

HAZELTREE



HTInstaller Guide

TABLE OF CONTENTS

Introduction	4
HTINSTALLER	4
Deployment Schema	4
Deployment schema types.....	5
HTInstaller System Requirements.....	7
Software & Hardware Requirements.....	7
APP Role requirements	7
WEB Role requirements	7
Database Role requirements	8
Additional Requirements	9
Servers Preparation	11
1. Create User accounts	11
2. Install Erlang OTP component.....	12
3. Install Rabbit MQ	13
Install RabbitMQ plugins	14
Erlang cookie file	15
RabbitMQ configuration	15
4. Start the HTInstaller	17
All-in-One Installation Instructions	18
1. HTInstaller Setup and License Agreement	18
2. Common parameters & Sync Manager Pipelines parameters.....	19
3. Installation type	19
4. User credentials & Optional modules	20
5. Network parameters.....	21
Available protocols on the server	22
Mobile API access.....	23
6. Database & Rabbit MQ parameters.....	24
7. SSO parameters.....	25
8. Proxy Parameters	26
9. Email parameters	27
10. External dependencies parameters	28
Redis / Ignite integration	29
11. Statistics Collection Parameters.....	30

12. Logging & Tracing Parameters	30
13. Octopus Deploy Server parameters	31
14. Common validation	32
15. Installation process	33
Multi-node Installation Instructions	34
1. HTInstaller Setup and License Agreement	35
2. Common parameters & Sync Manager Pipelines parameters	35
3. Installation type	36
3. User credentials & Optional modules	38
4. Network parameters	39
Available protocols on the server	40
Mobile API access	41
5. Database & Rabbit MQ parameters	41
6. SSO parameters	43
7. Proxy Parameters	44
8. Email parameters	45
9. External dependencies parameters	46
Redis / Ignite integration	47
10. Statistics Collection Parameters	48
11. Logging & Tracing Parameters	48
12. Octopus Deploy Server parameters	49
13. Common validation	50
14. Installation process	51
HTInstaller Client instructions	53
1. HTInstaller Client setup & License agreement	53
2. User credentials & Octopus tentacle	53
3. Octopus Tentacle parameters	55
4. Logging Parameters	56
5. Common validation process	57
6. Complete installation process	57
7. Return to HTInstaller	58
Appendix	59
Installation logs	59
SSL Certification in multi-node deployment plans	59
Validation errors	59

INTRODUCTION

HAZELTREE Hazeltree© is a compound multitask application that contains different modules developed for the variety of tasks required for effective treasury management. Hazeltree application can be customized individually for every client in order to meet their requirements and business needs. Due to its complexity, Hazeltree application requires an accurate, precise, and prepared deployment process. To streamline this process the Hazeltree company developed a standalone product named **HTInstaller©**: a tool that allows to automate the process of Hazeltree installation and control the deployment process.

HTINSTALLER

HTInstaller© is an own Hazeltree development. This product represents a tool that completely automates the process of Hazeltree application deployment. HTInstaller is a multiscreen installation wizard that controls all deployment steps and parameters critical for its work.

BENEFITS OF HTINSTALLER

HTInstaller is shipped to every client along with the Hazeltree application package. Enjoy the benefits of the HTInstaller deployment, as the HTInstaller:

- ✓ ...allows to completely automate the process of installation.
- ✓ ...streamlines the process of the Hazeltree application premature configuration.
- ✓ ...allows to control every aspect of the deployment step.
- ✓ ...manages the deployment on different complexity levels.
- ✓ ...provides with clean and clear understanding of the Hazeltree application architecture.
- ✓ ...allows to momentarily catch and fix deployment errors.
- ✓ ...can adjust to the client's changing visions on deployment.

Deployment is a process of server configuration and installation of the Hazeltree components. It is a sophisticated process that comprises different actions which can be consolidated in three major steps:

1. [Deployment schema planning](#): develop your environment layout and server roles.
2. [Servers preparation](#): check the servers against system requirement and install the required software.
3. [Application deployment](#): install the Hazeltree application.

DEPLOYMENT SCHEMA

Deployment schema (or **Deployment plan**) is a layout of the environment that provides stable work of Hazeltree application. Selecting the deployment schema implies distribution of the server roles among the servers that constitute the future Hazeltree environment.

Term: **Server role** is a purposeful function delegated to the server that supports a set of assigned tasks and provide stable work of Hazeltree application. There are three possible server roles:

Server Role	Description
APP	Application server that runs the Hazeltree application and 3d party products supporting the application work.
WEB	IIS-based front-end server supporting application web-interface work.
DB	SQL database server that stores application databases.

DB ROLE

The **DB** role can be delegated to the **APP** or **WEB** server or it can be assigned to a segregated server. It is recommended that the database is deployed on a segregated server since the capacity of servers can be limited. If the database work fails due to insufficient capacity of the server, it can lead to stability and performance issues in the Hazeltree application's work.

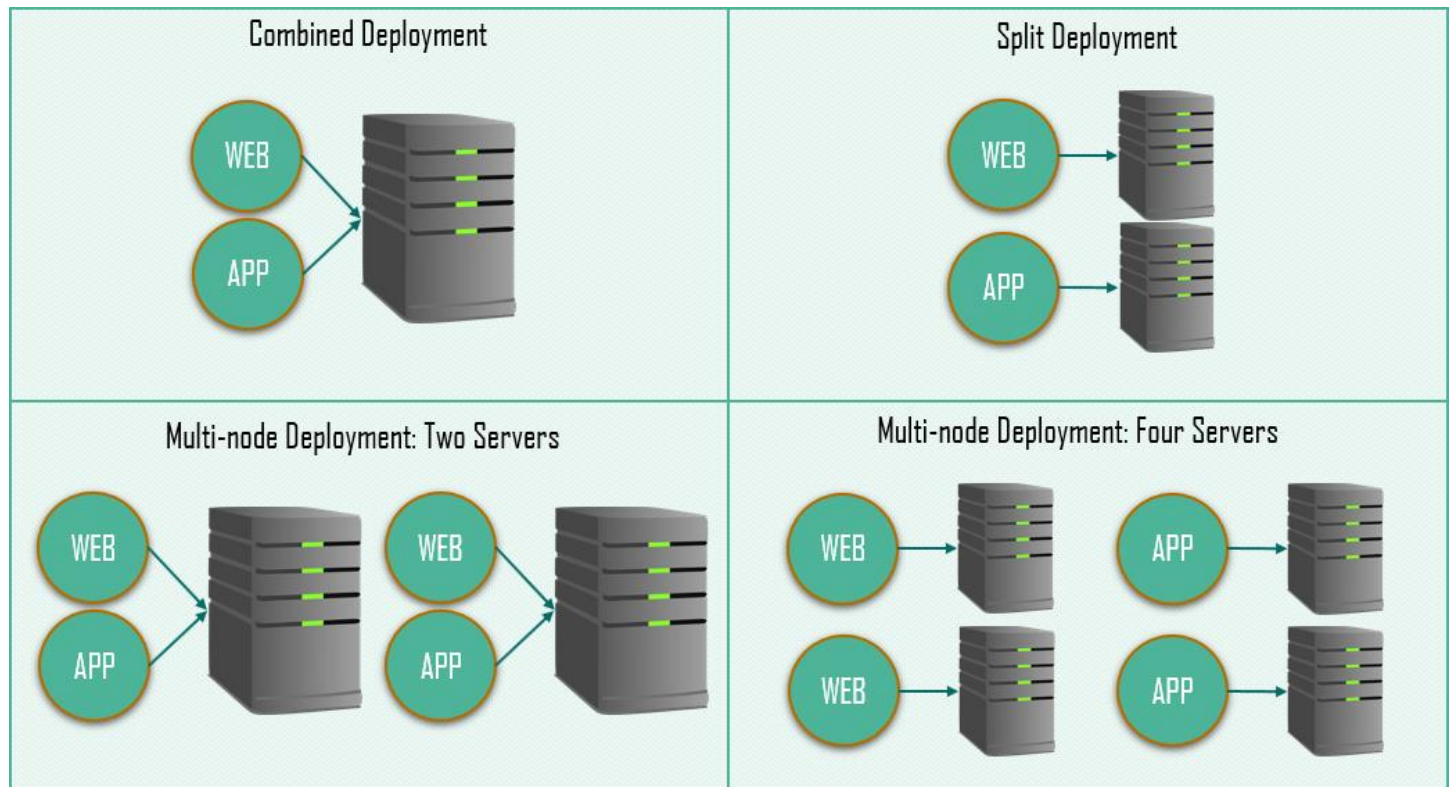
NOTE! The Database related processes are executed on the server with the **APP** role.

Server roles are combined in the most optimal, convenient, and secure combination for customers. The HTInstaller wizard offers several Deployment schemas.

DEPLOYMENT SCHEMA TYPES

Deployment schema type is a combination of server roles that support Hazeltree application's work. The HTInstaller wizard provides with an opportunity to select the most convenient and optimal deployment plan. Four deployment schema types are available for Hazeltree application:

- **Combined Deployment:** WEB and APP roles are assigned to one server.
- **Split Deployment:** WEB and APP roles are assigned to two separate servers.
- **Multi-node Deployment (Two Servers):** two separate servers both given WEB and APP roles.
- **Multi-node Deployment (Four Servers):** two WEB role servers and two APP role servers.



NOTE! The **DB role** (database server) is not considered as a determinant schema item because it is recommended to have a segregated database server regardless of the chosen Deployment schema. It is, however, can be assigned to any server included in the deployment plan.

See the example on the next page:

EXAMPLE

The company “Gartaryen Financing” is planning to implement the Combined Deployment schema due to its ease and simplicity. They decide to give the **WEB**, **APP** and **DB** server roles to one single server. The client’s initial layout looks like this:



Mister K. Grogo, the technical specialist of the “Gartaryen Financing”, is looking through the system requirements during the preparation for the Hazeltree deployment. He realizes that the server does not have enough hard drive space to store all three server roles functions. He suggests allocating a segregated server. This change of plan does not shift the deployment plan chosen by the “Gartaryen Financing” chief. New layout schema looks like this:



The deployment plan is selected in the HTInstaller wizard during the configuration process. However, it is strongly recommended to have a made-up deployment plan before the installation: it is critical to know which servers you must prepare for deployment and check against system requirements.

HTINSTALLER SYSTEM REQUIREMENTS

HTInstaller system requirements must be checked on every server that constitutes the deployment plan. System requirements are to be respected before the installation. All requirements refer to the hardware, software, and server configuration parameters.

SOFTWARE & HARDWARE REQUIREMENTS

Every role has its specific requirements that must be checked before the installation. In case of a missed component, the HTInstaller will most likely fail during the installation process or the installed Hazeltree application can work improperly. To avoid any issues during and after deployment, make sure that servers coincide all requirements.

APP ROLE REQUIREMENTS

Hardware	6 vCPUs
	8Gb RAM
	150Gb high performance disk (SSD)
Software	Microsoft Windows 2016 (64 bit). NOTE! <u>Windows 2008 and 2012 are no longer supported</u>
	Microsoft .Net Framework 4.8
	Microsoft .NET Core 3.1 Hosting Bundle (shipped with HTInstaller)
	Microsoft .NET Core 2.2 Hosting Bundle (shipped with HTInstaller)
	Jager 1.18 (both collector and agent)
	Erlang OTP 23.3.4
	RabbitMQ 3.8.9
	RabbitMQ Delayed Message Exchange Plug-in 3.8.9
	Microsoft Excel 2013 or above
	Microsoft Report Viewer
	Windows Task Scheduler
Windows Features	"NET-Framework-45-Core"

WEB ROLE REQUIREMENTS

Hardware	4 vCPUs
	6Gb RAM
	100Gb high performance disk (SSD)
Software	Microsoft Windows 2016 (64 bit). NOTE! <u>Windows 2008 and 2012 are no longer supported</u>
	Web Server (IIS)

	Microsoft .Net Framework 4.8
	Microsoft .NET Core 3.1.15 or higher
	Jager 1.18 (both UI and agent)
	Access Database Engine 2010
Windows Features	"Web-Server" "Web-Common-Http" "Web-WebServer" "Web-WebSockets" "Web-Default-Doc" "Web-Dir-Browsing" "Web-Http-Errors" "Web-Static-Content" "Web-Http-Redirect" "Web-Health" "Web-Performance" "Web-Security" "Web-Filtering" "Web-Basic-Auth" "Web-Client-Auth" "Web-Digest-Auth" "Web-Cert-Auth" "Web-IP-Security" "Web-Url-Auth" "Web-Windows-Auth" "Web-App-Dev" "Web-Net-Ext45" "Web-ASP" "Web-Asp-Net45" "Web-CGI" "Web-ISAPI-Ext" "Web-ISAPI-Filter" "Web-Includes" "Web-Mgmt-Tools" "Web-Mgmt-Console" "Web-Scripting-Tools" "Web-Mgmt-Service" "NET-Framework-45-Features" "NET-Framework-45-Core" "NET-Framework-45-ASPNET" "NET-WCF-Services45" "WAS"

DATABASE ROLE REQUIREMENTS

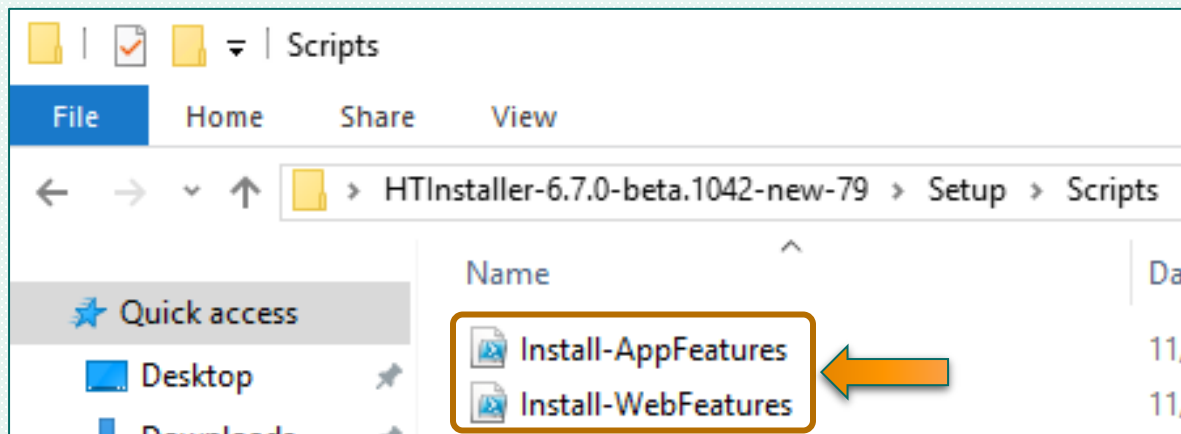
Hardware	8 vCPUs
	24Gb RAM
	300-500Gb high performance hard disk (SSD)

Software	Microsoft Windows 2016 (64 bit) with latest patches
	Microsoft SQL 2016 SP2 Standard (64 bit) with latest cumulative patches
Server configuration	Port 1433 is opened for APP role server
	IE Enhanced Security Configuration is off
	Set Server Collation to SQL_Latin1_General_CP1_CI_AS
	Install "Full-Text Search" instance feature on the SQL Server

WINDOWS FEATURES INSTALLATION

The installation of missing Windows Features is automated with the two PowerShell scripts shipped in the package along with the HTInstaller tool. To utilize the scripts, proceed to the **HTInstaller** folder > folder **Setup** > folder **Scripts**. The folder contains two PowerShell files:

- **Install-AppFeatures**
- **Install-WebFeatures**



Launch the **Install-AppFeatures** script of the **APP** server and the **Install-WebFeatures** script on the **WEB** server to install all necessary Windows Features. If any of required features are already installed, the script will simply skip them and install only missing items.

NOTE! It is recommended to manually check the Windows Features before installation.

INFO! Another important part that must be installed in order to properly use the HTInstaller application with no failures is the **Microsoft .NET Core 3.1 Hosting Bundle** and **Microsoft .NET Core 2.2 Hosting Bundle**. Both installation packages are shipped with the HTInstaller and can be found in the folder *Resources* (under the folder *Setup*).

ADDITIONAL REQUIREMENTS

Regardless of the server role, it is also a strong necessity to equip the server with a standard third-party applications kit. It ought to be installed on every server included in the deployment schema:

- **GNU Privacy Guard** (it is used for own encryption and when the feed data is encrypted)
- **NotePad++**
- **FileZilla** or compatible **SFTP** client
- **WinRAR** or **7zip**

- Adobe Acrobat Reader
- ELK 7.10
- Redis 5.0.6
- Apache Ignite 2.10.0

SERVICES PREPARATION

Servers preparation is a set of premature actions that must be performed on all servers of the chosen deployment schema.

The HTInstaller is designed to automatize the installation of the Hazeltree application. During the deployment process the HTInstaller needs administrator permissions and owner-level access to the database. The tool also uses the 3d party application Rabbit MQ which must be installed and properly configured.

Fresh installation is occurring on clean servers. Firstly, servers must be checked against system requirements. If requirements are respected, perform the following routine:

1. [Create two user accounts](#)
2. [Install Erlang OTP](#)
3. [Install RabbitMQ software](#)

INSTALLATION TYPES

The HTInstaller can be used for two types of installation:

- > **Fresh installation:** first Hazeltree deployment on clean server/servers.
- > **Update:** deployment of a new version on top of installed Hazeltree application.

In case of an update, prepare only those servers that were added to the schema.

1. CREATE USER ACCOUNTS

All servers included in the deployment schema with **WEB**, **APP** and **DB** roles must be equipped with two user accounts with particular set of permissions. These accounts are used by the HTInstaller during the installation process. See the table below:

Suggested AD account name	HTInstaller designation	Permissions
srv_AWS_HT_Install	User account to run Application services	1. Local Administrator on all servers 2. SQL SA or DB owner
srv_AWS_HT_Pool	User account to run WEB sites	1. SQL SA or DB owner

Create two user accounts through the Windows User management control panel and grant them permissions to the database. **NOTE!** In case you do not provide sufficient permissions listed above for the users accounts, the deploy will fail.

IMPORTANT: POSSIBLE ISSUES!

It is critical that the user account of the actual HTInstaller operator has database **sysadmin** permissions. If the database is deployed on a segregated server, provide the **sysadmin** permissions for the user account of the HTInstaller operator on a segregated server.

