



# **Areashell Access Management**

---

## Installation Guide

## Trademarks

Areashell and Areashell AM are trademarks of Areashell Inc.

All other brand and product names are trademarks or registered trademarks of their respective owners.

## Copyright

The information contained in this document is subject to change without notice and does not represent a commitment by Areashell Inc. The software described in this document is furnished under a license agreement and may be used or copied only in accordance with the terms of the agreement. No part of this manual or software may be reproduced or transmitted in any form or by any means, electronic or mechanical (including photocopying and recording), or transferred to information storage and retrieval systems without the written permission of Areashell Inc.

Copyright © Areashell Inc. 2019

All rights reserved.

## Contents

1. Introduction .....	4
2. System Configurations .....	4
2.1. Local System.....	5
2.2. Local System with Remote Access .....	6
2.1. Distributed Access Control System.....	7
2.2. Distributed Access Control System with Remote Access .....	8
3. System Requirements .....	9
3.1. Supported Platforms.....	9
3.1.1. Hardware Requirements .....	9
3.1.2. Supported Operating Systems.....	9
3.1.3. Supported Application Servers .....	9
3.1.4. Supported Databases.....	9
3.2. Network Requirements .....	10
3.3. Security Requirements .....	11
3.3.1. HTTP Security.....	11
3.3.2. Authentication and Authorization .....	11
4. Installing Areashell on a Windows Server .....	13
4.1. Installing Java Virtual Machine.....	13
4.2. Installing PostgreSQL Database Server.....	13
4.3. Creating the Areashell Database.....	19
4.4. Installing Areashell AM with WildFly 10 application server .....	19
4.4.1. Installing Areashell AM with WildFly 10 application server by the installation program in GUI Mode.....	19
4.4.2. Installing Areashell AM with WildFly 10 application server by the installation program in Console Mode .....	28
4.5. Installation Summary.....	32
5. Starting Areashell Access Management server .....	32
6. Launching the Areashell AM Management Console .....	33
7. Support.....	38

## 1. Introduction

## 2. System Configurations

Depending of existing IT infrastructure Areashell AM can be deployed in various scenarios. Some of the installation considerations are related to how the Areashell AM server should connect to the hardware controllers and how users and administrators will connect to the Areashell AM.

Depending of chosen deployment scenario Areashell AM server can be installed in corporate LAN network or in the corporate DMZ network zone.

In case of local closed physical access control system without requirements to support remote hardware controllers or remote users, Areashell AM can be installed inside the corporate LAN network.

If there are requirements to support remote hardware PACS controllers or to provide remote access to Areashell web console for remote users, for security reasons it is strongly recommended to install Areashell AM server in DMZ network zone. Optionally, Areashell AM server can be installed inside the Corporate LAN network, however it will require to open on corporate firewalls the network ports described in section "Network Requirements" to allow inbound connection from the Internet to Areashell AM server.

## 2.1. Local System

The Diagram 1 shows the deployment scenario for small local system with local connection of all computer hardware (system server and administrative workstations) and PACS hardware (controllers).

