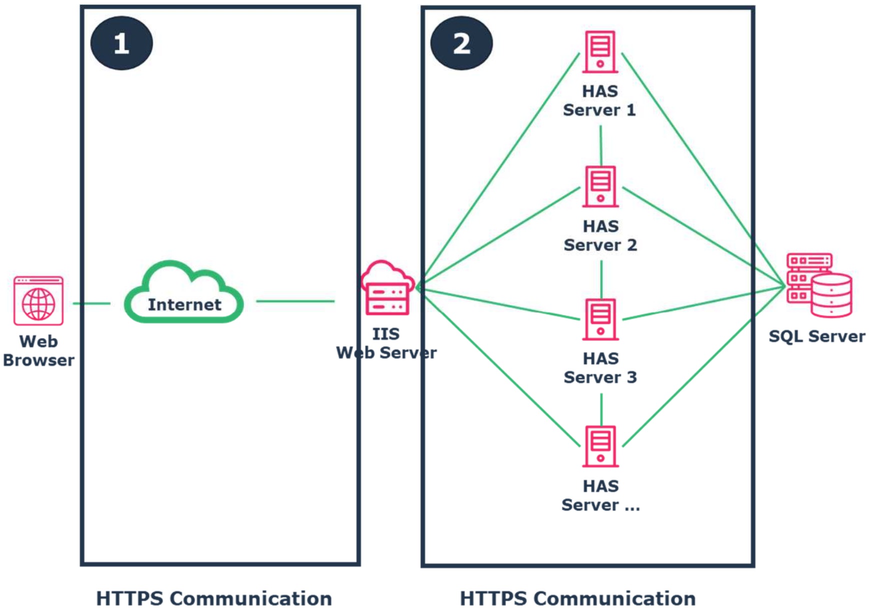
Read carefully this chapter if:

- you have chosen a secured deployment with HTTPS protocol.
- you have more than 1 server

There are 2 layers of communication for HTTPS:

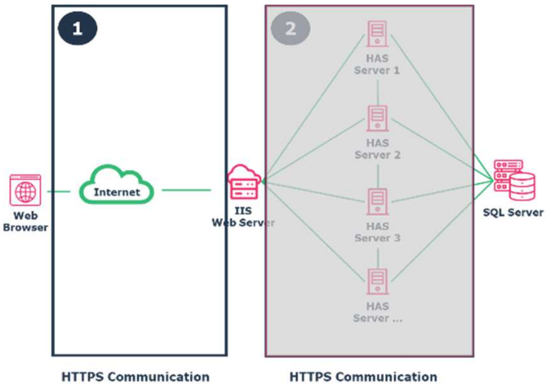
1: HTTPS Communication between the web browser and IIS Web Server

2: HTTPS Communication between the IIS web Server to HOPEX Application server and between HAS Server themselves.



Each layer/path has its own SSL Certificate.

4.1. Configuring public SSL Certificate (1)



This certificate is **generated by the customer**. Ensure that the generated certificate has:

- a Certificate Authorities and a Certificate Chains that are valid with Trusted Authorities.
- a Certification path that corresponds to the chosen DNS
- a set of Subject Alternative Name that corresponds to the chosen DNS.

To have a valid deployment you must import this SSL Certificate in all servers (IIS+HAS).

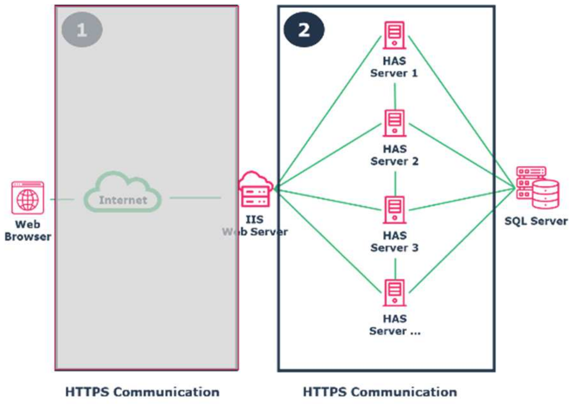
Perform the following task:

- Generate your own SSL signed certificate.
- For **each server (IIS+HAS),** repeat the step “4.3 Adding certificate on the server” where you had this certificate.

4.2. Configuring HAS Cluster node SSL Certificate (2)

This certificate is **generated by HAS at first launch by the first server**.

- This is a self-signed certificate with a 30-year validity
- This certificate is named **root.pfx** and is available on the first HAS Server of the farm
- This root certificate is used to generate a **node.pfx** certificate for each HAS node. This node.pfx is generated automatically.



To have a valid deployment you must import this **root.pfx** SSL Certificate in all servers (IIS+HAS). This certificate has no password.

Perform the following tasks:

1. Access the first HAS server installed.
2. Go to C:\...\HOPEX Application Server\<<port>>\.certificates folder.
3. Search for **root.pfx** file.
4. Copy and keep this file.
5. For **each server (IIS+HAS)**, repeat the step “4.3 Adding certificate on the server” using the **root.pfx** certificate you copied.
6. If prompted for a password, leave it blank, as this certificate has no password.

4.3. Adding certificate on the server

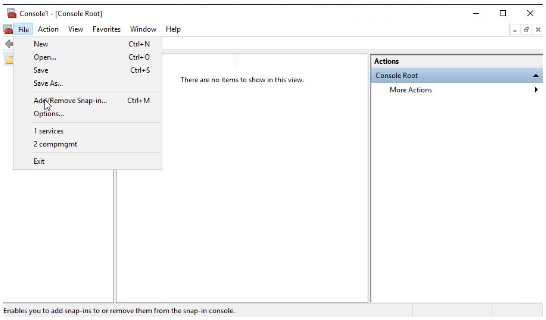
Follow the instruction provided by Microsoft to install the certificate in the local computer store:

https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/install-imported-certificates

1. In the search box, type mmc, and then click **OK**.
2. On the **File** menu, select **Add/Remove snap-in**.
3. In the Add/Remove Snap-in dialog box, select **Add**.
4. In the Add Standalone Snap-in dialog box, select **Certificates**, and then select **Add**.
5. In the Certificates snap-in dialog box, select **Computer account**, and then select **Next**.

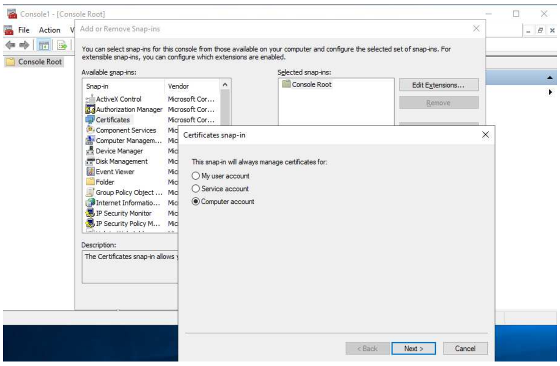
6. In the Select Computer dialog box, select **Local computer**: (the computer this console is running on), and then click **Finish**.
7. In the Add Standalone Snap-in dialog box, click **Close**.
8. In the Add/Remove Snap-in dialog box, click **OK**.
9. In the left pane of the console, double-click **Certificates** (Local Computer).
10. Right-click **Trusted Root Certification Authorities**, point to All Tasks, and then select **Import**.
11. On the Welcome to the Certificate Import Wizard page, click **Next**.
12. On the File to Import page, click **Browse**, locate your certificate file, and then click **Next**.
13. If the certificate has a password, enter the password on the Password page, and then click **Next**.
14. On the Certificate Store page, select Place all certificates in the following store, and then click **Next**.
15. Click **Finish**, and then click **OK** to confirm that the import was successful.

Some Screenshots of the process:



There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.



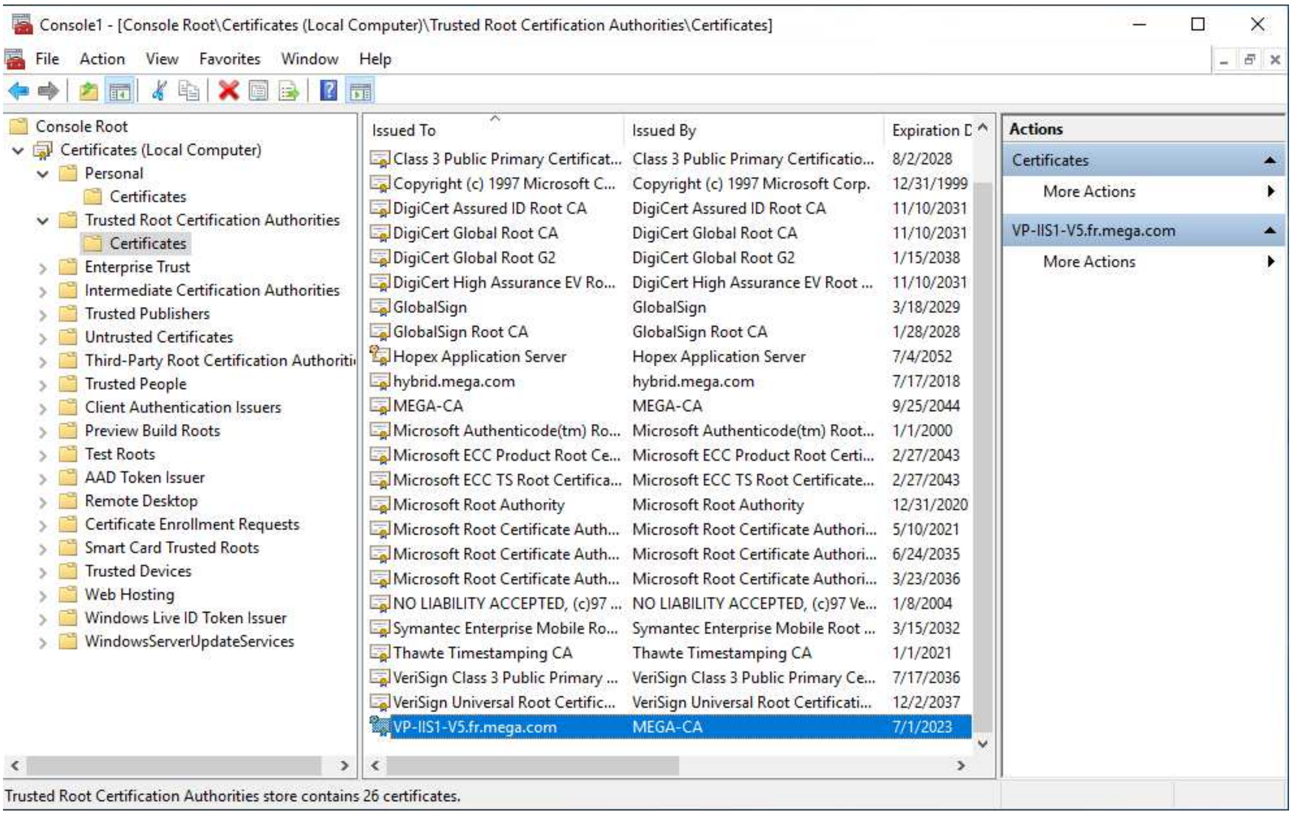
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

The Certificates snap-in allows

This snap-in will always manage certificates for:

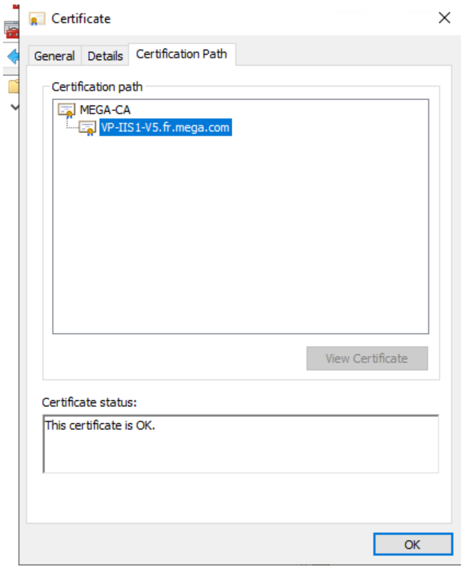
○ My user account
○ Service account
● Computer account

In this example the public certificate is named “VP-IIS1-V5.fr.mega.com”.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
AAD Token Issuer
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
WindowsServerUpdateServices
Actions
Certificates
More Actions
VP-IIS1-V5.fr.mega.com
More Actions

Issued To	Issued By	Expiration D
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/10/2031
GlobalSign	GlobalSign	3/18/2029
GlobalSign Root CA	GlobalSign Root CA	1/28/2028
Hopex Application Server	Hopex Application Server	7/4/2052
hybrid.mega.com	hybrid.mega.com	7/17/2018
MEGA-CA	MEGA-CA	9/25/2044
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1/1/2000
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate...	2/27/2043
Microsoft Root Authority	Microsoft Root Authority	12/31/2020
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/10/2021
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/24/2035
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/23/2036
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/8/2004
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/15/2032
Thawte Timestamping CA	Thawte Timestamping CA	1/1/2021
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/17/2036
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	12/2/2037
VP-IIS1-V5.fr.mega.com	MEGA-CA	7/1/2023

Trusted Root Certification Authorities store contains 26 certificates.



This certificate is OK.

If the certificate is not signed by a trusted authority, ensure that this certificate is present in all servers and laptops that will use the website.

Make sure that the certificate path is also present on all of the servers. Should one certificate path appear with a "red cross" fix it.

4.4. Creating and using a custom cluster SSL certificate

This SSL certificate is only for the communication between cluster nodes. This is not the public SSL certificate.

This is an optional step to perform **only if requested by your security team because self-signed certificate is not allowed.**

4.4.1. Creating a custom SSL certificate

Caution: this sub-chapter does not intent to present best practices in term of security to create an SSL certificate but only to show an example that works with required elements.

To create a valid root.pfx certificate you must comply with the following constraints:

- The certificate must be trusted and belong to a hierarchy of trusted certificate. Ideally owned by the customer.
- The certificate must embed its private key.
- The certificate must be CA Authority

1. Create a file called ca.cfg that will contain the required characteristic of your SSL certificate.

Adjust settings based on your company constrains.

ca.cfg file content
[req]
default_bits = 4096
default_keyfile = db.key
distinguished_name = req_distinguished_name
req_extensions = v3_ca
extensions = v3_ca
prompt = no
[req_distinguished_name]
C = FR
ST = Paris
L = Paris
O = mega.com
OU = mega.com
CN= localhost
emailAddress = contact@mega.com
[v3_ca]
basicConstraints = CA:TRUE

2. Create the certificate with these elements. Here is a sample script using openssl to create the certificate.

> *Create the certficate private key ans save it in the file rootCA.key*

```
openssl genrsa -out rootCA.key 4096
```

> *Create a crt file*

```
openssl req -x509 -new -nodes -key rootCA.key -days 1024 -config ca.cfg -extensions v3_ca -out rootCA.crt
```

> *Create an PFX file to be imported in all server of the cluster (HAS+IIS)*

```
openssl pkcs12 -export -out root.pfx -inkey rootCA.key -in rootCA.crt
```

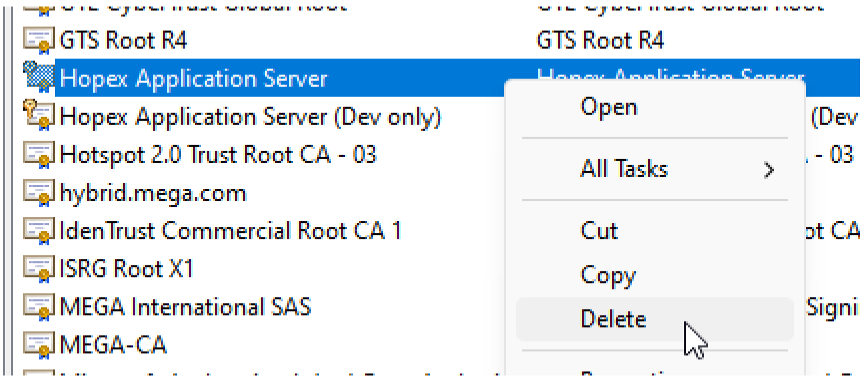
4.4.2. Use the custom cluster certificate.

To use the newly created certificate:

1. Clean existing self-signed root.pfx/node.pfx certificate. You may skip this step if you have never installed in HTTPS the cluster.
   - From the HAS Instance Manager stop all cluster instances/nodes.
   - For each **IIS** server and **HAS server** of the cluster:

a) Delete file **node.pfx** and **root.pfx** located in the default location here: C:\...\HOPEX Application Server\...\.certificates

b) From MMC console under **Certificates>Trusted Root Certification Authorities** delete the existing certificate called "HOPEX Application Server" and/or "HOPEX Application Server (Dev Only)



2. Import your new certificate.

For each **IIS** server and **HAS server** of the cluster:

a) Access **Certificates > Trusted Root Certification Authorities > Certificates** menu, right-click and select **All tasks > Import.** Make sure you import with a user that will give enough privilege to the certificate to be read by HAS later.

b) Click **Next**.

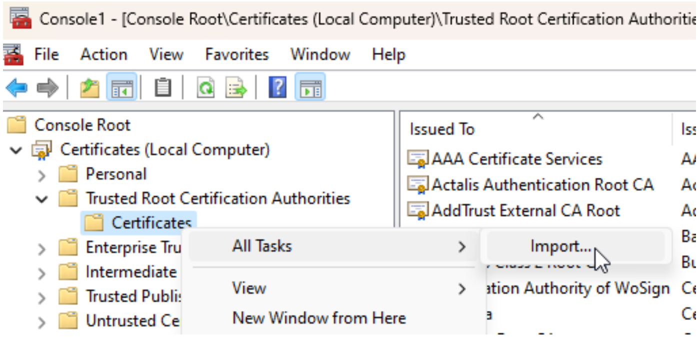
c) Browse and select the PFX file you just created.

d) Click **Next**.

e) When prompted enter the password for the private key if you have set one (in this example there is no password).

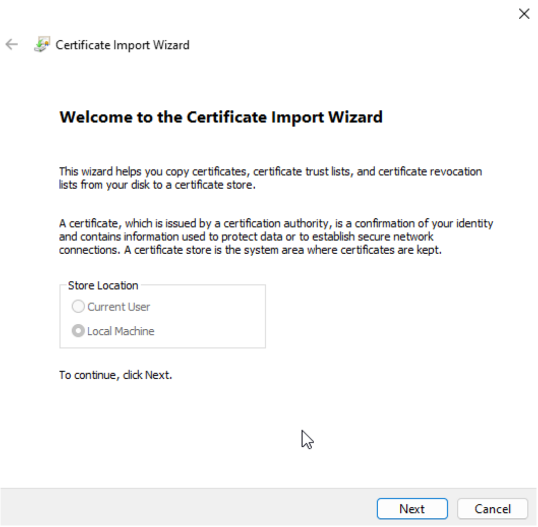
f) (optional) You may want to select "Mark this key as exportable. This will allow you to back up or transport your keys at a later stage" for future use if you lose the original file.

g) When prompted make sure to place this certificate in "Trusted Root Certification Authorities".



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authoritie

File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Tru
Intermediate
Trusted Publi
Untrusted Ce
Issued To
AAA Certificate Services
Actalis Authentication Root CA
AddTrust External CA Root
ation Authority of WoSign
All Tasks
Import...
View
New Window from Here



Certificate Import Wizard

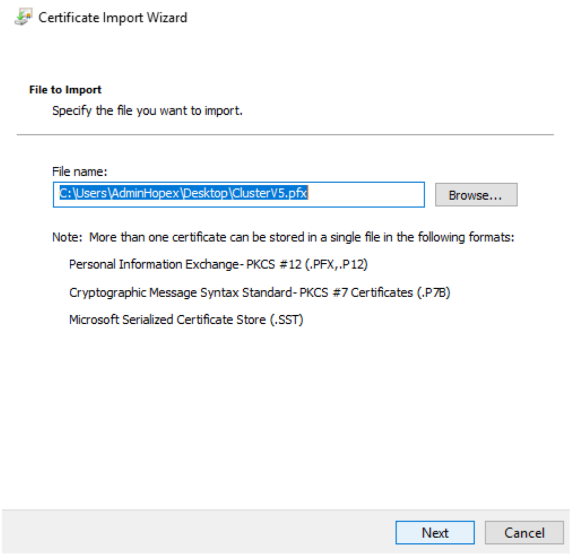
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.



Certificate Import Wizard

File to Import
Specify the file you want to import.

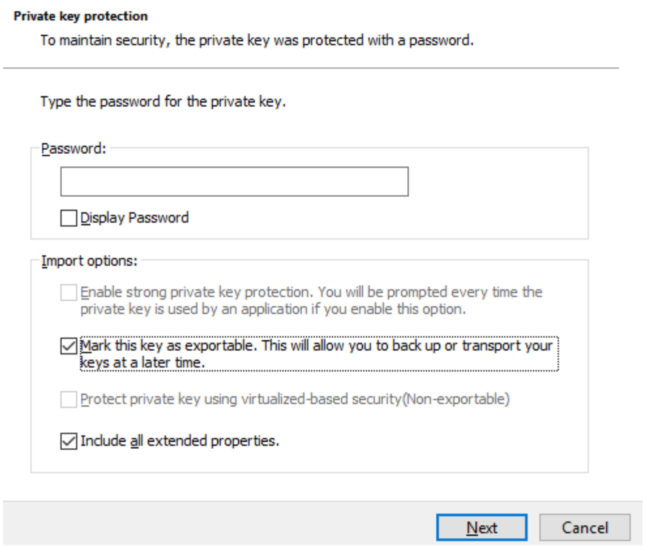
File name:
C:\Users\AdminHopex\Desktop\ClusterV5.pfx

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)



Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

□ Display Password

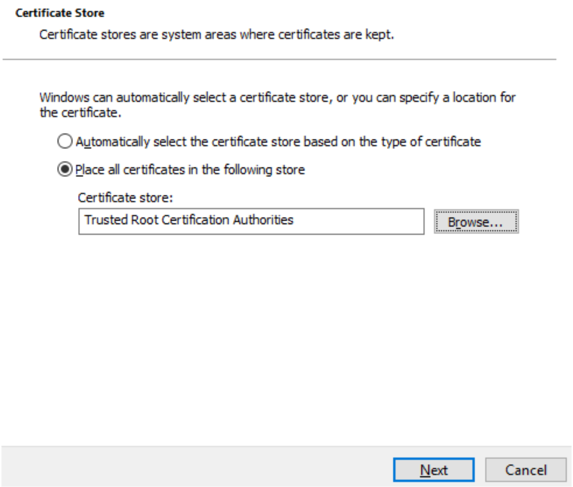
Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.



Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

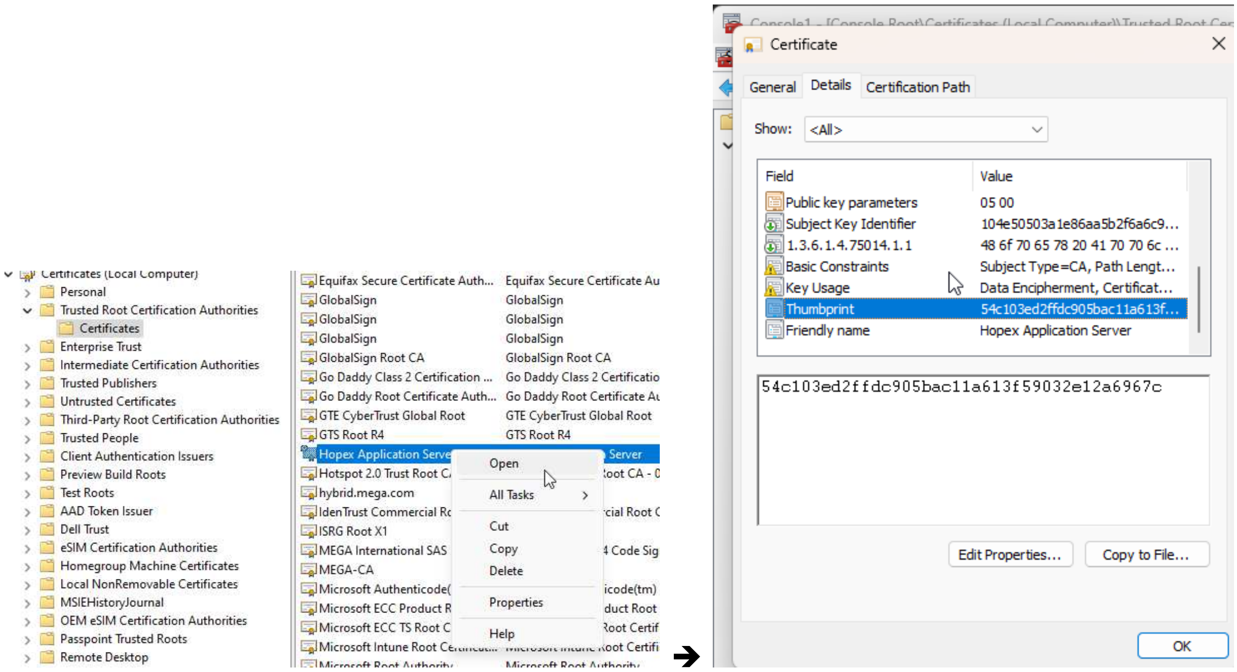
3. Get the thumbprint of your certificate.

a) From the MMC Console, search for your certificate.

b) Right-click the certificate and select Open.

c) In the **Details** tab, scroll down to **Thumbprint**.

d) Copy and save its **Value** for later use.


Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
AAD Token Issuer
Dell Trust
eSIM Certification Authorities
Homegroup Machine Certificates
Local NonRemovable Certificates
MSIEHistoryJournal
OEM eSIM Certification Authorities
Passpoint Trusted Roots
Remote Desktop
Equifax Secure Certificate Auth...
GlobalSign
GlobalSign Root CA
Go Daddy Class 2 Certification ...
Go Daddy Root Certificate Auth...
GTE CyberTrust Global Root
GTS Root R4
Hopex Application Server
Hotspot 2.0 Trust Root CA
hybrid.mega.com
IdenTrust Commercial Root CA
ISRG Root X1
MEGA International SAS
MEGA-CA
Microsoft Authenticode(tm)
Microsoft ECC Product Root
Microsoft ECC TS Root Certif
Microsoft Intune Root Certificat...
Microsoft Root Authority
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Cer
Certificate
General
Details
Certification Path
Show: <All>
Edit Properties...
Copy to File...
OK

Field	Value
Public key parameters	05 00
Subject Key Identifier	104e50503a1e86aa5b2f6a6c9...
1.3.6.1.4.75014.1.1	48 6f 70 65 78 20 41 70 70 6c ...
Basic Constraints	Subject Type=CA, Path Lengt...
Key Usage	Data Encipherment, Certificat...
Thumbprint	54c103ed2ffdc905bac11a613f...
Friendly name	Hopex Application Server

```
54c103ed2ffdc905bac11a613f59032e12a6967c
```

4. Use the thumbprint within the HAS Instance Manager:

a) Connect to HAS Instance manager.

b) Click the start button of the first node of the cluster.

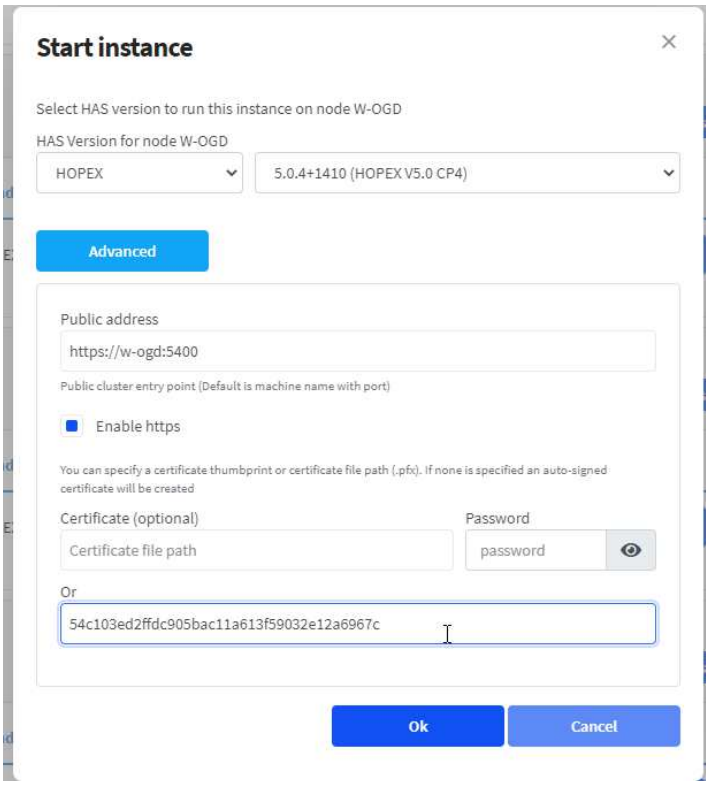
c) Click **Advanced**.

d) Past your thumbprint in the area planned for these purposes. Make sure the certificate file path and password are empty.

e) Click **OK**.

f) Wait for the first node to be fully running. Do not continue if this fails.

g) Repeat the operation on each node of the cluster.



Start instance

Select HAS version to run this instance on node W-OGD

HAS Version for node W-OGD: HOPEX | 5.0.4+1410 (HOPEX V5.0 CP4)

Public address: https://w-ogd:5400

Public cluster entry point (Default is machine name with port)

☑ Enable https

You can specify a certificate thumbprint or certificate file path (.pfx). If none is specified an auto-signed certificate will be created

Certificate (optional): Certificate file path

Password: password

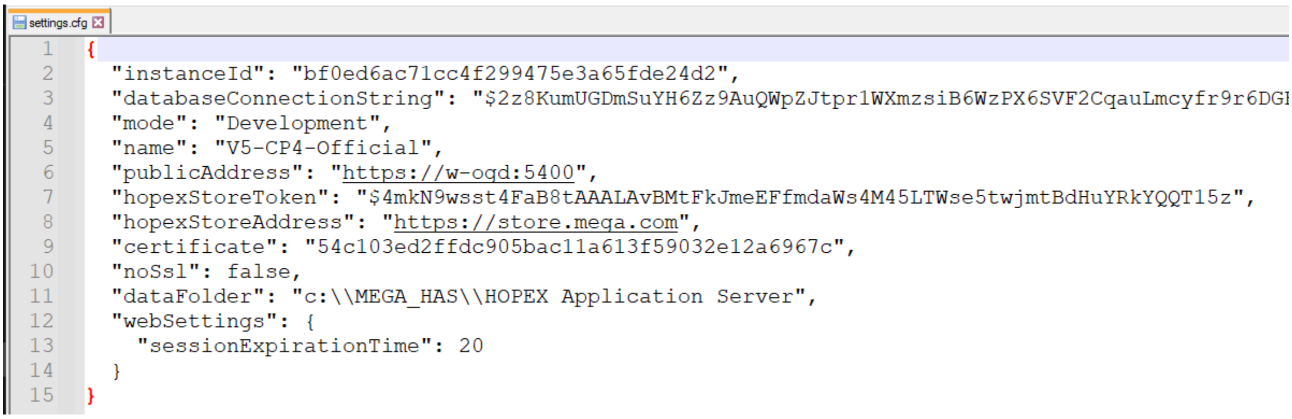
Or

54c103ed2ffdc905bac11a613f59032e12a6967c

5. Check everything is OK:

   a) Ensure all HAS instances are running for each node.

   b) Open the settings.cfg files of each node and ensure you see the certificate thumbprint.



```
{
  "instanceId": "bf0ed6ac71cc4f299475e3a65fde24d2",
  "databaseConnectionString": "$2z8KumUGDmSuYH6Zz9AuQWpZJtpr1WXmzsiB6WzPX6SVF2CqauLmcyfr9r6DGI
  "mode": "Development",
  "name": "V5-CP4-Official",
  "publicAddress": "https://w-ogd:5400",
  "hopexStoreToken": "$4mkN9wsst4FaB8tAAALAvBMtFkJmeEFfmdaWs4M45LTWse5twjmtBdHuYRkYQQT15z",
  "hopexStoreAddress": "https://store.mega.com",
  "certificate": "54c103ed2ffdc905bac11a613f59032e12a6967c",
  "noSsl": false,
  "dataFolder": "c:\\MEGA_HAS\\HOPEX Application Server",
  "webSettings": {
    "sessionExpirationTime": 20
  }
}
```

4.5. Disabling vulnerable cypher suites

In Windows Server 2019, TLS 1.0 and 1.1, which have known vulnerabilities, are activated by default.

It is highly recommended to disable vulnerable protocols by removing Schannel and cipher suite from the Windows registry.

You can use one of the following:

- directly from the **Windows registry**

To remove the Schannel and Cipher directly from the Windows registry, see Windows documentation.

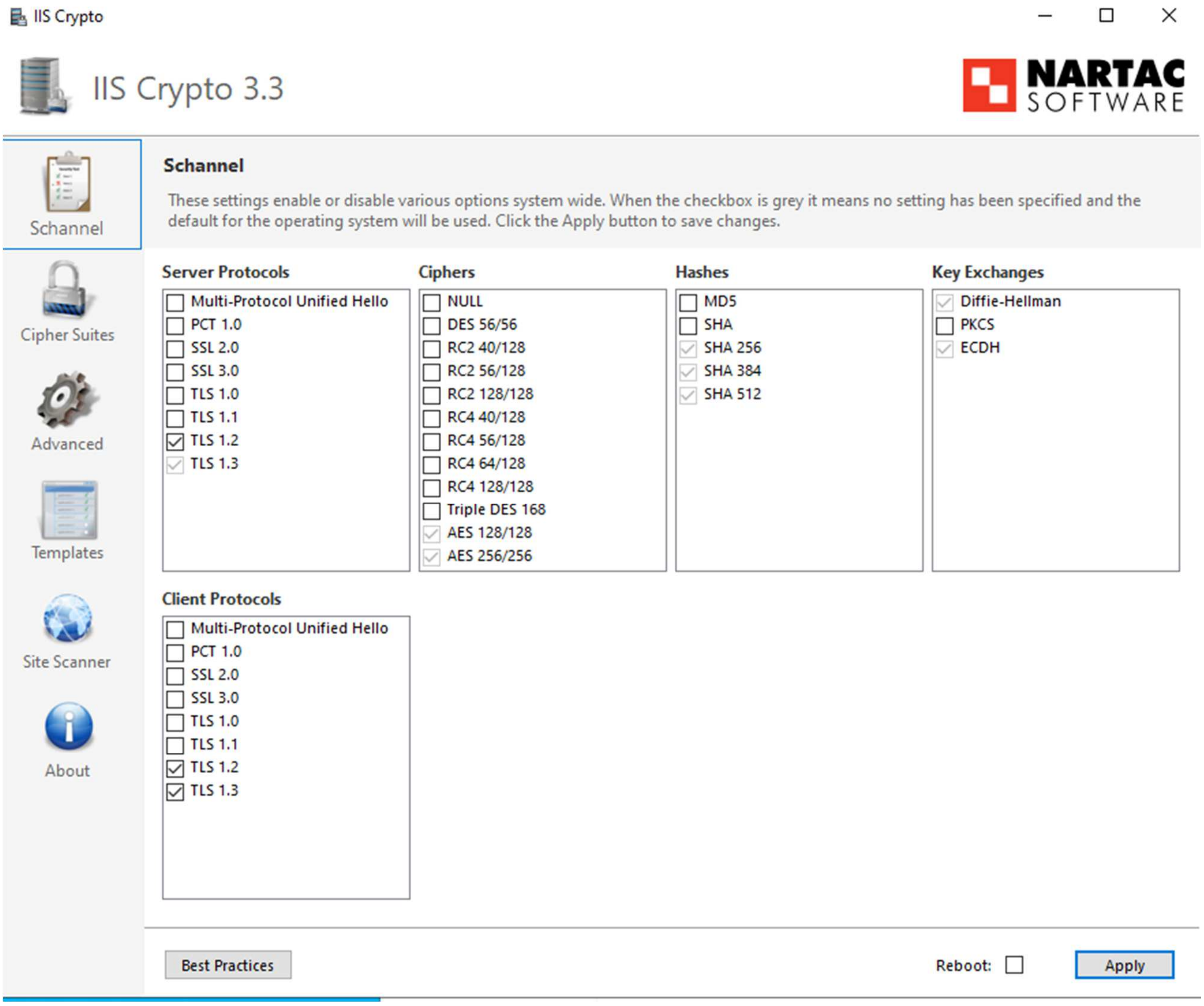
- using **IIS Crypto** (recommended)

  To download IIS Crypton: https://www.nartac.com/Products/IISCrypto/Download.

- using **script**

4.5.1. Disabling vulnerable cypher suites with IIS Crypto

1. Download IIS Crypto: https://www.nartac.com/Products/IISCrypto/Download.
2. Connect to **IIS Crypto**.
3. In **Schannel**, disable the vulnerable algorithms and protocols: TLS below 1.2, PKCS, MD5, SHA, DES, and RC4.



Schannel

These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.

Server Protocols
- ☐ Multi-Protocol Unified Hello
- ☐ PCT 1.0
- ☐ SSL 2.0
- ☐ SSL 3.0
- ☐ TLS 1.0
- ☐ TLS 1.1
- ☑ TLS 1.2
- ☑ TLS 1.3

Ciphers
- ☐ NULL
- ☐ DES 56/56
- ☐ RC2 40/128
- ☐ RC2 56/128
- ☐ RC2 128/128
- ☐ RC4 40/128
- ☐ RC4 56/128
- ☐ RC4 64/128
- ☐ RC4 128/128
- ☐ Triple DES 168
- ☑ AES 128/128
- ☑ AES 256/256

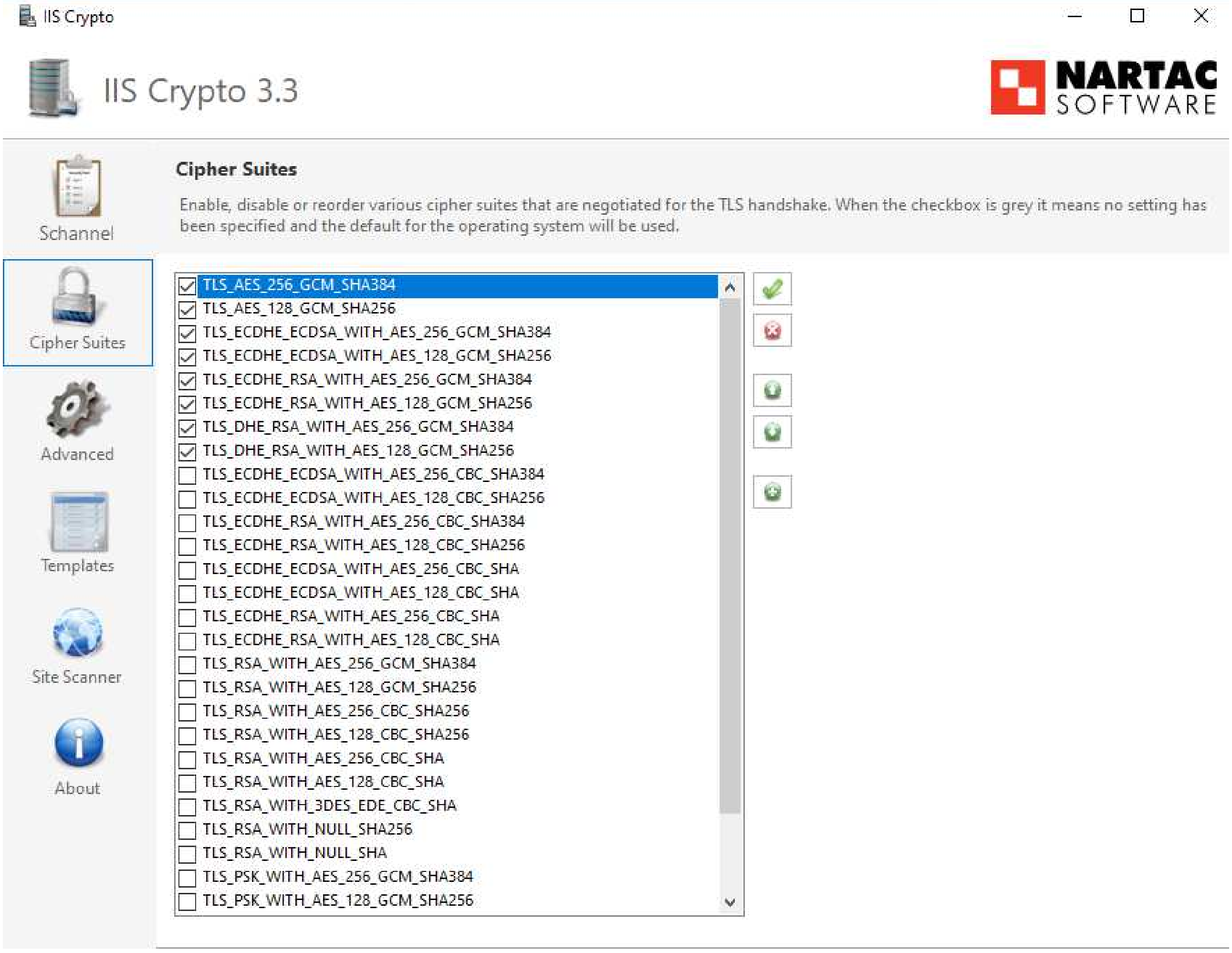
Hashes
- ☐ MD5
- ☐ SHA
- ☑ SHA 256
- ☑ SHA 384
- ☑ SHA 512

Key Exchanges
- ☑ Diffie-Hellman
- ☐ PKCS
- ☑ ECDH

Client Protocols
- ☐ Multi-Protocol Unified Hello
- ☐ PCT 1.0
- ☐ SSL 2.0
- ☐ SSL 3.0
- ☐ TLS 1.0
- ☐ TLS 1.1
- ☑ TLS 1.2
- ☑ TLS 1.3

Reboot: ☐

4. In **Cipher Suites**, disable other weak cipher suites:



Cipher Suites

Enable, disable or reorder various cipher suites that are negotiated for the TLS handshake. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used.

- ☑ TLS_AES_256_GCM_SHA384
- ☑ TLS_AES_128_GCM_SHA256
- ☑ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- ☑ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- ☑ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ☑ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- ☑ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- ☑ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- ☐ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- ☐ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- ☐ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- ☐ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- ☐ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- ☐ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- ☐ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- ☐ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- ☐ TLS_RSA_WITH_AES_256_GCM_SHA384
- ☐ TLS_RSA_WITH_AES_128_GCM_SHA256
- ☐ TLS_RSA_WITH_AES_256_CBC_SHA256
- ☐ TLS_RSA_WITH_AES_128_CBC_SHA256
- ☐ TLS_RSA_WITH_AES_256_CBC_SHA
- ☐ TLS_RSA_WITH_AES_128_CBC_SHA
- ☐ TLS_RSA_WITH_3DES_EDE_CBC_SHA
- ☐ TLS_RSA_WITH_NULL_SHA256
- ☐ TLS_RSA_WITH_NULL_SHA
- ☐ TLS_PSK_WITH_AES_256_GCM_SHA384
- ☐ TLS_PSK_WITH_AES_128_GCM_SHA256

For information about cipher suite and vulnerability see: https://ciphersuite.info/.

The best hardening is to disable all cipher suites with **cbc** or **no key exchange**. (others were already disabled by SChannel configuration).

4.5.2. Disabling vulnerable cypher suites using script

You need to disable those by running the:

- TLS1.0.reg
- TLS1.1.reg
- Triple DES 168.reg
- PCKS.reg
- RC4 128-128.reg

By default others are disabled

These scripts keep some "good but not perfect cipher-suite" suites like some with CBC (no PFS).

Download these scripts from the "Secure server toolkit.zip".

Make sure the .NET layer will accept to use TLS 1.2:

1. Through the Startup menu, go to “Run” and enter:
   regedit.exe

2. Browse through the registry until you reach the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319

3. In that key, create an entry of type DWORD (32 bit) with the following details:

   Name: SchUseStrongCrypto

   Value: 1

Reboot the server to take everything into account.

5. SQL Server configuration

5.1. Character encoding

Once the database is created, check that "Collation" is set to "**SQL_Latin1_General_CP1_CS_AS**". If the database is created from the HOPEX application (see 3.9.1 Creating a New "HOPEX environment"), the appropriate encoding is automatically configured.

5.2. Database user

You can connect to the database with 2 modes:

- **Native account ➔ easier choice**

  The connection to SQL server for HAS Instance and HOPEX Core module is done with this user/password from SQL server.

- **Windows/Domain account:** Trusted Connection

  The connection is made with the domain user that launch the process. Ensure all users that will launch the desktop application will be defined in SQL Server as well.

5.3. Database connection string

- If you are on a native account, you will use the login/password of SQL.
- If you are on the Windows/Domain account, you will add Trusted_Connection=true in the parameter.
- If you use a secure SQL connection you will need to had TrustServerCertificate=True in the parameter.
- Set the parameter Encrypt=false; or "true" if you use SSL communication. For ODBC Driver 18 the syntax "Encrypt=false;" is mandatory if you do not have SSL communication.

Caution: the value is either true/false or yes/no; In HAS Console the value are true/false in Administration.exe the value are yes/no

5.4. User grants

To run HOPEX Application server the database users need the following privilege and roles.

Common actions performed	• Create/Delete Database • Create/Update/Read/Write database structure (tables, procedures, index…) • Read/Write data access
Server roles	dbcreator(1) db_ddladmin db_datawriter db_datareader
Database roles	db_owner or public(2)
Server permissions	view server state

Should you restrict the role of database creation the DBA must create the databases manually following naming convention

(1) for Windows domain account we recommend you remove the db_creator role.

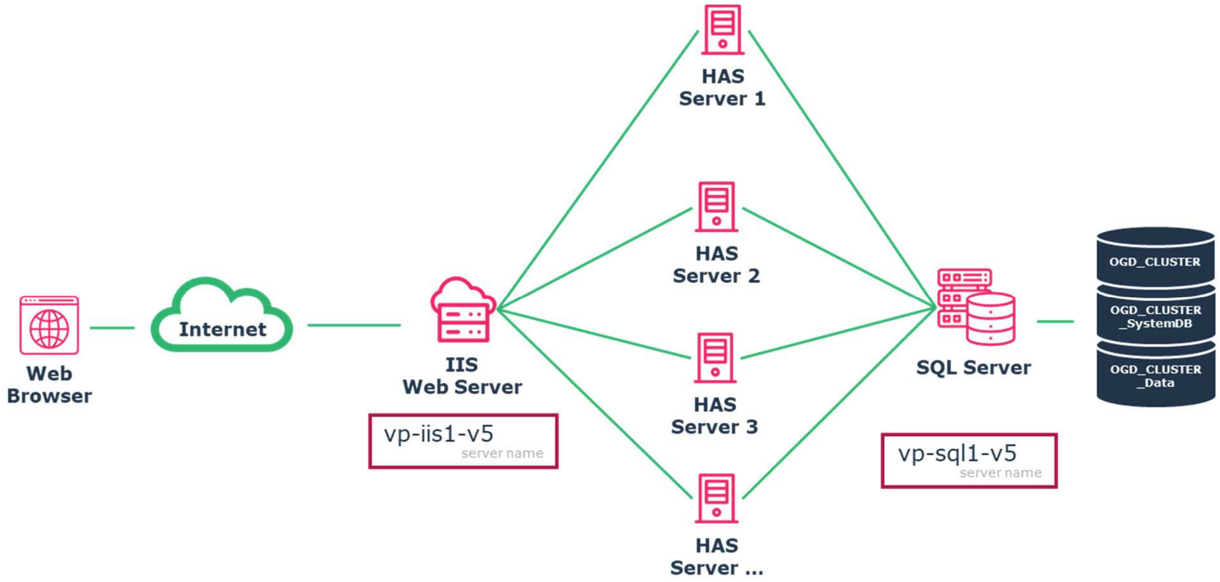
(2) Give public role to restrict access rights

6. Cluster installation

If you are not in a cluster, meaning you have only 1 Server (excluding database) you can skip this chapter.

6.1. Multiple HAS Server

This section details how to define a farm of servers for HAS. This schema represents the deployment to be considered:



This chapter explains the case where you have:

- No load balancer
- 1 server with IIS
- 2 servers for HAS.
- 1 SQL server

Should you have more than 2 HAS servers, repeat the same operation for each additional HAS Server.

Perform the following steps:

A. Configure IIS

B. Install HAS Server 1 as if it was alone and create the instance with this HAS Server 1

C. Install HAS Server 2. Ensure you set the same password for the HAS Instance manager for all HAS Server of the cluster

D. On each additional server Join the cluster

E. Adjust IIS configuration to add each HAS Server part of the cluster

6.1.1. Step A: Configure IIS

Perform the steps described in chapter:

- 2 IIS Web Server as if there was only 1 HAS Server

6.1.2. Step B: Install HAS Server 1

Perform the steps described in chapter:

- 3 HOPEX Application Server (HAS) installation
- 4 SSL Certificates configuration

Ensure that you can perform all the tests described in this chapter:

- 7 Installation

If any of those web front end does not work (HAS Console, HOPEX Web Front-End), fix it before proceeding.

6.1.3. Step C: Install additional HAS Server 2

Repeat the following actions for each additional HAS Server.

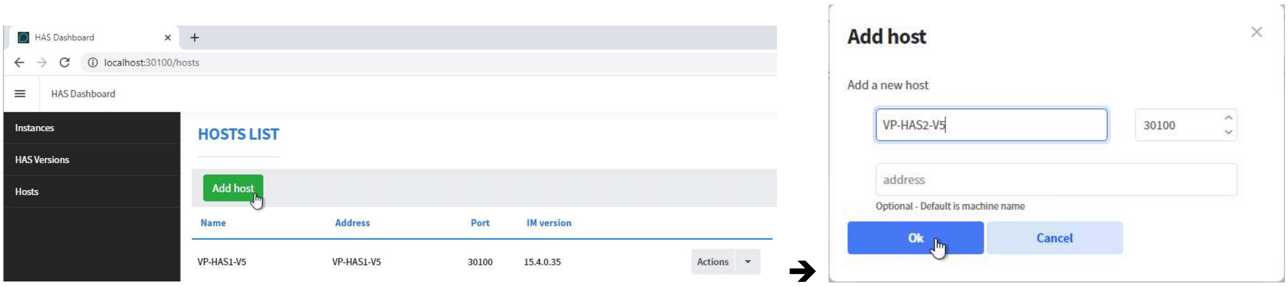
1. Access the additional HAS Server 2.
2. Perform **step 1 to 18** as described section **Installing HAS Instance Manager with the setup**.
3. Ensure you set the **same api-key password for the instance manager** for all HAS Servers.
4. Ensure you use the **same domain user** to launch HAS Instance Manager.

Do not create any HAS Instance from HAS Instance manager on Server 2

6.1.4. Step D: Join the cluster for each additional HAS Server

Repeat the following actions for each additional HAS Server.

1. Access the HAS Server 1 (the first server you installed).
2. Click **Hosts > add host**.
3. Enter the name of the server HAS Server 2 (no IP address). Keep the same HAS Instance manager port (default 30100).
4. Click **OK**.



Name	Address	Port	IM version
VP-HAS1-V5	VP-HAS1-V5	30100	15.4.0.35

VP-HAS2-V5 30100

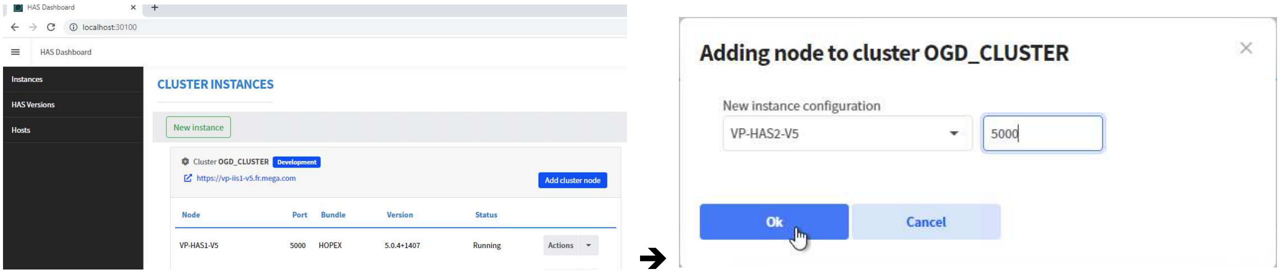
address

Optional - Default is machine name

5. Click **Instances**

6. Select your installed Instance and click **Add cluster node**

7. Select the HAS Server 2 and port number (use the same port for all cluster node 5000)



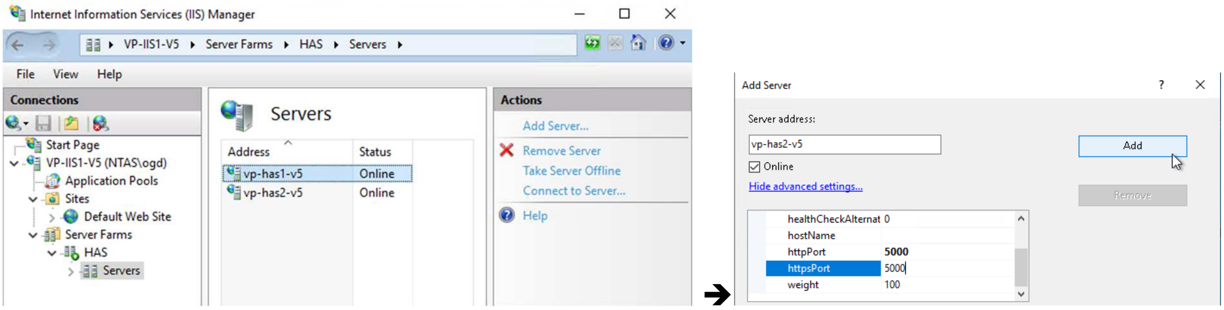
Node	Port	Bundle	Version	Status
VP-HAS1-V5	5000	HOPEX	5.0.4+1407	Running

New instance configuration: VP-HAS2-V5 5000

6.1.5. Step E: Adjust IIS configuration

Repeat the following actions for each additional IIS Server.

1. Access the **IIS Server**.
2. Open **IIS Manager**.
3. Expand **Server Farms**.
4. Expand the HAS server farm you have created in previous step.
5. Click **Server**.
6. Click **Add Server** to "HAS Server 2". In that example "vp-has2-v5"
7. Repeat the step described section 2.6.1 Creating a Server farms
8. **Error! Reference source not found.** Scroll to **always put both port** (HTTP/HTTPS).
   a. Click **Add.**
   b. Click **Finish**.



Address	Status
vp-has1-v5	Online
vp-has2-v5	Online

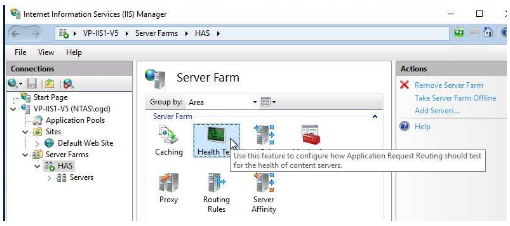
Server address: vp-has2-v5

☑ Online

healthCheckAlternat	0
hostName	
httpPort	5000
httpsPort	5000
weight	100

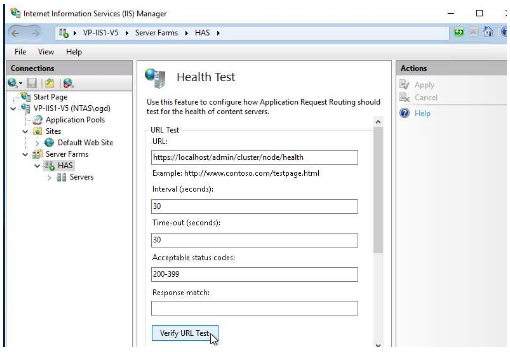
9. Check that all servers of the Cluster passes the **Health Test**.

- Click **Verify URL Test**



Use this feature to configure how Application Request Routing should test for the health of content servers.

➔



Use this feature to configure how Application Request Routing should test for the health of content servers.

URL Test

URL: https://localhost/admin/cluster/node/health

Example: http://www.contoso.com/testpage.html

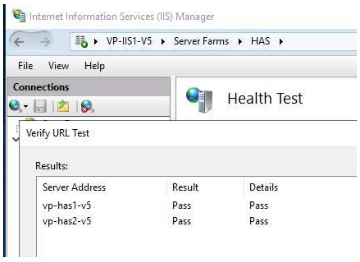
Interval (seconds): 30

Time-out (seconds): 30

Acceptable status codes: 200-399

Response match:

➔


Internet Information Services (IIS) Manager
VP-IIS1-V5 ▸ Server Farms ▸ HAS ▸
File View Help
Connections
Health Test

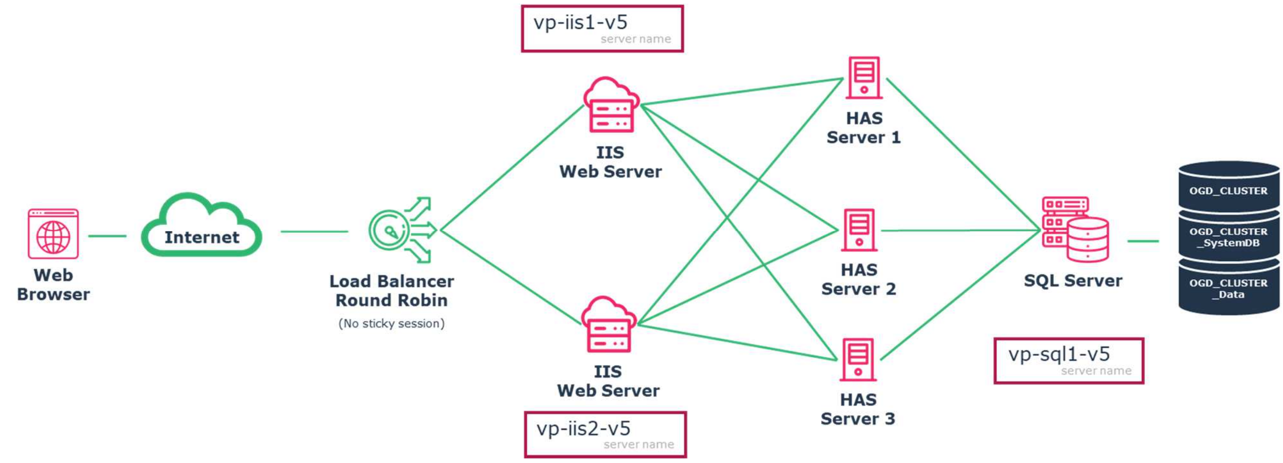
Verify URL Test

Results:

Server Address	Result	Details
vp-has1-v5	Pass	Pass
vp-has2-v5	Pass	Pass

6.2. Multiple IIS Server

This chapter details how to define a cluster with multiple IIS. This schema shows the deployment to be considered:



When you have multiple IIS Web Servers, you must add a **load balancer** in front.

You have multiple IIS Web servers because:

- You have IT constraints of redundancy for **high availability**
- You have **thousands of concurrent** users.

If you are not in this situation, you should reconsider having multiple IIS Servers.

Should you have more than 2 IIS Web server, repeat the same steps for each additional IIS Web Server:

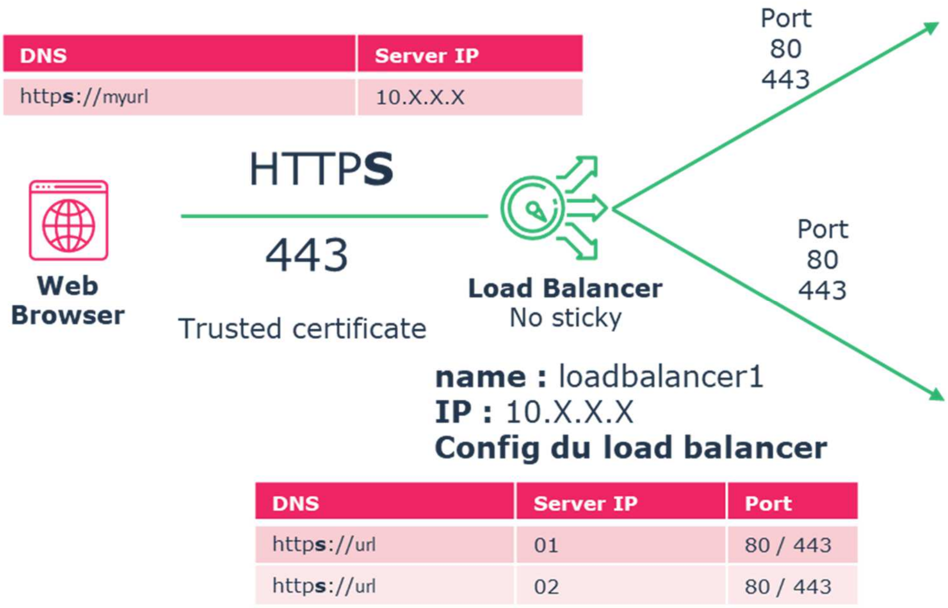
1. Perform the step A to E described in section "6.1 Multiple HAS Server". Repeat Step E for each IIS Server
2. Configure the load balancer

6.2.1. Configuring the load balancer

Configuration of the load balancer may depend on the chosen load balancer.

Ensure the following steps have been performed:

- The DNS URL is pointing toward the load balancer
- The load balancer has the list of all IIS Web server
- For easiness of deployment, have your load balancer pointing on port 80 and 443 on IIS Web Server.
- The load balancer is set to no sticky session mode.



DNS	Server IP
https://myurl	10.X.X.X

name : loadbalancer1
IP : 10.X.X.X
Config du load balancer

DNS	Server IP	Port
https://url	01	80 / 443
https://url	02	80 / 443

6.3. Multiple SQL Server

For such High availability of SQL Server, refer to Microsoft documentation about Always on deployment.

With HOPEX there are two main ways the SQL availability features can be used:

- High availability
- Disaster recovery

CAUTION: These are advance configurations for which only SQL Server expert will be able to guide you through such configuration.

For more information see: https://learn.microsoft.com/en-us/sql/database-engine/sql-server-business-continuity-dr?view=sql-server-ver16

7. Installation errors and tests

If you have followed the previous chapter about the installation your installation should work properly. Nonetheless, there are area that can prevent the installation to be successful. Follow the steps described below to ensure your installation is good.

All screenshots, in this documentation, are performed with Google Chrome. Error message may vary on Firefox or Edge.

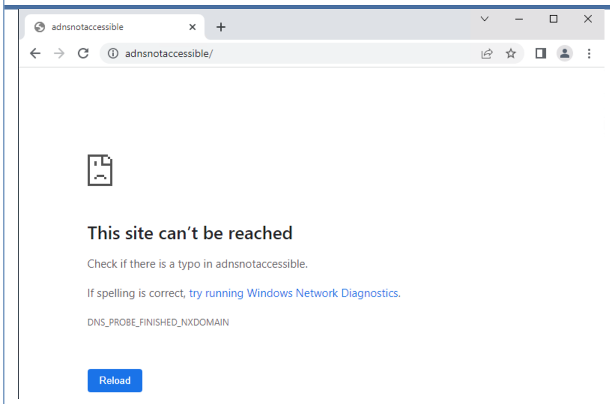
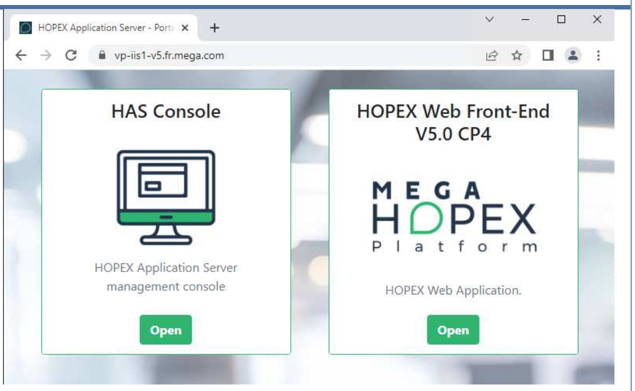
Ensure that:

- all servers of the cluster (IIS+HAS) have access to the public DNS
- all servers of the cluster (IIS+HAS) have valid SSL public certificate otherwise the public certificate must be on all servers.
- the root.pfx certificate is replicated on all servers.
- the cluster.cfg file is identical on each HAS server
- each HAS Instance Manager is launched by the same domain user.

7.1. Testing URL DNS

Ensure that the public DNS is accessible from all servers.

1. Go on **all servers (HAS+IIS)** in RDP (Remote Desktop Protocol) session.
2. From this RDP session open a **supported web browser**: Chrome, Firefox, Edge.
3. Enter your public URL. In this example https://vp-iis1-V5.fr.mega.com

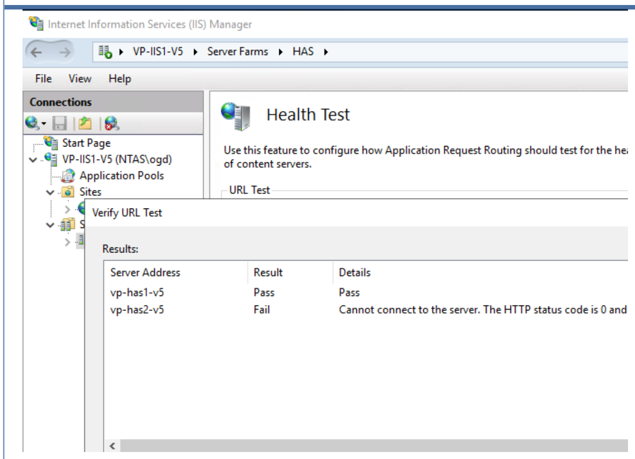
Test Failed	Test Successful
 This site can't be reached Check if there is a typo in adnsnotaccessible. If spelling is correct, try running Windows Network Diagnostics. DNS_PROBE_FINISHED_NXDOMAIN 	 HOPEX Application Server - Port vp-iis1-v5.fr.mega.com HAS Console HOPEX Application Server management console Open HOPEX Web Front-End V5.0 CP4 MEGA HOPEX Platform HOPEX Web Application. Open
This server cannot access your public DNS thus HOPEX will not work properly. Fix it before proceeding.	If you get a 502 error this test is successful, but some other configurations are invalid: see Checking communication between servers.

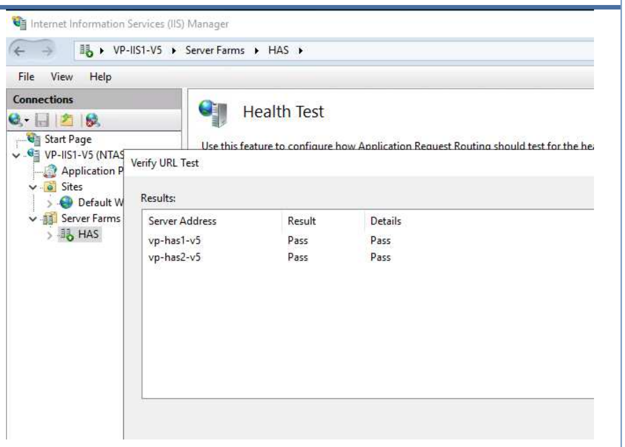
7.2. Checking communication between servers

7.2.1. From IIS to HAS Servers

Ensure that all HAS Server nodes can be visible from IIS:

1. Access **each IIS Web Server**.
2. Launch **IIS Management Console**.
3. Go on the **Server Farms**.
4. Go on **Health Test**.

<table>
<tr><th>Test Failed</th><th>Test Successful</th></tr>
<tr>
<td>

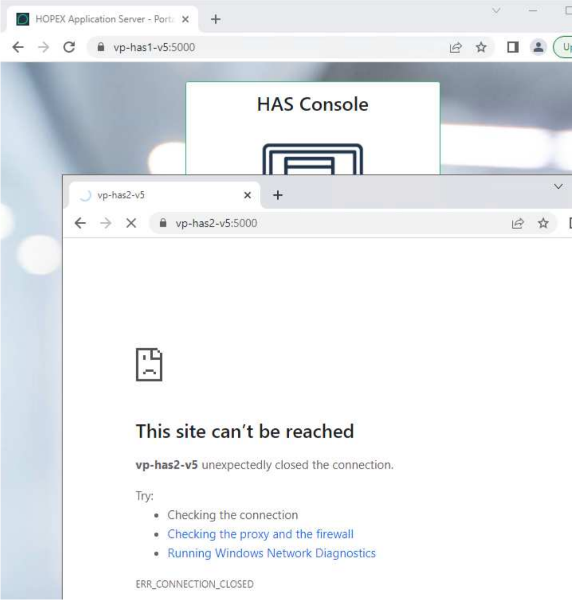
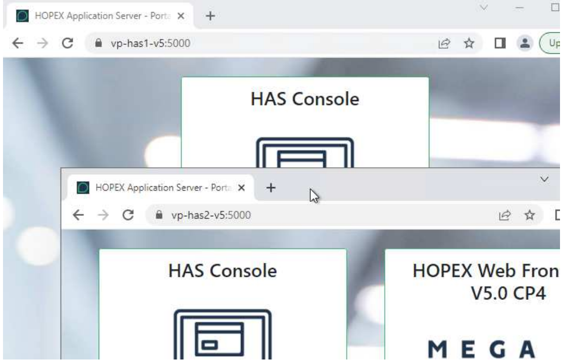
Use this feature to configure how Application Request Routing should test for the hea of content servers.
Verify URL Test
Results:<table><tr><th>Server Address</th><th>Result</th><th>Details</th></tr><tr><td>vp-has1-v5</td><td>Pass</td><td>Pass</td></tr><tr><td>vp-has2-v5</td><td>Fail</td><td>Cannot connect to the server. The HTTP status code is 0 and</td></tr></table></td>
<td>

Use this feature to configure how Application Request Routing should test for the hea
Verify URL Test
Results:<table><tr><th>Server Address</th><th>Result</th><th>Details</th></tr><tr><td>vp-has1-v5</td><td>Pass</td><td>Pass</td></tr><tr><td>vp-has2-v5</td><td>Pass</td><td>Pass</td></tr></table></td>
</tr>
<tr>
<td>If one of the servers has a <b>Result</b> “Fail”:
➔ Ensure the HTTP/HTTPS is properly configured.</td>
<td>If all of the servers of the farm have a <b>Result</b> “Pass”:
➔ The communication is successful.</td>
</tr>
</table>

7.2.2. Servers to HAS Servers

If you are in a cluster scenario and have several HAS Server.

1. Go on **all servers (HAS+IIS)** in RDP session
2. From this RDP session open a **supported web browser**: Chrome, Firefox, Edge.
3. Open 2 tabs in your web browser and on each tab enter the server internal address. In this example (adjust to your case):
   - Server 1: https://vp-has1-V5:5000
   - Server 2: https://vp-has2-V5:5000

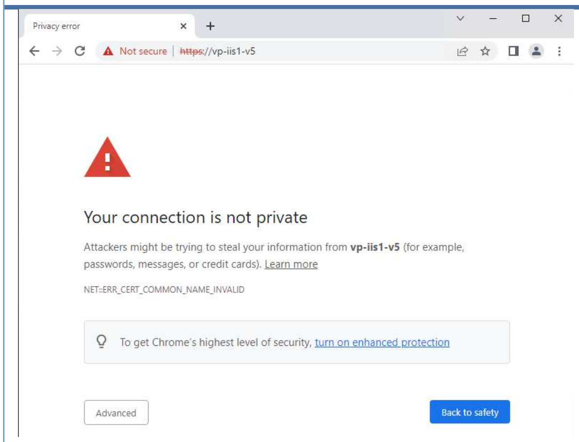
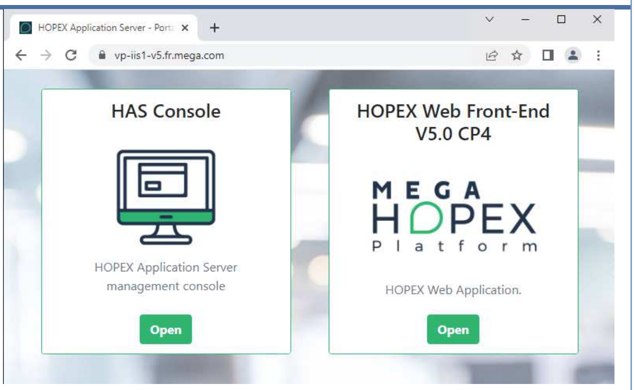
Test Failed	Test Successful
 HAS Console vp-has2-v5:5000 This site can't be reached **vp-has2-v5** unexpectedly closed the connection. Try: • Checking the connection • Checking the proxy and the firewall • Running Windows Network Diagnostics ERR_CONNECTION_CLOSED	 HAS Console vp-has2-v5:5000 HAS Console HOPEX Web Fron V5.0 CP4 MEGA
➔ Ensure server are visible from each other on the chosen port (default 5000)	➔ This allows you to check that each server is independently started properly

7.3. Testing SSL Certificates

7.3.1. Testing public certificate

To validate that the certificate generated by the customer is valid:

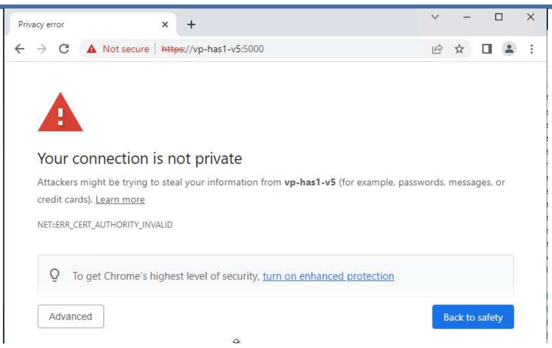
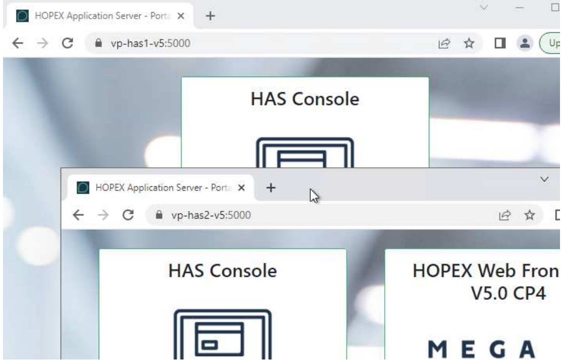
1. Access **all servers (HAS+IIS)** in RDP session
2. From this RDP session open a **supported web browser**: Chrome, Firefox, Edge.
3. Enter your public URL (In this example https://vp-iis1-V5.fr.mega.com).

Test Failed	Test Successful
 Privacy error Not secure | ~~https~~://vp-iis1-v5 Your connection is not private Attackers might be trying to steal your information from **vp-iis1-v5** (for example, passwords, messages, or credit cards). Learn more NET::ERR_CERT_COMMON_NAME_INVALID To get Chrome's highest level of security, turn on enhanced protection 	 HOPEX Application Server - Port vp-iis1-v5.fr.mega.com HAS Console HOPEX Application Server management console Open HOPEX Web Front-End V5.0 CP4 MEGA HOPEX Platform HOPEX Web Application. Open
If you get this message: • Ensure that the URL entered in the web browser is the same as the one defined in the SSL certificate. • Ensure that the SSL certificate is properly imported on **all servers (HAS+IIS)** windows certificate store.	

7.3.2. Testing self-signed HAS certificate

To validate that the root.pfx certificate has been properly imported on all servers and that each server has the same root.pfx certificate:

1. Access **IIS Web Server** in RDP session
2. From this RDP session open a **supported web browser**: Chrome, Firefox, Edge.
3. Open 2 tabs in your web browser and on each tab enter the server internal address. In this example (adjust to your case):
    - Server 1: https://vp-has1-V5:5000
    - Server 2: https://vp-has2-V5:5000

Test Failed	Test Successful
 Privacy error Not secure | ~~https~~://vp-has1-v5:5000 Your connection is not private Attackers might be trying to steal your information from **vp-has1-v5** (for example, passwords, messages, or credit cards). Learn more NET::ERR_CERT_AUTHORITY_INVALID To get Chrome's highest level of security, turn on enhanced protection Advanced Back to safety	 HOPEX Application Server - Port vp-has1-v5:5000 HAS Console HOPEX Application Server - Port vp-has2-v5:5000 HAS Console HOPEX Web Fron V5.0 CP4 MEGA
If one of the HAS Servers returns a Not Secure certificate: ➔ You must fix it.	

4. Repeat the operation:
   - Go on HAS Server 1 and test HAS Server 2 access
   - Go on HAS Server 2 and test HAS Server 1 access

If any fails to fix it:

1. Stop all HAS Servers.
2. Delete from all servers:
   - the file **root.pfx** located in C:\...\MEGA\Hopex Application Server\5000\.certificates
   - the certificate called "Hopex Application Server" imported in windows from the **mmc console**
3. Start HAS Server 1.
4. Repeat steps described in section "4.2 Configuring HAS Cluster node SSL Certificate (2)"

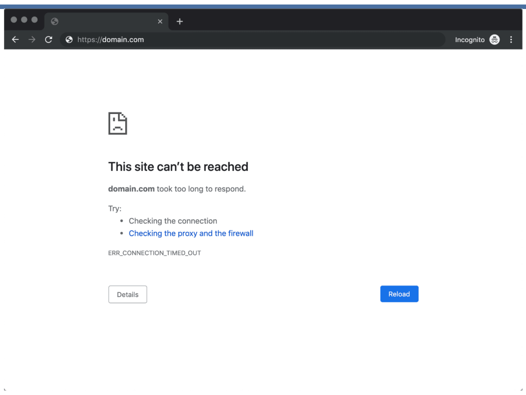
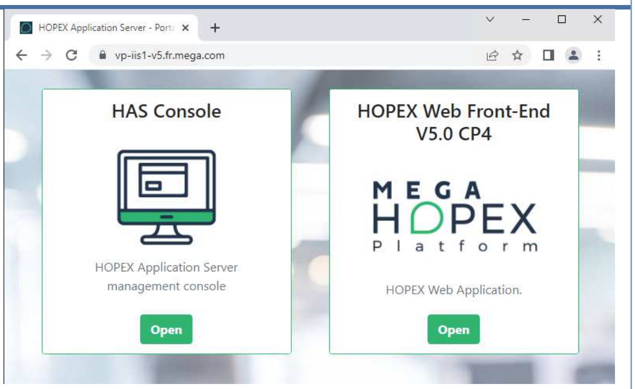
7.4. Testing HAS

7.4.1. Checking port 5000 is available

You may encounter situation where port 5000 is either blocked by a firewall or already in use.