If the user account of the HTInstaller operator is not provided with **sysadmin** permissions, the installation process will fail with an error: **"Cannot connect to Octopus Deploy database server"**. If you see this error, check the permissions of your user account in the SQL Server Management Studio:

⚠ Check database connection

Can not connect to Octopus Deploy database server by port 1433

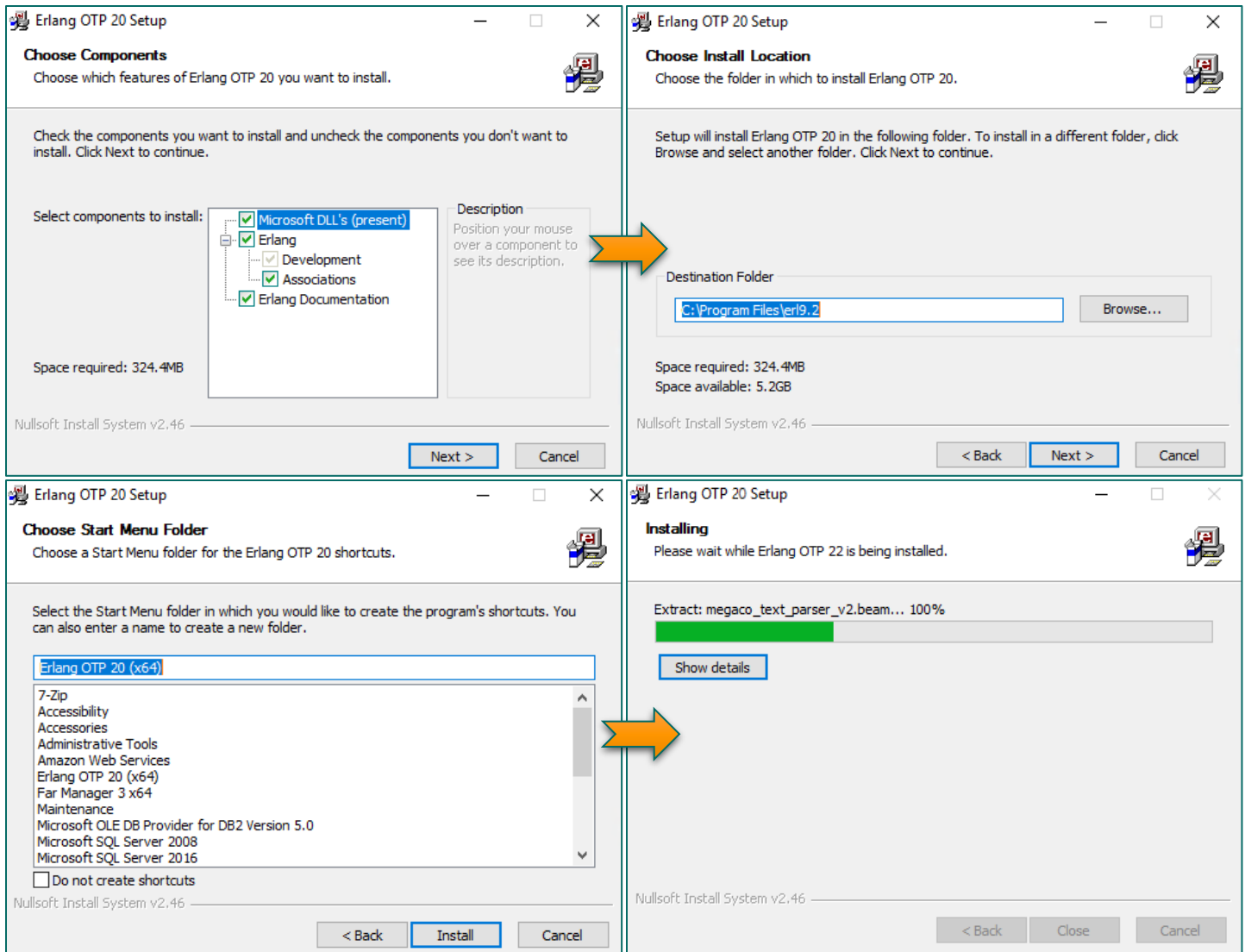
Verify database server and network configurations to continue.

2. INSTALL ERLANG OTP COMPONENT

Erlang is a concurrent functional programming language. **OTP** is a library of the Erlang language. It is used by the RabbitMQ software and is essential for the RabbitMQ correct work.

NOTE! In case you already have the Erlang OTP installed, skip this step, and proceed to the Rabbit MQ configuration.

Find the installation file of the OTP component in the package shipped along with the HTInstaller (path: archive **HTInstaller** > folder **Setup** > folder **Resources**). Copy the file on the server where the RabbitMQ software is to be installed. Launch the installation executable file and follow the wizard commands as shown below:



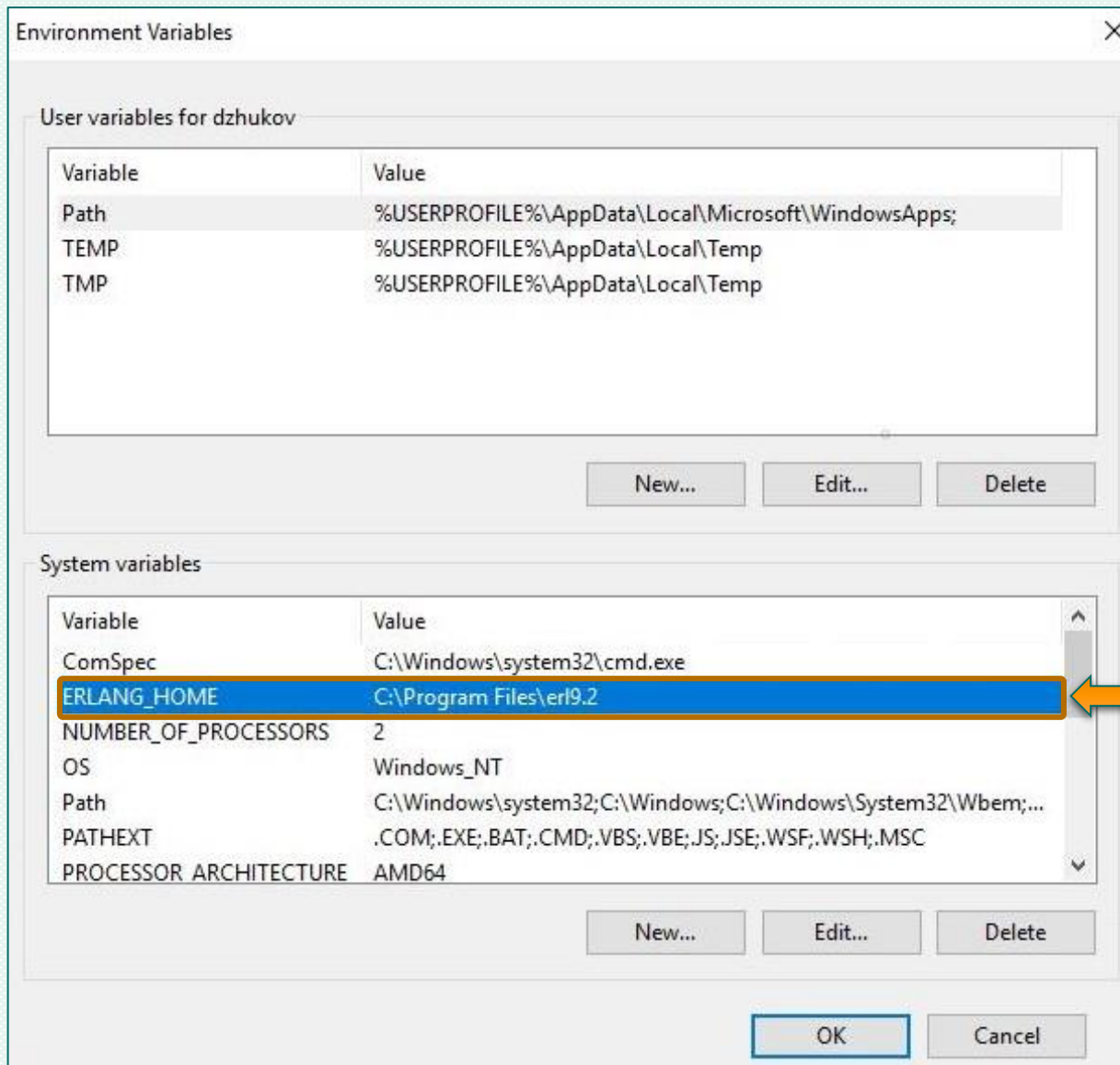
ERLANG SYSTEM VARIABLE

The Erlang OTP 20 component creates a new Windows system variable. It is needed for the Rabbit MQ software to operate correctly. After the installation is finished check if the variable **ERLANG_HOME** has been included in the register of the Windows environment variables.

Proceed to **This PC > Properties > Advanced System Settings > Environment Variables**. Search for the **ERLANG_HOME** variable.

ERLANG SYSTEM VARIABLE (CONTINUATION)

NOTE! If no variable is detected, create it manually. The value of the variable **ERLANG_HOME** must be a full path to the folder where the Erlang OTP has been installed (e.g. C:\Program Files\erl9.2)

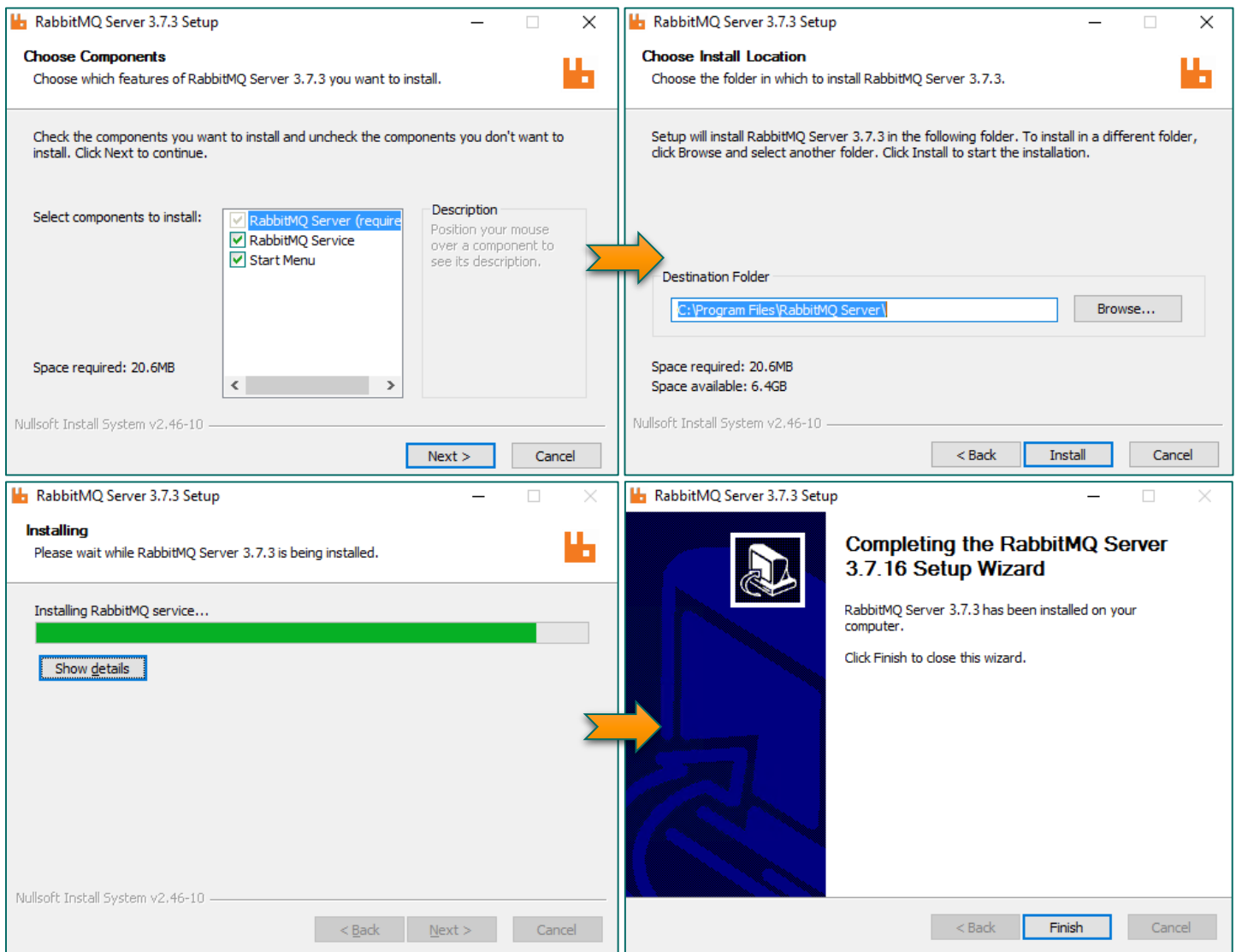


3. INSTALL RABBIT MQ

RabbitMQ is a messaging intermediary software that controls the interaction between different parts of application. The HTInstaller uses the RabbitMQ during the installation process. The RabbitMQ must be installed either on a separate server or on one of the servers of picked deployment schema.

NOTE! In case you already have RabbitMQ installed, skip the installation part, and proceed to the RabbitMQ configuration.

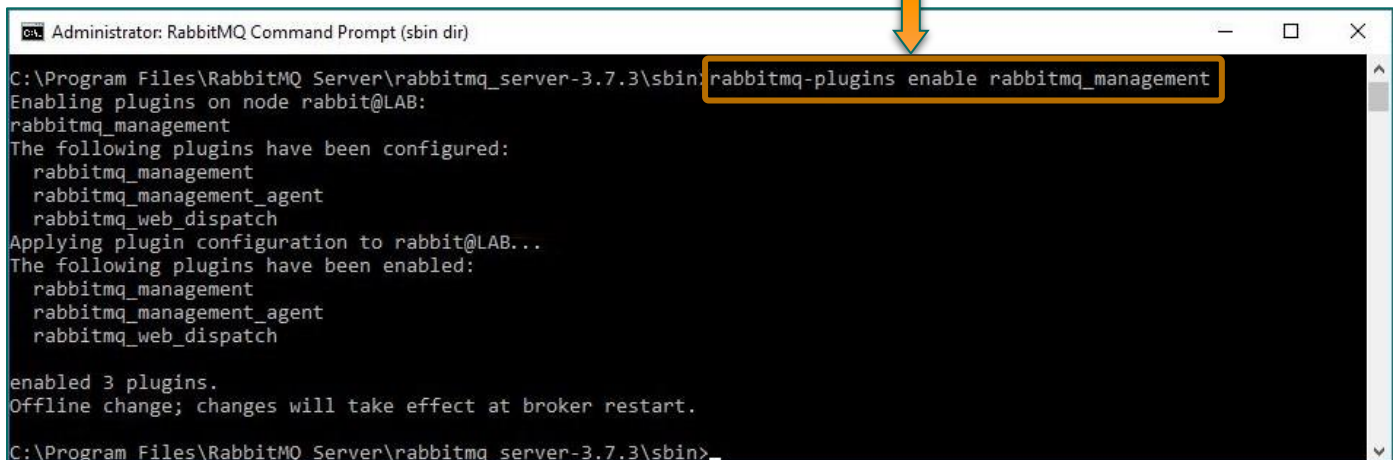
Find the RabbitMQ installation file in the package shipped along with the HTInstaller (path: archive **HTInstaller** > folder **Setup** > folder **Resources**). Copy it on the server where you installed the Erlang OTP component. Launch the installation executable file and follow the wizard commands as shown below:



INSTALL RABBITMQ PLUGINS

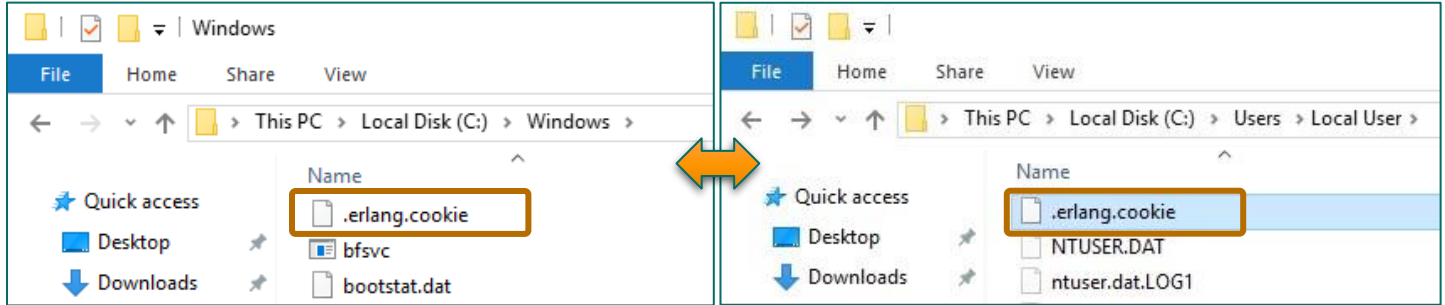
After the installation is complete, install the **RabbitMQ plugins**. Start the RabbitMQ Command Prompt and then execute the following command:

```
rabbitmq-plugins enable rabbitmq_management
```



ERLANG COOKIE FILE

The Rabbit MQ requires a specific **Erlang cookie file** put in the Windows root directory. Check if the file **.erlang.cookie** is located under the C:\Windows\:



NOTE! The .erlang.cookie is a hidden file. Change the view parameters to **Show hidden files, folder and drives** in the Folder settings to see the contents of the folder.

IMPORTANT! If the file .erlang.cookie is not detected in the Windows folder, copy it from the directory **Users**. File is located in the folder of the user account that installed the Erlang OTP component.

After the cookie file is verified to be in Windows directory, restart **RabbitMQ service**. The installation part is complete. You can proceed to the web interface of RabbitMQ to configure it properly.

RABBITMQ CONFIGURATION

RabbitMQ configuration requires all five above preparation steps completed:

1. Erlang OTP 20 component is installed.
2. Erlang variable persists in environment variables list.
3. RabbitMQ is installed.
4. RabbitMQ Plugins are installed.
5. Erlang cookie file is put in the Windows folder.

Proceed to the RabbitMQ portal and complete the configuration. To get to the RabbitMQ interface, open the browser and paste the URL: <http://localhost:15672/>. Log in using default credentials:

- **Username:** guest
- **Password:** guest



The RabbitMQ configuration requires creating a new user with administrator rights. This user will be used in the HTInstaller wizard during the installation. When in the RabbitMQ interface perform the following steps:

RabbitMQ 3.7.3 Erlang 20.2

Overview Connections Channels Exchanges Queues **Admin**

Users

▼ All users

Filter: ☐ Regex ?

Name	Can access virtual hosts	Has password
admin	/, Optimizer, SyncManager	•
guest	/	•

?

▼ Add a user

Username:

Password: (confirm)

Tags: ?

Set **Admin** | **Optimizer** | **Policymaker**
 Manage **Impersonator** | **None**

Add user

1. Press the tab **Admin** on the upper ribbon.
2. Go to **Add a user** section. Specify new RabbitMQ user credentials (e.g. username: admin, password: admin).
3. Add a tag **administrator** to the new user. Press **Admin** to set the tag. The tag grants the user administrator rights.
4. Press **Add user** button. New user populates the table in section **All users**.
5. Click on the new user name in the section **All users** to open the Set permission screen.