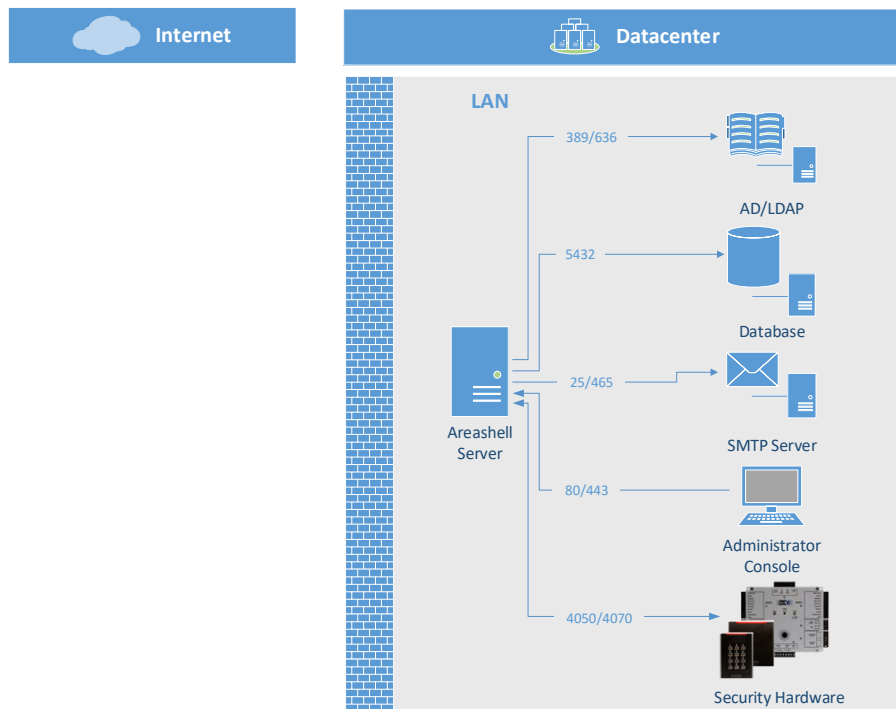


Diagram 1. Local Physical Access Control System

## 2.2. Local System with Remote Access

The Diagram 2 shows the deployment scenario for the system with local connection of system servers and all PACS hardware (controllers), but both local and remote connection of administrative and user workstations.

In that scenario for security reasons it is recommended to install Areashell AM server in DMZ network zone. Optionally, Areashell AM server can be installed inside the Corporate LAN network, however it will require all network firewall ports described in section "System Requirements" from the Internet to be allowed inbound to corporate LAN network where the server is placed to fully operate correctly.