To check port 5000:

1. Open your web browser.
2. Access the private server URL.
   - Server 1: https://vp-has1-V5:5000

Test Failed	Test Successful
 https://domain.com This site can't be reached **domain.com** took too long to respond. Try: • Checking the connection • Checking the proxy and the firewall ERR_CONNECTION_TIMED_OUT 	 HOPEX Application Server - Port vp-iis1-v5.fr.mega.com HAS Console HOPEX Application Server management console HOPEX Web Front-End V5.0 CP4 HOPEX Web Application.
➔ To fix, delete the instance and select another port number.	

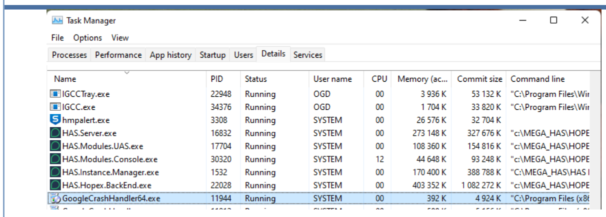
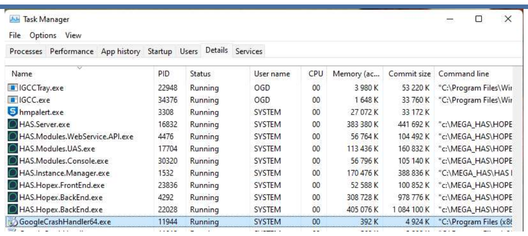
7.4.2. Checking running processes

When successfully running an instance should contain the following windows processes running:

- HAS.Instance.Manager.exe
- HAS.Server.exe
- HAS.Modules.Console.exe
- HAS.Modules.UAS.exe
- HAS.Hopex.BackEnd.exe
  - There should be two of type O and one of type J
- HAS.Hopex.FrontEnd.exe
- HAS.Modules.WebService.API.exe

To check the running processes:

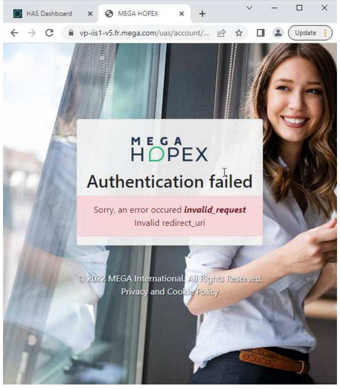
1. Open the **Windows Task Manager**.
2. Select **Details** tab.
3. Ensure you have the **Command line** column enabled.
4. Ensure you have waited enough time to let the processes launched.

<table>
<tr><th>Test Failed</th><th>Test Successful</th></tr>
<tr>
<td>

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
<table>
<tr><th>Name</th><th>PID</th><th>Status</th><th>User name</th><th>CPU</th><th>Memory (ac...</th><th>Commit size</th><th>Command line</th></tr>
<tr><td>IGCCTray.exe</td><td>22948</td><td>Running</td><td>OGD</td><td>00</td><td>3 936 K</td><td>53 132 K</td><td>"C:\Program Files\Wi</td></tr>
<tr><td>IGCC.exe</td><td>34376</td><td>Running</td><td>OGD</td><td>00</td><td>1 704 K</td><td>33 820 K</td><td>"C:\Program Files\Wi</td></tr>
<tr><td>hmpalert.exe</td><td>3308</td><td>Running</td><td>SYSTEM</td><td>00</td><td>26 576 K</td><td>32 704 K</td><td></td></tr>
<tr><td>HAS.Server.exe</td><td>16832</td><td>Running</td><td>SYSTEM</td><td>00</td><td>273 148 K</td><td>327 676 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Modules.UAS.exe</td><td>17704</td><td>Running</td><td>SYSTEM</td><td>00</td><td>108 360 K</td><td>154 816 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Modules.Console.exe</td><td>30320</td><td>Running</td><td>SYSTEM</td><td>12</td><td>44 648 K</td><td>93 248 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Instance.Manager.exe</td><td>1532</td><td>Running</td><td>SYSTEM</td><td>00</td><td>170 400 K</td><td>388 788 K</td><td>"C:\MEGA_HAS\HAS</td></tr>
<tr><td>HAS.Hopex.BackEnd.exe</td><td>22028</td><td>Running</td><td>SYSTEM</td><td>00</td><td>403 352 K</td><td>1 082 272 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>GoogleCrashHandler64.exe</td><td>11944</td><td>Running</td><td>SYSTEM</td><td>00</td><td>392 K</td><td>4 924 K</td><td>"C:\Program Files (x8</td></tr>
</table>
</td>
<td>

Task Manager
File Options View
Processes Performance App history Startup Users Details Services
<table>
<tr><th>Name</th><th>PID</th><th>Status</th><th>User name</th><th>CPU</th><th>Memory (ac...</th><th>Commit size</th><th>Command line</th></tr>
<tr><td>IGCCTray.exe</td><td>22948</td><td>Running</td><td>OGD</td><td>00</td><td>3 980 K</td><td>53 220 K</td><td>"C:\Program Files\Wi</td></tr>
<tr><td>IGCC.exe</td><td>34376</td><td>Running</td><td>OGD</td><td>00</td><td>1 648 K</td><td>33 760 K</td><td>"C:\Program Files\Wi</td></tr>
<tr><td>hmpalert.exe</td><td>3308</td><td>Running</td><td>SYSTEM</td><td>00</td><td>27 072 K</td><td>33 172 K</td><td></td></tr>
<tr><td>HAS.Server.exe</td><td>16832</td><td>Running</td><td>SYSTEM</td><td>00</td><td>383 380 K</td><td>441 692 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Modules.WebService.API.exe</td><td>4476</td><td>Running</td><td>SYSTEM</td><td>00</td><td>56 764 K</td><td>104 492 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Modules.UAS.exe</td><td>17704</td><td>Running</td><td>SYSTEM</td><td>00</td><td>113 436 K</td><td>160 832 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Modules.Console.exe</td><td>30320</td><td>Running</td><td>SYSTEM</td><td>00</td><td>56 796 K</td><td>105 140 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Instance.Manager.exe</td><td>1532</td><td>Running</td><td>SYSTEM</td><td>00</td><td>170 476 K</td><td>388 836 K</td><td>"C:\MEGA_HAS\HAS</td></tr>
<tr><td>HAS.Hopex.FrontEnd.exe</td><td>23836</td><td>Running</td><td>SYSTEM</td><td>00</td><td>52 588 K</td><td>100 852 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Hopex.BackEnd.exe</td><td>4292</td><td>Running</td><td>SYSTEM</td><td>00</td><td>308 728 K</td><td>978 776 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>HAS.Hopex.BackEnd.exe</td><td>22028</td><td>Running</td><td>SYSTEM</td><td>00</td><td>405 076 K</td><td>1 084 100 K</td><td>"c:\MEGA_HAS\HOPE</td></tr>
<tr><td>GoogleCrashHandler64.exe</td><td>11944</td><td>Running</td><td>SYSTEM</td><td>00</td><td>392 K</td><td>4 924 K</td><td>"C:\Program Files (x8</td></tr>
</table>
</td>
</tr>
<tr>
<td>➔ Read the HAS log to understand why the other processes did not start.</td>
<td></td>
</tr>
</table>

7.4.3. Checking login page

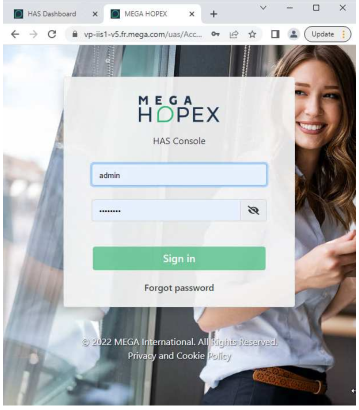
To test the installation

1. Open a **supported web browser**: Chrome, Firefox, Edge. From anywhere you can access the URL (not from the server itself)
2. Enter your public URL. In this example https://vp-iis1-V5.fr.mega.com
3. On the portal select either:
   - the HAS Console https://vp-iis1-V5.fr.mega.com/console
   - HOPEX Web Front End https://vp-iis1-V5.fr.mega.com/hopex

<table>
<tr><th>Test Failed</th><th>Test Successful</th></tr>
<tr>
<td>


Authentication failed

Sorry, an error occured *invalid_request*
Invalid redirect_uri

© 2022 MEGA International. All Rights Reserved.
Privacy and Cookie Policy
</td>
<td>


HAS Console

admin

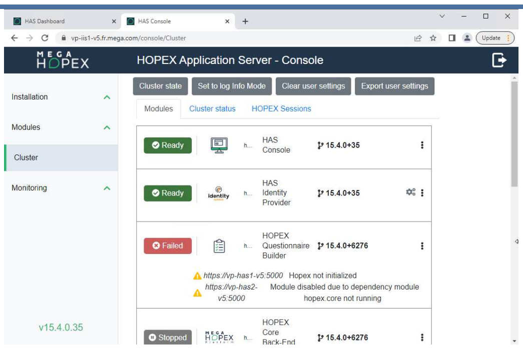
•••••••••

© 2022 MEGA International. All Rights Reserved.
Privacy and Cookie Policy
</td>
</tr>
<tr>
<td>➔ Ensure the URL you wrote in the web browser is the same
➔ Ensure the SSL certificate is valid
➔ Ensure your SSO configuration is valid</td>
<td></td>
</tr>
</table>

7.4.4. Login to HAS Console

To conclude that your installation is valid from an **HAS point of view** (regardless of functional modules):

1. Open a **supported web browser**: Chrome, Firefox, Edge. From anywhere you can access the URL (not from the server itself).
2. Enter your public URL. In this example https://vp-iis1-V5.fr.mega.com
3. On the portal select:
   - the HAS Console https://vp-iis1-V5.fr.mega.com/console

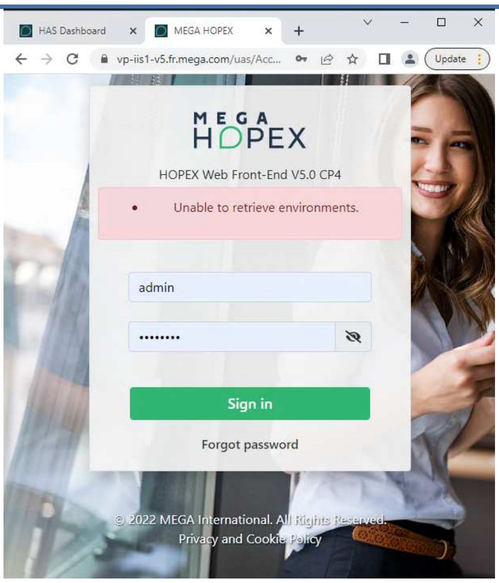
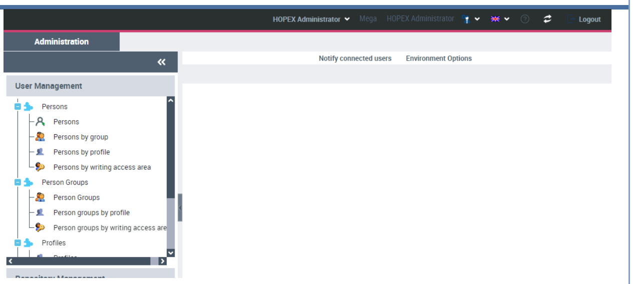
Test Failed	Test Successful
	 HAS Dashboard HAS Console vp-iis1-v5.fr.mega.com/console/Cluster HOPEX Application Server - Console Cluster state Set to log Info Mode Clear user settings Export user settings Installation Modules Cluster Monitoring v15.4.0.35 Modules Cluster status HOPEX Sessions Ready h... HAS Console 15.4.0+35 Ready h... HAS Identity Provider 15.4.0+35 Failed h... HOPEX Questionnaire Builder 15.4.0+6276 ⚠ https://vp-has1-v5:5000 Hopex not initialized ⚠ https://vp-has2-v5:5000 Module disabled due to dependency module hopex.core not running Stopped h... HOPEX Core Back-End 15.4.0+6276
➔ If you are unable to connect read the log.	

7.5. Testing Web HOPEX

7.5.1. Login to Web Front End

To conclude that your installation is valid from an **end-user point of view**:

1. Open a **supported web browser**: Chrome, Firefox, Edge. From anywhere you can access the URL (not from the server itself)
2. Type your public URL. In my example https://vp-iis1-V5.fr.mega.com
3. On the portal select either
   a. the HAS Console https://vp-iis1-V5.fr.mega.com/hopex
4. As a login use “Mega” with default password “Hopex”
5. If prompted select HOPEX Administrator profile.

Test Failed	Test Successful
 HAS Dashboard MEGA HOPEX vp-iis1-v5.fr.mega.com/uas/Acc... MEGA HOPEX HOPEX Web Front-End V5.0 CP4 • Unable to retrieve environments. admin •••••••• Sign in Forgot password © 2022 MEGA International. All Rights Reserved. Privacy and Cookie Policy	 HOPEX Administrator Mega HOPEX Administrator Logout Administration Notify connected users Environment Options User Management Persons Persons Persons by group Persons by profile Persons by writing access area Person Groups Person Groups Person groups by profile Person groups by writing access are Profiles
➔ If you are unable to connect read the log. ➔ If you get **Unable to retrieve environments**, ensure the domain user has the right password or access right to shared folder.	

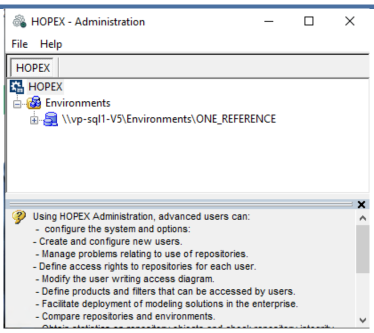
7.6. Testing Desktop client

Complementary to testing the Web part you need to test the Desktop part as well. This desktop part is used mainly for development platform. if it doesn't work it can be a sign of an unproper installation.

7.6.1. Login to Administration.exe

This is to validate that HAS Server node has been properly configured.

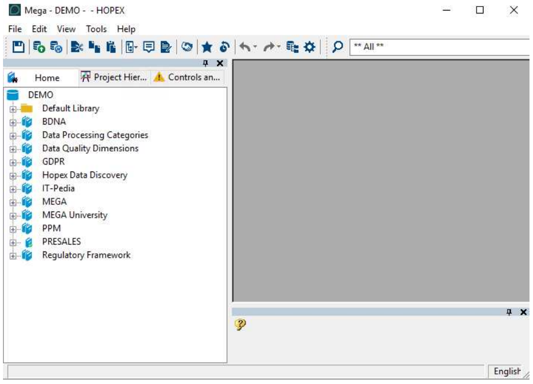
1. Go on **all HAS servers** in RDP session.
2. Go in the installation folder. Default: C:\...\HOPEX Application Server\5000
3. Launch Administration.exe

Test Failed	Test Successful
The process does not launch and closes immediately Or The process launches with error message	 HOPEX - Administration File Help HOPEX HOPEX Environments \\vp-sql1-V5\Environments\ONE_REFERENCE Using HOPEX Administration, advanced users can: - configure the system and options: - Create and configure new users. - Manage problems relating to use of repositories. - Define access rights to repositories for each user. - Modify the user writing access diagram. - Define products and filters that can be accessed by users. - Facilitate deployment of modeling solutions in the enterprise. - Compare repositories and environments.
➔ Read Windows Event logs ➔ Read megaerrr logs ➔ Ensure HAS Server is up and running ➔ Ensure access to must license works	

7.6.2. Login to HOPEX.exe

To validate that HAS Server node has been properly configured:

1. Go on **all HAS servers** in RDP session.
2. Go in the installation folder. Default: C:\...\HOPEX Application Server\5000
3. Launch HOPEX.exe.
4. Login "Mega" with default password "Hopex".

Test Failed	Test Successful
The process does not launch and closes immediately Or The process launches with error message	 Mega - DEMO - - HOPEX File Edit View Tools Help ** All ** Home Project Hier... Controls an... DEMO Default Library BDNA Data Processing Categories Data Quality Dimensions GDPR Hopex Data Discovery IT-Pedia MEGA MEGA University PPM PRESALES Regulatory Framework English
➔ Read Windows Event logs ➔ Read megaerrr logs ➔ Ensure HAS Server is up and running ➔ Ensure access to must license works	

8. Installation in multi-tenant scenarios

HOPEX supports multi-tenant at infrastructure level. A same server can be used to host several customers.

Multi-tenant capability is not supported at the following levels:

- database

  Each database is independent and do no share tables/columns/data.

  ➔ This ensures highest security for our customers' data.

- application

  Each deployment is autonomous and do not share exe or dll.

  ➔ This enables to have customers in different versions and updates.

Multi-tenant capabilities are available to manage:

- multiple environments or instance.
- multiple versions on the same server.

8.1. Multi-environments – Multi-instances

HOPEX V5 supports multiple installations on the same server. This type of deployment is useful when you:

- want to put the PRED-PROD and PROD on the same server.
- have several HOPEX Environments (SystemDb) for historical reason.

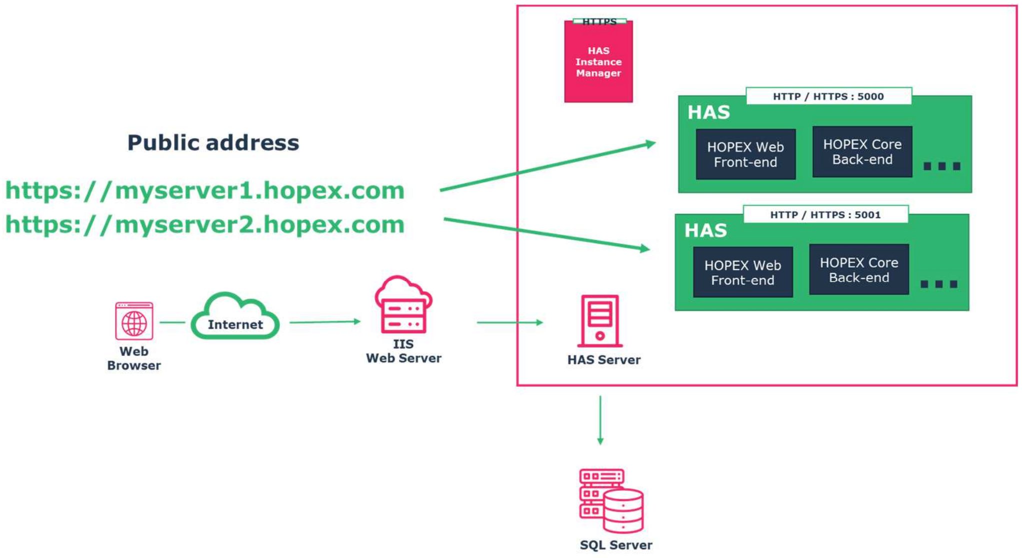
  For new customer, this scenario is not recommended.

When doing so you need to adjust IIS configuration to run properly this type of deployment.

Moreover, make sure you size the server accordingly. Each additional instance on a server requires a minimum of 8Gb of RAM.

The architecture pattern of such installation is the following:

- each Instance as a dedicated DNS
- each instance as a dedicated port allocated



The installation of HAS Server:

- is the same process as described in previous chapters.
- You may need to adjust the IIS configuration described from previous chapter as described below.

8.1.1. Configure IIS

8.1.1.1. Public DNS and SSL for each instance

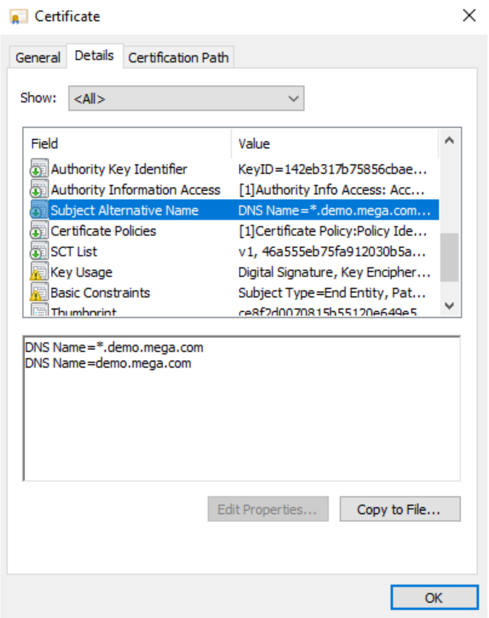
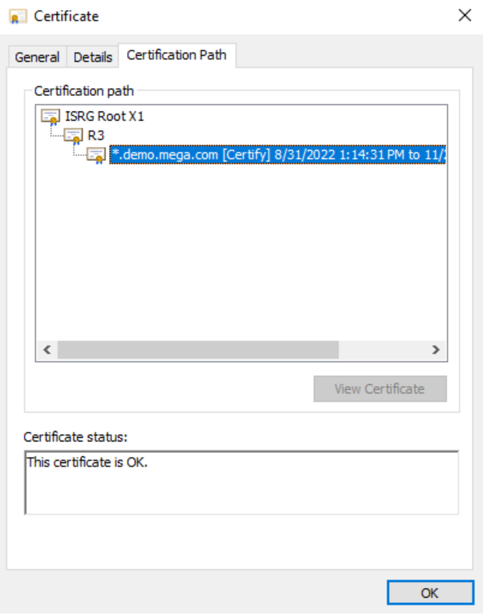
For each instance you must have a DNS.

For example:

- Instance 1 – PROD: https://prod.hopex.com
- Instance 2 – PRE-PROD: https://preprod.hopex.com

Moreover, your SSL Certificate must be valid for both DNS, so either you have:

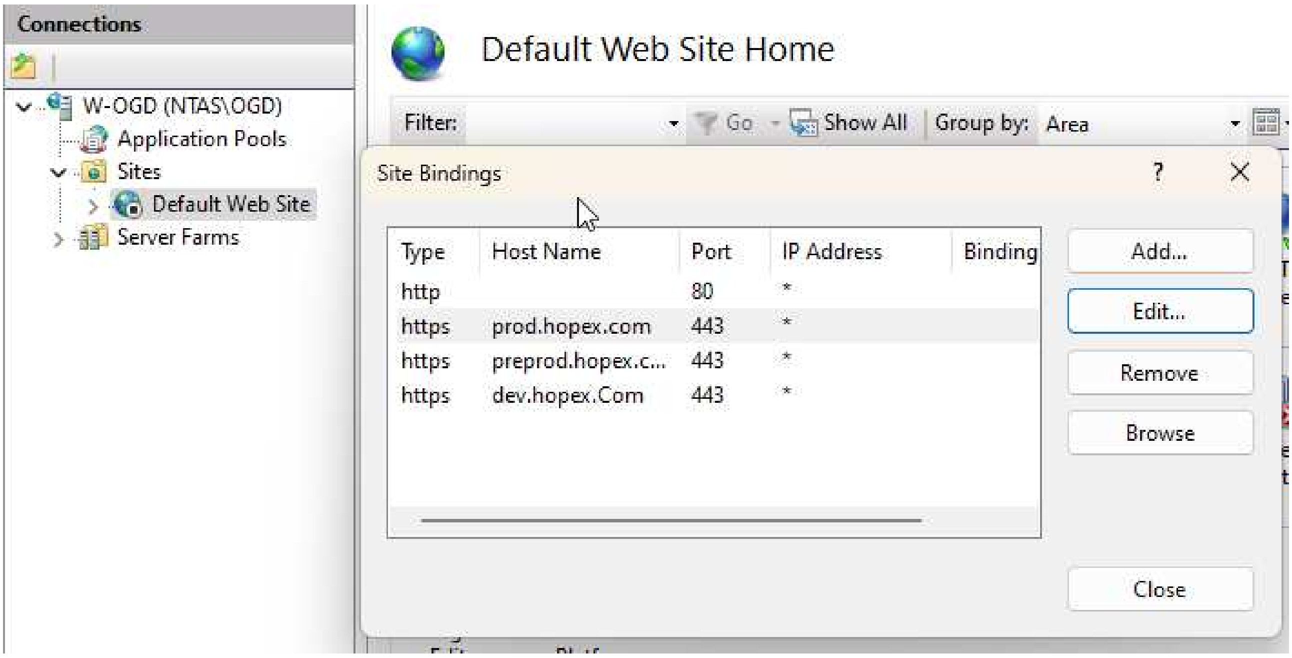
- a wild card SSL certificate. Example: *.hopex.com
- all the alternative DNS name defined in your certificate prod.hopex.com, preprod.hopex.com…

Example of alternative DNS certificate	Example of Wild card certificate
 Certificate General Details Certification Path Show: <All> Field Value Authority Key Identifier KeyID=142eb317b75856cbae… Authority Information Access [1]Authority Info Access: Acc… Subject Alternative Name DNS Name=*.demo.mega.com… Certificate Policies [1]Certificate Policy:Policy Ide… SCT List v1, 46a555eb75fa912030b5a… Key Usage Digital Signature, Key Encipher… Basic Constraints Subject Type=End Entity, Pat… Thumbprint ce8f2d0070815b55120e649e5 DNS Name=*.demo.mega.com DNS Name=demo.mega.com Edit Properties… Copy to File… OK	 Certificate General Details Certification Path Certification path ISRG Root X1 R3 *.demo.mega.com [Certify] 8/31/2022 1:14:31 PM to 11/ View Certificate Certificate status: This certificate is OK. OK

If you do not have a wildcard certificate you need to add extra binding in your IIS website. In that case:

1. Go on your Default Web site.
2. Right-click and Edit Binding.
3. Add a binding for each URL.
4. Enter a Hostname for each URL that matches the SSL Certificate.

Example:



Type	Host Name	Port	IP Address	Binding
http		80	*	
https	prod.hopex.com	443	*	
https	preprod.hopex.c...	443	*	
https	dev.hopex.Com	443	*	

8.1.1.2. Create a server Farm for each instance

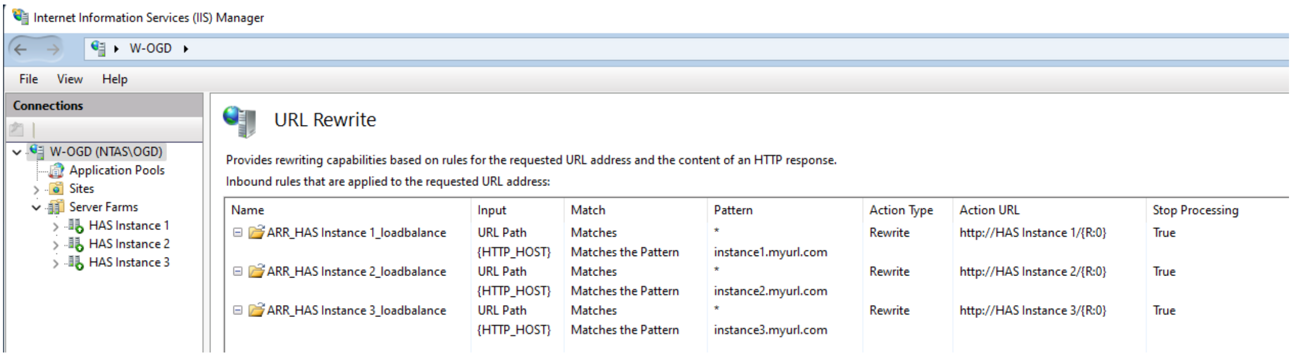
For each Instance you must create a server farm as described section "2.6 Configuring Server Farm - ARR"

Make sure you enter the right port number. In doubt check the IIS config file as described section "2.8.3 Checking configuration (optional)"

8.1.1.3. Create a rewrite rule for each instance

For each Instance, you have an URL Rewrite rule that you need to ensure has the proper condition.

Example with 3 instances. You can see 3 farms, 3 URL Rewrite rule that each have a condition.



Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	Action URL	Stop Processing
ARR_HAS Instance 1_loadbalance	URL Path	Matches	*	Rewrite	http://HAS Instance 1/{R:0}	True
	{HTTP_HOST}	Matches the Pattern	instance1.myurl.com			
ARR_HAS Instance 2_loadbalance	URL Path	Matches	*	Rewrite	http://HAS Instance 2/{R:0}	True
	{HTTP_HOST}	Matches the Pattern	instance2.myurl.com			
ARR_HAS Instance 3_loadbalance	URL Path	Matches	*	Rewrite	http://HAS Instance 3/{R:0}	True
	{HTTP_HOST}	Matches the Pattern	instance3.myurl.com			

8.1.2. Domain users

The domain user used is the same for all the instances. So, this domain user must have access to:

- all HOPEX Environment shared folders and Must license
- the database in case of Trusted Connection.

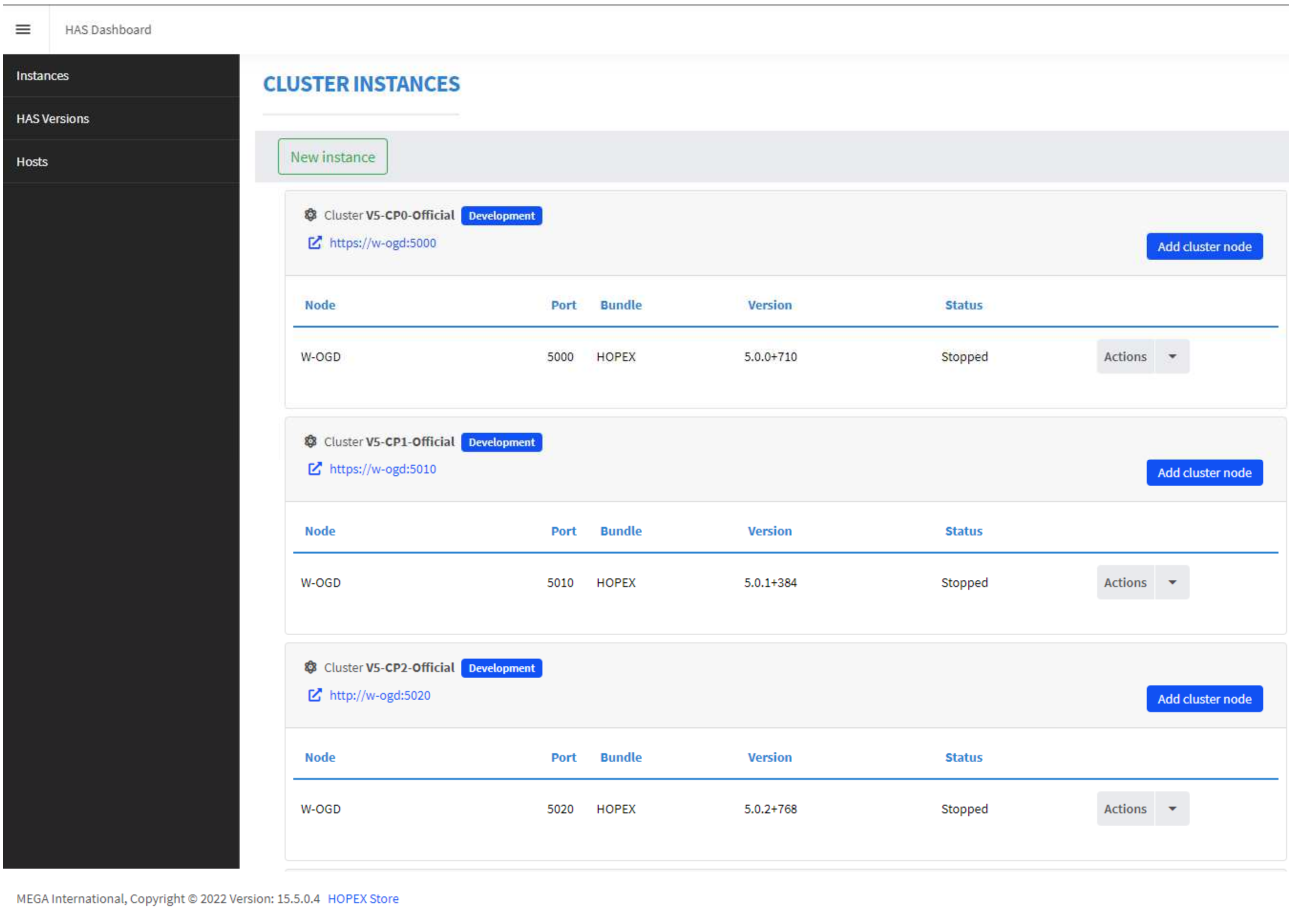
8.2. Multi-version scenario

This scenario concerns the following situation:

- If you are migrating or want to preview some features without changing you existing version.
- If you are a partner or a developer, you may need to work alternatively with different version of HOPEX. In that context you may want to have several versions installed: V5 CP2, V5 CP3, V5 CP4…

This installation of this scenario is the same as the multi-environment / multi-instance.

Just ensure the **HAS Instance manager is its latest version** and that you have all the prerequisites that correspond to each version you want to use.



CLUSTER INSTANCES

Cluster **V5-CP0-Official** Development
https://w-ogd:5000

Node	Port	Bundle	Version	Status
W-OGD	5000	HOPEX	5.0.0+710	Stopped

Cluster **V5-CP1-Official** Development
https://w-ogd:5010

Node	Port	Bundle	Version	Status
W-OGD	5010	HOPEX	5.0.1+384	Stopped

Cluster **V5-CP2-Official** Development
http://w-ogd:5020

Node	Port	Bundle	Version	Status
W-OGD	5020	HOPEX	5.0.2+768	Stopped

MEGA International, Copyright © 2022 Version: 15.5.0.4 HOPEX Store

Recommendations:

- Give explicit name to the cluster
- Give port number to ease understanding which version you are looking at.

  For example, set port 5100 for V5 CP1, 5200 for V5 CP2, 5210 for V5 CP1 HF1… Caution some port may be already in use by other applications.

9. Other installation topics

This section corresponds to specific use case.

9.1. Using Server API

If you are coming from a previous MEGA HOPEX version, you might have used our server API. This server API in VB, JAVA or C# enables to run external programs and communicate with HOPEX. If you have not used this **Server API**, use our **REST API** and ignore this section.

To enable this Server API, you must reference your installation in Windows registry.

CAUTION: There can be only one instance reference in the registry at a time.

Steps to perform:

1. Go in your installation folder. Default: C:\ProgramData\HOPEX Application Server\5000
2. Run the PowerShell script "HOPEX-regserver.ps1". You must run it with sufficient privilege:
    - Rights to run PowerShell script
    - Rights to write in the Windows Registry.
3. Repeat this operation each time you install an HF / CP or major version.

9.2. Publishing Static Website

Read this section if you are creating and publishing static website with HOPEX.

In HOPEX V5 you can publish a static website:

- directly in HOPEX Application Server ➔ **recommended choice.**
- in IIS as a web application

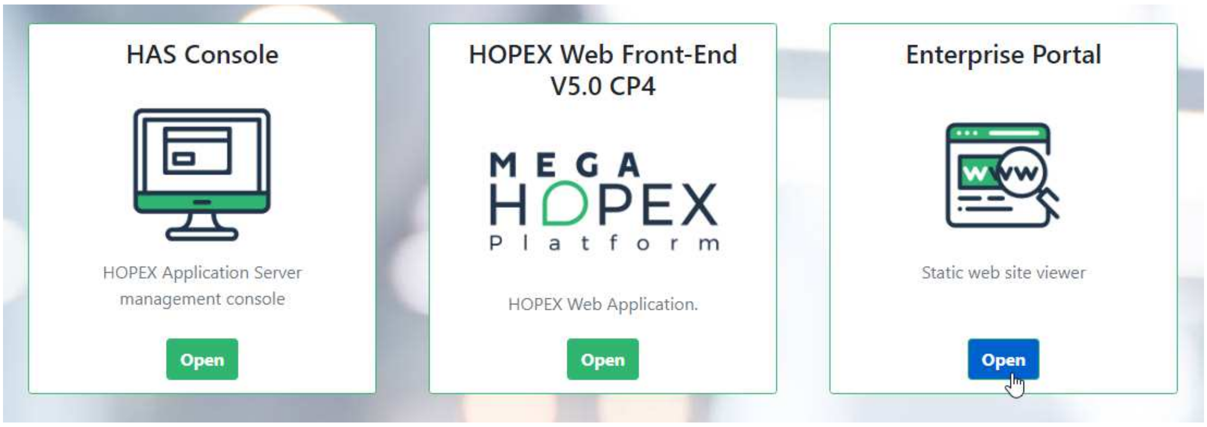
9.2.1. Publish In HAS Instance

For this scenario either:

- From the **HOPEX Store**, download the Enterprise Portal Application package https://store.mega.com/modules/details/website.static.navigator.bundle
- From the **HAS Console > Modules**, install the "Enterprise Portal Application package" module.

Follow the instruction from the store and read the Read.me file located here C:\...\HOPEX Application Server\...\.shadowFiles\website.static.content

When your static website is generated, it can be accessed from the HAS portal or directly from the URL https://www.myurl.com/website.static.navigator

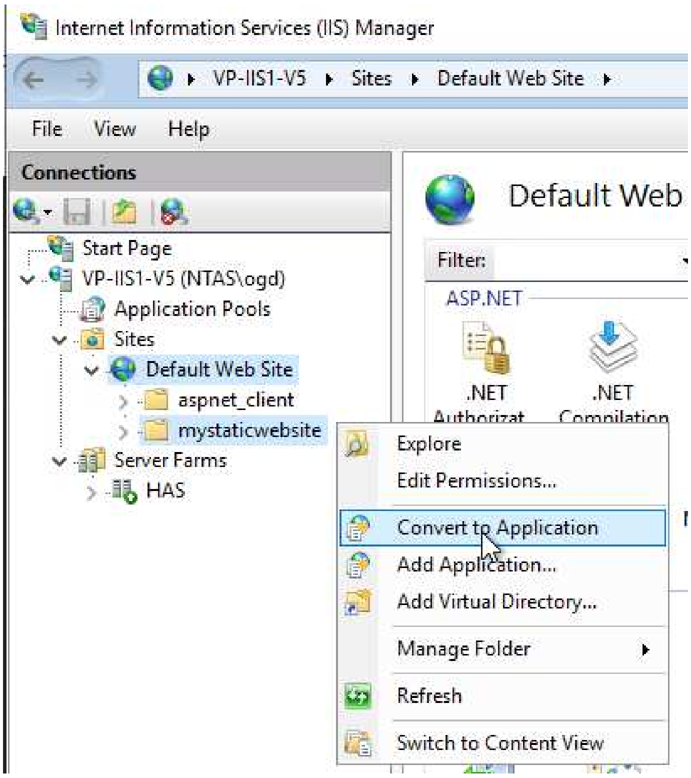


9.2.2. Publish In IIS

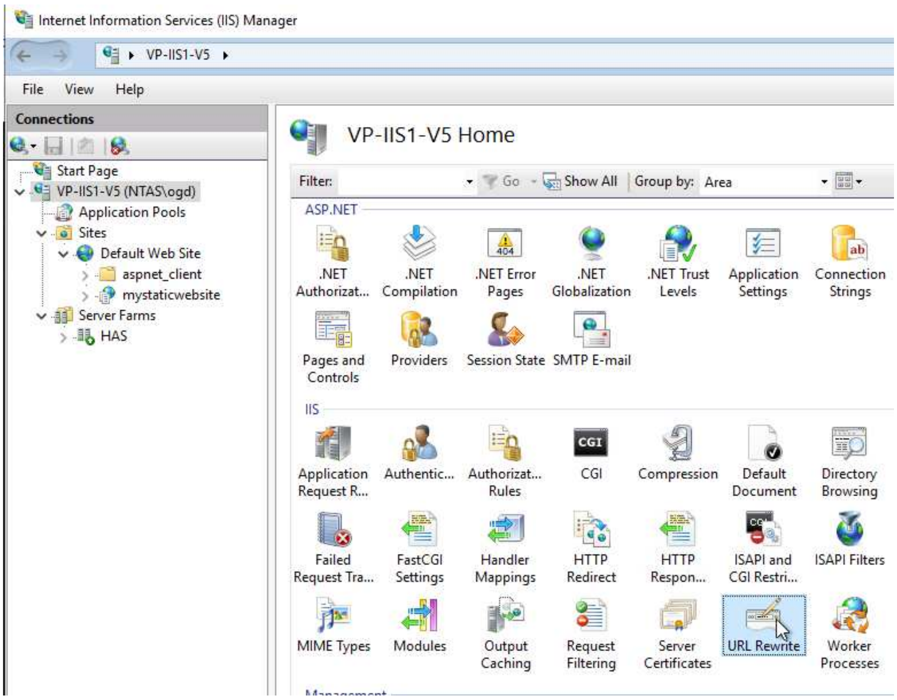
In this scenario you generate your static website and then manually publish it on IIS. You need to configure IIS to enable user to access this website.

To configure IIS:

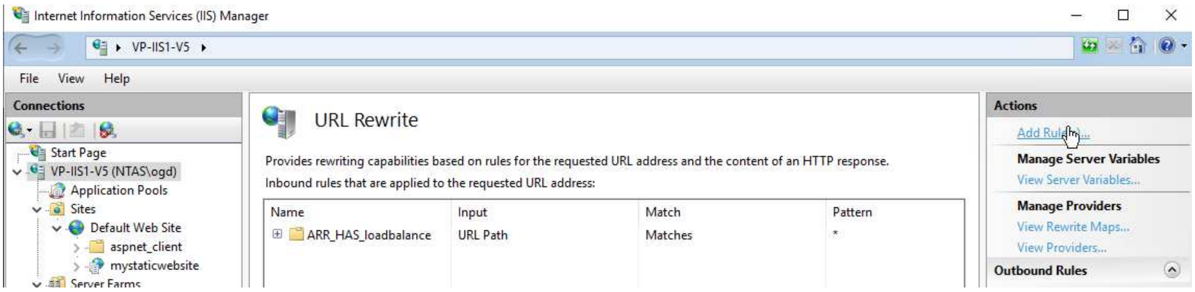
1. Create your IIS Application from the folder by converting it to Application.



2. In **IIS**, go to root level and double-click **URL Rewrite**.



3. Click **Add Rule**.

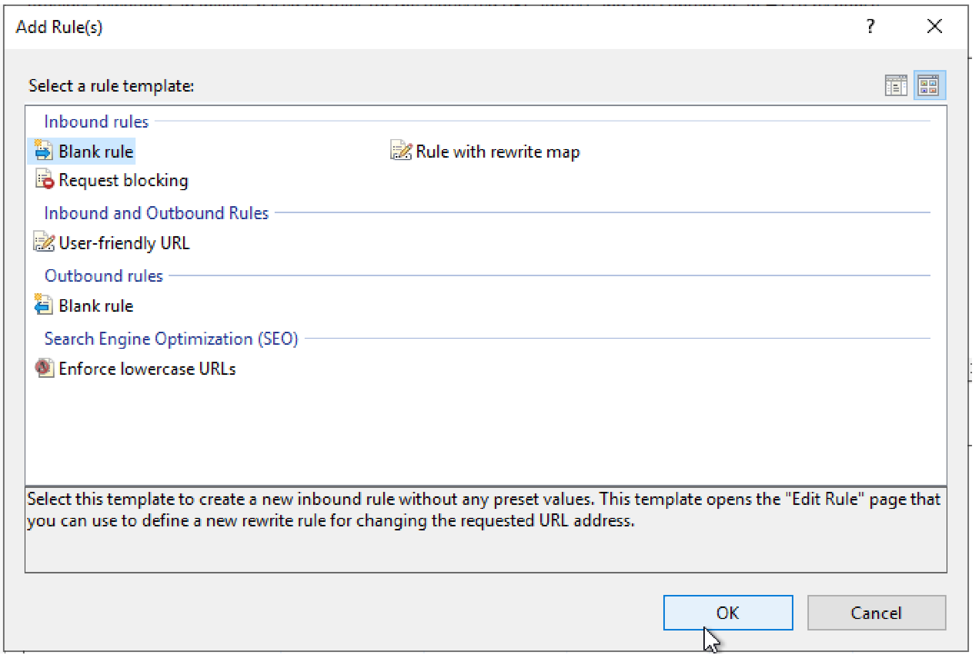


Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern
ARR_HAS_loadbalance	URL Path	Matches	*

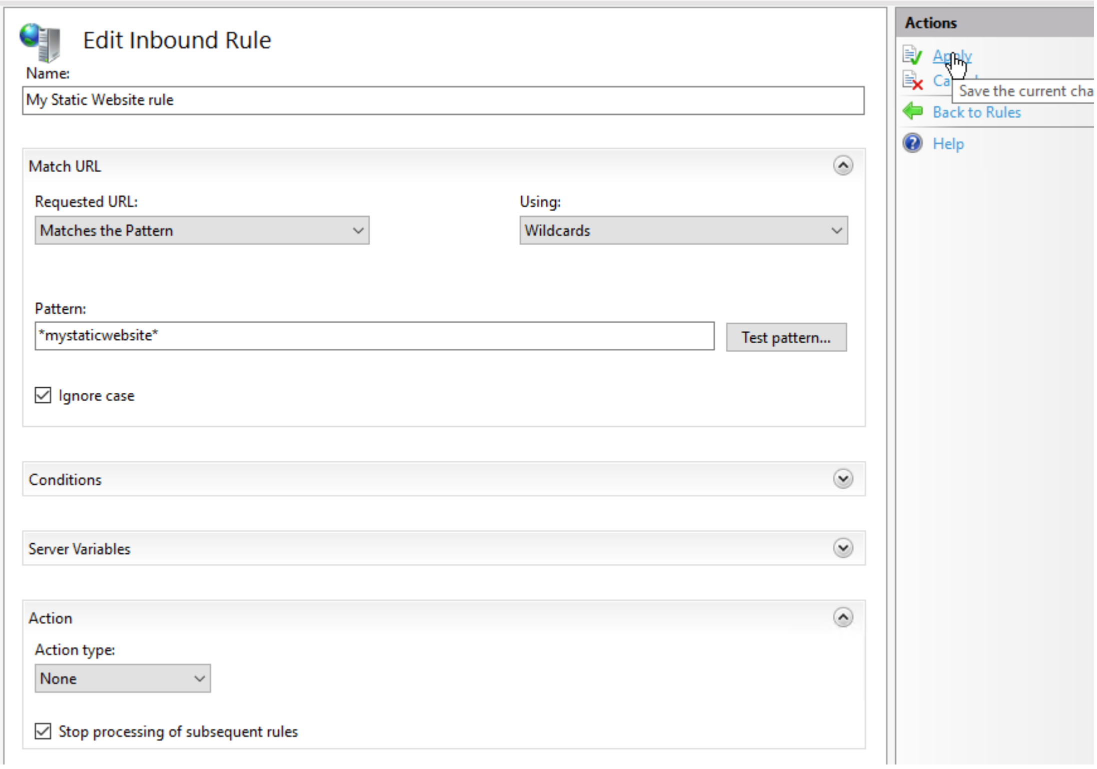
4. Select **Blank Rule**.



Select this template to create a new inbound rule without any preset values. This template opens the "Edit Rule" page that you can use to define a new rewrite rule for changing the requested URL address.

5. Click **OK**.

6. Fill in the rule
   - **Name**
   - **Using**: “Wildcard”
   - **Pattern:** “*mystaticwebsite*” where mystaticwebsite is the name of the folder in IIS of your website
   - **Action Type**: “None”
   - Select **Stop processing subsequent rule**.
   - Click **Apply**.



Edit Inbound Rule

Name: My Static Website rule

Match URL

Requested URL: Matches the Pattern

Using: Wildcards

Pattern: *mystaticwebsite*

☑ Ignore case

Conditions

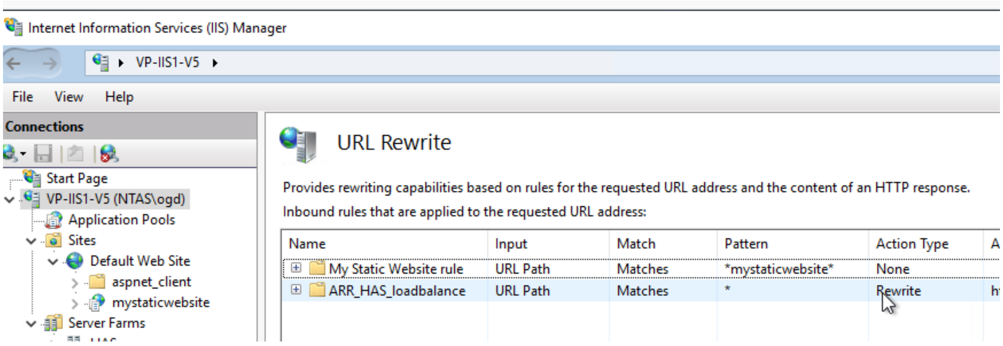
Server Variables

Action

Action type: None

☑ Stop processing of subsequent rules

7. In the list of rules select the rule you just created.



Internet Information Services (IIS) Manager

URL Rewrite

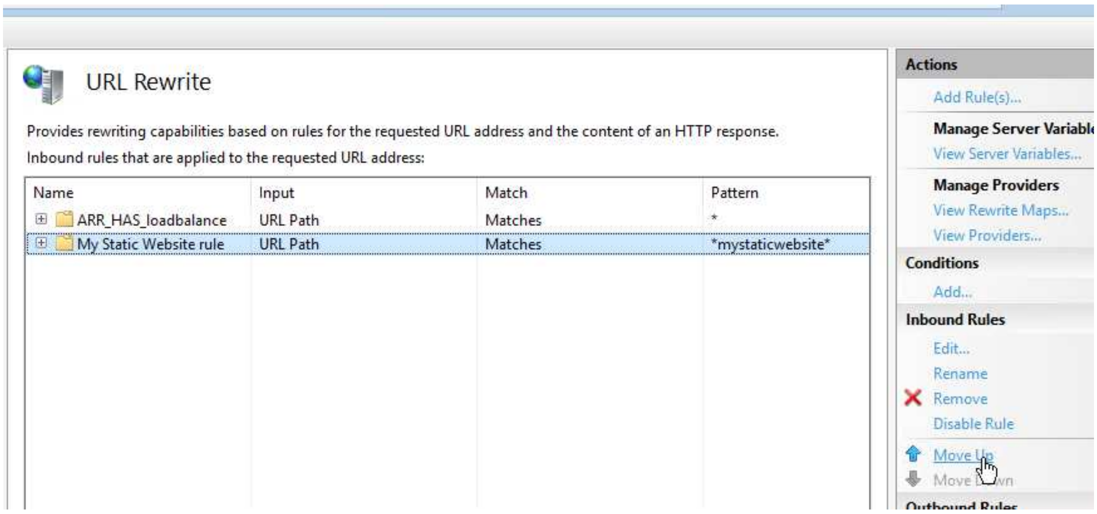
Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	A
My Static Website rule	URL Path	Matches	*mystaticwebsite*	None	
ARR_HAS_loadbalance	URL Path	Matches	*	Rewrite	h

8. Click **Move Up** until your rule is at the top of the list.

9. Access your static website from your preferred web browser. For example: https://www.myurl.com/mystaticwebsite



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern
ARR_HAS_loadbalance	URL Path	Matches	*
My Static Website rule	URL Path	Matches	*mystaticwebsite*

10. Post installation checklist

Review this checklist before calling MEGA support.

Ensure each line is marked as "**done**". For each item where the status is "**not done**", refer to the appropriate section to fix it.

	Layer	Action to check	Status
1	SQL Server	**Microsoft SQL Server** version: **2019** or **2022**	
2	SQL Server	The port used by SQL Server: TCP 1433 UDP1434	
3	SQL Server	Does SQL Server use encrypt connection?	
4	SQL Server	Does SQL user is properly defined?	
	Repeat for each server		
10	IIS Server	**Windows Server** version: **2016** or **2019** or **2022**	
11	IIS Server	SSL Certificate validity date *(if HTTPS/SSL)*	
12	IIS Server	URL based on certificate is the same as on the web browser	
13	IIS Server	IIS Default Website Binding port is 80 or 443	
14	IIS Server	HAS Server farm exist	
15	IIS Server	All HAS Server are present in the HAS Server Farm	
16	IIS Server	Health test URL is defined	
17	IIS Server	Proxy timeout value is set to 120s	
18	IIS Server	There is a URL rewrite rule for the server farm	
19	IIS Server	There is an URL rewrite rule condition with HTTP_HOST	
20	IIS Server	The URL rewrite rule is in HTTP or HTTPS	
21	IIS Server	Ensure HTTP(S) is the same on URL Rewrite, Binding and Health	
22	IIS Server	Testing the URL DNS work as described in chapter 7.1	
23	IIS Server	Testing server communication work as described in chapter 7.2	
243	IIS Server	Testing SSL Certificate works as described in chapter 7.3	
	Repeat for each server		
30	HAS Server	**Windows Server** version: **2016** or **2019** or **2022**	
31	HAS Server	.NET 8 **Hosting Bundle** is installed	
32	HAS Server	.NET 8 SDK is installed for **DEV** Server	
33	HAS Server	.NET Framework **4.8** is installed	
34	HAS Server	C++ Redistributable **x64** 2015-2022 is installed	
35	HAS Server	Ensure **SMB** is enabled / File Server	
36	HAS Server	ODBC Driver 17 or 18 for SQL Server x64 is installed	
37	HAS Server	non-interactive **Desktop Heap** min. value: **8192**	
38	HAS Server	The server has access to the store web URL (optional)	
39	HAS Server	HAS Instance Manager service in present	
40	HAS Server	HAS Instance Manager service is launched by domain user or Local System	
41	HAS Server	HAS Instance Manager is accessible http://localhost:30100	
42	HAS Server	The domain user is local Administrator of the server	
43	HAS Server	The domain user as access to share folder (license & Env.)	
44	HAS Server	The instance is created and running in Instance Manager	
45	HAS Server	The instance is properly deployed in 5000 folder.	
46	HAS Server	The instance internal URL is responding	
47	HAS Server	The public URL written in the web browser is the same as in the SSL certificate and the same as in the settings.cfg	
48	HAS Server	All settings.cfg file are identical across all HAS Server	
49	HAS Server	All cluster.cfg file are identical across all HAS Server	
50	HAS Server	Testing HAS work as described in chapter 7.4	
51	HAS Server	Testing Web client work as described in chapter 7.5	
52	HAS Server	Testing Desktop client work as described in chapter 7.6	
60	Client Laptop	You have **Chrome/Firefox/Edge** in supported version	

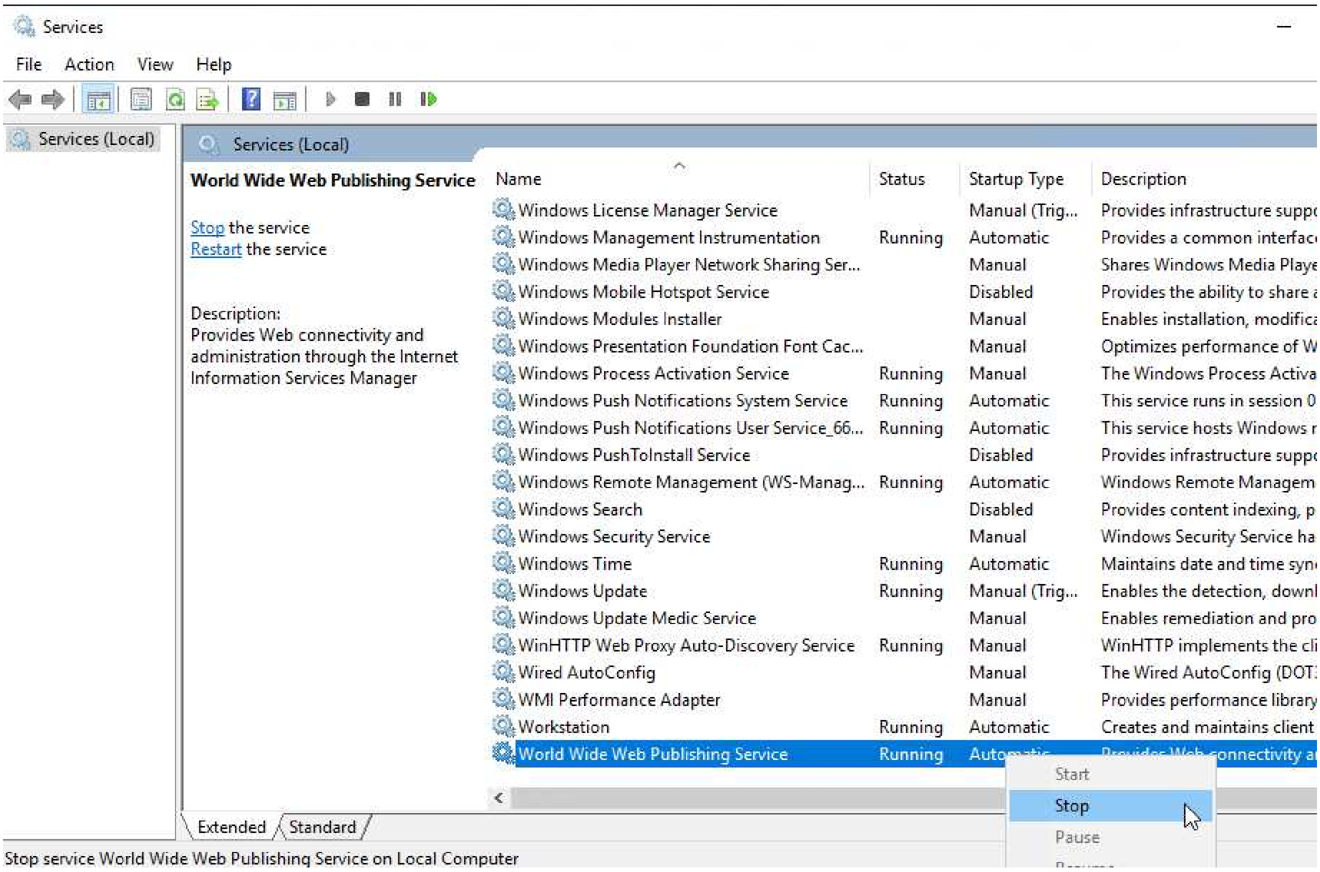
	Layer	Action to check	Status
61	Client Laptop	You have Office tools Word (optional)	

11. Uninstallation procedure

Should you want to remove HOPEX to make a clean re-install please follow the instructions below.

11.1. Removing IIS

Ensure IIS service is stopped prior to start these steps.



World Wide Web Publishing Service

Stop the service
Restart the service

Description:
Provides Web connectivity and administration through the Internet Information Services Manager

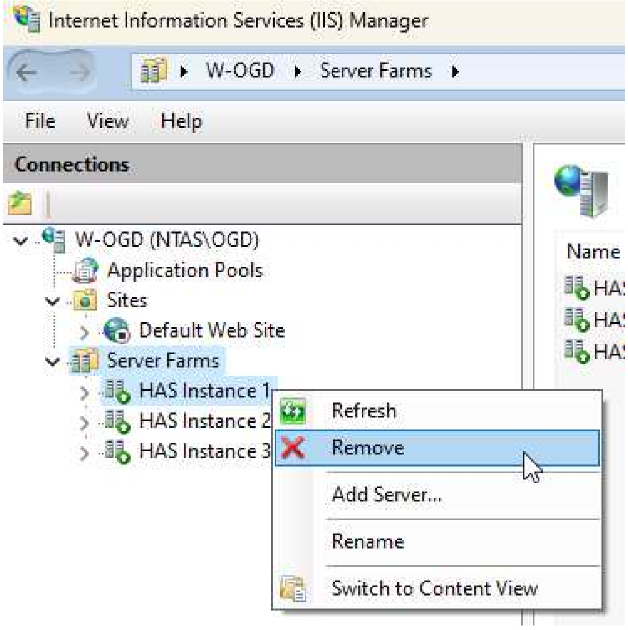
Name	Status	Startup Type	Description
Windows License Manager Service		Manual (Trig...	Provides infrastructure suppo
Windows Management Instrumentation	Running	Automatic	Provides a common interfac
Windows Media Player Network Sharing Ser...		Manual	Shares Windows Media Playe
Windows Mobile Hotspot Service		Disabled	Provides the ability to share a
Windows Modules Installer		Manual	Enables installation, modifica
Windows Presentation Foundation Font Cac...		Manual	Optimizes performance of W
Windows Process Activation Service	Running	Manual	The Windows Process Activa
Windows Push Notifications System Service	Running	Automatic	This service runs in session 0
Windows Push Notifications User Service_66...	Running	Automatic	This service hosts Windows r
Windows PushToInstall Service		Disabled	Provides infrastructure suppo
Windows Remote Management (WS-Manag...	Running	Automatic	Windows Remote Managem
Windows Search		Disabled	Provides content indexing, p
Windows Security Service		Manual	Windows Security Service ha
Windows Time	Running	Automatic	Maintains date and time syn
Windows Update	Running	Manual (Trig...	Enables the detection, downl
Windows Update Medic Service		Manual	Enables remediation and pro
WinHTTP Web Proxy Auto-Discovery Service	Running	Manual	WinHTTP implements the cli
Wired AutoConfig		Manual	The Wired AutoConfig (DOT:
WMI Performance Adapter		Manual	Provides performance library
Workstation	Running	Automatic	Creates and maintains client
World Wide Web Publishing Service	Running	Automatic	Provides Web connectivity a

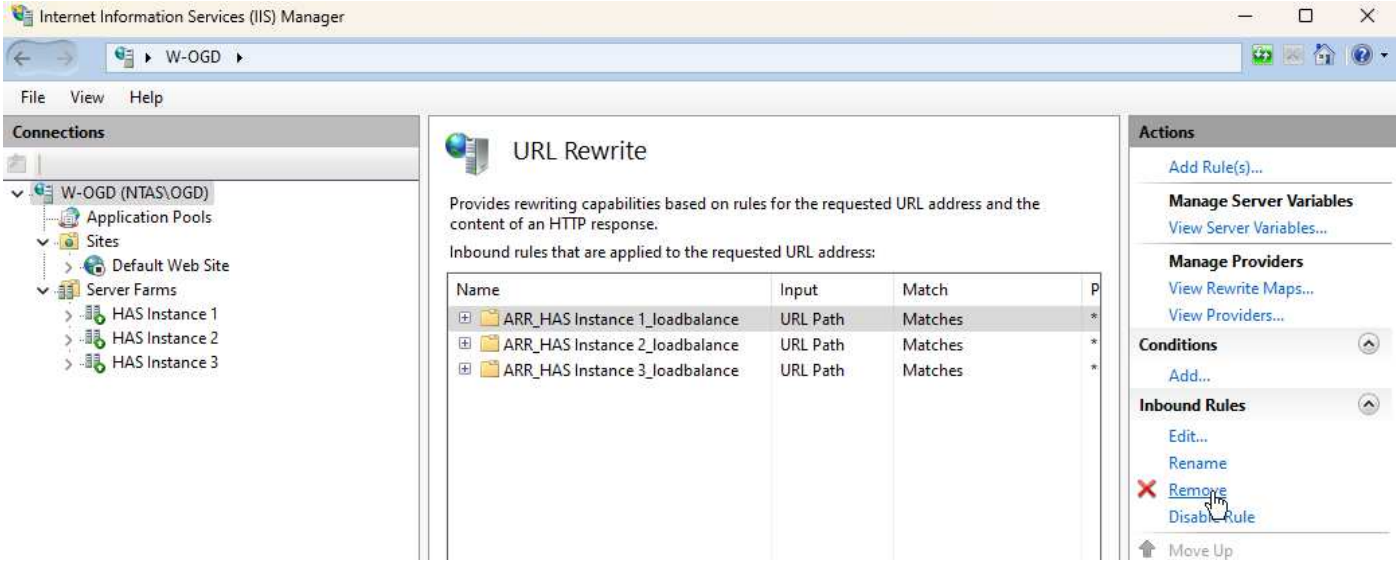
Stop service World Wide Web Publishing Service on Local Computer

11.1.1. Configuration removal

From IIS Manager remove all configurations that you have performed:

- Remove the server Farms
- Remove any rewrite rules you have created
- Remove any custom binding you have set

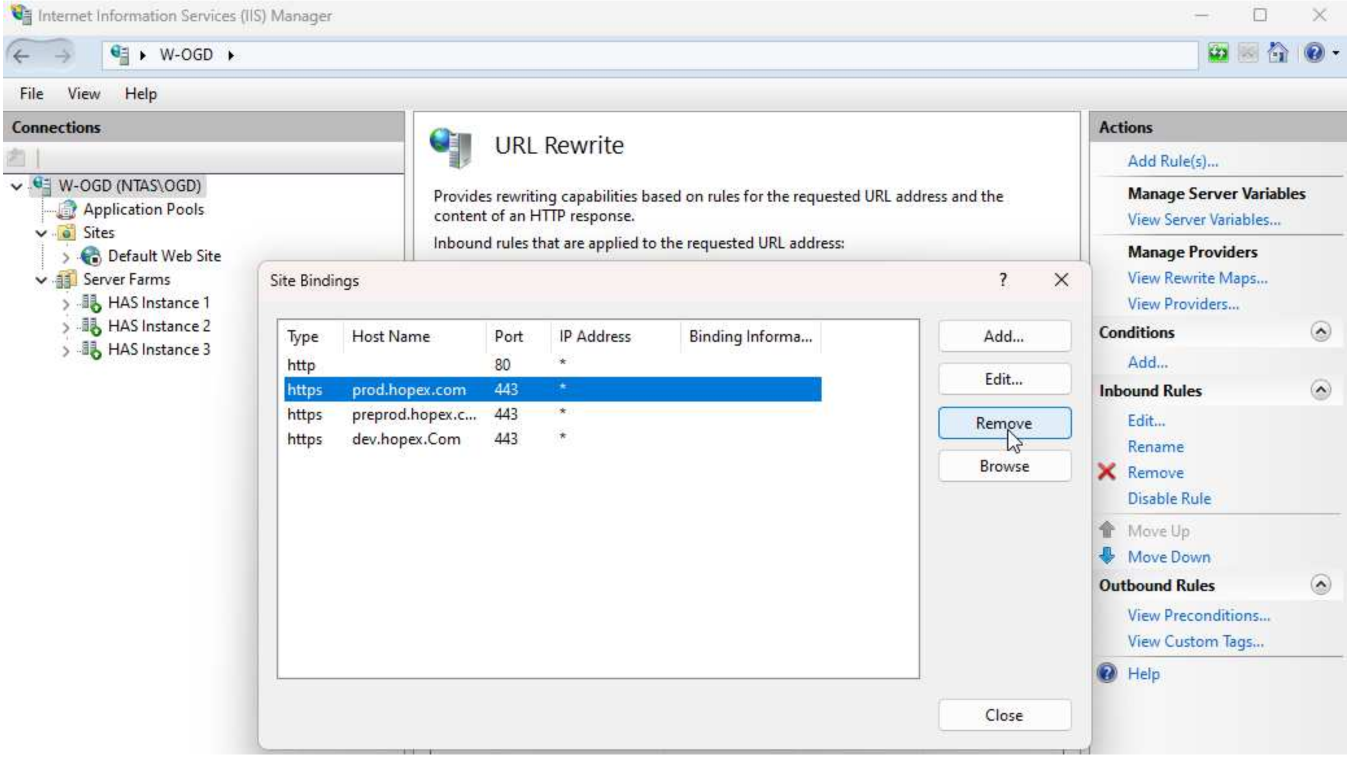




Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	P
ARR_HAS Instance 1_loadbalance	URL Path	Matches	*
ARR_HAS Instance 2_loadbalance	URL Path	Matches	*
ARR_HAS Instance 3_loadbalance	URL Path	Matches	*



Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

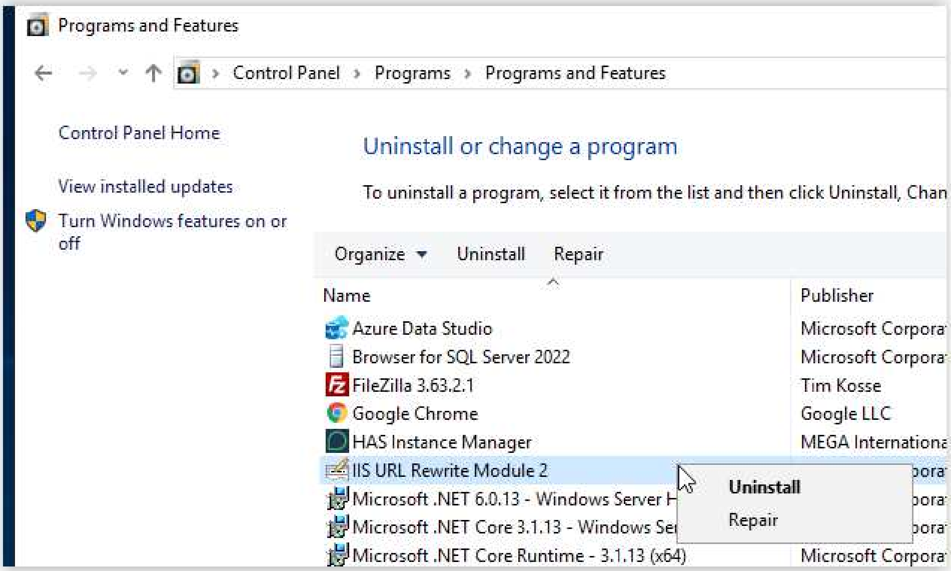
Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https	prod.hopex.com	443	*	
https	preprod.hopex.c...	443	*	
https	dev.hopex.Com	443	*	

11.1.2. Prerequisite removal (optional)

Should you want to fully reset the prerequisite component installed you can:

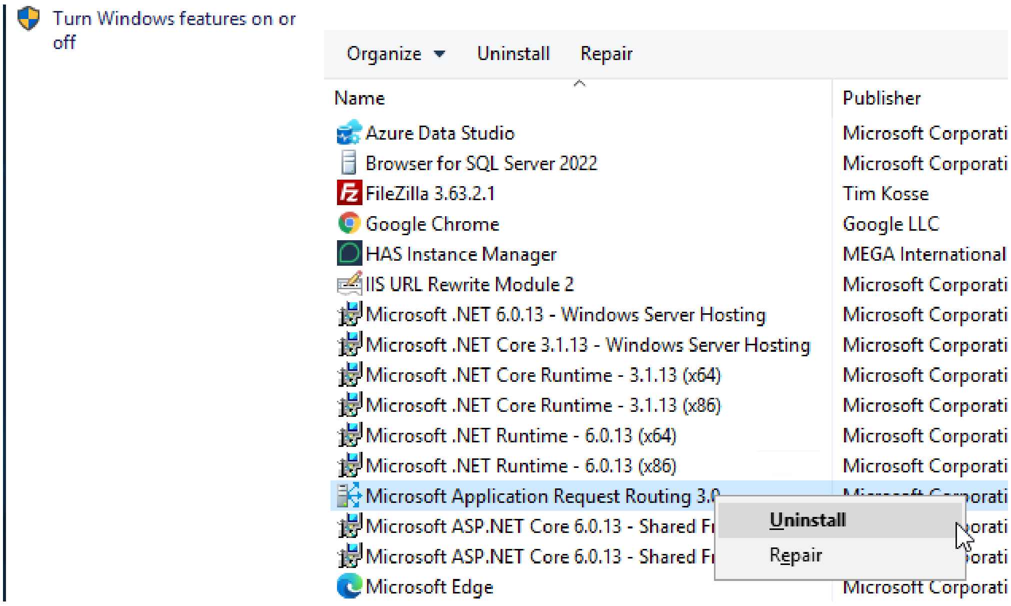
- Uninstall URL rewrite
- Uninstall ARR
- Uninstall IIS

Note: IIS, ARR and URL Rewrite might store configuration files that may not be removed when uninstalling.