▼ Permissions

Current permissions

Virtual host	Configure regexp	Write regexp	Read regexp	
/	.*	.*	.*	Clear
Optimizer	.*	.*	.*	Clear
SyncManager	.*	.*	.*	Clear

Set permission

Virtual Host:

Configure regexp:

Write regexp:

Read regexp:

Set permission

6. Select / value from the dropdown **Virtual Host**.
7. Press **Set permission** button to save changes.
8. Repeat for **Optimizer** and **SyncManager** values in the dropdown **Virtual Host**. The **Current permissions** table has to have all three values.

This sequence of actions finalizes the RabbitMQ configuration. You can now quit the RabbitMQ interface. The server preparation is fully complete. You can proceed to the HTInstaller instructions to deploy the Hazeltree application.

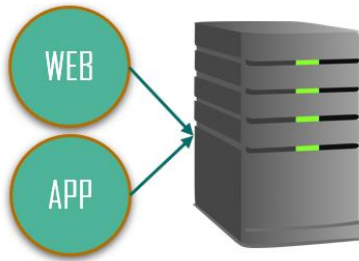
4. START THE HTINSTALLER

The HTInstaller must be used only after the servers are completely prepared, the system requirements are checked, and all the necessary software is installed on the servers. Depending on chosen deployment schema, the installation can involve either one server or multiple servers:

- [All-in-One](#): Combined Deployment on one server.
- [Multiple servers](#): Split Deployment / Multi-node Deployment: Two Servers / Multi-node Deployment: Four Servers.

The HTInstaller instructions vary basing on the chosen deployment type and how many servers are involved in the installation process.

ALL-IN-ONE INSTALLATION INSTRUCTIONS



Combined Deployment (or All-in-One Deployment) is a type of installation that assigns both **WEB** and **APP** roles of the Hazeltree application to one server. Therefore, all of the WEB and APP components are installed on one server. The database location does not change the deployment type: it can be deployed on the same server or on a segregated server.

If the All-in-One (Combined) type is chosen as a deployment plan, then follow the below instructions to install the Hazeltree application.

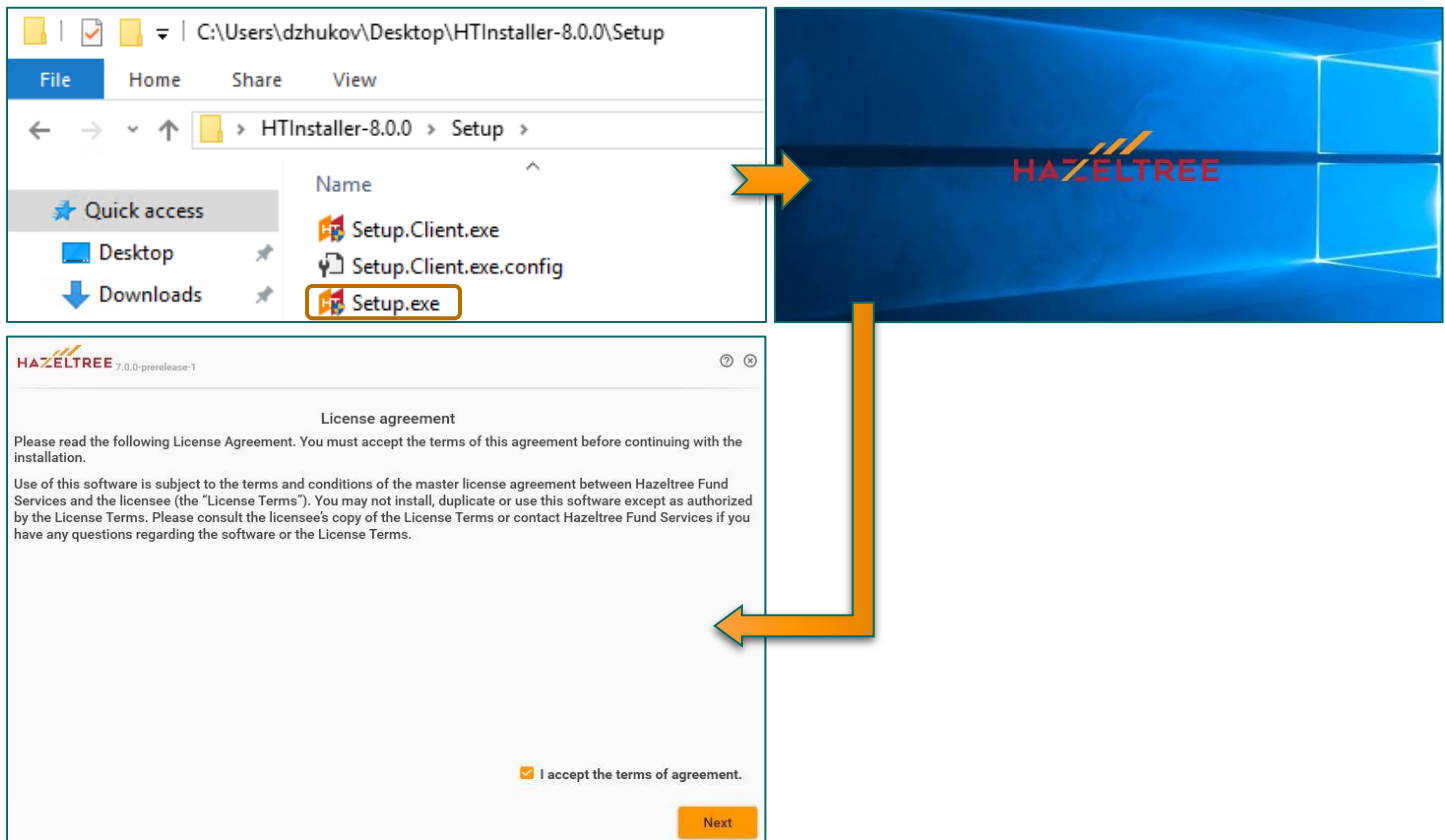
CHECK SERVER CAPACITY

The All-in-One concept is easier to plan and deploy with HTInstaller. However, the server that takes on **WEB** and **APP** responsibilities must be checked against the requirements for both roles. It is critical to verify that the server is powerful enough to process all operations for **WEB** and **APP** roles. Special treat must be applied in case the database is also deployed on this server.

1. HTINSTALLER SETUP AND LICENSE AGREEMENT

Deliver the HTInstaller package to the server that is planned to have both APP and WEB parts of the Hazeltree application. Unzip and then open the HTInstaller folder. Proceed to the subfolder **Setup**.

Launch the HTInstaller by double click on the Setup executable file. Read and accept the license agreement. Check the box **I accept the terms of agreement** and press **Next** to start the deployment process.



2. COMMON PARAMETERS & SYNC MANAGER PIPELINES PARAMETERS

Specify common parameters (Company information and Installation directories) and, if needed, Sync Manager pipeline parameters.

1. **Installation directory:** specify the folder for the Hazeltree installation.
2. **Feeds directory:** specify the folder for the incoming Feeds files. It can be changed any time later.
3. **Company Code:** a short code that represents the client’s company name. It is provided by the Hazeltree Support.
4. **FQDN:** Fully Qualified Domain Name for the Windows Active Directory (e.g. wayne.local).
5. **Sync Manage pipeline parameters:** switch on the pipeline feature and then specify Ports, Gateways Ports, and the URL of the custom server.

SYNC MANAGER PIPELINE FEATURE

Sync Manager® is a standalone product designed for supporting and managing the data, that is transported and processed in the Hazeltree application. The **Pipeline** feature allows users to sequentially process the files, store the tracking long of them, and display them in the user interface. To install the feature for the Hazeltree application, mark the **Enable** switch in on position and specify *Ports*, *Gateway Ports* and *custom server URL*.

3. INSTALLATION TYPE

Select the installation type. In All-in-One type of installation, one must pick the Combined deployment type.

6. **Installation type:** select the Combined Deployment installation type from the dropdown for All-in-One plan.
7. **Servers:** pool of servers of the selected All-in-One deployment schema.

DATABASE SERVER

The Combined Deployment implies that **APP** and **WEB** roles are installed on one server. The **DB** role can be assigned to the same server (therefore it combines all three roles) or it can be delegated to a segregated server. Either way, the location of the database does not impact the combination of the *Combined Deployment* installation type.

4. USER CREDENTIALS & OPTIONAL MODULES

Sign in with two prematurely created Active Directory users: first user runs Application services; the second user runs WEB sites. Then specify the optional modules for installation.

8. **User accounts log in:** sign in with two users (one that runs Application services, second that runs Web sites).
9. **Data Hub Client:** specify the incoming dataflow source: through Data Hub or directly from addressers.
10. **Mobile Gateway:** specify if the Hazeltree application can be accessed through the mobile API gateway.

Term: **Data Hub** is a specific mechanism in the Hazeltree environment that is responsible for processing and delivering data received from the clients' sources: brokers, accounting parties, banks, etc. The Data Hub allows to process sensitive information safely, keep the data in a secure vault and streamline the data feeding processes. The Data Hub operates through the preinstalled workflows embedded in **Sync Manager** standalone application.

DATA HUB CLIENT

The clients can seize upon the opportunity to redirect their dataflow through the Data Hub. This method is safer and faster than getting Feed files from the senders and processing them the regular way. Being the Data Hub client means that the data delivery to the endpoint will be executed and controlled by Hazeltree.

IMPORTANT! The clients deployed on the servers of Hazeltree have the configured workflows embedded in the Sync Manager; therefore, they start getting the data immediately. The on-premises clients must have the Sync Manager workflows reconfigured for the data to reach their endpoint. The reconfiguration is carried out by the Hazeltree Implementation Team.

5. NETWORK PARAMETERS

Specify the network parameters for the Internet and Intranet: protocols, addresses, external and internal ports, and SSL certificates if needed.

11. **Protocol:** select the combination of HTTP and HTTPS protocols for WEB Site, WEB API, and Mobile API access.
12. **WEB Site address:** specify the web address of the Hazeltree application site.
13. **External port:** specify the external port for the access to the WEB Site outside of the server.
14. **SSL Certificate:** select the SSL Certificate for the WEB Site access from the list of certificates installed on the server.
15. **WEB API address:** specify the web address of the WEB API access point.
16. **Internal port:** specify the internal port for the access to the WEB API.
17. **SSL Certificate:** select the SSL Certificate for the WEB API access from the list of certificates installed on the server.

COMBINATION OF PROTOCOLS

The HTTP protocols for WEB Site and API (WEB and Mobile) can be secured with SSL certificates. It is possible to establish HTTPS secure connections for all access points. Additionally, you can specify the secured connections selectively. Possible combinations are available in the Protocol dropdown:

- WEB Site: https
- WEB API: https
- WEB Site: http
- WEB API: http
- WEB Site: https
- WEB API: http

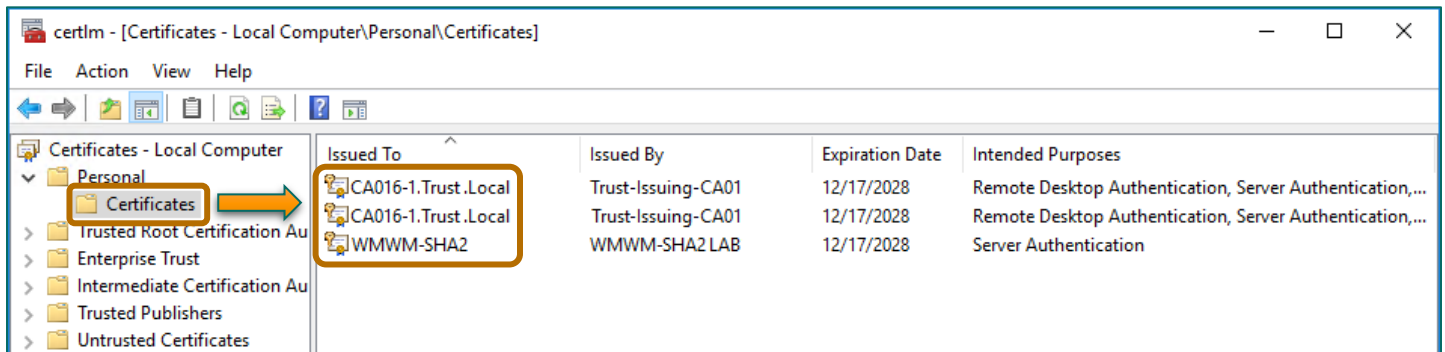
COMBINATION OF PROTOCOLS (CONTINUATION)

NOTE! The selection of any combination including HTTPS protocol activates the SSL Certificate dropdown fields on the HTInstaller screen. Based on the number of the HTTPS protocols in the selected combination, it can be one field (**WEB site SSL Certificate**), two fields (**WEB Site SSL Certificate** and **WEB API SSL Certificate**) or three fields (**WEB Site SSL Certificate**, **WEB API SSL Certificate**, and **Mobile API SSL Certificate**).

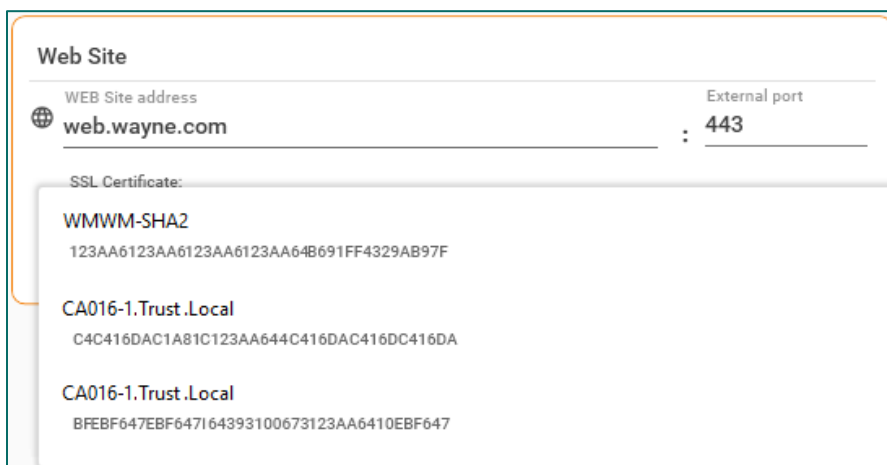
AVAILABLE PROTOCOLS ON THE SERVER

In case the combination of protocols includes a HTTPS protocol (either for WEB Site only or for both WEB Site and WEB API), the SSL Certificate dropdown fields appear in the corresponding sections. One has to select the required SSL certificate from the dropdown. The dropdown is automatically populated with the list of the SSL certificates installed on the server.

To make sure that the SSL Certificates are installed on the server and will become available in the HTInstaller wizard during the deployment, proceed to **Manage computer certificates** under the server **Control Panel**. Expand the folder **Personal** and open the subfolder **Certificates** to see the list of installed SSL certificates:



IMPORTANT! The HTInstaller does not recognize the SSL Certificates sitting in the folder **Web Hosting** (even for the WEB Site connectivity encryption). Therefore, make sure that the certificates you intend to utilize are placed in the **Personal** folder. The HTInstaller recognizes the SSL certificates automatically. It allows to select the required certificate from the dropdown field for Web Site, Web API and Mobile API sections:

**ON-PREMISES CERTIFICATES**

When the clients on Hazeltree servers are provided with the SSL certificates by default, the On-premises clients must have their own SSL certificates. In case you do not have any, make sure to issue the required number of SSL certificates with a help of a certified Trust center. Import the certificates to be able to select them in the HTInstaller wizard.

NOTE! The WEB site, WEB API and Mobile API must use different SSL Certificates released for three different URLs. However, the wildcard type SSL Certificate can be used for all access points simultaneously.

WEB SITE, WEB API & MOBILE API ADDRESSES AND PORTS

It is required to specify **WEB Site**, **WEB API** and **Mobile API** addresses' DNS names and ports. Specified ports must be prematurely opened in the server firewall. HTInstaller will automatically create sites in the IIS Manager and index proper bindings.

IMPORTANT!

In case the net infrastructure implies the Load Balancer server, specify the Load Balances DNS name and ports for both WEB site and API access. The ports must be prematurely opened in the Load Balancer firewall.

MOBILE API ACCESS

The Hazeltree provides clients with a mobile application that allows users to manage their voucher approvals. With a help of the mobile application a user with approver role can approve/reject transactions using remote access to the pending vouchers list. The mobile application works through the Mobile API connectivity point. It has to be turned on the screen **Select optional modules to install**. The Mobile API connection can be secured with the SSL certificate alike the WEB Site and WEB API connections:

Mobile API

Mobile API address

mobileapi.wayne.com

Internal port

9443

SSL Certificate:

WMWM-SHA2

13F993F99B13F990F123AA1313F91313F13F9913F99

6. DATABASE & RABBIT MQ PARAMETERS

Specify connectivity parameters to the database and the RabbitMQ parameters.

18. **Database server name of DNS:** specify the database server name. The database can be installed on the same APP/WEB server or on a segregated server. If the database is installed on the same APP/WEB server, then copy the APP/WEB server DNS name here.
19. **Use port switch:** turn on the switch to specify a port different from the default TCP SQL port (1433).
20. **Port:** specify the custom port when Use port switch is in “turned on” position.
21. **RabbitMQ server name or DNS:** specify the RabbitMQ server name. The RabbitMQ can be installed on the same APP/WEB server or on a segregated server. If the RabbitMQ is installed on the same APP/WEB server, then copy the APP/WEB server DNS name here.
22. **Management plugin port:** specify the port for the RabbitMQ web access (default value: 15672).
23. **Regular connections port:** specify the port for connection to the RabbitMQ application (default value: 5672).
24. **RabbitMQ Administrator account:** log in with the credentials of the RabbitMQ administrator.

DATABASE INSTANCES

The SQL server can work in two regimes: with instances and without instances, basing on the number of databases it contains. The database server DNS name depends on the regime:

- **With Instances:** specify the database instance in the DNS name (e.g. LAB007-DB007\DB01).
- **Without Instances:** specify solely the database DNS server name (e.g. LAB007-DB007).

USE PORT SWITCH

The HTInstaller uses the default TCP SQL port 1433 to connect to the database when the switch **Use port** is in off position. There are cases when the client’s infrastructure implies the database connectivity through a different port (mostly for security reasons). In this case, the installer can turn on the **Use port** switch and then specify a custom port:

NOTE! If the SQL server does have instances and the port is different from default, it is not mandatory to turn on specify this port. The service **SQL browser** will automatically pull the port from the DNS name.

IMPORTANT: POSSIBLE ISSUES!

Do not utilize the Use port switch in case the environment has a **dynamic ports** system. This will crush the deploy. The dynamics ports are pulled automatically by the **SQL browser** service.

IMPORTANT: POSSIBLE ISSUES!

Extreme accuracy and caution must be applied in case the database contains numerous instances. If you specify the correct DNS name of the database instance but with an incorrect port, the HTInstaller will refer to the instance which port you specified. This can corrupt existing neighboring database and lead to the irreversible data loss.