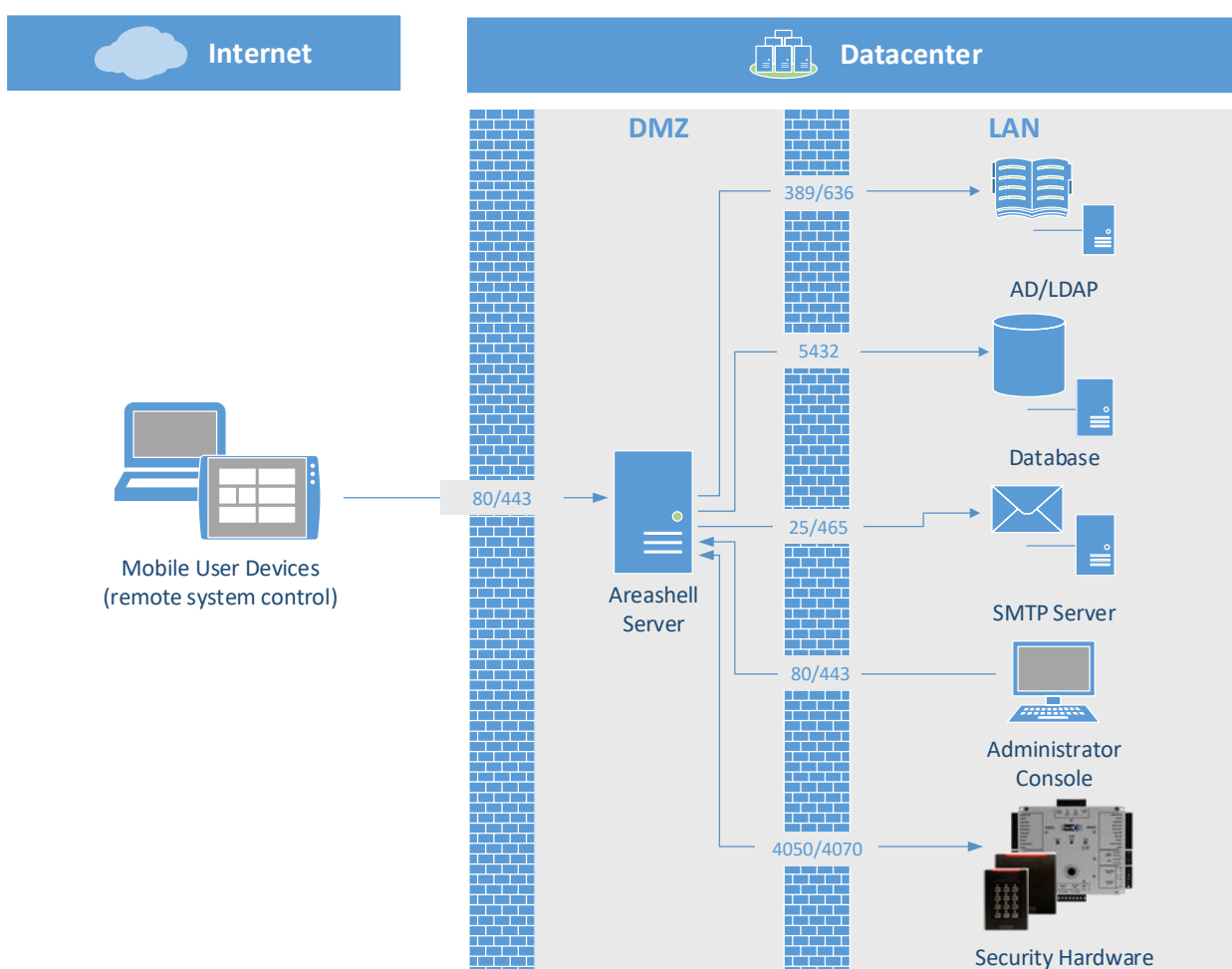


Diagram 2. Local Physical Access Control System with Remote Access

## 2.1. Distributed Access Control System

The Diagram 3 shows the deployment scenario with local connection of all computer hardware (system server and administrative workstations), but with both local and remote connection of the PACS hardware (controllers).

In that scenario for security reasons it is recommended to install Areashell AM server in DMZ network zone. Optionally, Areashell AM server can be installed inside the Corporate LAN network, however it will require all network firewall ports described in section "System Requirements" from the Internet to be allowed inbound to corporate LAN network where the server is placed to fully operate correctly.