Programs and Features
Control Panel › Programs › Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
Organize
Uninstall
Repair
Uninstall
Repair

To uninstall a program, select it from the list and then click Uninstall, Chan

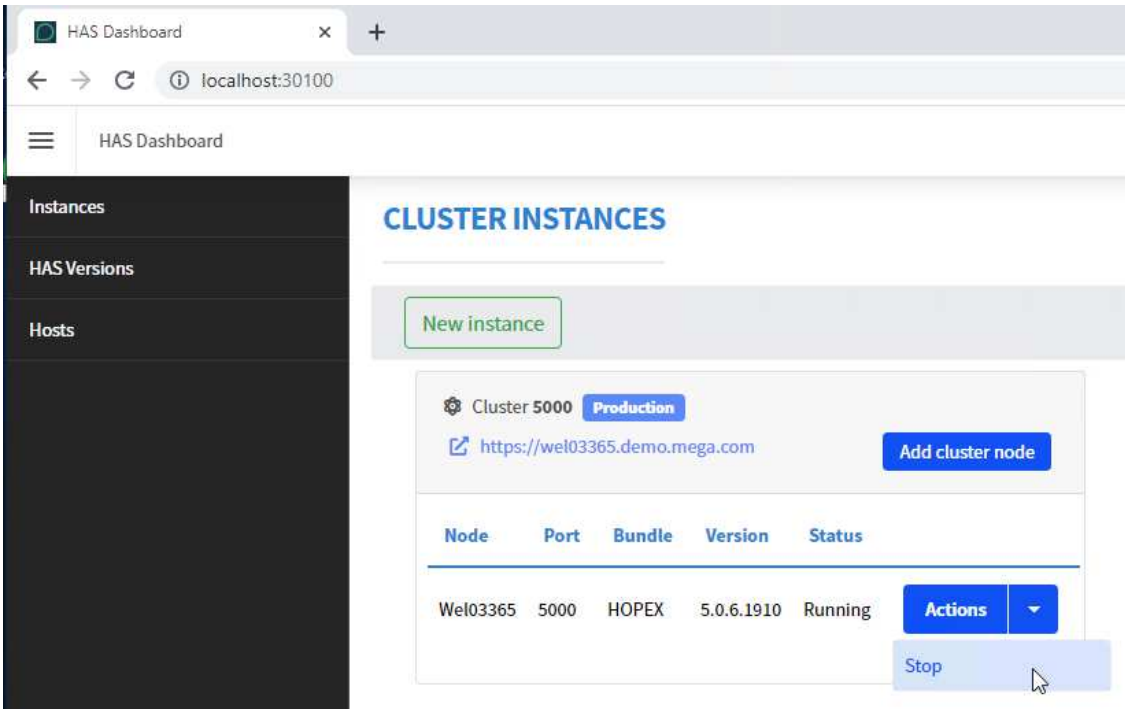
Name	Publisher
Azure Data Studio	Microsoft Corpora
Browser for SQL Server 2022	Microsoft Corpora
FileZilla 3.63.2.1	Tim Kosse
Google Chrome	Google LLC
HAS Instance Manager	MEGA Internationa
IIS URL Rewrite Module 2	pora
Microsoft .NET 6.0.13 - Windows Server H	pora
Microsoft .NET Core 3.1.13 - Windows Se	pora
Microsoft .NET Core Runtime - 3.1.13 (x64)	Microsoft Corpora


Turn Windows features on or off
Organize
Uninstall
Repair
Name
Publisher
Azure Data Studio
Microsoft Corporati
Browser for SQL Server 2022
Microsoft Corporati
FileZilla 3.63.2.1
Tim Kosse
Google Chrome
Google LLC
HAS Instance Manager
MEGA International
IIS URL Rewrite Module 2
Microsoft Corporati
Microsoft .NET 6.0.13 - Windows Server Hosting
Microsoft Corporati
Microsoft .NET Core 3.1.13 - Windows Server Hosting
Microsoft Corporati
Microsoft .NET Core Runtime - 3.1.13 (x64)
Microsoft Corporati
Microsoft .NET Core Runtime - 3.1.13 (x86)
Microsoft Corporati
Microsoft .NET Runtime - 6.0.13 (x64)
Microsoft Corporati
Microsoft .NET Runtime - 6.0.13 (x86)
Microsoft Corporati
Microsoft Application Request Routing 3.0
Microsoft ASP.NET Core 6.0.13 - Shared Fr
Microsoft ASP.NET Core 6.0.13 - Shared Fr
Microsoft Edge
Microsoft Corporati
Uninstall
Repair

11.2. Removing HOPEX applications

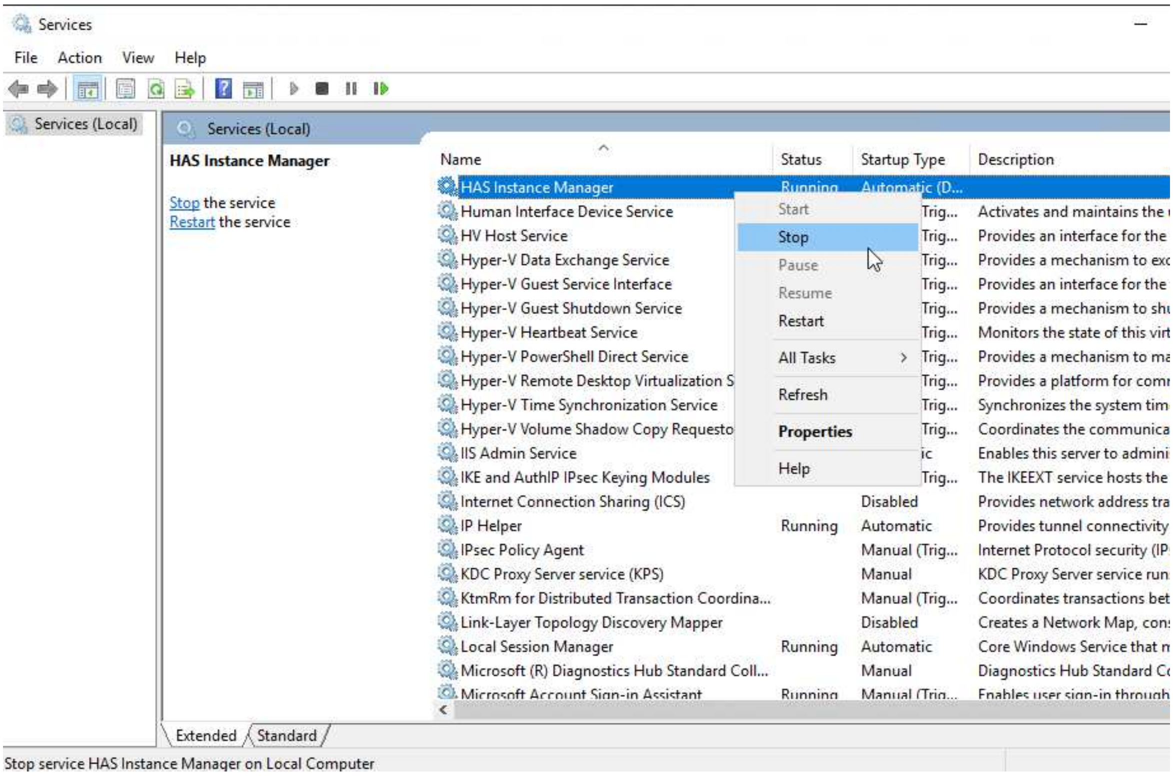
Ensure HAS Instance and HAS Instance Manager are stopped prior to start these steps:

- Stop the instance within the HAS instance manager



Node	Port	Bundle	Version	Status
Wel03365	5000	HOPEX	5.0.6.1910	Running

- Stop the HAS Instance manager service within Windows service manager



HAS Instance Manager

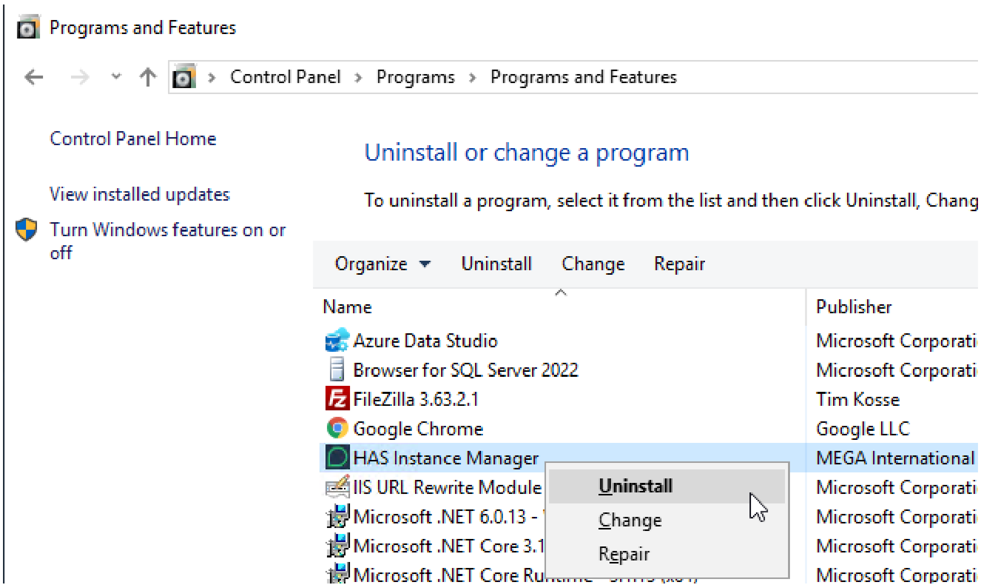
Stop the service
Restart the service

Name	Status	Startup Type	Description
HAS Instance Manager	Running	Automatic (D...	
Human Interface Device Service		Trig...	Activates and maintains the
HV Host Service		Trig...	Provides an interface for the
Hyper-V Data Exchange Service		Trig...	Provides a mechanism to exc
Hyper-V Guest Service Interface		Trig...	Provides an interface for the
Hyper-V Guest Shutdown Service		Trig...	Provides a mechanism to shu
Hyper-V Heartbeat Service		Trig...	Monitors the state of this virt
Hyper-V PowerShell Direct Service		Trig...	Provides a mechanism to ma
Hyper-V Remote Desktop Virtualization S		Trig...	Provides a platform for comr
Hyper-V Time Synchronization Service		Trig...	Synchronizes the system tim
Hyper-V Volume Shadow Copy Requesto		Trig...	Coordinates the communica
IIS Admin Service		ic	Enables this server to admini
IKE and AuthIP IPsec Keying Modules		Trig...	The IKEEXT service hosts the
Internet Connection Sharing (ICS)		Disabled	Provides network address tra
IP Helper	Running	Automatic	Provides tunnel connectivity
IPsec Policy Agent		Manual (Trig...	Internet Protocol security (IP
KDC Proxy Server service (KPS)		Manual	KDC Proxy Server service run
KtmRm for Distributed Transaction Coordina...		Manual (Trig...	Coordinates transactions bet
Link-Layer Topology Discovery Mapper		Disabled	Creates a Network Map, con:
Local Session Manager	Running	Automatic	Core Windows Service that r
Microsoft (R) Diagnostics Hub Standard Coll...		Manual	Diagnostics Hub Standard Co
Microsoft Account Sign-in Assistant	Running	Manual (Trig...	Enables user sign-in through

Stop service HAS Instance Manager on Local Computer

11.2.1. Uninstalling Application

1. From Control Panel >> Programs >> Programs and Features select “Uninstall or change program.
2. Search for HAS Instance Manager and uninstall.



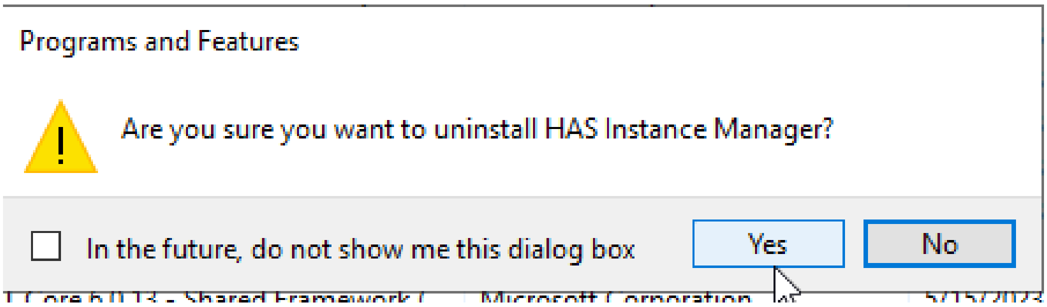
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Chang

Name	Publisher
Azure Data Studio	Microsoft Corporati
Browser for SQL Server 2022	Microsoft Corporati
FileZilla 3.63.2.1	Tim Kosse
Google Chrome	Google LLC
HAS Instance Manager	MEGA International
IIS URL Rewrite Module	Microsoft Corporati
Microsoft .NET 6.0.13 -	Microsoft Corporati
Microsoft .NET Core 3.1	Microsoft Corporati
Microsoft .NET Core Ru	Microsoft Corporati

3. When prompted click **Yes**.

   If you did not stop prior the HAS Instance Manager, you will be asked to stop it.



Programs and Features

Are you sure you want to uninstall HAS Instance Manager?

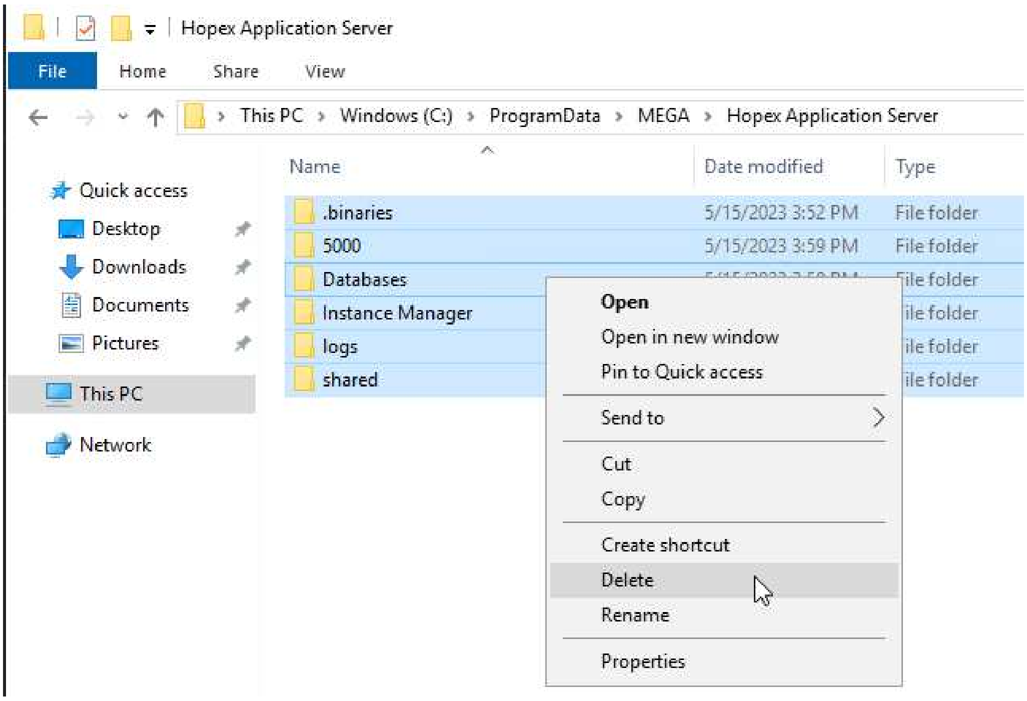
□ In the future, do not show me this dialog box

11.2.2. Deleting files

1. Open a Windows file explorer and go to the installation location.

   Default: C:\ProgramData\MEGA\Hopex Application Server

2. Select all folders and files and delete them.

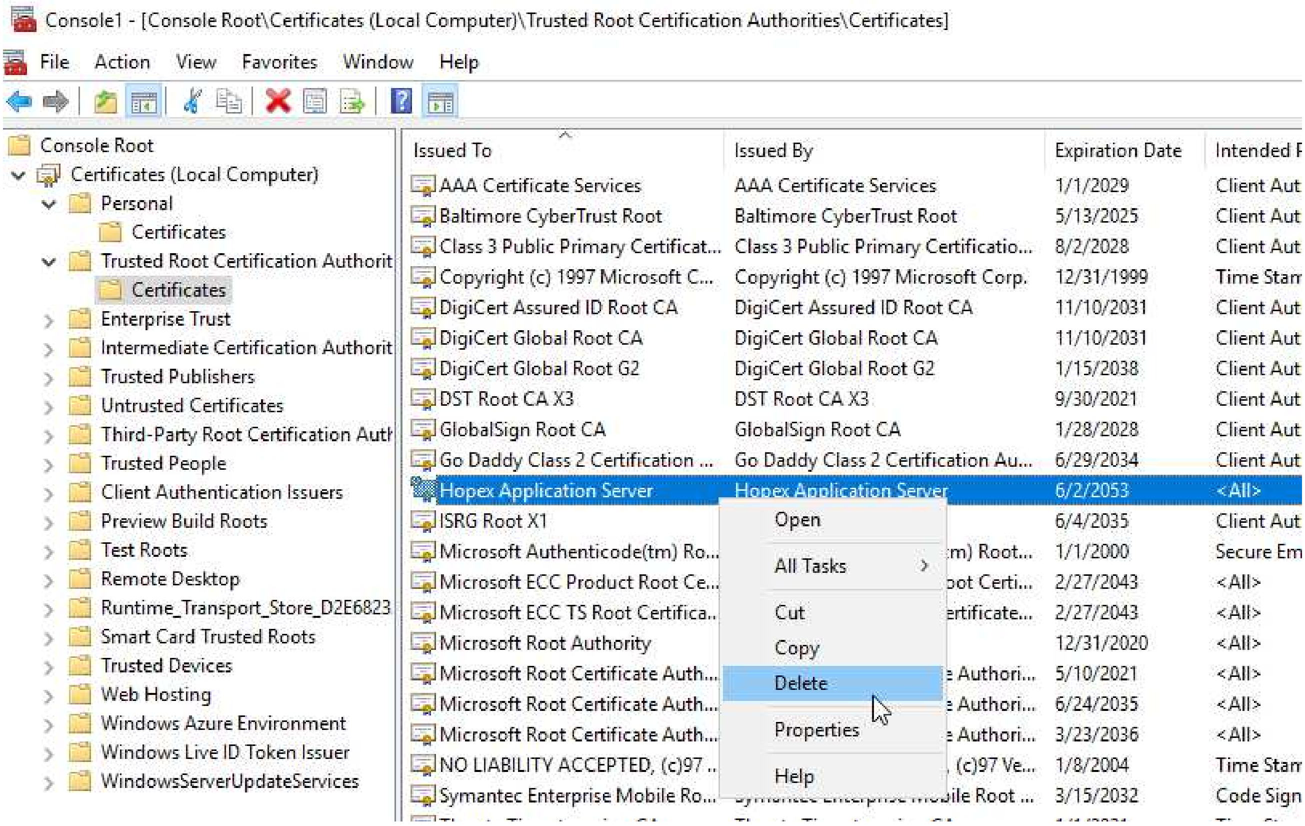


Name	Date modified	Type
.binaries	5/15/2023 3:52 PM	File folder
5000	5/15/2023 3:59 PM	File folder
Databases		File folder
Instance Manager		File folder
logs		File folder
shared		File folder

If you did not stop the HAS instance you won't be able to delete all files. Restart the server and retry.

11.2.3. Removing SSL Certificate

1. Open an MMC console and add Certificates snap-in.
2. In **Trusted Root Certification Authorities** search for **Hopex Application Server** or custom SSL certificate you may have used.
3. **Delete** it.



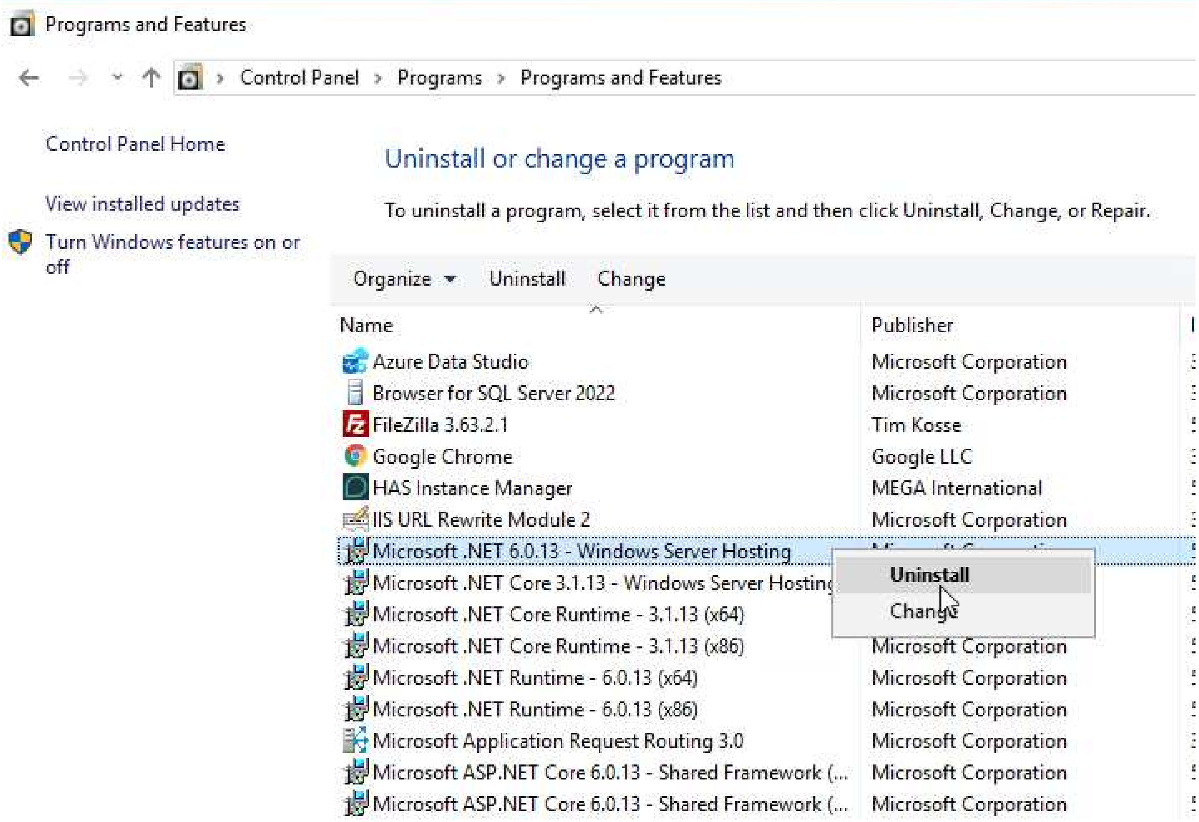
Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended F
AAA Certificate Services	AAA Certificate Services	1/1/2029	Client Aut
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Client Aut
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028	Client Aut
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stam
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	Client Aut
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031	Client Aut
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Aut
DST Root CA X3	DST Root CA X3	9/30/2021	Client Aut
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Aut
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Client Aut
Hopex Application Server	Hopex Application Server	6/2/2053	<All>
ISRG Root X1		6/4/2035	Client Aut
Microsoft Authenticode(tm) Ro...	m) Root...	1/1/2000	Secure Em
Microsoft ECC Product Root Ce...	oot Certi...	2/27/2043	<All>
Microsoft ECC TS Root Certifica...	ertificate...	2/27/2043	<All>
Microsoft Root Authority		12/31/2020	<All>
Microsoft Root Certificate Auth...	Authori...	5/10/2021	<All>
Microsoft Root Certificate Auth...	Authori...	6/24/2035	<All>
Microsoft Root Certificate Auth...	Authori...	3/23/2036	<All>
NO LIABILITY ACCEPTED, (c)97 ...	, (c)97 Ve...	1/8/2004	Time Stam
Symantec Enterprise Mobile Ro...	...ile Root ...	3/15/2032	Code Sign

11.2.4. Uninstalling prerequisites (optional)

If not used by any other component, you can also uninstall the prerequisites to clean your server.

1. From Control Panel > Programs > Programs and Features, select **Uninstall or change a program**.
2. Delete any Microsoft .NET 3.1, 6.0, or 8.0: Windows Server Hosting Bundle, SDK, Core Runtime…



Programs and Features

Control Panel › Programs › Programs and Features

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher
Azure Data Studio	Microsoft Corporation
Browser for SQL Server 2022	Microsoft Corporation
FileZilla 3.63.2.1	Tim Kosse
Google Chrome	Google LLC
HAS Instance Manager	MEGA International
IIS URL Rewrite Module 2	Microsoft Corporation
Microsoft .NET 6.0.13 - Windows Server Hosting	
Microsoft .NET Core 3.1.13 - Windows Server Hosting	
Microsoft .NET Core Runtime - 3.1.13 (x64)	
Microsoft .NET Core Runtime - 3.1.13 (x86)	Microsoft Corporation
Microsoft .NET Runtime - 6.0.13 (x64)	Microsoft Corporation
Microsoft .NET Runtime - 6.0.13 (x86)	Microsoft Corporation
Microsoft Application Request Routing 3.0	Microsoft Corporation
Microsoft ASP.NET Core 6.0.13 - Shared Framework (...	Microsoft Corporation
Microsoft ASP.NET Core 6.0.13 - Shared Framework (...	Microsoft Corporation

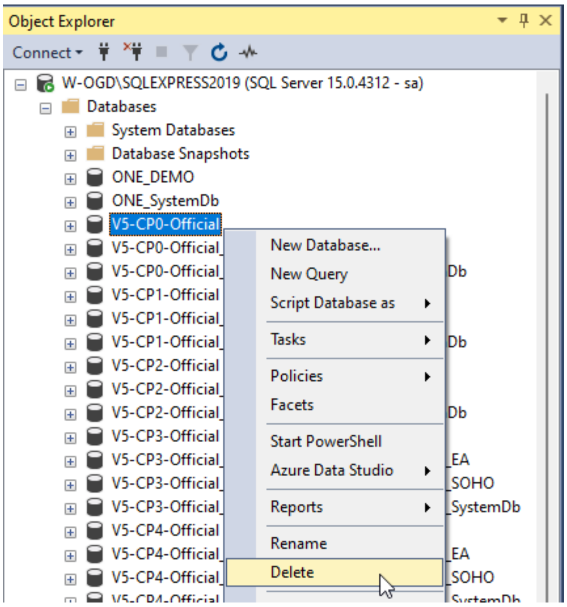
11.3. Removing RDBMS databases

You may want also to delete:

- The HAS Instance database that contains all the configuration
- The Environment SystemDB and Repositories: **only** if you don't want to use HOPEX anymore forever.

From your preferred tool delete the instance database.

Default name: HAS_5000



12. FAQ

12.1.1. How to reset HAS Instance Manager API Key / password ?

The information is stored in the hopex.yml file located by default here: C:\...\HOPEX Application Server\Instance Manager

1. Stop HAS Instance manager.
2. Edit the HOPEX.yml file.
3. Edit the ApiKey section and enter your new password.
4. Restart HAS Instance manager.

12.1.2. What are the default user's login/password?

For HAS Instance the default user is: admin with password Hopex that you need to change at first connection.

12.1.3. Do I need IIS Application pool?

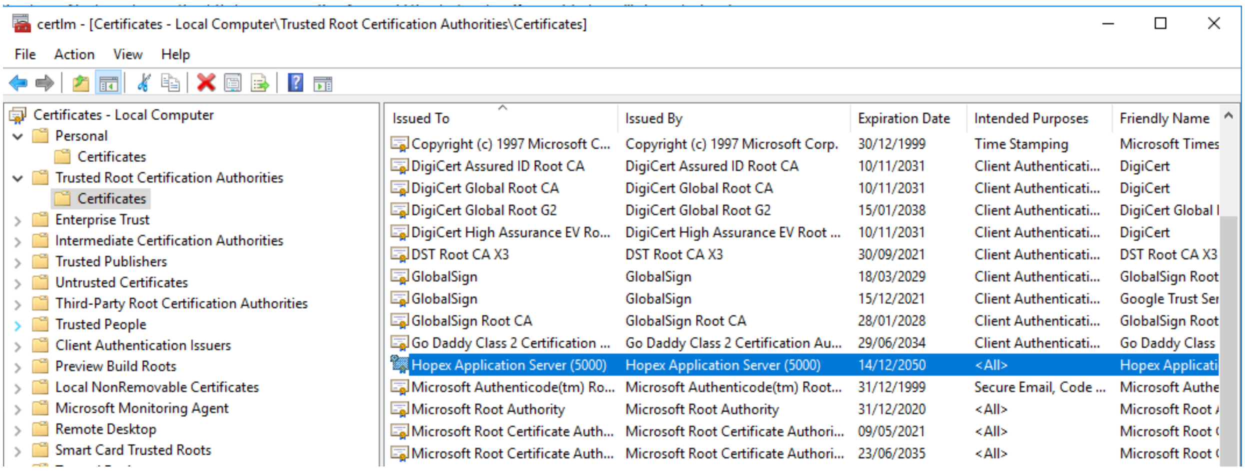
No

12.1.4. Access rights to certificate at installation is no valid.

When you install HAS and HAS modules are not starting. If you see the following message in HAS-Starting log:

[Error] - Failed to create certificate request. It is often due to an access denied to the CA certificate. Keyset does not exist

Go to your certificate and delete "Hopex Application Server (5000)". Restart HAS Server. If the certificate does not appear check domain user access right.



certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]

File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Local NonRemovable Certificates
Microsoft Monitoring Agent
Remote Desktop
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	30/12/1999	Time Stamping	Microsoft Times
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Client Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Client Authenticati...	DigiCert Global I
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10/11/2031	Client Authenticati...	DigiCert
DST Root CA X3	DST Root CA X3	30/09/2021	Client Authenticati...	DST Root CA X3
GlobalSign	GlobalSign	18/03/2029	Client Authenticati...	GlobalSign Root
GlobalSign	GlobalSign	15/12/2021	Client Authenticati...	Google Trust Ser
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Client Authenticati...	GlobalSign Root
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29/06/2034	Client Authenticati...	Go Daddy Class
Hopex Application Server (5000)	Hopex Application Server (5000)	14/12/2050	<All>	Hopex Applicati
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	31/12/1999	Secure Email, Code ...	Microsoft Authe
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<All>	Microsoft Root /
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	09/05/2021	<All>	Microsoft Root (
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/06/2035	<All>	Microsoft Root (

12.1.5. When should I restart HAS Instance or HAS Instance Manager?

HAS Instance manager does not restart the instance.

Each HAS Instance can be restarted by the HAS Instance manager or the HAS Instance itself.

12.1.6. Can I limit the role of a node in a cluster?

Should you have a cluster with several HAS you may want to limit the usage of a node to server batch.

For each server:

1. Access the HAS console.
2. In the navigation menus, select **Modules > Modules Settings**.
3. Click ✎ **Edit Cluster Configuration**.
4. In the **Tags** field, configure each node as required.
   Add “!back” or “!Jobs” to remove these roles.

   For example, enter the following to dedicate the batch tasks to node 1 only:

   For Node 1 (https://vp-has1-v5:5000) dedicated to the jobs, **Tags**: “!back”

   For Node 2 (https://vp-has2-v5:5000) no jobs, **Tags**: “!Jobs”

   For Node 3 (https://vp-has3-v5:5000) no jobs, **Tags**: “!Jobs”

Alternative: for each server, edit the cluster.cfg file to add the tag: “!back” or “!Jobs”.

```
[
  {
    "address": "https://vp-has1-v5:5000",
    "tags": ["!Back"],
    "hostName": "VP-HAS1-V5",
    "port": 5000
  },
  {
    "address": "https://vp-has2-v5:5000",
    "tags": ["!Jobs"],
    "hostName": "VP-HAS2-v5",
    "port": 5000
  }

  {
    "address": "https://vp-has3-v5:5000",
    "tags": ["!Jobs"],
    "hostName": "VP-HAS3-v5",
    "port": 5000
  }
]
```

How to Migrate to Hopex Aquila 6.2

1. Summary

This document is a guideline for migration to Aquila once the project has decided to migrate to Hopex Aquila (Hopex V6.2).

Before making this decision, it is essential to review the release note web site https://releasenotes.saas.mega.com

Migration is allowed with a specific CP for source and target version.

Source version	**Target version** **(direct migration path)**
HOPEX V4.0 CP7	Hopex Aquila V6.2 **last hotfix**
HOPEX V5.0 CP3/CP4/CP5/CP6/CP7/CP8/CP9	Hopex Aquila V6.2 **last hotfix**
Hopex Aquila V6.0 RTM/SP1/SP2	Hopex Aquila V6.2 **last hotfix**

For previous versions or releases (HOPEX V1R3, HOPEX V2, HOPEX V2R1, HOPEX V3) it is necessary to perform an intermediate upgrade to HOPEX V4.0.
If you do not know which path to follow, consult the page Hopex Aquila on HOPEX Store https://store.mega.com/

This article is focused on migration from HOPEX V5.0 to Hopex Aquila V6.2.

For upgrade from Hopex Aquila V6.0 to Hopex Aquila V6.2:

1. Install .NET 8.
2. Upgrade specific additional module update for .NET 8 (if used).
3. Follow the document 'How to Upgrade a Hopex Bundle'.

Note that technical architecture has changed in a significant way after HOPEX V4.0.
Therefore, architecture, sizing and administration procedures designed for HOPEX V4.0 and below versions must be reviewed for Hopex Aquila.
See the online documentation for Hopex Aquila, PLATFORM - Installation and Deployment > **HOPEX Application Server (HAS) Architecture Overview**.

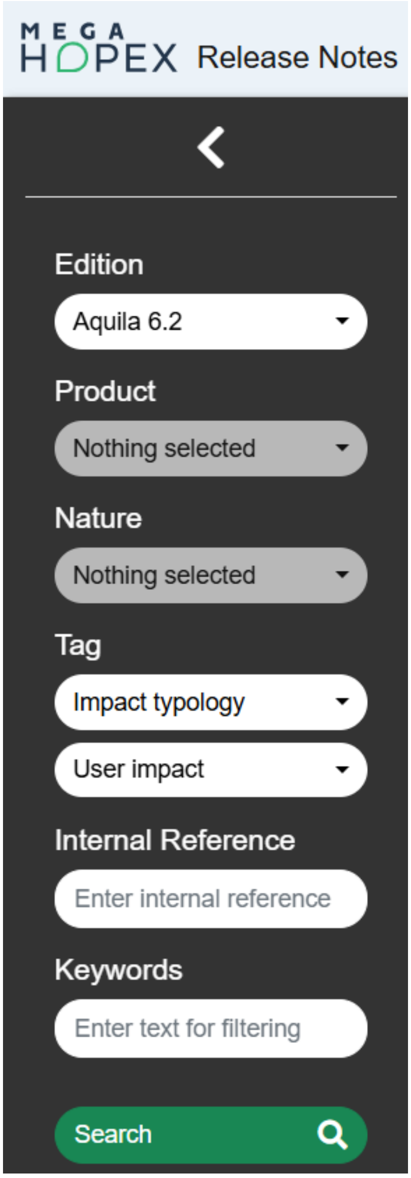
2. Prerequisites

2.1. Review release notes of Hopex Aquila

The release notes are available via a web site on MEGA Community.
Direct URL is **https://releasenotes.saas.mega.com/RNA/RnView**

First, select all Aquila editions (Aquila 6.0, Aquila 6.0 SP1, Aquila 6.0 SP2, Aquila 6.1, Aquila 6.2...) and click **Search** to get search results. Then you can refine the search results by using filters.

Filter	**Indication**
Product	Check each of the products you use You can also select All products
Nature	Check Changes, Deprecated, Removed



MEGA HOPEX Release Notes

Edition: Aquila 6.2

Product: Nothing selected

Nature: Nothing selected

Tag: Impact typology

User impact

Internal Reference: Enter internal reference

Keywords: Enter text for filtering

2.2. Check metamodel, workspaces and workflows

In the source version, for each environment:

Check	Detail
Check that version of environment is aligned with version of programs	Run HOPEX.exe and check that no message is displayed such as 'The versions of HOPEX and the MetaModel are not aligned (HOPEX=X.XX.XXX.XXXX - MetaModel=Y.YY.YYYY.YYYY)…'
Check that environment compiles without error	Run Windows Administration Console (administration.exe) and compile the environment. If the environment compilation generates a log entry in the HOPEX error log, you should fix such errors before migrating your data
Check that no private workspace (ex-transactions) persists	In Windows Administration Console (administration.exe), check workspaces. If a private workspace persists, dispatch or delete it.
Check that each workflow is completed	Certain workflows (regarding Application and Software Technology) are removed with Hopex Aquila. Therefore, it will not be possible to resume them in Aquila.
Password of the login 'System'	Check that the password of the login 'System' is known or set to empty before migration. This is very important since it will be requested to login with 'System'.

2.3. Backup data in SQL Server (production)

Perform SQL backups (.BAK files) for:

- SystemDb
- Data repository
- HAS configuration database

Example for an environment named Standard and instance port 5000

- Standard_SystemDb
- Standard_MasterData
- Standard_HAS_5000

2.4. Backup additional files

2.4.1. Backup main configuration files (production)

Level	Detail
Installation	Files: megasite.ini.generated and MegaModule.json.generated Default location: C:\ProgramData\MEGA\Hopex Application Server\<instance>\.shadowFiles\hopex.core\<version>\Cfg
Environment	File: Megaenv.ini

	Default location: C:\ProgramData\MEGA\Hopex Application Server\<instance>\Repos

2.4.2. Backup customization module (production)

In Hopex Aquila, customizations are packaged in a module has.custom.
By default, it is a file HOPEX Application Server Customization-XX.haspkg located by default in C:\ProgramData\MEGA\Hopex Application Server\<instance>\Modules\has.custom.

It will be necessary to transform this folder to a customization module (has.custom).
See online documentation for Hopex Aquila, **MODULES > Customization Lifecycle Management**.

2.5. Identify key configuration items

This applies to production.

2.5.1. Identify Hopex products used (production)

Hopex administrator should be aware of the Hopex products used.

Otherwise, you can identify them from the Hopex license used.
It is a .Must file.
There is no default location but you can identify the license folder from the file megasite.ini.generated saved previously. It contains the path of the license:

[Must Licence]
Path=<**license folder**>

Browse this folder, edit the file .Must.
You can get the list of products and their codes in the section [MEGAComponentInfo]:

[MEGAComponentInfo]
(**LAN**) Hopex MainUser=30 ; 0
(**MTS2**) Hopex Power Studio= 1 ; 0
(**HBPA**) Hopex Business Process Analysis=20 ; 0
(**HITA**) Hopex IT Architecture V2=10 ; 0

2.5.2. Identify authentication used (production)

Hopex administrator should be aware of the authentication mode used.

Several authentication modes are available up to HOPEX V5.0.

Authentication mode	Check in HOPEX V5.0	Supported in Aquila
OpenID	HAS Console, browse Modules > Authentication > Identify providers > Open ID Active is checked	Yes

SAML2	HAS Console, browse Modules > Authentication > Identify providers > SAML2 Active is checked	Yes
Windows (IIS)	HAS Console, browse Modules > Authentication > Identify providers > Windows Active is checked	Yes
HOPEX (MEGA)	HAS Console, browse Modules > Authentication > Identify providers > HOPEX Active is checked	Yes
LDAP	Installation options Installation > User Management > LDAP Authentication mode is set to 'LDAP'	**No**

2.5.3. Identify modules used (production)

Hopex administrator should be aware of the Hopex products used.

Otherwise, to make you can take a screenshot of the page Cluster status in HAS Console (menu Cluster > Cluster status).
You can also identify them from the folder structure.
Browse module folder located by default in C:\ProgramData\MEGA\Hopex Application Server\<instance>\Modules.
For each module used, the is a subfolder with the version.

You can build a table such as:

Example if additional module	Version
has.custom	15.2.0+13
hopex360	15.7.0+6617
sample.datatypes	15.6.12+6579

2.5.4. Identify profiles used (production)

The Hopex administrator should be aware of the profiles used in Hopex.

Otherwise, you can use the following query in Hopex.
Connect with Hopex Administrator or Hopex Customizer to run the query with the wider possible vision.

```
Select [Profile] Into @PL1 Where [Profile Assignment]
Select [Profile] Into @PL2 Where [Super Profile] in @PL1
Select [Profile] From @PL1 Or @PL2
```

3. Install Test Platform

3.1. Install Hopex Aquila (development)

There are technical requirements. See online documentation for Hopex Aquila **HOPEX Application Server (HAS) Architecture Overview**, in particular section 'Software Technology Stack'.

Note two important prerequisites:

4. **Installation of NET Core 8 (NET 8)**
5. **Update of HAS Instance Manager to version 16.1.0.119 or higher**

For the installation procedure, see online documentation for Hopex Aquila **HOPEX Application Server (HAS) Installation Guide**.

3.2. Initialize migration document (development)

A specific migration document should be created. It will detail all steps required to migrate:

- From source version (HOPEX V5.0 CPX)
- To target version Hopex Aquila (Hopex V6.2 SPx)

Whenever a test feedback identifies an additional step, this step should be added to the documented so that migration can be played again from source data.

3.3. Restore data in SQL Server (development)

Data must be initialized in development from a copy of production data (down data alignment). It is essential to use test data that are representative from production data.

Example: Restore copy of production data of HOPEX V5.0.

Production data of HOPEX V5.0	Development data in Hopex Aquila V6.2 Copy of production data HOPEX V5.0
Standard_SystemDb	Migration1_SystemDb
Standard_MasterData	Migration1_MasterData
Standard_HAS_5000	Migration1_HAS_5001

3.4. Create a HAS Instance (development)

In Instance Manager console, create a HAS Instance in mode Development in version Hopex Aquila. This is necessary to tune the customization module.

It is recommended to reuse the HAS Database created previously (ex: Migration_HAS_5000). For this, enter this name as Cluster name when creating the HAS Instance. Otherwise, a new HAS Database will be created and certain settings of the source version (in particular, user settings) will not be restored.

After this step:

- A Hopex Environment is configured (mapped to database restored previously, see Restore data in SQL Server (development)
- A Hopex license is configured

3.5. Complete HAS instance (development)

As a general rule, each module deployment must be completed by environment automatic update. In the context of the migration, environment automatic update will be run later in step 3.

3.5.1. Deploy migration module (development)

In HAS Console, install module Hopex Environment Migration Package Aquila (hopex.core.migrate) in version **17.0.0+6771**.
This module is required to upgrade SystemDb to version Hopex Aquila.

3.5.2. Deploy customization module (development)

If customization exist, customization module (has.custom) must be deployed and adapted if necessary. Install this module from HAS Console.

Note that customization module must be deployed **before** upgrade of data.

Note also that the version of customization module available on HOPEX Store is only a template. Only project has the real version to use. This version is incremented when module content is updated following the appropriate procedure.

Due to security changes (macro calling CreateObject), code needs to be updated for Hopex Aquila.
See also release note for Hopex Aquila, reference #56811.

3.5.3. Deploy additional modules (development)

Reminder:
When a HAS instance is created, keys modules (called system modules, grouped in a bundle) are installed automatically. Other modules are called additional modules.

In HAS Console, install additional modules (menu Modules > Module List, Add new).

For each additional module used in the source version except customization module (has.custom):

- Search the module, ex: IT-Pedia (itpm.itpedia).
- Select the public version of the module compatible with Hopex Aquila V6.2:
  - Use version 17.1.X if it exists.

Note that each module deployment must be completed by environment automatic update.

Specific modules need to be updated for .NET 8.0 if used:

- IT-Pedia (itpm.itpedia): version **17.1**.0+6835 or higher
- ServiceNow Integration (servicenow.integrations.hopex): version **2.0**.0+54 or higher
- HOPEX GraphQL IDE (graphql.ide): version **8.0**.0+15 or higher
- Enterprise Portal (website.static.navigator): version **16.1**.0+5 or higher
- Static Website Macros (website.static.macros): version **16.1**.0+5 or higher
- HOPEX Cyber Resilience (hopex.cyber-resilience): version **17.1**.0+6805 or higher
- HOPEX Data Discovery Standalone (tool.data.discovery): version **17.1**.0+6829 or higher
- HOPEX Data Discovery (data.discovery): version **17.1**.0+6829 or higher
- AI-Driven APM (tool.itpm.apmauto): version **17.1**.0+6827 or higher
- HOPEX Simulation Engine (simulation.engine): version **17.1**.1+6827 or higher

If you use module Archimate 3.1, it is strongly recommended to install version **17.1**.x (17.1.0+6820 or higher) or to benefit from the new features.

3.5.4. Customization of module hopex360

From HOPEX Aquila V6.1, a new version **17.1**.x of module hopex360 (17.1.0+6838 or higher) is available.

- New look and feel (compliant with Aquila visual identity)
- Improve accessibility (web accessibility)
- Updated content (compliant with Aquila methodology changes)

The previous version can also be used (version 17.0.0+6662)

Good practices when customizing a web site from hopex360 template consists in:

- Duplicating standard web site template and its components
- Customizing the duplicated web site template

When this is done, your customization is independent from the standard web site template and its components.

This means that:

- It will not be impacted by a change in standard module hopex360
- It will not benefit from fixed and improvement of standard module hopex360

3.5.5. Update configuration (development)

When the HAS instance was created, various settings (megasitesettings) have been initialized.

Situation	Impact	Recommendations
An existing HAS Database has been re-used (recommended)	Settings of source installation have been restored	Check that settings of source installation are valid for this HAS Instance (Development)
A new HAS Database has been created	Settings are default settings for Hopex Aquila	Check that settings of source installation are valid for this HAS Instance (Development)

Situation	Impact	Recommendations
		Replace certain settings with settings of source installation backed up previously

Section that could be updated:	Sections that should not be updated:
[System] [General] [Mail] [Filter] …	[Customization] [Must Licence] [HOPEX] [HAS] [Environment Shortcuts] [SQL SERVER CONFIG]

In a similar way, environment level settings (options) have been initialized with default settings for Hopex Aquila.
It is recommended to replace certain settings with settings of source environment backed up previously (Megaenv.ini).

Section that could be updated:	Sections that should not be updated:
[Filter-Available] [Filter] …	[Env.Def] [DbReferences]

Such changes in configuration should be documented in the specific migration document.

4. Run Data Upgrade

4.1. Run automatic environment upgrade

To upgrade data, see the online documentation for Hopex Aquila: PLATFORM - Administration > Administrator Guide > Environments > Updating an environment

It is useful to record start time and end time of environment upgrade processing in the specific migration document for future references.

Note that duration can vary according to migration path, infrastructure and volume of data. Anyway, this is a heavy processing that lasts several hours. Verify that the machine will not shut down (or go to sleep or hibernate).

4.2. Check logs and environment compilation

Automatic environment upgrade runs various conversion tools that could meet errors. Review report tabs and logs. Check that no compilation error is reported.

(MegaCrdxx.txt located by default in <Hopex environment folder>)
megaerrxx.txt log (located by default in C:\ProgramData\MEGA\Hopex Application Server\<instance>\Logs

File	Default location
Environment report (MegaCrdYYYYMM.txt)	C:\ProgramData\MEGA\Hopex Application Server\<instance>\Repos\<environment folder>
megaerr log (megaerrYYYYMMDD.txt)	C:\ProgramData\MEGA\Hopex Application Server\<instance>\Logs

After this step:

- Hopex environment must compile without error.

4.3. Backup migrated data

Perform SQL backups (.BAK files) for this intermediate steps. In case of a further error requesting to restore data, this will be a stable point of restore.

Example for an environment named Migration and instance port 5001:

- Migration1_SystemDb
- Migration1_MasterData
- Migration1_HAS_5001

5. Post-migration

5.1. Review changes of Hopex Aquila

Review again the release notes on MEGA Community to focus on changes and items removed and deprecated.

- An item **removed** in Hopex Aquila can no longer be used in this version.

6. An item **deprecated** in Hopex Aquila still be used in this version.
   However it will be removed in a future version, and it is recommended not to use it.

Direct URL is **https://releasenotes.saas.mega.com**

Key changes **(not exhaustive list)**	**Indications**
Product removed	Discuss with the account manager to see if MEGA has an offer suited to your need.
Profiles removed	This will impact the web desktops (GUI) and workflow definitions used. This can also impact custom features plugged on web desktop. Switch to recommended profiles
Profiles deprecated	Think about switching to recommended profiles
Authentication mode removed	LDAP authentication is removed. Think about implementing SAML2 or OpenID
Look of homepage	With new web desktops (GUI), the look of the homepage is different. It is no longer possible to display tiles.
Cards view	With new web desktops (GUI), a cards view provides an overview of the essential properties.
Macros calling CreateObject	From Hopex Aquila V6.0, it is forbidden to call CreateObject in a macro for security reason (example Set fso = CreateObject("Scripting.FileSystemObject")
…	

MEGA can assist you in managing changes. For this please contact your Service Director.

5.2. Study adaptations to Hopex Aquila

Once changes and impacts are identified to need to decide and plan changes.

Common changes (not exhaustive list)	Comment
Adapt homepage	Tiles displayed by default or tiles added manually (Add tiles) can be replaced with links (shared for the profile). A customization is needed for this. Shortcut tiles created from objects (add to homage page) are converted automatically to links.
Adapt customization of made to removed profiles	Custom features (ex: menu item calling a specific processing) plugged on web desktop need to be adapted to the new web desktop.
Adapt fully customized profiles	A specific study is needed.
Adapt custom profiles and	Custom features plugged on web desktop.
Adapt cards view	Cards view are configured for standard Metaclass. A customization is needed to configure custom MetaClass.

MEGA can assist you in any kind of adaptation. For this, please contact your Service Director.

See the online documentation for Hopex Aquila:

- **Adapt homepage:** PLATFORM - Customization (Windows) > Customizing the User Interface > Versatile Desktop > Using a Working Environment Template (WET) … Customizing the Quick Access block
- **Adapt web desktop**: PLATFORM - Customization (Windows) > Customizing the User Interface > Versatile Desktop

Note that customizations (external files, update of SystemDb) must follow a procedure used by the customization module (has.custom) and be documented.

5.3. Test customizations and interfaces

Once customizations are made, customizations need to be checked.
If a test plan exists, follow it.
Otherwise, an inventory is needed to identify and check customizations.

Main customization types	Indication
Report Template	Run a check each custom template on sample data
Report Template (MS Word)	Run a check each custom template on sample data
Web site	Run and check each custom web site
Workflow Definitions	Run and check each custom workflow on sample data
MetaPropertyPage	Check each custom property page on sample data

Questionnaire Template Assessment Template	Run and check each assessment template on sample data

Interfaces and authentication also need to be checked.
If a test plan exists, follow it.
Otherwise, an inventory is needed to identify and check interfaces.

Main items	**Comment**
Web site generation scheduler	Run and check scheduler. Review should be based on initial functional specifications
GraphQL	Check API key used. Check connection to GraphQL interface
Web services	Review web services execution. Review should be based on initial functional specifications. It may be necessary to re-generate API keys
External authentication (SAML2, OpenID, IIS)	Configure and check authentication. Review should be based on initial functional specifications
…	

It is useful to have access to data and customizations in the source version to compare source and target.

Note that if several HAS instances exist on a machine, only one can run components using Administration API script at a given moment.
See later in this document: How to set a HAS Instance as current in registry?

5.4. Organize UAT session

Once data is migrated and customizations are checked, it is required to test the end user scenarios and data (diagrams…).
If a test plan exists, follow it.
Otherwise, it is recommended to organize UAT.

5.5. Loop until migration is ready

Each negative test feedback should lead to a change in the migration procedure.

A change can be:

- A data or customization reprocessing in the source version
- A change in configuration (modules deployed, options…) in the target version
- A change in customization in the target version
- A fix on Hopex Aquila provided by MEGA

Each change should be documented in the specific migration document.
Each change in customization should be packaged in the customization module.

Then a new migration loop is needed to test changes:

- Initialize again test platform (restore again production data…)
- Follow specific migration document (updated version)

- Test data and customization

When no significant test feedback is detected, you can run the migration for real:

- Initialize again test platform (restore again production data…)
- Follow specific migration document (final version)

MEGA can assist you and manage the whole migration process. For this, please contact your Service Director.

6. FAQs

6.1.1. Why a customization module (has.custom)?

Various customization can be made, for example

- .MGS files (shapes)
- .JAR files (java code)
- .JSON (GraphQL Schema)

In Hopex Aquila, external files (customizations) and well as new system update should be package in a customization module (has.custom). This enables to capture and deploy customization easily.

6.1.2. What is the list of system modules

When a HAS instance is created, keys modules (called system modules, grouped in a bundle) are installed automatically. Other modules are called additional modules.

List of system modules.

Module code	Module
has.console	HAS Console
has.uas	HAS Identity Provider
hopex.assessment	HOPEX Questionnaire Builder
Hopex.core	HOPEX Core Back-End Aquila
hopex.dtpx	HOPEX Aquila
hopex.graphql	HOPEX GraphQL
hopex.redis	HOPEX Redis
hopex.rest.api	HOPEX REST API
hopex.rest.api	HOPEX Server Supervisor Module
hopex.specific.assets	HOPEX Aquila specific assets

6.1.3. Error Inconsistent format for MetaAttribute

During environment automatic upgrade of when accessing data, an error can be displayed of logged such as

> Inconsistent format for MetaAttribute "EA44305544424043A" (304630847021378116). Physical Format (X). Meta Format (L).

This reveals a data inconsistency that needs to be addressed.
See KB 00009355 in MEGA Community for more details.

6.1.4. Cannot find the option to enable data modification

The option was moved and renamed to 'Authorize Hopex data modification'
Note that it is not recommended to use this option.
If you need to configure it, go in options, display Extended level, browse group 'Installation > Customization'.

6.1.5. Warning 'Run the menu 'Perform SQL conversion on the repository' to perform the upgrade

This means that the format of tables in SQL Server must be converted.
You need to run a menu **Perform SQL conversion on the repository** from the Administration Console (Administration.exe).

6.1.6. Warning 'Your environment requires an update for compatibility with your version of HOPEX…'

This warning report that the system database is not up to date. This occurs if the programs have been updated and the environment has not/not yet been updated.

You can click 'No' and trigger the upgrade of the environment later (menu **Environment Automatic Update**)

6.1.7. Warning 'Writing access diagram is not compiled. The diagram should be recompiled …'

Certain actions can leave the writing access diagram (ex-User diagram/Authorization diagram) is in a state not compiled.

To compile the writing access diagram, see online documentation for Hopex Aquila:
PLATFORM - Administration > Administrator Guide > Data Writing Access > Managing Users from the Writing Access Diagram > Compiling the Writing Access Diagram

6.1.8. How to set a HAS Instance as current in registry?

If several HAS instances exist on a machine, only one can run components using Administration API script at a given moment.
Before each execution of components using Administration API script, it is required to reference Mega.Application.
This is done using a powershell script (HOPEX-regserver.ps1) installed at the root folder of the HAS Instance.

How to Upgrade a Hopex Bundle

1. FOREWORD

1.1. HAS instance

In HOPEX Application Server (HAS) deployment, an installation is named instance.

Each HAS Instance is mapped to:

- a Port: 5000, 5001, 5002…
- a version of Hopex
- one mode: Development, Training, Staging (synonym: Test, QA...), Production.
- one Hopex environment. Using multiple environments is not supported

HAS Instances are managed by a program named Instance Manager.

1.2. HAS module

In HAS deployment, each component is delivered as a **module**.

Each module has its version and dependencies.

A module is a .haspkg file.

Module	System module	Short description
HOPEX Core Back-End Aquila	Yes	Core of Hopex platform Code: **hopex.core**
HAS Identity Provider	Yes	Component used for authentication Code: **has.uas**
HOPEX360	No	Web site Template Code: **hopex360**
…		

1.3. HAS bundle

System modules are packaged in a **bundle** named 'HOPEX'.

Non-system modules are available as independent modules.

A bundle is a .haspackages folder containing a set of .haspkg files.

A bundle packages a combination of modules in different versions compatible with each other.

Example:

Bundle	Module	Version
Bundle 6.0.1+301 (HOPEX Aquila)	HAS Console	16.0.1+181
	HAS Identity Provider	16.0.1+181
	HOPEX Questionnaire Builder	17.0.1+6659
	HOPEX Core Back-End Aquila	17.0.1+6659
	HOPEX Environment Installation Package Aquila	17.0.0+6583

	HOPEX Aquila	17.0.1+6659
	HOPEX GraphQL	7.87.507+6551
	HOPEX Redis	6.2.6+41.0.2
	HOPEX REST API	7.87.507+6551
	HOPEX Server Supervisor Module	20.0.0+5
	HOPEX Aquila specific assets	6.0.7

1.4. Service Pack in HAS deployment

A Service Pack (SP) provides a consistent set of fixes within a major version of Hopex. GUI should be stable. For each version, several SPs are scheduled and heavily tested by QA department.

An SP enables to update the system module of an HAS instance. It is installed via a bundle.

There are not SP for non-system module.

The SPs provided for the bundle are cumulative.

E.g.: HOPEX Aquila 6.0 SP2 includes fixes provided for HOPEX Aquila 6.0 SP1.

Each SP of a bundle is a new version of this bundle. It updates all the system modules included in this bundle. Each component of the related module is replaced.

Modules and Bundles can be downloaded and installed via administration consoles provided access to HOPEX Store is available online (https://store.mega.com/).

Bundles can be first downloaded as offline package and installed offline afterward.

There are two typical deployment contexts for HOPEX Application Server (HOPEX programs)

- HOPEX programs are deployed on a single server. There is no concern to replicate updated programs.
- HOPEX programs are deployed on multiple servers (**cluster deployment**). There is a concern to replicate updated programs to each server (node) of the cluster.

So far, deployment of bundles (hotfix update, SP updates) in cluster is not automatic.

It is required to download and install bundle on each server of the cluster.

2. UPGRADING A HOPEX BUNDLE

This procedure applies to both single server deployment and cluster deployment. It is required to download and install the bundle on each server.

Prerequisites:

- Identify the **bundle** to install (target bundle).

  E.g.: 6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])

  This information is usually provided by MEGA Technical Support.
- Identify the url of the **HAS Instance Manager Console**

  E.g.: http://localhost:30100/
- Identify the **HAS instance** to upgrade (target HAS instance)

  E.g.: preproduction instance http://svr0101:5001/

  This information is provided by the project.
- Know the **credentials** for the HAS Console of this instance.

  This information is provided by the project.
- Know the **credentials** for the Instance Manager Console.

  This information is provided by the project.
- Check that no user is connected to the HAS instance.

2.1. Update of Instance Manager

Certain SPs require an update of the Instance Manager.

Condition	Update of Instance Manager	Comment
Upgrading to **Aquila 6.1**	Update to HAS Instance Manager 16.1.x version	.Net 8 support
…		

Update of Instance Manager is performed systematically if you run Hopex installer (e.g.: new installation, offline installation).

To perform a new installation, see *HOPEX Application Server Installation* document in online documentation.

Note that, if the expected version of .NET core is not installed, the Instance Manager will not restart. **Verify that this prerequisite fulfilled before running the setup.exe**.

2.2. Online procedure (internet access)

The procedure applies to a HAS instance.

Prerequisites:

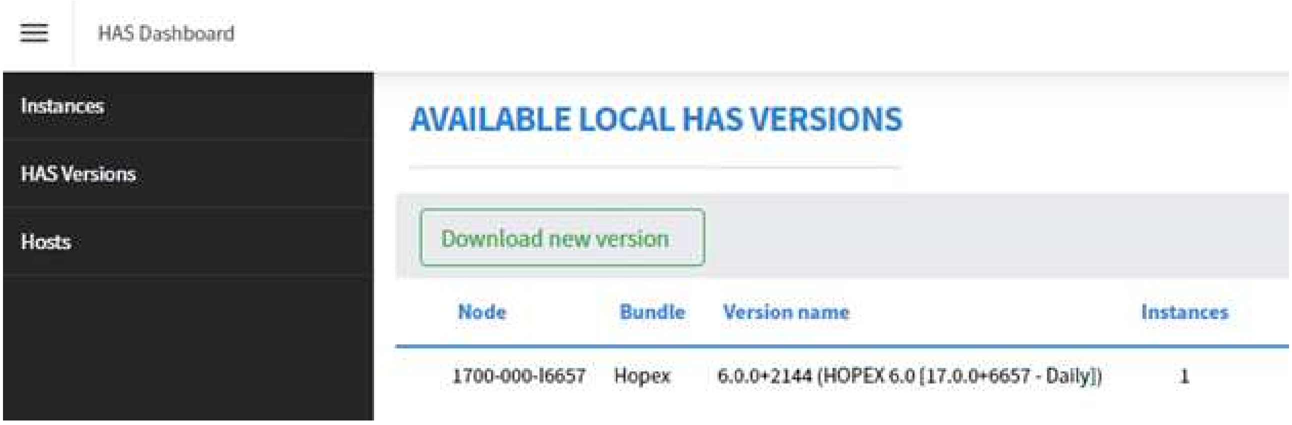
- You can access HOPEX store: **https://store.mega.com**.
- You have an installation key.

For each HAS instance:

1) Enter the url of the HAS Agent Console.

   E.g.: http://localhost:30100/

2) In the left menu, select **HAS Versions**.



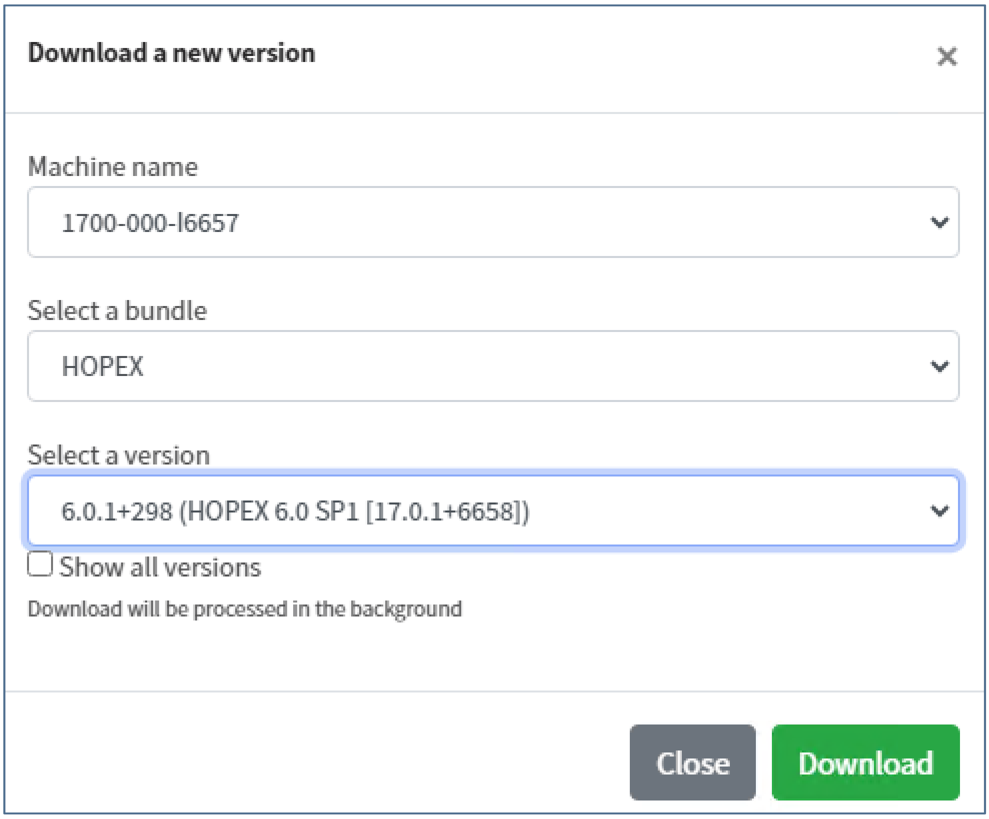
AVAILABLE LOCAL HAS VERSIONS

Node	Bundle	Version name	Instances
1700-000-I6657	Hopex	6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])	1

3) Click **Download new version**.

4) In the list, select carefully the version to install**.**

   E.g.: 6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])



Download a new version

Machine name: 1700-000-I6657

Select a bundle: HOPEX

Select a version: 6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])

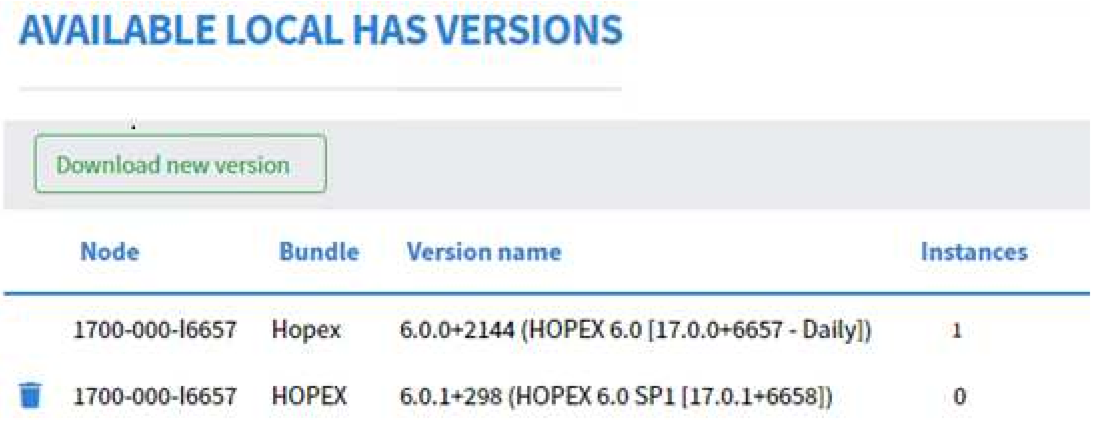
☐ Show all versions

Download will be processed in the background

5) Click **Download**.

Wait a few minutes up to the end of the download (100% then extraction).
A new folder is created in C:\ProgramData\MEGA\Hopex Application Server\.binaries\HOPEX\<version>

E.g.: C:\ProgramData\MEGA\Hopex Application Server\.binaries\HOPEX\V6.0.1+298

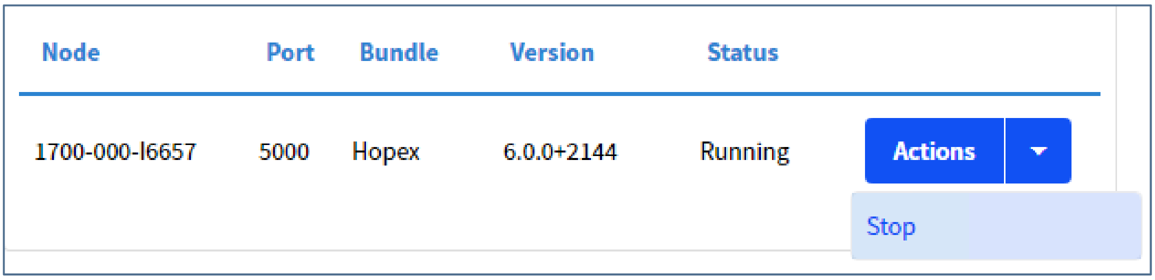


AVAILABLE LOCAL HAS VERSIONS

	Node	Bundle	Version name	Instances
	1700-000-I6657	Hopex	6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])	1
🗑	1700-000-I6657	HOPEX	6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])	0

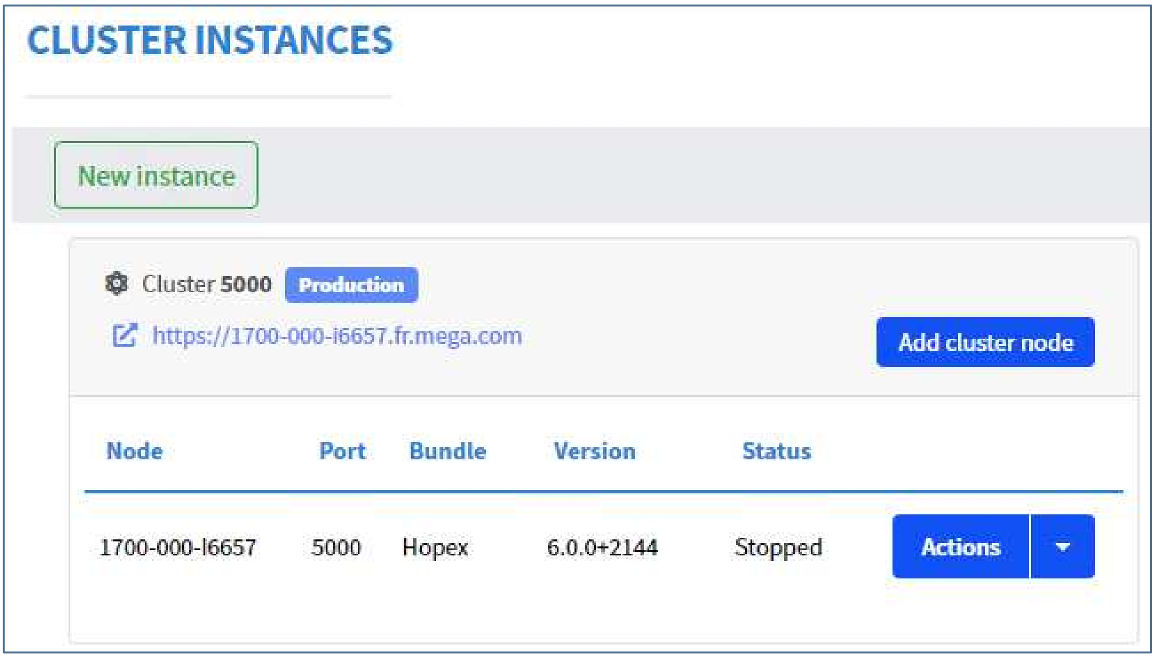
6) In the left menu, select **Instances**.

7) In the target instance row, click **Action > Stop** and confirm action.



Node	Port	Bundle	Version	Status
1700-000-I6657	5000	Hopex	6.0.0+2144	Running

The HAS instance stops (status **Stopped**)



CLUSTER INSTANCES

Cluster 5000 Production

https://1700-000-i6657.fr.mega.com

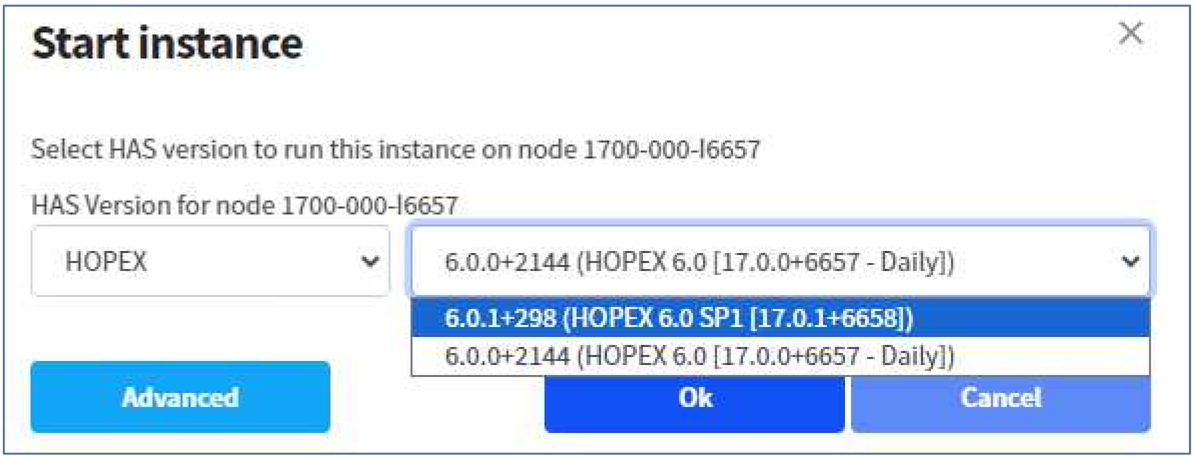
Node	Port	Bundle	Version	Status
1700-000-I6657	5000	Hopex	6.0.0+2144	Stopped

8) In the target instance row, click **Actions > Start**.

9) In the **Start instance** window, select carefully the target bundle and click **OK.**

E.g.: 6.0.1 +298 (HOPEX 6.0 SP1)

The HAS instance starts.



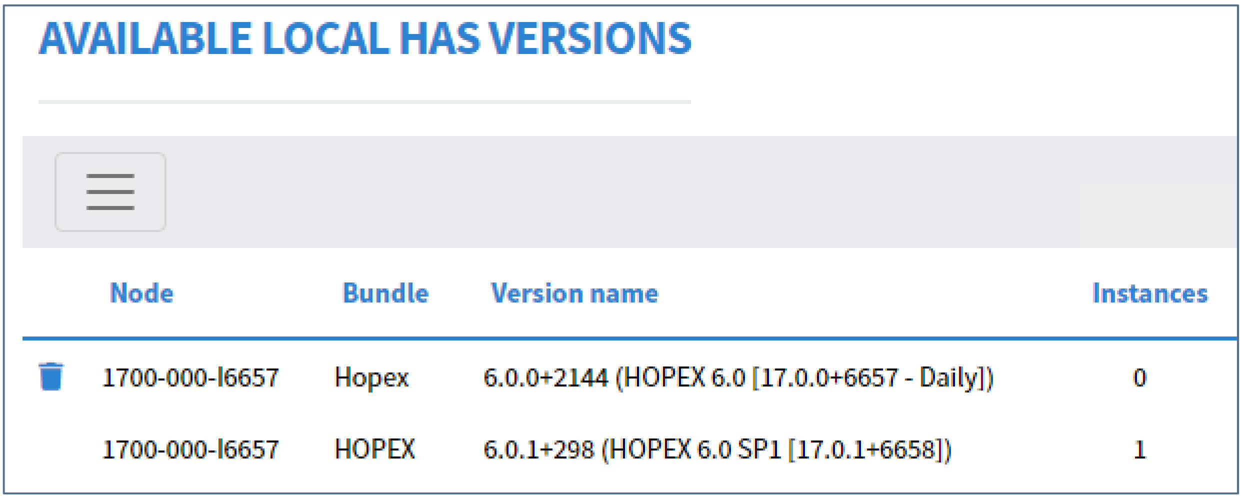
Start instance

Select HAS version to run this instance on node 1700-000-I6657

HAS Version for node 1700-000-I6657: HOPEX, 6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])

6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])
6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])
Advanced
Ok
Cancel

10) In the left menu, select **HAS Versions**.



AVAILABLE LOCAL HAS VERSIONS

	Node	Bundle	Version name	Instances
🗑	1700-000-I6657	Hopex	6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])	0
	1700-000-I6657	HOPEX	6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])	1

11) You can delete previous version, if there is no associated instance: click its corresponding 🗑.

E.g.: 6.0.0+2144 version

12) Access the HAS Console related to the target instance and check that all modules are loaded.

2.3. Offline procedure (no internet access)

The procedure applies to a HAS instance.

Prerequisite: you have received a folder containing an offline package (downloaded previously).

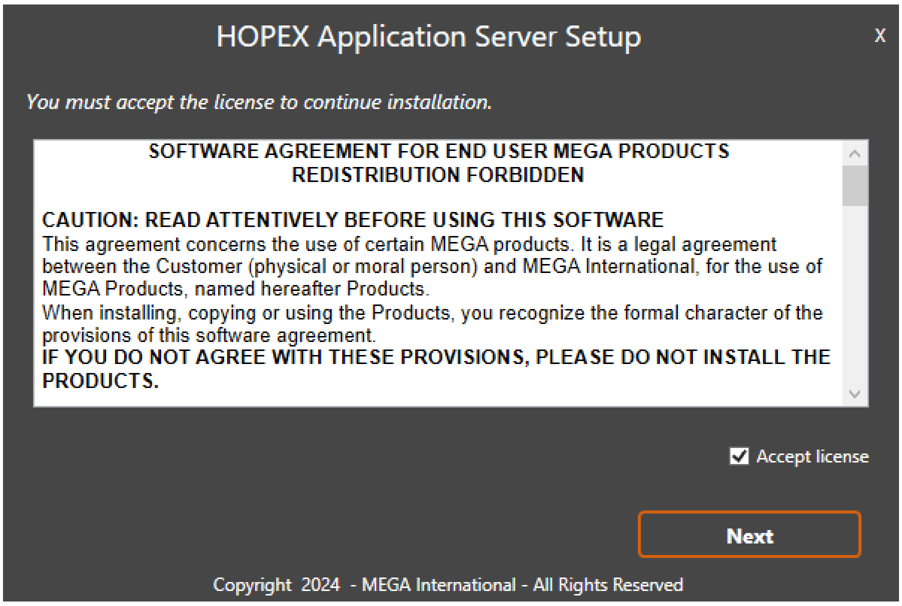
➔ To create an offline package, see ***HOPEX Application Server (HAS) Installation Guide***.

Browse the folder containing the offline package related to the hotfix. It contains:

- a file: has.setup.exe.
- a folder: .haspackages.

Procedure:

1) Run **has.setup.exe** as an administrator.
2) Check **Accept license** and click **Next**.



HOPEX Application Server Setup

You must accept the license to continue installation.

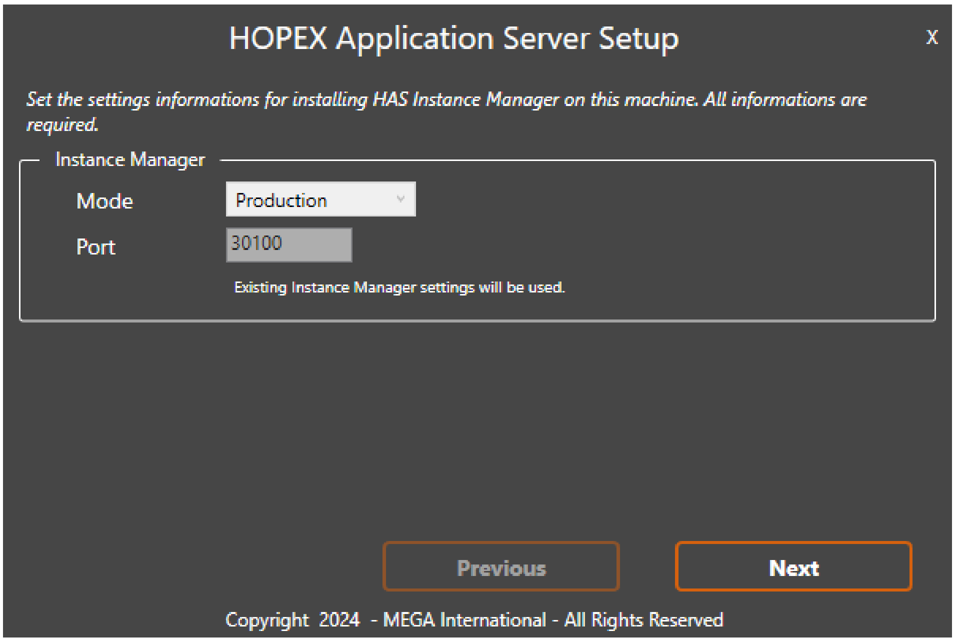
SOFTWARE AGREEMENT FOR END USER MEGA PRODUCTS
REDISTRIBUTION FORBIDDEN

CAUTION: READ ATTENTIVELY BEFORE USING THIS SOFTWARE
This agreement concerns the use of certain MEGA products. It is a legal agreement between the Customer (physical or moral person) and MEGA International, for the use of MEGA Products, named hereafter Products.
When installing, copying or using the Products, you recognize the formal character of the provisions of this software agreement.
IF YOU DO NOT AGREE WITH THESE PROVISIONS, PLEASE DO NOT INSTALL THE PRODUCTS.

☑ Accept license

Copyright 2024 - MEGA International - All Rights Reserved

3) Keep existing settings for HOPEX Agent and click **Next**.



HOPEX Application Server Setup

Set the settings informations for installing HAS Instance Manager on this machine. All informations are required.

Instance Manager

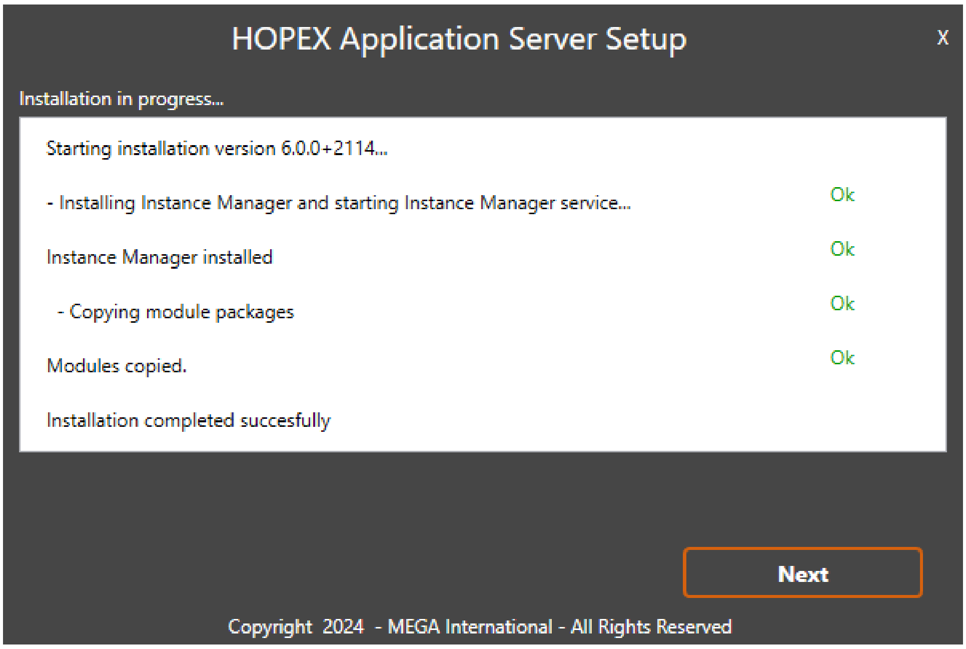
Mode: Production

Port: 30100

Existing Instance Manager settings will be used.

Copyright 2024 - MEGA International - All Rights Reserved

The package is installed.
A message is displayed: 'Installation completed successfully'.