Always remember! The database port has priority over the database DNS name. This is a default design implemented by the Microsoft Corporation. Always check the port accuracy before utilizing the Use Port switch.

NOTE! In case the port has no references to other neighboring instances in the database, the deploy process will crush.

7. SSO PARAMETERS

Specify Single Sign-On parameters and two-factor authentication parameters if needed.

HAZELTREE 8.0.0

Specify SSO parameters

Cookie Expiration In Minutes: 25

Cookie Same Site Strict Policy: Lax (26)

Authentication Mode: Duo (27)

Duo parameters (28):

- Host: wayne.duo.com
- Integration key: [redacted]
- Application key: [redacted]
- Secret key: [redacted]

Back Next

25. **Cookie Expiration Time:** specify the user session expiration time in minutes.

26. **Cookie Same Site Strict Policy:** select the cookie policy: none, lax or strict.

27. **Authentication Mode:** select the authentication mode (none or two-factor DUO authentication).

28. **Duo parameters:** specify the parameters for two-factor DUO authentication: Host, Integration key, Application key, Secret key.

TWO FACTOR DUO AUTHENTICATION

The HTInstaller provides with opportunity to establish a secure two-factor authentication with the DUO company. To establish the two-factor authentication the user must specify the following parameters:

All parameters required for DUO activation can be found in the DUO account. In case you do not have a DUO account but still need the two-factor authentication, create the DUO account prematurely.

In case the two-factor authentication is not selected, the authentication mode will be automatically set to **None** value.

8. PROXY PARAMETERS

Specify the proxy server parameters: host, port, bypass addresses, etc.

29. **Enable proxy switch**: turn on the switch to identify if there is a proxy server in your infrastructure.

30. **Proxy host**: specify the proxy server host IP address or DNS name.

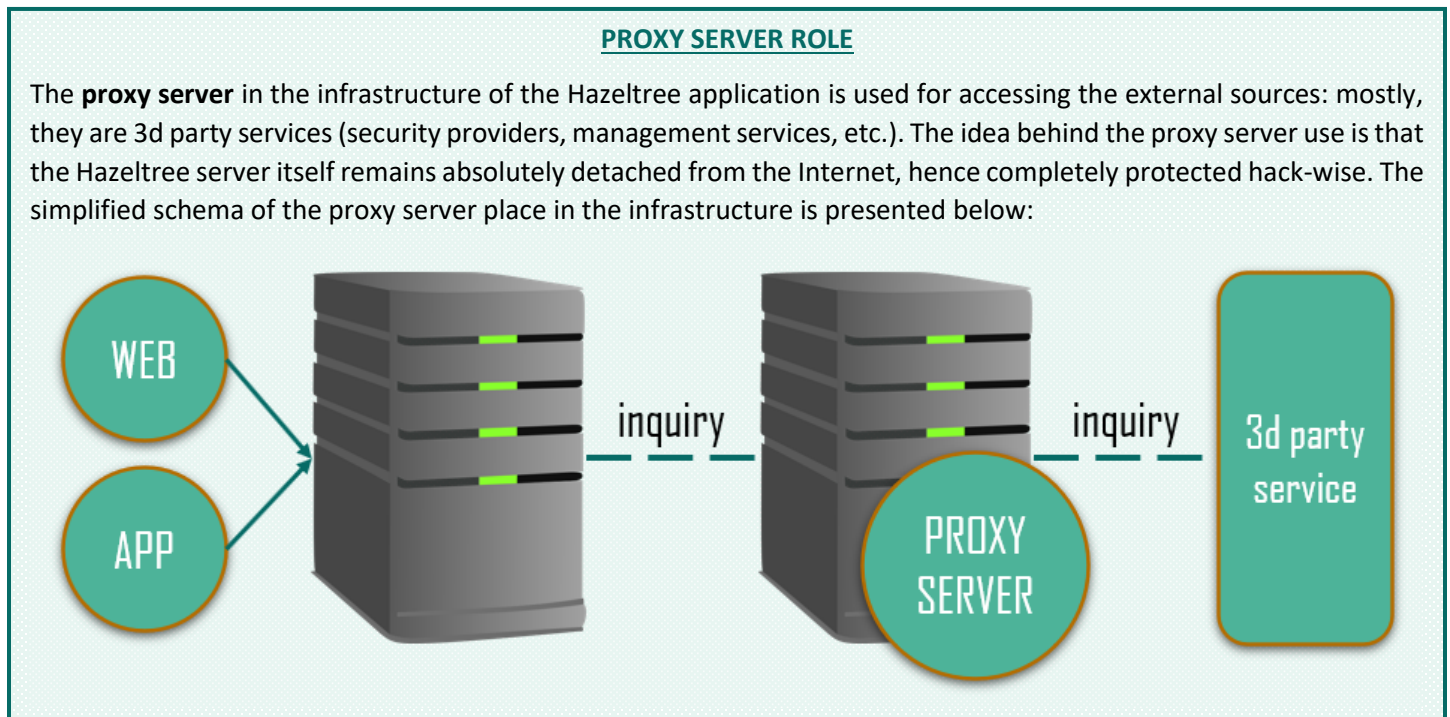
31. **Port**: specify the port for connection to the proxy server.

32. **Proxy settings**: set up the proxy server settings by checking/leaving blank the proxy server parameters.

33. **Enable Bypass proxy for local addresses switch**: turn on the switch to identify the list of local addresses that can be accessed passing over the proxy server.

34. **Bypass addresses**: list of local addresses that can be accessed passing over the proxy server.

35. **Add bypass address:** type in the IP address or DNS name of the bypass local address and hit plus icon to add it to the list.



9. EMAIL PARAMETERS

Specify the email server settings and email user account credentials if needed.

HAZELTREE 8.0.0

Specify Email parameters

Email server settings

36

From Address

mail@wayne.com

SMTP Host

smtp.wayne.com

Port

25

Use SSL

☒

Use email user account

37

☐

Email user account

38

Username

bruce.wayne@wayne.com

Password

••••••

Back

Next

36. **Email server settings:** specify the email server settings: From address, SMTP Host, port, and SSL encryption.

37. **Use email user account switch:** turn on the switch to designate the account of the email sender.

38. **Email user account credentials:** type in the sender credentials to verify the sender's mailbox on the SMTP server.

EMAIL SERVER

The **email server** is used to send out the email using the SMTP protocol. The From Address specified in the Email server settings section will always be the sender email address. The personal mailbox can be used for authentication purposes (specifically if the SMTP connectivity is encrypted with the SSL protocol).

10. EXTERNAL DEPENDENCIES PARAMETERS

Specify the external dependencies (Security hub, Operations Manager, Caching system, etc.) and their parameters.

HAZELTREE 8.5.0-rc.49e8a47

Specify external dependencies parameters

Security Hub

Url **39**
https://qa-sechub:8412/

Client secret
MT-Wayne-PROD01

Operations Manager

Url **40**
https://qa-sechub:8417/

Client secret
&Yut4hw97cfn9P&4hch4p9H\$ &g4pf

Environment

Short Name **41**
MT-Wayne-PROD01

Caching

☒ Enabled **42**

Source Type **43**
redis ignite

Caching location (connection string) **44**
cache1-prd,ssl=true,abortconnect=false,defaultDatabase=99

External Data

☒ Enabled **45**

Source Type **46**
redis ignite

External Data Location (connection string) **47**
cache1-prd,ssl=true,abortconnect=false,defaultDatabase=99

Back Next

39. **Security Hub:** in case you utilize a Security Hub (Hazeltree or third-party) type in the Security Hub URL.
40. **Operations Manager:** external public API access point (*in development*).
41. **Environment:** if you the Redis included in the environment, specify the short name of the Redis data block identifier.
42. **Caching:** flag the checkbox if you want to enable the caching process for the Hazeltree application.
43. **Source Type:** select the caching system (*redis* or *ignite*) to integrate with Hazeltree application.
44. **Caching Location:** specify the connection string of the selected Caching system.
45. **External Data:** flag the checkbox if you want to enable cache data export for Hazeltree application.
46. **Source Type:** select the caching system (*redis* or *ignite*) to integrate with Hazeltree application.
47. **External Data Location:** specify the connection string of the external cache data management system.

REDIS / IGNITE INTEGRATION

To significantly reduce the data loading time, the design of the Hazeltree application can be expanded with the third-party services that allows to cache the latest inquiry data. There are two services that can be integrated with Hazeltree application: **Redis** and **Ignite**.

Term: **Redis** is a third-party in-memory data structure service that implements a distributed in-memory database accessed on the key-value basis. The Redis database has optional durability.

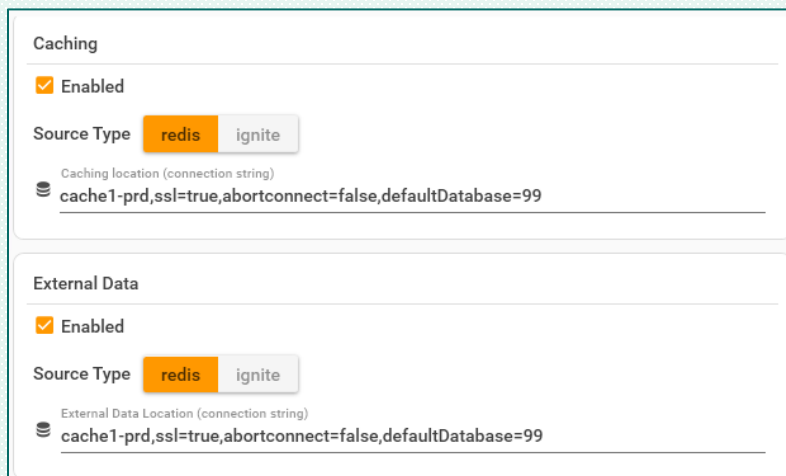
Term: **Ignite** is a third-party in-memory data structure service that features an in-memory computing platform which includes an in-memory data grid, in-memory database, and streaming analytics.

REDIS / IGNITE 411

The Hazeltree application refers directly to the database and retrieves the inquired data when the Web site form sends inquiries for an update or page refresh. The data transition to the endpoint occupies time proportional to the volume of the inquired data. The inclusion of the caching service (Redis or Ignite) significantly reduces the loading time: once the data is transferred to the Hazeltree application, it is cached in the external outsource service. Therefore, the next user inquires will receive the data from the Redis or Ignite cache.

To implement the caching system into the Hazeltree structure, client must specify the following parameters in the HTInstaller wizard:

- **Environment:** the identifier of the Redis data block referring to installed environment.
- **Caching Location:** the connection string to the local cache vault.
- **External Data Location:** the connection string to the external data cache vault.



The screenshot shows the HTInstaller wizard configuration for Caching and External Data. The Caching section has a checkbox for 'Enabled' which is checked, and a 'Source Type' dropdown menu with 'redis' selected. Below this is a text field for 'Caching location (connection string)' containing the value 'cache1-prd,ssl=true,abortconnect=false,defaultDatabase=99'. The External Data section also has a checkbox for 'Enabled' which is checked, and a 'Source Type' dropdown menu with 'redis' selected. Below this is a text field for 'External Data Location (connection string)' containing the same value 'cache1-prd,ssl=true,abortconnect=false,defaultDatabase=99'.

11. STATISTICS COLLECTION PARAMETERS

Specify the Statistics Collection parameters for the Elastic Search engine.

The screenshot shows the HazelTree 9.0.6 configuration window titled "Specify Statistics Collection parameters". It features a toggle switch for "Statistics Collection Enabled" which is turned on. Below this is a text input field for "Elastic Search Uri" containing the URL "https://elst-qa0198/-PROD01". At the bottom are "Back" and "Next" buttons.

HAZELTREE 9.0.6

Specify Statistics Collection parameters

☒ Statistics Collection Enabled

Elastic Search Uri
https://elst-qa0198/-PROD01

Back Next

48. **Statistics Collection Enabled**: switch the setting to turn on the gathering of statistics data by the Elastic engine.

49. **Elastic Search Uri**: specify the link to the Elastic Search engine.

12. LOGGING & TRACING PARAMETERS

Specify the Elastic Search parameters for tracking the Hazeltree application logs.

The screenshot shows the HazelTree 8.5.0-rc.49e8a47 configuration window titled "Specify Logging and Tracing parameters". It contains two sections. The first section, "Elastic Search Enabled", has a toggle switch turned on and includes a text input for "Elastic Search Uri" with the value "https://elstc-qa0198-PROD01". The second section, "OpenTracing Enabled", has a toggle switch turned on. At the bottom are "Back" and "Next" buttons.

HAZELTREE 8.5.0-rc.49e8a47

Specify Logging and Tracing parameters

☒ Elastic Search Enabled

Elastic Search Uri
https://elstc-qa0198-PROD01

☒ OpenTracing Enabled

Back Next

- 50. **Elastic Search engine parameters:** a no-sql database oriented on the full-text search that vaults the logs produced with the Hazeltree application.
- 51. **Elastic Search Url:** the URL link to the Elastic Search engine that is put to the Hazeltree configuration file in order to direct the log stream to the Elastic vault.
- 52. **Kibana Uri:** a web user interface that allows to conveniently read the logs stored within the Elastic Search.
- 53. **Open Tracing:** : a switch that allows to change the tracing mode to **(Open) Enabled**.

13. OCTOPUS DEPLOY SERVER PARAMETERS

Specify the Octopus server parameters: Administrator account, installation directories, ports, etc.

HAZELTREE 8.0.0

Specify Octopus Deploy Servers parameters

Administrator account

Octopus admin username
admooctopus

Octopus admin user password

Installation directories

Installation directory for Octopus Deploy Server
C:\Program Files\Octopus\Server

Installation directory for Octopus Deploy Tentacle
D:\Apps\Octopus\Tentacle

Instance directory
C:\Program Files\Octopus\Instance

ADVANCED

Back Next

Advanced

Server port
80

Listen port
10944

Tentacle port
10933

☒ Drop Server instance if exists

- 54. **Octopus Administrator account:** type in with the Octopus administrator credentials.
- 55. **Installation directories:** specify the installation directories of the Octopus Deploy Server, Tentacle, and Instance.
- 56. **Server port:** specify the Octopus server port (default value: 80).
- 57. **Listen port:** : specify the Octopus listen port (default value: 10944).
- 58. **Tentacle port:** specify the Octopus tentacle port (default value: 10933).
- 59. **Drop Server instance if exists:** flag the checkbox in case the Hazeltree application is already installed on the server.

Term: **Octopus** is a third-party deployment and release management system that is designed to automate complex deployments.

OCTOPUS ADMINISTRATOR ACCOUNT

To initiate a deploy, the HTInstaller must authenticate itself as the Octopus Administrator. Insert the administrator credentials if you already have an Administrator account. In case the Administrator account is not created, specify random username and password. The HTInstaller wizard creates the Administrator account automatically.

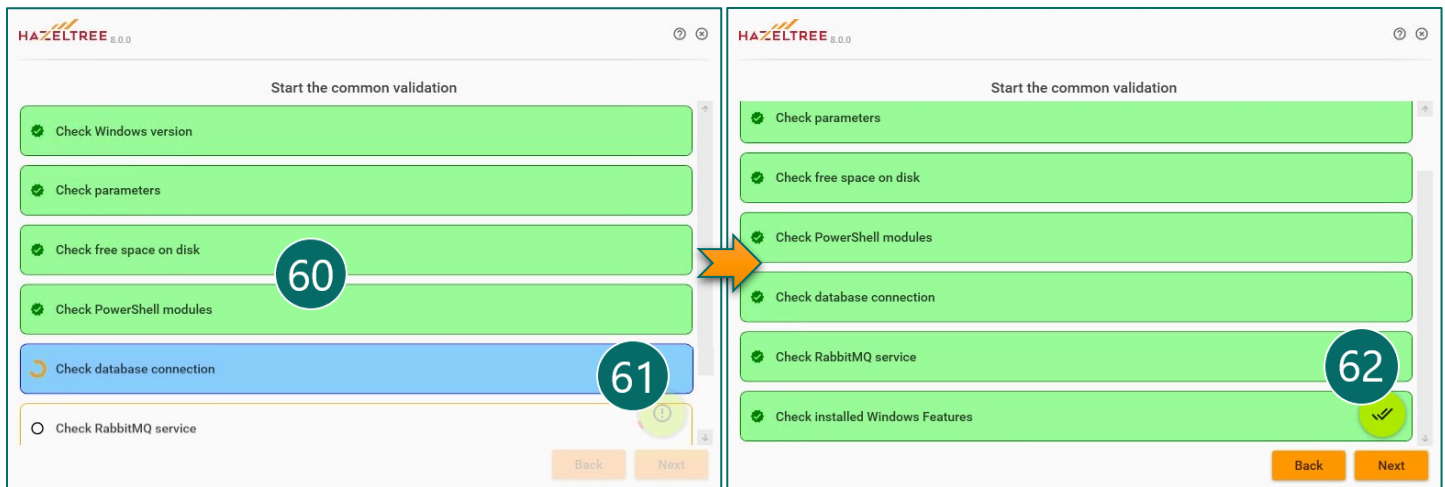
DROP SERVER INSTANCE IF EXISTS

The checkbox **Drop Server instance if exists** must be checked if the network parameters, specified previously, included the HTTPS protocol for any of the access points (WEB site, WEB API, Mobile API). The checkbox is always checked by default.

NOTE! Dropping the Server instance does not erase any data from the database.

14. COMMON VALIDATION

Start the common validation of the deployment components and check the result.



60. **Validation tests:** list of the validation tasks that the HTInstaller checks against system requirements.

61. **Start validation tests:** press the button to start the validations tests.

62. **Validation result:** passed validation sign turns green and activates the Next button. In case of failed tests, the exclamation mark is displayed on the sign. Fix the errors and repeat the validation tests.

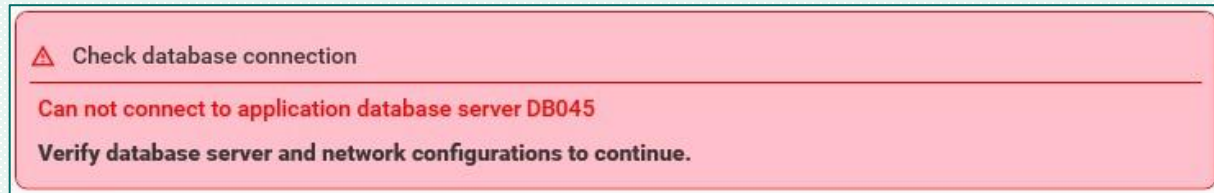
FAILED VALIDATION TESTS

During the common validation step, the tests can fail. The failure of the test means that the system requirement is not complied, and the subsequent deployment cannot be started. The failed test is complimented with the error text that allows to disclose the issue root and operatively eliminate it.