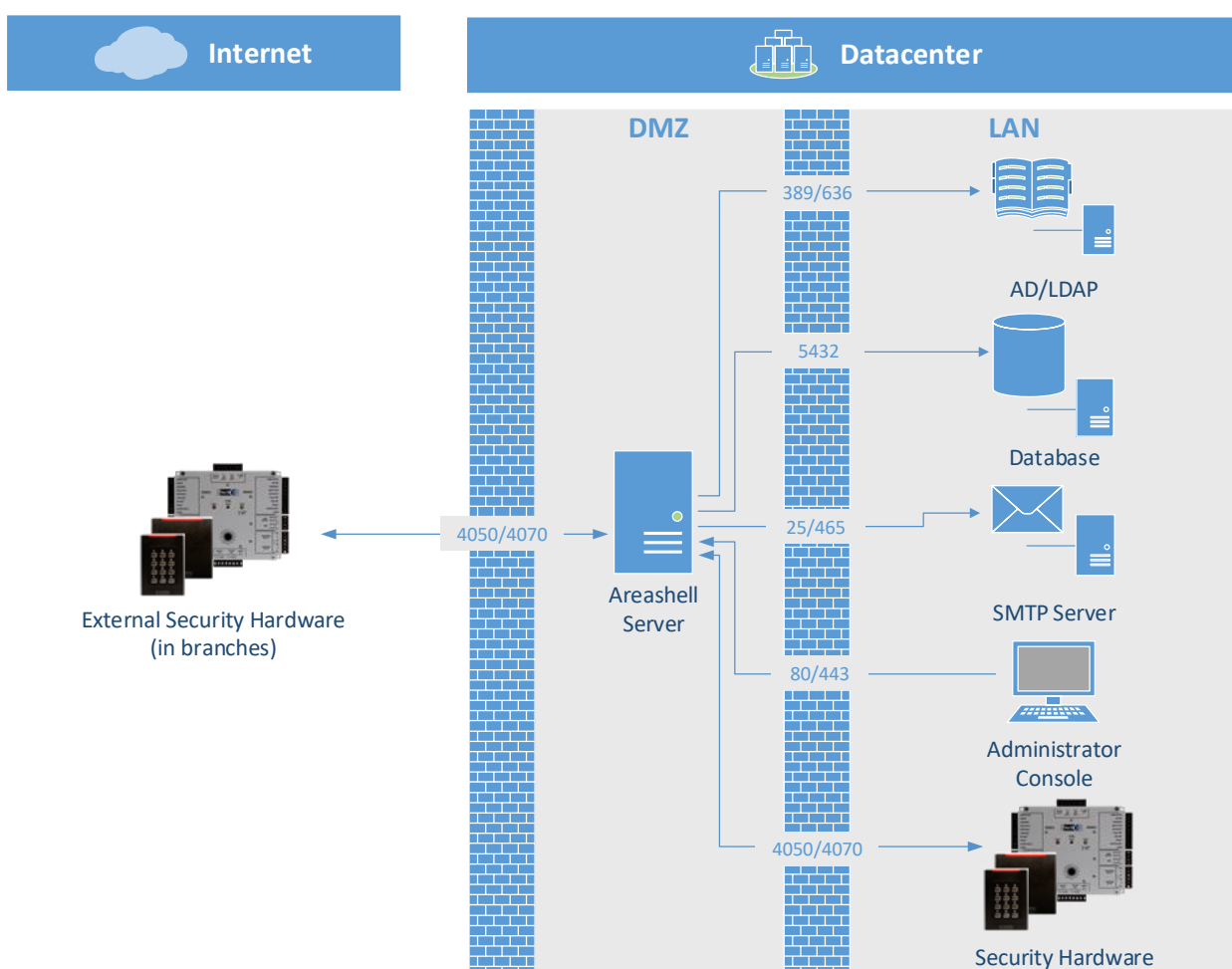


Diagram 3. Distributed Physical Access Control System

## 2.2. *Distributed Access Control System with Remote Access*

The Diagram 4 shows the deployment scenario with centralized deployment of the Areashell AM server and support of local or remote connection of PACS hardware (controllers) and administrative and user workstations.

In that scenario for security reasons it is recommended to install Areashell AM server in DMZ network zone. Optionally, Areashell AM server can be installed inside the Corporate LAN network, however it will require all network firewall ports described in section "System Requirements" from the Internet to be allowed inbound to corporate LAN network where the server is placed to fully operate correctly.