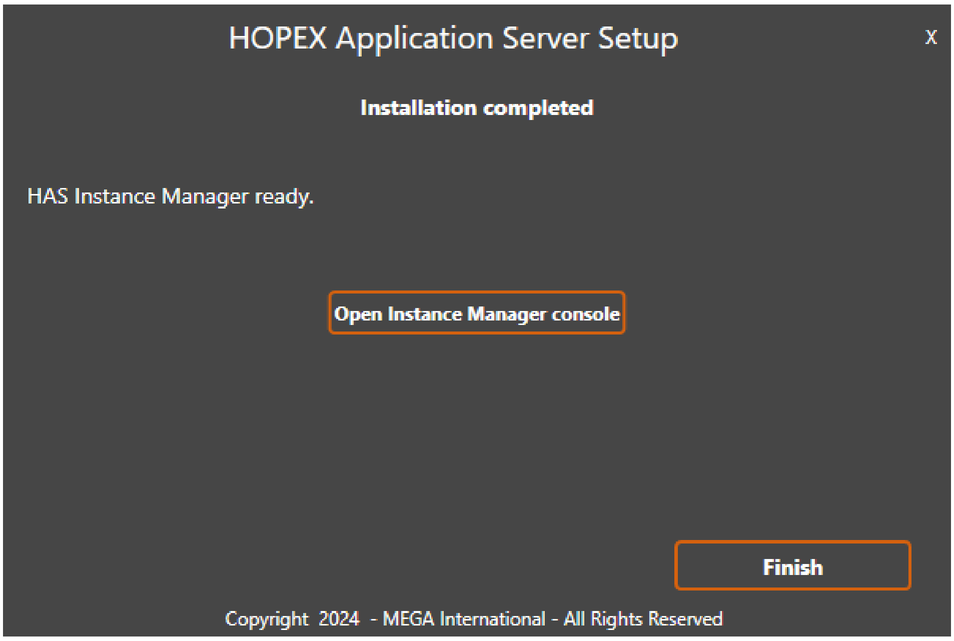
HOPEX Application Server Setup

Installation in progress...

```
Starting installation version 6.0.0+2114...
- Installing Instance Manager and starting Instance Manager service...   Ok
Instance Manager installed                                                Ok
 - Copying module packages                                                Ok
Modules copied.                                                           Ok
Installation completed succesfully
```

Copyright 2024 - MEGA International - All Rights Reserved

4) Click **Next**.



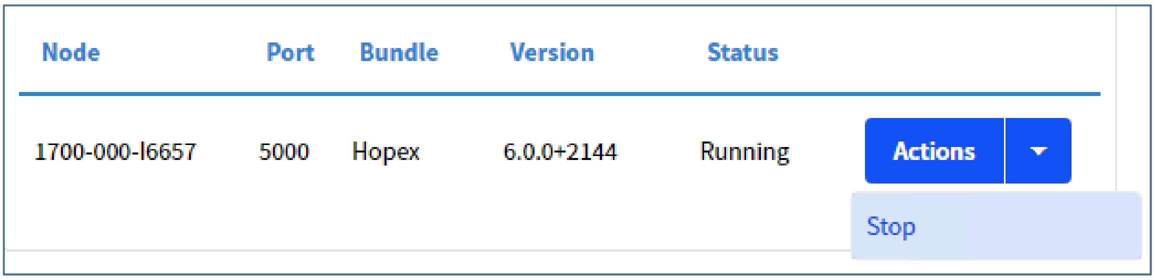
HOPEX Application Server Setup

Installation completed

HAS Instance Manager ready.

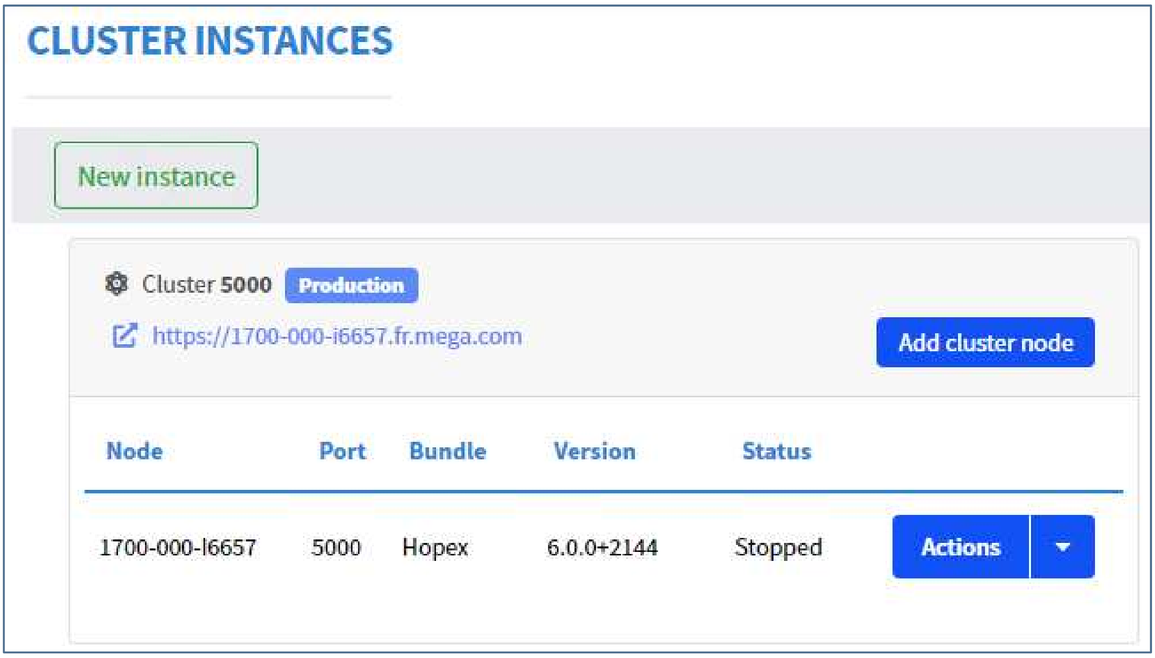
Copyright 2024 - MEGA International - All Rights Reserved

5) Click **Open Instance Manager console**
6) Login to **Instance Manager console**.
7) In the left menu, select **Instances**.
8) In the target instance row, click **Action > Stop** and confirm action.



Node	Port	Bundle	Version	Status
1700-000-I6657	5000	Hopex	6.0.0+2144	Running

The HAS instance stops (status **Stopped**)



CLUSTER INSTANCES

Cluster **5000** Production

https://1700-000-i6657.fr.mega.com

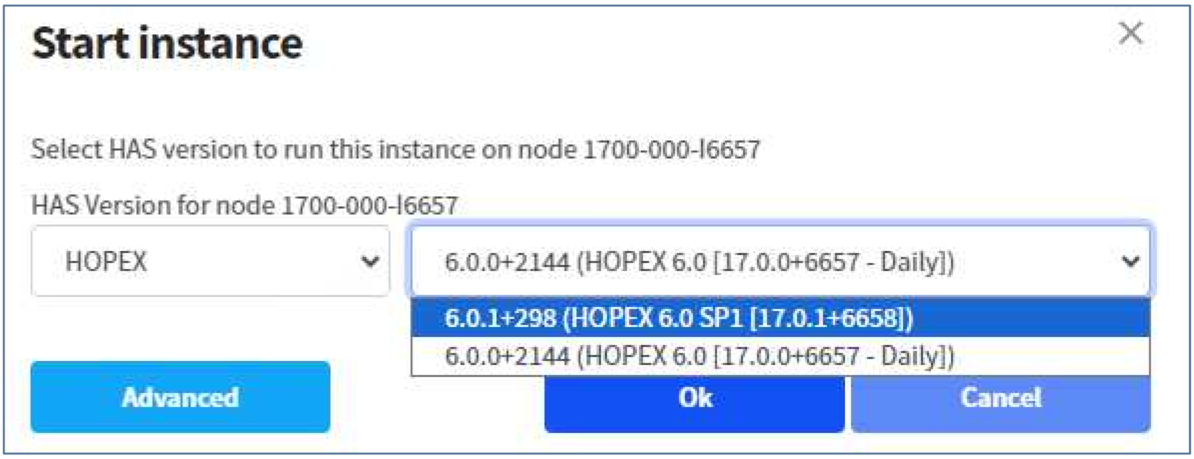
Node	Port	Bundle	Version	Status
1700-000-I6657	5000	Hopex	6.0.0+2144	Stopped

9) In the target instance row, click **Actions > Start**

10) In the **Start instance** window, select carefully the target bundle and click **OK.**

    E.g.: 6.0.1 +298 (HOPEX 6.0 SP1)

The HAS instance starts.



Start instance

Select HAS version to run this instance on node 1700-000-I6657

HAS Version for node 1700-000-I6657

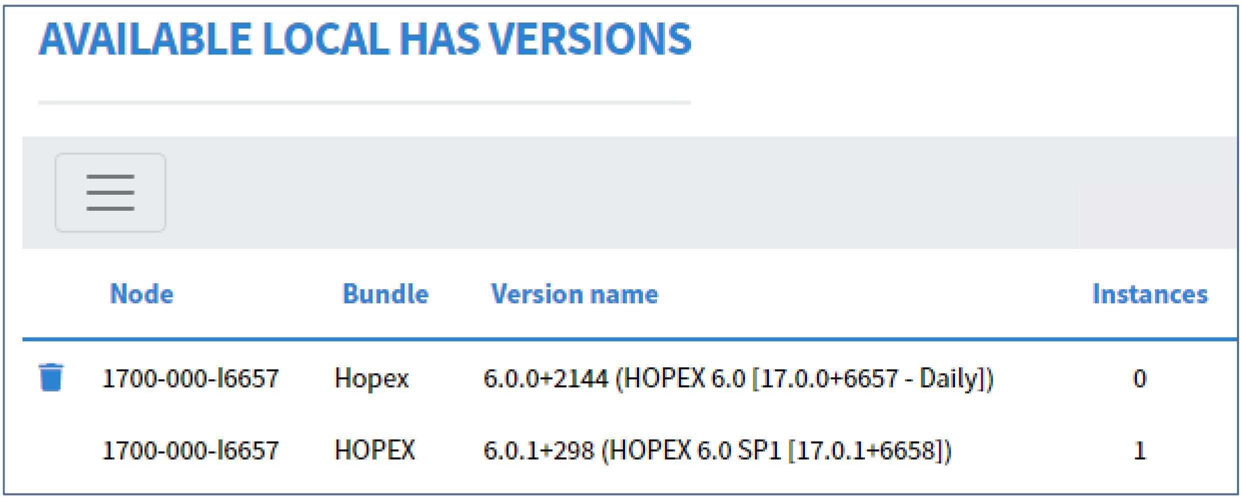
HOPEX

6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])

6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])

6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])

11) In the left menu, select **HAS Versions**.



AVAILABLE LOCAL HAS VERSIONS

	Node	Bundle	Version name	Instances
🗑	1700-000-I6657	Hopex	6.0.0+2144 (HOPEX 6.0 [17.0.0+6657 - Daily])	0
	1700-000-I6657	HOPEX	6.0.1+298 (HOPEX 6.0 SP1 [17.0.1+6658])	1

12) You can delete previous version, if there is no associated instance: click its corresponding 🗑.

    E.g.: 6.0.0+2144 version

13) Access the HAS Console related to the target instance and check that all modules are loaded.

3. FAQS

3.1.1. How to check that no user is connected to the HAS instance?

Check list of workspaces in Administration.exe.

Use supervision console.

3.1.2. How to prevent that a user connects to the HAS instance during hotfix installation?

You need to warn end users.

3.1.3. I did not install the version I wanted to. How to restore the previous version of the module?

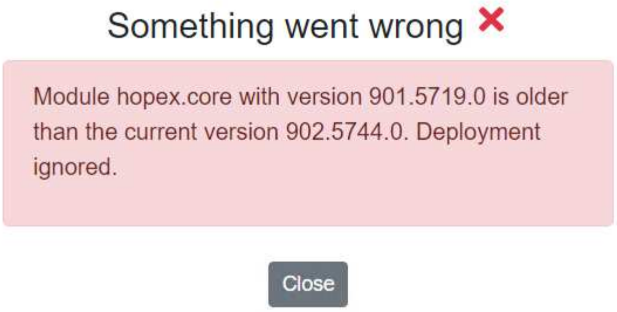
You need to download again and install again the expected version of the module.

3.1.4. How to verify that no workspace exists in read/write mode?

Check the workspace list in Administration.exe.

3.1.5. Error Something went wrong. Module X with version YY is older that the current version ZZ. Deployment is ignored!

This means that the version selected cannot be installed since it is older that the current version. Only upgrade is possible, not downgrade.

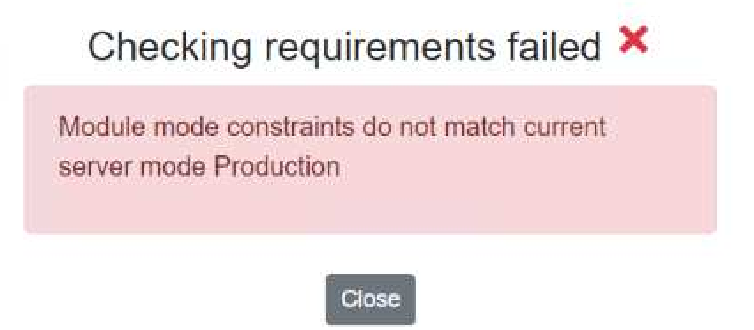


Something went wrong ✕

Module hopex.core with version 901.5719.0 is older than the current version 902.5744.0. Deployment ignored.

3.1.6.Error: Module mode constraints do not match current server mode Production

This means that the version selected cannot be installed since it is not compatible with the current installation.



Checking requirements failed ✕

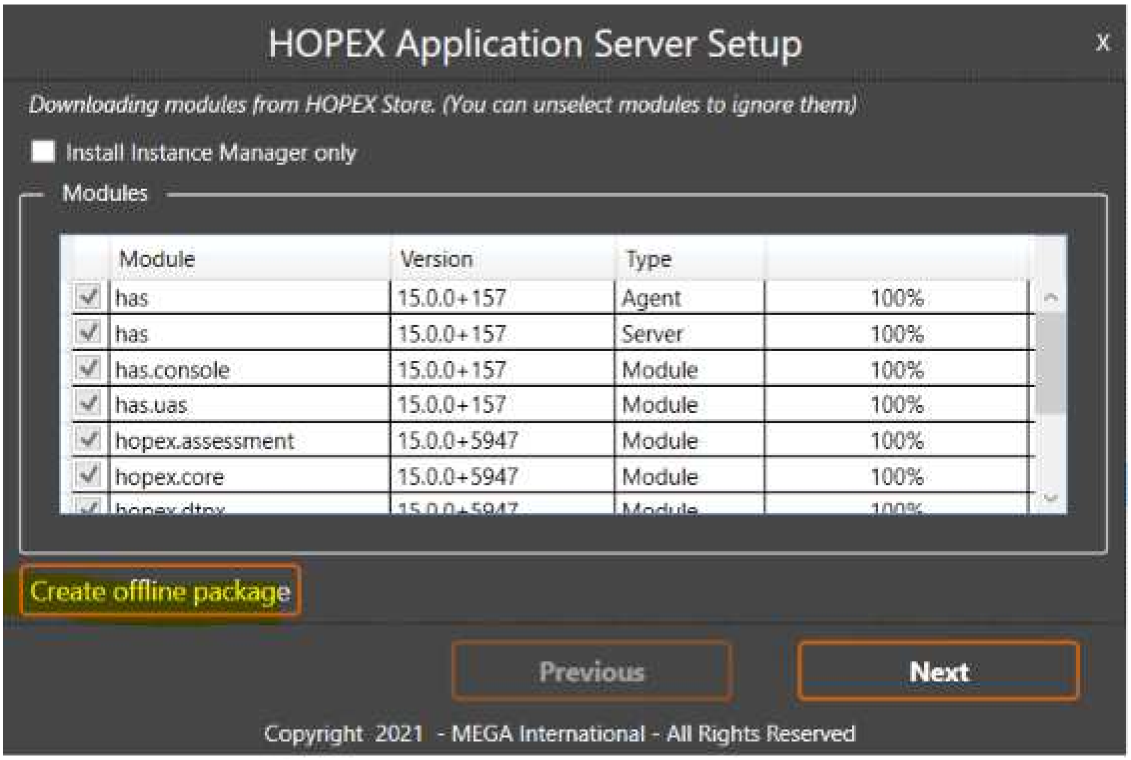
Module mode constraints do not match current server mode Production

3.1.7.How to create an offline package?

You need an internet access to HOPEX Store.

Run HAS installer, ex: Hopex.Application.Server-1.0.94.Setup.exe

Start installation as usual but click **Create offline package**



HOPEX Application Server Setup

Downloading modules from HOPEX Store. (You can unselect modules to ignore them)

□ Install Instance Manager only

Modules

	Module	Version	Type	
☑	has	15.0.0+157	Agent	100%
☑	has	15.0.0+157	Server	100%
☑	has.console	15.0.0+157	Module	100%
☑	has.uas	15.0.0+157	Module	100%
☑	hopex.assessment	15.0.0+5947	Module	100%
☑	hopex.core	15.0.0+5947	Module	100%
☑	hopex.dtpx	15.0.0+5947	Module	100%

Copyright 2021 - MEGA International - All Rights Reserved

3.1.8.Unexpected login message 'You are not authorized to access this page'

When trying to login to HAS console, a message 'You are not authorized to access this page' is displayed. It likely that you tried to connect with a different login than the administrator login (Admin). Use administrator login to connect.

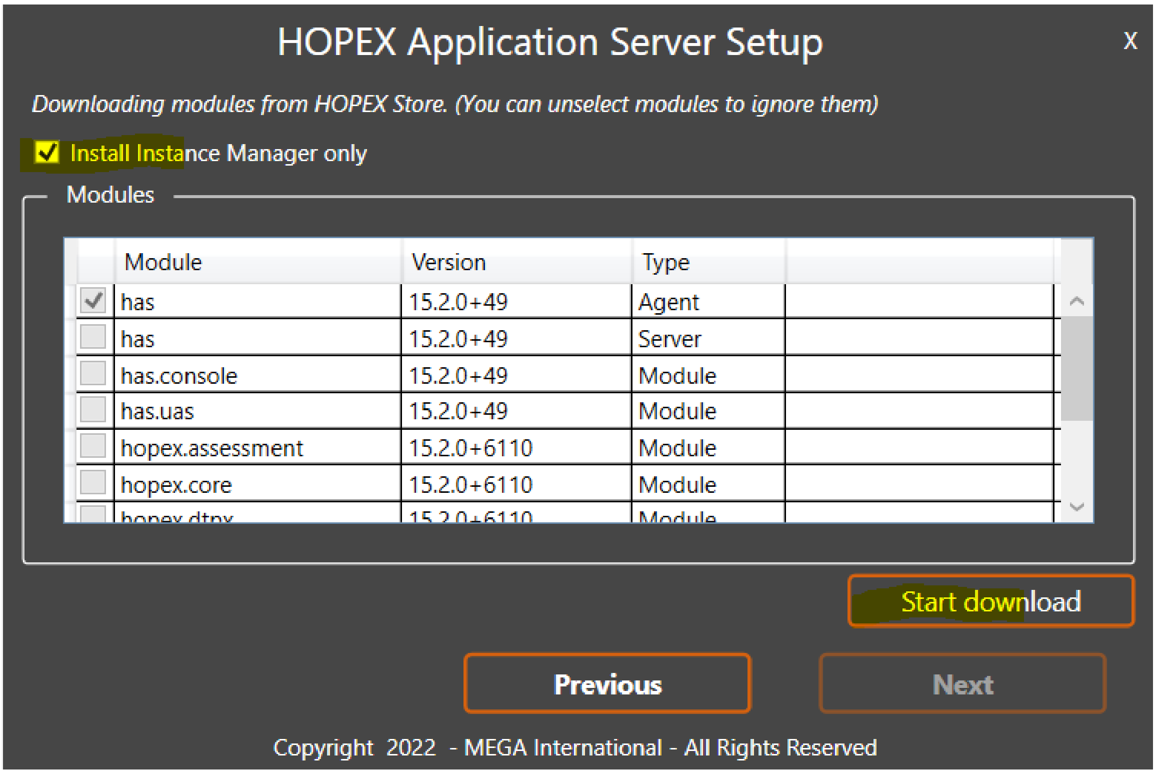
3.1.9.Unexpected error 'The Sql Server Client could not be found. ODBC Driver 17 for SQL Server may not be installed'

As said, ODBC Driver 17 for SQL Server is not installed. This is a technical requirement. Download and install ODBC Driver 17 for SQL Server.

3.1.10. Can I use the installer to update only the Instance manager

Yes. Run installer and check only Install Instance Manager Only.

Note that if the expected version of .NET core is not installed, the Instance Manager ill not restart. Verify that this pre-requisite fulfilled before running the setup.exe.



HOPEX Application Server Setup

Downloading modules from HOPEX Store. (You can unselect modules to ignore them)

☑ Install Instance Manager only

Modules

	Module	Version	Type
☑	has	15.2.0+49	Agent
□	has	15.2.0+49	Server
□	has.console	15.2.0+49	Module
□	has.uas	15.2.0+49	Module
□	hopex.assessment	15.2.0+6110	Module
□	hopex.core	15.2.0+6110	Module
□	hopex.dtpx	15.2.0+6110	Module

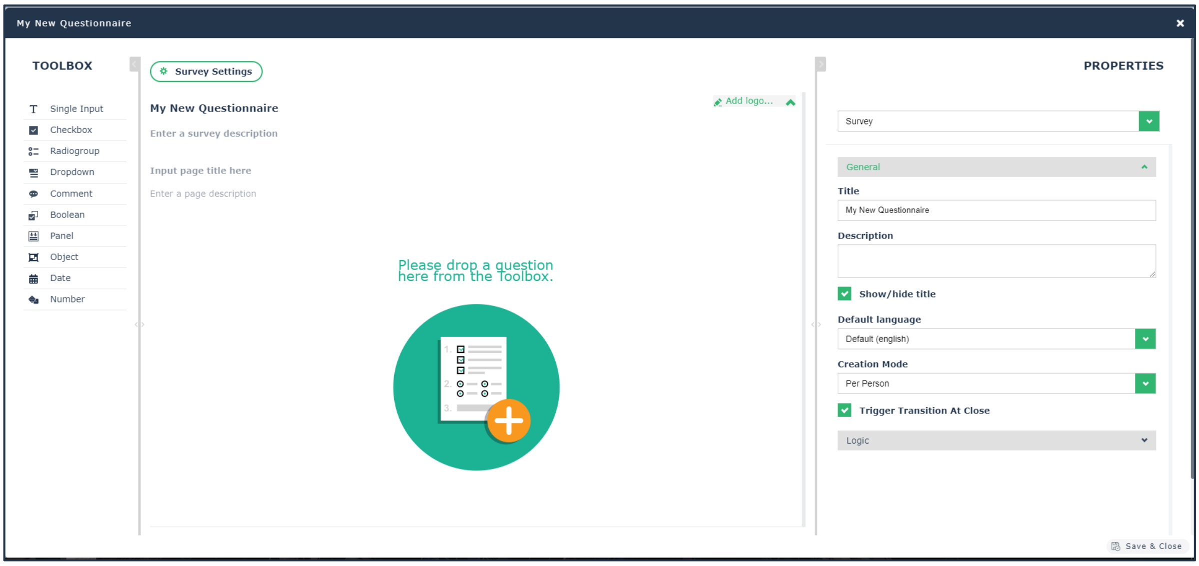
Copyright 2022 - MEGA International - All Rights Reserved

How to Migrate to Questionnaire Builder

1. Introduction

This document provides information about the impacts of the Questionnaire Builder module for existing HOPEX users. It is intended to help understand what has been done to ensure a smooth transition to Questionnaire Builder.

NOTE: For more information on how to manage questionnaire templates through Questionnaire Builder, see the following section: **Common Features > Managing Assessments > Managing Questionnaire Templates.**



My New Questionnaire

Title: My New Questionnaire

☑ Show/hide title

Default language: Default (english)

Creation Mode: Per Person

☑ Trigger Transition At Close

Questionnaire Builder provides a completely renovated and modern user experience when it comes to building questionnaires for your assessment campaigns.

2. Questionnaire Template Migration Process

Before migrating to HOPEX V5, make sure all assessment/execution campaigns are closed.

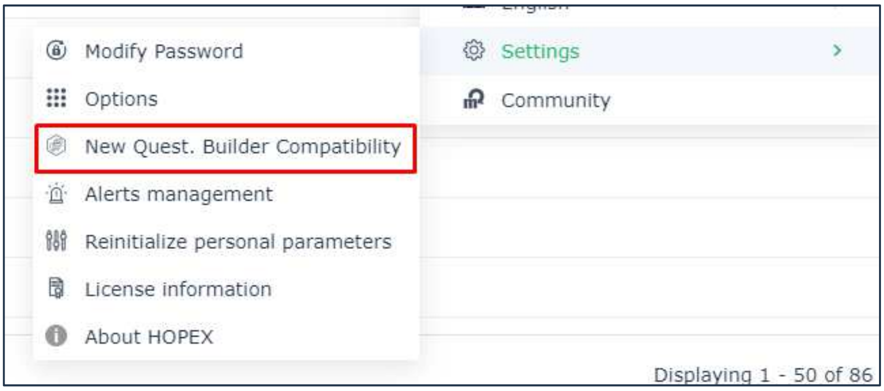
Once the migration towards the new version is completed, the following happens:

- All existing Questionnaire Templates are automatically flagged based on whether they are fully compatible with Questionnaire Builder or not.
- Question Groups defined on objects, like Test and Execution Steps for Controls, are converted to Questionnaire Templates, to provide a consistent user experience.
- All simple and multiple Direct Assessments propose a new layout to the respondent.

After migration, you can use the Questionnaires Templates Compatibility report. It enables you to double check if some elements of your existing questionnaire templates have not been converted due to compatibility issues.

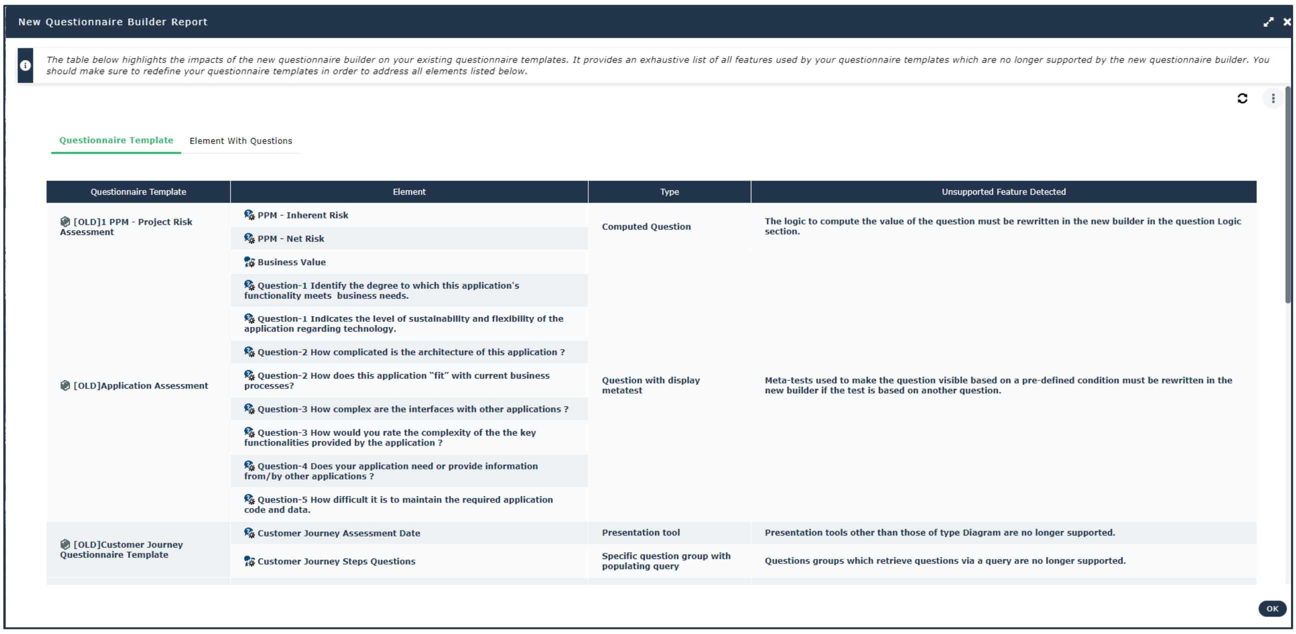
2.1. Compatibility Analysis Report

To have a comprehensive understanding of the impacts of Questionnaire Builder on existing questionnaire templates, a dedicated report is available via the main menu.



This report browses all existing questionnaire templates and questions defined on HOPEX elements (like control execution and test steps). The report shows all the elements that are no longer compatible with Questionnaire Builder, with a small description of the identified issue.

This report is informative only. It should be used to make sure the migration has not introduced any major disruption from a functionality perspective.



The table below highlights the impacts of the new questionnaire builder on your existing questionnaire templates. It provides an exhaustive list of all features used by your questionnaire templates which are no longer supported by the new questionnaire builder. You should make sure to redefine your questionnaire templates in order to address all elements listed below.

Questionnaire Template	Element	Type	Unsupported Feature Detected
[OLD]1 PPM - Project Risk Assessment	PPM - Inherent Risk	Computed Question	The logic to compute the value of the question must be rewritten in the new builder in the question Logic section.
	PPM - Net Risk		
[OLD]Application Assessment	Business Value	Question with display metatest	Meta-tests used to make the question visible based on a pre-defined condition must be rewritten in the new builder if the test is based on another question.
	Question-1 Identify the degree to which this application's functionality meets business needs.		
	Question-1 Indicates the level of sustainability and flexibility of the application regarding technology.		
	Question-2 How complicated is the architecture of this application ?		
	Question-2 How does this application "fit" with current business processes?		
	Question-3 How complex are the interfaces with other applications ?		
	Question-3 How would you rate the complexity of the the key functionalities provided by the application ?		
	Question-4 Does your application need or provide information from/by other applications ?		
	Question-5 How difficult it is to maintain the required application code and data.		
[OLD]Customer Journey Questionnaire Template	Customer Journey Assessment Date	Presentation tool	Presentation tools other than those of type Diagram are no longer supported.
	Customer Journey Steps Questions	Specific question group with populating query	Questions groups which retrieve questions via a query are no longer supported.

2.2. Not Compatible Questionnaire Templates

If you try to open a non-compatible questionnaire template, an informative wizard lists all the questionnaire elements not supported by Questionnaire Builder.

You can either decide to edit the questionnaire to remove the concerned elements or launch the new builder: the elements which are not compatible will simply be disregarded by Questionnaire Builder.

2.3. Compatible Questionnaire Templates

If you try to open a compatible questionnaire template, Questionnaire Builder will automatically open in full screen mode.

3. Question Types

Questionnaire Builder not only introduces new question types. It also renames some of the question types originally provided by HOPEX.

The table below provides detailed information regarding the mapping between old HOPEX question types and new ones.

Each HOPEX question type has a dedicated section to further explain how Questionnaire Builder handles it.

HOPEX Question Type	New Builder Question Type
Text	Comment
Vertical Radio	Radiogroup
ComboList	Dropdown
Multiple Answer Type	Depending on content
Date	Date
Number	Number
Boolean	Boolean
Multiple Values	Object
Short	Number
Duration	Single Input
Object	Object
OK/NO/NA	Dropdown
Percent	Single Input
Signed Number	Single Input
String	Single Input
Question Group	Panel

3.1. Text

The question type "Text" has been renamed into "Comment".

3.2. Vertical Radio

The question type "Vertical Radio" has been renamed into "Radiogroup".

3.3. ComboList

The question type "ComboList" has been renamed into "Dropdown".

3.4. Multiple Answer Type

HOPEX provided a question of type "Multiple Answer Type". This type of question allowed to define several sub-questions of different types.

This type of question is no longer available in the new Builder. In case of existing questions of type "Multiple Answer Type", the new Builder automatically converts them into elementary questions (one per type).

3.5. Date

The question type "Date" still exists and has kept its original name.

3.6. Number

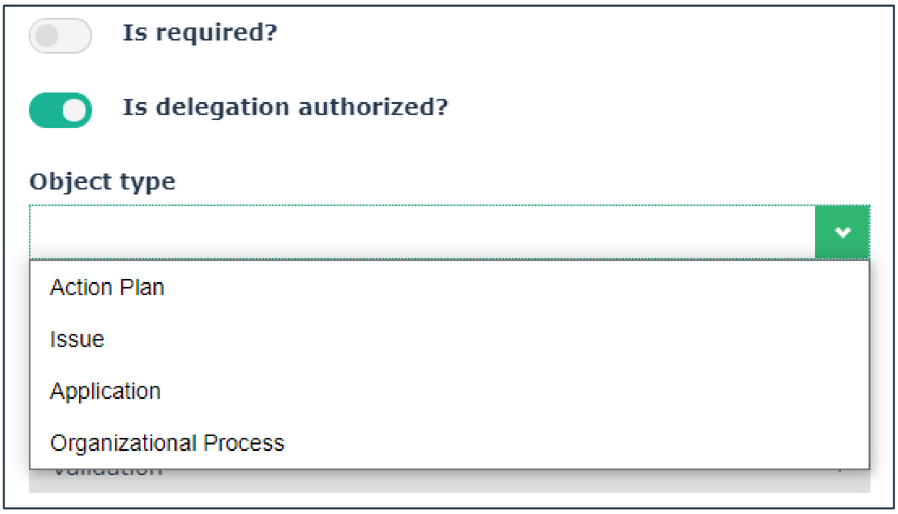
The question type "Number" still exists and has kept its original name.

3.7. Boolean

The question type "Boolean" still exists and has kept its original name.

3.8. Multiple Values

The question type "Multiple Values" has been renamed into "Object". A parameter in the question's property pane allows to define which HOPEX object must be used to answer the question.



○ Is required?

● Is delegation authorized?

Object type

3.9. Short

The "Short" question type no longer exists. All its instances are automatically converted into the "Number" equivalent type.

3.10. Duration

The question type "Duration" does no longer exist. All its instances are automatically converted into the type "Single Input" which allows to answer with a string of characters.

3.11. Object

The “Object” question type still exists and has kept its original name. Nevertheless, only a limited number of HOPEX meta-classes are proposed in the standard version. These meta-classes are connected to the ~dmuyO(mWU1AW[Answered Element] metaclass. Therefore, if additional meta-classes must be proposed for questions of type “Object”, you just need to connect them to this metaclass.

The comprehensive list of meta-classes available in the standard is as follows:

- Action Plan
- Issue
- Application
- Organizational Process
- ~jdFzaq1Bkyb1[Column]
- ~YXRV)88Dp0G1[Attribute]
- ~JafR4ysPDHU0[Part]
- ~bSvJYPrkR9)V[Computed Concept Component]
- ~dZEodwirR1N8[Computed Part]
- ~0XEovwirRTR8[Computed Attribute]
- ~0(eRvBHhKnzc[Information Item Component]
- ~Dr22mynkRHv7[Computed Concept Information Item]
- ~PKkZR)eOBz80[Concept Component]
- ~OYRZREhzC1y0[Concept Type Component]

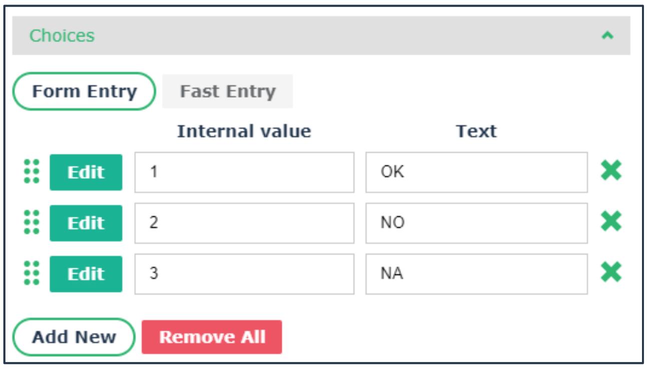
3.12. OK/NO/NA

The “OK/NO/NA” question type no longer exists. All its instances are automatically converted into the “Dropdown” equivalent type.

3.12.1. Aggregation Schemas

When creating new questions of OK/NO/NA type that must be used in the context of standard aggregation schemas, it is important to add the following values to the possible answers’ internal values:

- Internal Value = 1 for possible answer “OK”
- Internal Value = 2 for possible answer “NO”
- Internal Value = 3 for possible answer “NA”



Internal value	Text
1	OK
2	NO
3	NA

3.13. Percent

The "Percent" question type no longer exists. All its instances are automatically converted into the "Single Input" type which allows to answer with a string of characters.

3.14. Signed Number

The "Signed Number" question type no longer exists. All its instances are automatically converted into the "Single Input" type which allows to answer with a string of characters.

3.15. String

The "String" question type has been renamed into "Single Input".

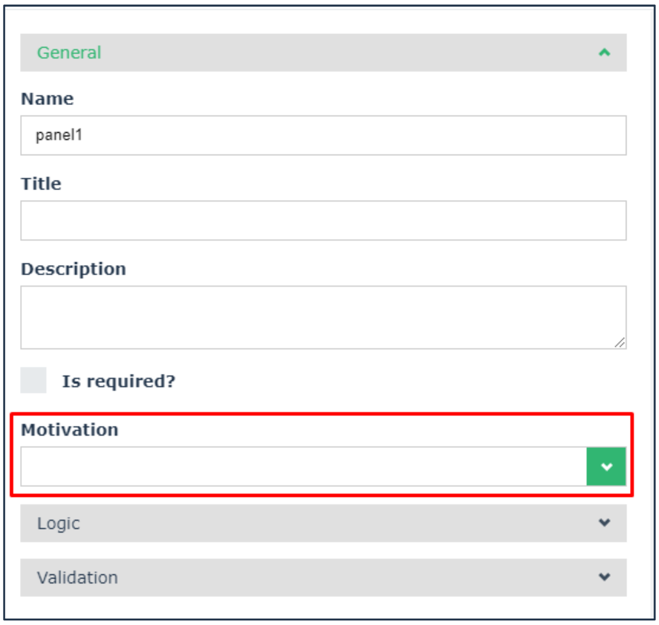
3.16. Question Group

In HOPEX a question of "Question Group" type was used for two main use cases:

1) To group multiple questions.
2) To dynamically select questions defined on meta-lasses or objects (e.g., on controls for execution and test steps).

Both use cases are still supported with the new questionnaire builder via the renamed "Panel" question type.

To specify whether the question panel should be dynamically populated with questions belonging to a specific "Questionning Motive", a dedicated parameter called "Motivation" has been added to the panel property pane.



General

Name: panel1

Title:

Description:

□ Is required?

Motivation:

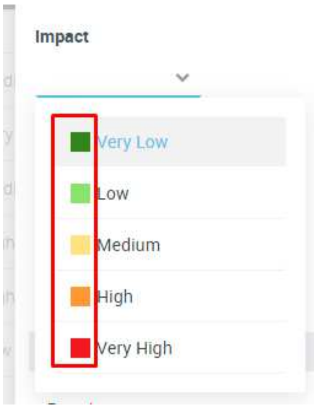
3.17. Checkbox

It is a new question type which allows to define questions with multiple possible answers of "checkbox" type.

4. Removed/Reviewed Features

4.1. Pictures in drop-down questions

Drop down questions cannot display colored icons next to the drop-down value. This was the case for questions like "Risk Impact" which were displaying a colored squared icon, based on the answer.

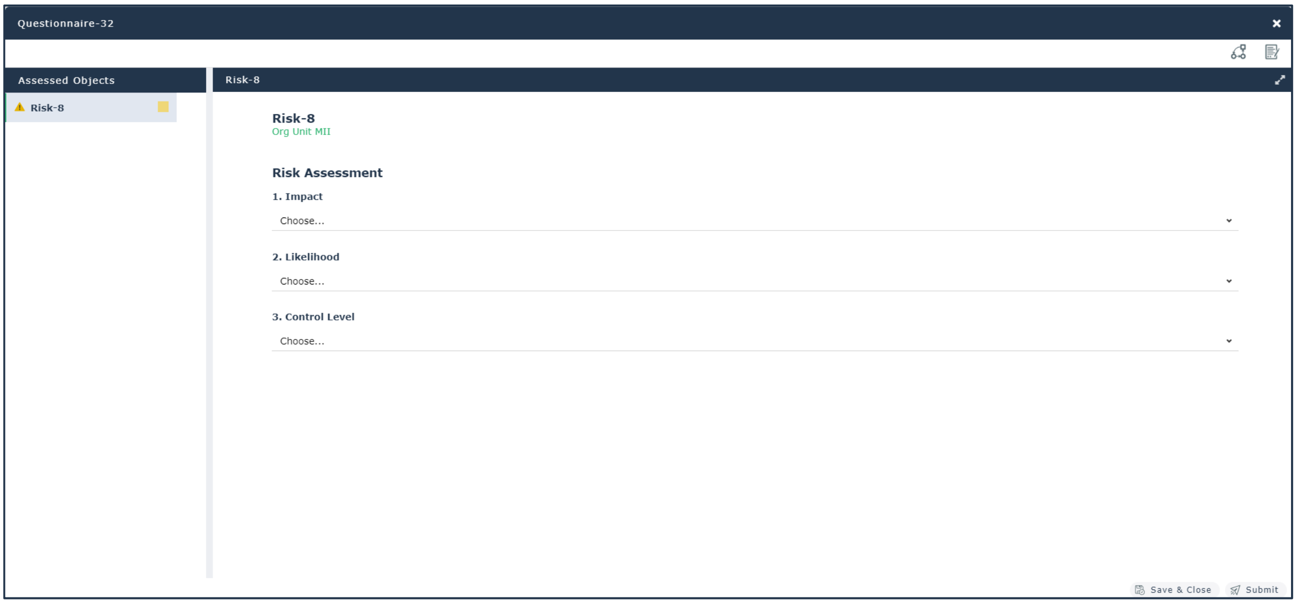


4.2. Create HOPEX Object as answer to question

In HOPEX V5 it is not possible to create HOPEX objects when answering questions of "Object" type. The only option is to select an existing one.

4.3. Questionnaire Layout

With Questionnaire Builder, a lot of effort was put into designing a new layout proposed to questionnaire's respondents. This new layout replaces the old ones. Therefore, tabular entry is no longer provided as an option to answer questionnaires.



4.4. Questionnaire Template Presentation

It is no longer possible to define a Questionnaire Template Presentation on the Questionnaire Template.

The only option which is still available is accessible via the properties pane of the questionnaire. It is the property:

- **Creation Mode** – To define how the questionnaires should be created in the context of a campaign (one per person, one per assessed object, one per context)

The following options are no longer available:

- Presentation Mode
- Matrix number per page
- Introduction Page Displaying
- Display an ending page
- Checks Page Displaying
- Question Comment Display
- Display a page to add documents
- Each Question in a group Displaying
- Context in a group
- Context group folded
- Scoring Displaying
- Historic Displaying
- Trigger Transition At Close
- Display explanatory documents
- Display explanatory external references

4.5. Presentation Tools

These objects are no longer supported. Nevertheless, for questionnaires on processes, the new layout automatically allows access to the process diagram, when it exists.

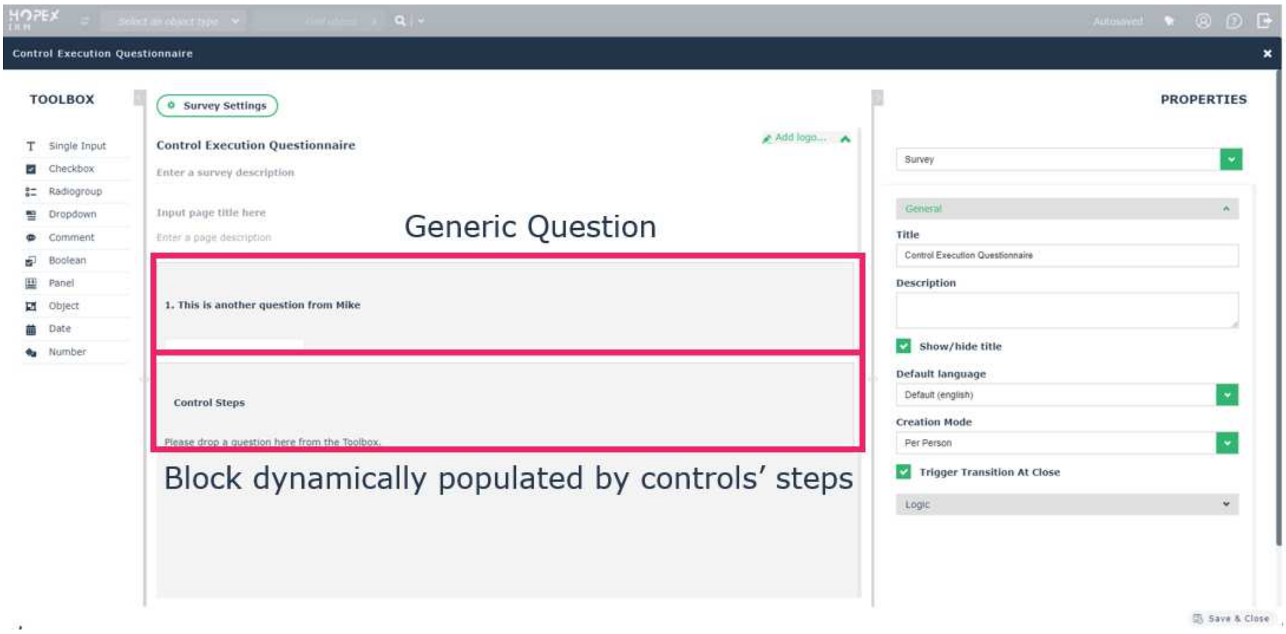
4.6. Inherited Questions

HOPEX allowed to define questions at the metaclass level, so that they would be automatically fetched on questionnaires assessing the metaclass instances. A practical example of this mechanism is the “Inherited Control Steps”: questions defined at the Control metaclass level, that would be automatically fetched by questionnaires assessing controls.

This mechanism is no longer supported, and it has been replaced by another one.

Customers using inherited questions must re-create them in the questionnaire template used by their campaign (e.g., the “Control Execution Questionnaire” questionnaire template for the “Control Execution” assessment template).

The following screenshot shows an example of the “Control Execution Questionnaire” questionnaire template used by Control Execution assessment campaigns, where a generic question has been created, followed by a block which is dynamically populated by the control steps.



Control Execution Questionnaire

1. This is another question from Mike

Control Steps

Please drop a question here from the Toolbox.

Survey

Title: Control Execution Questionnaire

Description:

☑ Show/hide title

Default language: Default (english)

Creation Mode: Per Person

☑ Trigger Transition At Close

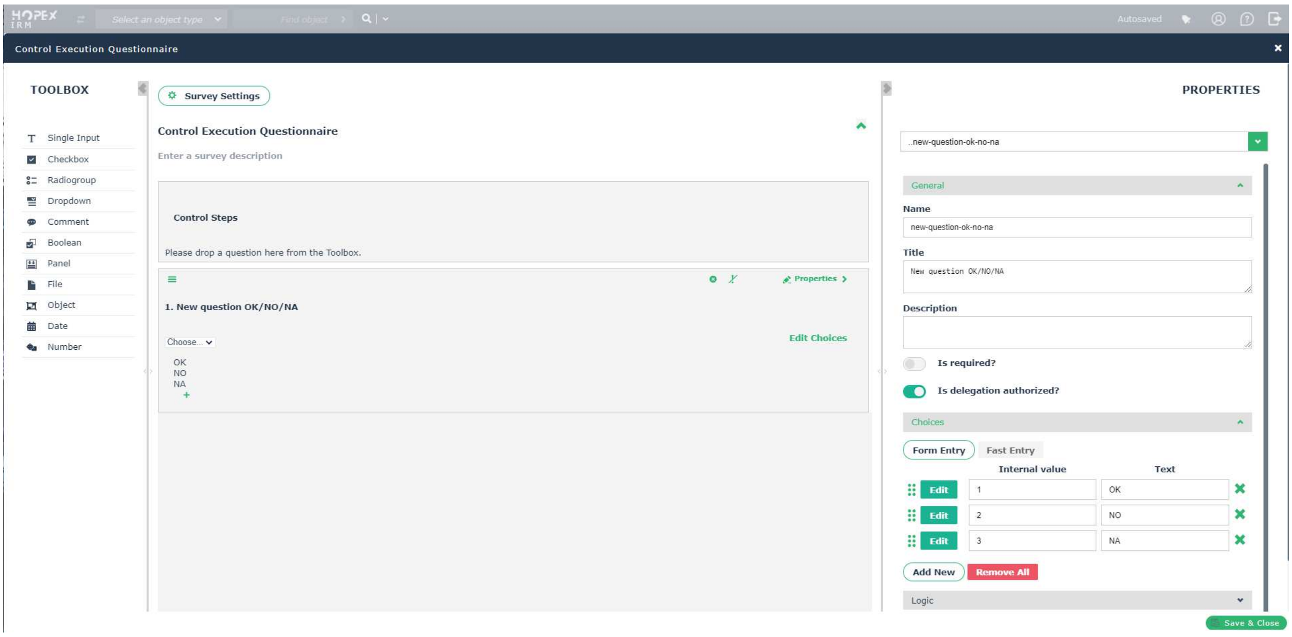
Logic

4.6.1. Aggregation of Inherited Controls Steps

When creating generic questions, you might want to include the question answers in an aggregation schema. To do so, you must make sure to connect the question answer to the existing scoring rule.

Below is an example where a new question of “dropdown” type, with possible answers “OK”, “NO” and “NA”, called “New question OK/NO/NA” is defined in the questionnaire template used by control execution campaigns.

The question will be asked with respect to all controls in the scope of the campaign. To make sure it is included in the aggregation schema launched once the campaign’s session has been closed, the user must connect its answer to the existing “OK/KO Scoring Rule” scoring rule.



Control Execution Questionnaire

Enter a survey description

Control Steps

Please drop a question here from the Toolbox.

1. New question OK/NO/NA

Choose...

OK
NO
NA

..new-question-ok-no-na

Name: new-question-ok-no-na

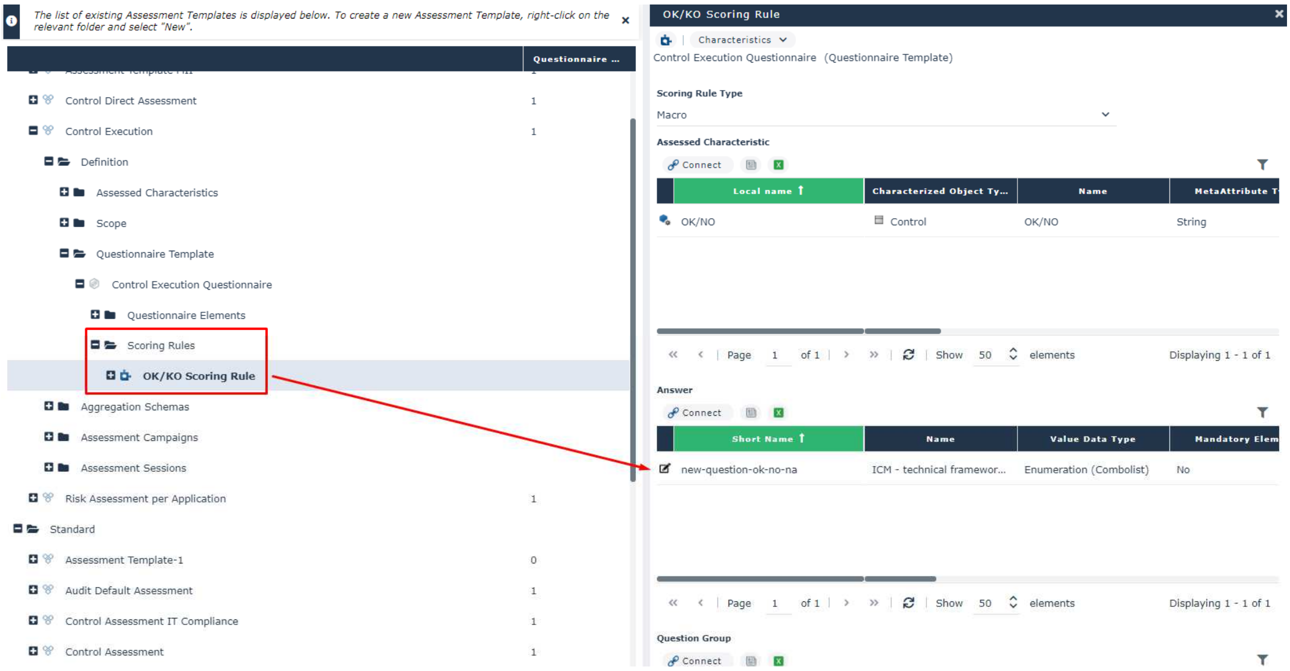
Title: New question OK/NO/NA

Description:

Is required?

Is delegation authorized?

Internal value	Text
1	OK
2	NO
3	NA



The list of existing Assessment Templates is displayed below. To create a new Assessment Template, right-click on the relevant folder and select "New".

	Questionnaire ...
Control Direct Assessment	1
Control Execution	1
Definition	
Assessed Characteristics	
Scope	
Questionnaire Template	
Control Execution Questionnaire	
Questionnaire Elements	
Scoring Rules	
OK/KO Scoring Rule	
Aggregation Schemas	
Assessment Campaigns	
Assessment Sessions	
Risk Assessment per Application	1
Standard	
Assessment Template-1	0
Audit Default Assessment	1
Control Assessment IT Compliance	1
Control Assessment	1

OK/KO Scoring Rule

Control Execution Questionnaire (Questionnaire Template)

Scoring Rule Type: Macro

Assessed Characteristic

Local name	Characterized Object Ty...	Name	MetaAttribute T
OK/NO	Control	OK/NO	String

Answer

Short Name	Name	Value Data Type	Mandatory Elem
new-question-ok-no-na	ICM - technical framewor...	Enumeration (Combolist)	No

Question Group

4.6.2. Inherited Test Steps

It is no longer possible to define inherited test steps to be used within Test Sheets.

4.7. Meta Tests

In older versions, HOPEX allowed to define meta tests of two types on each question:

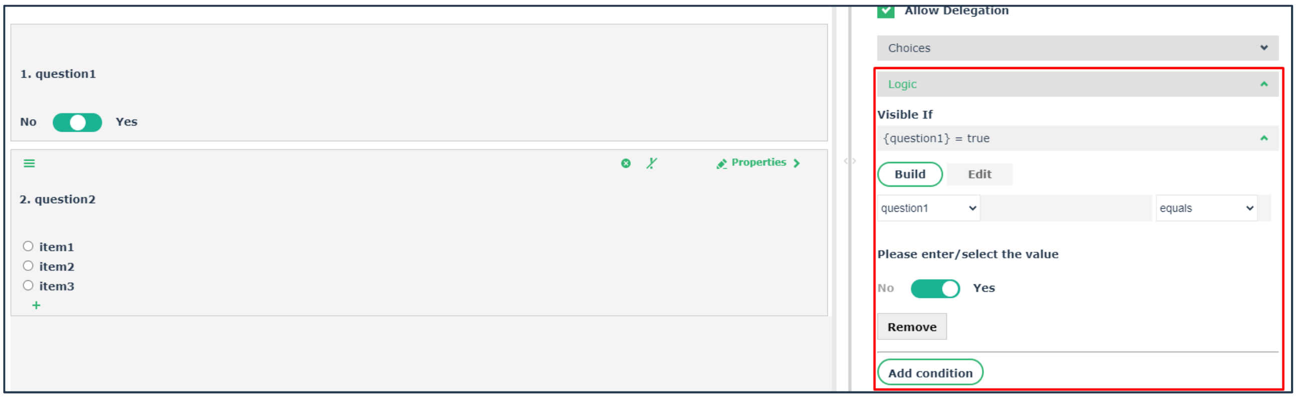
1. Those defining whether a question should be visible/mandatory or not based on the answer to previous question(s)
2. Those whose logic depends on actual HOPEX data

The former type of meta-tests will have to be rewritten in the new Questionnaire Builder.

The latter are still supported, and can be defined, accessing the question property page from HOPEX.

4.7.1. Write Logical Expressions in the new Builder

To write logical expressions affecting whether a question is visible, or mandatory based on pre-defined conditions, the user must use the dedicated Logic section, available in the new Questionnaire Builder, accessing the question property pane.



4.8. Delegation

Delegation must now be defined at the question level. By default, every question can be delegated, otherwise the option must be disabled in the question properties pane.

This means that it is no longer possible to define delegation either at the questionnaire template level or question group level.

4.9. Questions Group Populated by Query

HOPEX allowed to define question groups which were dynamically populated by a query. This mechanism is no longer available.

4.10. Questions with Link Answered Objects

HOPEX allowed to define questions whose answer would be automatically linked to the assessed object. This mechanism was used, for instance, when answering a question via a Business Document which was then connected to the assessed object.

This feature is no longer available.

4.11. Computed Questions

HOPEX allowed to create questions whose answer was automatically computed.

This feature is no longer available.

RDBMS Repository Installation Guide

Contents

Summary

This technical article describes the procedures and best practices for deploying the HOPEX application on a relational database server (SQL Server).

This deployment applies to **HOPEX Aquila**.

Generalities

Unsupported HOPEX Features in RDBMS Storage

When a HOPEX repository is stored on an RDBMS, HOPEX does not support the following features:

- MySQL RDBMS
- Oracle RDBMS
- Offline mode
- Repository protection
- Mixed environments
    - MEGA proprietary format (GBMS storage format) repository and repositories stored on an RDBMS. For example, a GBMS environment (SystemDb) and one or more repositories stored on SQL Server. The opposite is also not supported (SQL Server environment with GBMS repositories within).

Expected Advantages

The advantages expected from an RDBMS deployment are:

- Compliance with company-wide IT standards.
- Guarantee of scalability and security.
- Quicker dispatch time. In particular with "big" HOPEX private workspaces (HOPEX private workspaces with many creations/deletions/updates).

With this type of architecture, HOPEX supports global deployment on the same repository. In particular, it enables bypassing some limits related to the GBMS storage format.

- Maximum limit of 510 concurrent private workspaces per environment. No limit is identified in the HOPEX application for SQL Server storage format.
- Maximum limit of 24 GB of data per HOPEX repository. No limit is identified in the HOPEX application for SQL Server storage format.

With the RDBMS storage format, the HOPEX environment contains unshared files. All the data accessed during the execution of the HOPEX application is stored in the RDBMS. The RDBMS guarantees scalability and security.

Licensing

The "HOPEX repository storage (SQL Server)" product is required on the license to gain access to the RDBMS storage feature. The license can be dedicated to the workstation or shared by a group of users. All users connecting to HOPEX must have access to this license as well as to other products (HOPEX IT Architecture…).

Infrastructure Requirements

RDBMS Client

An RDBMS Client is necessary on each workstation that uses HOPEX with data stored on an RDBMS.

- **SQL Server**

Installation of Microsoft ODBC Driver 17 or 18 for SQL Server is required.

This Microsoft ODBC Driver 17 or 18 for SQL Server is compatible with the 2019 versions of SQL Server. See corresponding Microsoft articles for more details:

System Requirements, Installation, and Driver Files - ODBC Driver for SQL Server | Microsoft Docs

Download it from Microsoft download website:

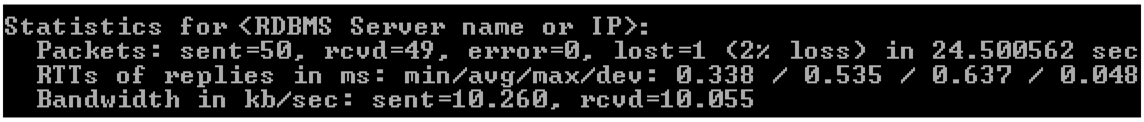
https://aka.ms/downloadmsodbcsql

Network Capability to Database Server

On a client computer running HOPEX, it is recommended to ping the RDBMS server with a filled buffer to have an evaluation of the infrastructure. To do this, download the **hrPING** freeware tool available at https://www.cfos.de/en/ping/ping.htm. To use this tool, you must first accept the terms of the licence. Use it with the following command in a command window from a computer that will be running HOPEX:

```
hrping.exe –W –l 5000 –n 50 –y <RDBMS Server name or IP>
```

Example for this command output:



```
Statistics for <RDBMS Server name or IP>:
  Packets: sent=50, rcvd=49, error=0, lost=1 (2% loss) in 24.500562 sec
  RTTs of replies in ms: min/avg/max/dev: 0.338 / 0.535 / 0.637 / 0.048
  Bandwidth in kb/sec: sent=10.260, rcvd=10.055
```

If the value returned for **"RTTs of replies in ms/avg"** (0.535 in the example) is higher than 1 ms, contact MEGA. See hrPING help for details on this command.

Database Server

The following sections will help your database administrator (DBA) size the Database server according to the profiles and the number of HOPEX users you plan to use.

Server disk size

Each new object takes up 30 KB on a disk (object with its attributes and links).

If you activate the HOPEX Repository Log file each action on the HOPEX repository creates an object.

You should reserve 5GB on the server disk.

Reminder:

HOPEX will stop working if the datafile is full. To avoid this, the databases can be created with the autoextend property activated. If this is not possible, the datafiles growth must be monitored carefully in order to provide more space if fullness is about to be reached.

Number of connections opened by HOPEX on the RDBMS for each HOPEX workstation

This information will help you define the amount of memory (RAM) required for the database instance used to run HOPEX on the database server

- **SQL Server**

One connection is used for each RDBMS storage. It means that, when a HOPEX User is connected to HOPEX, two connections to SQL Server are open (one for the SystemDb and one for the User repository).

An additional connection is used for each RDBMS storage when you use the HOPEX locks.

Each opened connection uses 24 KB of memory on the SQL Server.

HOPEX RDBMS Diagnostic Utility

Purpose

MEGA provides a Java based utility that should be used before starting to use environments and repositories on an RDBMS. This utility runs several tests for which the results will be compared to some memorized values corresponding to a situation where HOPEX is likely to have close-to-optimum performances.

The **RDBMS Diagnostic** utility is available in MEGA HOPEX Store (store.mega.com).

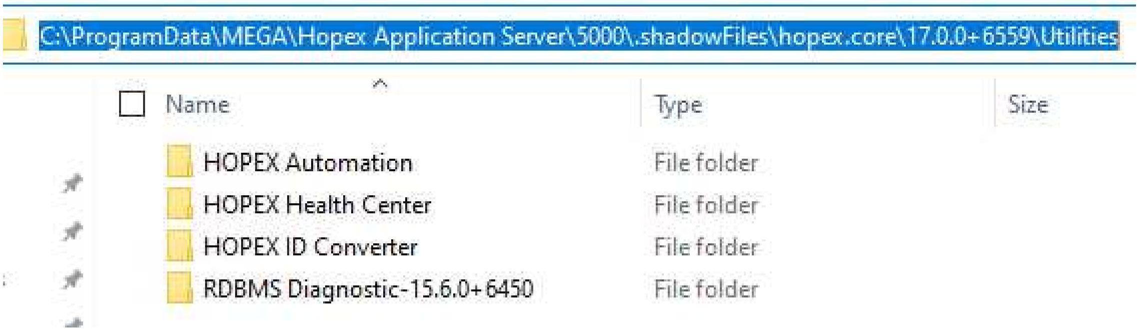
Running the RDBMS Diagnostic Utility

A batch file was created to run the tool.

To run the RDBMS Diagnostic Utility:

1. From MEGA HOPEX Store (store.mega.com), download **RDBMS Diagnostic** module.
2. Extract the content of the "RDBMS Diagnostic.zip" compressed file, for example in the **<HOPEX installation> > Utilities** folder:

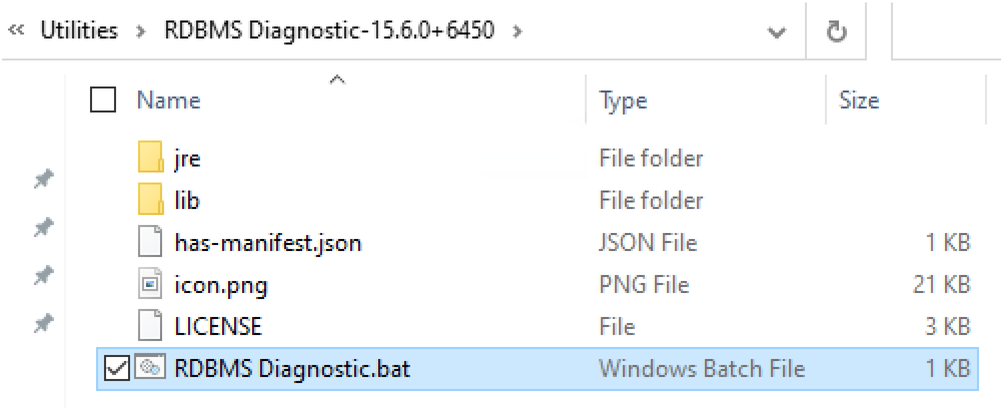
```
For example: ``C:\ProgramData\MEGA\HOPEX Application
Server\5000\.shadowFiles\hopex.core\15.6.0+6366\Utilities``
```



C:\ProgramData\MEGA\Hopex Application Server\5000\.shadowFiles\hopex.core\17.0.0+6559\Utilities

Name	Type	Size
HOPEX Automation	File folder	
HOPEX Health Center	File folder	
HOPEX ID Converter	File folder	
RDBMS Diagnostic-15.6.0+6450	File folder	

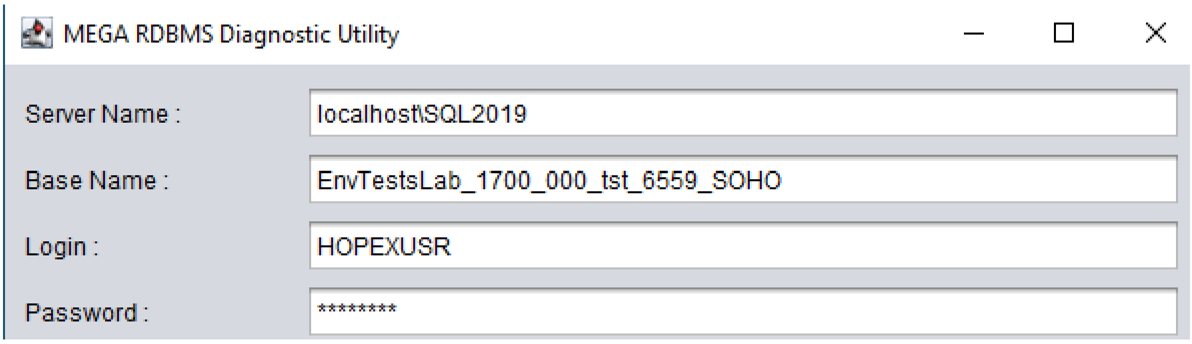
3. In the **RDBMS Diagnostic** folder, execute the **RDBMS Diagnostic.bat**.



« Utilities › RDBMS Diagnostic-15.6.0+6450 ›

□ Name	Type	Size
jre	File folder	
lib	File folder	
has-manifest.json	JSON File	1 KB
icon.png	PNG File	21 KB
LICENSE	File	3 KB
☑ RDBMS Diagnostic.bat	Windows Batch File	1 KB

4. Enter the connection information to the RDBMS storage that is the target for hosting the HOPEX data:
   - the server name
   - a database name



MEGA RDBMS Diagnostic Utility

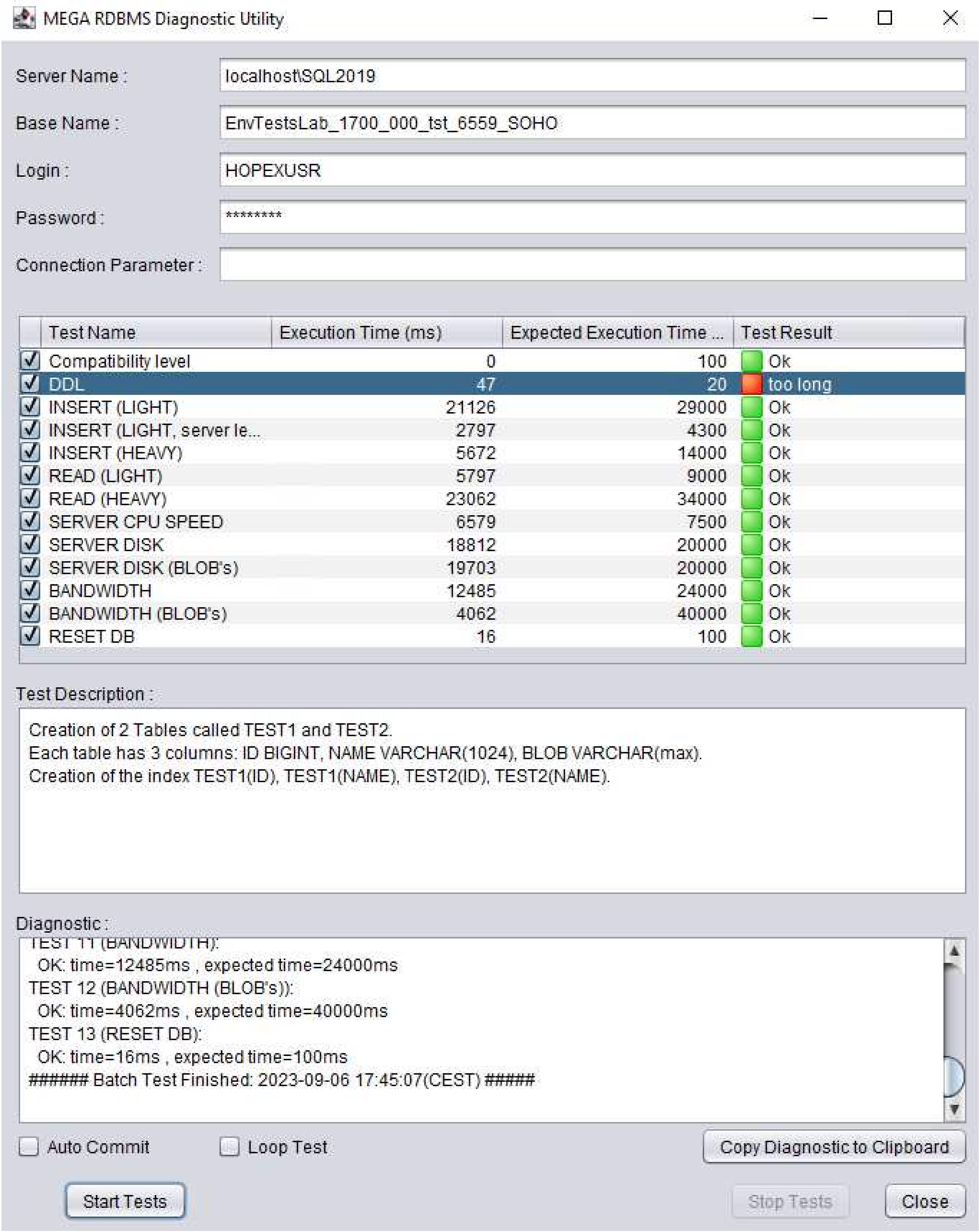
Server Name :	localhost\SQL2019
Base Name :	EnvTestsLab_1700_000_tst_6559_SOHO
Login :	HOPEXUSR
Password :	********

5. Click **Start Tests**.

6. To get consistent times, the **Expected Execution Time** values were recorded after running the utility more than once and noticing that the values were stable.

   So to get results that can be considered valid, run the utility twice and consider the values of the 2nd run.

Here is an example of test results:



Server Name : localhost\SQL2019

Base Name : EnvTestsLab_1700_000_tst_6559_SOHO

Login : HOPEXUSR

Password : ********

Connection Parameter :

	Test Name	Execution Time (ms)	Expected Execution Time ...	Test Result
☑	Compatibility level	0	100	🟩 Ok
☑	DDL	47	20	🟥 too long
☑	INSERT (LIGHT)	21126	29000	🟩 Ok
☑	INSERT (LIGHT, server le...	2797	4300	🟩 Ok
☑	INSERT (HEAVY)	5672	14000	🟩 Ok
☑	READ (LIGHT)	5797	9000	🟩 Ok
☑	READ (HEAVY)	23062	34000	🟩 Ok
☑	SERVER CPU SPEED	6579	7500	🟩 Ok
☑	SERVER DISK	18812	20000	🟩 Ok
☑	SERVER DISK (BLOB's)	19703	20000	🟩 Ok
☑	BANDWIDTH	12485	24000	🟩 Ok
☑	BANDWIDTH (BLOB's)	4062	40000	🟩 Ok
☑	RESET DB	16	100	🟩 Ok

Test Description :

Creation of 2 Tables called TEST1 and TEST2.
Each table has 3 columns: ID BIGINT, NAME VARCHAR(1024), BLOB VARCHAR(max).
Creation of the index TEST1(ID), TEST1(NAME), TEST2(ID), TEST2(NAME).

Diagnostic :

```
TEST 11 (BANDWIDTH):
  OK: time=12485ms , expected time=24000ms
TEST 12 (BANDWIDTH (BLOB's)):
  OK: time=4062ms , expected time=40000ms
TEST 13 (RESET DB):
  OK: time=16ms , expected time=100ms
###### Batch Test Finished: 2023-09-06 17:45:07(CEST) #####
```

□ Auto Commit   □ Loop Test

SQL Server support

SQL Server Requirements

Encoding

After the database has been created, verify that "Collation" is set to "SQL_Latin1_General_CP1_CS_AS". If the database is created from the HOPEX application, the appropriate encoding is automatically configured.

User management

When the HOPEX application accesses the HOPEX data stored in the RDBMS, it uses an SQL connection string. This connection string refers to a user account that has certain privileges for the instance.

This user can either be a native account, or a Windows account:

- **Native account**:
  - **Pros:** unique account, configured for everyone that runs the Web Front-End or Windows Front-End clients.
  - **Cons:** thought to be less secure.
- **Windows accounts/Domain account:** Trusted Connection
  - **Pros:** do not set up any connection string in the tool.
  - **Cons:** need to authorize several Windows accounts to have direct access to the data: the service account that runs the Instance manager, every user that needs to run the Windows Front-End client (Administration.exe or Hopex.exe).

Privileges for native account

You can have several kinds of SQL server users in relation to the customer security policy:

- **Standard security policy:** the user account is enabled to manage databases. This is the easiest solution especially if the SQL Server instance is dedicated to HOPEX.

User type	Comment	Server roles	Database roles	Server permissions
User with maximum privileges	Allowed to manage any database (create database, delete database, data read access, data write access, update database structure)	dbcreator	db_owner (1)	View server state (3)

- **Advanced security policy:** only the DBA is allowed to create new databases following specific naming rules. A user is required to use the existing databases.

User type	Comment	Server roles	Database roles	Server permissions
User with limited privileges	Allowed to use an existing database (data read access, data write access, update database structure)	public	db_owner (2)	View server state (3) sys.dm_db_index_physical_stats sys.indexes sys.stats FUNCTION::DB_ID

(1) db_owner role is automatically assigned by the system when a database is created.

(2) db_owner role is manually assigned by the DBA after database creation.

(3) To consult the view 'sys.dm_exec_sessions' for the server.

```
GRANT SELECT ON sys.dm_db_index_physical_stats TO [User];
GRANT SELECT ON sys.indexes TO [User];
GRANT SELECT ON sys.stats TO [User];
GRANT EXECUTE ON FUNCTION::DB_ID TO [[User];
```

The HOPEX application will create table, columns and index objects dynamically. The right to create Procedures is mandatory. Trigger, functions and view objects are not used.

Privileges for Windows accounts

Since this configuration requires to grant access to the different databases to several Windows accounts, and especially to accounts of people running the thick client of the application, it is recommended to limit those rights to a minimum, to reduce the risk of harming the application by directly modifying or deleting data.

- **Advanced security policy:** only the DBA is allowed to create new databases following specific naming rules. A user is required to use the existing databases.

User type	Comment	Server roles	Database roles	Server permissions
User with limited privileges	Allowed to use an existing database (data read access, data write access, update database structure)	public	db_ddladmin, db_datawriter and db_datareader (2)	View server state (3) sys.dm_db_index_physical_stats sys.indexes sys.stats FUNCTION::DB_ID

(2) These roles are manually assigned by the DBA after database creation.

(3) To consult the view 'sys.dm_exec_sessions' for the server.

```
GRANT SELECT ON sys.dm_db_index_physical_stats TO [User];
GRANT SELECT ON sys.indexes TO [User];
GRANT SELECT ON sys.stats TO [User];
GRANT EXECUTE ON FUNCTION::DB_ID TO [[User];
```

The HOPEX application will create table, columns and index objects dynamically. The right to create Procedures is mandatory. Trigger, functions and view objects are not used.

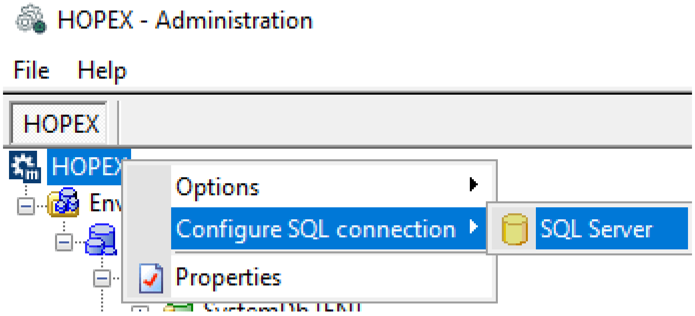
The Windows users **should not** have the “db_creator” server role.

Defining a HOPEX SQL Server Connection

A **Configure SQL Connection** menu is available in the HOPEX Administration application at different levels (site, environment, and repository) if the license contains the Repository Storage (SQL Server) product.