See the example on the next page:

EXAMPLE

During the common validation step, the test **Check database connection** has failed with an error: **Cannot connect to application database server**:



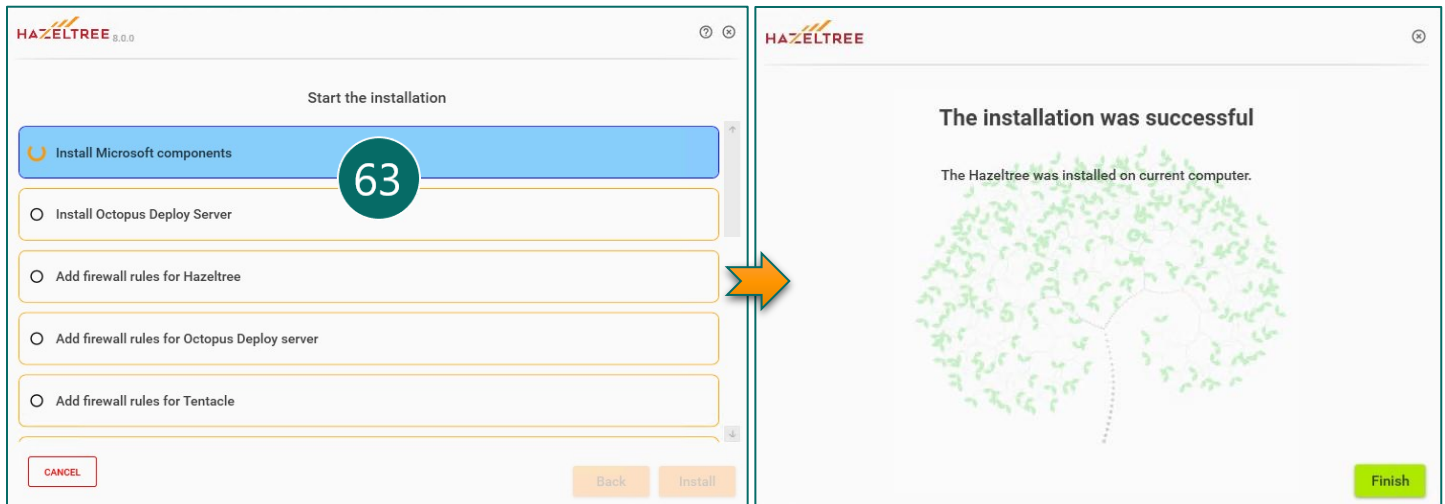
The basic possible issues behind this error are well-known:

- User put an incorrect database URL or instance in the HTInstaller wizard.
- User put an incorrect port in the HTInstaller wizard.
- The port is closed on the database server.
- The database server is down.
- The database or instance is not created.
- Proper permissions are not delegated to the user, the operator of the HTInstaller.

Check the HTInstaller specified parameters and the database server to troubleshoot the issue, fix it and run the common validation routine again.

15. INSTALLATION PROCESS

Proceed to the deployment process: start the installation and wait upon its completion.

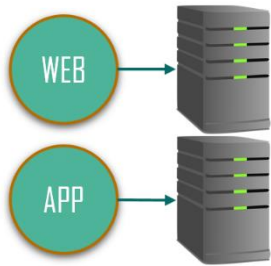


63. Installation steps: check the installation steps displayed on the HTInstaller wizard screen. Successful installation will be followed with the message **The installation was successful**. Click Finish to exit HTInstaller wizard.

INSTALLATION PROCESS REVIEW

Users can review the installation process with detailed logs from the Octopus web interface. To open the Octopus web page, proceed to the URL: [http://\[serverURL\]:80/HTInstaller](http://[serverURL]:80/HTInstaller). Log in with Administrator credentials and review the installation process from there.

MULTI-NODE INSTALLATION INSTRUCTIONS



Multiple servers Deployment (or **Multi-node Deployment**) is a type of installation that implies distributing the **WEB** and **APP** roles of the Hazeltree application to several servers. The roles schema can be designed in various combinations. Identical to the All-in-One Deployment plan the database location not change the deployment type: it can be deployed on any server of the schema or on a segregated server.

The Multi-node Deployment routine follows a similar routine of the HTInstaller wizard with several additional actions.

The Multi-node Deployment plan has three options:

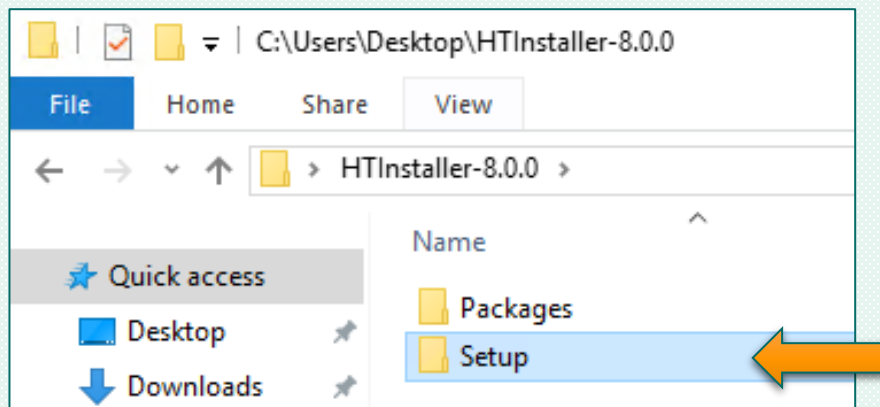
- **Split Deployment:** separate servers for WEB and APP roles.
- **Multi-node Deployment (Two Servers):** two separated servers both given WEB and APP roles.
- **Multi-node Deployment (Four Servers):** four separated servers: two WEB roles and two APP role servers.

CHECK SERVERS CAPACITY

The Multi-node Deployment requires good planning and accurate treatment of all servers included in the selected schema. All servers must be checked against the system requirements of their roles. In case of **Multi-node Deployment (Two Servers)** plan, the **APP** and **WEB** roles are assigned to both servers simultaneously. It is critical to verify that all servers are powerful enough to process all operations for WEB and APP roles. Special treat must be applied in case the database is also deployed on one of these servers.

COPY SETUP FOLDER

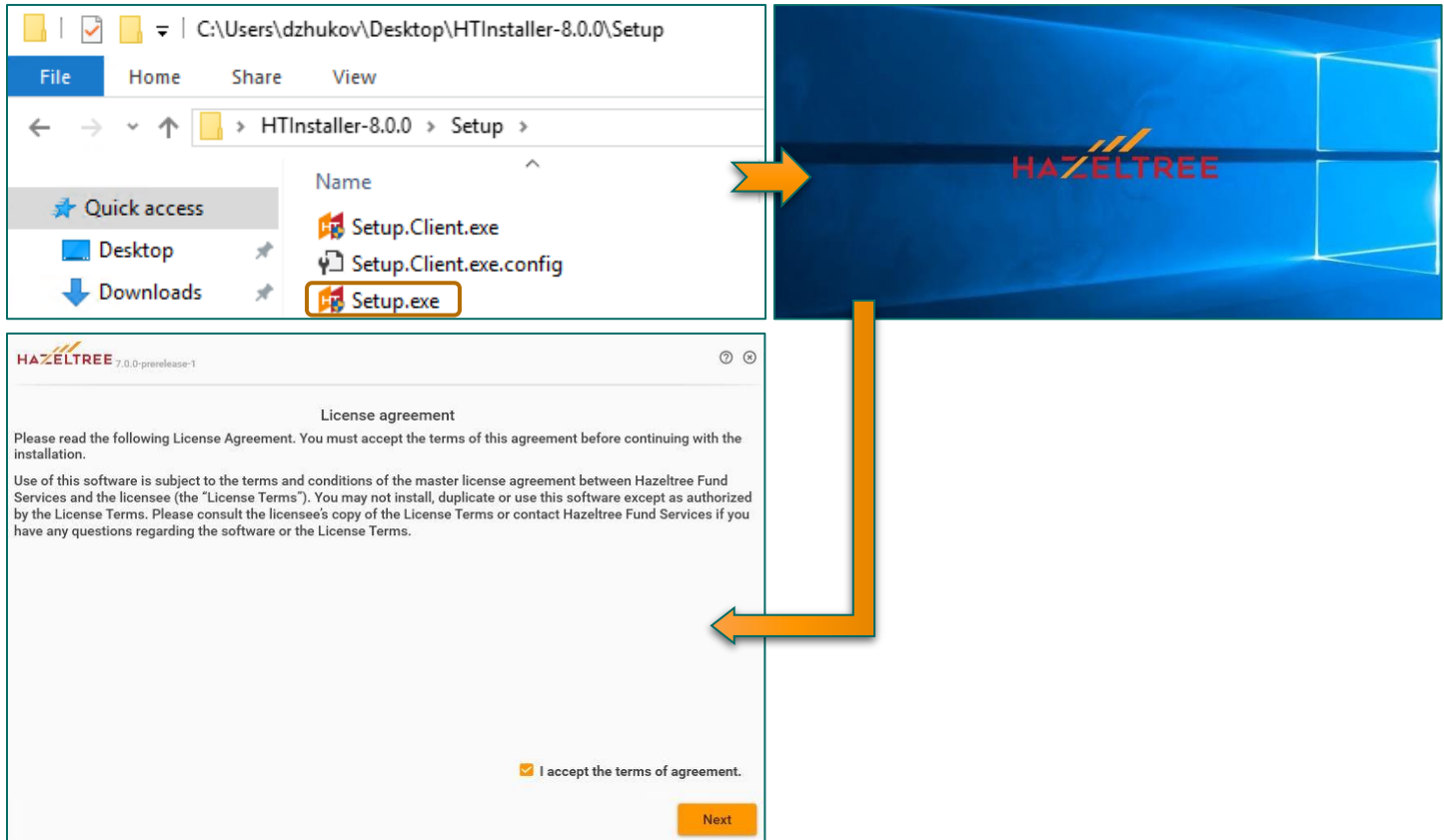
An extra action must be performed before conducting the deployment with the HTInstaller wizard. Copy the folder **Setup** from the HTInstaller archive to the rest of the servers included in the chosen schema. For example, if the **Split Deployment** plan is selected, copy the Setup folder to the second server:



1. HTINSTALLER SETUP AND LICENSE AGREEMENT

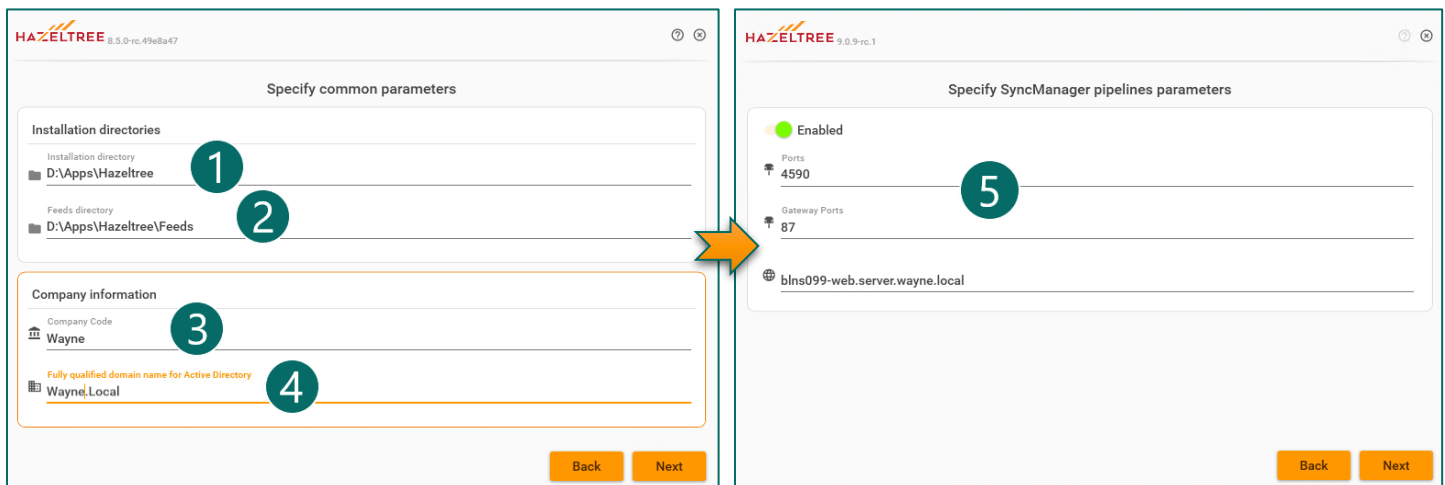
Deliver the HTInstaller package to the server that is planned to have both APP and WEB parts of the Hazeltree application. Unzip and then open the HTInstaller folder. Proceed to the subfolder **Setup**.

Launch the HTInstaller by double click on the Setup executable file. Read and accept the license agreement. Check the box **I accept the terms of agreement** and press **Next** to start the deployment process.



2. COMMON PARAMETERS & SYNC MANAGER PIPELINES PARAMETERS

Specify common parameters (Company information and Installation directories) and, if needed, Sync Manager pipeline parameters.



1. **Installation directory:** specify the folder for the Hazeltree installation.

2. **Feeds directory:** specify the folder for the incoming Feeds files. It can be changed any time later.
3. **Company Code:** a short code that represents the client's company name. It is provided by the Hazeltree Support.
4. **FQDN:** Fully Qualified Domain Name for the Windows Active Directory (e.g. wayne.local).
5. **Sync Manage pipeline parameters:** switch on the pipeline feature and then specify Ports, Gateways Ports, and the URL of the custom server.

SYNC MANAGER PIPELINE FEATURE

Sync Manager® is a standalone product designed for supporting and managing the data, that is transported and processed in the Hazeltree application. The **Pipeline** feature allows users to sequentially process the files, store the tracking long of them, and display them in the user interface. To install the feature for the Hazeltree application, mark the **Enable** switch in on position and specify *Ports*, *Gateway Ports* and *custom server URL*.

3. INSTALLATION TYPE

Select the installation type. In Multi-node type of installation, one can pick one of three available options from the dropdown.

HAZELTREE 8.0.0

Specify installation type

Installation type

6

Split Deployment
Separate servers for WEB and APP roles.

Servers:

APP **current computer**

WEB

7 DB

Back Next

6. **Installation type:** select one of the multi-node deployment schemas from the dropdown.
7. **Servers:** pool of servers of the selected multi-node deployment schema. The schema shows all presumed server with indication of the current computer.

DATABASE SERVER

The Multi-node Deployment plan implies distribution of the **APP** and **WEB** roles amongst numerous servers. The **DB** role can be assigned to any of the servers of chosen schema (therefore it combines two or three roles) or it can be delegated to a segregated server. Either way, the location of the database does not impact the selected installation type.

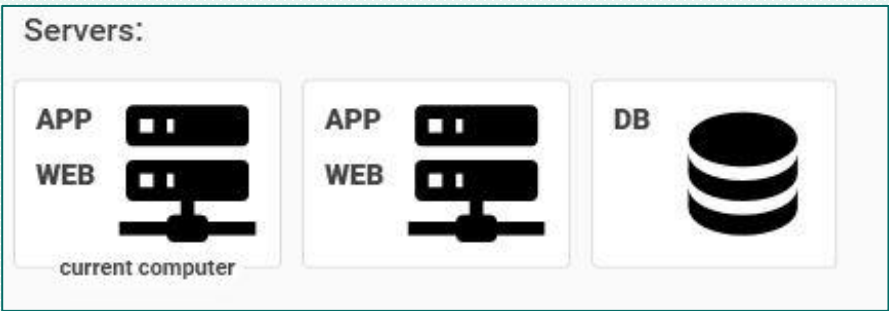
DEPLOYMENT SCHEMAS

The Multi-node Deployment can be implemented in three possible combinations or **APP** and **WEB** servers. Review the options below:

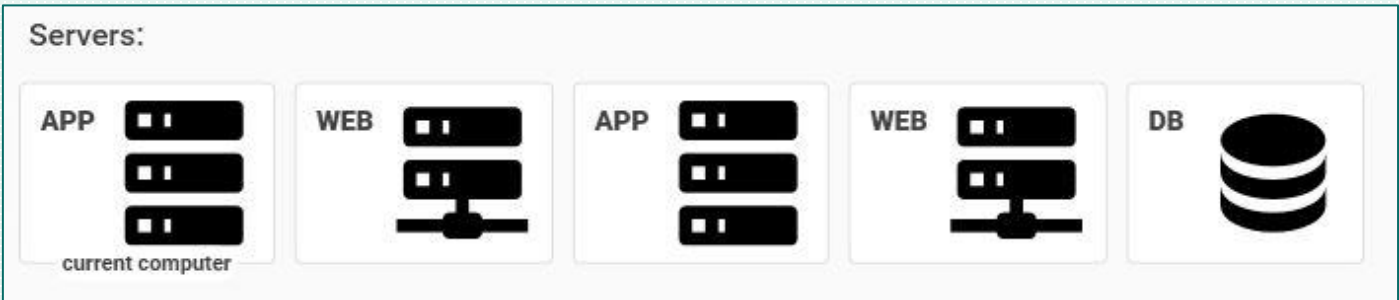
• Split Deployment:



• Multi-node Deployment (two servers):



• Multi-node Deployment (four servers):



3. USER CREDENTIALS & OPTIONAL MODULES

Sign in with two prematurely created Active Directory users: first user runs Application services; the second user runs WEB sites. Then specify the optional modules for installation.

8. **User accounts log in:** sign in with two users (one that runs Application services, second that runs Web sites).

9. **Data Hub Client:** specify the incoming dataflow source: through Data Hub or directly from addressers.

10. **Mobile Gateway:** specify if the Hazeltree application can be accessed through the mobile API gateway.

Term: **Data Hub** is a specific mechanism in the Hazeltree environment that is responsible for processing and delivering data received from the clients' sources: brokers, accounting parties, banks, etc. The Data Hub allows to process sensitive information safely, keep the data in a secure vault and streamline the data feeding processes. The Data Hub operates through the preinstalled workflows embedded in the Sync Manager standalone application.

DATA HUB CLIENT

The clients can seize upon the opportunity to redirect their dataflow through the Data Hub. This method is safer and faster than getting Feed files from the senders and processing them the regular way. Being the Data Hub client means that the data delivery to the endpoint will be executed and controlled by Hazeltree.

IMPORTANT! The clients deployed on the servers of Hazeltree have the configured workflows embedded in the Sync Manager; therefore, they start getting the data immediately. The on-premises clients must have the Sync Manager workflows reconfigured for the data to reach their endpoint. The reconfiguration is carried out by the Hazeltree Implementation Team.

MOBILE GATEWAY

The **Mobile gateway** switch determines if the Hazeltree application will be exposed to the Mobile API access. It is required if the client utilizes the Hazeltree mobile application.

INFO! The Hazeltree provides clients with a mobile application that allows users to manage their voucher approvals. With a help of the mobile application the user with an approver role can approve/reject transactions operatively using remote access to the pending vouchers list. The mobile application works through the Mobile API connectivity point which is the Mobile gateway.

4. NETWORK PARAMETERS

Specify the network parameters for the Internet and Intranet: protocols, addresses, external and internal ports, and SSL certificates if needed.