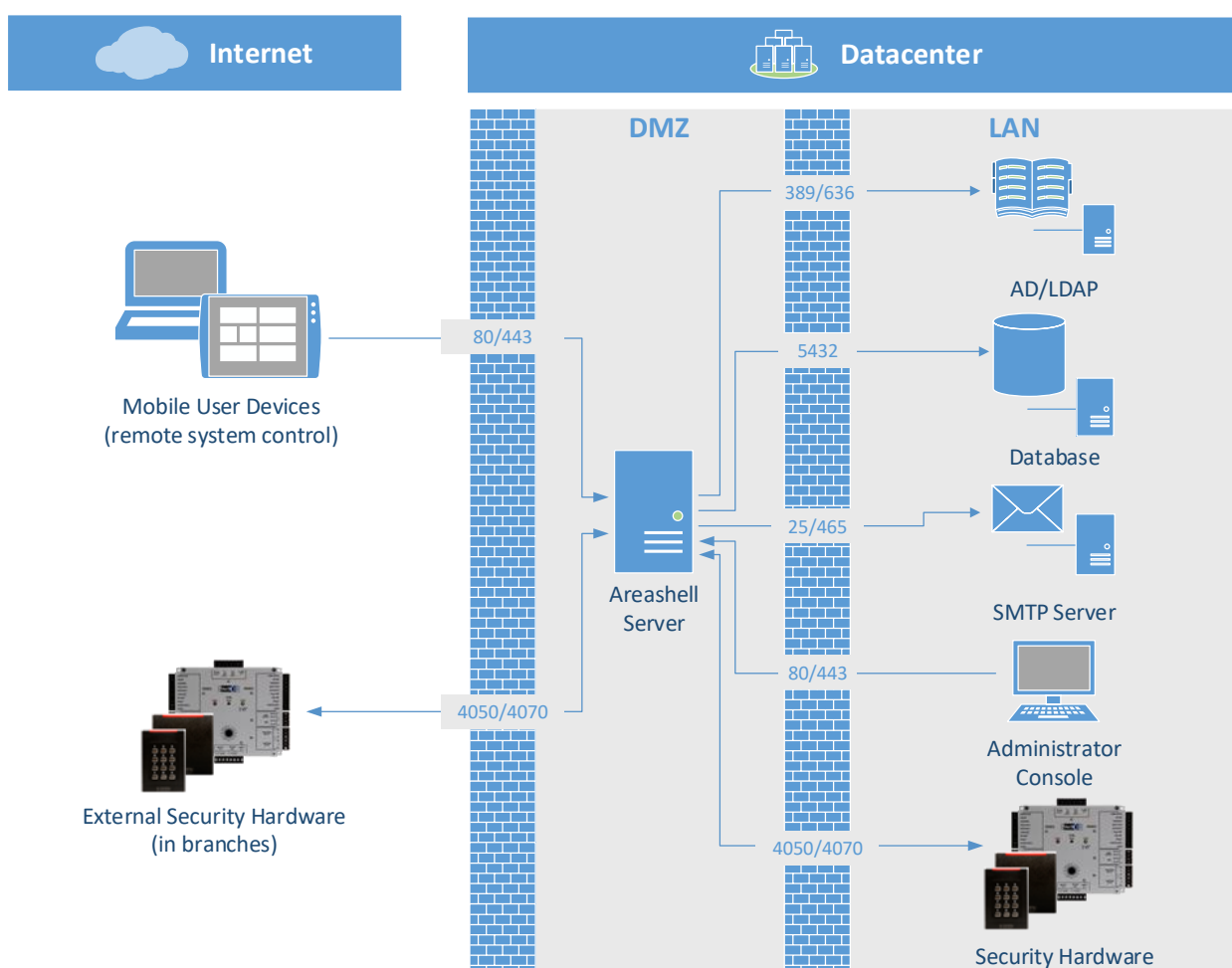


Diagram 4. Distributed Physical Access Control System with Remote Access

## 3. System Requirements

### 3.1. *Supported Platforms*

#### 3.1.1. Hardware Requirements

Areashell AM should be installed on a standalone physical server or dedicated virtual machine.

The minimum system configuration to install and run Areashell AM server is:

- Physical or Virtual Server host environment;
- 1 Intel server architecture CPU 2.0 GHz and above;
- 4 GB RAM minimum;
- 500 MB free disk space minimum;
- 1 Fast Ethernet network adapter.

#### 3.1.2. Supported Operating Systems

Installation and running Areashell AM server is supported on next operating systems:

- Microsoft Windows 2008 Server R2 Standard or Enterprise Edition
- Red Hat Enterprise Linux 6
- CentOS Linux 6

In production configuration it is recommended to install server on 64-bit platform.

#### 3.1.3. Supported Application Servers

It is required to install Java SE JDK.

Installation and running Areashell AM server is supported on next versions of JDK:

- Oracle Java SE 8 JDK (JDK Download Edition) update 8 and above

**Note:** Oracle Java components must be downloaded separately from the Oracle download web site.

On 64-bit platform it is recommended to install and use 64-bit version of JDK.

Areashell AM should be installed on Java EE 7 Full Profile application server.