Procedure with a native SQL account

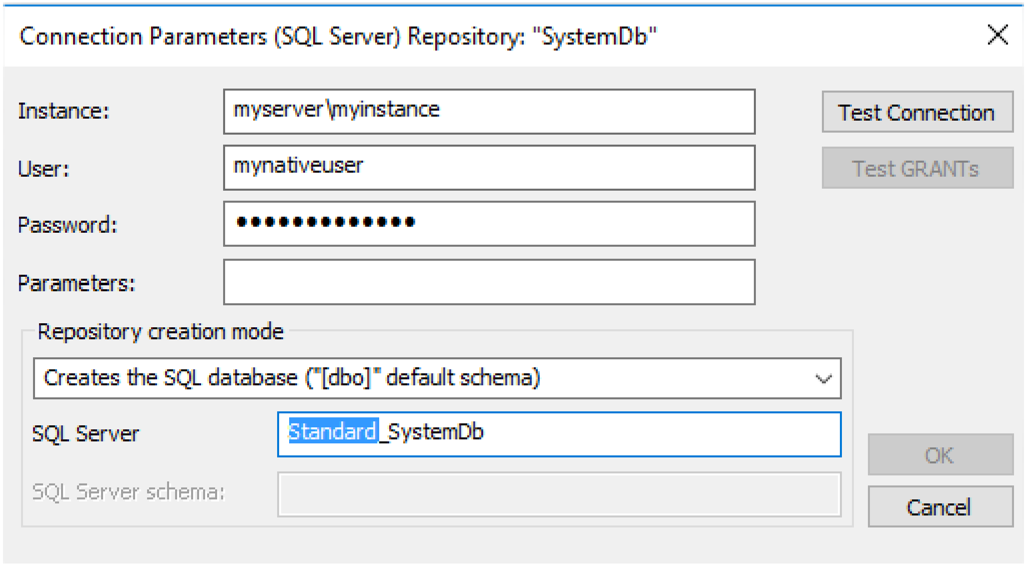
1. Start HOPEX **Administration.exe**.
2. Right-click HOPEX (the root of the administration tree) and select **Configure SQL connection > SQL Server**.



3. Enter the connection parameters.
   - **Instance:** <machine network name>\<SQL Server instance name> (1)

     Example for a standalone installation with SQL Express: MyMachine\SQLEXPRESS
   - **User:** user enabled to access/update SQL Server
   - **Password:** password of the user enabled to access/update SQL Server

     ⚠ **Warning:** Ensure this password is consistent with MS SQL rules, see MS related documentation.
4. Click **Connection Test** to check the connection parameters.



Connection Parameters (SQL Server) Repository: "SystemDb"

Instance: myserver\myinstance

User: mynativeuser

Password: •••••••••••••

Parameters:

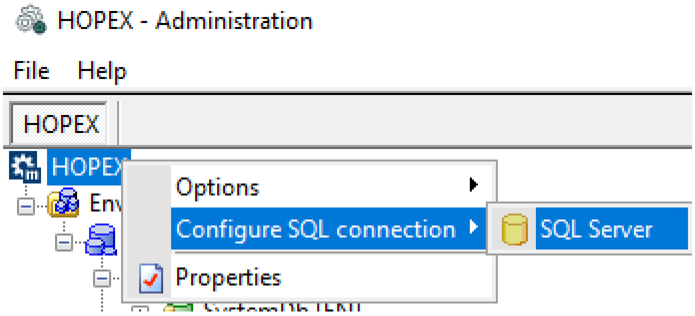
Repository creation mode: Creates the SQL database ("[dbo]" default schema)

SQL Server: Standard_SystemDb

SQL Server schema:

Procedure when using Windows authentication

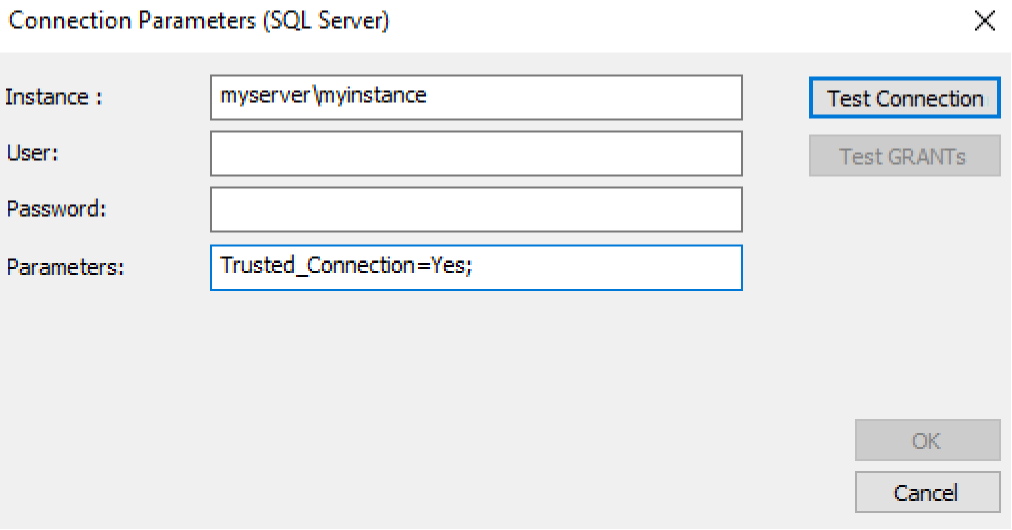
1. Start HOPEX **Administration.exe**.
2. Right-click HOPEX (the root of the administration tree) and select **Configure SQL connection > SQL Server**.



3. Set the connection parameters.
   - **Instance:** <machine network name>\<SQL Server instance name> (1)

     Example for a standalone installation with SQL Express: MyMachine\SQLEXPRESS
   - **User:** leave blank
   - **Password:** leave blank
   - **Parameters :** set "Trusted_Connection=Yes;"

     You may need to add Encrypt=no or Encrypt=Yes
4. Click **Connection Test** to check the connection parameters.



Connection Parameters (SQL Server)

Instance : myserver\myinstance

User:

Password:

Parameters: Trusted_Connection=Yes;

Creating an Environment

The environment creation mainly consists in creating a SystemDb repository. For SQL server, two creation modes are available from HOPEX:

- Creating a new database on the SQL Server (standard security policy)
- Using an existing database of the SQL Server (advanced security policy)

Prerequisite

Before creating an environment, download the ***HOPEX Environment Installation Package Aquila*** module from HOPEX store (https://store.mega.com/modules/details/hopex.core.install) and import it in HAS Console modules.

Creating a new SystemDb database

Prerequisite:

- Identify the SQL connection parameters (RDBMS instance, user, password)
- Identify the location of the environment folder on the file server

Procedure:

1. Start HOPEX **Administration.exe**.
2. Right-click the **Environments** folder and select **New**.
3. Enter the environment **Name**.

   This creates a folder on the file server.
4. (If needed) Change the **Location**.
5. Click **OK**.
6. Confirm or change SQL Connection parameters.
7. As the **Repository Creation Mode** select “Create Database”.
8. Click **Test Connection** to check that the SQL Server is reachable. This step must be successful for the process to continue.
9. Click **Test GRANTs** to check different actions (table creations, indexing columns etc.) that are necessary for HOPEX to be able to work. This step must be also successful for the process to continue.
10. Click **OK** to start the environment creation.

Result:

- A SystemDb repository stored in the selected RDBMS instance is created.
- A folder (HOPEX environment folder) is created at the selected location. This folder contains several files and subfolders (Db, Mega_usr, SysDb).

Using an existing SystemDb database

Prerequisite:

- Identify the SQL connection parameters (RDBMS instance, user, and password).
- Identify the location of the environment folder on the file server.
- **Check that the "Collation" property of the database is set to "SQL_Latin1_General_CP1_CS_AS".**
- Identify the exact name of the user database in the SQL Server. It follows this naming rule:

  ```
  <EnvironmentName>_SystemDb
  ```

  ```
  Example: MyEnvironment_SystemDb
  ```

  Note: the environment name must match the environment folder.

Procedure:

1. Start HOPEX **Administration.exe**.
2. Right-click the **Environments** folder and select **New**.
3. Enter the environment "Name" (in this example : "Name" = "MyEnvironment") This creates a folder.
4. (If needed) Modify the **Location**.
5. Click **OK**.
6. Confirm or change the SQL Connection parameters.
7. As **Repository Creation Mode** select "Uses an existing SQL database ("[dbo]" default schema)".
8. Click **Test connection** to check that the SQL Server is reachable.

   This step must be successful for the process to continue. If "Use existing database" option was specified, this test tries to connect to the database matching the following pattern: "MyEnvironment_SystemDb". This test must be successful for the process to continue.
9. Click **Test Grants** to check different actions (tables creations, indexing columns etc.) that are necessary for HOPEX to be able to work. This test must be also successful for the process to continue.
10. Click **OK** to start the environment creation.

Result:

- The SystemDb repository is initialized.
- A folder (HOPEX environment folder) is created at the selected location. This folder contains several files and subfolders (Db, Mega_usr, SysDb).
- Default users:
  - **Identifier**: System, **Password:** Hopex (or empty for previous HOPEX versions)
  - **Identifier:** Mega, **Password:** Hopex (or empty for previous HOPEX versions)

Creating a Repository

Two creation modes are available from HOPEX:

- Creating a new database on the SQL Server (standard security policy).
- Using an existing database of the SQL Server (advanced security policy).

Creating a new SQL Server database

Prerequisites:

- Identify the SQL connection parameters (RDBMS instance, user, and password).

Procedure:

1. Start HOPEX **Administration.exe**.
2. Connect to the environment concerned.

   Use for example: **Identifier**: System, **Password**: Hopex (or empty for previous HOPEX versions).
3. Right-click the **Repositories** folder and select **New**.
4. Enter the repository **Name**.
5. Keep the default **Location**.
6. Keep the **Import module standard data** option selected.

   This option enables to import the .xmg files of the modules already deployed on the HAS instance.

   Note: If you create several repositories, clear the **Import module standard data** option and once all of your repositories are created launch the **Environment Automatic Update**. Else, keep the option selected for the last repository creation only.
7. Click **OK**.
8. Confirm or change the SQL Connection parameters.
9. As **Repository creation mode** keep “Creates the SQL database ("[dbo]" default schema)".
10. Click **Test connection**. The test must be successful for the process to continue.
11. Click **Test GRANTs**. The test must be successful for the process to continue.
12. Click **OK** to create the new database

Result:

- A repository is created in SQL server. It follows this naming rule:

  ```
  <EnvironmentName>_<RepositoryName>

  Example: MyEnvironment_SQLServerRepository
  ```

- A folder is created in the specified location.

  This folder contains an EMV and an EMQ file.

Using an existing SQL Server database

Prerequisites:

- Identify the SQL connection parameters (RDBMS instance, user, and password).
- **Verify that the property 'Collation' of the database is set to 'SQL_Latin1_General_CP1_CS_AS'**
- Identify the exact name of the user database in the SQL Server. It follows this naming rule:

  ```
  <EnvironmentName>_<RepositoryName>
  ```

  ```
  Example: MyEnvironment_SQLServerRepository
  ```

  Note that the environment name must match the actual environment folder.

Procedure:

1. Start HOPEX **Administration.exe**.
2. Connect to the environment concerned.
3. Right-click the **Repositories** folder and select **New**.
4. Enter the repository **Name**.

   ```
   E.g.: SQLServerRepository
   ```

5. Click **OK**.
6. Confirm or change the SQL Connection parameters.
7. As **Repository Creation Mode** select “Uses an existing SQL database (“[dbo]” default schema)”.
8. Click **Test** to check that the login can be performed and that the database exists.
9. Click **Test connection**. The test must be successful for the process to continue.
10. Click **Test GRANTs**. The test must be successful for the process to continue.
11. Click **OK**.

Result:

- A repository is referenced in the SQL server and initialized.

  ```
  Example: MyEnvironment_SQLServerRepository
  ```

- A folder is created in the specified location.

  ```
  <this folder contains a .EMV and a .EMQ file.
  ```

HOPEX Private Workspaces Cleanup

This procedure is used to delete the data of terminated private workspaces of HOPEX Users. It is necessary to clean up these data often in order to reduce database growth and preserve good performances. We recommend running this procedure every week if you have less than 10 users and every night if you have more than 10 users.

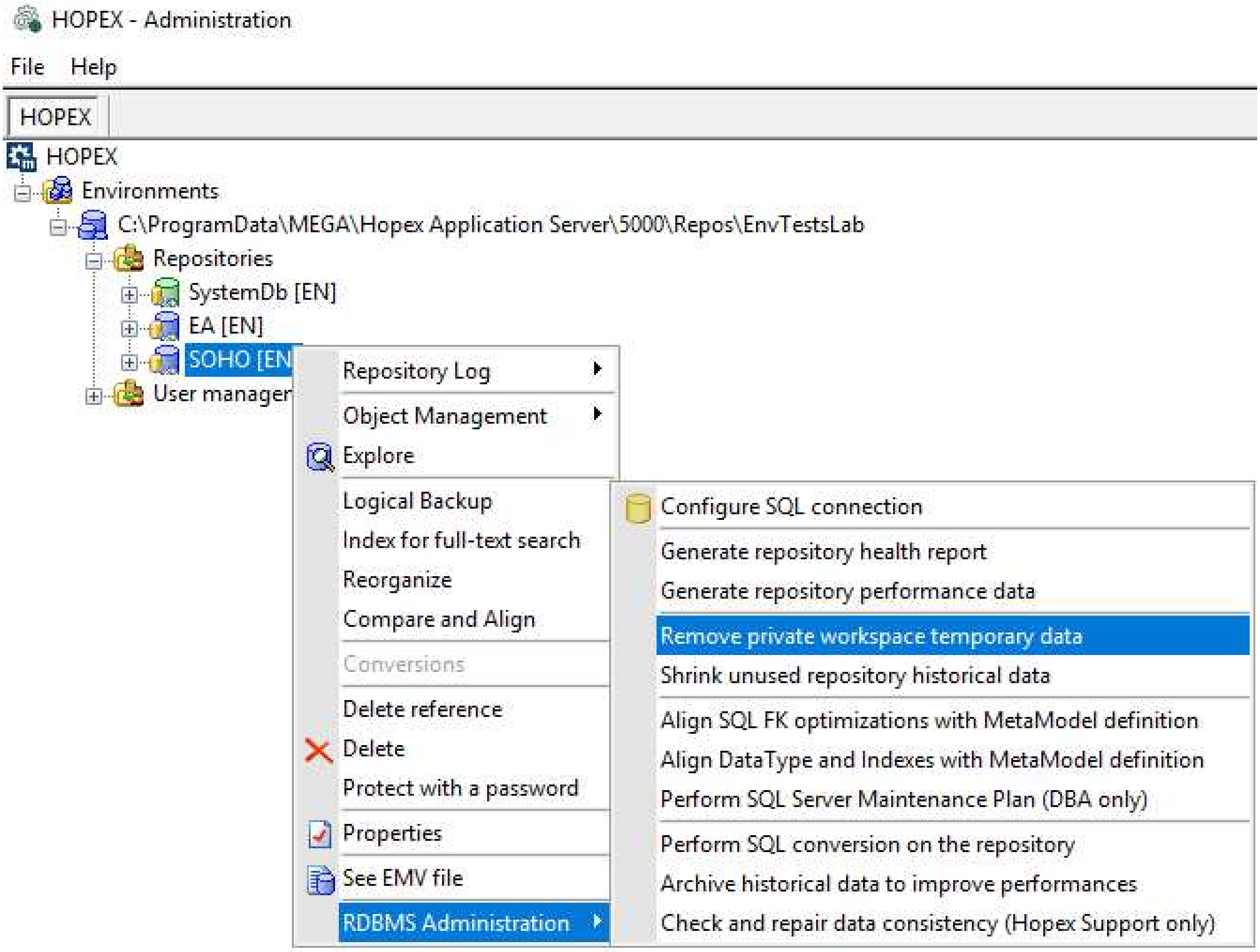
Installing the procedure

Warning: You must repeat this procedure for each HOPEX Repository and the SystemDb.

1. Right-click your HOPEX repository and select **RDBMS Administration > Remove private workspace temporary data**.

   This will launch SP_CLEAN_MEGA_DATABASE and if the procedure:

   - does not exist, the application will create it.
   - already exists, it is overwritten by this action.


HOPEX - Administration
File
Help
HOPEX
HOPEX
Environments
C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\EnvTestsLab
Repositories
SystemDb [EN]
EA [EN]
SOHO [EN
User manager
Repository Log
Object Management
Explore
Logical Backup
Index for full-text search
Reorganize
Compare and Align
Conversions
Delete reference
Delete
Protect with a password
Properties
See EMV file
RDBMS Administration
Configure SQL connection
Generate repository health report
Generate repository performance data
Remove private workspace temporary data
Shrink unused repository historical data
Align SQL FK optimizations with MetaModel definition
Align DataType and Indexes with MetaModel definition
Perform SQL Server Maintenance Plan (DBA only)
Perform SQL conversion on the repository
Archive historical data to improve performances
Check and repair data consistency (Hopex Support only)

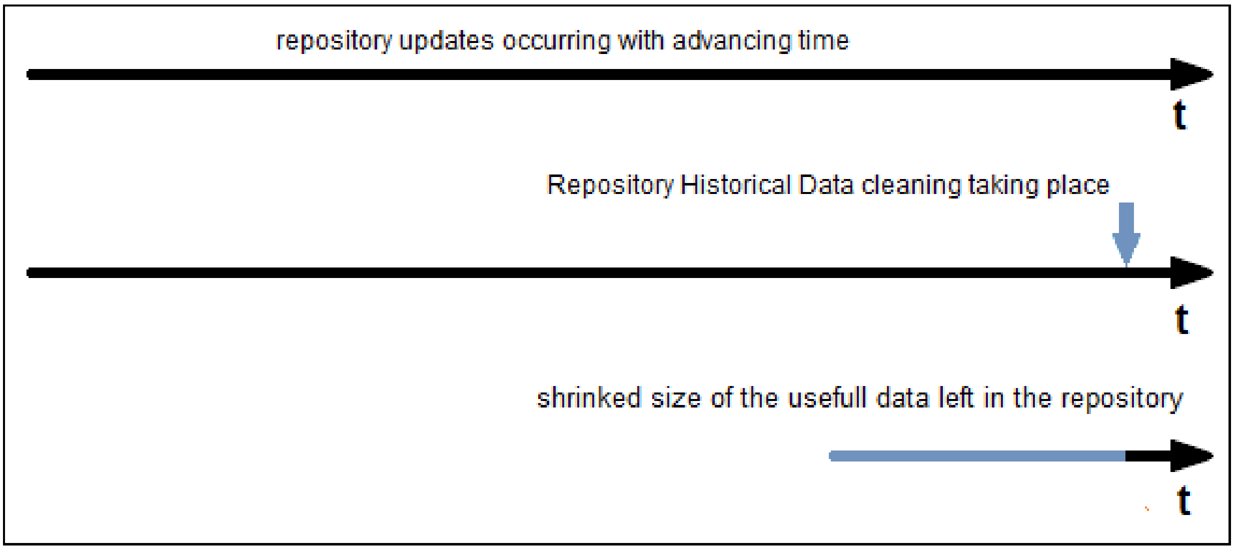
HOPEX Historical Data Cleanup

This procedure is used to delete the historical data of the HOPEX repository. Each time a HOPEX object is updated, the previous data is kept in database. That method insures a high data security even when connection to SGBD is interrupted. It is necessary to clean up these data often in order to reduce database growth and preserve good performances. This clean-up will have no impact on the repository logfile. We recommend running this procedure every week if you have less than 10 users and every night if you have more than 10 users.

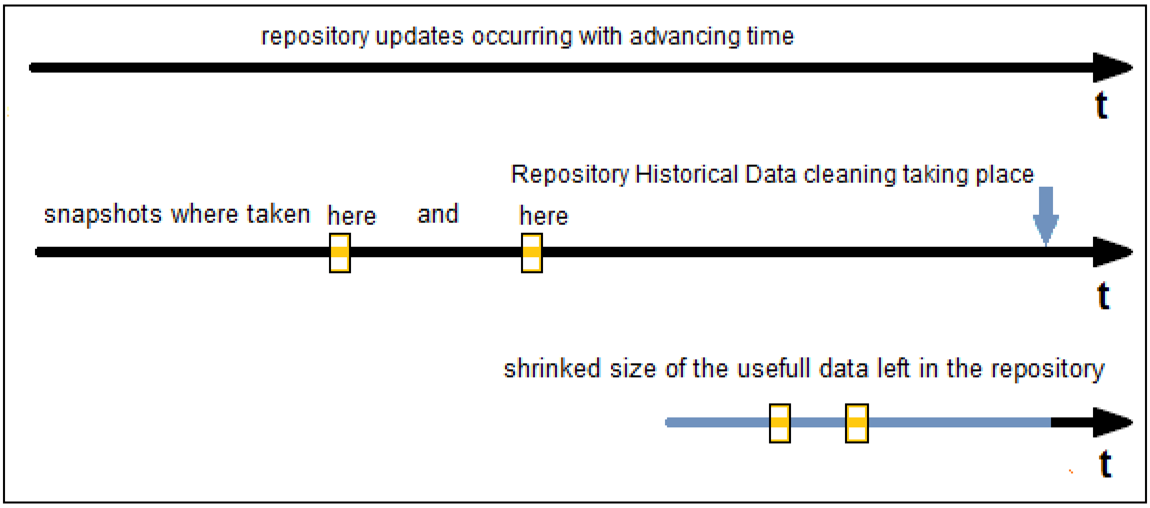
Before cleaning Historical Data

Historical data are used in the Repository Snapshot mechanism. See HOPEX Common Features > Other Features > Using Repository Snapshots: **Repository Snapshot Prerequisites** section for more details.

If you need to have Repository Snapshots taken, be aware that it will not be possible anymore for the period of time covered by the cleanings. In other words, if you need Repository Snapshots, be sure to take them before the procedure runs.


repository updates occurring with advancing time
t
Repository Historical Data cleaning taking place
t
shrinked size of the usefull data left in the repository
t

In this first illustrated case, all archived states were deleted, so all the space that these archived states were using is reclaimed physically (an actual delete in the tables was issued for every one of them).


repository updates occurring with advancing time
t
Repository Historical Data cleaning taking place
snapshots where taken here and here
t
shrinked size of the usefull data left in the repository
t

In this second example, all archived states were also deleted except those corresponding to the state of the repository when the 2 Snapshots were taken.

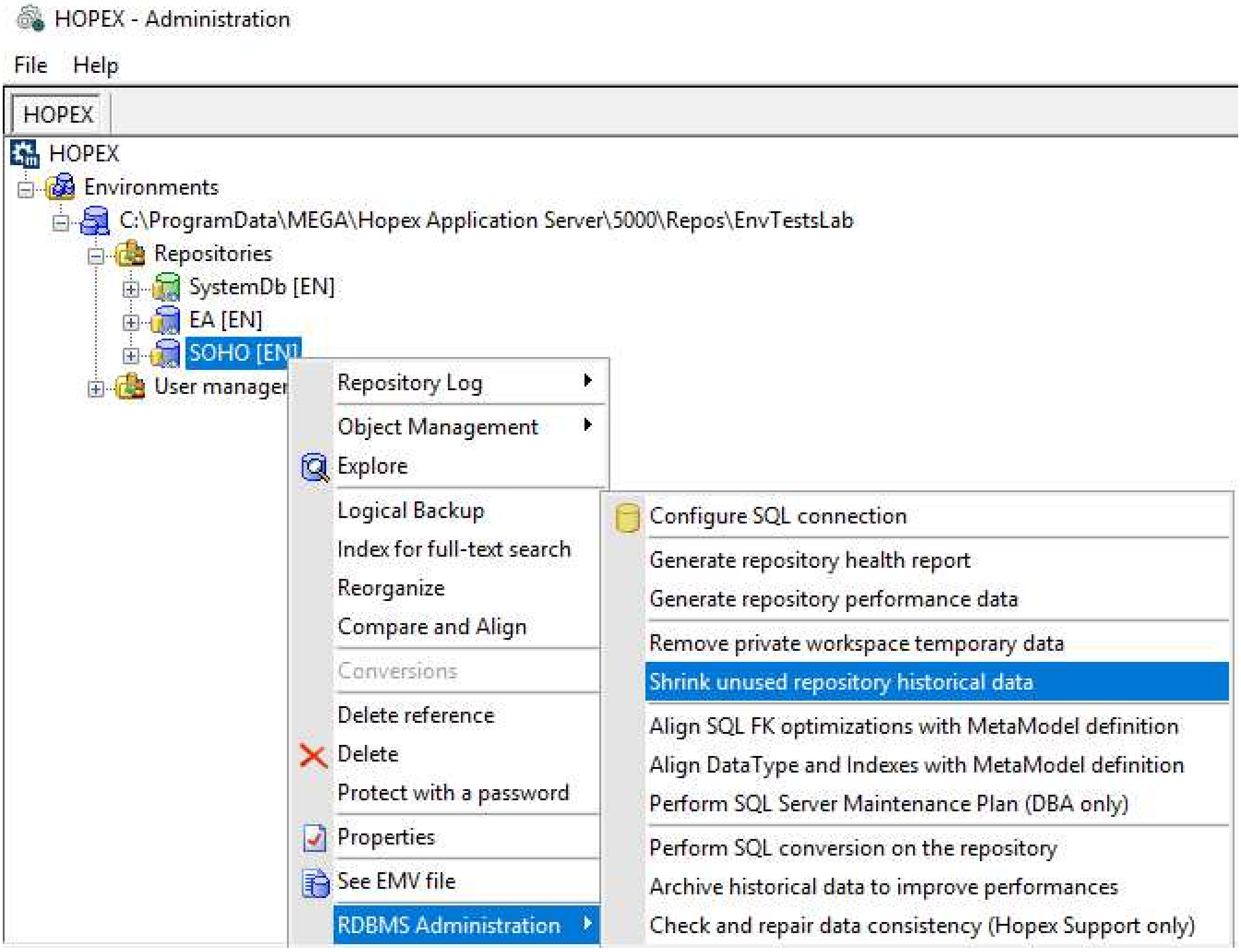
In this case, the data corresponding to the repository state for the Snapshot(s) is saved and it is thanks to this saving that special features will be available within this repository regarding this data.

Installing the procedure

Warning : You must repeat this procedure for each HOPEX Repository and the SystemDb.

1. Right-click your **HOPEX repository** and select **RDBMS Administration > Shrink unused repository historical data**.

   This launches SP_CONSOLIDATE_MEGA_DATABASE and if the procedure does not exist, the application creates it. If the procedure already exists, it is overwritten by this action.


HOPEX - Administration
File
Help
HOPEX
HOPEX
Environments
C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\EnvTestsLab
Repositories
SystemDb [EN]
EA [EN]
SOHO [EN]
User manager
Repository Log
Object Management
Explore
Logical Backup
Index for full-text search
Reorganize
Compare and Align
Conversions
Delete reference
Delete
Protect with a password
Properties
See EMV file
RDBMS Administration
Configure SQL connection
Generate repository health report
Generate repository performance data
Remove private workspace temporary data
Shrink unused repository historical data
Align SQL FK optimizations with MetaModel definition
Align DataType and Indexes with MetaModel definition
Perform SQL Server Maintenance Plan (DBA only)
Perform SQL conversion on the repository
Archive historical data to improve performances
Check and repair data consistency (Hopex Support only)

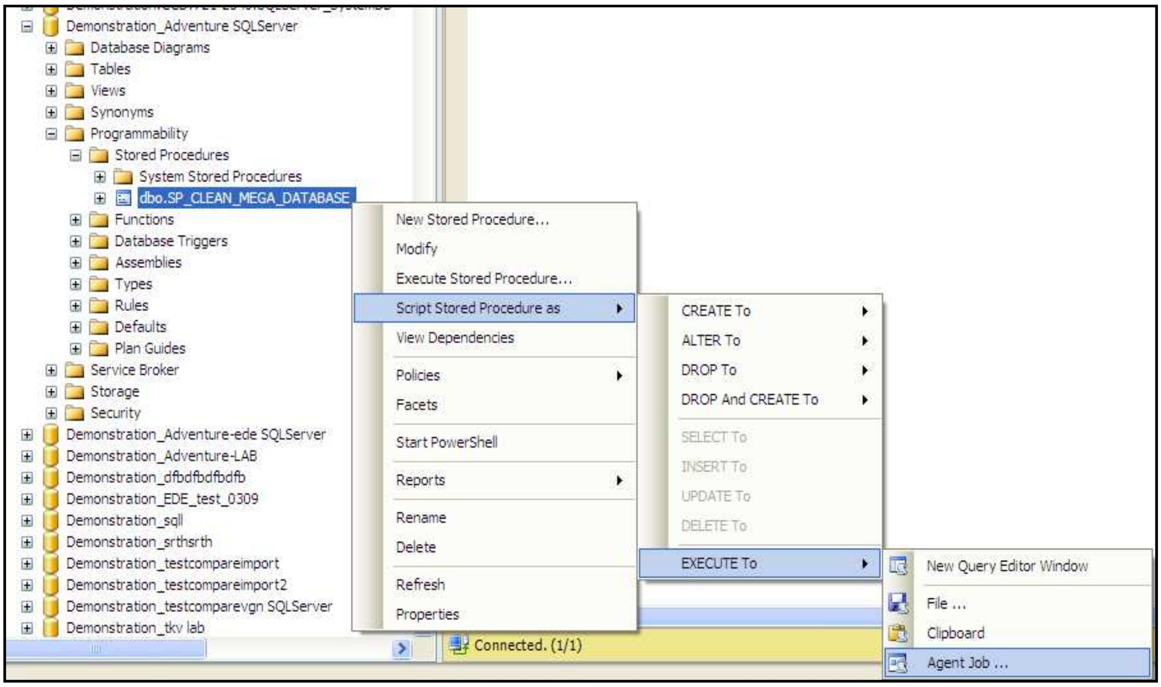
Batching Cleanup procedures for SQL Server

It is very important to run the two procedures on a regular basis. So If you do not want to have to remember to click on the corresponding menus in the Administration.exe program every time that each of the procedure should run, you can batch it using SQL Server agent job.

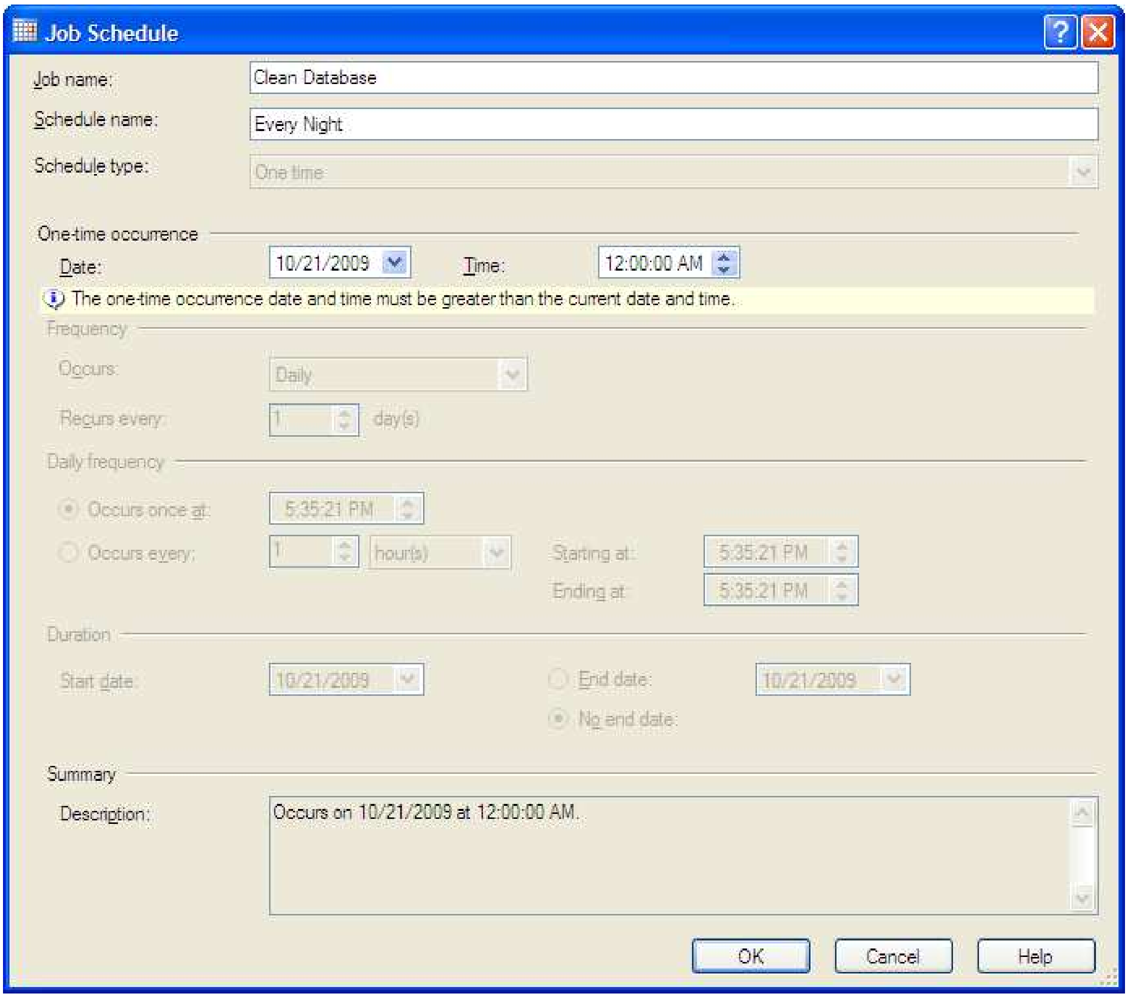
1. Using **SQL Server Management Studio**, find the SQL Server database that corresponds to the HOPEX repository for which you want to batch the stored procedure.

   Reminder : the database will be named following this rule <EnvironmentName_RepositoryName>.

2. In **Programmability > Stored Procedures** folder, right-click this procedure and select **Script Stored Procedure as > Execute to > Agent job**.



Enter a name for the job and the schedule.



Job Schedule

Job name: Clean Database

Schedule name: Every Night

Schedule type: One time

One-time occurence

Date: 10/21/2009 Time: 12:00:00 AM

The one-time occurrence date and time must be greater than the current date and time.

Frequency

Occurs: Daily

Recurs every: 1 day(s)

Daily frequency

● Occurs once at: 5:35:21 PM

○ Occurs every: 1 hour(s) Starting at: 5:35:21 PM

Ending at: 5:35:21 PM

Duration

Start date: 10/21/2009 ○ End date: 10/21/2009

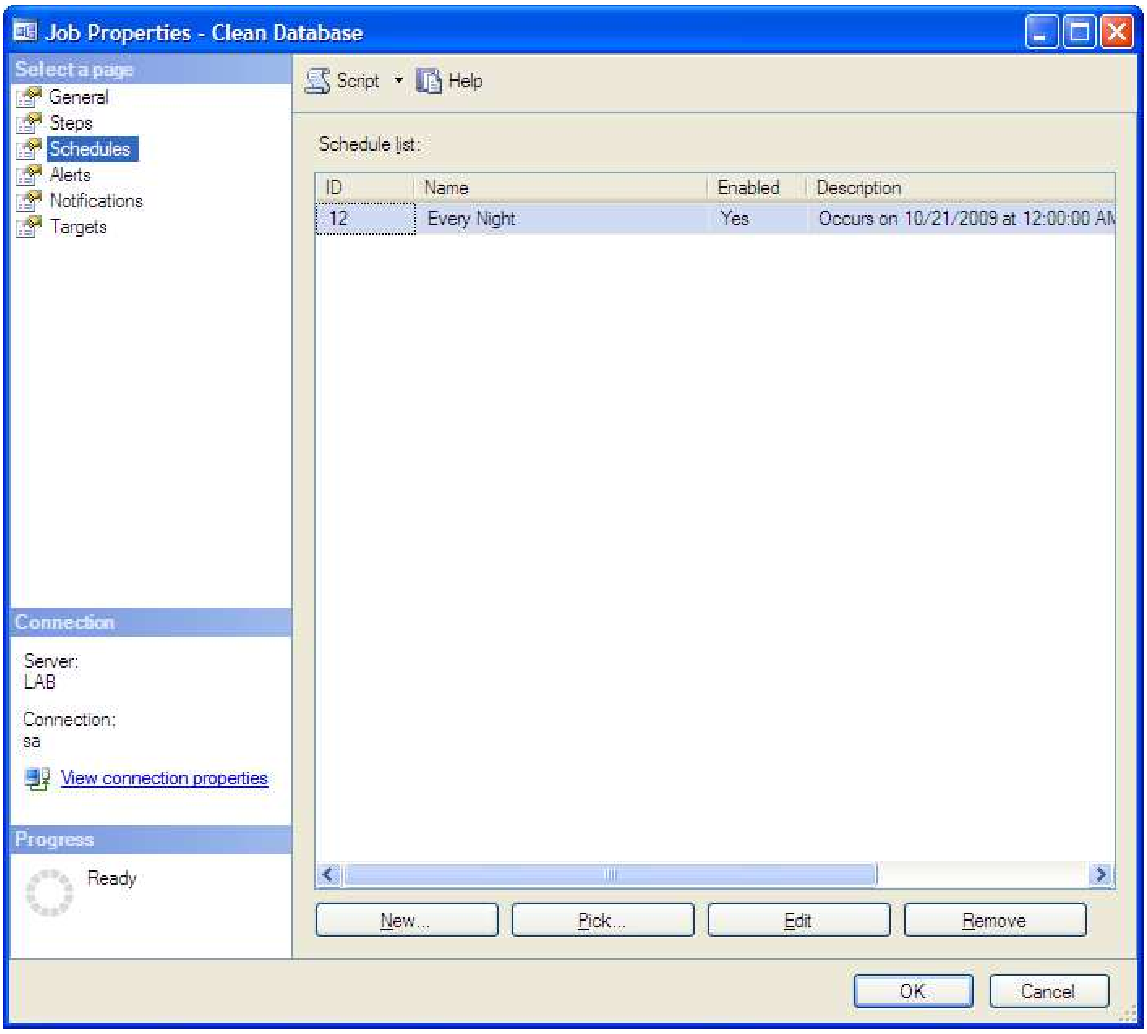
● No end date:

Summary

Description: Occurs on 10/21/2009 at 12:00:00 AM.

The job is created.

3. Right-click this job and select **Properties**.
4. Select the **Schedules** tab and click **Edit**.



Server:
LAB

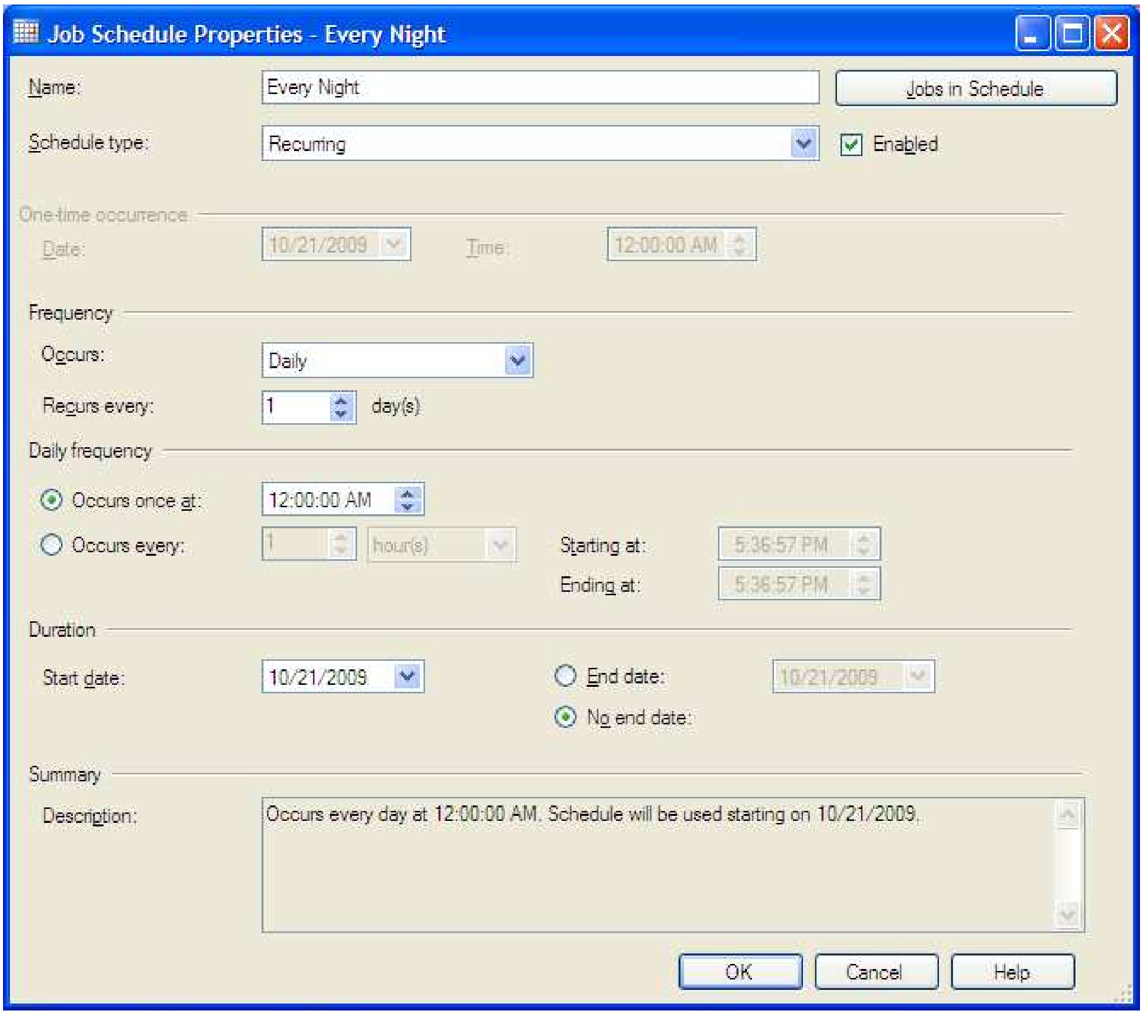
Connection:
sa

Ready

Schedule list:

ID	Name	Enabled	Description
12	Every Night	Yes	Occurs on 10/21/2009 at 12:00:00 AM

5. Set up the schedule to execute the job every night.



Job Schedule Properties - Every Night

Name: Every Night

Schedule type: Recurring ☑ Enabled

One-time occurrence

Date: 10/21/2009 Time: 12:00:00 AM

Frequency

Occurs: Daily

Recurs every: 1 day(s)

Daily frequency

● Occurs once at: 12:00:00 AM

○ Occurs every: 1 hour(s) Starting at: 5:36:57 PM Ending at: 5:36:57 PM

Duration

Start date: 10/21/2009 ○ End date: 10/21/2009

● No end date:

Summary

Description: Occurs every day at 12:00:00 AM. Schedule will be used starting on 10/21/2009.

Maintenance tasks

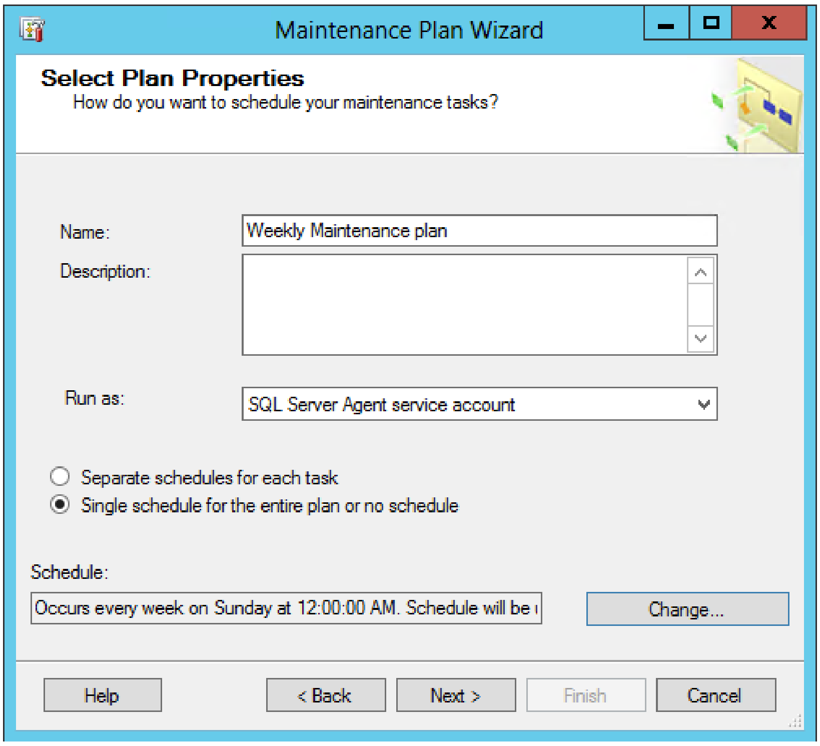
The SQL Server databases need to be maintained, in order to keep the best possible performances. Tasks such as “update of the statistics”, “reorganize or rebuild of the indexes”, “shrink of the databases”, as well as backups, need to be run regularly.

We recommend set up the standard maintenance plans of SQL Server to manage those tasks. The backups can be excluded, if they are done through another chanel.

Also, we can imagine to put the execution of the HOPEX cleanup procedures (see previous chapter) as the preliminary step to the SQL Server job that will run the maintenance tasks.

You can find below some screenshots of a default maintenance plan (with backups), with SQL Server 2012. It can be adapted to your version, and your rules :

1. Create a maintenance plan using the SQL Server wizard (in SQL Server Management Studio).
2. Give it a name and a schedule (click **Change**).



Maintenance Plan Wizard

Select Plan Properties

How do you want to schedule your maintenance tasks?

Name: Weekly Maintenance plan

Description:

Run as: SQL Server Agent service account

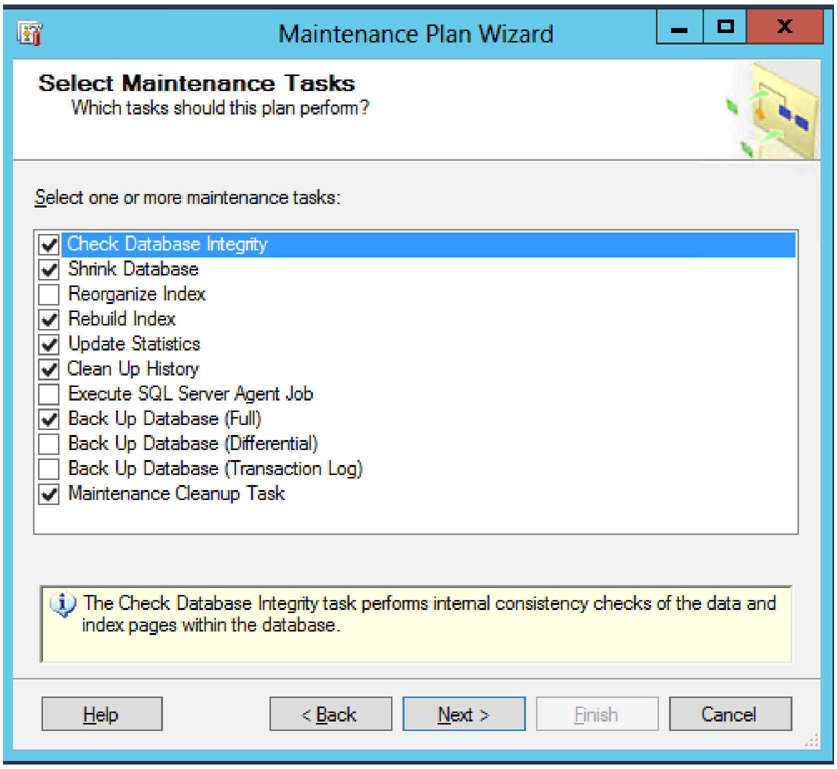
○ Separate schedules for each task

● Single schedule for the entire plan or no schedule

Schedule:

Occurs every week on Sunday at 12:00:00 AM. Schedule will be u

3. Select the following maintenance tasks:



Maintenance Plan Wizard

Select Maintenance Tasks

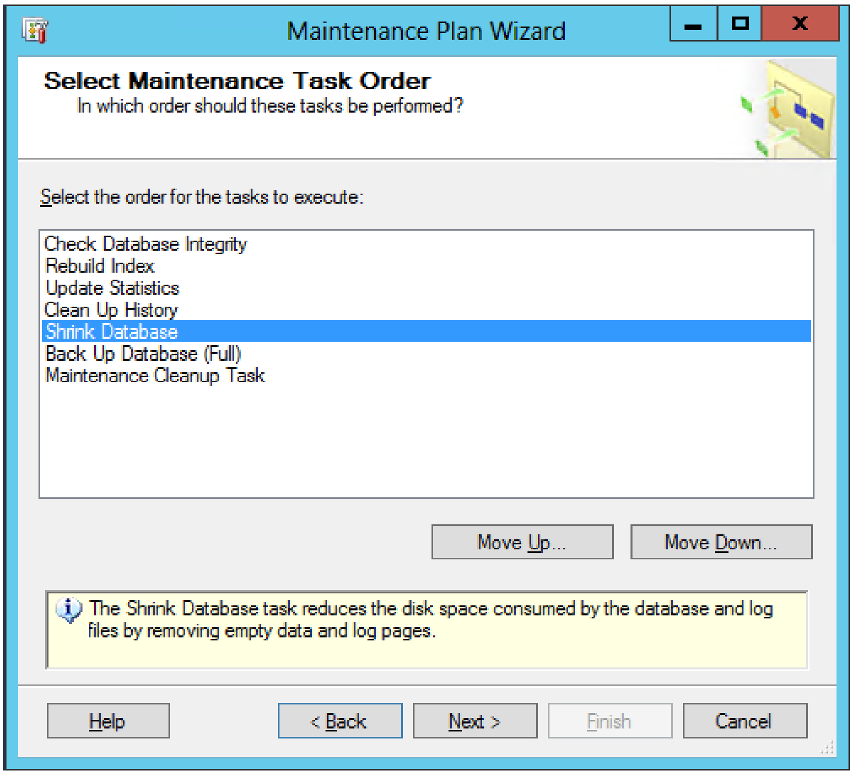
Which tasks should this plan perform?

Select one or more maintenance tasks:

- ☑ Check Database Integrity
- ☑ Shrink Database
- □ Reorganize Index
- ☑ Rebuild Index
- ☑ Update Statistics
- ☑ Clean Up History
- □ Execute SQL Server Agent Job
- ☑ Back Up Database (Full)
- □ Back Up Database (Differential)
- □ Back Up Database (Transaction Log)
- ☑ Maintenance Cleanup Task

The Check Database Integrity task performs internal consistency checks of the data and index pages within the database.

4. Order the maintenance tasks as follows:



Maintenance Plan Wizard

Select Maintenance Task Order

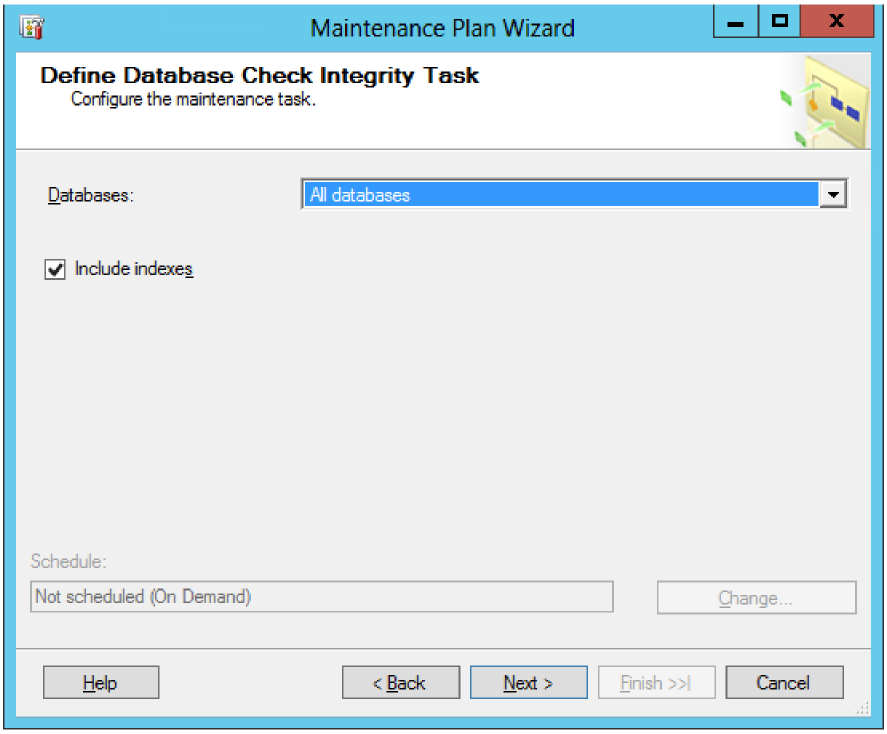
In which order should these tasks be performed?

Select the order for the tasks to execute:

Check Database Integrity
Rebuild Index
Update Statistics
Clean Up History
Shrink Database
Back Up Database (Full)
Maintenance Cleanup Task

The Shrink Database task reduces the disk space consumed by the database and log files by removing empty data and log pages.

5. Check all databases (including the system databases):



Maintenance Plan Wizard

Define Database Check Integrity Task

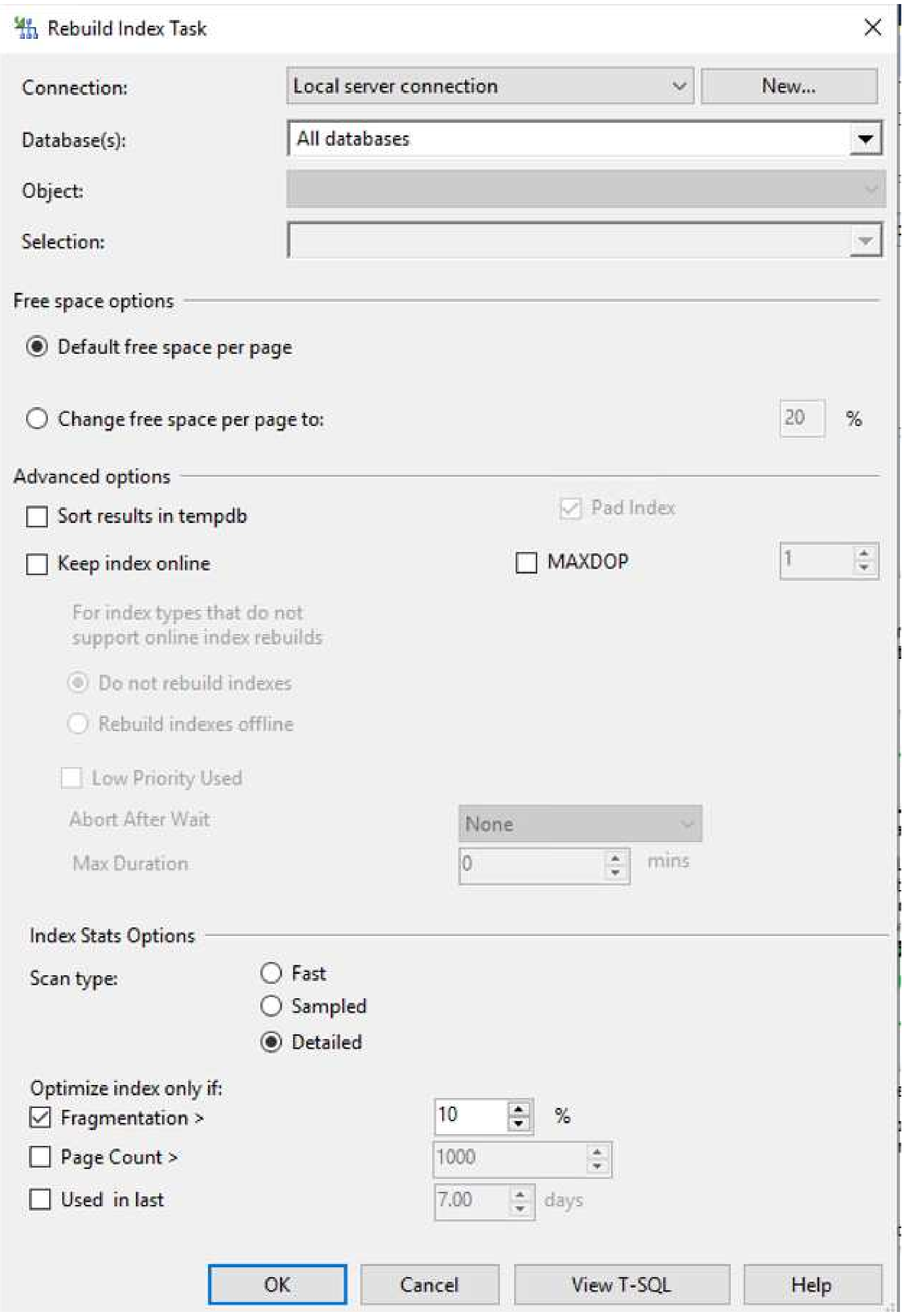
Configure the maintenance task.

Databases: All databases

☑ Include indexes

Schedule: Not scheduled (On Demand)

6. Rebuild indexes for the user databases:



Rebuild Index Task

Connection: Local server connection

Database(s): All databases

Object:

Selection:

Free space options

● Default free space per page

○ Change free space per page to: 20 %

Advanced options

□ Sort results in tempdb

☑ Pad Index

□ Keep index online

□ MAXDOP 1

For index types that do not support online index rebuilds

● Do not rebuild indexes

○ Rebuild indexes offline

□ Low Priority Used

Abort After Wait: None

Max Duration: 0 mins

Index Stats Options

Scan type:

○ Fast

○ Sampled

● Detailed

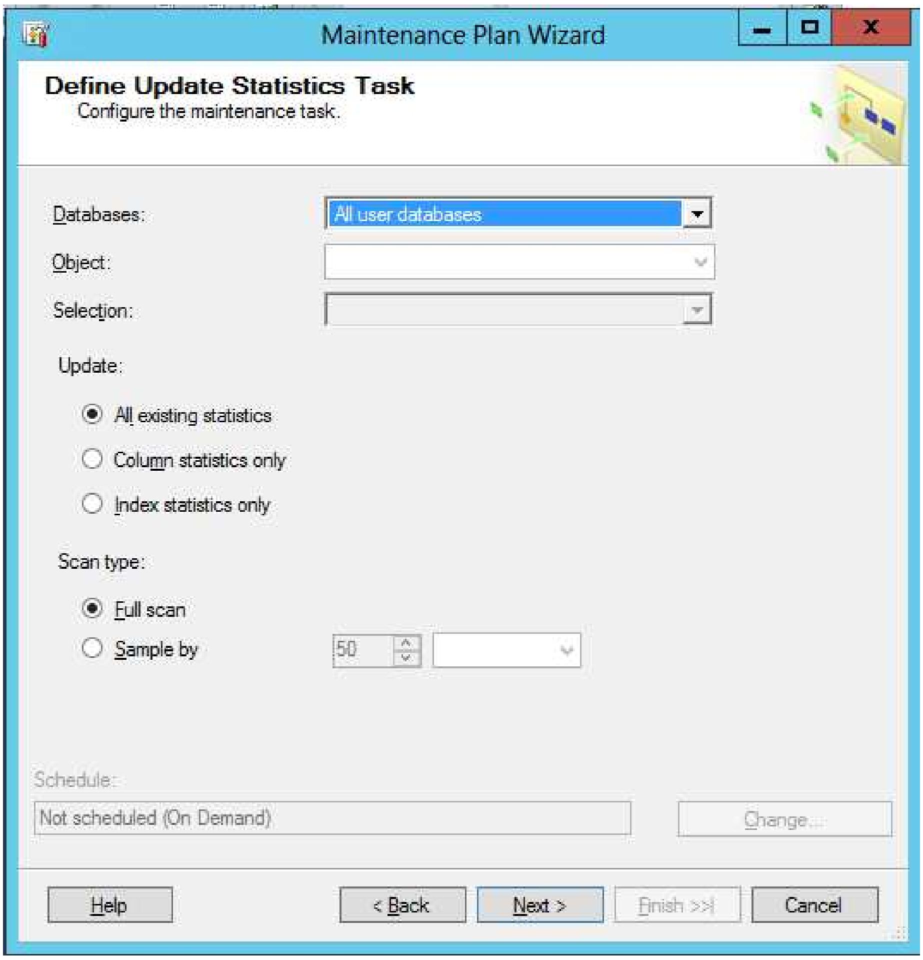
Optimize index only if:

☑ Fragmentation > 10 %

□ Page Count > 1000

□ Used in last 7.00 days

7. Same thing for the update of the statistics:



Maintenance Plan Wizard

Define Update Statistics Task

Configure the maintenance task.

Databases: All user databases

Object:

Selection:

Update:

● All existing statistics

○ Column statistics only

○ Index statistics only

Scan type:

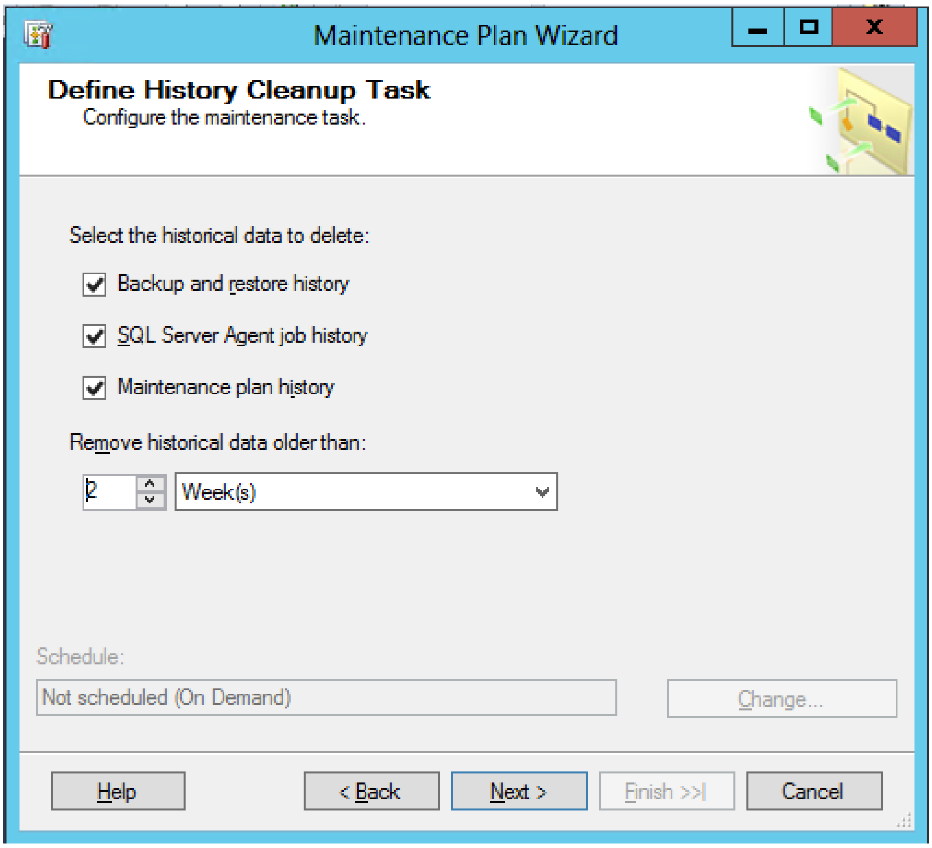
● Full scan

○ Sample by 50

Schedule:

Not scheduled (On Demand)

8. Define how long the log files will be kept:



Define History Cleanup Task

Configure the maintenance task.

Select the historical data to delete:

☑ Backup and restore history

☑ SQL Server Agent job history

☑ Maintenance plan history

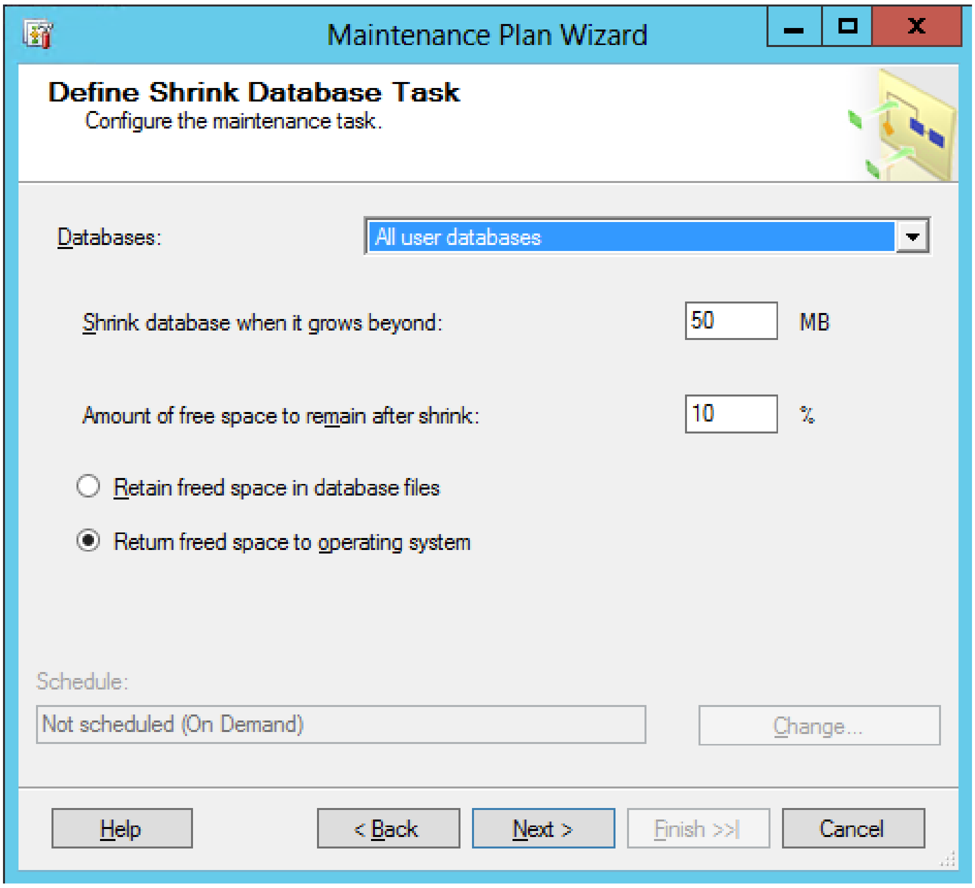
Remove historical data older than:

2 Week(s)

Schedule:

Not scheduled (On Demand)

9. Shrink all user databases, or at least the HOPEX databases:



Define Shrink Database Task

Configure the maintenance task.

Databases: All user databases

Shrink database when it grows beyond: 50 MB

Amount of free space to remain after shrink: 10 %

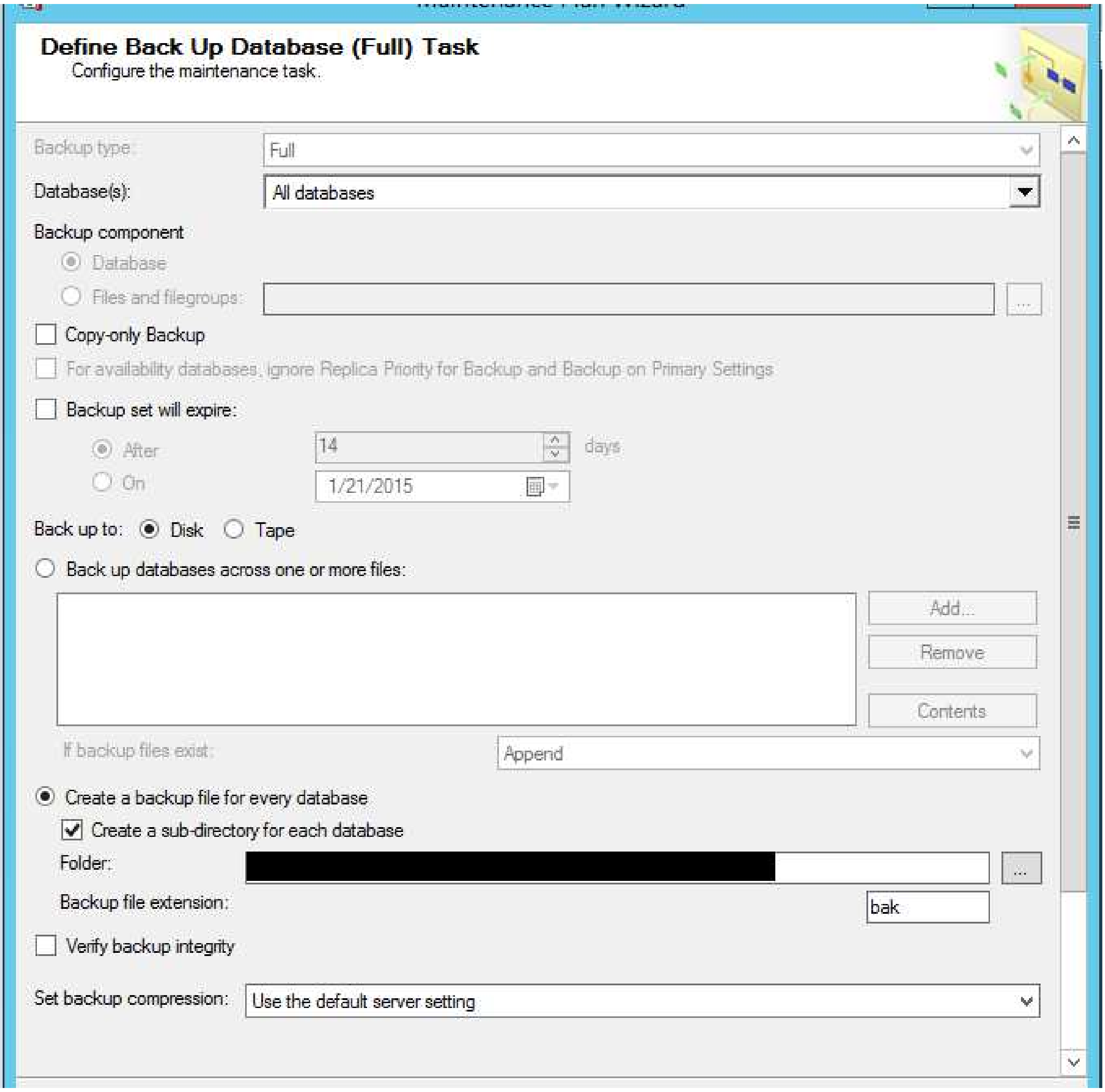
○ Retain freed space in database files

● Return freed space to operating system

Schedule:

Not scheduled (On Demand)

10. Backup all databases, choose the destination folder, and if you want to have subfolders for each database:



Define Back Up Database (Full) Task

Configure the maintenance task.

Backup type: Full

Database(s): All databases

Backup component

○ Database

○ Files and filegroups:

□ Copy-only Backup

□ For availability databases, ignore Replica Priority for Backup and Backup on Primary Settings

□ Backup set will expire:

● After 14 days

○ On 1/21/2015

Back up to: ● Disk ○ Tape

○ Back up databases across one or more files:

Add... Remove Contents

If backup files exist: Append

● Create a backup file for every database

☑ Create a sub-directory for each database

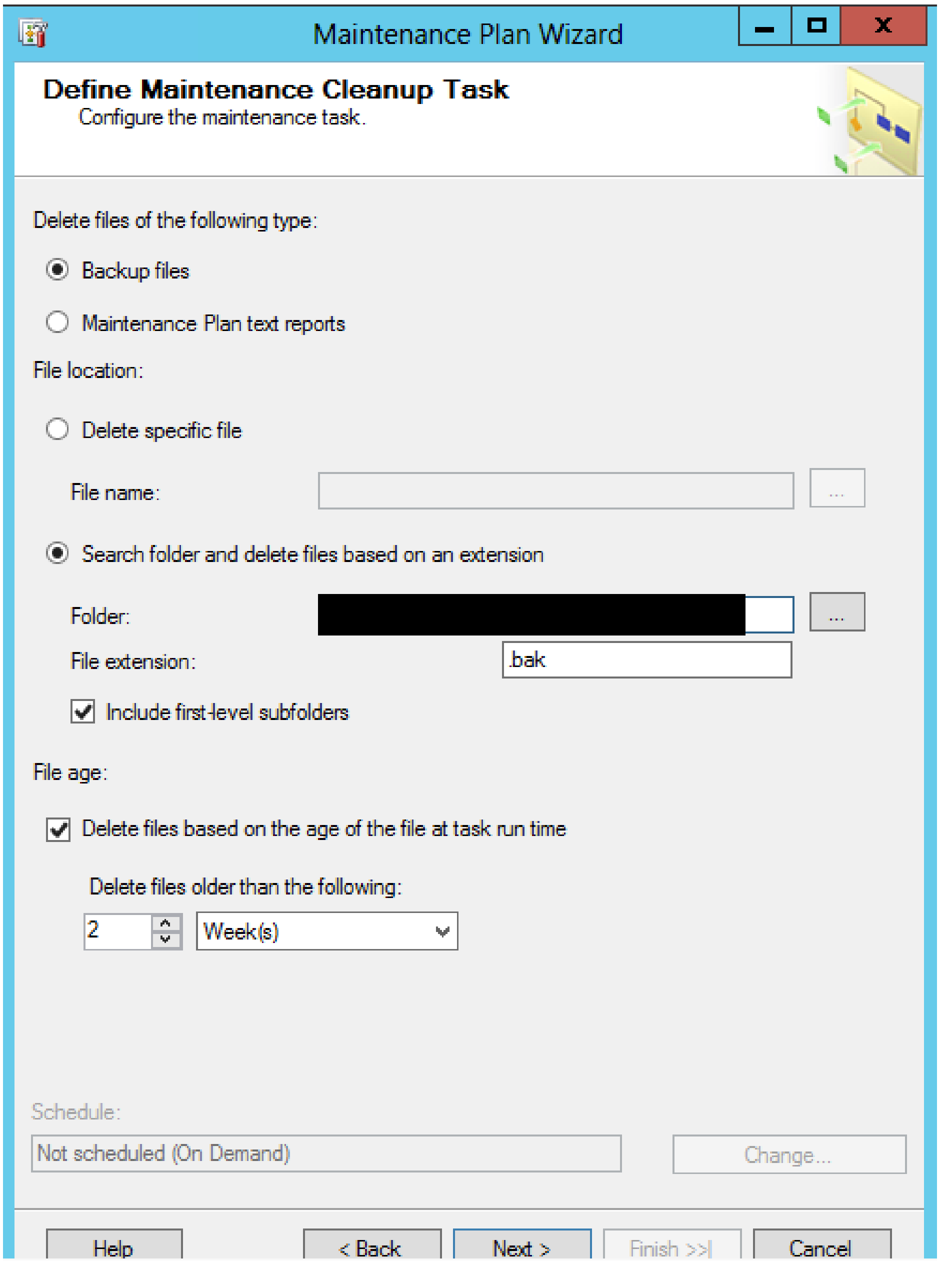
Folder: [redacted]

Backup file extension: bak

□ Verify backup integrity

Set backup compression: Use the default server setting

11. Provide the folder where the backups are being stored, the extension, and if you want to include subfolders, as well as how long you want to keep the files before deleting them:



Define Maintenance Cleanup Task

Configure the maintenance task.

Delete files of the following type:

● Backup files

○ Maintenance Plan text reports

File location:

○ Delete specific file

File name:

● Search folder and delete files based on an extension

Folder: [redacted]

File extension: .bak

☑ Include first-level subfolders

File age:

☑ Delete files based on the age of the file at task run time

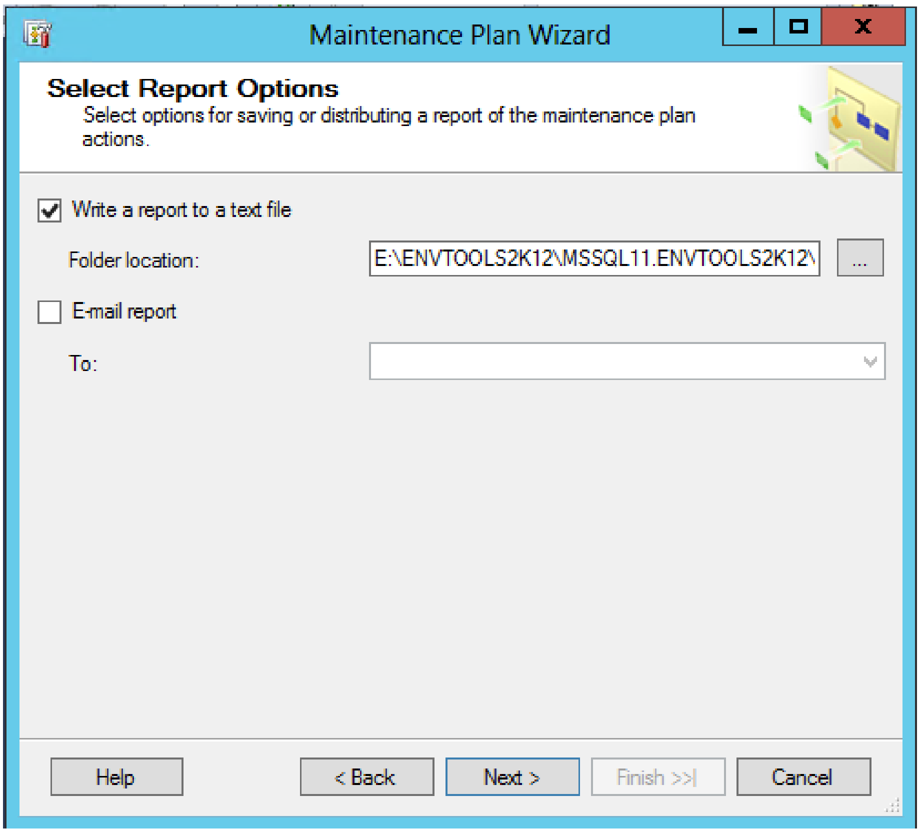
Delete files older than the following:

2 Week(s)

Schedule:

Not scheduled (On Demand)

12. Keep the default :



Maintenance Plan Wizard

Select Report Options

Select options for saving or distributing a report of the maintenance plan actions.