HAZELTREE 8.0.0

Specify network parameters

Protocol 11

- WEB Site: https
- WEB API: https

Web Site

WEB Site address 12 : External port 13 443

SSL Certificate: 14

WMWM-SHA2

D6E91E9139132430F123AE913B6E913432E91313

Web API

WEB API address 15 : Internal port 16 8443

SSL Certificate: 17

WMWM-SHA2

EE9133F9E913243EE913AE913E913E91329AE913

Back Next

11. **Protocol:** select the combination of HTTP and HTTPS protocols for WEB Site, WEB API, and Mobile API access.
12. **WEB Site address:** specify the web address of the Hazeltree application site.
13. **External port:** specify the external port for the access to the WEB Site outside of the server.
14. **SSL Certificate:** select the SSL Certificate for the WEB Site access from the list of certificates installed on the server.
15. **WEB API address:** specify the web address of the WEB API access point.
16. **Internal port:** specify the internal port for the access to the WEB API.
17. **SSL Certificate:** select the SSL Certificate for the WEB API access from the list of certificates installed on the server.

COMBINATION OF PROTOCOLS

The HTTP protocols for WEB Site and API (WEB and Mobile) can be secured with SSL certificates. It is possible to establish HTTPS secure connections for all access points. Additionally, you can specify the secured connections selectively. Possible combinations are available in the Protocol dropdown:

- WEB Site: https
- WEB API: https
- WEB Site: http
- WEB API: http
- WEB Site: https
- WEB API: http

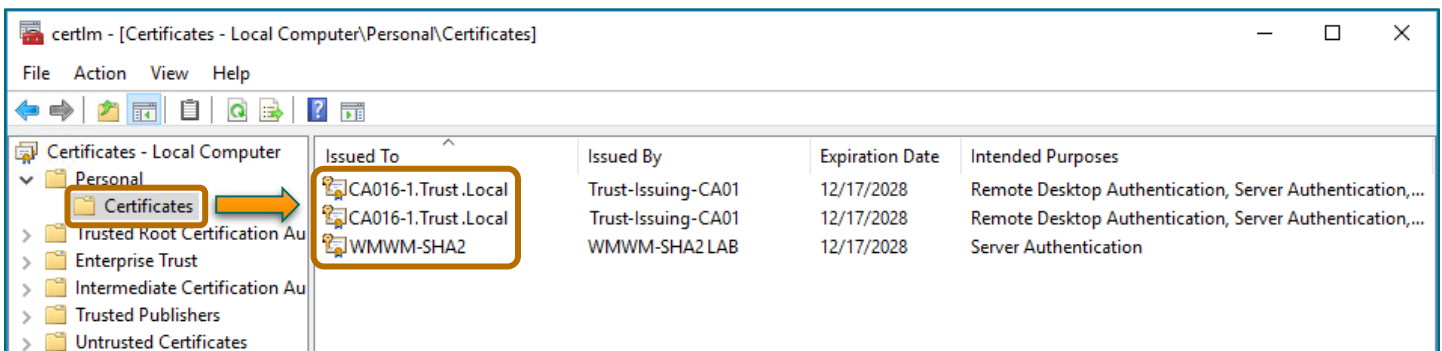
COMBINATION OF PROTOCOLS (CONTINUATION)

NOTE! The selection of any combination including HTTPS protocol activates the SSL Certificate dropdown fields on the HTInstaller screen. Based on the number of the HTTPS protocols in the selected combination, it can be one field (**WEB site SSL Certificate**), two fields (**WEB Site SSL Certificate** and **WEB API SSL Certificate**) or three fields (**WEB Site SSL Certificate**, **WEB API SSL Certificate**, and **Mobile API SSL Certificate**).

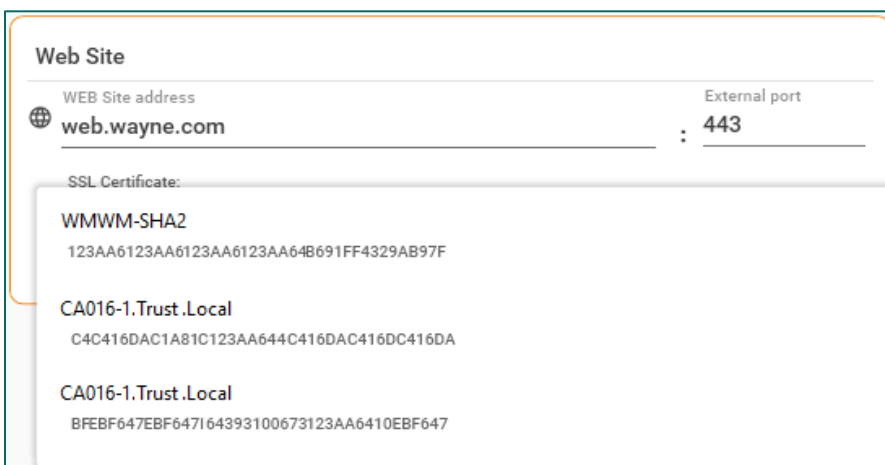
AVAILABLE PROTOCOLS ON THE SERVER

In case the combination of protocols includes a HTTPS protocol (either for WEB Site only or for both WEB Site and WEB API), the SSL Certificate dropdown fields appear in the corresponding sections. One has to select the required SSL certificate from the dropdown. The dropdown is automatically populated with the list of the SSL certificates installed on the server.

To make sure that the SSL Certificates are installed on the server and will become available in the HTInstaller wizard during the deployment, proceed to **Manage computer certificates** under the server **Control Panel**. Expand the folder **Personal** and open the subfolder **Certificates** to see the list of installed SSL certificates:



IMPORTANT! The HTInstaller does not recognize the SSL Certificates sitting in the folder **Web Hosting** (even for the WEB Site connectivity encryption). Therefore, make sure that the certificates you intend to utilize are placed in the **Personal** folder. The HTInstaller recognizes the SSL certificates automatically. It allows to select the required certificate from the dropdown field for Web Site, Web API and Mobile API sections:

**ON-PREMISES CERTIFICATES**

When the clients on Hazeltree servers are provided with the SSL certificates by default, the On-premises clients must have their own SSL certificates. In case you do not have any, make sure to issue the required number of SSL certificates with a help of a certified Trust center. Import the certificates to be able to select them in the HTInstaller wizard.

NOTE! The WEB site, WEB API and Mobile API must use different SSL Certificates released for three different URLs. However, the wildcard type SSL Certificate can be used for all access points simultaneously.

WEB SITE, WEB API & MOBILE API ADDRESSES AND PORTS

It is required to specify **WEB Site**, **WEB API** and **Mobile API** addresses' DNS names and ports. Specified ports must be prematurely opened in the server firewall. HTInstaller will automatically create sites in the IIS Manager and index proper bindings.

IMPORTANT!

In case the net infrastructure implies the Load Balancer server, specify the Load Balances DNS name and ports for both WEB site and API access. The ports must be prematurely opened in the Load Balancer firewall.

MOBILE API ACCESS

The Hazeltree provides clients with a mobile application that allows users to manage their voucher approvals. With a help of the mobile application a user with approver role can approve/reject transactions using remote access to the pending vouchers list. The mobile application works through the Mobile API connectivity point. It has to be turned on the screen **Select optional modules to install**. The Mobile API connection can be secured with the SSL certificate alike the WEB Site and WEB API connections:

Mobile API

Mobile API address

mobileapi.wayne.com

Internal port

: 9443

SSL Certificate:

WMWM-SHA2

13F993F99B13F990F123AA1313F91313F13F9913F99

5. DATABASE & RABBIT MQ PARAMETERS

Specify connectivity parameters to the database and the RabbitMQ parameters.

HAZELTREE 8.0.0

Specify database parameters

Database

Database server name or DNS

DB004\DB4

18

Use port:

19

port

60408

20

Specify RabbitMQ parameters

RabbitMQ server

RabbitMQ server name or DNS

LAB1

21

Management plugin port

15672

22

Regular connections port

5672

23

RabbitMQ Administrator account

Username

admin

24

Password

.....

SIGN IN

Back

Next

18. **Database server name of DNS:** specify the database server name. The database can be installed on the same APP/WEB server or on a segregated server. If the database is installed on the same APP/WEB server, then copy the APP/WEB server DNS name here.
19. **Use port switch:** turn on the switch to specify a port different from the default TCP SQL port (1433).
20. **Port:** specify the custom port when Use port switch is in “turned on” position.
21. **RabbitMQ server name or DNS:** specify the RabbitMQ server name. The RabbitMQ can be installed on the same APP/WEB server or on a segregated server. If the RabbitMQ is installed on the same APP/WEB server, then copy the APP/WEB server DNS name here.
22. **Management plugin port:** specify the port for the RabbitMQ web access (default value: 15762).
23. **Regular connections port:** specify the port for connection to the RabbitMQ application (default value: 5672).
24. **RabbitMQ Administrator account:** log in with the credentials of the RabbitMQ administrator.

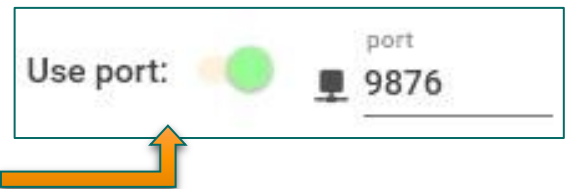
DATABASE INSTANCES

The SQL server can work in two regimes: with instances and without instances, basing on the number of databases it contains. The database server DNS name depends on the regime:

- **With Instances:** specify the database instance in the DNS name (e.g. LAB007-DB007\DB01).
- **Without Instances:** specify solely the database DNS server name (e.g. LAB007-DB007).

USE PORT SWITCH

The HTInstaller uses the default TCP SQL port 1433 to connect to the database when the switch **Use port** is in off position. There are cases when the client’s infrastructure implies the database connectivity through a different port (mostly for security reasons). In this case, the installer can turn on the **Use port** switch and then specify a custom port:



NOTE! If the SQL server does have instances and the port is different from default, it is not mandatory to turn on specify this port. The service **SQL browser** will automatically pull the port from the DNS name.

IMPORTANT: POSSIBLE ISSUES!

Do not utilize the Use port switch in case the environment has a **dynamic ports** system. This will crush the deploy. The dynamics ports are pulled automatically by the **SQL browser** service.

IMPORTANT: POSSIBLE ISSUES!

Extreme accuracy and caution must be applied in case the database contains numerous instances. If you specify the correct DNS name of the database instance but with an incorrect port, the HTInstaller will refer to the instance which port you specified. This can corrupt existing neighboring database and lead to the irreversible data loss.

Always remember! The database port has priority over the database DNS name. This is a default design implemented by the Microsoft Corporation. Always check the port accuracy before utilizing the Use Port switch.

NOTE! In case the port has no references to other neighboring instances in the database, the deploy process will crush.

6. SSO PARAMETERS

Specify Single Sign-On parameters and two-factor authentication parameters if needed.

HAZELTREE 8.0.0

Specify SSO parameters

Cookie Expiration In Minutes: 15 (25)

Cookie Same Site Strict Policy: Lax (26)

Authentication Mode: Duo (27)

Duo parameters (28):

- Host: wayne.duo.com
- Integration key
- Application key
- Secret key

Back Next

25. **Cookie Expiration Time:** specify the user session expiration time in minutes.

26. **Cookie Same Site Strict Policy:** select the cookie policy: none, lax or strict.

27. **Authentication Mode:** select the authentication mode (none or two-factor DUO authentication).

28. **Duo parameters:** specify the parameters for two-factor DUO authentication: Host, Integration key, Application key, Secret key.

TWO FACTOR DUO AUTHENTICATION

The HTInstaller provides with opportunity to establish a secure two-factor authentication with the DUO company. To establish the two-factor authentication the user must specify the following parameters:

Duo parameters

Host (required)

Application key (required)

Integration key (required)

Secret key (required)

All parameters required for DUO activation can be found in the DUO account. In case you do not have a DUO account but still need the two-factor authentication, create the DUO account prematurely.

In case the two-factor authentication is not selected, the authentication mode will be automatically set to **None** value.

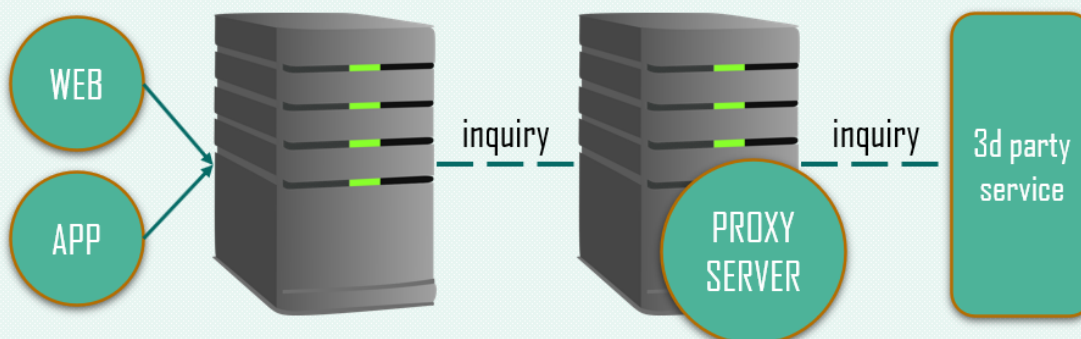
7. PROXY PARAMETERS

Specify the proxy server parameters: host, port, bypass addresses, etc.

29. **Enable proxy switch:** turn on the switch to identify if there is a proxy server in your infrastructure.
30. **Proxy host:** specify the proxy server host IP address or DNS name.
31. **Port:** specify the port for connection to the proxy server.
32. **Proxy settings:** set up the proxy server settings by checking/leaving blank the proxy server parameters.
33. **Enable Bypass proxy for local addresses switch:** turn on the switch to identify the list of local addresses that can be accessed passing over the proxy server.
34. **Bypass addresses:** list of local addresses that can be accessed passing over the proxy server.
35. **Add bypass address:** type in the IP address of DNS name of the bypass local address and hit plus icon to add it to the list.

PROXY SERVER ROLE

The **proxy server** in the infrastructure of the Hazeltree application is used for accessing the external sources: mostly, they are 3d party services (security providers, management services, etc.). The idea behind the proxy server use is that the Hazeltree server itself remains absolutely detached from the Internet, hence completely protected hack-wise. The simplified schema of the proxy server place in the infrastructure is presented below:



8. EMAIL PARAMETERS

Specify the email server settings and email user account credentials if needed.

HAZELTREE 8.0.0

Specify Email parameters

Email server settings 36

From Address
mail@wayne.com

SMTP Host
smtp.wayne.com

Port
25

☒ Use SSL

Use email user account 37

☒

Email user account

Username
bruce.wayne@wayne.com 38

Password
••••••••

Back Next

36. **Email server settings:** specify the email server settings: From address, SMTP Host, port, and SSL encryption.

37. **Use email user account switch:** turn on the switch to designate the account of the email sender.

38. **Email user account credentials:** type in the sender credentials to verify the sender's mailbox on the SMTP server.

EMAIL SERVER

The **email server** is used to send out the email using the SMTP protocol. The From Address specified in the Email server settings section will always be the sender email address. The personal mailbox can be used for authentication purposes (specifically if the SMTP connectivity is encrypted with the SSL protocol).

9. EXTERNAL DEPENDENCIES PARAMETERS

Specify the external dependencies (Security hub, Operations Manager, Caching system, etc.) and their parameters.

The screenshot shows the 'Specify external dependencies parameters' configuration page in the HazelTree 8.5.0-rc.49e8a47 interface. The page is divided into five sections, each with a title and a list of parameters. The parameters are numbered 39 through 47. The sections are: Security Hub, Operations Manager, Environment, Caching, and External Data. The Caching and External Data sections have a 'Source Type' dropdown menu with 'redis' and 'ignite' options. The 'Back' and 'Next' buttons are at the bottom right.

HAZELTREE 8.5.0-rc.49e8a47

Specify external dependencies parameters

Security Hub

39 **Url**
https://qa-sechub:8412/

Client secret
MT-Wayne-PROD01

Operations Manager

40 **Url**
https://qa-sechub:8417/

Client secret
&Yut4hw97cfn9P&4hch4p9H\$ &g4pf

Environment

41 **Short Name**
MT-Wayne-PROD01

Caching

42 ☒ **Enabled**

43 **Source Type**
redis ignite

44 **Caching location (connection string)**
cache1-prd, ssl=true, abortconnect=false, defaultDatabase=99

External Data

45 ☒ **Enabled**

46 **Source Type**
redis ignite

47 **External Data Location (connection string)**
cache1-prd, ssl=true, abortconnect=false, defaultDatabase=99

Back **Next**

39. **Security Hub**: in case you utilize a Security Hub (Hazeltree or third-party) type in the Security Hub URL.

40. **Operations Manager**: external public API access point (*in development*).

41. **Environment:** if you the Redis included in the environment, specify the short name of the Redis data block identifier.
42. **Caching:** flag the checkbox if you want to enable the caching process for the Hazeltree application.
43. **Source Type:** select the caching system (*redis* or *ignite*) to integrate with Hazeltree application.
44. **Caching Location:** specify the connection string of the selected Caching system.
45. **External Data:** flag the checkbox if you want to enable cache data export for Hazeltree application.
46. **Source Type:** select the caching system (*redis* or *ignite*) to integrate with Hazeltree application.
47. **External Data Location:** specify the connection string of the external cache data management system.

REDIS / IGNITE INTEGRATION

To significantly reduce the data loading time, the design of the Hazeltree application can be expanded with the third-party services that allows to cache the latest inquiry data. There are two services that can be integrated with Hazeltree application: **Redis** and **Ignite**.

Term: **Redis** is a third-party in-memory data structure service that implements a distributed in-memory database accessed on the key-value basis. The Redis database has optional durability.

Term: **Ignite** is a third-party in-memory data structure service that features an in-memory computing platform which includes an in-memory data grid, in-memory database, and streaming analytics.

REDIS / IGNITE 411

The Hazeltree application refers directly to the database and retrieves the inquired data when the Web site form sends inquiries for an update or page refresh. The data transition to the endpoint occupies time proportional to the volume of the inquired data. The inclusion of the caching service (Redis or Ignite) significantly reduces the loading time: once the data is transferred to the Hazeltree application, it is cached in the external outsource service. Therefore, the next user inquires will receive the data from the Redis or Ignite cache.

To implement the caching system into the Hazeltree structure, client must specify the following parameters in the HTInstaller wizard:

- **Environment:** the identifier of the Redis data block referring to installed environment.
- **Caching Location:** the connection string to the local cache vault.
- **External Data Location:** the connection string to the external data cache vault.

Caching

☒ Enabled

Source Type

redis ignite

Caching location (connection string)

cache1-prd,ssl=true,abortconnect=false,defaultDatabase=99

External Data

☒ Enabled

Source Type

redis ignite

External Data Location (connection string)

cache1-prd,ssl=true,abortconnect=false,defaultDatabase=99

10. STATISTICS COLLECTION PARAMETERS

Specify the Statistics Collection parameters for the Elastic Search engine.