**Note:** WildFly 14 server is included in Areashell AM installation bundle and will be installed as a part of the Areashell AM installation process.

#### 3.1.4. Supported Databases

Running Areashell AM server is supported with next databases:

- PostgreSQL 9, 10, or 11

### 3.2. Network Requirements

In case of installation of the Areashell AM server in DMZ network zone, it will need to have a static IP address that is reachable from the public Internet, as well as a registered and published DNS host name so that workstations and hardware controllers can reach the server. It is strongly recommended to use a separate A-record or CNAME record for any host in a DMZ network zone for anonymity of the true server host name.

There are several ports that must be configured on the network between the Internet and the DMZ and between the DMZ and the LAN. The following table provides a guide for the TCP/IP port requirements for the Areashell AM connections.

TCP Port	Source	Destination	Description
8080 <sup>1</sup>	Internet and Corporate LAN	Areashell AM server	Access to Areashell AM Management Console (HTTP)
8443 <sup>1</sup>	Internet and Corporate LAN	Areashell AM server	Secure access to Areashell AM Management Console (HTTPS)
389 or 636 <sup>2</sup>	Areashell AM server	LDAP / Active Directory Services	Integration Areashell AM with corporate directory service.
5432 <sup>3</sup>	Areashell AM server	Dedicated database server	Required only in case of using the dedicated database management server.
25	Areashell AM server	SMTP server	Sending email notifications to administrators and users.  If your corporate SMTP server uses a different port, make sure that your corporate firewall does not block that port.
4050	Areashell AM server	HID hardware controllers	Data exchange between Areashell AM server and HID VertX hardware controllers (connection from Areashell)

<sup>1</sup> Any other port could be chosen at the time of the installation.

<sup>2</sup> Depending of the port, used by corporate directory service.

<sup>3</sup> Depending of the port, used by dedicated database server. The default value for PostgreSQL server is 5432 or 5433.

4070	HID hardware controllers	Areashell AM server	Data exchange between HID VertX hardware controllers and Areashell AM server (connection from HID VertX)
------	--------------------------	---------------------	--

### 3.3. *Security Requirements*

#### 3.3.1. HTTP Security

It is recommended to use SSL data encryption to secure communications between clients and Areashell AM Management Console. Areashell AM Installation Program creates and deploys to WildFly application server self-signed SSL certificate for HTTPS connections to Areashell Management Console. For more security, it is recommended to create and use signed by trusted certificate authority SSL certificate. For more information please refer to the Deployment Configurations section.

The new certificate can be installed to WildFly server with using Java keytool utility.

Use keystore password, set at the time of Areashell AM installation.

For additional instructions please refer to the keytool utility documentation:

<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>

#### 3.3.2. Authentication and Authorization

Areashell AM supports different methods of user authentication:

- Authentication using LDAP or Active Directory (recommended)
- Authentication using local Areashell AM database
- Other method are also available.

In case of authentication using the local Areashell database user names and hashes of passwords are stored in the Areashell database. It is possible to register new user account by creating it with using the Areashell AM Management console. The current limitation of this method is that all users have the same administrative permissions in Areashell AM Management Console. This will be improved in next versions of the Areashell AM.

When using LDAP or Active Directory authentication the corporate directory service is used for user authentication and role retrieval

In case of integration with corporate directory service Microsoft Active Directory, special service account should be registered in that directory service. It is recommended to set secure password for that account. Password should not expire. The name and the password of that account should not be changed. This account should have permissions to search the directory.

It is possible to create different user groups in LDAP Directory or Active Directory and include users to that groups to manage users' permissions in Areashell AM Management Console.