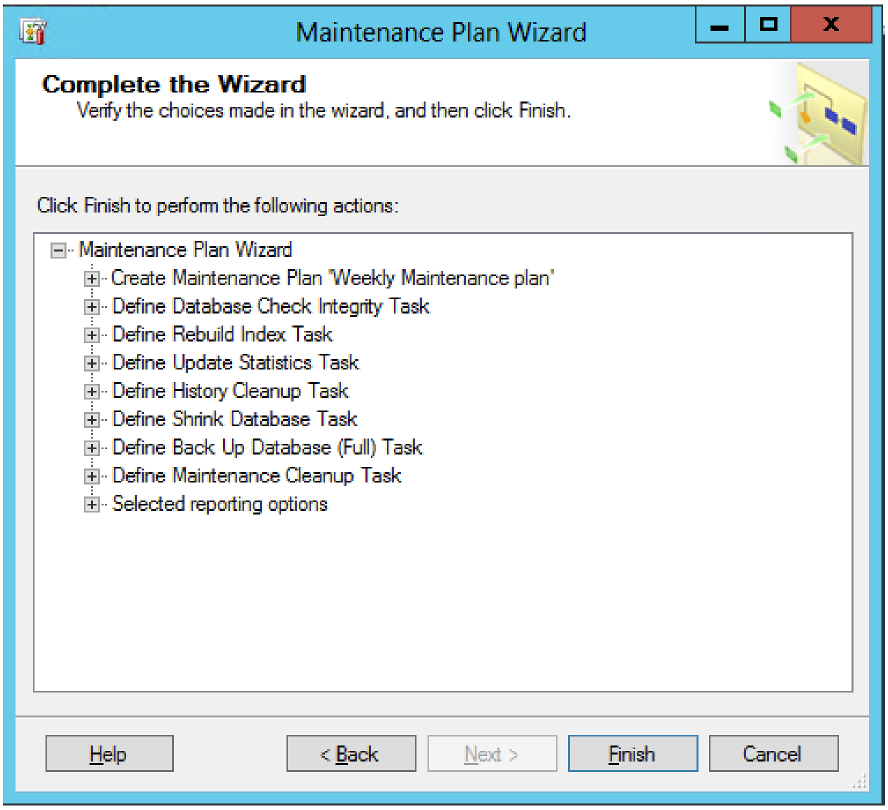
☑ Write a report to a text file

Folder location: E:\ENVTOOLS2K12\MSSQL11.ENVTOOLS2K12\

□ E-mail report

To:

13. Click **Finish** to create the maintenance plan, and the SQL Server job:



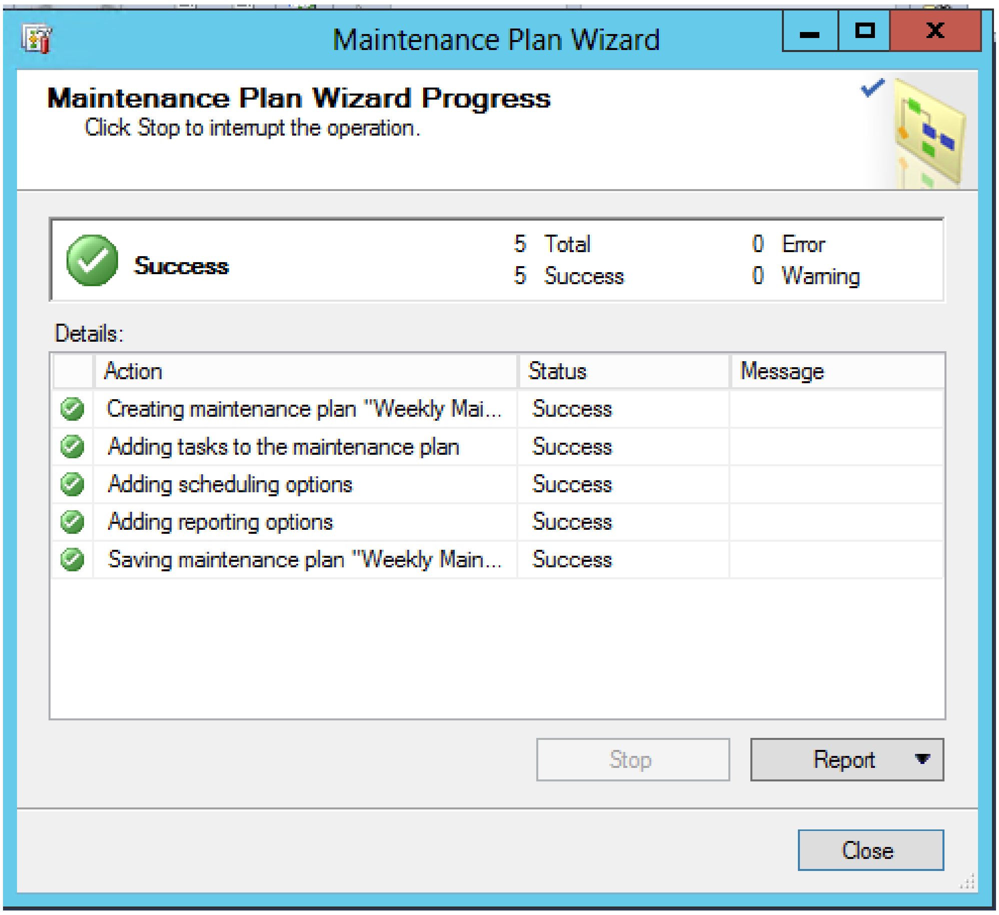
Maintenance Plan Wizard

Complete the Wizard

Verify the choices made in the wizard, and then click Finish.

Click Finish to perform the following actions:

- Maintenance Plan Wizard
  - Create Maintenance Plan 'Weekly Maintenance plan'
  - Define Database Check Integrity Task
  - Define Rebuild Index Task
  - Define Update Statistics Task
  - Define History Cleanup Task
  - Define Shrink Database Task
  - Define Back Up Database (Full) Task
  - Define Maintenance Cleanup Task
  - Selected reporting options



Maintenance Plan Wizard Progress

Click Stop to interrupt the operation.

Success

5	Total	0	Error
5	Success	0	Warning

Details:

	Action	Status	Message
✓	Creating maintenance plan "Weekly Mai...	Success	
✓	Adding tasks to the maintenance plan	Success	
✓	Adding scheduling options	Success	
✓	Adding reporting options	Success	
✓	Saving maintenance plan "Weekly Main...	Success	

HOPEX RDBMS repositories specific administration actions

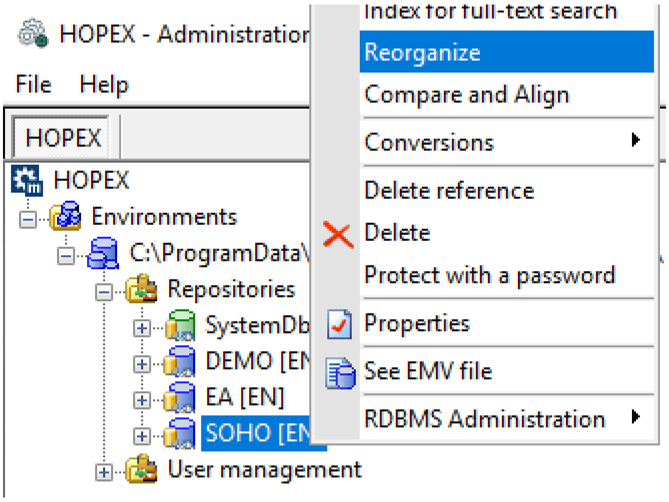
Migrating Your Data from One Storage Support to Another

Previous versions of Hopex were compatible with GBMS (proprietary Mega data format), and Oracle. This section shows how to convert data from one of those to SQL Server.

General procedure:

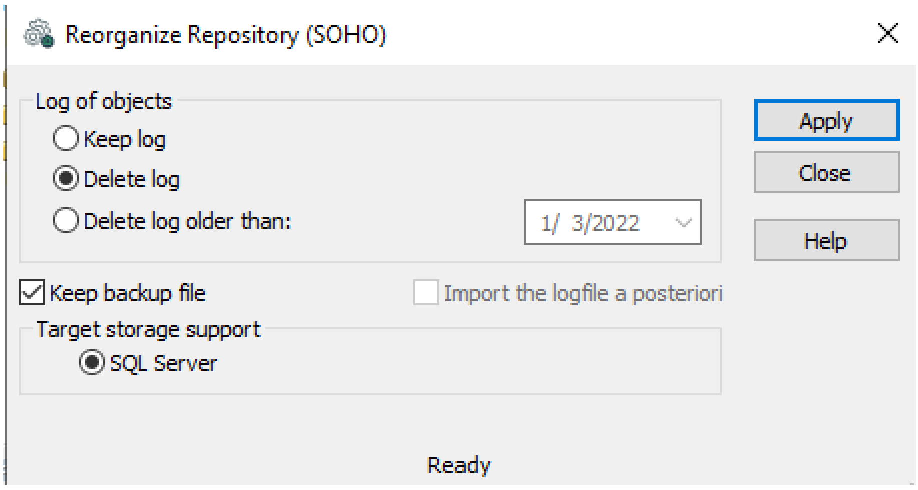
1. Start HOPEX **Administration.exe**.
2. Connect to the environment containing the repositories to be migrated.
3. Expand the **Repositories** folder.
4. Right-click a repository and select **Reorganize**.

NB: Launch a complete environment migration starting with the data repositories and finishing with the SystemDb repository.



To reorganize a repository:

1. Select the expected **Target storage support**.



Reorganize Repository (SOHO)

Log of objects

○ Keep log

● Delete log

○ Delete log older than: 1/ 3/2022

☑ Keep backup file

□ Import the logfile a posteriori

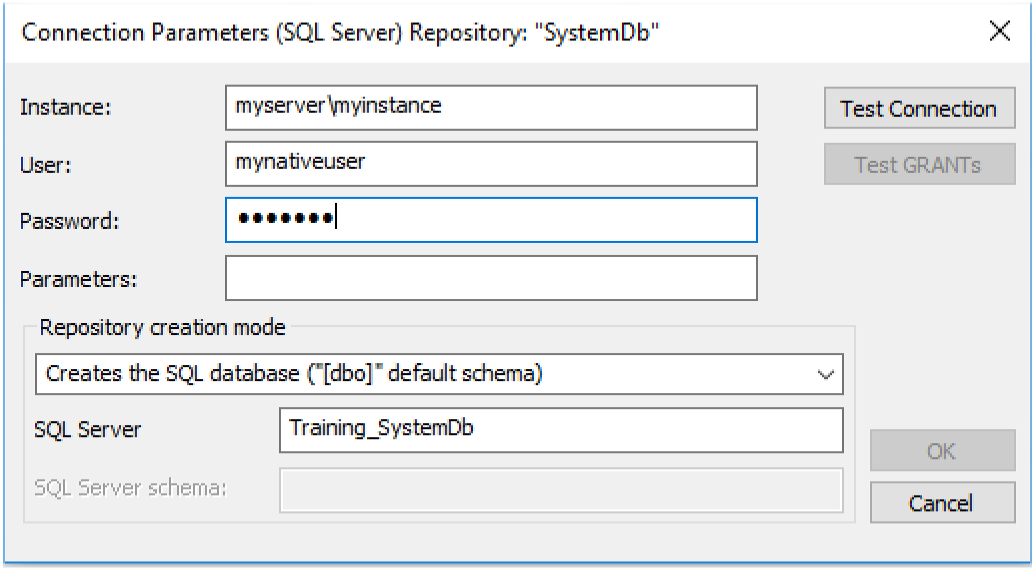
Target storage support

● SQL Server

Ready

2. Click **Apply** to start the reorganization.

   You are prompted to confirm or change the SQL Connection parameters.



Connection Parameters (SQL Server) Repository: "SystemDb"

Instance: myserver\myinstance

User: mynativeuser

Password: ●●●●●●●

Parameters:

Repository creation mode

Creates the SQL database ("[dbo]" default schema)

SQL Server: Training_SystemDb

SQL Server schema:

The **Test connection** step must be successful for the process to continue.

The **Test GRANTs** step must be successful for the process to continue.

Note: To be successful, there should be no storage on the Sql Server concerning a HOPEX repository with the same name in a same HOPEX environment.

If your Sql Server User does not have the right to create databases, you need to ask your DBA to create an Sql Server database following the naming rule: <EnvironmentName>_<RepositoryName>. You should then choose the option “Use existing Sql Server Database”.

Results:

- The database is now migrated to the SQL Server storage.
- The .emq (SQL Server) file corresponding to the newly created repository storage is created.
- The Megaenv.ini file is updated.

- The logical backup file, used during the process, is stored in the 'work' folder of the source repository.
- This backup is named according to the following format: Bkp_Date_BaseName.mgr .

Restoring a HOPEX environment from formatted data

In some cases, in HOPEX Administration, you need to recreate a repository from an existing set of data (a previously HOPEX formatted repository). For example, after a physical corruption (disk crash) of the machine hosting the HOPEX repository folder tree.

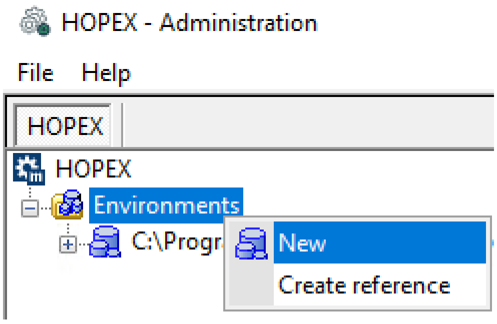
In such a situation, since the repository folder contains files indicating the way to reach the data and on which database server it can be found, the data could be considered lost from a HOPEX point of view.

It is necessary to understand that, from then on, HOPEX needs a new way to access the data inside the RDBMS. This is why this action is seen as a **Restoration** of the data: a re-creation of the repository folder structure allowing to re-save the way to access the data.

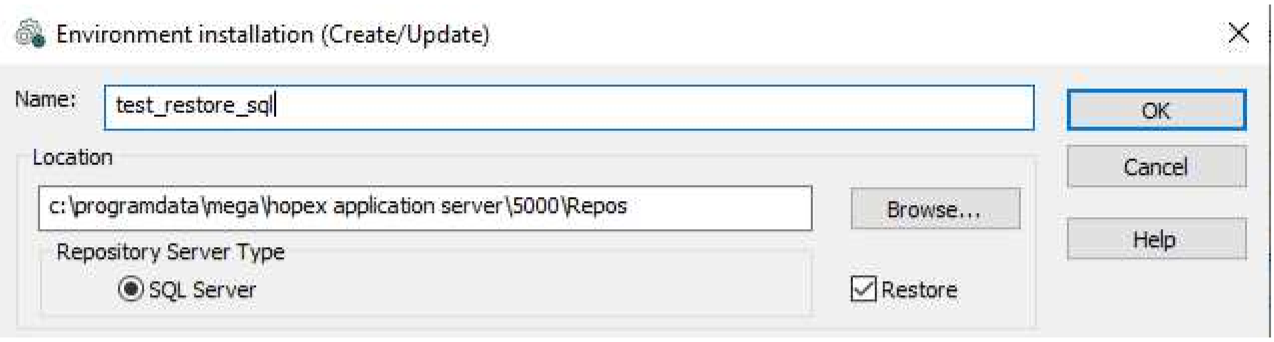
This method can also be used for duplicating an environment from a production infrastructure to a test infrastructure (or vice versa). For doing so, all the repositories (including the SystemDb) must be duplicated first in the RDBMS. The restoration can then be done on the duplicates repositories, starting with the SystemDb.

Restoring an environment (SystemDb repository)

1. Start HOPEX **Administration.exe**.
2. Right-click the **Environments** folder and select **New**.



3. In **Name**, enter the name of the environment that is to be restored (the exact same name as the one used for the first creation).
4. Select **Restore**.


Environment installation (Create/Update)

Name: test_restore_sql

Location

c:\programdata\mega\hopex application server\5000\Repos

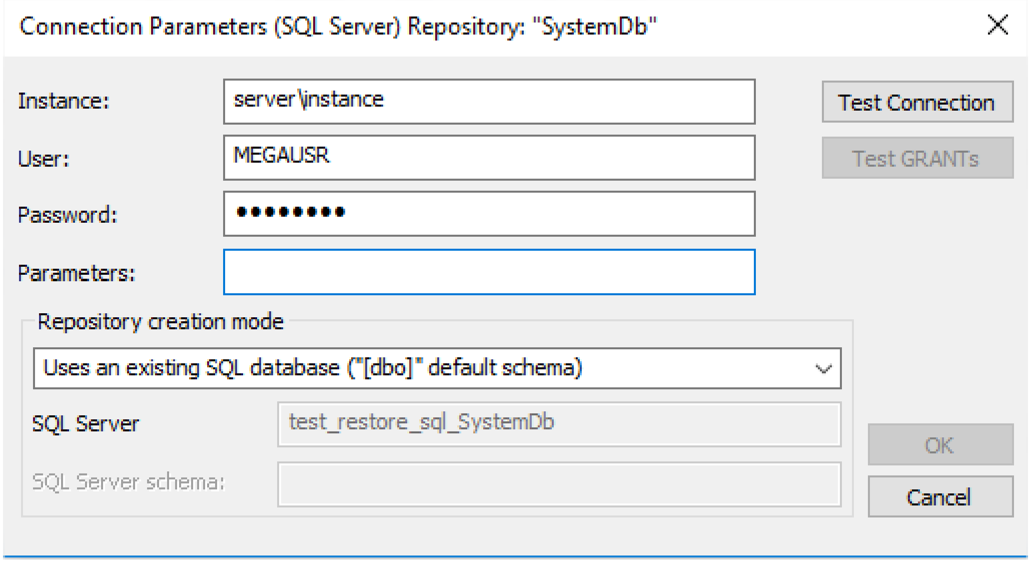
Repository Server Type

● SQL Server

☑ Restore

5. Click **OK**.

6. Specify the connection parameters for accessing the RDBMS where the HOPEX -yet-unreachable data is located.



Connection Parameters (SQL Server) Repository: "SystemDb"

Instance: server\instance

User: MEGAUSR

Password: •••••••••

Parameters:

Repository creation mode

Uses an existing SQL database ("[dbo]" default schema)

SQL Server: test_restore_sql_SystemDb

SQL Server schema:

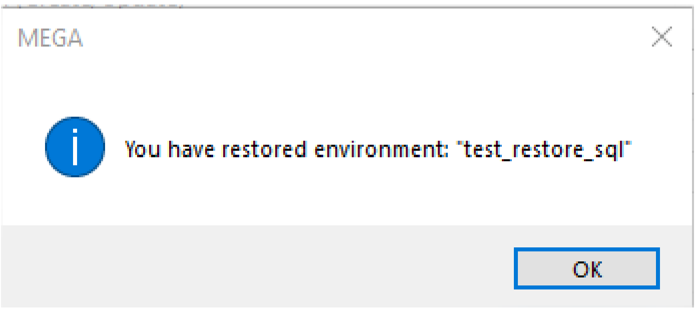
7. Click **Test Connection.**

   The test must be successful for the process to continue.

8. Click **Test GRANTs.**

   The test must be successful for the process to continue.

9. Click **OK**.
   The SystemDb repository is restored.



MEGA

You have restored environment: "test_restore_sql"

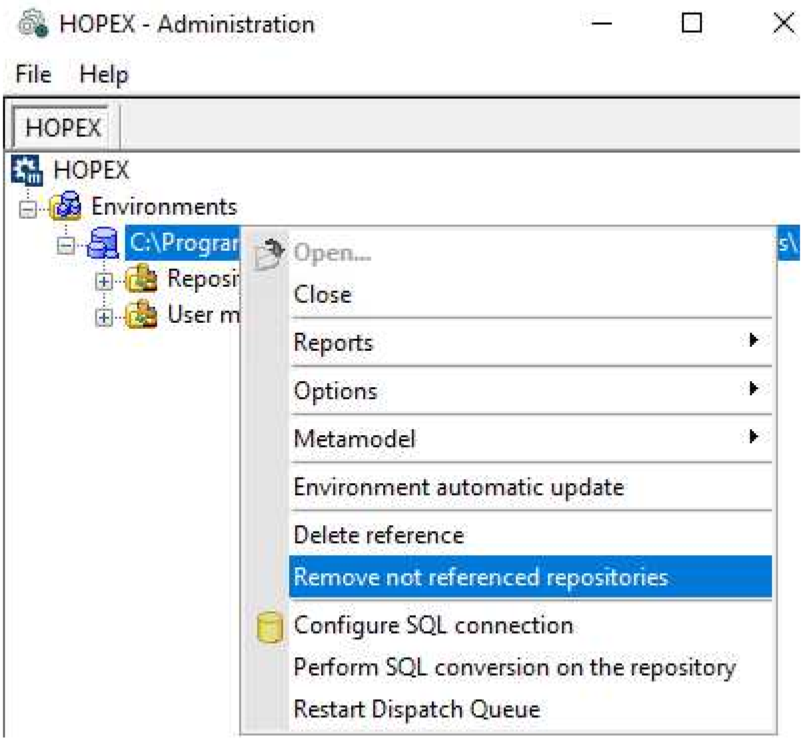
Once these actions are performed successfully, there are a few more actions to perform to be able to restore the repositories that were referenced into the newly restored environment.

At this point, if you open the environment that was just restored, you will see the following warning message: "**The <repository name> is not referenced**").

The reason is that the environment that was just restored has "a knowledge" of the repositories that should be referenced in it but the references for those repositories do not yet exist in the folder tree structure of the newly restored environment.

To be able to re-reference the required repositories by restoration in this environment, you must first purge that "knowledge":

1. Right-click the Environment and select **Remove not referenced repositories**:



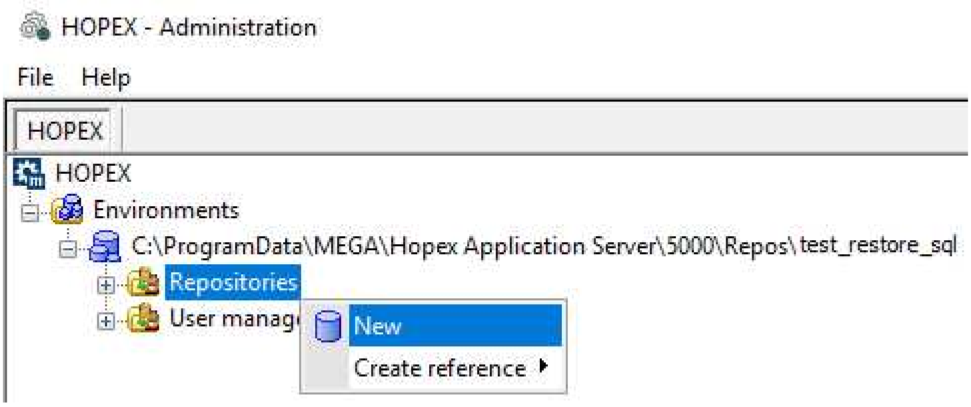
Important notes	- DO NOT use **Remove not referenced repositories** if the environment is in use somewhere else as it will delete the references to the repositories there too! - Use it only on an environment that is a physical copy on the RDBMS storage side. - Be carefull that the repositories also must be restored from a physical RDBMS copy (see next chapter for repositories restoration). - Not taking care of this would lead to situations where users might think that they are using different sets of data when they are actually using and modifying **the same repositories.**

Restoring a data repository

Note: A repository can only be restored within an environment that has the same name as the one in which the repository was originally created. An environment with the same name can be recreated before restoring the repository in it or the actual environment can be restored beforehand.

To restore a data repository:

1. Start HOPEX **Administration.exe**.
2. Connect to the environment in which you want to restore the repository.
3. Right-click the **Repositories** folder and select **New**.



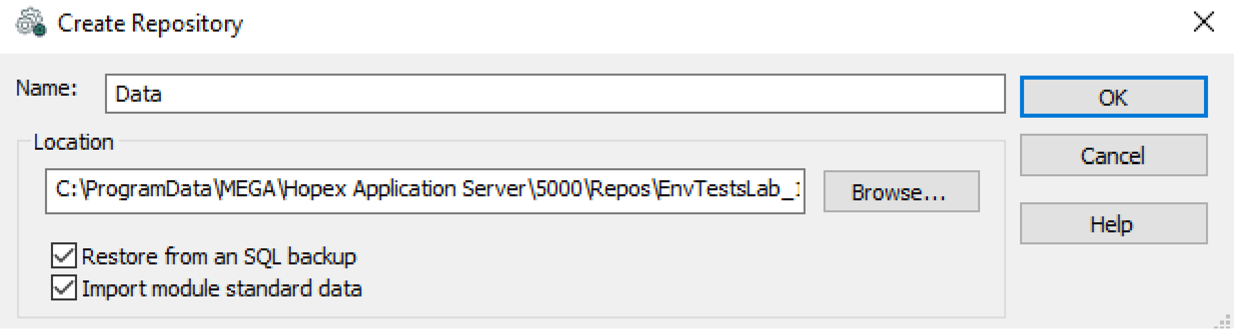
4. In **Name**, enter the name of the repository that is to be restored (the exact same name as the one used for the first creation).

5. Select **Restore from an SQL backup**.

6. Keep the **Import module standard data** option selected.

   This option enables to import the .xmg files of the modules already deployed on the HAS instance.

   Note: If you restore several repositories, clear the **Import module standard data** option and once all of your repositories are restored launch the **Environment Automatic Update**. Else, keep the option selected for the last repository restoration only.


Create Repository

Name: Data

Location

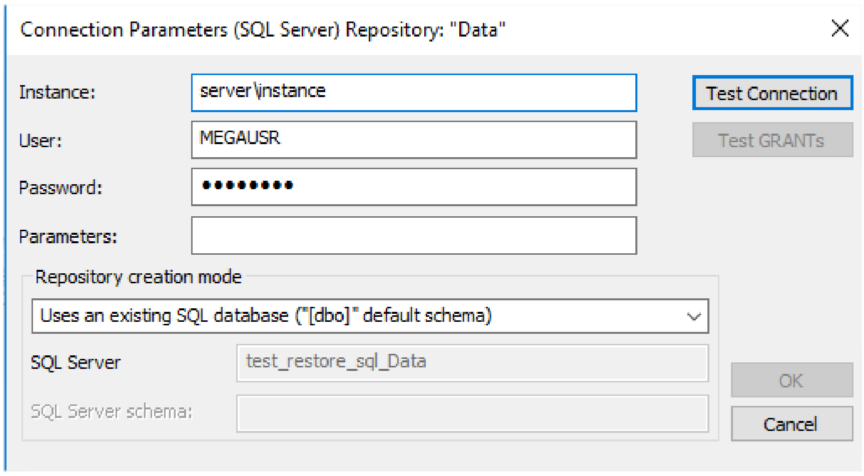
C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\EnvTestsLab_

☑ Restore from an SQL backup

☑ Import module standard data

7. Click **OK**.

8. Specify the connection parameters for accessing the RDBMS where the HOPEX -yet-unreachable data is located.


Connection Parameters (SQL Server) Repository: "Data"

Instance: server\instance

User: MEGAUSR

Password: ••••••••

Parameters:

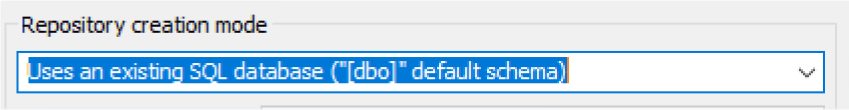
Repository creation mode

Uses an existing SQL database ("[dbo]" default schema)

SQL Server: test_restore_sql_Data

SQL Server schema:

NB: the "Creation Mode" parameter is disable (the choice is not possible) when "Restore from an SQL backup" is selected. As in this case, HOPEX is actually told to re-attach to physical data so no database creation or repository initialization will be carried out.



Repository creation mode

Uses an existing SQL database ("[dbo]" default schema)

9. Click **Test Connection.**

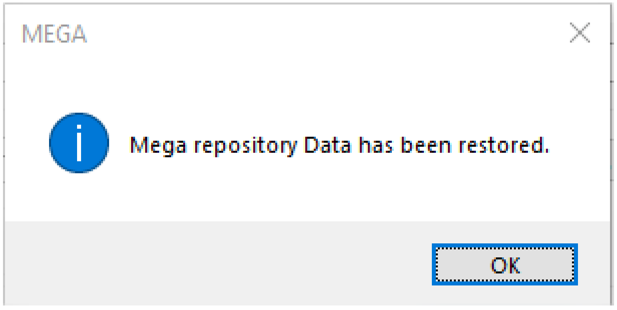
   The test must be successful for the process to continue.

10. Click **Test GRANTs**.

    The test must be successful for the process to continue.

11. Click **OK**.

    The repository is restored.



MEGA

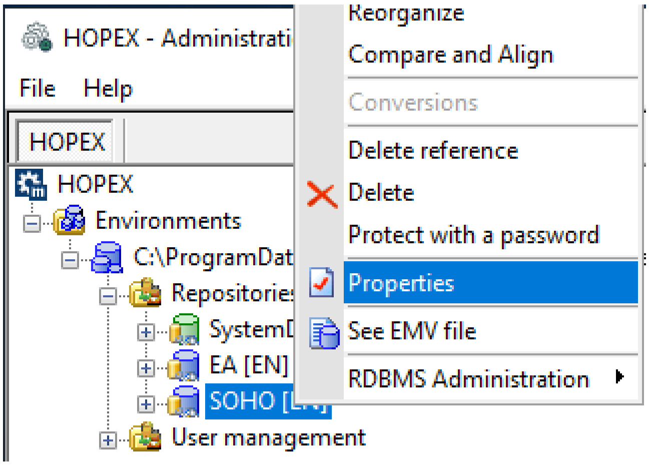
Mega repository Data has been restored.

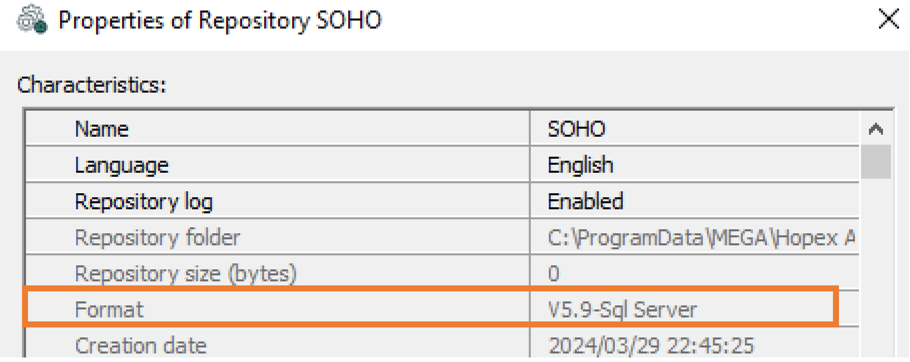
Handling of HOPEX RDBMS repositories specific internal format

There is an internal format used by HOPEX when accessing a repository that is stored on **SQL Server**.

To view this internal format version:

1. Start HOPEX **Administration.exe**.
2. Right-click the HOPEX repository (either SystemDb or data repository) and select **Properties**.




Properties of Repository SOHO

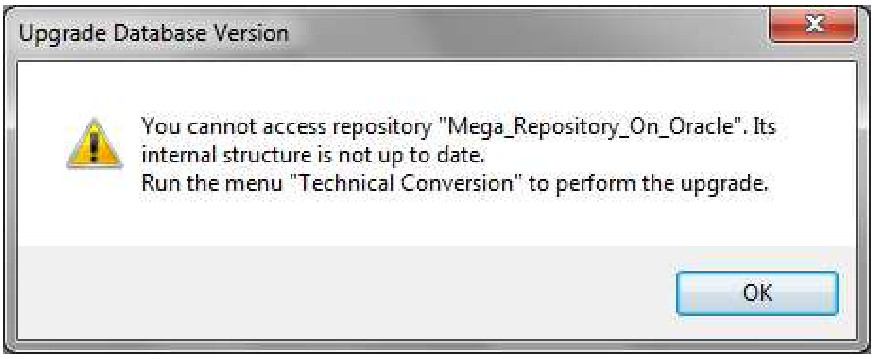
Characteristics:

Name	SOHO
Language	English
Repository log	Enabled
Repository folder	C:\ProgramData\MEGA\Hopex A
Repository size (bytes)	0
Format	V5.9-Sql Server
Creation date	2024/03/29 22:45:25

When upgrading your HOPEX installation (applying a Cumulative Update or migrating your data from a HOPEX SP version to the next one), there might be some modifications leading to a new **internal format** version.

Menus are available to manually activate this **internal format** upgrade.

When you need to upgrade the **internal format** version, you are prompted to do it:


Upgrade Database Version

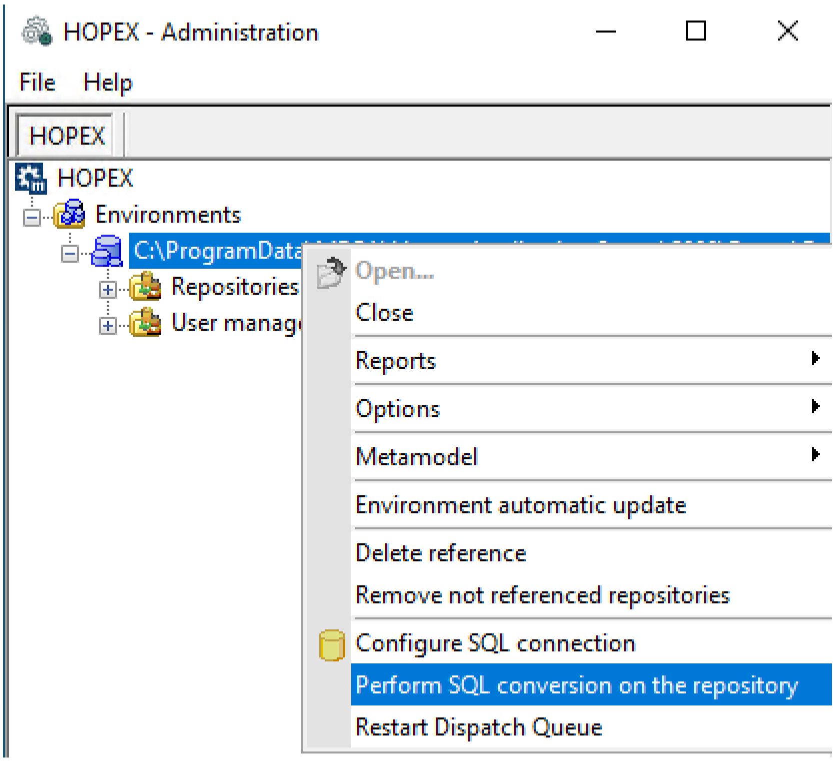
You cannot access repository "Mega_Repository_On_Oracle". Its internal structure is not up to date.
Run the menu "Technical Conversion" to perform the upgrade.

OK

Note: The technical conversion of the repositories of the environment must be done before upgrading to the environment:

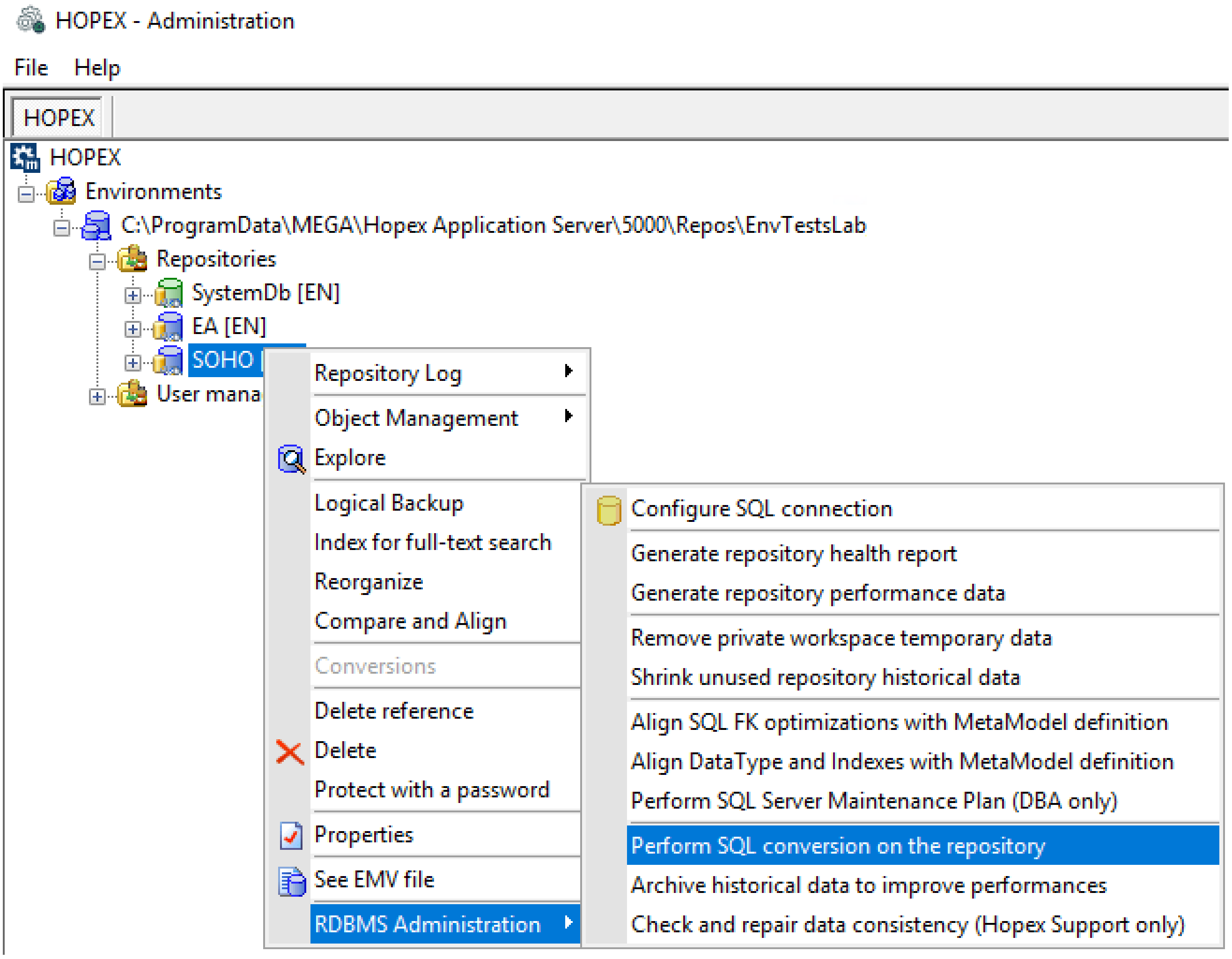
1. Apply the technical conversion on the SystemDb:

   Right-click the environment and select **Perform SQL conversion on the repository**.



2. Apply the technical conversion on the other data repositories of the environment:

   For each repository, right-click the repository and select **RDBMS Administration > Perform SQL conversion on the repository.**


HOPEX - Administration
File
Help
HOPEX
HOPEX
Environments
C:\ProgramData\MEGA\Hopex Application Server\5000\Repos\EnvTestsLab
Repositories
SystemDb [EN]
EA [EN]
SOHO
User mana
Repository Log
Object Management
Explore
Logical Backup
Index for full-text search
Reorganize
Compare and Align
Conversions
Delete reference
Delete
Protect with a password
Properties
See EMV file
RDBMS Administration
Configure SQL connection
Generate repository health report
Generate repository performance data
Remove private workspace temporary data
Shrink unused repository historical data
Align SQL FK optimizations with MetaModel definition
Align DataType and Indexes with MetaModel definition
Perform SQL Server Maintenance Plan (DBA only)
Perform SQL conversion on the repository
Archive historical data to improve performances
Check and repair data consistency (Hopex Support only)

Vocabulary

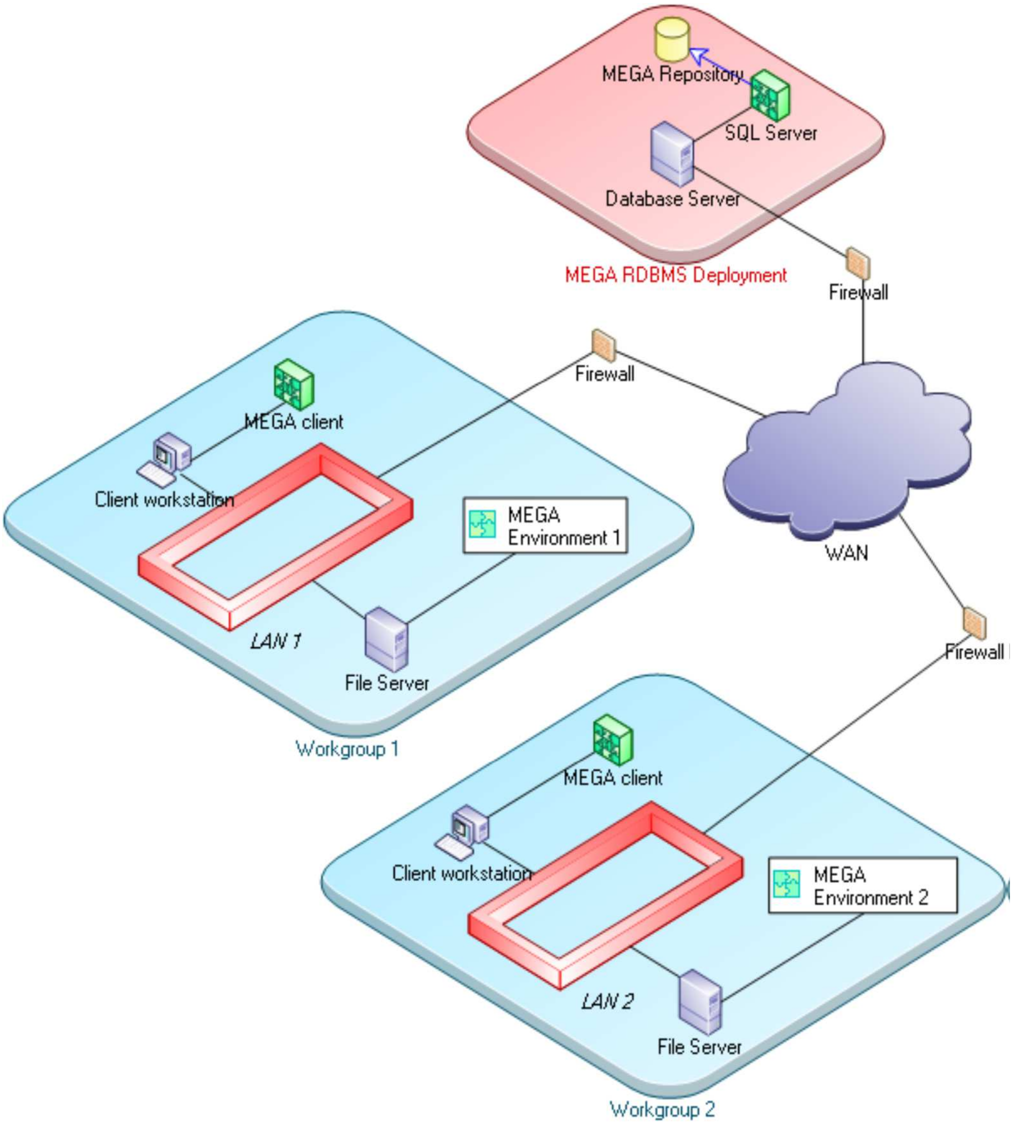
Term	Comment
Database	A database is a collection of data, usually in the form of tables or files, under the control of a database management system (DBMS).
Database server (hardware)	A database server is a machine providing database services to other machines. In this document the database server is a machine running relational database management systems. A database server can host one or several instances. Example: • Server 'iba.company.com' • Server '192.888.777.666' • Server 'SQL02'
DBA	The DataBase Administrator is responsible for administering, monitoring, and maintaining the database.
DBMS	A DataBase Management System (DBMS) is a set of software programs that controls the organization, storage, management, and retrieval of data in a database. Example: GBMS, Oracle…
GBMS	GBMS is MEGA's historical proprietary DBMS.
HOPEX Environment	On RDBMS installations, an environment is a group of directories where HOPEX generates documents, log files, etc.
RDBMS	Relational DataBase Management System. Examples: Oracle, SQL Server, DB2 Universal Database,…
Repository	A repository is a structured collection of data. A HOPEX repository is a collection of HOPEX data. Data is structured in relation to a metamodel. Object names are often unique within the repository or with a namespace of the repository.
Schema	A schema object is a logical data storage structure.

Term	Comment
	In Oracle, it is a collection of objects (example: tables, views, indexes, procedures, functions…) mapped to an Oracle user. A schema is stored in one/several tablespace objects of the database. **It is strongly recommended to isolate each HOPEX Repository in a separate Oracle schema (User Repositories AND SystemDb repository)**
Storage format	HOPEX term. It defines the type of DBMS storing HOPEX data. Possible value is SQL Server: storage in SQL Server DBMS.
SystemDb repository	HOPEX Term. It is a HOPEX repository that stores system data, such as, user definition, metamodel definition, template definitions, queries, diagram configuration. This data can be shared by all user repositories within a HOPEX environment. A SystemDb repository is associated to one/several user repositories.
User repository	HOPEX Term. This is a HOPEX repository storing data, such as diagrams, org-units...

Appendix - FAQs

Is it possible to share user repositories and the SystemDb repository through user's workgroups that do not share a file server?

Yes. You can duplicate HOPEX Environment on each side to obtain this kind of configuration.



Is it possible to have a user repository stored on a GBMS and a SystemDb repository stored on a SQL server?

No. Some features might work but it is not tested an not supported. Moreover many specific features will not work.

Is it possible to consult the data from a SQL Server?

It is technically possible and supported (e.g.: SELECT statement). However, this requires knowledge of the HOPEX RDBMS implementation and the HOPEX Metamodel. It is much easier to query the data from within HOPEX.

Is it possible to update the data from an SQL Server?

It is technically possible but **NOT supported** (e.g.: UPDATE or DELETE statement). This requires the knowledge of the HOPEX RDBMS implementation and of the HOPEX Metamodel. Data updates must be performed from within HOPEX. All updates from outside the HOPEX application are made at the customer's risk. Consequences of inappropriate updates will not be supported.

Hopex Unified Authentication Service

1. Unified Authentication Service Overview

Unified Authentication Service (UAS) is Hopex web-based authentication system. UAS is a centralized service, which enables to manage several authentication types:

- External authentication or Single Sign-On (SSO)

  SSO is an authentication system enabling users to login with a single ID and password to access Hopex and any other Customer application types like web or mobile, access control for APIs, and federation (support for external identity providers like Google and enterprise identity management systems via SAML2).

  UAS manages two standard authentication protocols:

  - **SAML2**

    Security Assertion Markup Language 2.0 (SAML 2.0) is a version of the SAML standard for exchanging authentication and authorization data between security domains.

    SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end-user) between a SAML authority (Identity Provider), and a SAML consumer (Service Provider).

    SAML2 Specifications: https://tools.ietf.org/html/rfc7522

  - **Open ID Connect**

    OpenID Connect (OIDC) enables to implement a centralized identity federation and respond to SSO issues.

    OIDC specifies an HTTP Restful authentication interface and relies on the OAuth2 protocol to do delegation authorization, i.e. in most of the cases, the end user no longer needs to directly provide credentials to a third-party application. OIDC also uses the JSON Web Token (JWT) exchange formalism to convey user identities to applications, as well as their roles / entitlements.

    Open ID Specifications: http://openid.net/connect/

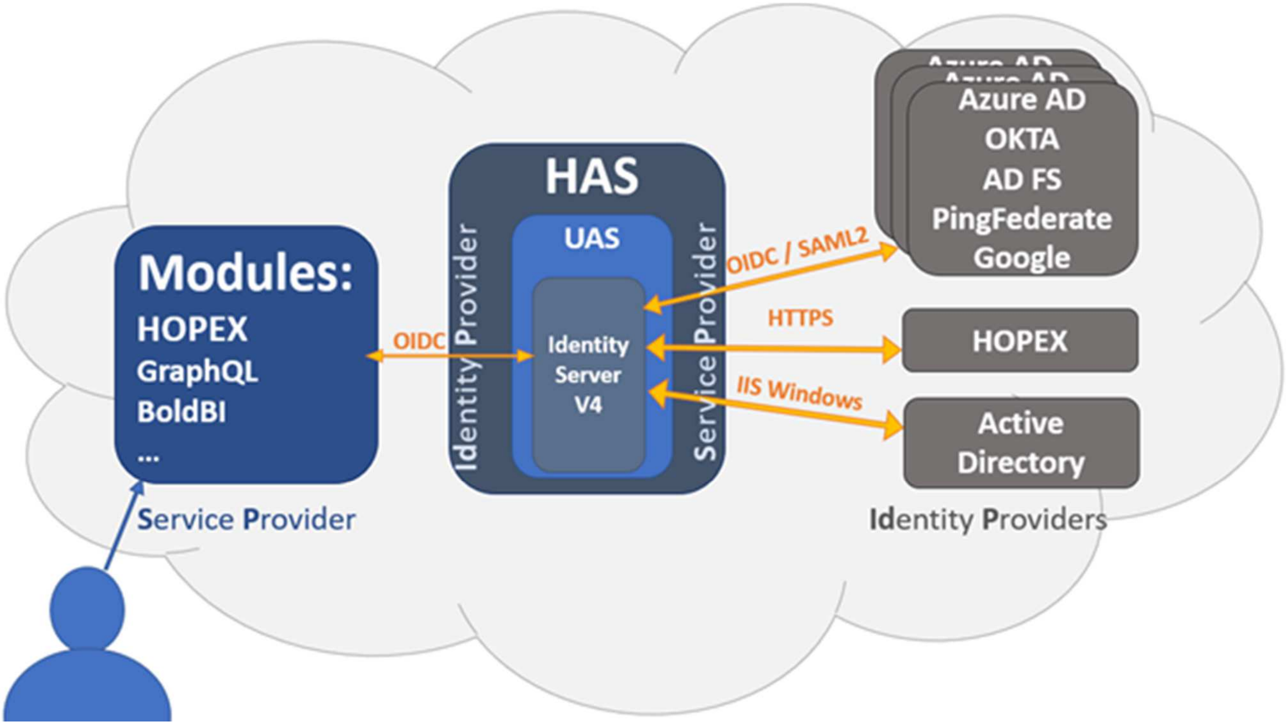
  These protocols are supported by some Identity Providers (IDPs) like Azure AD, AD FS, OKTA, Google.

- Authentication through Hopex platform

  If you do not have any external authentication module, you can use Hopex platform to manage user authentication (HOPEX or Windows).

  ➔ See *Hopex Administration (Web)* documentation for information regarding authentication through Hopex platform.

If needed, you can define several providers of OpenID and/or SAML2 types.


Modules:
HOPEX
GraphQL
BoldBI
...
Service Provider
OIDC
HAS
UAS
Identity Provider
Identity Server V4
Service Provider
OIDC / SAML2
HTTPS
IIS Windows
Azure AD
Azure AD
Azure AD
OKTA
AD FS
PingFederate
Google
HOPEX
Active Directory
Identity Providers

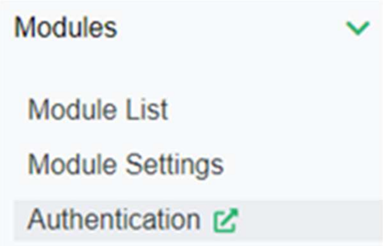
2. Configuring UAS Options

2.1. Configuring authentication options

UAS options are configured in HAS console.

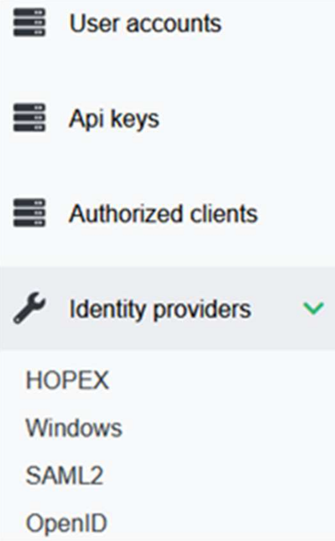
To configure authentication options:

1) Connect to **HAS** console.
2) Access the **Authentication** module.
   a. In the left pane, expand **Modules**.



   b. Click Authentication.

3) In UAS Administration, click the **Identity providers** section.



4) Select the Identity provider you want to configure.
5) Click **Create**.
6) To activate this Identity Provider, select **Active**.
7) You can configure as many Identity providers as you want.
   - ➢ See Identity Provider Option Description.

2.2. Identity Provider Option Description

The identity provider options are the following:

- **HOPEX**, see Hopex provider section
- **IIS Windows**, see IIS Windows provider section

SAML2, see

- SAML2 provider section
- **Open ID Connect**, see OpenID Connect (OIDC) provider section

2.2.1. Hopex provider

The Hopex provider is the Hopex default provider, which displays a login page with username and password.

To authenticate Hopex users, use Hopex User Native Authentication.

➔ See *Hopex Administration* documentation: “Authentication in Hopex” section.

2.2.2. IIS Windows provider

With the IIS Windows provider Hopex users are authenticated by Windows Authentication.

To configure IIS Windows provider, define the following parameters:

- **Display Name**

  Defines the name of the button displayed on the login page for IIS Windows Identity provider.

  Default value: “Windows”

- **Windows Roles**

  As some logins belong to several (hundreds) groups you might need to filter Hopex related groups. If you do not filter the groups, you might get http 400 errors, due to the size of cookies generated from the claims retrieved.

- **ClaimForRoles**

  Enter the name of the claim used for the role.

- **Windows Source Identifier**

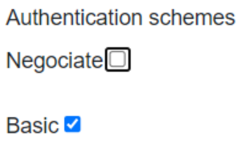
  You can define the property used to identify the connection.

  - **Standard (by default)**
  - **sAMAccountName**
  - **EmployeeId**

- **Authentication schemes**

  If IIS and HAS:

  - are on the same machine, keep the default settings (**Negociate** and **Basic** seleted)
  - are not on the same machine (e.g.: in a cluster mode) you must clear **Negociate**.



Authentication schemes

Negociate ☐

Basic ☑

2.2.3. SAML2 provider

SAML 2.0 is an XML based framework, used to describe and exchange security information. It can be used for Single Sign On (SSO), Identity Management and Federation.

To use SAML2 provider, you must set UAS in SSL Mode.

UAS manages only Service Provider (SP) initiated SSO and not Identity Provider (IDP) initiated SSO.

For examples regarding SAML2 Identity Provider implementation see:

- OKTA Configuration with SAML2
- Pingfederate Configuration with SAML2
- Azure AD Configuration with SAML2

To configure SAML2 Identity provider, define the following parameters:

In the **General** tab:

- **Display Name**

  Defines the name of the button displayed on the login page for SAML2 Identity provider.

- **Entity Identifier (Entity Id)**

  Entity Identifier is the identity of the Service Provider to use when sending requests to the Identity Provider and presenting the Service Provider in metadata.

- **Metadata location**

  Location of the metadata for the Identity Provider. Automatically enabled.

  The location can be a URL, an absolute path to a local file, or an app relative path (e.g.: ~/App_Data/IdpMetadata.xml). By default, the Entity Id is interpreted as the metadata location (this is a convention).

- **Groups Authorized**

  As some logins belong to several (hundreds) groups you might need to filter Hopex related groups. If you do not filter the groups, you might get http 400 errors, due to the size of cookies generated from the claims retrieved.

- **ClaimForRoles**

  Enter the name of the claim used for the role.

- **ClaimForSub**

  Enter the name of the claim used for the sub.

- **ModulePath**

  Application root relative path for Saml2 Assertion Consumer EndPoint.

  By default: "AuthServices".

  It is used in the calculation of the url.

  In case several SAML2 are configured, they must have a distinct ModulePath value.

In the **Certificate and signature** tab:

- **Certificate friendly name**

  Certificate used by the service provider for signing or decryption.

- **Want assertion signed**

Select this option if you want the assertions to be signed.

- **Want AuthnRequests signed**

  Select this option if you want this Identity Provider to get the AuthRequests signed.

- **Authenticate Request Signing Behavior**

  You can modify the authenticate request signing behavior:

  - **"IfIdpWantAuthnRequestsSigned" (by default): signs AuthnRequests if the Identity Provider is configured for it.**
  - **"always": always signs AuthnRequests. AuthnRequestsSigned is set to true in metadata.**
  - **"never": never signs AuthnRequests.**

- **Certificate use**

  Allows to sign and/or encrypt SAML2 assertions.

  You can modify the certificate use:

  - **Both (by default)**
  - **Signing**
  - **Encryption**

In the **Organization** tab:

- **Name / Email / Url**

  Enter the information (name, email, URL) describing the organization responsible for the entity.

In the **Contact** tab:

- **Email**

  Enter the collection of contacts for the SAML2 entity.

2.2.4. OpenID Connect (OIDC) provider

Use the OpenID Connect (OIDC) provider to authenticate Hopex users with an OpenID Connect account by OAUTH2.

For examples regarding OpenID Connect Identity Provider implementation see:

- OKTA Configuration with OpenID Connect
- Pingfederate Configuration with OpenID Connect

Prerequisite: authentication is performed using the Authorization Code Flow (response_type=code) only.

All tokens are returned from the Token Endpoint

(source: https://openid.net/specs/openid-connect-core-1_0.html#toc).

The Authorization Code Flow returns an Authorization Code to the Client, which can then exchange it for an ID Token and an Access Token directly. This provides the benefit of not exposing any tokens to the User Agent and possibly other malicious applications with access to the User Agent.

The Authorization Server can also authenticate the Client before exchanging the Authorization Code for an Access Token.

The Authorization Code flow is suitable for Clients that can securely maintain a Client Secret between themselves and the Authorization Server.

The Authorization Code Flow goes through the following steps:

1. Client prepares an Authentication Request containing the desired request parameters.
2. Client sends the request to the Authorization Server.
3. Authorization Server Authenticates the End-User.
4. Authorization Server obtains End-User Consent/Authorization.
5. Authorization Server sends the End-User back to the Client with an Authorization Code.
6. Client requests a response using the Authorization Code at the Token Endpoint.
7. Client receives a response that contains an ID Token and Access Token in the response body.
8. Client validates the ID token and retrieves the End-User's Subject Identifier.

To configure OpenID Connect provider, define the following parameters:

- **Display Name**

  Defines the name of the button displayed on the login page for OpenID Connect Identity provider.

  This name is also used in the calculation of the RedirectURL (specific to OpenID Connect protocol), which is also displayed on the login page.

- **Authority server url**

  This URL defines the OpenID server location.

- **Proxy Url**

  If the proxy is configured on the same server as UAS, this url defines the output url for the protocol to reach its endpoints (e.g.: DiscoveryEndPoint and TokenEndPoint).

- **Client Identifier**

  Is the identifier of your application.

- **Secret client**

  You can use either:

  - the Secret > Client Secret (less secure), or
  - a **Certificate** defined by a **Thumbprint** and an **Audience**, which is the Token EndPoint url of your IdentityServer, so as to read the Access Token via this certificate.

- **Scopes**

  Each OpenID server must support the OpenId scope that provides the JWT (JSON Web Token) claims (https://datatracker.ietf.org/doc/html/rfc7519).

  In addition, OpenID server can support other scopes like email.profile from which other claims are provided.

- **ClaimForRoles**

  Enter the name of the claim used for the role.

- **ClaimForSub**

  Enter the name of the claim used for the sub.

- **MetadataAddress server url**

The **DiscoveryEndPoint** url provides the metadata of the OpenID Connect identity provider. It provides information like endpoint token and scopes.

Usually, you do not need to enter this URL as it comes from the Authority Server URL. It should be:

```
[Authority Server url]/.well-known/openid-configuration
```

- **Groups Authorized**

  As some logins belong to several (hundreds) groups you might need to filter Hopex related groups. If you do not filter the groups, you might get http 400 errors, due to the size of cookies generated from the claims retrieved.

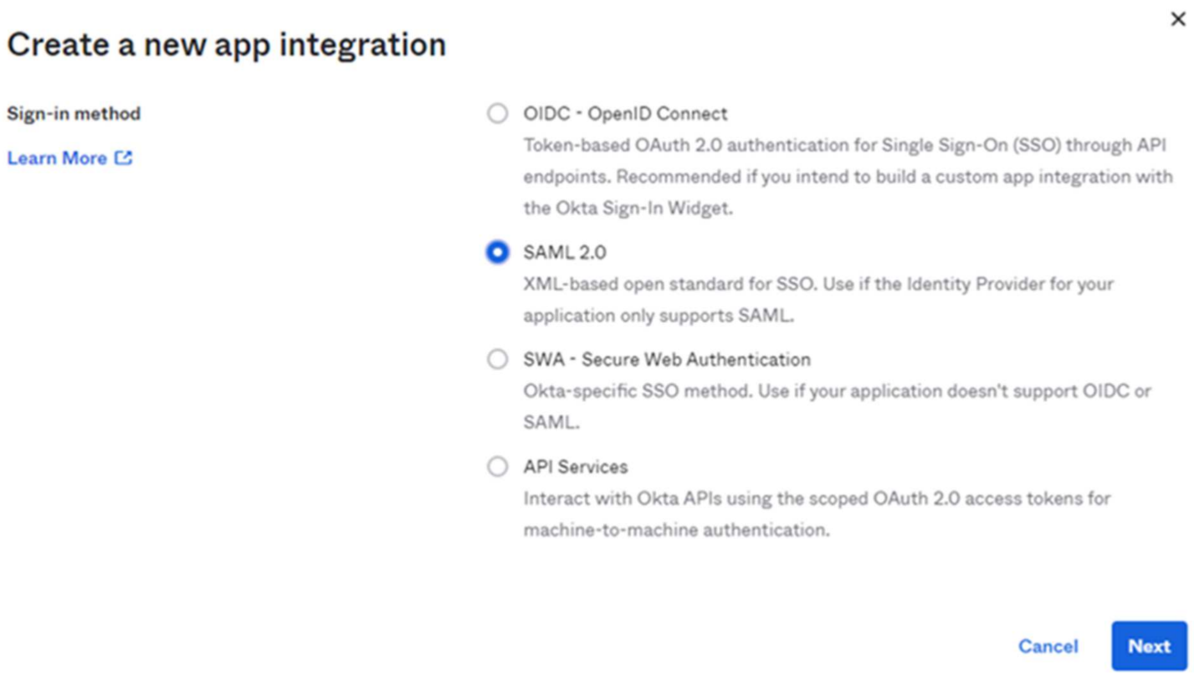
3. Configuration Examples

3.1. OKTA Configuration with SAML2

3.1.1. Configuring OKTA application

To configure OKTA application:

1) Connect to your OKTA account.
2) Go to **Admin Portal > Applications**: create an application.
3) Select **SAML2** sign-in method.



Create a new app integration

Sign-in method

Learn More

○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

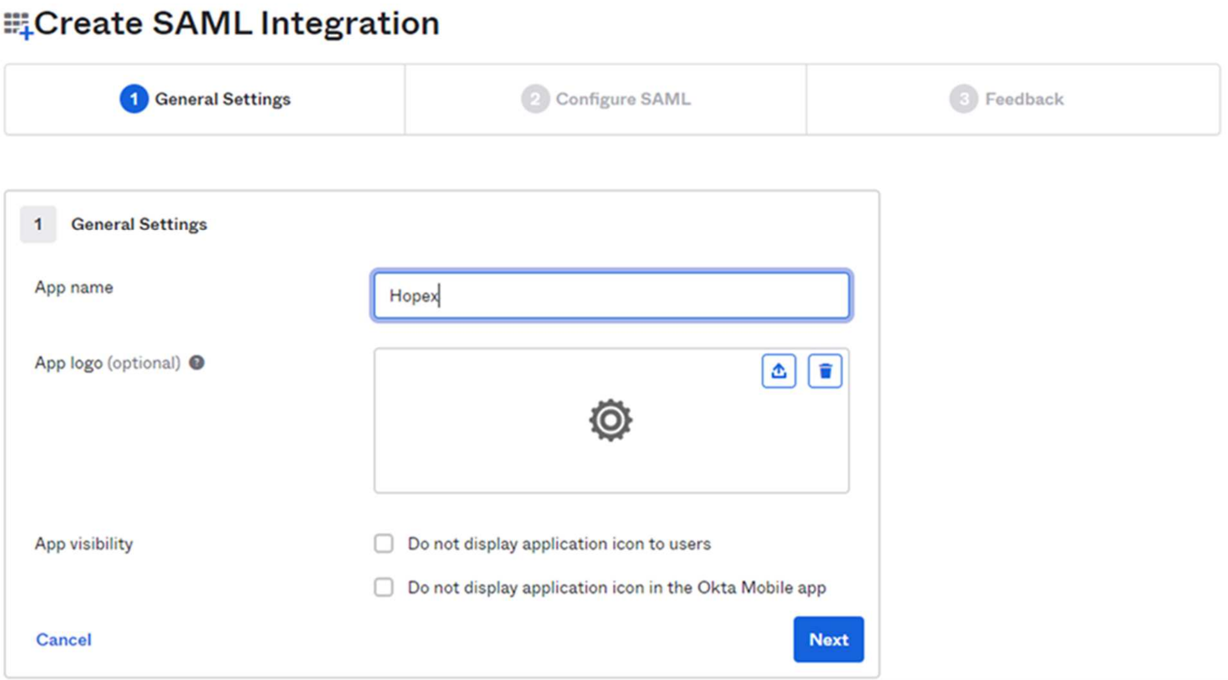
● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

4) Click **Next**.
5) In **General Settings**:
   - Enter the **App name**.

     `Example: Hopex`



Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

1 General Settings

App name: Hopex

App logo (optional)

App visibility

□ Do not display application icon to users

□ Do not display application icon in the Okta Mobile app

Cancel | Next

6) Click **Next**.

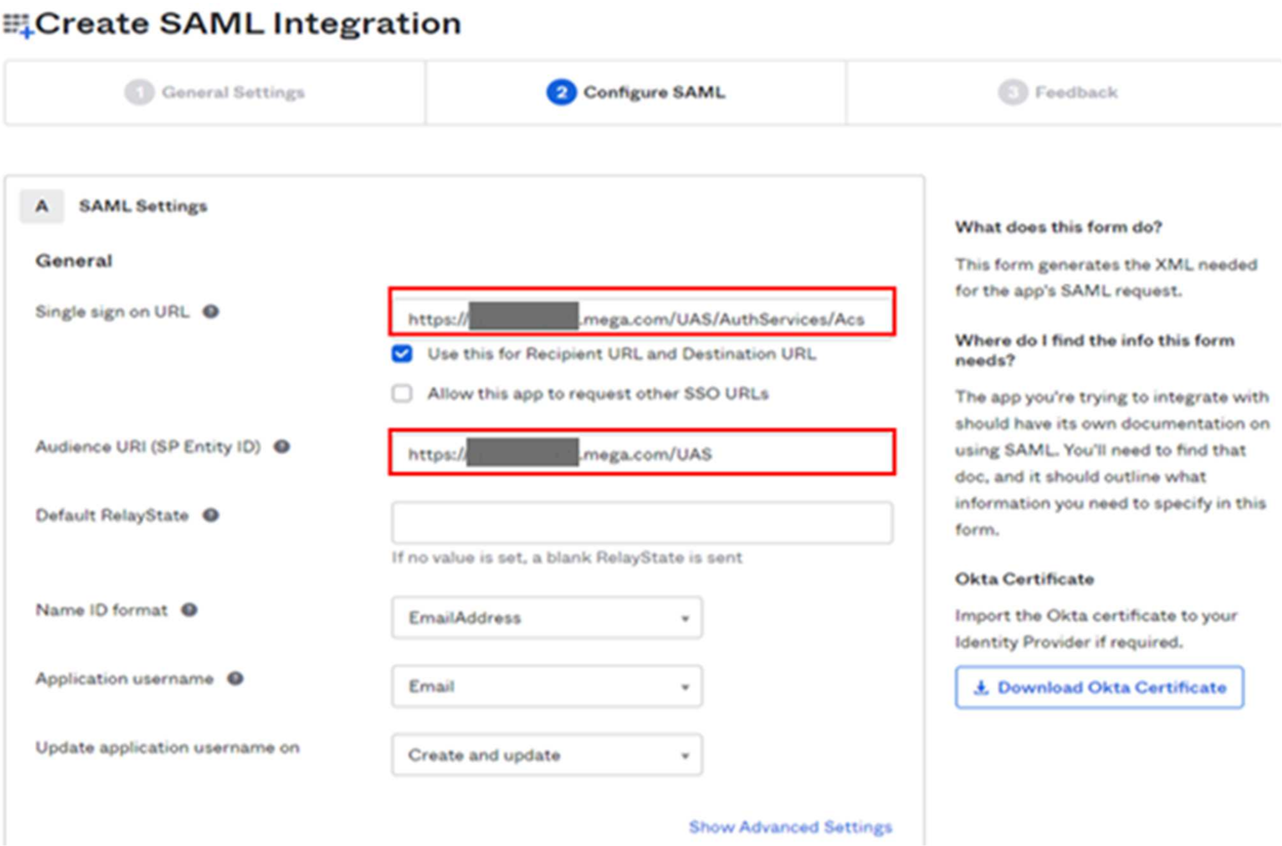
7) In **Configure SAML**:

- Enter **Single Sign on URL** with the following URL syntax:

  https://<server name>/UAS/AuthServices/Acs

- Enter **Audience URI** with the following URL syntax:

  https://<server name>/UAS



Create SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

A SAML Settings

General

Single sign on URL: https://[redacted].mega.com/UAS/AuthServices/Acs

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https:/[redacted].mega.com/UAS

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Email

Update application username on: Create and update

Show Advanced Settings

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

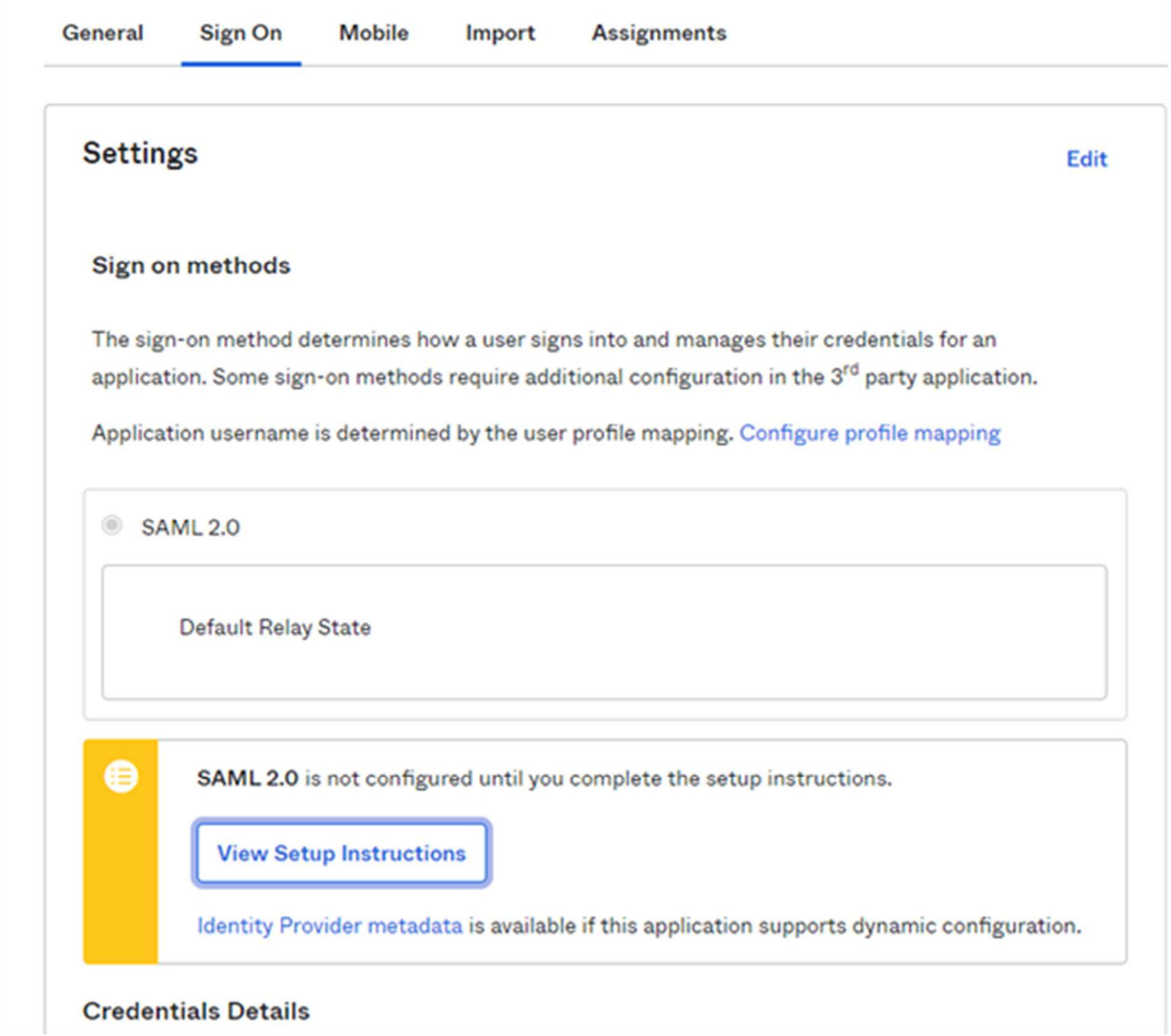
- In **Attribute Statements**, add an attribute:

- **Name**: “sub”
- **Value**: user.email.

8) Click **Finish**.

At the end of the App creation, from the **View Setup Instructions**, write down the following information carefully as you will need it for the UAS configuration:

- **Identity Provider Issuer**
- **Identity Provider metadata**



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

Default Relay State

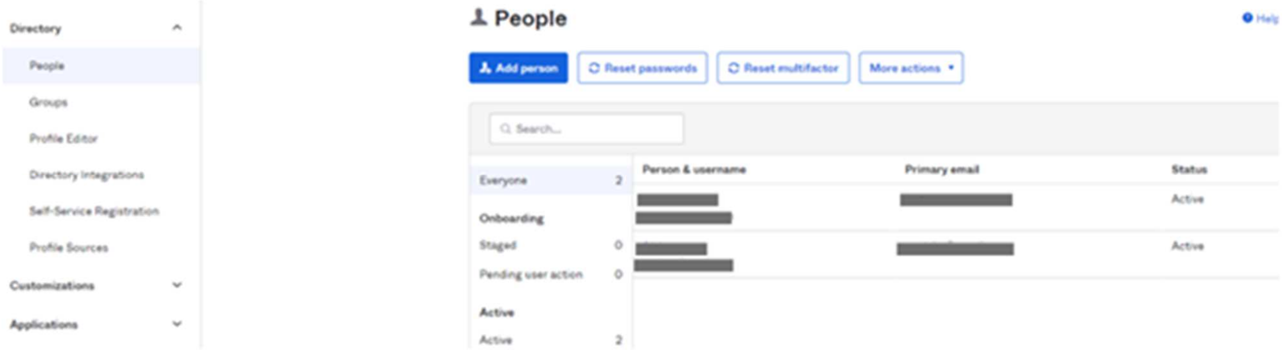
SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

Credentials Details

9) Create users that are allowed to connect to Hopex with OKTA \ SAML2 authentication:

   a. In **Directory > People**: click **Add person**.

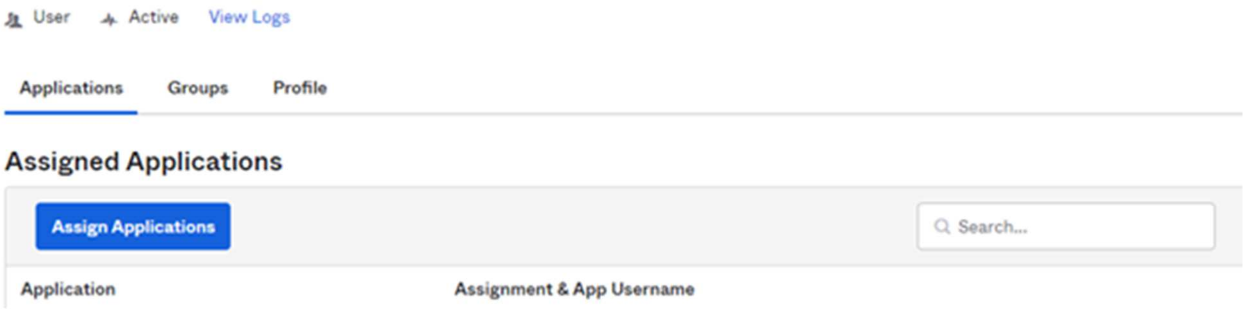


Person & username	Primary email	Status
[redacted]	[redacted]	Active
[redacted]	[redacted]	Active

b. Enter the person characteristics and **Save**.

c. Click the user to access its properties

d. Click **Assign Applications** and assign the OKTA application ("Hopex") to the user.