The screenshot shows the HazelTree 9.0.6 configuration window titled "Specify Statistics Collection parameters". It features a toggle switch for "Statistics Collection Enabled" which is turned on. Below this is a text input field for "Elastic Search Uri" containing the URL "https://elst-qa0198/-PROD01". At the bottom are "Back" and "Next" buttons.

HAZELTREE 9.0.6

Specify Statistics Collection parameters

☒ Statistics Collection Enabled

Elastic Search Uri
https://elst-qa0198/-PROD01

Back Next

48. **Statistics Collection Enabled**: switch the setting to turn on the gathering of statistics data by the Elastic engine.

49. **Elastic Search Uri**: specify the link to the Elastic Search engine.

11. LOGGING & TRACING PARAMETERS

Specify the Elastic Search parameters for tracking the Hazeltree application logs.

The screenshot shows the HazelTree 8.5.0-rc.49e8a47 configuration window titled "Specify Logging and Tracing parameters". It contains two sections. The first section, "Elastic Search Enabled", has a toggle switch turned on and includes a text input for "Elastic Search Uri" with the value "https://elstc-qa0198-PROD01". The second section, "OpenTracing Enabled", has a toggle switch turned on. At the bottom are "Back" and "Next" buttons.

HAZELTREE 8.5.0-rc.49e8a47

Specify Logging and Tracing parameters

☒ Elastic Search Enabled

Elastic Search Uri
https://elstc-qa0198-PROD01

☒ OpenTracing Enabled

Back Next

50. **Elastic Search engine parameters:** a no-sql database oriented on the full-text search that vaults the logs produced with the Hazeltree application.
51. **Elastic Search Url:** the URL link to the Elastic Search engine that is put to the Hazeltree configuration file in order to direct the log stream to the Elastic vault.
52. **Kibana Uri:** a web user interface that allows to conveniently read the logs stored within the Elastic Search.
53. **Open Tracing:** : a switch that allows to change the tracing mode to **(Open) Enabled**.

12. OCTOPUS DEPLOY SERVER PARAMETERS

Specify the Octopus server parameters: Administrator account, installation directories, ports, etc.

HAZELTREE 8.0.0

Specify Octopus Deploy Servers parameters

Administrator account

Octopus admin username: admooctopus

Octopus admin user password: [password field]

Installation directories

Installation directory for Octopus Deploy Server: C:\Program Files\Octopus\Server

Installation directory for Octopus Deploy Tentacle: D:\Apps\Octopus\Tentacle

Instance directory: C:\Program Files\Octopus\Instance

ADVANCED

Back Next

Advanced

Server port: 80

Listen port: 10944

Tentacle port: 10933

☒ Drop Server instance if exists

54. **Octopus Administrator account:** type in with the Octopus administrator credentials.
55. **Installation directories:** specify the installation directories of the Octopus Deploy Server, Tentacle, and Instance.
56. **Server port:** specify the Octopus server port (default value: 80).
57. **Listen port:** : specify the Octopus listen port (default value: 10944).
58. **Tentacle port:** specify the Octopus tentacle port (default value: 10933).
59. **Drop Server instance if exists:** flag the checkbox in case the Hazeltree application is already installed on the server.

Term: **Octopus** is a third-party deployment and release management system that is designed to automate complex deployments.

OCTOPUS ADMINISTRATOR ACCOUNT

To initiate a deploy, the HTInstaller must authenticate itself as the Octopus Administrator. Insert the administrator credentials if you already have an Administrator account. In case the Administrator account is not created, specify random username and password. The HTInstaller wizard creates the Administrator account automatically.

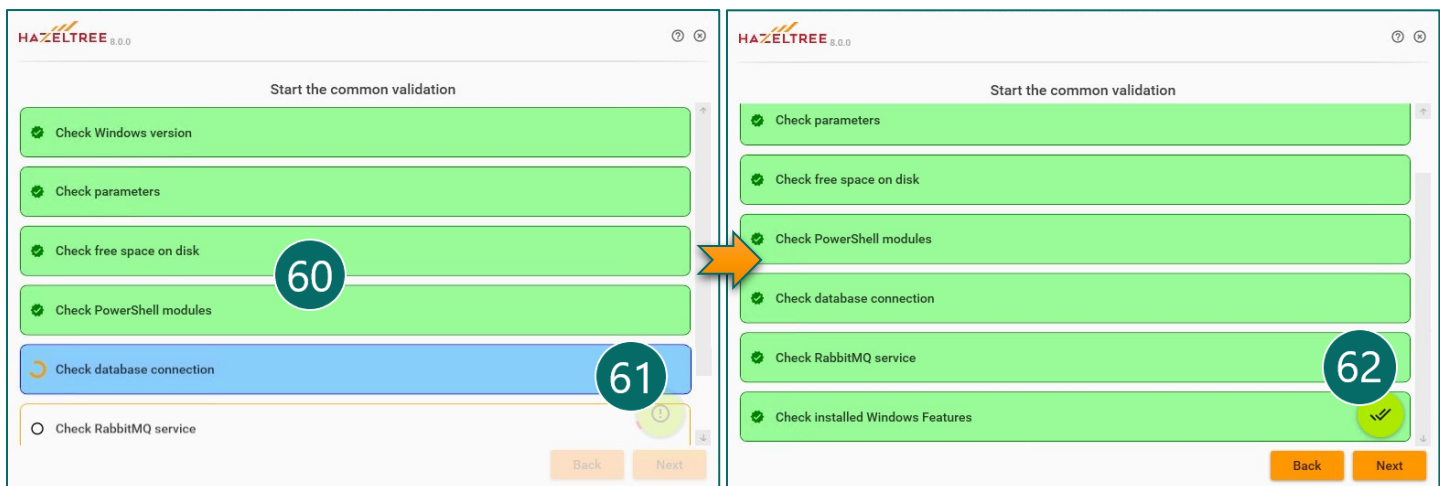
DROP SERVER INSTANCE IF EXISTS

The checkbox **Drop Server instance if exists** must be checked if the network parameters, specified previously, included the HTTPS protocol for any of the access points (WEB site, WEB API, Mobile API). The checkbox is always checked by default.

NOTE! Dropping the Server instance does not erase any data from the database.

13. COMMON VALIDATION

Start the common validation of the deployment components and check the result.



60. **Validation tests:** list of the validation tasks that the HTInstaller checks against system requirements.

61. **Start validation tests:** press the button to start the validations tests.

62. **Validation result:** passed validation sign turns green and activates the Next button. In case of failed tests, the exclamation mark is displayed on the sign. Fix the errors and repeat the validation tests.

FAILED VALIDATION TESTS

During the common validation step, the tests can fail. The failure of the test means that the system requirement is not complied, and the subsequent deployment cannot be started. The failed test is complimented with the error text that allows to disclose the issue root and operatively eliminate it.

See the example on the next page.

EXAMPLE

During the common validation step, the test **Check database connection** has failed with an error: **Cannot connect to application database server**:



⚠ Check database connection
Can not connect to application database server DB045
Verify database server and network configurations to continue.

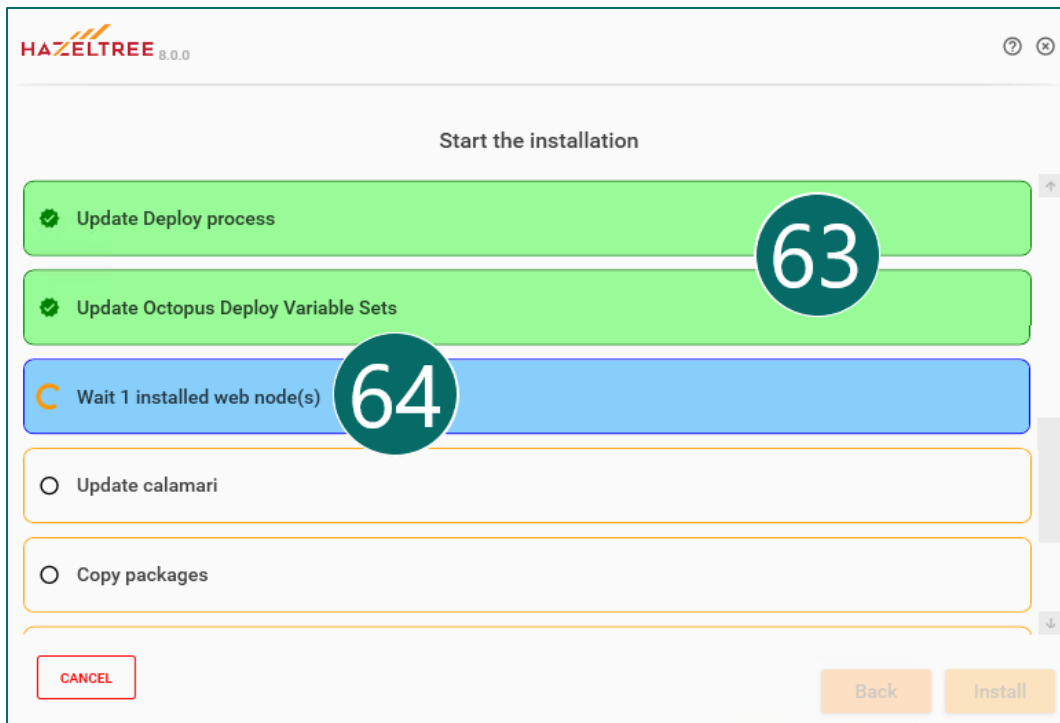
The basic possible issues behind this error are well-known:

- User put an incorrect database URL or instance in the HTInstaller wizard.
- User put an incorrect port in the HTInstaller wizard.
- The port is closed on the database server.
- The database server is down.
- The database or instance is not created.
- Proper permissions are not delegated to the user, the operator of the HTInstaller.

Check the HTInstaller specified parameters and the database server to troubleshoot the issue, fix it and run the common validation routine again.

14. INSTALLATION PROCESS

Proceed to the installation routine. Start and wait until the HTInstaller prompts for a client HTInstaller part installation on other nodes of the Deployment schema.



63. Installation steps: check the installation steps displayed on HTInstaller wizard screen. Successful steps turn green. Failed steps turn red and display error message within the step frame.

64. **Setup client step:** HTInstaller wizard displays the step **Wait installed node**. The number of steps depends on the number of servers in Deployment schema.

WAIT APP/WEB NODE

The installation process of the multi-node deployment plan requires the Octopus tentacles traversed on all servers of the deployment schema. To establish the connection between primary (installation) server and another server, the HTInstaller Client tool must be installed on the latter. During the installation routine, the HTInstaller wizard displays a sequence of required client installations:

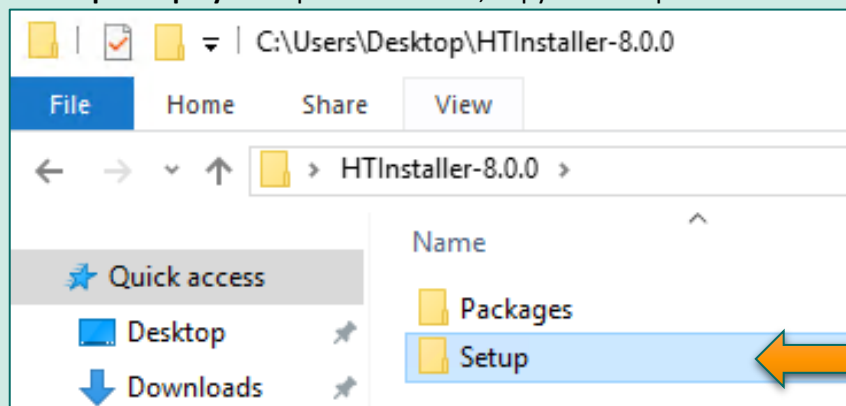
- **Split deployment:** requires one HTInstaller Client installation step.
- **Multi-node deployment (two servers):** requires one HTInstaller Client installation step.
- **Multi-node deployment (four servers):** requires three HTInstaller Client installation steps.

NOTE! When you see the displayed installation flag “**Wait 1 installed WEB/APP node(s)**”, leave the HTInstaller be and proceed to the server with WEB/APP role accordingly. Then follow the [HTInstaller Client](#) instructions.

 Wait 1 installed web node(s)

IMPORTANT: VERIFY SETUP FOLDER IS COPIED!

Before conducting the installation verify that the Setup folder has been copied over to the rest of the servers of the schema. If not, copy the folder **Setup** from the HTInstaller archive to the servers included in the schema. For example, if the **Split Deployment** plan is selected, copy the Setup folder to the server with the **WEB** role:



HTINSTALLER CLIENT INSTRUCTIONS

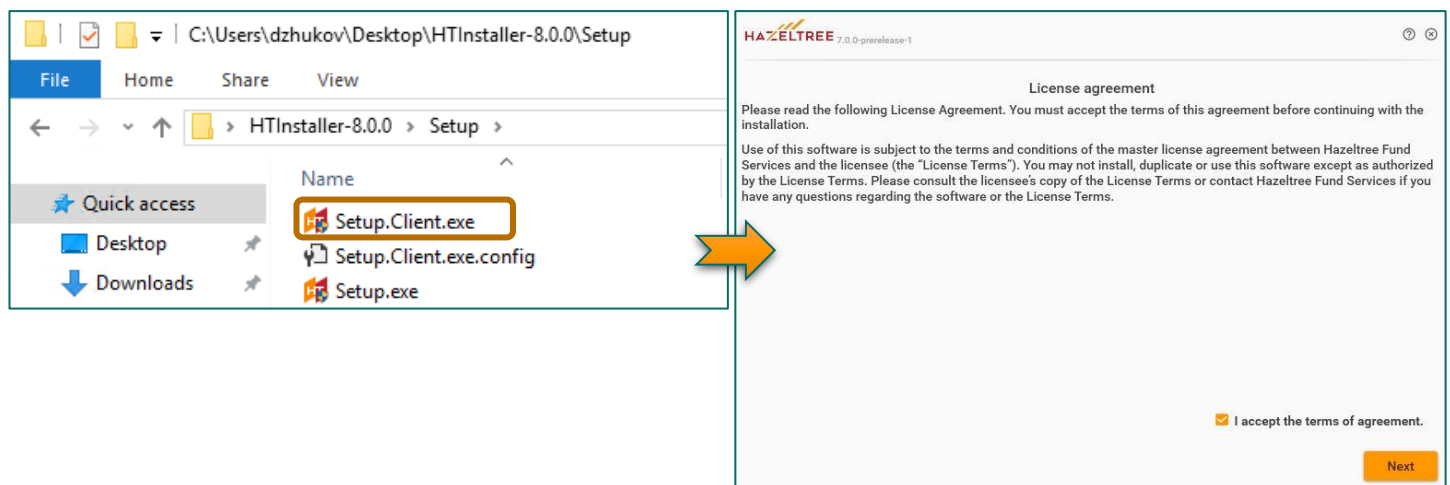
HTInstaller Client is a client part of the HTInstaller wizard with identical user interface and similar deployment steps. The client part is required to establish a connection between the primary server that runs the HTInstaller and the nodes. Once the connection is settled, one can finalize the installation and complete the Hazeltree multi-node deployment process.

INFO! When you see the displayed flag **“Wait 1 installed WEB/APP node(s)”** on the HTInstaller installation process, leave the HTInstaller be and proceed to the server with WEB/APP role accordingly.

Wait 1 installed web node(s)

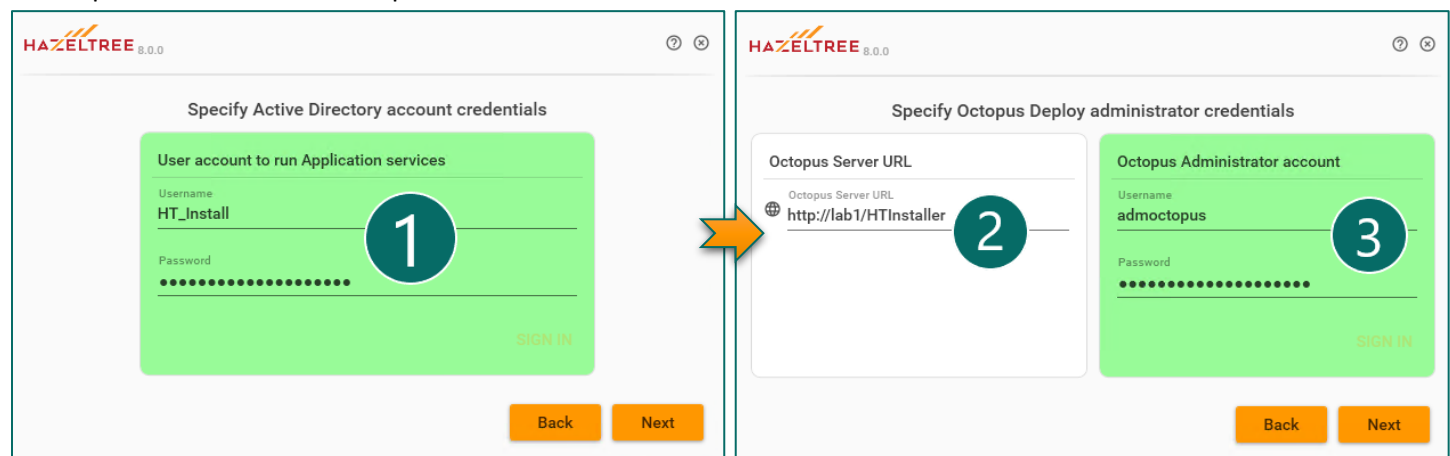
1. HTINSTALLER CLIENT SETUP & LICENSE AGREEMENT

Basing on the HTInstaller installation **Wait Installed node** flags, consistently proceed to servers of APP and WEB roles. Find the **Setup.Client** executable file in the folder **Setup**.



2. USER CREDENTIALS & OCTOPUS TENTACLE

Log in with the Active Directory Domain Services users credentials for Application services and then specify the Octopus Server parameters and the Octopus Administrator credentials.



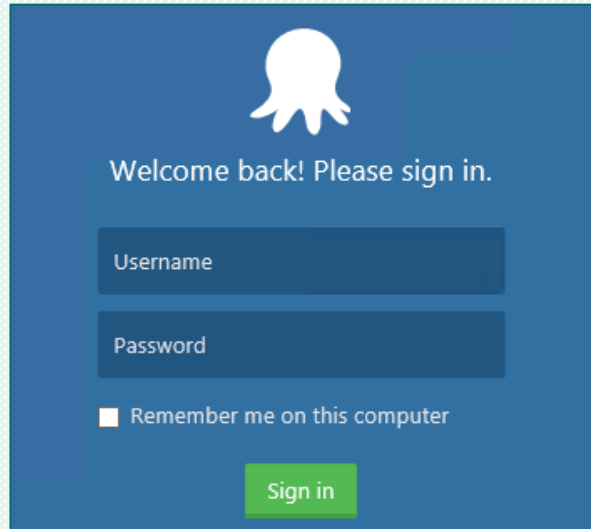
1. **Application services user:** log in with the credentials of the user that runs Application services.
2. **Octopus Server URL:** specify the Octopus Server URL. It can be taken from the primary installation server with deployed Octopus Server.