The following table provides a list of supported group names :

Group Name	Areashell AM Management Console Permissions
Administrators	Full access permissions, including, but not limited: <ul style="list-style-type: none"> <li>- view and edit settings of hardware, policies, users;</li> <li>- control hardware and areas;</li> <li>- generate event reports;</li> <li>- and others.</li> </ul>
PeopleManagers	<ul style="list-style-type: none"> <li>- View policies;</li> <li>- Register new users;</li> <li>- View and edit user data;</li> <li>- Generate event reports.</li> </ul>
Receptionists	<ul style="list-style-type: none"> <li>- View and edit policies;</li> <li>- Register new users;</li> <li>- View and edit users' data;</li> <li>- View and edit users' policies;</li> <li>- Generate event reports.</li> </ul>
Guards	<ul style="list-style-type: none"> <li>- View policies;</li> <li>- View user data</li> <li>- View status and control hardware;</li> <li>- View status and control areas (rooms, areas, groups of areas)</li> <li>- Generate event reports.</li> </ul>
-	Any authenticated user, not included into any of the supported user groups, can open Areashell AM Console, but do not receive any permissions to work in the system.

These names can be modified manually in the next file after installation of the system:

*wildfly-14.0.1.Final/standalone/configuration/areashell-groups.properties*

## 4. Installing Areashell on a Windows Server

### 4.1. *Installing Java Virtual Machine*

Areashell requires the Java™ SE Development Kit 8 (JDK) to be installed prior to installing the Areashell software.

**Note:** Oracle Java components must be downloaded separately from the download web site.

To install the Java™ SE Development Kit:

1. Visit the following link:  
<https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>
2. Agree to the Oracle Binary Code License Agreement for Java SE
3. Download the appropriate EXE file labeled with "jdk-7u17-windows-x64.exe"
4. Install Java SE following your platform's installation instructions:  
<http://docs.oracle.com/javase/7/docs/webnotes/install/index.html>
5. Clean up temporary Java SE installation files, if needed

### 4.2. *Installing PostgreSQL Database Server*

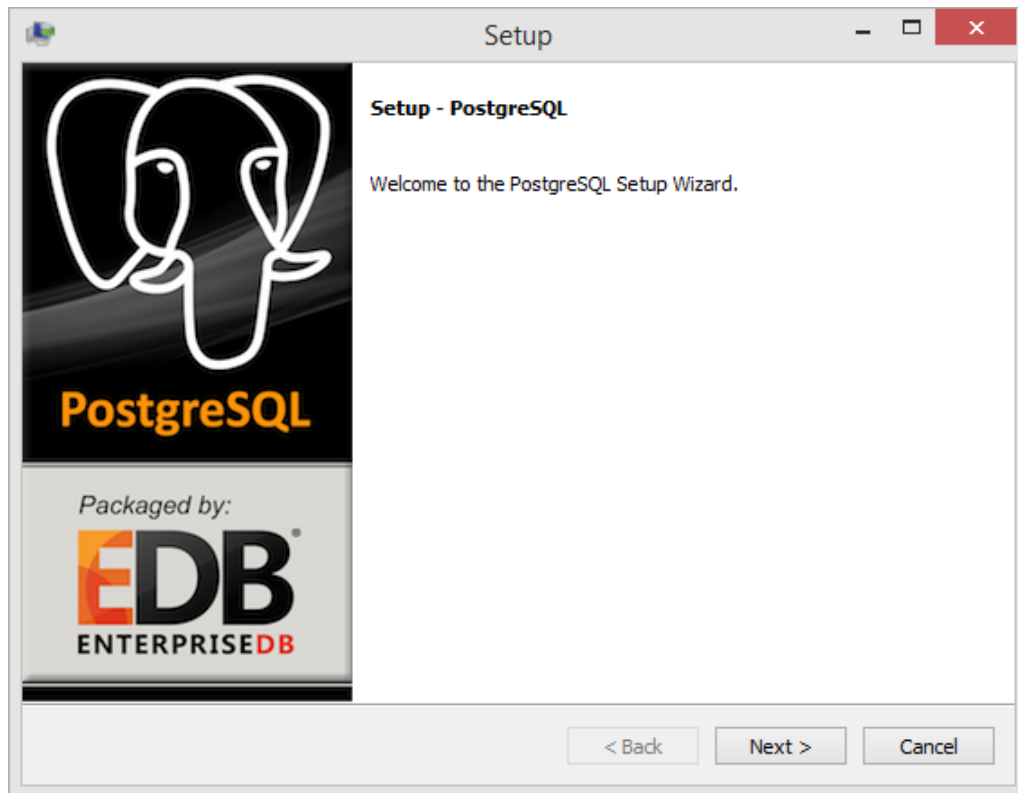
The database management server must be installed before installing the Areashell. It is recommended to use PostgreSQL 9, 10, or 11 database management server.