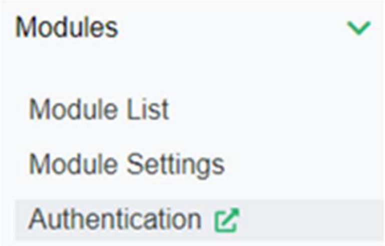
3.1.2. Configuring UAS with OKTA

To configure UAS with OKTA:

1) Connect to **HAS** console.

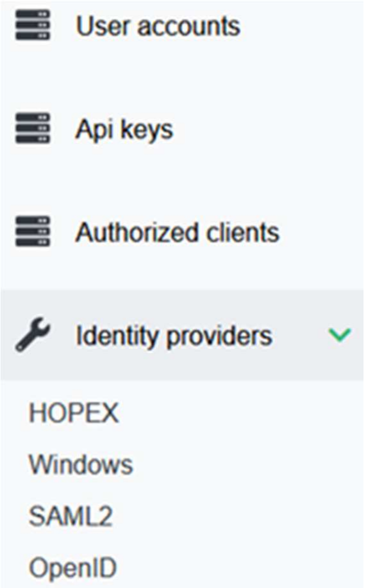
2) Access the **Authentication** module.

   a. In the left pane, expand **Modules**.



   b. Click **Authentication**.

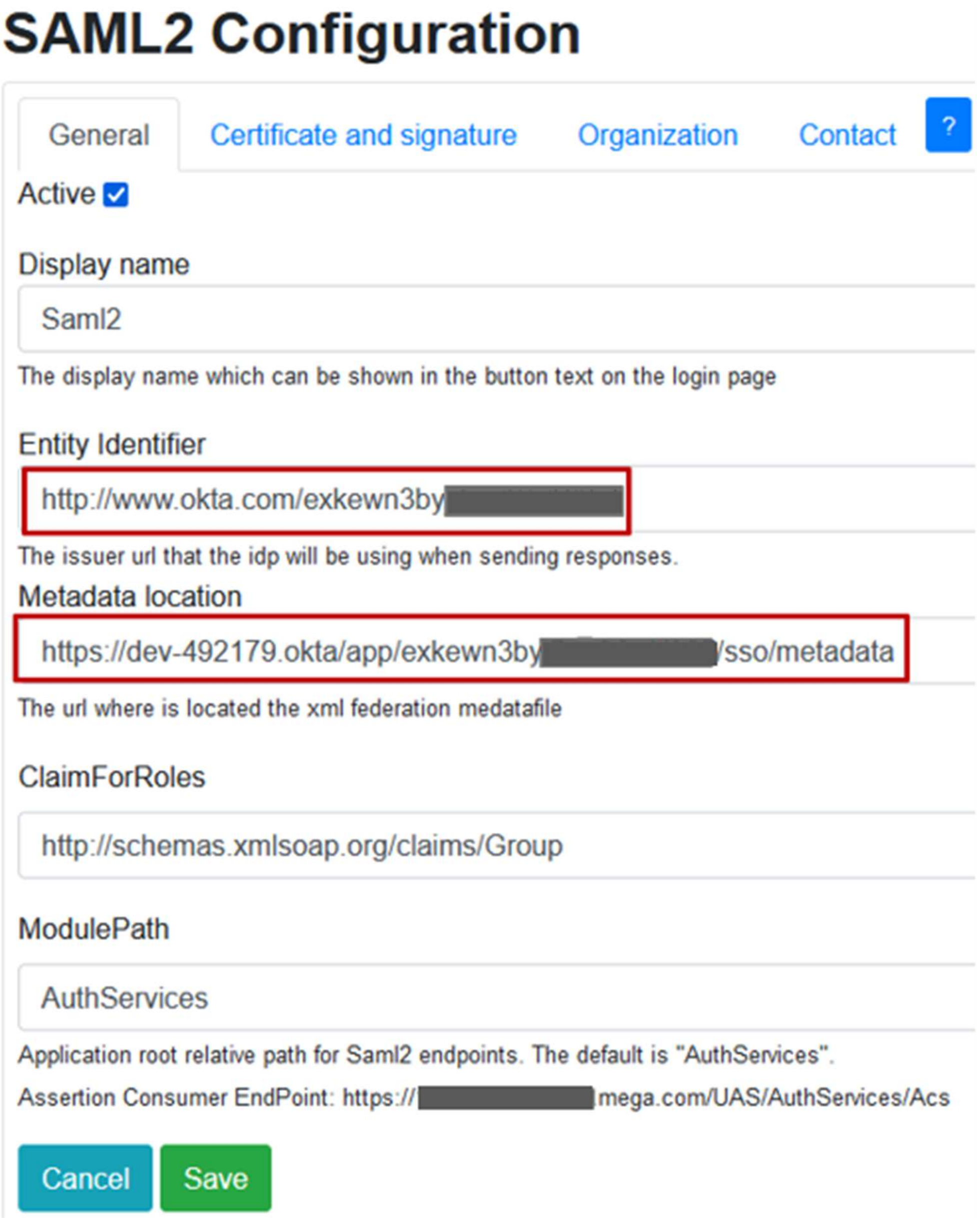
3) In **UAS Administration**, in the **Identity providers** section, select **SAML2**.



4) Click **Create**.

5) In **SAML2 Configuration**, to activate SAML2 Identity Provider, select **Active** and enter the required information:

- **Entity Identifier**
- **Metadata Location**



SAML2 Configuration

Active ☑

Display name

Saml2

The display name which can be shown in the button text on the login page

Entity Identifier

http://www.okta.com/exkewn3by[redacted]

The issuer url that the idp will be using when sending responses.

Metadata location

https://dev-492179.okta/app/exkewn3by[redacted]/sso/metadata

The url where is located the xml federation medatafile

ClaimForRoles

http://schemas.xmlsoap.org/claims/Group

ModulePath

AuthServices

Application root relative path for Saml2 endpoints. The default is "AuthServices".

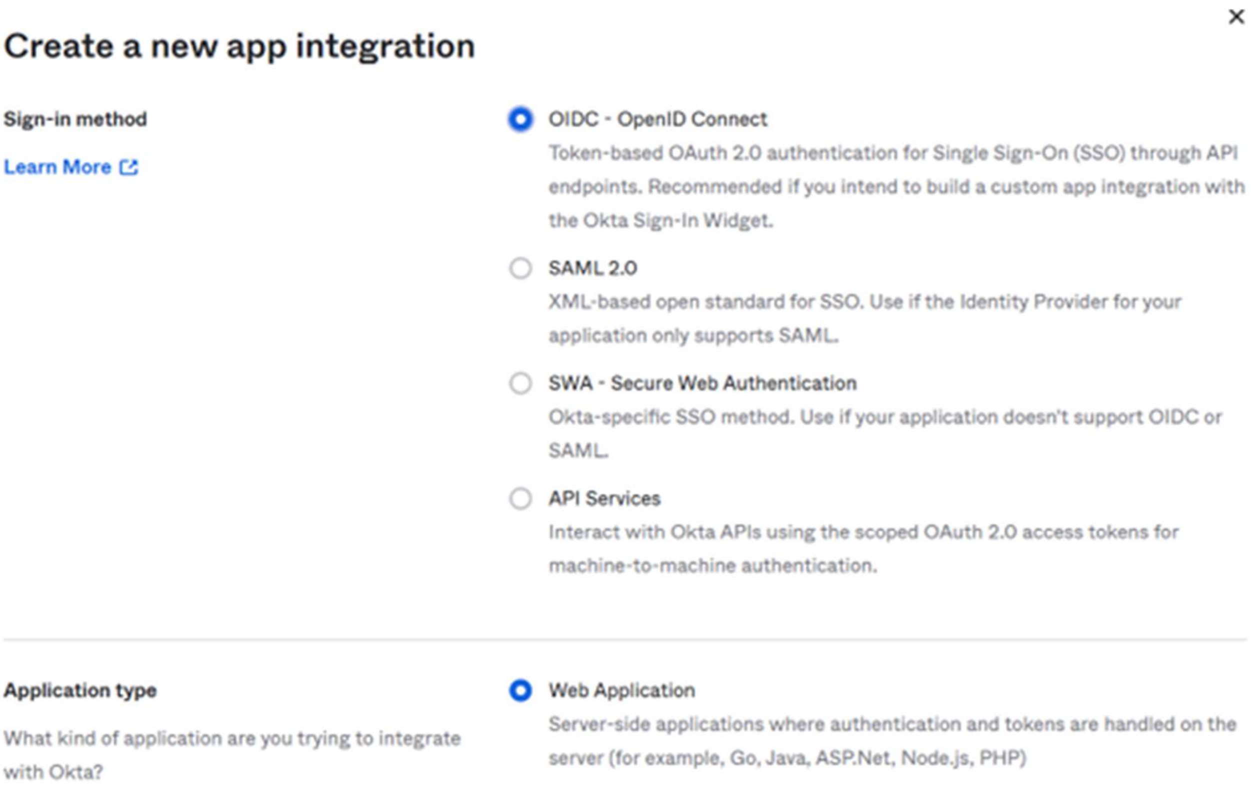
Assertion Consumer EndPoint: https://[redacted]mega.com/UAS/AuthServices/Acs

3.2. OKTA Configuration with OpenID Connect

3.2.1. Configuring OKTA application

To configure OKTA application:

1) Connect to your OKTA account.
2) Go to **Admin Portal > Applications**: create an application.
3) Select:
    - **Sign-in method**: “OIDC – OpenID Connect“
    - **Application type**: “Web Application”.



Create a new app integration

×

Sign-in method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

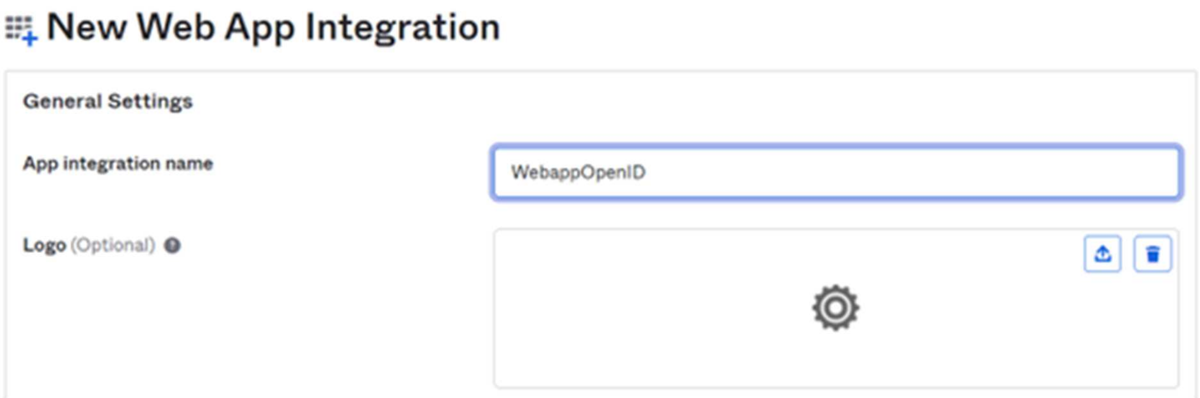
● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

4) Click **Next**.

5) In **General Settings**:

- Enter the **App integration name**.

  `Example: WebappOpenID`



New Web App Integration

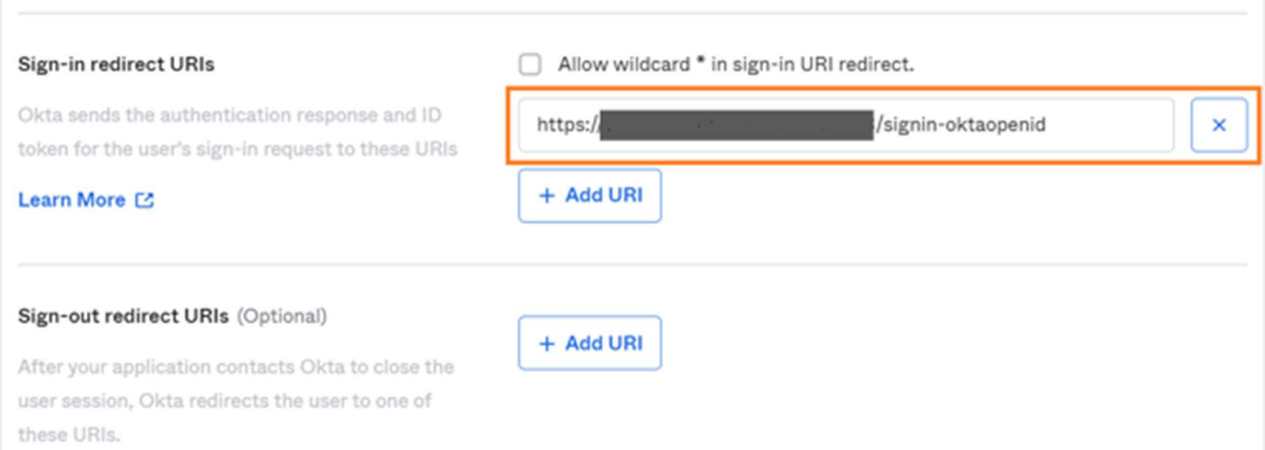
General Settings

App integration name: WebappOpenID

Logo (Optional)

- Enter the **Sign-in redirect URIs** with the following URL syntax:

  https://<server name>/signin-oktaopenid (in lower case letters)



Sign-in redirect URIs

☐ Allow wildcard * in sign-in URI redirect.

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

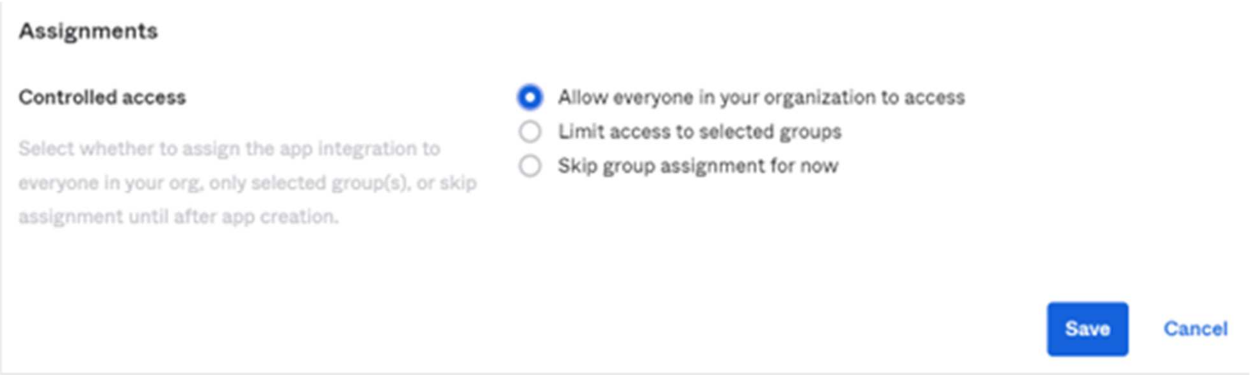
https:/[redacted]/signin-oktaopenid

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

- In **Assignments**: select your **Controlled access**.

  For example: "Allow everyone in your organization to access"



Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

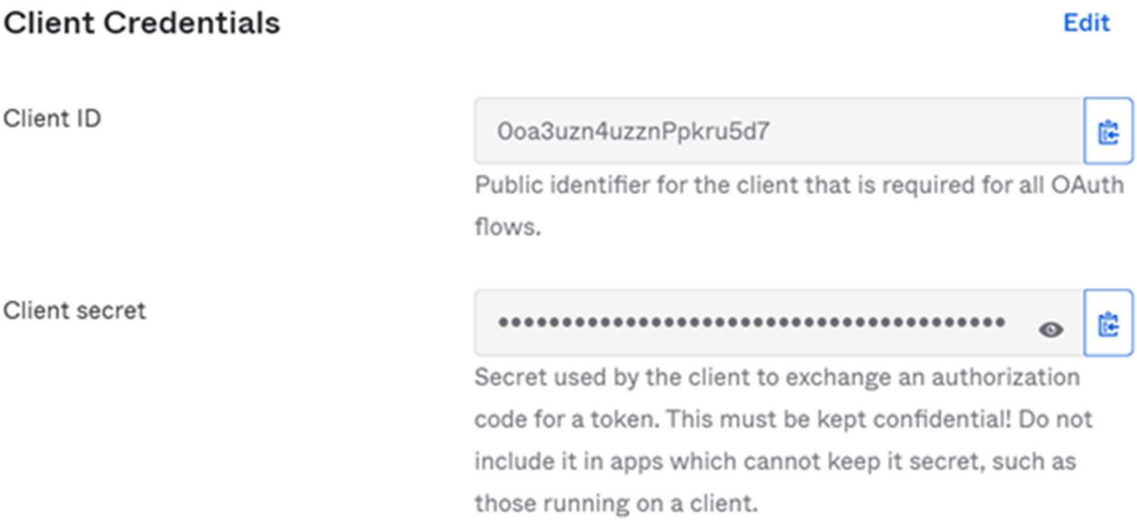
● Allow everyone in your organization to access
○ Limit access to selected groups
○ Skip group assignment for now

6) Click **Save**.

   You get **Client Credentials** information.

7) Write down the following information carefully as you will need it for UAS configuration:

   - **Client ID**
   - **Client secret**



Client Credentials

Client ID: 0oa3uzn4uzznPpkru5d7

Public identifier for the client that is required for all OAuth flows.

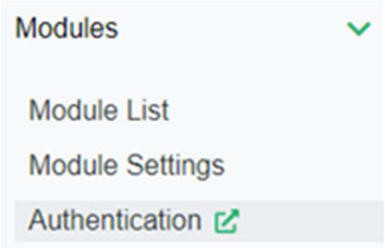
Client secret: ••

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

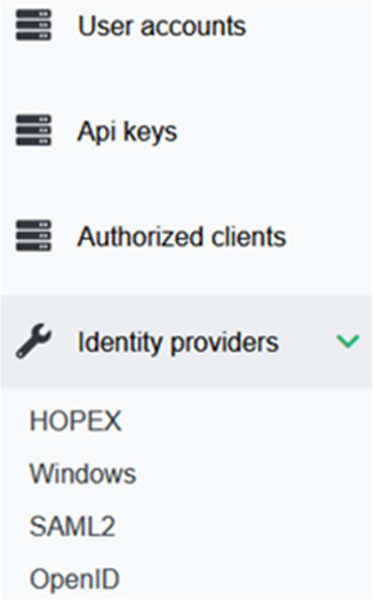
3.2.2. Configuring UAS with OKTA

To configure UAS with OKTA:

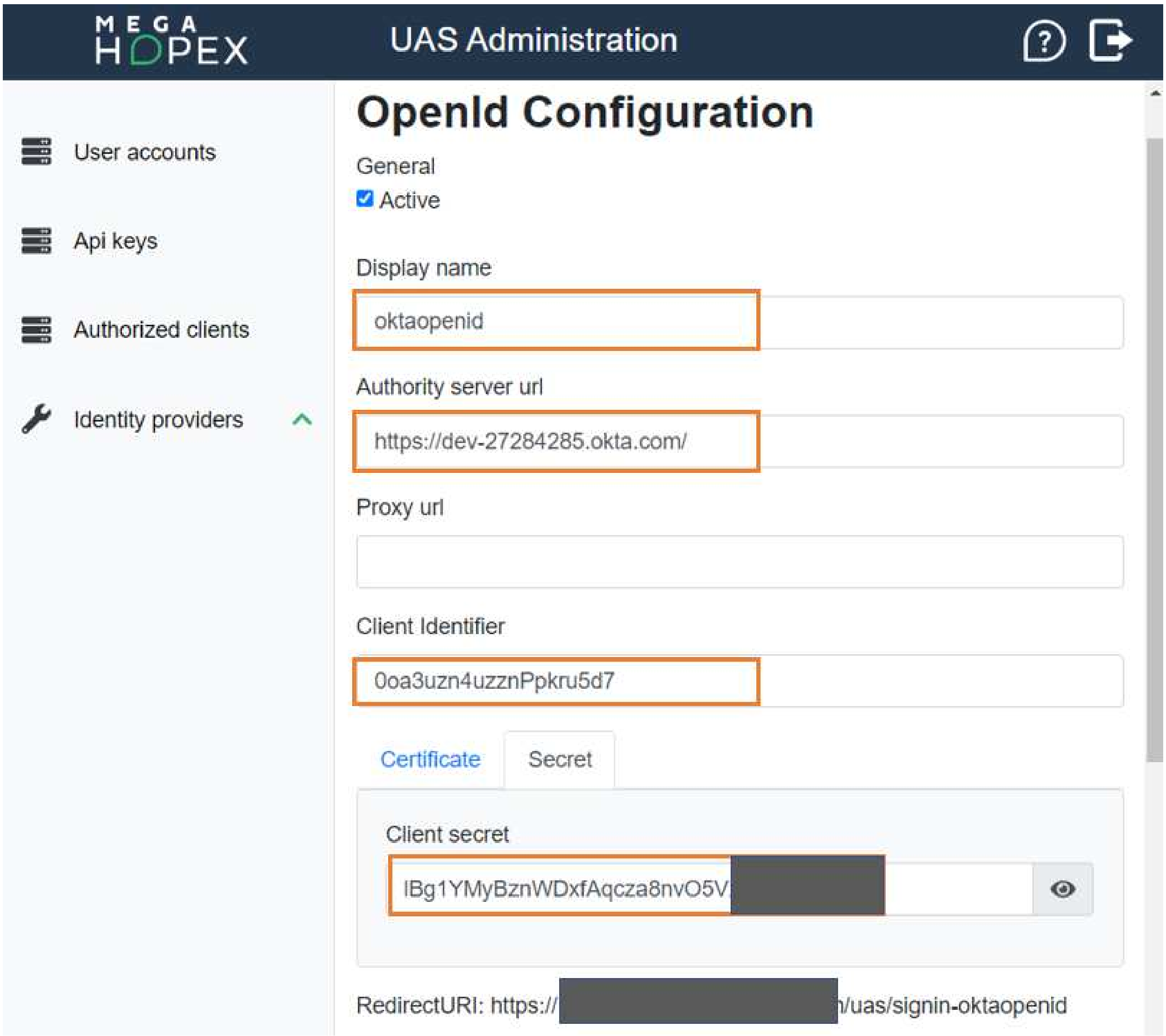
1) Connect to **HAS** console.
2) Access the **Authentication** module.
   a. In the left pane, expand **Modules**.



   b. Click **Authentication**.
3) In **UAS Administration**, in the **Identity providers** section, select **OpenID**.



4) Click **Create**.
5) In **OpenId Configuration**, to activate OpenId Identity Provider, select **Active** and enter the required information:
   - **Authority server url**
   - **Client Identifier**
   - **Client secret**



OpenId Configuration

General

☑ Active

Display name: oktaopenid

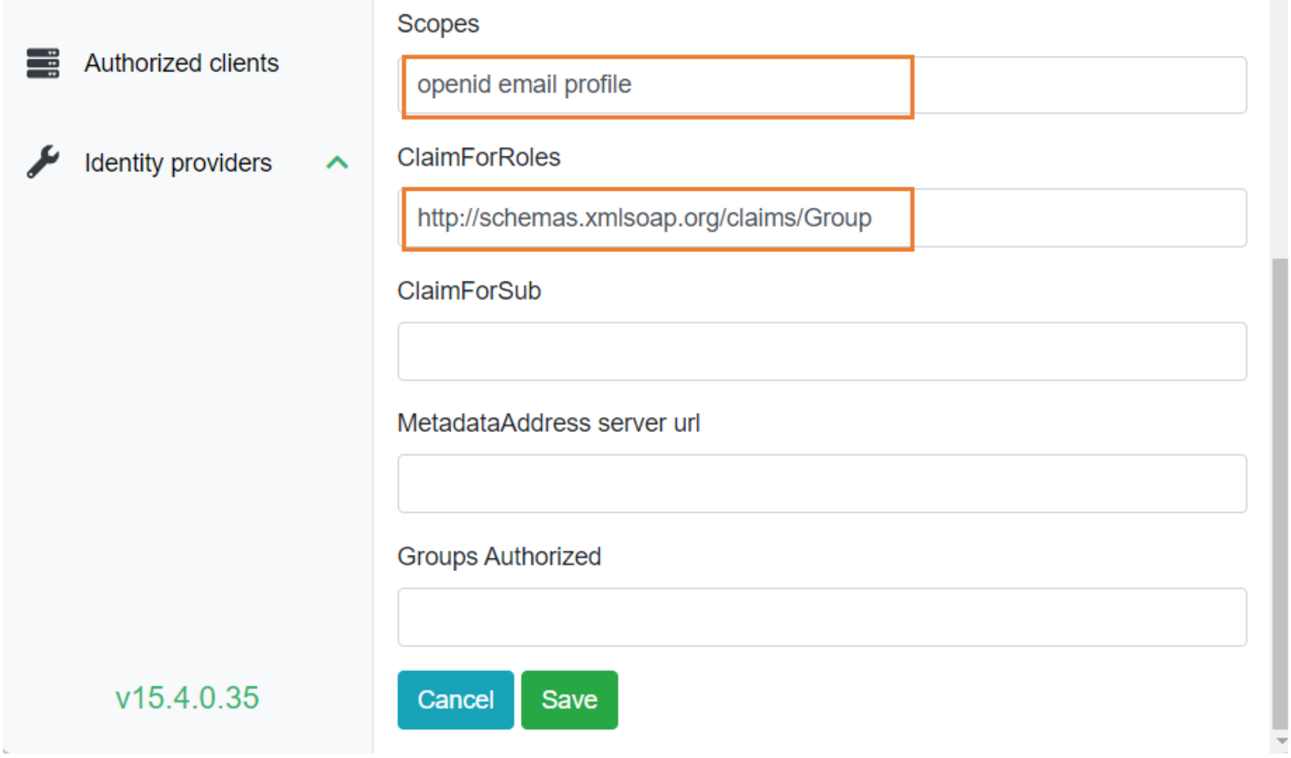
Authority server url: https://dev-27284285.okta.com/

Proxy url:

Client Identifier: 0oa3uzn4uzznPpkru5d7

Client secret: lBg1YMyBznWDxfAqcza8nvO5V[redacted]

RedirectURI: https://[redacted]/uas/signin-oktaopenid



Scopes: openid email profile

ClaimForRoles: http://schemas.xmlsoap.org/claims/Group

ClaimForSub:

MetadataAddress server url:

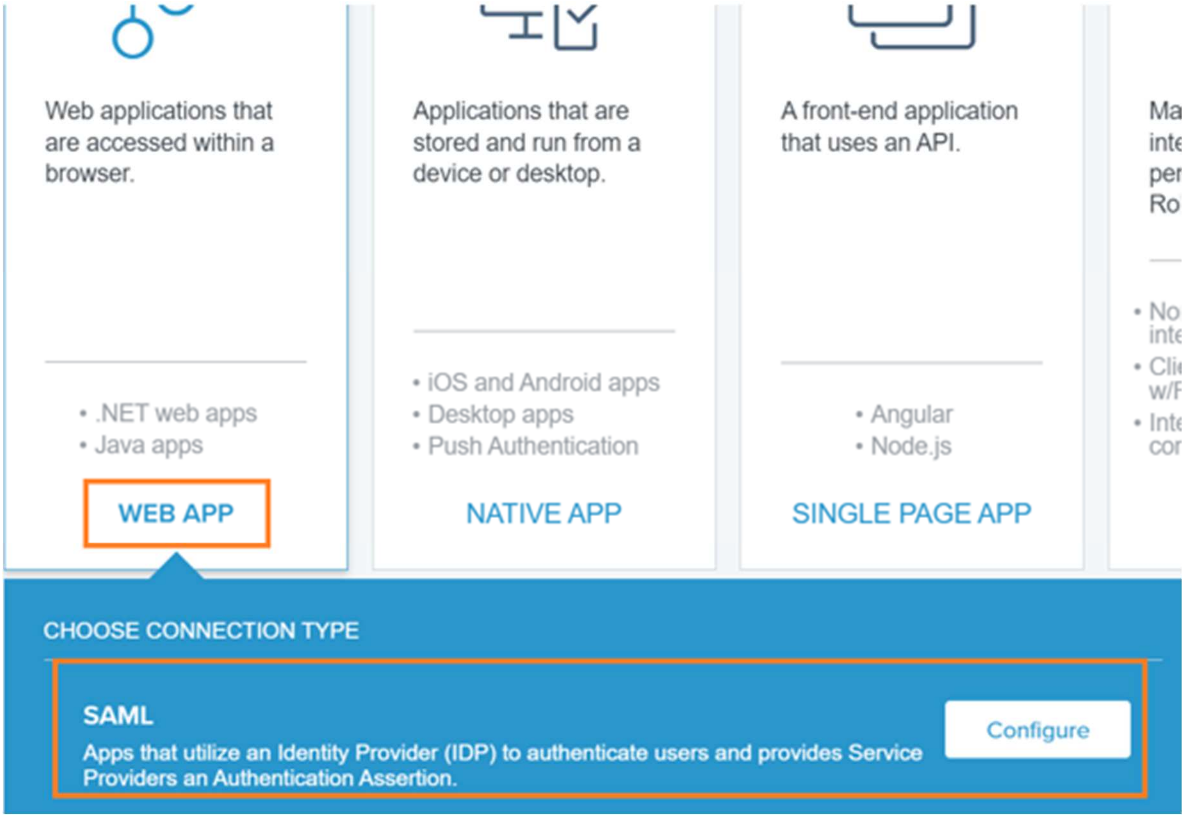
Groups Authorized:

3.3. Pingfederate Configuration with SAML2

3.3.1. Configuring Pingfederate application

To configure Pingfederate application:

1) Connect to your Pingfederate account.
2) Go to **Admin Portal > Applications**: create a Web application with SAML sign-in method:
   - **WEB APP**
   - **SAML**



Web applications that are accessed within a browser.

- .NET web apps
- Java apps

WEB APP

Applications that are stored and run from a device or desktop.

- iOS and Android apps
- Desktop apps
- Push Authentication

NATIVE APP

A front-end application that uses an API.

- Angular
- Node.js

SINGLE PAGE APP

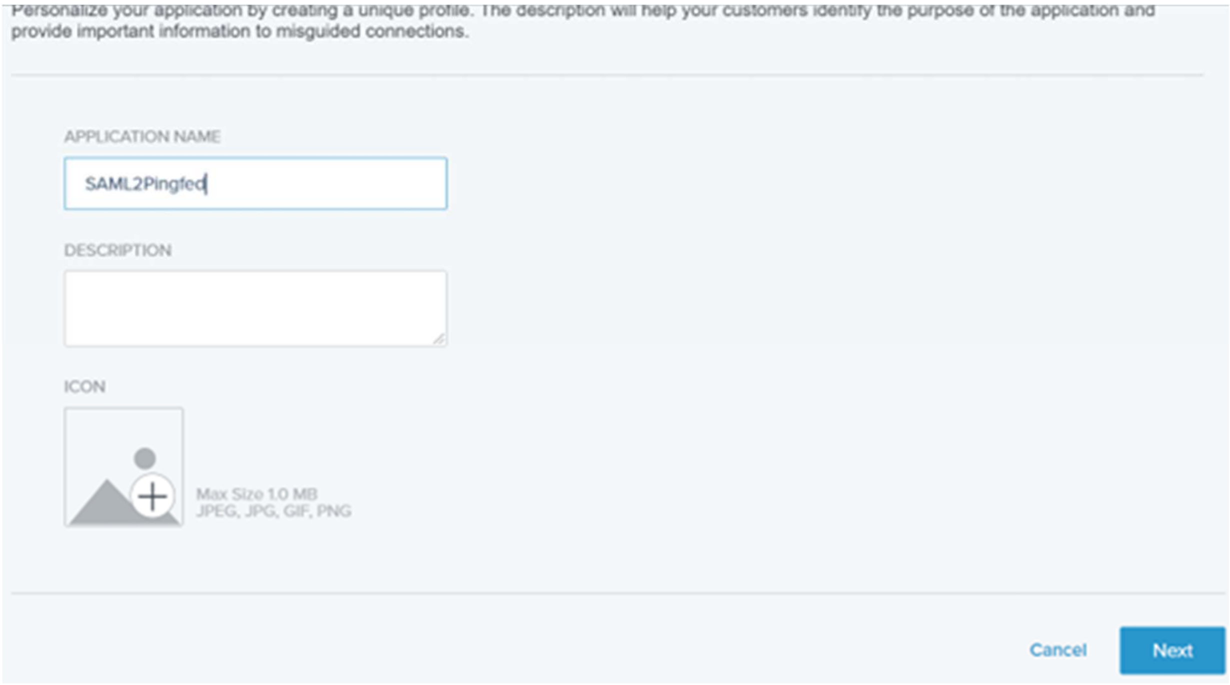
CHOOSE CONNECTION TYPE

SAML

Apps that utilize an Identity Provider (IDP) to authenticate users and provides Service Providers an Authentication Assertion.

3) Click **Configure**.
4) Enter the **Application name**.

```
Example: SAML2Pingfed
```



Personalize your application by creating a unique profile. The description will help your customers identify the purpose of the application and provide important information to misguided connections.

APPLICATION NAME

SAML2Pingfed

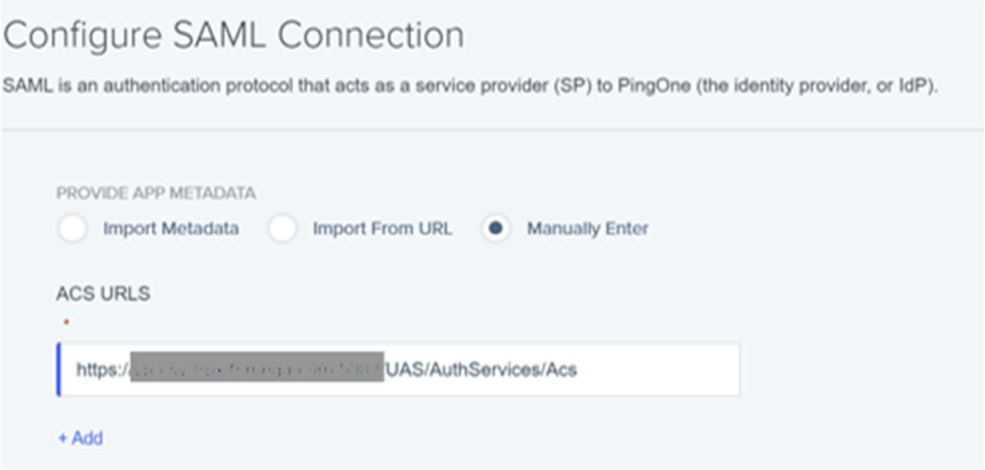
DESCRIPTION

ICON

Max Size 1.0 MB
JPEG, JPG, GIF, PNG

5) Click **Next**.

6) **Configure SAML Connection** as follows:



Configure SAML Connection

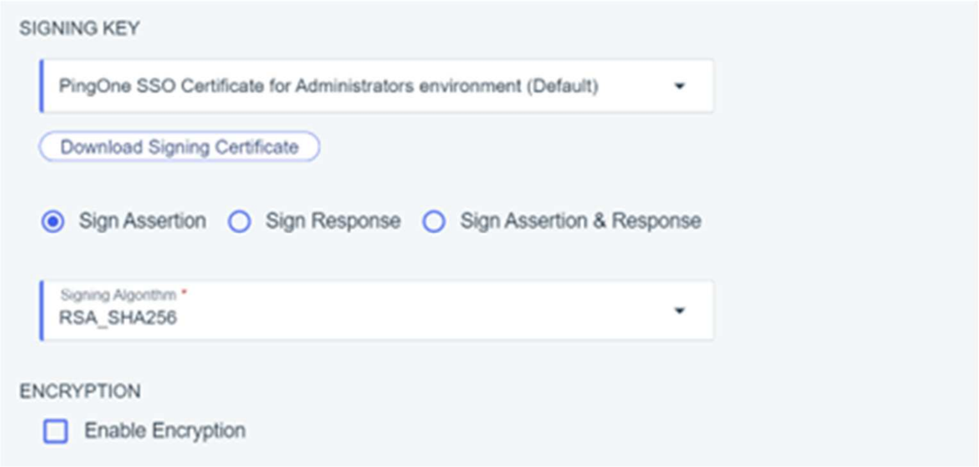
SAML is an authentication protocol that acts as a service provider (SP) to PingOne (the identity provider, or IdP).

PROVIDE APP METADATA

○ Import Metadata ○ Import From URL ● Manually Enter

ACS URLS

https:/[redacted]UAS/AuthServices/Acs



SIGNING KEY

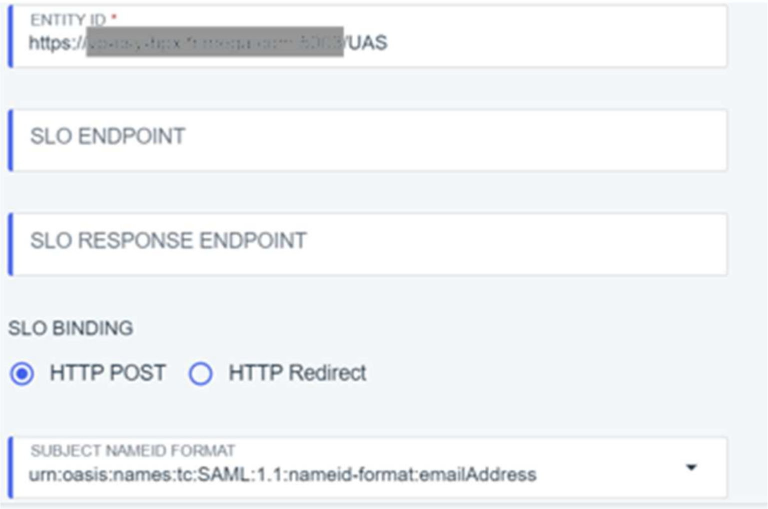
PingOne SSO Certificate for Administrators environment (Default)

● Sign Assertion ○ Sign Response ○ Sign Assertion & Response

Signing Algorithm *
RSA_SHA256

ENCRYPTION

□ Enable Encryption



ENTITY ID *
https://[redacted]/UAS

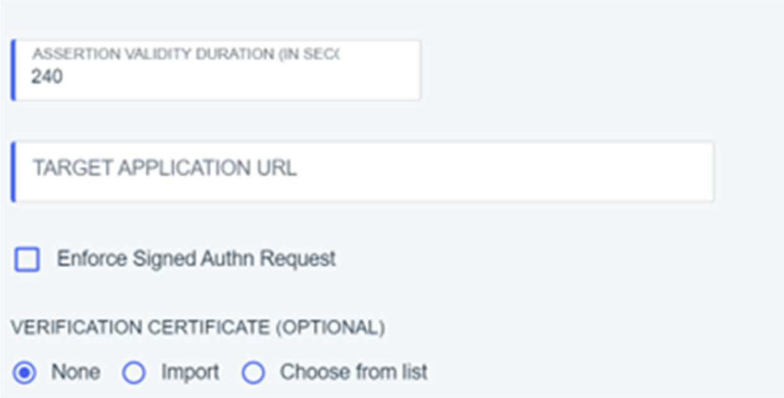
SLO ENDPOINT

SLO RESPONSE ENDPOINT

SLO BINDING

● HTTP POST ○ HTTP Redirect

SUBJECT NAMEID FORMAT
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress



ASSERTION VALIDITY DURATION (IN SEC(
240

TARGET APPLICATION URL

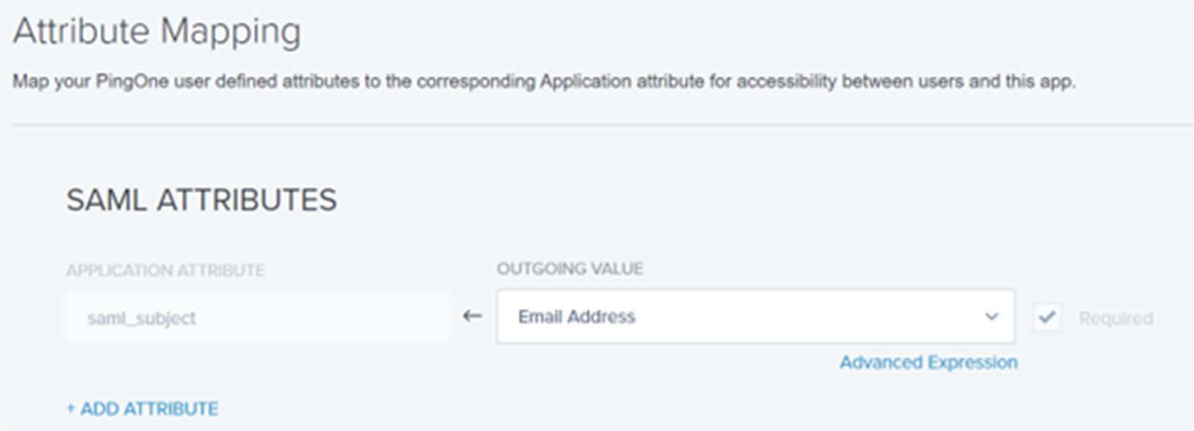
□ Enforce Signed Authn Request

VERIFICATION CERTIFICATE (OPTIONAL)

● None ○ Import ○ Choose from list

7) Click **Save and Continue**.

8) In **SAML ATTRIBUTES**, add an attribute statement “sub” and select “Email Address” as **Outgoing value**.



Attribute Mapping

Map your PingOne user defined attributes to the corresponding Application attribute for accessibility between users and this app.

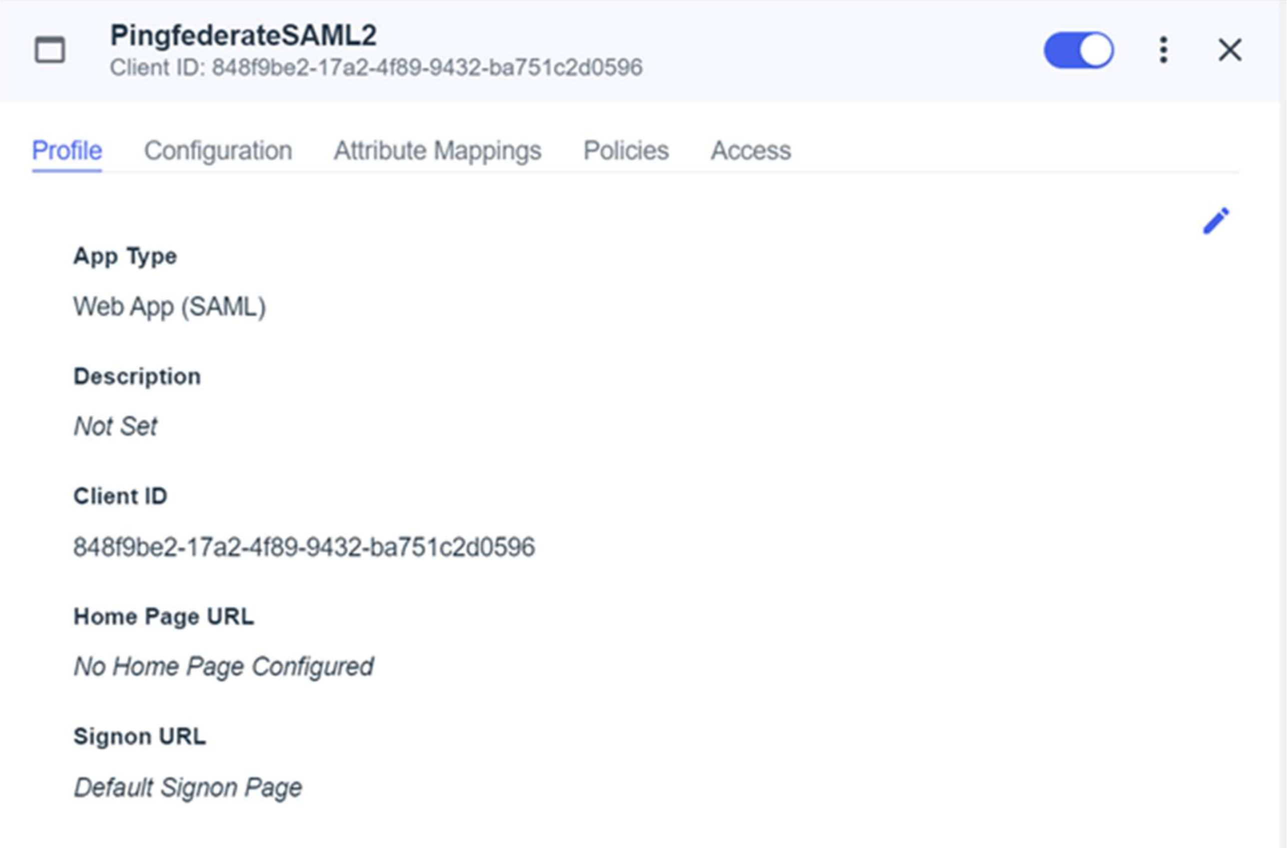
SAML ATTRIBUTES

APPLICATION ATTRIBUTE		OUTGOING VALUE	
saml_subject	←	Email Address	✓ Required

9) Click **Save and Close**.

10) Write down the following information carefully as you will need it for UAS configuration:

- **Client ID**



PingfederateSAML2

Client ID: 848f9be2-17a2-4f89-9432-ba751c2d0596

App Type

Web App (SAML)

Description

Not Set

Client ID

848f9be2-17a2-4f89-9432-ba751c2d0596

Home Page URL

No Home Page Configured

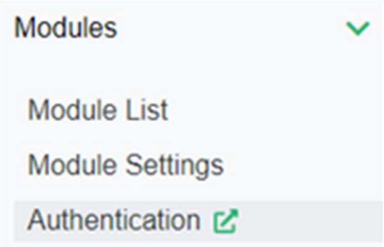
Signon URL

Default Signon Page

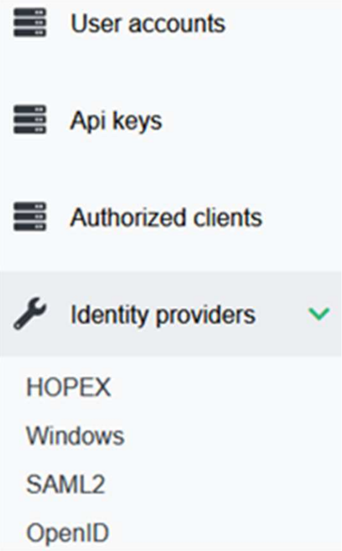
3.3.2. Configuring UAS with Pingfederate

To configure UAS with Pingfederate:

1) Connect to **HAS** console.
2) Access the **Authentication** module.
   a. In the left pane, expand **Modules**.



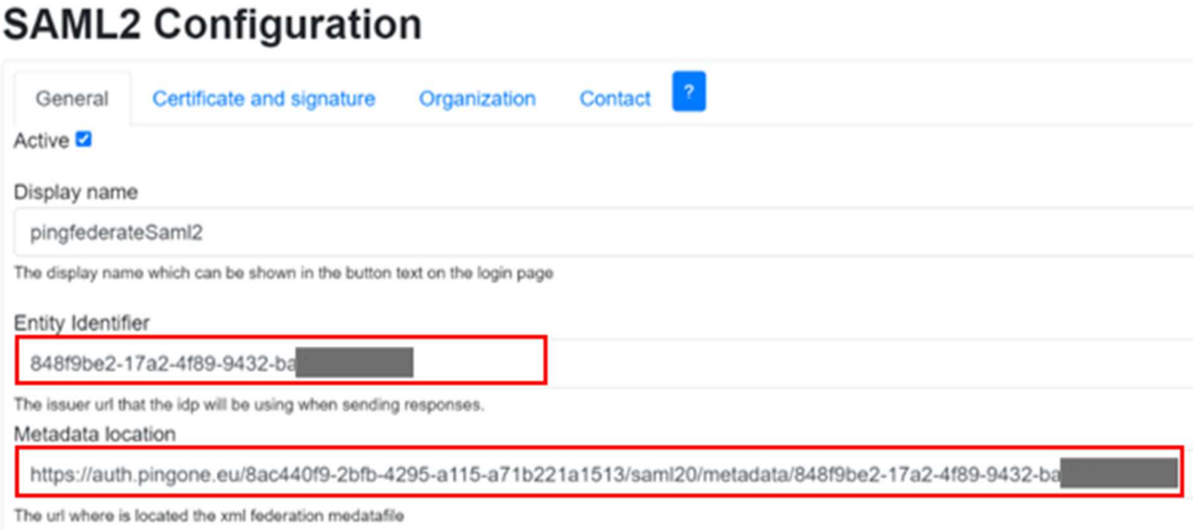
   b. Click **Authentication**.
3) In **UAS Administration**, in the **Identity providers** section, select **SAML2**.



4) Click **Create**.

5) In SAML2 Configuration, to activate SAML2 Identity Provider, select **Active** and enter the required information:

- **Entity Identifier**
- **Metadata location**



SAML2 Configuration

Active ☑

Display name

pingfederateSaml2

The display name which can be shown in the button text on the login page

Entity Identifier

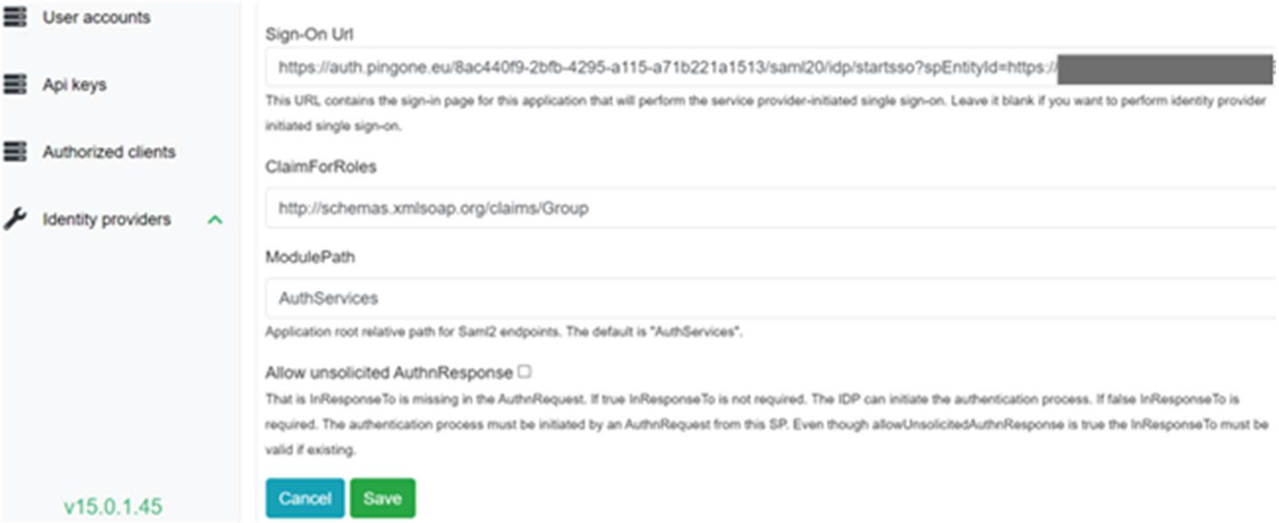
848f9be2-17a2-4f89-9432-ba[redacted]

The issuer url that the idp will be using when sending responses.

Metadata location

https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/saml20/metadata/848f9be2-17a2-4f89-9432-ba[redacted]

The url where is located the xml federation medatafile



Sign-On Url

https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/saml20/idp/startsso?spEntityId=https://[redacted]

This URL contains the sign-in page for this application that will perform the service provider-initiated single sign-on. Leave it blank if you want to perform identity provider initiated single sign-on.

ClaimForRoles

http://schemas.xmlsoap.org/claims/Group

ModulePath

AuthServices

Application root relative path for Saml2 endpoints. The default is "AuthServices".

Allow unsolicited AuthnResponse □

That is InResponseTo is missing in the AuthnRequest. If true InResponseTo is not required. The IDP can initiate the authentication process. If false InResponseTo is required. The authentication process must be initiated by an AuthnRequest from this SP. Even though allowUnsolicitedAuthnResponse is true the InResponseTo must be valid if existing.

6) Click **Save**.

   To save and apply your changes, the instance and all related nodes need to be restarted. Any connected user will be disconnected.

7) **Click I understand the consequences, restart**.

3.4. Pingfederate Configuration with OpenID Connect

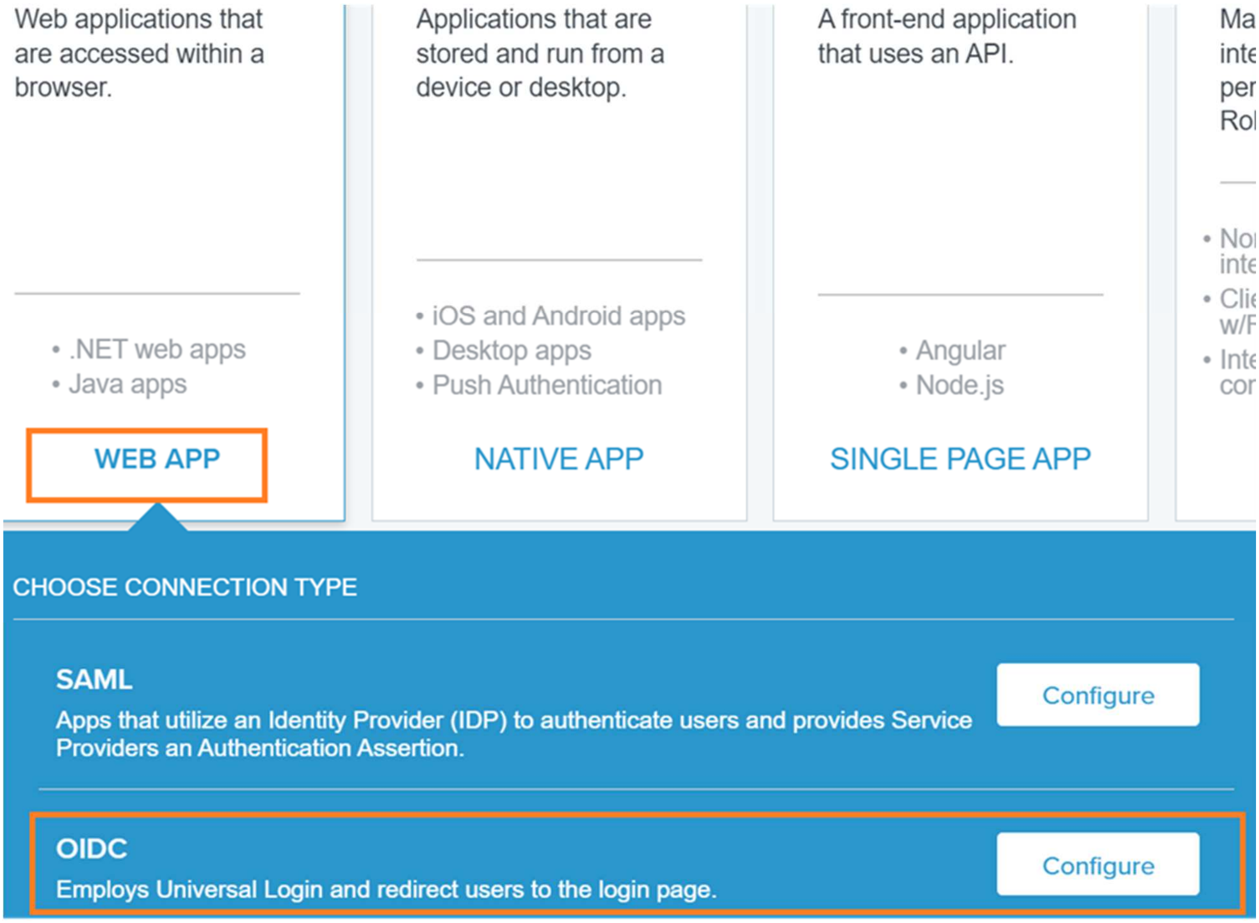
3.4.1. Configuring Pingfederate application with OpenID Connect

To configure Pingfederate application:

1) Connect to your Pingfederate account.

8) Go to **Admin Portal > Applications**: create a Web application with OIDC sign-in method:

   - **WEB APP**
   - **OIDC**



Web applications that are accessed within a browser.

- .NET web apps
- Java apps

WEB APP

Applications that are stored and run from a device or desktop.

- iOS and Android apps
- Desktop apps
- Push Authentication

NATIVE APP

A front-end application that uses an API.

- Angular
- Node.js

SINGLE PAGE APP

Ma inte per Rol

- Nor inte
- Clie w/F
- Inte cor

CHOOSE CONNECTION TYPE

SAML
Apps that utilize an Identity Provider (IDP) to authenticate users and provides Service Providers an Authentication Assertion.

Configure

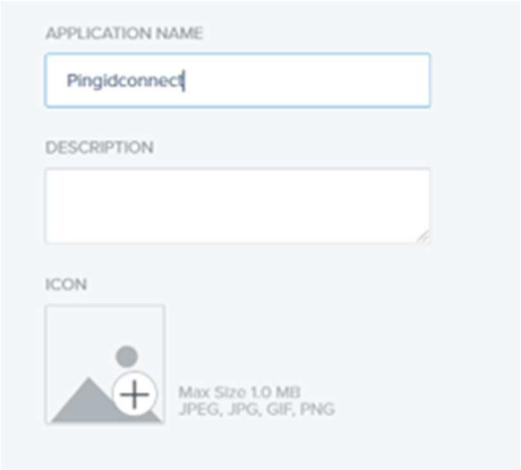
OIDC
Employs Universal Login and redirect users to the login page.

Configure

9) Click **Configure**.

10) Enter an **Application Name**.

```
Example: Pingidconnect
```



APPLICATION NAME: Pingidconnect

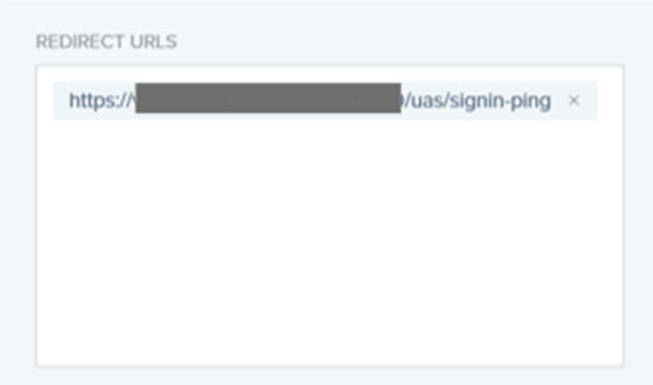
DESCRIPTION

ICON

11) Click **Next**.

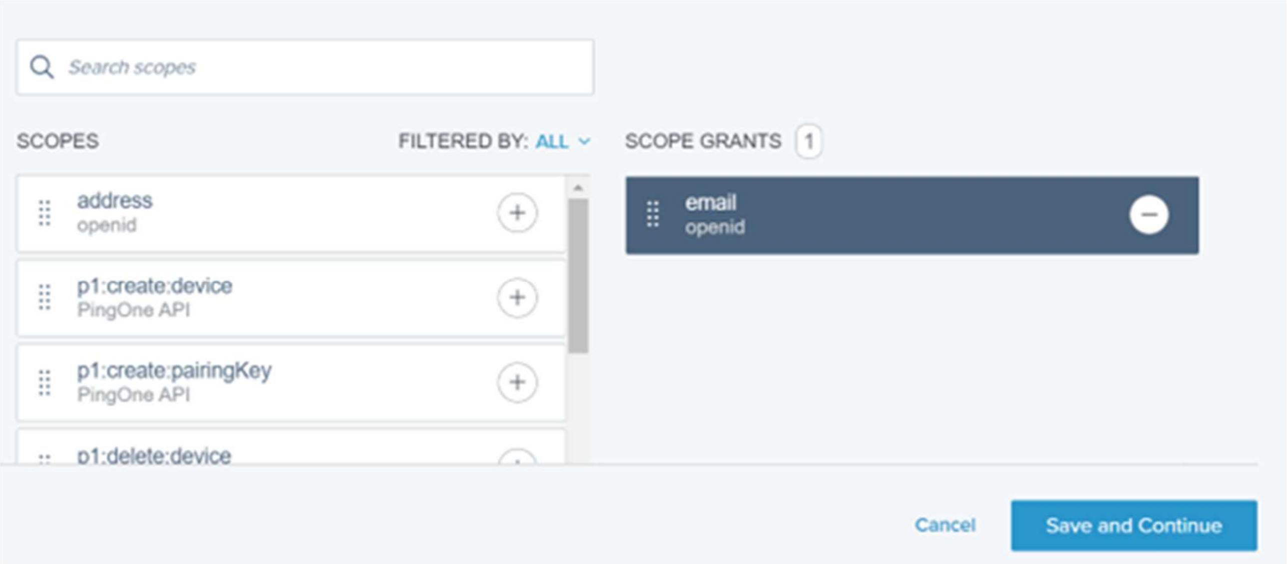
12) In **Redirect URLS** enter the URL in the following format:

Error! Hyperlink reference not valid. name>/uas/signin-ping

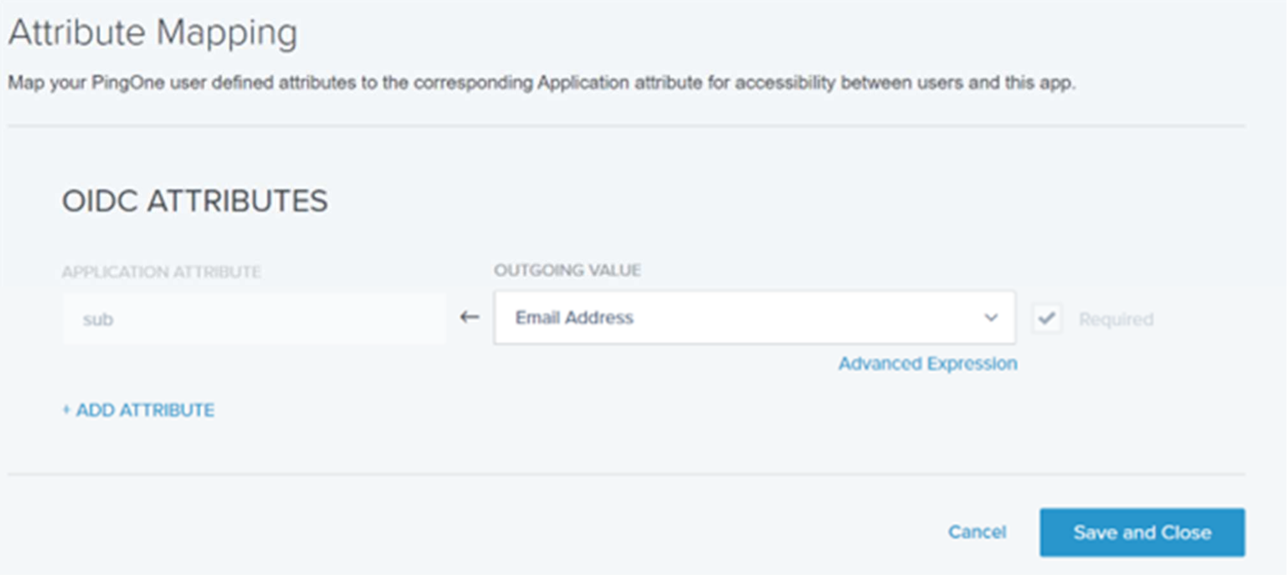


REDIRECT URLS

https://[redacted]/uas/signin-ping ×



13) Click **Save and Continue**.



Attribute Mapping

Map your PingOne user defined attributes to the corresponding Application attribute for accessibility between users and this app.

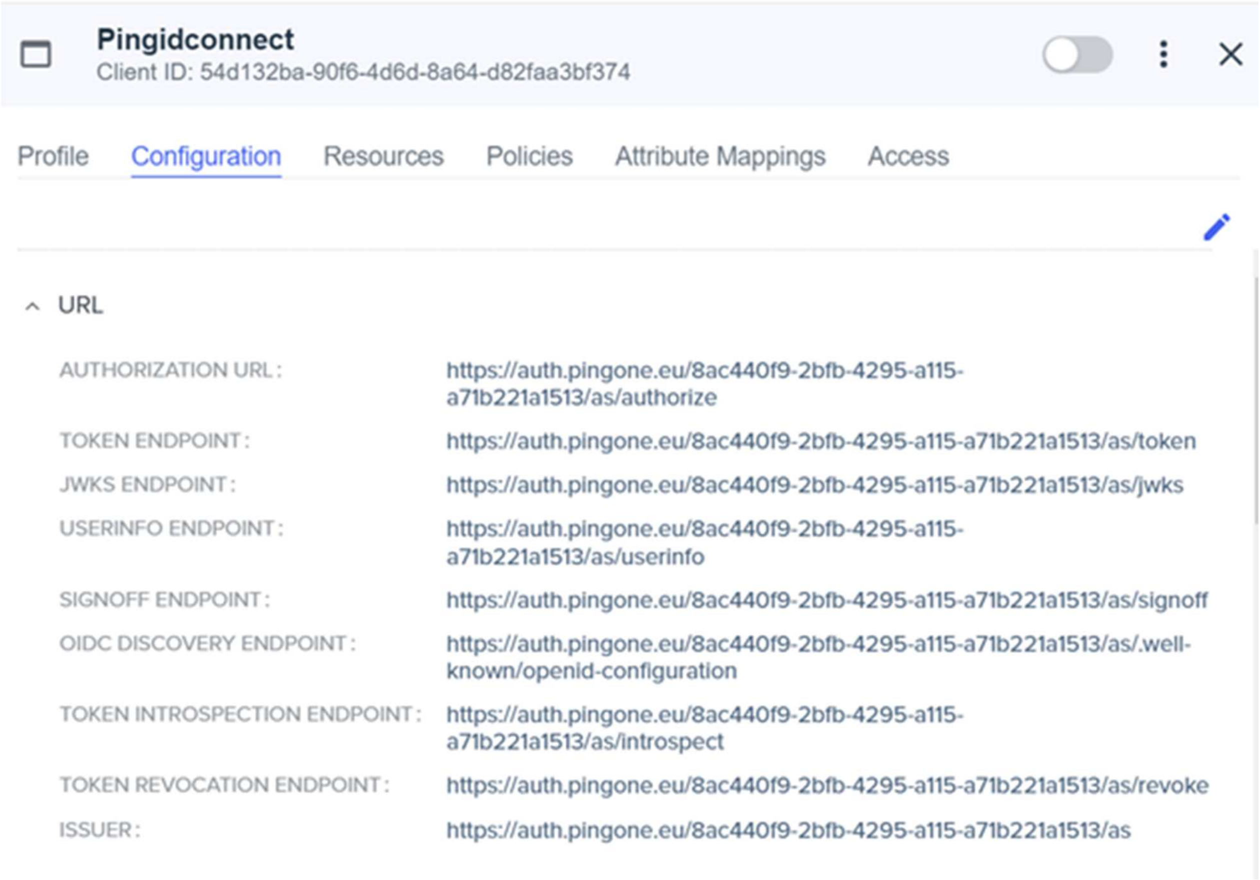
OIDC ATTRIBUTES

APPLICATION ATTRIBUTE		OUTGOING VALUE	
sub	←	Email Address	✓ Required

14) Click **Save and Close**.

15) Write down the following information carefully as you will need it for UAS configuration:

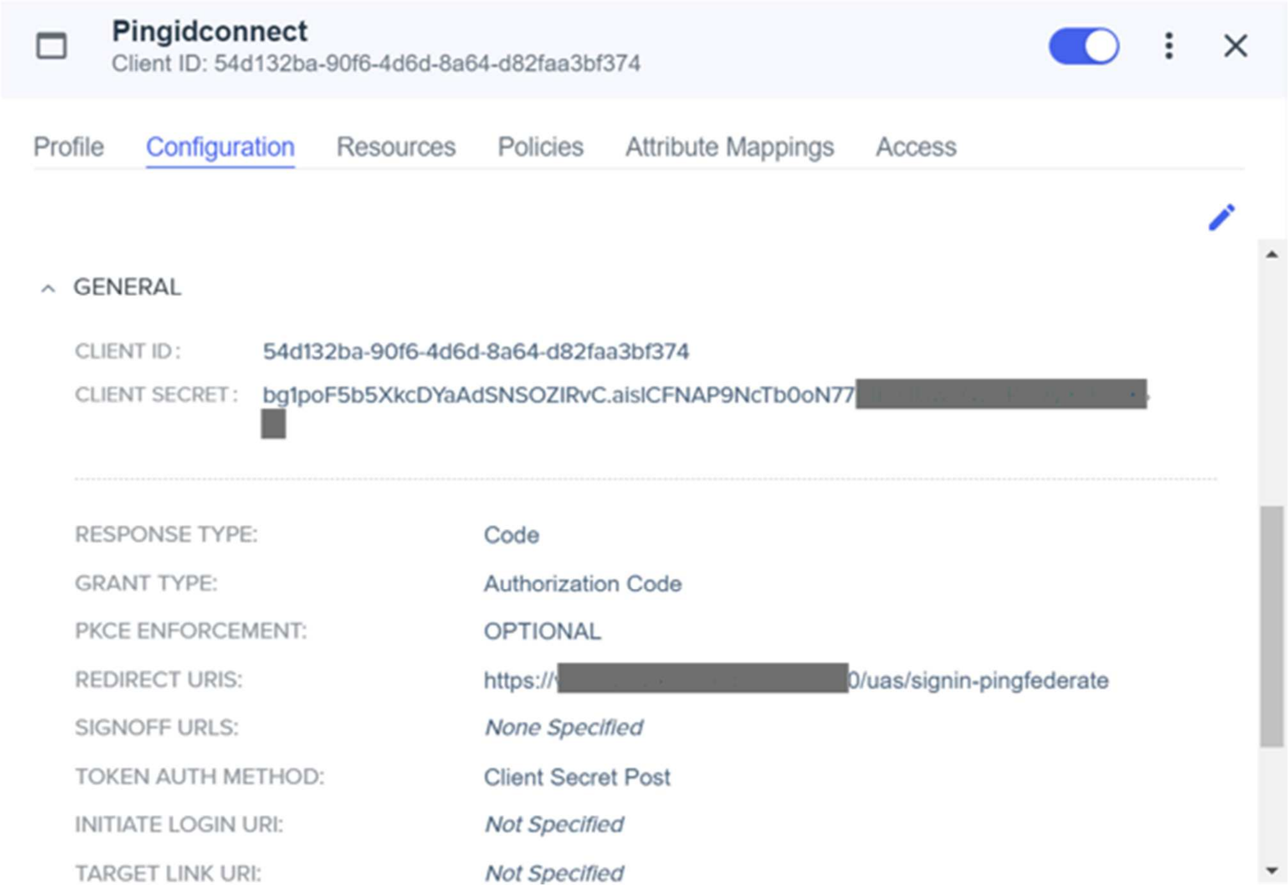
- **Client ID**
- **Client secret**



Pingidconnect
Client ID: 54d132ba-90f6-4d6d-8a64-d82faa3bf374

URL

AUTHORIZATION URL :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/authorize
TOKEN ENDPOINT :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/token
JWKS ENDPOINT :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/jwks
USERINFO ENDPOINT :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/userinfo
SIGNOFF ENDPOINT :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/signoff
OIDC DISCOVERY ENDPOINT :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/.well-known/openid-configuration
TOKEN INTROSPECTION ENDPOINT :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/introspect
TOKEN REVOCATION ENDPOINT :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as/revoke
ISSUER :	https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as



Pingidconnect
Client ID: 54d132ba-90f6-4d6d-8a64-d82faa3bf374

GENERAL

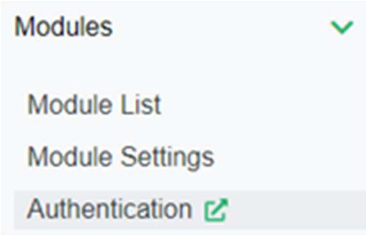
CLIENT ID :	54d132ba-90f6-4d6d-8a64-d82faa3bf374
CLIENT SECRET :	bg1poF5b5XkcDYaAdSNSOZIRvC.aisICFNAP9NcTb0oN77[redacted]

RESPONSE TYPE:	Code
GRANT TYPE:	Authorization Code
PKCE ENFORCEMENT:	OPTIONAL
REDIRECT URIS:	https://[redacted]0/uas/signin-pingfederate
SIGNOFF URLS:	*None Specified*
TOKEN AUTH METHOD:	Client Secret Post
INITIATE LOGIN URI:	*Not Specified*
TARGET LINK URI:	*Not Specified*

3.4.2. Configuring UAS with Pingfederate

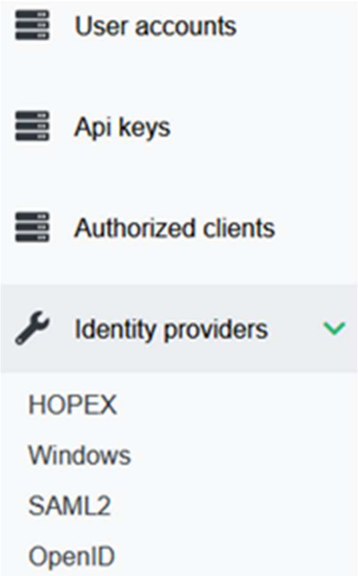
To configure UAS with OKTA:

1) Connect to **HAS** console.
2) Access the **Authentication** module.
    a. In the left pane, expand **Modules**.

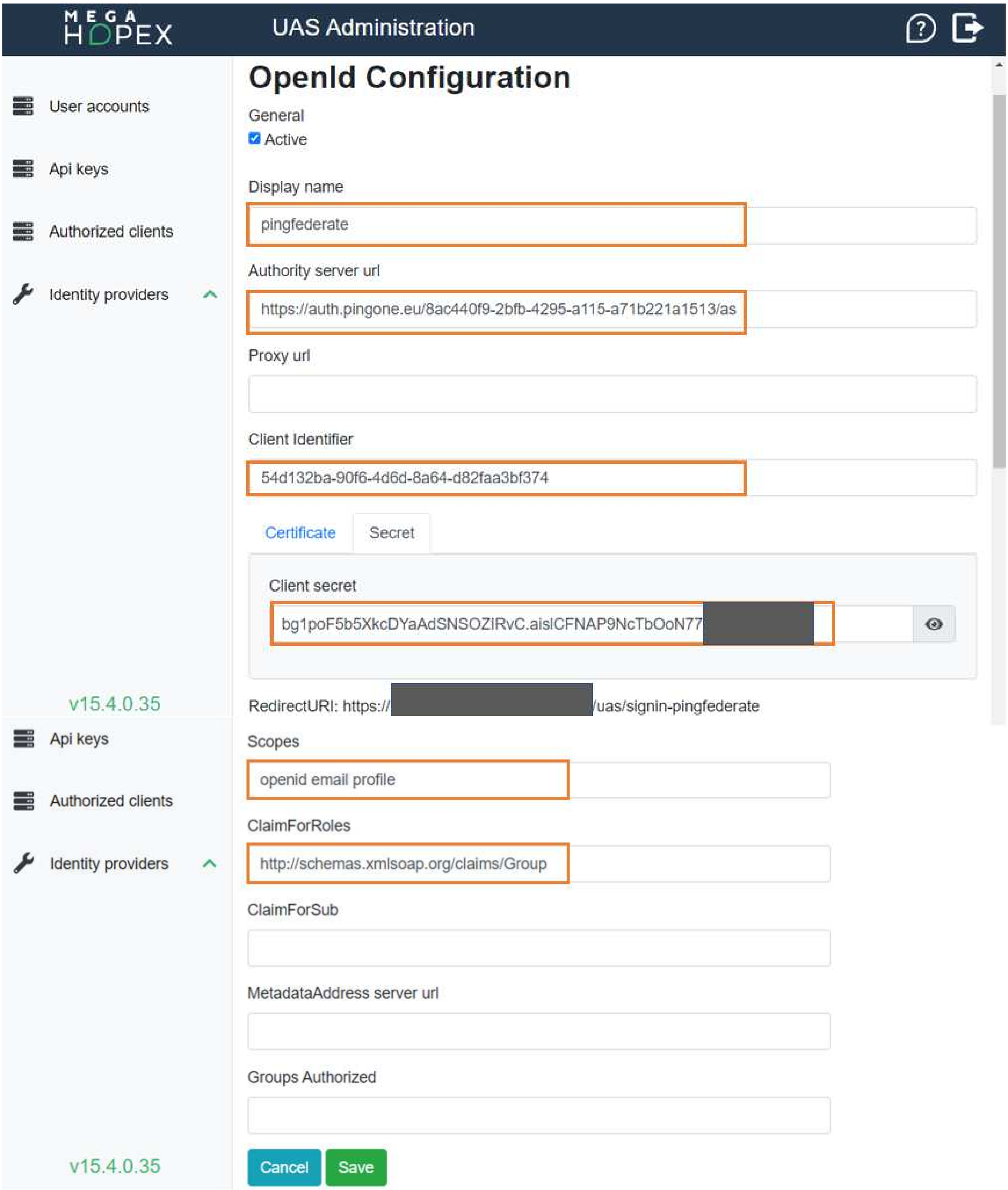


    b. Click **Authentication**.

3) In **UAS Administration**, in the **Identity providers** section, select **SAML2**.