3. **Octopus Administrator account:** log in with the credentials of the Octopus administrator.

OCTOPUS SERVER URL

The **Octopus** service manages the process of deployment by connecting all servers involved in the deployment process with specific tunnels called **tentacles**. To create a tentacle endpoint on a server, you must specify the Octopus server (primary installation server that runs the HTInstaller wizard). The Octopus URL represents a primary server URL with the **/HTInstaller** part (e.g. [http://\[serverURL\]/HTInstaller](http://[serverURL]/HTInstaller)).

NOTE! The server URL can always be checked on the primary server. Proceed to any Internet browser and paste the Octopus Server URL. If the browser displays the Octopus login form, then the URL is correct:

A screenshot of the Octopus login interface. It features a blue background with a white octopus logo at the top. Below the logo, the text "Welcome back! Please sign in." is displayed. There are two input fields: "Username" and "Password". Below these fields is a checkbox labeled "Remember me on this computer". At the bottom, there is a green "Sign in" button.

Welcome back! Please sign in.

Username

Password

☐ Remember me on this computer

Sign in

3. OCTOPUS TENTACLE PARAMETERS

Specify the Octopus Tentacle parameters: server role, SSL certificates and installation directories.

Specify Tentacle parameters

Tentacle role **4**

☐ App ☒ Web ☒ Mobile

SSL: **5**

WEB Site Certificate **6**

WEB API Certificate **7**

Mobile API Certificate **8**

Back Next

Advanced

Installation directory **9**

D:\Apps\Octopus\Tentacle

Instance directory **10**

C:\Program Files\Octopus\Instance\Tentacle

Port **11**

10933

4. **Tentacle role:** specify the server role (APP, WEB or Mobile) of the tentacle server by marking the checkboxes next to the role names.
5. **SSL switch:** turn on the switch in case the connection between the servers must be secured with the SSL certificate.
6. **WEB Site Certificate:** select the SSL certificate from the dropdown to secure the connection to the WEB server.
7. **WEB API Certificate:** select the SSL certificate from the dropdown to secure the API connection.
8. **Mobile API Certificate:** select the SSL certificate from the dropdown to secure the Mobile API connection.
9. **Installation directory:** specify the location of the Octopus Tentacle installation directory (default location: Tentacle folder under the Octopus folder).
10. **Instance directory:** specify the location of the Octopus Tentacle instance (default location: Tentacle folder under the Octopus Installation directory folder).
11. **Port:** specify Octopus Tentacle port (default value: 10933).

TENTACLE ROLE

The multi-node deployment implies the allocation of the server roles among different servers included in the schema. Basing on the Deployment plan made up before the installation, specify the server roles in the HTInstaller Client:

- **APP**
- **WEB**
- **Mobile API**

SSL CERTIFICATES

The SSL certification is available for the HTTPS protocol that establishes secured connection the primary server and the endpoint server. If the Deployment schema implies a solo APP server, the SSL switch will be disabled for this server:

Tentacle role

☒ App ☐ Web ☐ Mobile

SSL: ☐

The servers with WEB role and Mobile API service can be provided with SSL certification for the HTTPS connection establishment. The SSL certification depends on the combination of protocols selected in the HTInstaller wizard earlier.

IMPORTANT: POSSIBLE ISSUES!

The SSL Certification must be provided in case the primary HTInstaller was set to HTTPS protocols any combination. If the SSL Certificates were specified in the primary HTInstaller but were not specified in on the HTInstaller Client side, the deployment process will fail.

IMPORTANT!

The SSL Certificates must be installed on the HTInstaller Client server. The HTInstaller Client wizard will automatically recognize existing SSL Certificates and populate the dropdown fields with them. If more than one SSL Certificate are installed on the server, the user will see the whole set in the dropdown.

NOTE!

WEB site, WEB API and Mobile API connection must use different SSL Certificates released for three different URLs. However, it is possible to utilize the wildcard SSL Certificate. The wildcard type of the SSL Certificate can be used for all three access points simultaneously.

4. LOGGING PARAMETERS

Specify the Elastic Search Engine parameters for keeping the Hazeltree logs of the server in the Elastic vault.

HAZELTREE 8.5.0

Specify Logging parameters

☒ Elastic Search Enabled 12

Elastic Search Uri 13
https://01-elk-zona.com

Kibana Ur 14
https://01-elk-zona.com

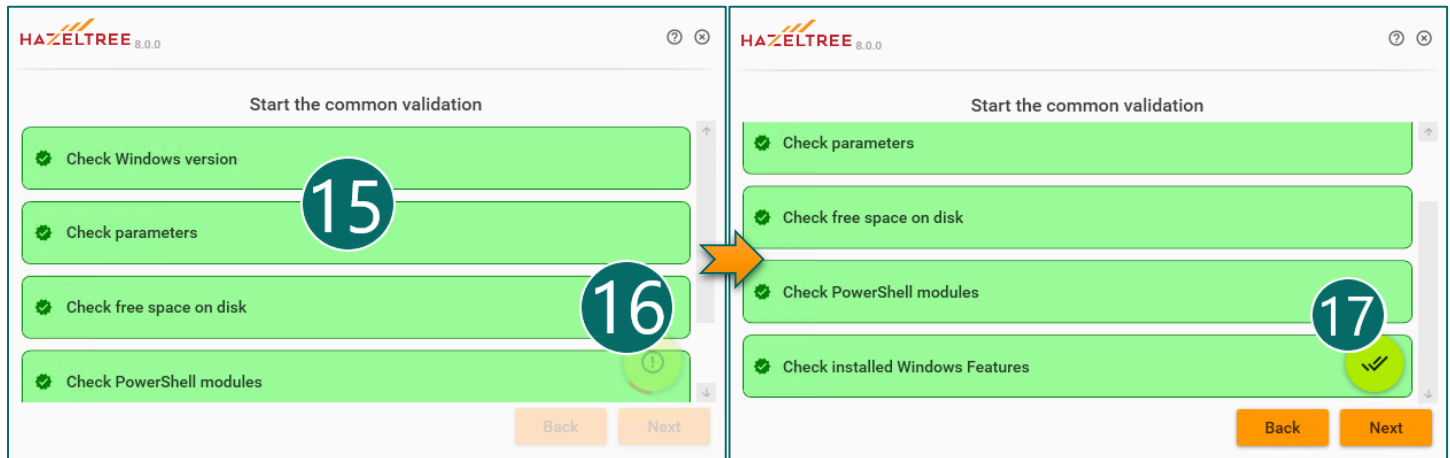
Back Next

12. Elastic Search Enabled: on-off switch that allows to turn on the no-sql database oriented on the full-text search that vaults the logs produced with the Hazeltree application.

13. **Elastic Search Uri:** the URL link to the Elastic Search engine that is put to the Hazeltree configuration file in order to direct the log stream to the Elastic vault.
14. **Kibana Url:** a web user interface that allows to conveniently read the logs stored within the Elastic Search.

5. COMMON VALIDATION PROCESS

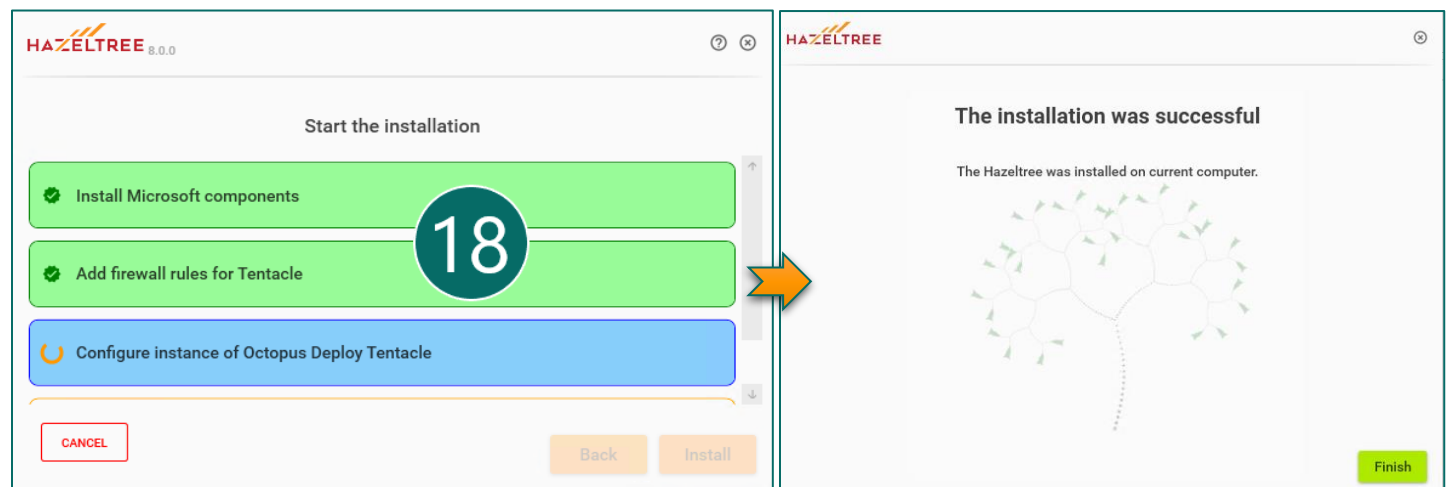
Start the common validation tests and check with results.



15. **Validation tests list:** the list of validation tasks that the HTInstaller Client runs to check the server against system requirements. Successful tests turn green. Failed tests turn red and display error messages.
16. **Start validation tests:** press the button to start the validation tests.
17. **Validation steps passed successfully:** passed validation turns green and activates the Next button. In case of failed tests, the red exclamation mark is displayed.

6. COMPLETE INSTALLATION PROCESS

Start the installation process and wait till it is successfully completed.



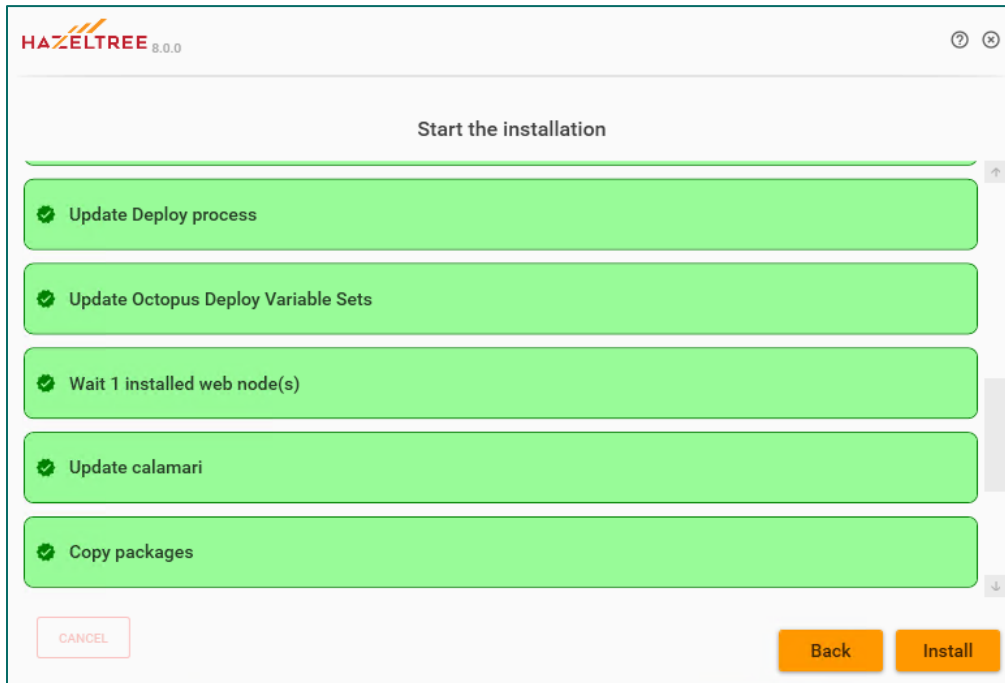
18. **Installation steps:** check the displayed installation steps. Successful steps turn green. Failed steps turn red and display error messages. Press Finish button to complete the HTInstaller.

VALIDATION & INSTALLATION ERRORS

In case the system requirements are respected, and the installation settings are specified accurately, the HTInstaller Client validation and installation processes go smoothly. In case the wizard displays an error, examine the error text, and fix the issue. The error text contains detailed information about the problem and allows to spot the trouble point instantly.

7. RETURN TO HTINSTALLER

After the HTInstaller Client is successfully completed, get back to the primary installation server and continue the installation process in the HTInstaller.



MORE NODES?..

Depending on the number of nodes in the selected Deployment plan, repeat the same HTInstaller Client routine for every server involved in the deployment process. When all nodes have the installed HTInstaller Client part, the main deployment process will be continued automatically in the HTInstaller. Wait for the process to finalize.

After the deployment is completed, press the button **Finish** to quit the HTInstaller. The Hazeltree application is installed and prepared for the welcome.

APPENDIX

Appendix section contains some additional information regarding the HTInstaller and the deployment process that was not mentioned in the main part of the guide.

INSTALLATION LOGS

Sometimes users can experience difficulties with the installation process due to various reasons. Whenever that happens, refer to the Hazeltree Support team for assistance. Before referring to the Support team, get the detailed logs of the installation process. They are located in the installation folder **Hazeltree > Octopus > Logs** (e.g. C:\Program Files\Hazeltree\Octopus\Logs). The logs contain detailed information about all errors and help isolate the issue and resolve it operatively.

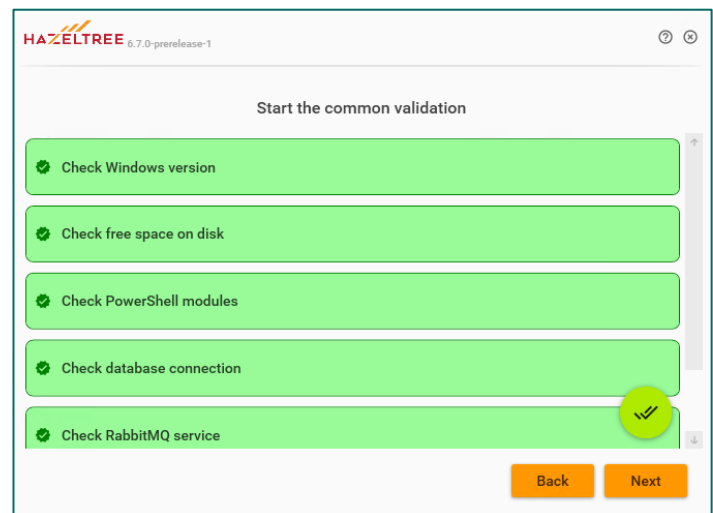
SSL CERTIFICATION IN MULTI-NODE DEPLOYMENT PLANS

It is critical that the SSL certification is consistent on primary server (runs HTInstaller) and all nodes (run HTInstaller Client). If the SSL certificates are specified in the HTInstaller, it is an absolute must to specify the SSL Certificates in the HTInstaller Clients with **WEB** server roles.

VALIDATION ERRORS

Before launching the installation process, the HTInstaller puts the servers on test, checking them against common system requirements. There are six major steps of validation:

- Check Windows version
- Check free space on disk
- Check PowerShell modules
- Check database connection
- Check RabbitMQ service
- Check installed Windows Features



If a test fails validation, the HTInstaller will not activate the **Next** button to start the installation. Failed tests turn red. The error is embedded in the test item frame. Follow the instructions in the error message to resolve the issue by yourself. When the issue is resolved, run the tests again.

See the example below:

EXAMPLE

The HTInstaller operator T. Greyjoy starts the validation and sees that the test **“Check free space on disk”** has failed. The error message says to clean up the disk space and resume installation:

⚠ Check free space on disk

Not enough free disk space on C:\ drive!

Please, clean it up, and resume installation.

EXAMPLE (CONTINUATION)

The user T. Greyjoy cleans up (or adds) the disk space on the server according to the system requirements of the guide. Then he runs the validation tests again. This time the test **“Check database connection”** has failed with an error message: **“Verify database server and network configurations to continue”**:

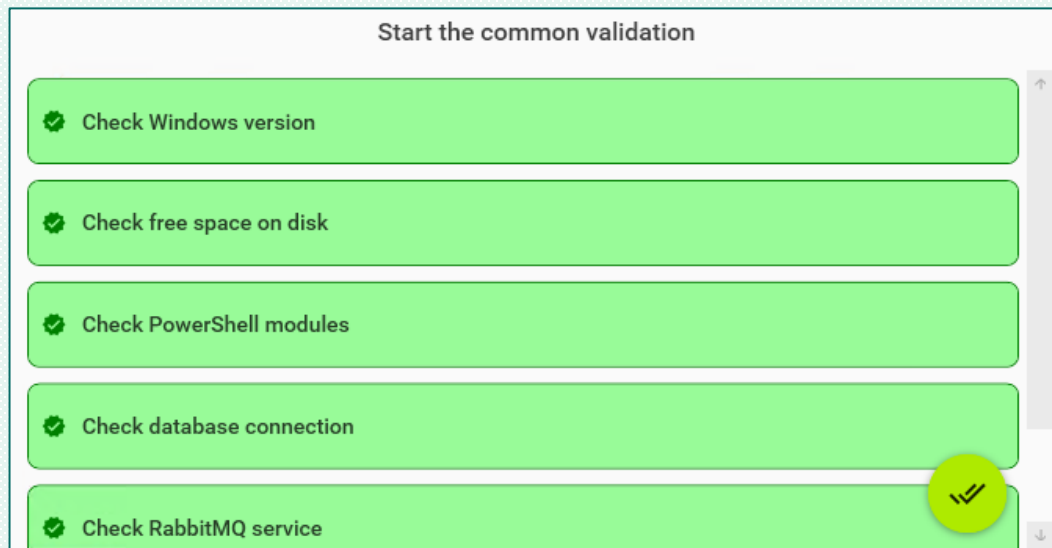


The basic possible issues behind this error are well-known:

- User put an incorrect database URL or instance in the HTInstaller wizard.
- User put an incorrect port in the HTInstaller wizard.
- The port is closed on the database server.
- The database server is down.
- The database or instance is not created.
- Proper permissions are not delegated to the user, the operator of the HTInstaller.

The user T. Greyjoy checks the database against all possible causes and finds out that the reason behind the error is that the HTInstaller operating user is not provided **sysadmin** rights for the database: therefore, the connection between the HTInstaller and the database cannot be established. After the rights are delegated to the user account of mister T. Greyjoy the issue is resolved.

The third attempt of validation is successful: all the tests turn green and the installation can be started.



HAZELTREE