4) Click **Create**.
5) In **OpenId Configuration**, to activate OpenId Identity Provider, select **Active** and enter the required information:
    - **Authority server url**
    - **Client Identifier**
    - **Client secret**



OpenId Configuration

General

☑ Active

Display name: pingfederate

Authority server url: https://auth.pingone.eu/8ac440f9-2bfb-4295-a115-a71b221a1513/as

Proxy url:

Client Identifier: 54d132ba-90f6-4d6d-8a64-d82faa3bf374

Certificate | Secret

Client secret: bg1poF5b5XkcDYaAdSNSOZIRvC.aislCFNAP9NcTbOoN77[redacted]

RedirectURI: https://[redacted]/uas/signin-pingfederate

Scopes: openid email profile

ClaimForRoles: http://schemas.xmlsoap.org/claims/Group

ClaimForSub:

MetadataAddress server url:

Groups Authorized:

Cancel | Save

6) Click **Save**.

3.5. Azure AD Configuration with SAML2

3.5.1. Configuring Azure AD application

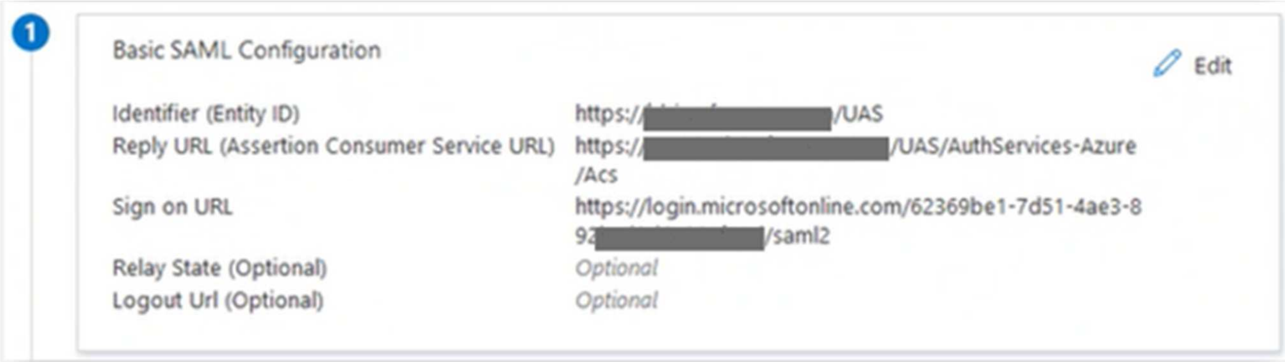
→ Follow Microsoft documentation for detailed configuration: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-setup-sso.

To configure Azure AD application:

1) Connect to your Azure AD account.
2) In **Enterprise applications** create an application (e.g.: “Azure AD SAML Toolkit”).
3) Access the SAML SSO configuration page (e.g.: in the **Manage** section > **Single Sign-On** page > **SAML**)
4) Configure the Azure AD application as follows:

In **Basic SAML Configuration**:

- **Reply URL (Assertion Consumer Service URL)** enter the reply URL in the following format: https://<server name>/UAS/AuthServices-Azure/Acs

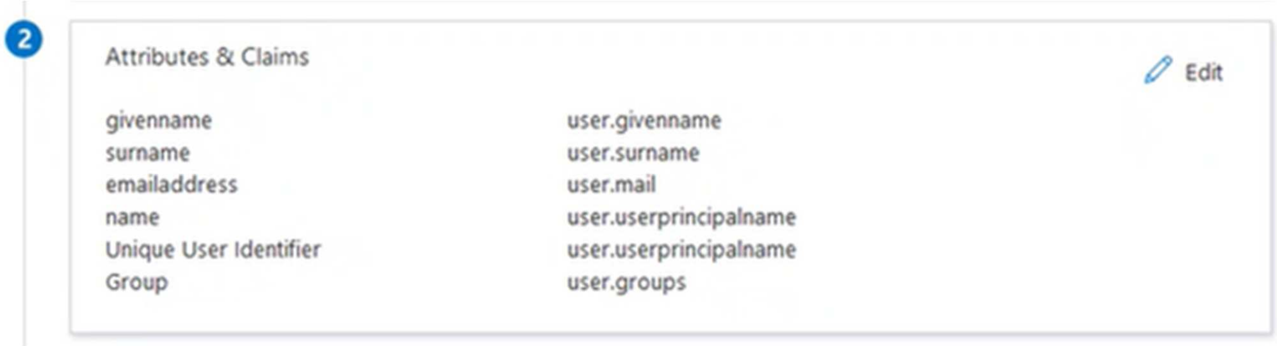


Basic SAML Configuration

Identifier (Entity ID)	https://[redacted]/UAS
Reply URL (Assertion Consumer Service URL)	https://[redacted]/UAS/AuthServices-Azure/Acs
Sign on URL	https://login.microsoftonline.com/62369be1-7d51-4ae3-8 92[redacted]/saml2
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

In **Attributes & Claims**, configure at least one attribute and claim.

```
Example: emailaddress   user.mail
```

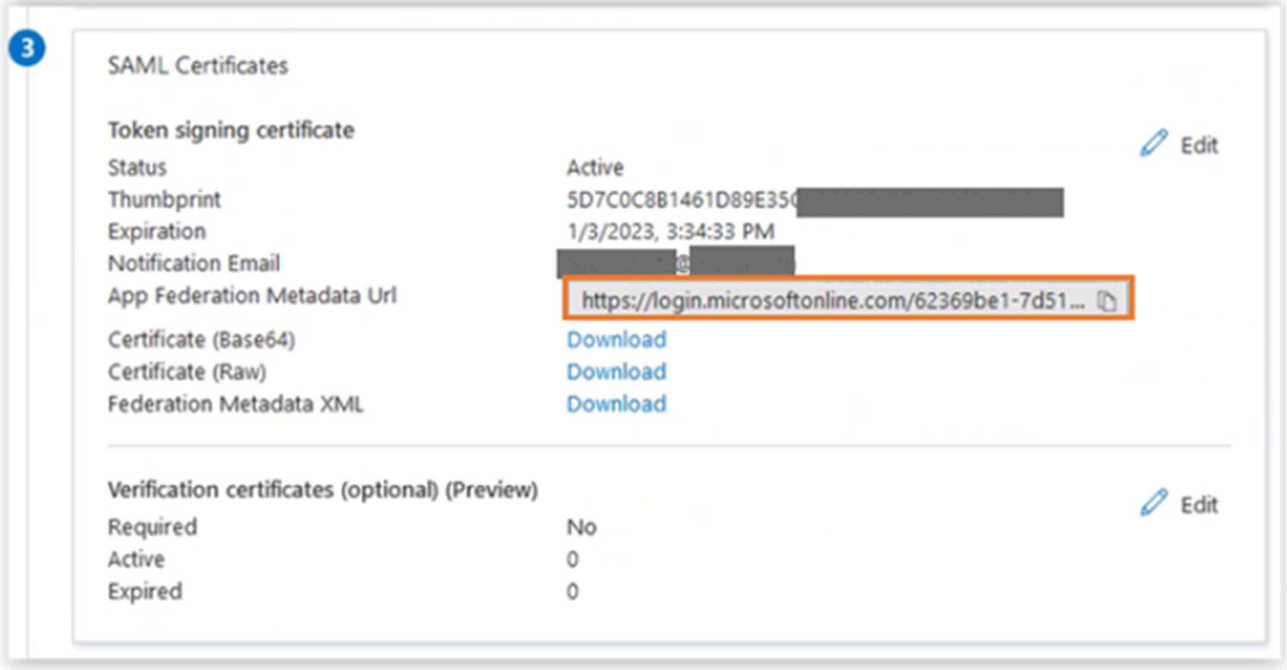


Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

In **SAML Certificates**, write down the following information carefully as you will need it for UAS configuration:

- **App Federation Metadata Url**



3

SAML Certificates

Token signing certificate

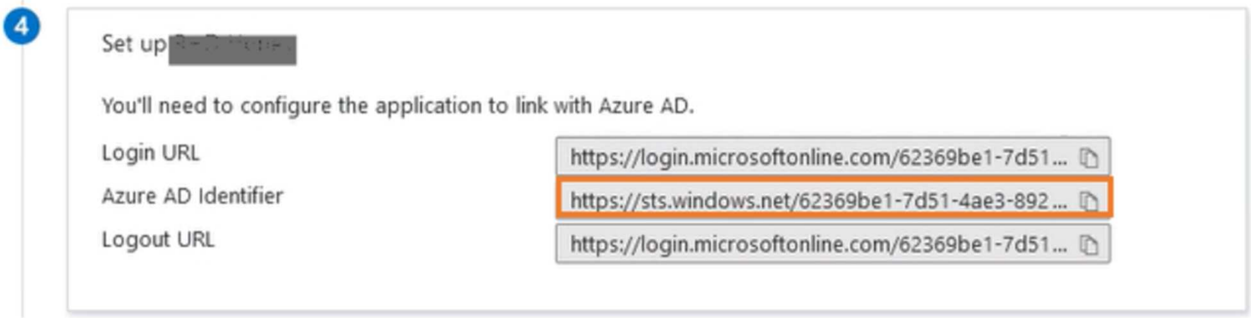
Status	Active
Thumbprint	5D7C0C8B1461D89E35[redacted]
Expiration	1/3/2023, 3:34:33 PM
Notification Email	[redacted]@[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/62369be1-7d51...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) (Preview)

Required	No
Active	0
Expired	0

In **Set up <application name>**, write down the following information carefully as you will need it for UAS configuration:

- **Azure AD identifier**



4

Set up [redacted]

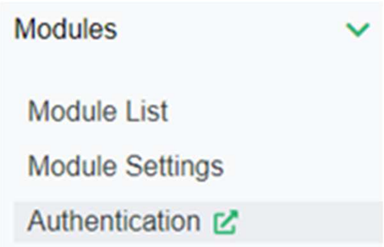
You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/62369be1-7d51...
Azure AD Identifier	https://sts.windows.net/62369be1-7d51-4ae3-892...
Logout URL	https://login.microsoftonline.com/62369be1-7d51...

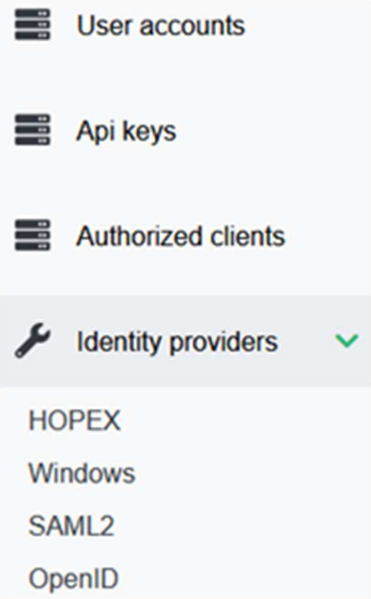
3.5.2. Configuring UAS with Azure AD

To configure UAS with Azure AD:

1) Connect to **HAS** console.
2) Access the **Authentication** module.
   a. In the left pane, expand **Modules**.



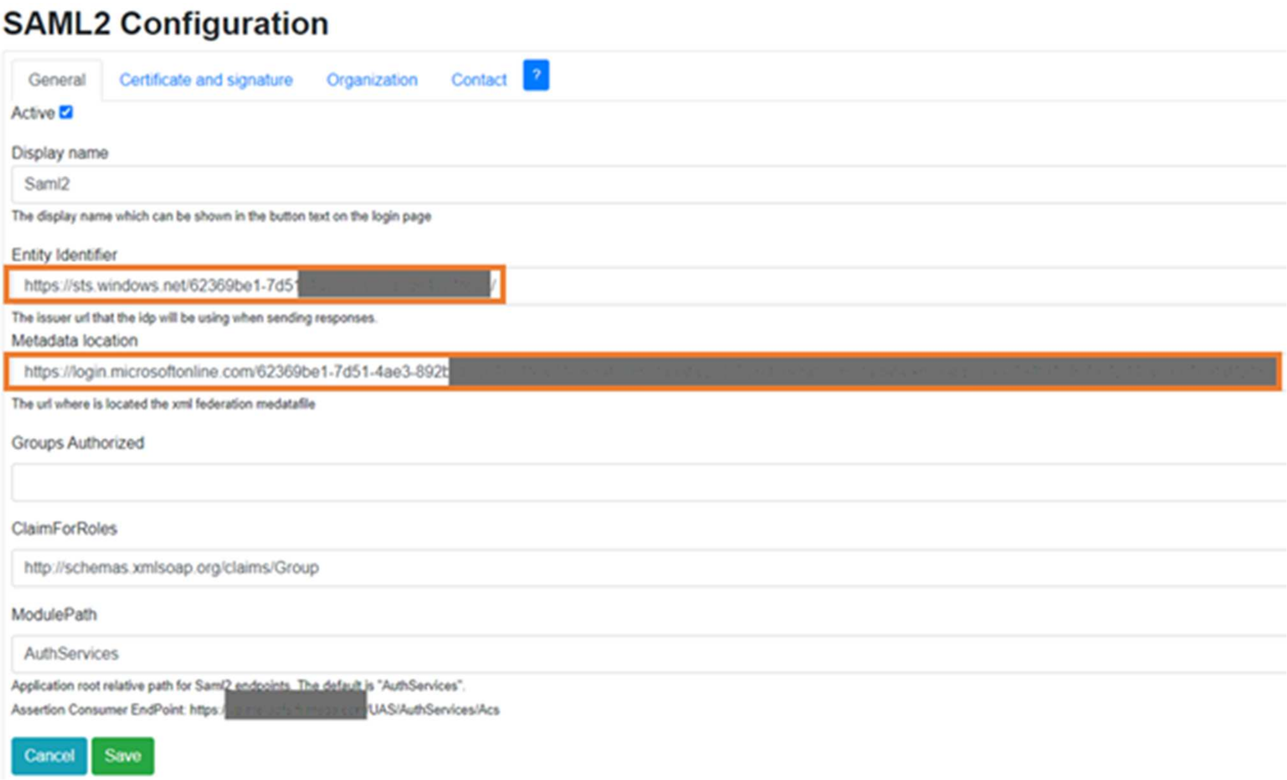
   b. Click **Authentication**.
3) In **UAS Administration**, in the **Identity providers** section, select **SAML2**.



4) Click **Create**.

5) In SAML2 Configuration, to activate SAML2 Identity Provider, select **Active** and enter the required information:

- **Entity Identifier**
- **Metadata location**



SAML2 Configuration

General | Certificate and signature | Organization | Contact | ?

Active ☑

Display name

Saml2

The display name which can be shown in the button text on the login page

Entity Identifier

https://sts.windows.net/62369be1-7d5[redacted]/

The issuer url that the idp will be using when sending responses.

Metadata location

https://login.microsoftonline.com/62369be1-7d51-4ae3-892b[redacted]

The url where is located the xml federation medatafile

Groups Authorized

ClaimForRoles

http://schemas.xmlsoap.org/claims/Group

ModulePath

AuthServices

Application root relative path for Saml2 endpoints. The default is "AuthServices".

Assertion Consumer EndPoint: https:/[redacted]/UAS/AuthServices/Acs

Cancel | Save

3.6. Azure AD Configuration with OpenID Connect

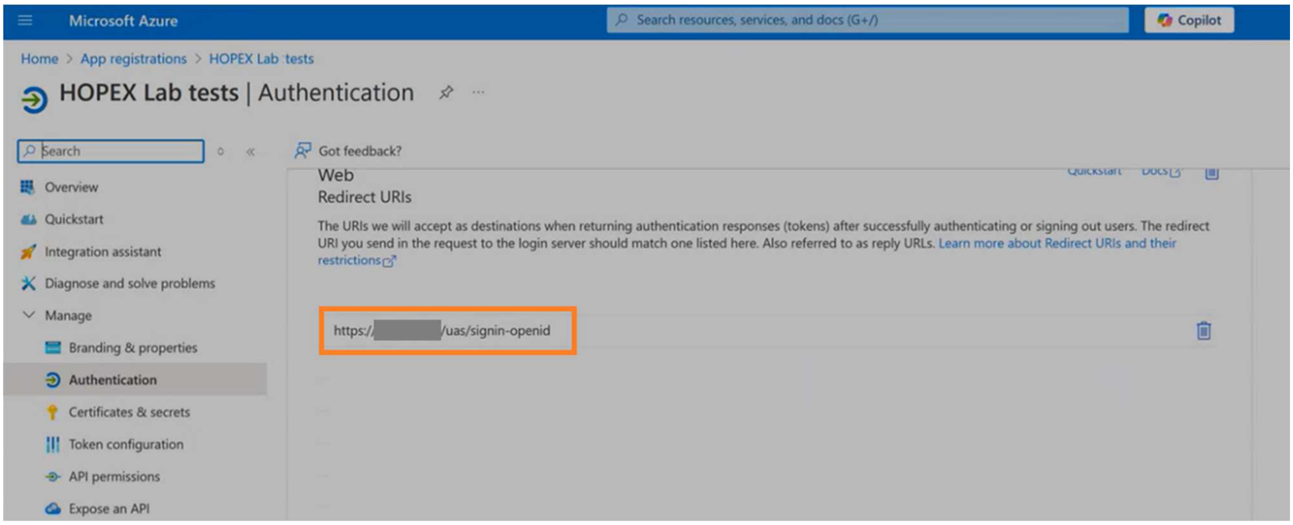
3.6.1. Configuring Azure AD application

➔ Follow Microsoft documentation for detailed configuration: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/add-application-portal-setup-oidc-sso.

To configure Azure AD application:

1) Connect to your Microsoft Entra admin center.
2) Browse to **Identity** > **Applications** > **App registrations** and select **New registration**.
3) Enter the required information and select **Register** to complete the initial app registration.
4) Navigate to **Identity** > **Applications** > **Enterprise applications** and select the app you created.
5) Configure it as follows:

   In **App registrations** > **Authentication**, enter the redirect URL from UAS Administration.



Web

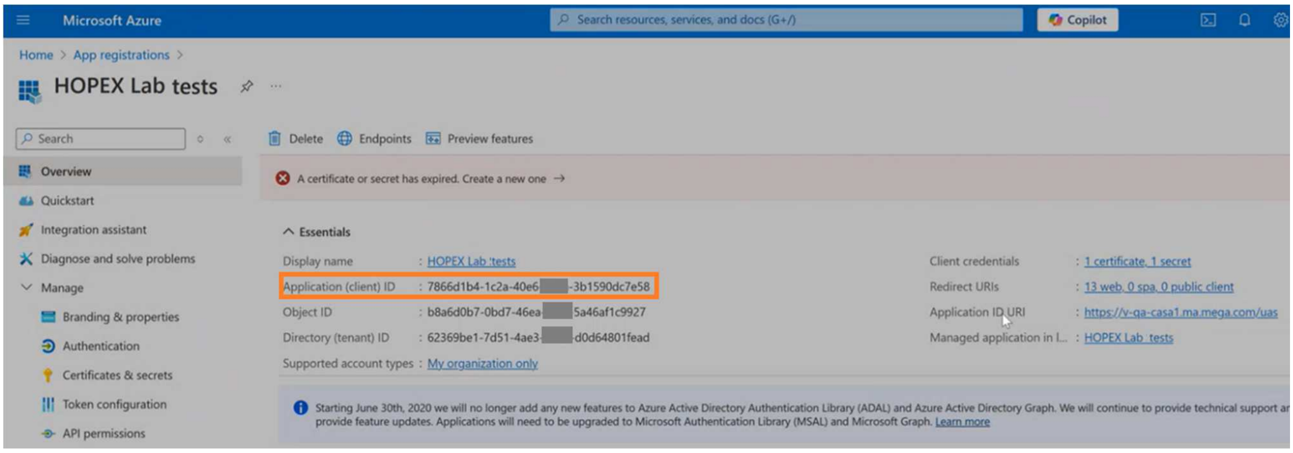
Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

https://[redacted]/uas/signin-openid

In **Overview**, write down the following information carefully as you will need it for UAS configuration:

- Application (client) ID



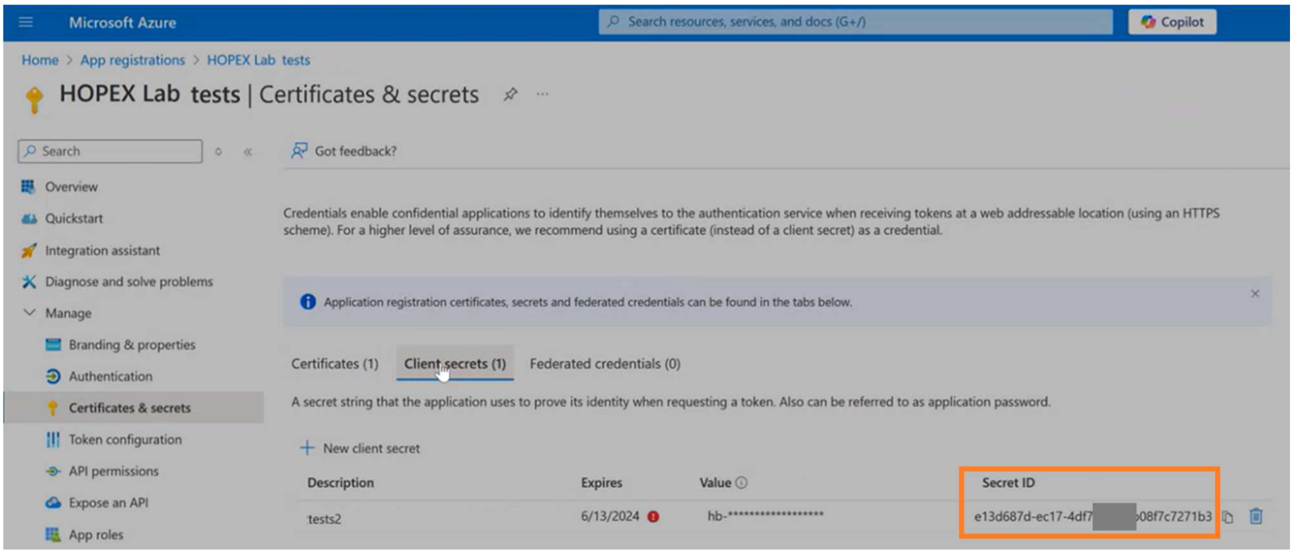
A certificate or secret has expired. Create a new one →

Display name	: HOPEX Lab tests	Client credentials	: 1 certificate, 1 secret
Application (client) ID	: 7866d1b4-1c2a-40e6[redacted]-3b1590dc7e58	Redirect URIs	: 13 web, 0 spa, 0 public client
Object ID	: b8a6d0b7-0bd7-46ea[redacted]5a46af1c9927	Application ID URI	: https://v-qa-casa1.ma.mega.com/uas
Directory (tenant) ID	: 62369be1-7d51-4ae3[redacted]d0d64801fead	Managed application in l...	: HOPEX Lab tests
Supported account types	: My organization only		

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support ar provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

In **Certificates & secrets**, write down the following information carefully as you will need it for UAS configuration:

- Either copy the Certificate ID or the Secret ID.



HOPEX Lab tests | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

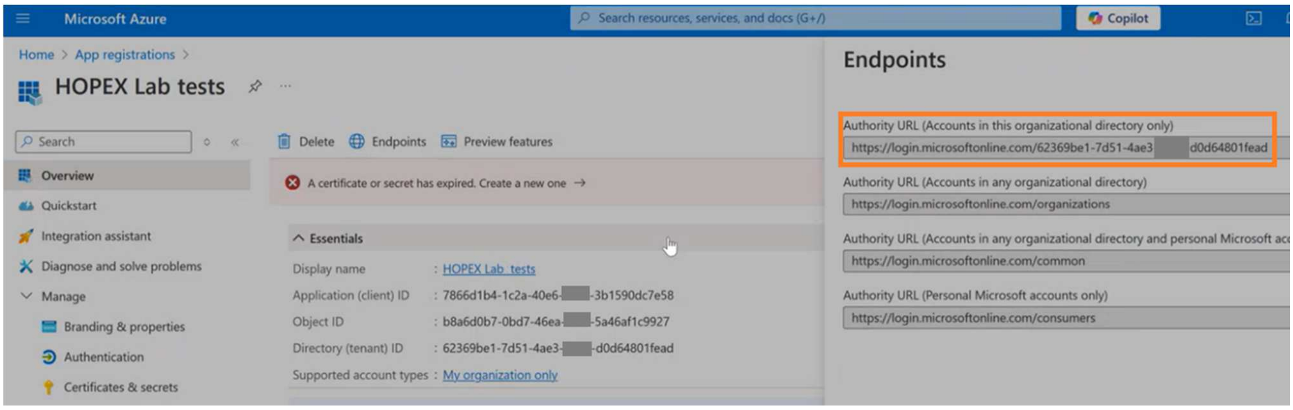
Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
tests2	6/13/2024	hb-******************	e13d687d-ec17-4df7[redacted]08f7c7271b3

In **Overview > Endpoints**, write down the following information carefully as you will need it for UAS configuration:

- Authority URL



HOPEX Lab tests

A certificate or secret has expired. Create a new one →

Display name : HOPEX Lab tests
Application (client) ID : 7866d1b4-1c2a-40e6-[redacted]-3b1590dc7e58
Object ID : b8a6d0b7-0bd7-46ea-[redacted]-5a46af1c9927
Directory (tenant) ID : 62369be1-7d51-4ae3-[redacted]-d0d64801fead
Supported account types : My organization only

Endpoints

Authority URL (Accounts in this organizational directory only)
https://login.microsoftonline.com/62369be1-7d51-4ae3[redacted]d0d64801fead

Authority URL (Accounts in any organizational directory)
https://login.microsoftonline.com/organizations

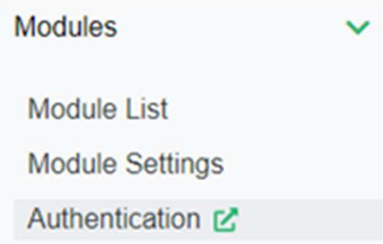
Authority URL (Accounts in any organizational directory and personal Microsoft ac
https://login.microsoftonline.com/common

Authority URL (Personal Microsoft accounts only)
https://login.microsoftonline.com/consumers

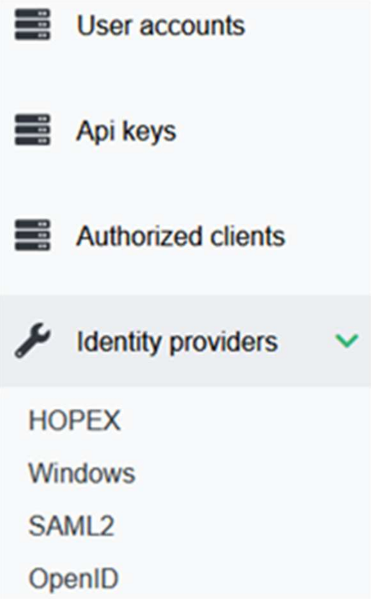
3.6.2. Configuring UAS with Azure AD

To configure UAS with Azure AD:

1) Connect to **HAS** console.
2) Access the **Authentication** module.
   - In the left pane, expand **Modules**.



   - Click **Authentication**.
3) In **UAS Administration**, in the **Identity providers** section, select **OpenID**.



User accounts

Api keys

Authorized clients

Identity providers

HOPEX

Windows

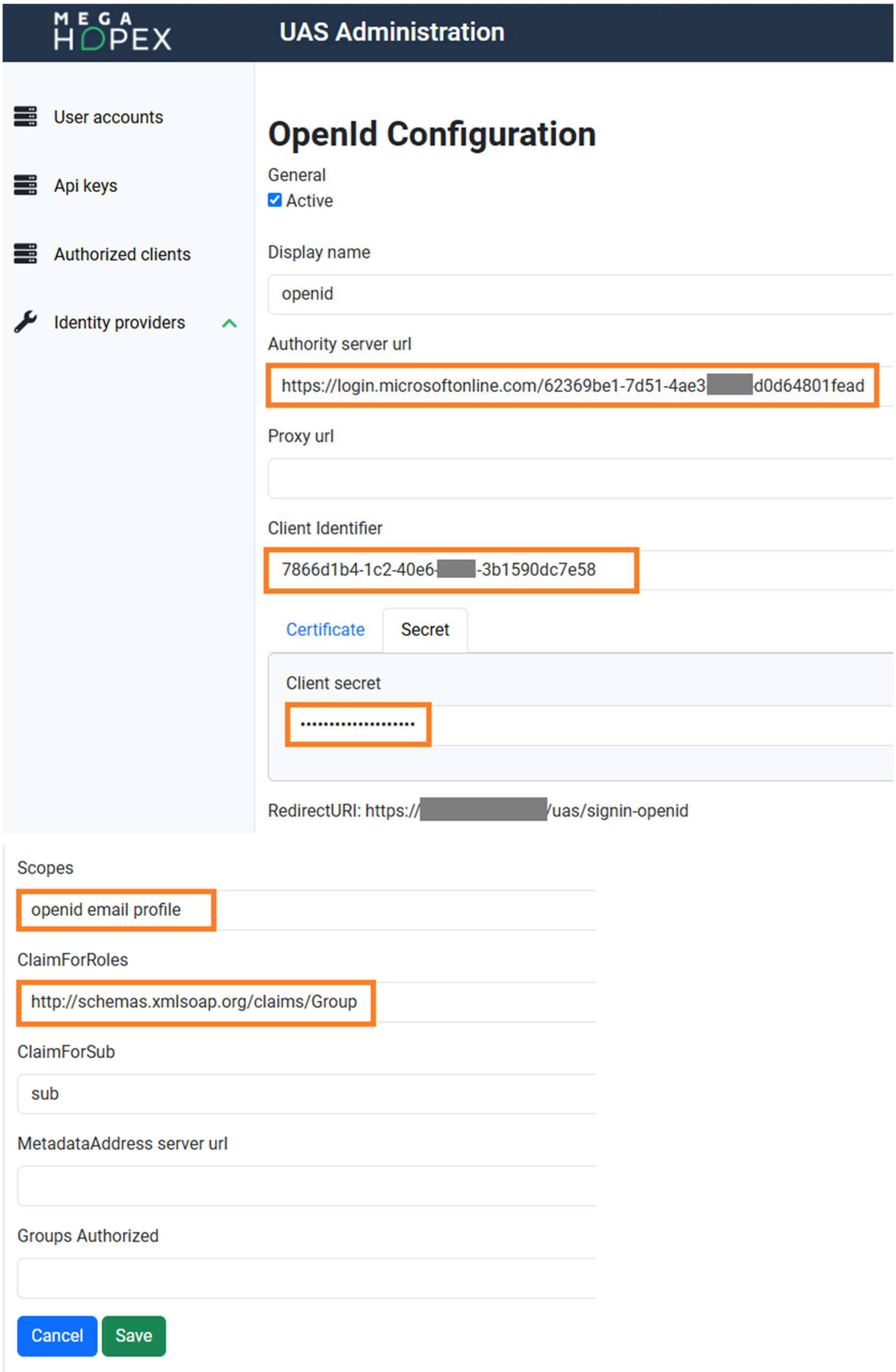
SAML2

OpenID

4) Click **Create**.

5) In OpenID Configuration, select **Active** to activate OpenID Identity Provider and enter the required information:

   - **Authority server url**
   - **Client Identifier**
   - Either **Client certificate** or **Client secret**



OpenId Configuration

General

☑ Active

Display name: openid

Authority server url: https://login.microsoftonline.com/62369be1-7d51-4ae3[redacted]d0d64801fead

Proxy url:

Client Identifier: 7866d1b4-1c2-40e6-[redacted]-3b1590dc7e58

Client secret: ••••••••••••••••••••

RedirectURI: https://[redacted]/uas/signin-openid

Scopes: openid email profile

ClaimForRoles: http://schemas.xmlsoap.org/claims/Group

ClaimForSub: sub

MetadataAddress server url:

Groups Authorized:

6) Click **Save**.

4. Terminology

4.1. Client

A client is a piece of software that requests tokens from UAS - either for authenticating a user or for accessing a resource (also often called a relying party or RP). A client must be registered with the OP.

Examples: Web applications, native mobile or desktop applications, Single Page Applications (SPA), server processes etc.

4.2. User

A user is a person who is using a registered client to access his/her data.

4.3. Scope

Scopes are identifiers for resources that a client wants to access. This identifier is sent to the OP during an authentication or token request.

By default, every client can request tokens for every scope, but you can restrict that.

They come in two flavors.

4.3.1. Identity scopes

Requesting identity information (aka claims) about a user, e.g. his name or email address, is modeled as a scope in OpenID Connect.

There is for example a scope called profile that includes first name, last name, preferred username, gender, profile picture and more. You can read about the standard scopes here and you can create your own scopes in UAS to model your own requirements.

4.3.2. Resource scopes

Resource scopes identify web APIs (also called resource servers) - you could have for example a scope named calendar that represents your calendar API.

4.4. Authentication/Token Request

Clients request tokens from the OP. Depending on the scopes requested, the OP will return an identity token, an access token, or both.

4.4.1. Identity Token

An identity token represents the outcome of an authentication process. It contains at a bare minimum an identifier for the user (called the sub aka subject claim). It can contain additional information about the user and details on how the user authenticated at the OP.

4.4.2. Access Token

An access token allows access to a resource. Clients request access tokens and forward them to an API. Access tokens contain information about the client and the user (if present). APIs use that information to authorize access to their data.

MUST Licence Installation Guide

Summary

Check if a more recent version of this document is available in online documentation (MEGA Community).

This document describes the procedures necessary for installing Must licences with HOPEX V5.0 and higher CP.

It applies to all Front-ends.

It does not describe:

- System requirements and possible architectures (see architecture overview documentation).
- How to install a product release (see installation documentation).
- How to manage installations (see administrator manuals).
- How products are licenced (see licensing documentation).

1. Foreword

HOPEX Must is the usual type of licences provided by MEGA Sales administration to enable execution of HOPEX software. It is a proprietary technology of MEGA.

To obtain or update your licence, contact your sales representative.

- A UNC will be requested.
- A .must licence file will be sent with installation instructions.

A Must licence:

- Is a file with a. must extension.
- Contains the definition of the licence (locking information, expiration date and list of products).
- Is locked on a shared folder (UNC address).
- Is required to run HOPEX Web Front-End (HOPEX Application Server).
- Is required to rub HOPEX Windows Front-end (for customization).

It is distinct from installation key required to install HOPEX V5.0 or higher version.
An installation key is a string such as mg.5i1542vixa7ptl9qocsev4zico5tzgqpzqnfc.
It will define the list of modules available for download and installation in HOPEX Store (https://store.mega.com/).

A Must licence is usually programmed with distinct **solutions**.
Ex: HOPEX Business Process Analysis (code HBPA)
Licence tokens provide access to the particular solution.

A Must licence can also be programmed with **value packs**.
A value pack is a set of HOPEX Solution used as a whole.
Licence tokens provide access to all the solutions of the value pack.

As a convention, value packs and solutions will be named as products later in this document.

Each product can be managed in different modes.

Mode	Description	Example
Dedicated mode	License tokens is dedicated to a specific user. This user is sure to get this token.	20 registered users 2 tokens APM assigned to User U0001 User U0002
Shared mode	License token is shared with users Only users configured as possible user for the product (subset of registered users) can use the token provided if is available	20 registered users 2 token APM for 4 users User U0001 User U0004 User U0005 User U0007 16 (20-4) other users cannot use them
Concurrent mode (floating mode)	License token is shared with users Any registered user can use a token provided it is available.	20 registered users 5 token APM

There are tree exclusive types of users.

Type	Description	Example
Viewer users	consult data, search, use collaboration features Cannot edit properties or diagrams	profile Application Owner
Contributor user	consult data, search, perform limited updates, use collaboration feature Cannot edit diagrams	profile Application Contributor
Main users	consult data, search, perform all updates in particular via diagram editor, use collaboration features	profile ITPM Functional Administrator

2. Get a licence from Sales Administration

There are three situations where you will need a new Must licence:

- When you purchase HOPEX products (new license).
- When you negotiate a different licence content (licence update).
- When you relocate Must licence folder (licence relocation).

To obtain or update your licence, contact your sales representative.

- A UNC will be requested.
- A Must licence file will be sent by MEGA Sales Administration.

2.1. Choose a machine to host the licence folder

If you do not have the technical skills or the authorization required for this step, contact your system administrator.

Recommendations:

- With single server deployment, use the HOPEX Server.
- With multiple server's deployment, choose one of the back-end servers.
- Target server should be an efficient file server.
- At runtime, file access will be made from module HOPEX Core.

2.2. Create a licence folder

If you do not have the technical skills or the authorization required for this step, contact your system administrator.

Create a shared folder, as far as possible in a DFS.
The licence folder must be accessible as a UNC address, meaning a shared folder with one unique address on the network.

Examples of authorized sharing:
\\Server001\Licences
\\Domain01\Applications\HOPEX\Licences (DFS)
\\Server001.Domain01.com\Licences (FQDN)
Examples of unauthorized sharing:
\\Server002\c$\ HOPEX\Licences (administrative share)
M:\Licences (network letter)

Notes:

- The shared folder name will be used a parameter for programming the licence. If it changes, the license will no longer be valid.
- The licence folder must be accessible as a UNC with permission **modify** to all Windows account that run HOPEX Core components. If you want to configure smarter permissions, consult the 'FAQs and troubleshooting' section of this document.

2.3. Get licence file

Send the shared folder path to MEGA Sales Administration when requested.
You will get a .must file valid for this path

3. Install Must licence

3.1. Copy Must licence file

Once you have a .must licence file valid for a shared folder path:

- Browse the shared folder path, ex: \\Server001\Licences.
- Copy the .must licence file (ex: Licence-Y9999.must) to this folder.

You can check there is no mismatch by viewing licence file content with a text editor.

Licence file content	… [MEGAShareLicence] **MG_SERVER_PATH**=\\Server001\Licences\Licence-Y9999.must …..
Check	MG_SERVER_PATH = <share folder path> \ <.Must licence file> -> OK

3.2. Configure file permissions

At runtime, files will be created dynamically in a hidden subfolder in the licence folder.
It is necessary to configure file permissions so that execution is correct.

Grant the permission **Modify** for the licence folder (ex: \\Server001\Licences and its subfolders) to Windows account that run HOPEX Core components.
The list of windows users varies with the front-end:

Front-end	Users to be configured
Web Front-end (HOPEX Application Server)	Local user SYSTEM by default (1)
Windows Front-end (customization or administration)	Local user SYSTEM by default (1) Each account allowed to • Run HOPEX.exe for customization tasks • Run Administration.exe for administration tasks • Run Licensing.exe

(1) if another account is used, configure identify of windows service **HAS Instance Manager**.

3.3. Specify licence folder during installation

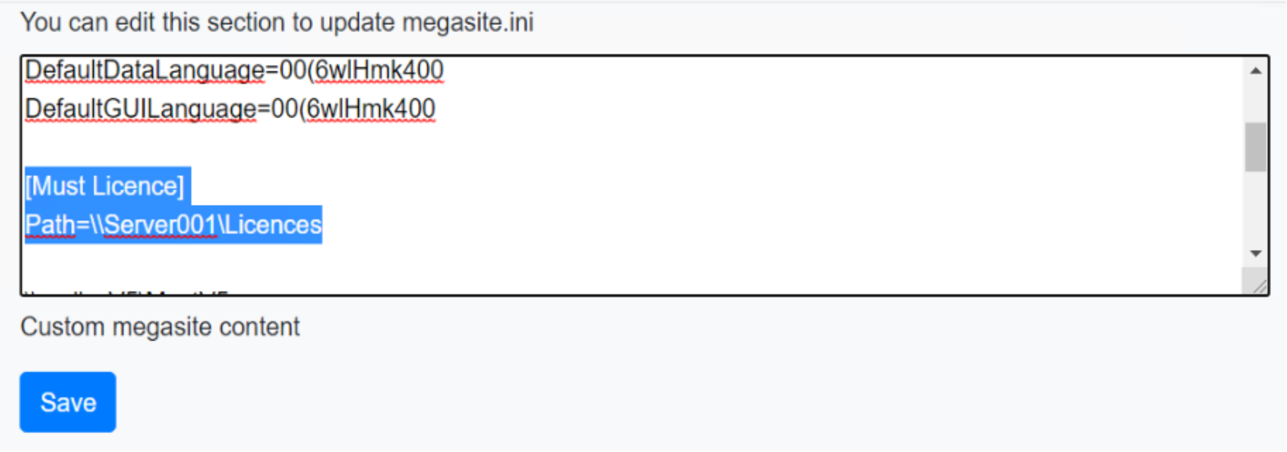
From HOPEX V5.0 and HOPEX Application Server, deployment is different from previous versions.

Installation of the license is a step of the overall installation procedure.

- Installation of HAS Instance Manager
- Creation of HAS instance.
  - Licence folder can be specified (optional)
  - HOPEX Core programs are installed
  - A configuration database is created.
- Configuration of the HAS instance.
  - Licence folder must be specified if not done earlier.
- Restart of the HAS Instance.

To install HOPEX Application server, follow document HOPEX Application Server - Installation V5.0 EN.
The key step is 'Adding Must license to MegaSite.ini setting'

You must be ready to add the following section
[Must Licence]
Path=<licence folder>



You can edit this section to update megasite.ini

```
DefaultDataLanguage=00(6wlHmk400
DefaultGUILanguage=00(6wlHmk400

[Must Licence]
Path=\\Server001\Licences
```

Custom megasite content

This specification is saved in the configuration database used by the HAS instance.

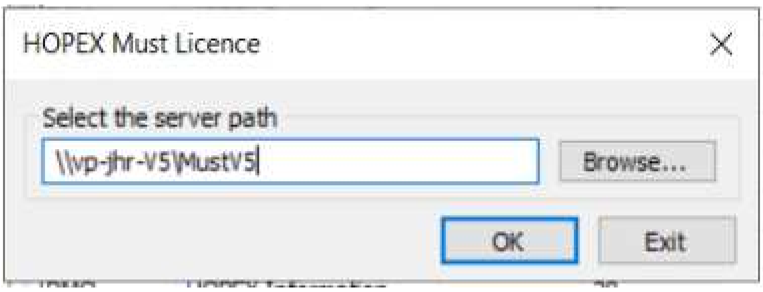
4. Configuration and monitoring procedures

4.1. Must licence utility (Licensing.exe)

A utility **Licensing.exe** is available in the folder of the HAS instance
ex: C:\ProgramData\MEGA\Hopex Application Server\5000

Run **Licensing.exe**

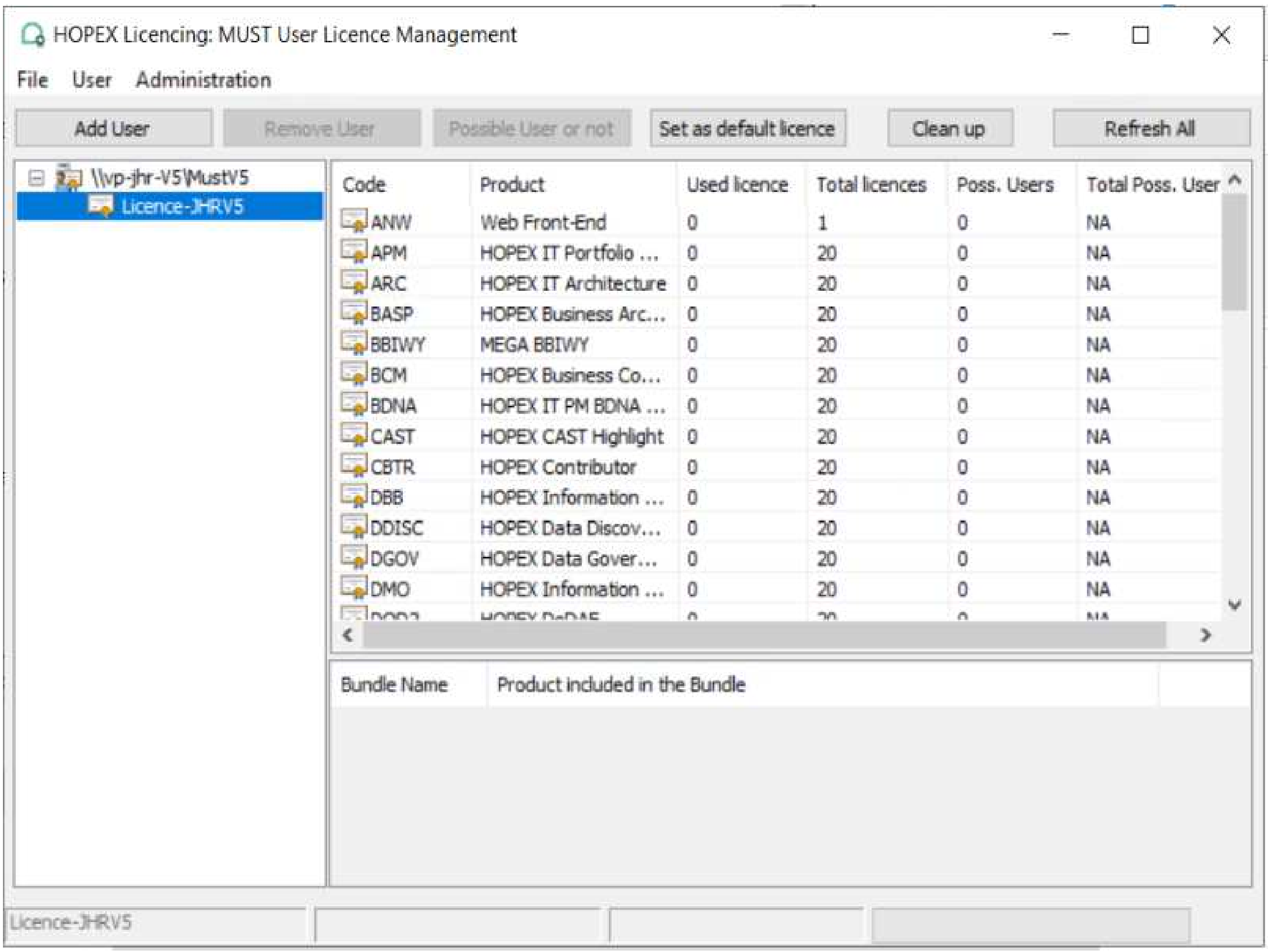
- A path is requested
- Select the license folder path
- Licence is loaded.



HOPEX Must Licence

Select the server path

\\vp-jhr-V5\MustV5



HOPEX Licencing: MUST User Licence Management

Code	Product	Used licence	Total licences	Poss. Users	Total Poss. User
ANW	Web Front-End	0	1	0	NA
APM	HOPEX IT Portfolio ...	0	20	0	NA
ARC	HOPEX IT Architecture	0	20	0	NA
BASP	HOPEX Business Arc...	0	20	0	NA
BBIWY	MEGA BBIWY	0	20	0	NA
BCM	HOPEX Business Co...	0	20	0	NA
BDNA	HOPEX IT PM BDNA ...	0	20	0	NA
CAST	HOPEX CAST Highlight	0	20	0	NA
CBTR	HOPEX Contributor	0	20	0	NA
DBB	HOPEX Information ...	0	20	0	NA
DDISC	HOPEX Data Discov...	0	20	0	NA
DGOV	HOPEX Data Gover...	0	20	0	NA
DMO	HOPEX Information ...	0	20	0	NA

Bundle Name	Product included in the Bundle

4.2. Set a default licence

It is possible to specify a default licence if several Must licences exist.

In Licensing.exe

- Select the license in the left pane.
- Click on button **Set as default licence** in the top toolbar.

4.3. Manage users using a license

This is important in several situations:

- Several Must licences exist: users should be allocated in the different licences unless a default licence is specified.
- Shared licence: possible users should be specified beforehand.
- Dedicated licence: named users should be specified beforehand.

Users are identified by their login in HOPEX.
Ex: the HOPEX login of John Smith is 'U0001'

Add a user to a licence

In Licensing.exe

- Select the license in the left tree.
- Click on button **Add user** in the top toolbar.
  A window **Add user to a licence** is displayed.
- enter the login name (Ex: enter 'U0001' for the user 'John Smith is 'U0001') and click **OK**.

Remove a user from a licence

In Licensing.exe

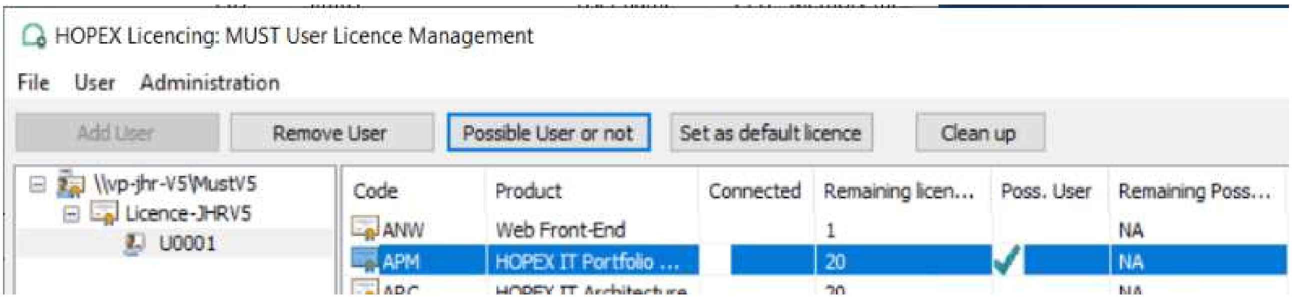
- Select the license in the left tree.
- Select the user to remove in the left tree
- Click on button **Remove user** in the top toolbar.

4.4. Configure a user as a possible user of a product

Set a user as possible user

In Licensing.exe

- Select the license in the left tree.
- Select the product to be configured in the top right pane.
- Select the user to be set as a possible user of the product.
- Click on button **Possible user or not**.
  A green checkmark is displayed in the column **Poss. User.**



\\vp-jhr-V5\MustV5
Licence-JHRV5
U0001

Code	Product	Connected	Remaining licen...	Poss. User	Remaining Poss...
ANW	Web Front-End		1		NA
APM	HOPEX IT Portfolio ...		20	✓	NA
ABC	HOPEX IT Architecture		20		NA

This specification is saved by creating a file in a subfolder of the licence folder ex: create file <licence folder>\Licence-Y9999\USERS\U0001.usr-APM-MEGA.

Remove a user as possible user
In Licensing.exe

- Select the license in the left tree.
- Select the product to be configured in the top right pane.
- Select the user to be set as a possible user of the product.
  A green checkmark is displayed in the column **Poss. User.**
- Click on button **Possible user or not**.
  The green checkmark is removed in the column **Poss. User.**

4.5. Clean up licence tokens

In Licensing.exe

- Select the license in the left tree.
- Click on button **Clean up**.

This action purges unexpected token files.

4.6. Monitor licence use

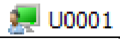
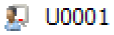
The utility **Licensing.exe** displays several elements:

- A top menu (File, User, Administration) and a toolbar 'Add User, Remove User..)
- The left tree displays the Must licence available in the selected folder.
- The top right pane displays the products available for the selected licence.
- The bottom right pane displays the bundle definition, if any.

The licence status is displayed in the left tree:

Display	Status	Possible causes
Licence-T0001	Valid	-
Licence-T0001	Invalid	Licence has expired Locking failed: the folder address containing the licence file does not match the expected UNC

The user status is displayed in the left tree:

Display	Status
 U0001	Connected
 U0001	Not connected

The top right pane has several columns. The list is different if a user or a licence is selected:

- **Code**: the code of the technical product.
- **Product**: the name of the technical product.
- **Connected**: the number of users currently logged in to the product (this figure changes over time).
- **Used licences**: the number of licence tokens currently used for the product (this figure changes over time).
- **Remaining licences**: the number of licence tokens currently available for the product (this figure changes over time).
- **Total licences**: the number of licence tokens programmed for the product (this figure does not changes over time).
- **Poss. User:** the number of users that are set as possible users of the product (this figure changes over time).
- **Remaining Poss. Users**: the number possible users currently available for the product (this figure changes over time).
- **Total Poss. Users**: the number possible users programmed for the product (this figure does not changes over time).

5. Customizing the command line

With HOPEX out of the box, it is not necessary to change command lines.
This can be useful if you need to

- Design new profiles.me
- Use value packs.
- Tune license vision of a specific user.

Remember that it is not recommended to alter command line of standard profiles.

Each product is associated to a product code.
Ex: HOPEX Business Process Analysis code 'HBPA'

A property **Command line** can be configured at several levels:

Level	Comment
Profile level	Configuration at this level is recommended. As there are less profiles than users, configuration is easier to maintain.
User level (Login)	Configuration at this level is NOT recommended. It is mainly available for compatibility with previous versions.

At each level, it is possible to specify a command line according to the type of user chosen.

Type of users	Possible syntax	Examples
Main users	/RW'<list of product codes>' /RO'< list of product codes>	/RW'DMO;HBPA' /RW'DMO;HBPA' /RO'DBB'
Viewer users	/HV'<list of product codes>'	/HV'HBPA'
Contributor users	/HC'<list of product codes>'	/HC'APM'

Where:

- /RW: defines a list of product code accessed in read/write mode.
  Note that /K (previous specification) is equivalent to '/RW'
- /RO: is optional and defines a list of product code accessed in read/only mode.
  Note that /RO is only a complement to /RW and cannot be used without /RW.
  Do not use /RO command lines to provide a consultation access. Use viewer users instead.
- /RW, /HV and /HC are exclusive. They cannot be mixed in a command line.

5.1. Configure main users (/RW /RO)

Configure profile command line
Use the /RW syntax and eventually /RO syntax and quote product codes.
Ex:
/RW'APM,HBPA' for main users on APM
/RW'APM,HBPA' /RO'DBB' for main users on APM and consultation on DBB

It is not possible to use /RO without /RW
Ex
/RO 'APM,DBB' is not allowed

5.2. Configure viewer profiles (/HV)

By convention, a product programmed in dedicated mode will use the VIEW counter. Check the licence.

Extract of licence description	Comment
[MEGAComponentInfo]	
(LAN) HOPEX MainUser=3 ; 0	Counter of main users (shared mode)
(RSQ) Repository Storage (SQL Server)=YES	-
(DMO) HOPEX Logical Data=3 ; 5	-
(SUP) HOPEX Power Supervisor=1 ; 1	Programmed in shared mode
(APM) HOPEX IT Portfolio Management=1 ; 1	Programmed in dedicated mode
(ANW) Web Front-End=NO	Programmed in dedicated mode
(HPP) HOPEX Productivity Pack=NO	-
(HBPA) HOPEX Business Process Analysis=3 ;	-
3	Programmed in dedicated mode
(CBTR) HOPEX Contributor=1 ; 0	Counter of contributor users
(VIEW) HOPEX Viewer=1 ; 0	**Counter of view users**
APM_F=5 ; 0	Programmed in concurrent mode
LAN_D=5 ; 0	Counter of main users (dedicated mode)
LAN_F=3 ; 0	Counter of main users (concurrent mode)
[MEGABundleInfo]	
APM_F=APM	
LAN_D=LAN	
LAN_F=LAN	

Configure profile command line
Use the /HV syntax and quote product codes.
Ex: /HV'APM,DBB'

5.3. Configure contributor profiles (/HC)

By convention, a product programmed in dedicated mode will use the CBTR counter. Check the licence.

Extract of licence description	comment
[MEGAComponentInfo]	
(LAN) HOPEX MainUser=3 ; 0	Counter of main users (shared mode)
(RSQ) Repository Storage (SQL Server)=YES	-
(DMO) HOPEX Logical Data=3 ; 5	-
(SUP) HOPEX Power Supervisor=1 ; 1	Programmed in shared mode
(APM) HOPEX IT Portfolio Management=1 ; 1	Programmed in dedicated mode
(ANW) Web Front-End=NO	Programmed in dedicated mode
(HPP) HOPEX Productivity Pack=NO	-
(HBPA) HOPEX Business Process Analysis=3 ; 3	- Programmed in dedicated mode
(CBTR) HOPEX Contributor=1 ; 0	**Counter of contributor users**
(VIEW) HOPEX Viewer=1 ; 0	Counter of view users
APM_F=5 ; 0	Programmed in concurrent mode
LAN_D=5 ; 0	Counter of main users (dedicated mode)
LAN_F=3 ; 0	Counter of main users (concurrent mode)
[MEGABundleInfo]	
APM_F=APM	
LAN_D=LAN	
LAN_F=LAN	

Configure profile command line:
Use the /HC syntax and quote product codes.
Ex: /HC'APM,HBPA'

5.4. Configure profiles for value packs

A value pack is a set of products used as a whole.
ex: value pack VPP_F aggregates the following products:
APM;ADES;DBB;DMO;ERML;HBPA;HBAS;BASP;HCJ;HITA;HITS;PPM;IDEA;INFA;HAM.

By convention, a product programmed via a value pack will use the counter of the value pack code. Check the licence.

Extract of licence description	Comment
[MEGAComponentInfo]	
(LAN) HOPEX MainUser=10 ; 0	
(RSQ) Repository Storage (SQL Server)=YES	
(SUP) HOPEX Power Supervisor=1 ; 1	
(MTS2) HOPEX Power Studio=1 ; 1	
(CBTR) HOPEX Contributor=10 ; 0	
LAN_D=1 ; 1	
VPP_F=10 ; 0	**Counter of value pack**
[MEGABundleInfo]	
LAN_D=LAN	
VPP_F=APM;ADES;DBB;DMO;ERML;HBPA;HBAS;BASP;HCJ;HITA;HITS;PPM;IDEA;INFA;HAM;	**code and definition of value pack**

Configure profile command line:
Use the /RW or /HC or /HV syntax and quote product codes.
Ex:
/RW'VPP_F' for main users.
/HC'VPP_F' for contributor users.
/HV'VPP_F' for viewer users.

6. Inside

6.1. Licence check at login

When HOPEX is run by user U0001:

1. Configuration is read to identify the licence folder mapped to the HAS instance.
2. Licence folder is read to identify
   - The authorized licence file for this user.
   - The definition of the licence
   - The possible products for this user
   - The available tokens for each product of the license
3. Command line is read at both profile and login level to identify the requested products
4. Connection is refused if:
   - Command line is inconsistent
   - Products tokens are not available
5. Connection is allowed otherwise
   Possible user files can be created dynamically
   Token files are created according to product used

6.2. Token requested at runtime

Web Front-End (HOPEX Application Server)

Context	Must licence checked	Main counter used	Tokens requested	Command line considered
HOPEX Main users (Common situation)	Yes	LAN	One token per Product One token LAN (2)	Yes
HOPEX Main users (controlled multi front-end)	Yes (1)	LAN	One token per Product One token LAN (2)	Yes
HOPEX Contributor	Yes	CBTR	One token for CBTR	Yes
HOPEX Viewer	Yes	VIEW	One token for VIEW	Yes
Web Service API	No (3)	-	-	-

(1) ANW product should be programmed.
Ex: ANW is required to run ARC (controlled multi front-end).
(2) LAN or LAN_D, or LAN_F.
(3) UAS token is requested

With Windows Front-end (customization or Administration)

Context	Must licence checked	Tokens requested	Command line considered
Administration.exe	Yes	One token SUP One token LAN (1)	No
HOPEX.exe with HOPEX Power Studio (MTS2)	Yes	One token MTS2 One token LAN (1)	Yes

6.3. Files access

A licence folder can contain one or more licences.
For each licence, a hidden folder is created with the licence name

Ex:
<licence folder>\Licence-Y9999.must licence file
<licence folder>\Licence-Y9999 hidden folder

The hidden folder contains 2 subfolders.

Folder	Description	Example
TOKENS	Enables to count product tokens used at runtime Each product has a subfolder 1 token = 1 file	When user U0001 opens a session with product APM, a file TOKEN-CA58CCE4613838E4-u-U0001.tkn-APM is created automatically in <hidden folder>\TOKENS\APM Where • U0001 is login name • APM is product code • CA58CCE4613838E4 is an ID generated at runtime This file will be deleted automatically when users U0001 logs out (end of session)
USERS	Enables to configure possible user Flat list 1 possible user seat = 1 file	When U0002 is set as possible user of HBPA, a file U0002.usr-HBPA-MEGA is created in <hidden folder>\USERS where • U0002 is login name • HBPA is product code This file is not deleted automatically

A file Router.ini is created in the licence folder.
It saves:

- The default licence if any
- The assignment of users (logins) to licences

7. FAQs and Troubleshooting

7.1.1. Do I have to configure possible users?

This is not mandatory. Possible user tokens are generated dynamically at runtime.
When user U0001 logs as main user, a token is requested for each product mentioned in the command line (/RW). If possible user seats are available, U0001 is automatically configured as a possible user for the requested products.
It can be necessary to manage assignment of possible users.

7.1.2. Do I have to add each user in Licensing.exe?

This is not mandatory. Users (logins) are added dynamically at runtime.
It can be necessary to declare explicitly users that did not yet connect and you want to manage assignment of possible users.

7.1.3. How can I prevent the dynamic declaration of possible users?

There is no way of preventing a user who is not explicitly configured from logging in. If a possible user seat is available, the system will set a user requesting a token as a possible user. To fully control the assignment, it is recommended you configure possible users beforehand.

7.1.4. Is my licence shared, concurrent or dedicated?

Licencing mode (dedicated, share, concurrent) is not set at licence level but at product level

To check the licensing mode, you need to understand the .Must licence
The mode depends on the combination of 2 digits.
<Licence Product>=T ; U
Where:
T: tokens
U: users

Licensing mode	Example
Dedicated mode (T=U)	(HITA) HOPEX IT Architecture=20 ; 20
Shared mode (T< U)	(HITA) HOPEX IT Architecture=20 ; 25
Concurrent mode/floating mode (T>U, U=0)	(HITA) HOPEX IT Architecture=20 ; 0

7.1.5. Error: The license file XX is not valid. The crypted path does not correspond to the license path file

Possible reasons:

- The path of the folder containing the Must licence file does not match the path programmed in the licence.
- The path of the folder quoted in the configuration does not match the path programmed in the licence.
- The licence file name does not match the file name programmed in the licence (licence file was renamed).

Updating Virtual Reports

1. Introduction

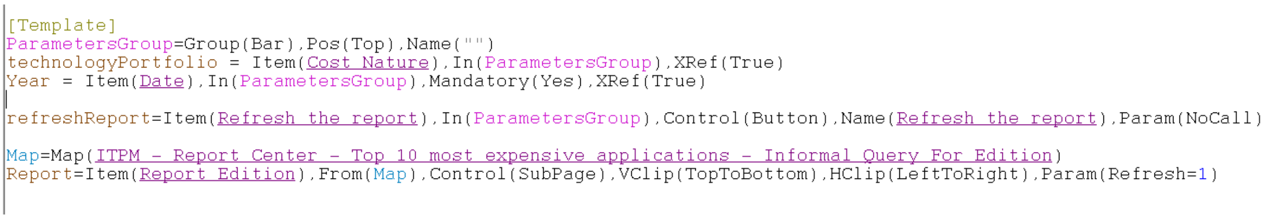
This document describes how to update existing virtual reports to use the new Report Tool.

This applies starting from Hopex V5.

2. Virtual Reports with Report Edition

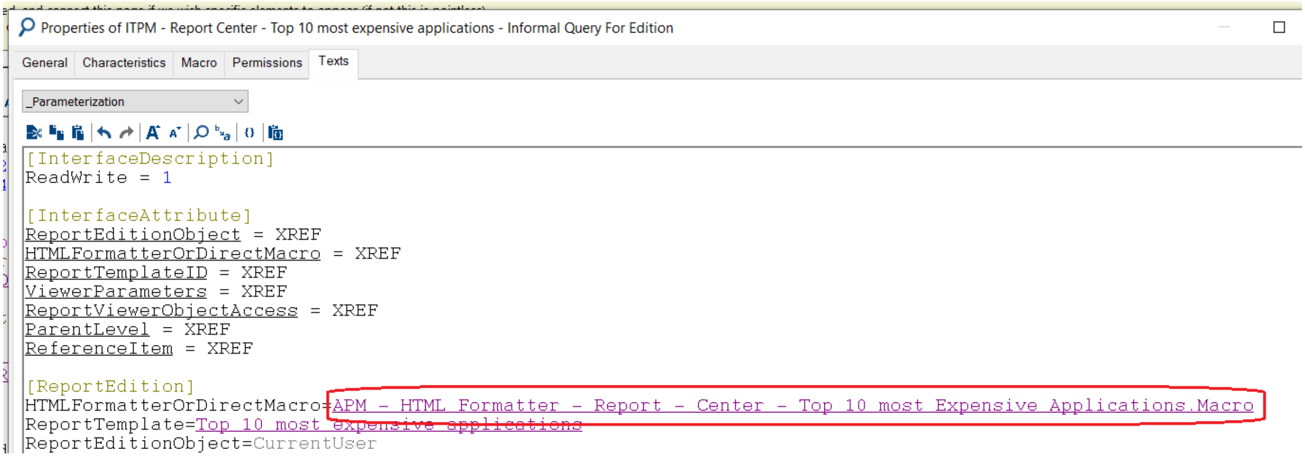
2.1. Identifying the macro to edit

These reports are defined in Property Pages which define a specific informal query and use the Report Edition generic subpage:



```
[Template]
ParametersGroup=Group(Bar),Pos(Top),Name("")
technologyPortfolio = Item(Cost Nature),In(ParametersGroup),XRef(True)
Year = Item(Date),In(ParametersGroup),Mandatory(Yes),XRef(True)

refreshReport=Item(Refresh the report),In(ParametersGroup),Control(Button),Name(Refresh the report),Param(NoCall)

Map=Map(ITPM - Report Center - Top 10 most expensive applications - Informal Query For Edition)
Report=Item(Report Edition),From(Map),Control(SubPage),VClip(TopToBottom),HClip(LeftToRight),Param(Refresh=1)
```

The report formatter macro must be updated. It is defined in the informal query _Parameterization attribute:


Properties of ITPM - Report Center - Top 10 most expensive applications - Informal Query For Edition
General
Characteristics
Macro
Permissions
Texts
_Parameterization

```
[InterfaceDescription]
ReadWrite = 1

[InterfaceAttribute]
ReportEditionObject = XREF
HTMLFormatterOrDirectMacro = XREF
ReportTemplateID = XREF
ViewerParameters = XREF
ReportViewerObjectAccess = XREF
ParentLevel = XREF
ReferenceItem = XREF

[ReportEdition]
HTMLFormatterOrDirectMacro=APM - HTML Formatter - Report - Center - Top 10 most Expensive Applications.Macro
ReportTemplate=Top 10 most expensive applications
ReportEditionObject=CurrentUser
```

2.2. Updating the macro

Perform the following two changes to this macro:

- After the report creation part, add the following code :

```
 …

 Set oAnalysisPlugin =
oRoot.CurrentEnvironment.GetMacro("~9MuFp4qmBD40[Analysis Plugin]")

 …

 Set oAnalysis = oAnalysisPlugin.newAnalysisFromXMLString(oRoot,
oXmlAnalysisBuilder.xmlAnalysis)

 …

 'Report tool parameterization

 dim sUserData

 sUserData = oGenerationContext.UserData

 if sUserData <> "" then

   oAnalysis.setReportCmpId(oAnalysisPlugin.getReportCmpId(sUserData))

 end if
```

- Remove the HTML Header and Body added to the string returned at the end of the Generate sub.

```
sout = sout & "<!DOCTYPE HTML PUBLIC ""-//W3C//DTD HTML 4.01
      Transitional//EN""
      ""http://www.w3.org/TR/html4/loose.dtd""><html><head>" _

              & oRoot.CurrentEnvironment.GetMacro("~gu3rWUjw4D70[Html Complete
      Analysis]").getCssAndJsReferences (oRoot, oGenerationContext) &
      oAnalysisPlugin.getCssJs(oRoot,oGenerationContext) _

              & "</head><body class=""nae"">" _

              & oAnalysis.Generate("HTML",oGenerationContext,null) _

              & "</body></html>"
```

You get now :

```
sout = oAnalysis.Generate("HTML",oGenerationContext,null)
```

3. Virtual reports without Report Edition

3.1. Updating the Property Page

The MetaPropertyPage or Macro which defines the viewer control must be updated. It contains this kind of definition:

```
myReport=Item(~H(IbRVABTP9B[MyReportMacro) ,From(Map)
    ,Control(Viewer),Param(DirectMacro)
```

- The new Report control must be used instead of Viewer, so the previous line should be changed to:

```
myReport=Item(~H(IbRVABTP9B[MyReportMacro) ,From(Map) ,Control(Report)
    ,Param(DirectMacro)
```

> ***Warning:*** *MyReportMacro must be a* ***Macro*** *and not an HTMLFormatter, it is therefore mandatory to define a DirectMacro. If you have defined an HTMLFormatter, you can use its existing macro.*

3.2. Updating the macro

Proceed as described section 2.2 Updating the macro.

4. Finding my customized virtual reports

4.1. Finding Virtual reports with Report Edition

to get all specific informal queries, use the following query:

```
Select [Query] Where [_Parameterization] Like "#HTMLFormatterOrDirectMacro#"
And [Creator] Not = "j6L3BsG8kW60"
```

Then, modify the HTML Formatter macro or Direct Macro as described section 2.2 Updating the macro.

4.2. Finding Virtual reports without Report Edition

They can be defined in a MetaPropertyPage or in a Macro defining a MetaPropertyPage or in a custom JAVA project defining a MetaPropertyPage.

To find them, use the following queries:

```
Select [MetaPropertyPage] Where [_Parameterization] Like "#control(viewer)#"
And [Creator] Not = "j6L3BsG8kW60"

Select [Macro] Where [VB Script] Like "#control(viewer)#" And [Creator] Not =
"j6L3BsG8kW60"
```

And find occurrences of the following string in custom JAVA files:

```
Control(Viewer)
```

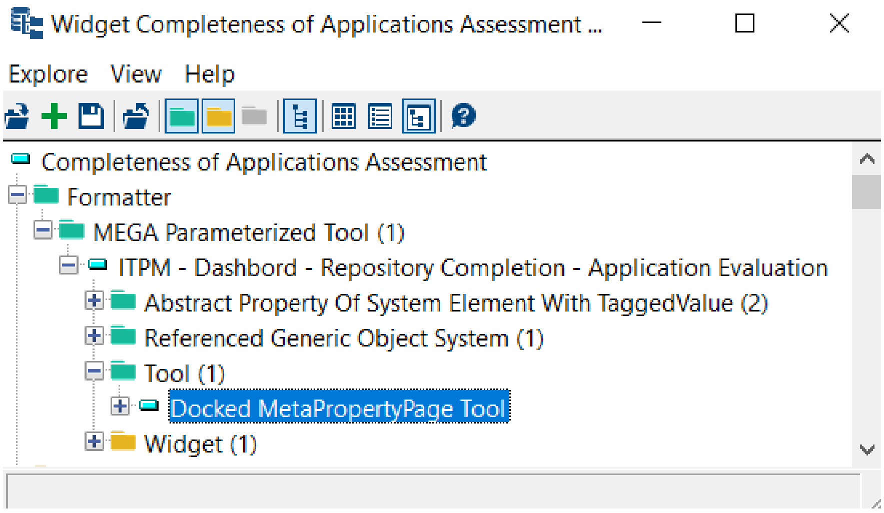
Then, modify the Page as described in section 3.1 Updating the Property Page to use the new Control **Report** and the Direct Macro used by this Control as described section 3.2 Updating the macro.

5. Updating Widgets based on a Tool

5.1. Finding Widgets based on a Tool

Updatable Widgets use a MEGA Parameterized Tool as Formatter. This Tool is a Docked MetaPropertyPage Tool. The viewer control is defined in the Parameterized Tool Property Page.

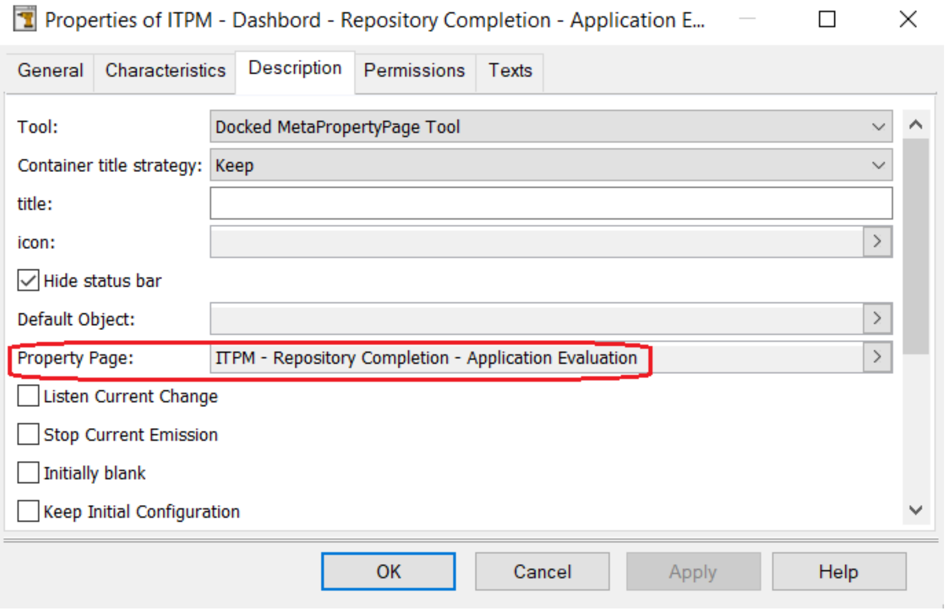
For example:



Completeness of Applications Assessment
- Formatter
  - MEGA Parameterized Tool (1)
    - ITPM - Dashbord - Repository Completion - Application Evaluation
      - Abstract Property Of System Element With TaggedValue (2)
      - Referenced Generic Object System (1)
      - Tool (1)
        - Docked MetaPropertyPage Tool
      - Widget (1)

5.2. Updating the Property Page

The property page to update is defined in the Tool Description page:



Properties of ITPM - Dashbord - Repository Completion - Application E...

Tool: Docked MetaPropertyPage Tool

Container title strategy: Keep

title:

icon:

☑ Hide status bar

Default Object:

Property Page: ITPM - Repository Completion - Application Evaluation

□ Listen Current Change

□ Stop Current Emission

□ Initially blank

□ Keep Initial Configuration

It must be updated as described section 3.1 Updating the Property Page.

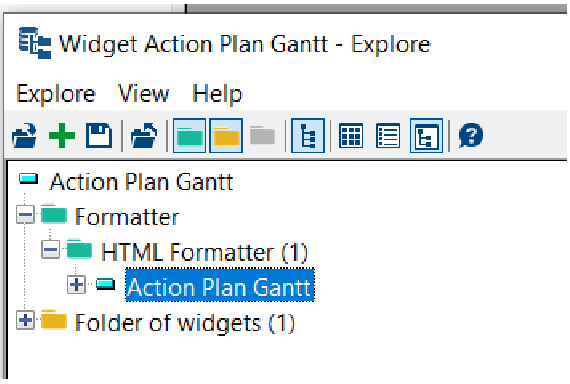
5.3. Updating the Macro

The report formatter macro defined in this Property Page must be updated as described section 2.2 Updating the macro.

6. Updating Widgets based on a Formatter

These widgets define an HTML Formatter.

For example:



Widget Action Plan Gantt - Explore

```
Action Plan Gantt
⊟ Formatter
   ⊟ HTML Formatter (1)
      ⊞ Action Plan Gantt
⊞ Folder of widgets (1)
```

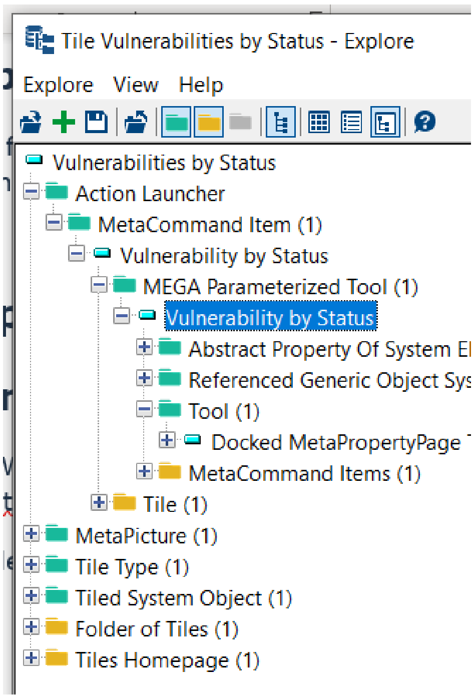
This formatter should be removed. It must be replaced by a MEGA Parameterized Tool using the Docked MetaPropertyPage Tool. The MetaPropertyPage must use the new Report control as described section 3.1 Updating the Property Page. The HTML Formatter macro can be reused but only as a DirectMacro. It must also be modified as described section 3.2 Updating the macro.

7. Updating Tiles based on a Tool

7.1. Finding Tiles based on a Tool

Updatable Tiles define a MEGA Parameterized Tool in the hierarchy of their definition. This Tool is a Docked MetaPropertyPage Tool. The viewer control is defined in the Parameterized Tool Property Page.

For example:



Tile Vulnerabilities by Status - Explore

Explore View Help

- Vulnerabilities by Status
  - Action Launcher
    - MetaCommand Item (1)
      - Vulnerability by Status
        - MEGA Parameterized Tool (1)
          - Vulnerability by Status
            - Abstract Property Of System El
            - Referenced Generic Object Sys
            - Tool (1)
              - Docked MetaPropertyPage
            - MetaCommand Items (1)
        - Tile (1)
  - MetaPicture (1)
  - Tile Type (1)
  - Tiled System Object (1)
  - Folder of Tiles (1)
  - Tiles Homepage (1)

7.2. Updating the Property Page

Proceed as described section 3.1 Updating the Property Page.

7.3. Updating the Macro

The report formatter macro defined in this Property Page must be updated as in section 2.2 Updating the macro.