This installation guide covers the default installation of Areashell AM on a Windows Server using the PostgreSQL Database management server. Installation of other database servers are not covered in this guide. Please refer to vendor's guides to support the installation and configuration of other database server prior to installation of the Areashell AM.

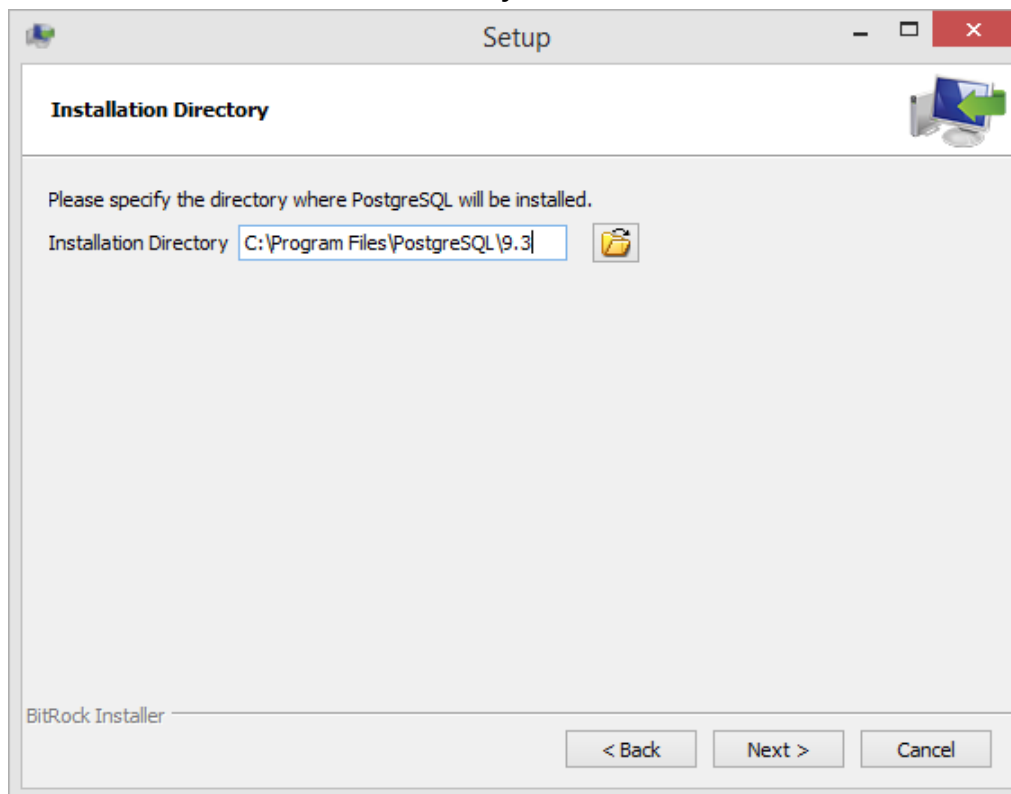
The latest version of PostgreSQL database management server for Windows can be downloaded from EnterpriseDB web site.

1. Download the required version of the installation program of PostgreSQL from EnterpriseDB web site:  
<http://www.enterprisedb.com/products-services-training/pgdownload>  
or from PostgreSQL web site:  
<http://www.postgresql.org/download>
2. Refer to the installation instructions in the PostgreSQL Installation Guide:  
<https://www.enterprisedb.com/docs/en/10.0/instguide/toc.html>

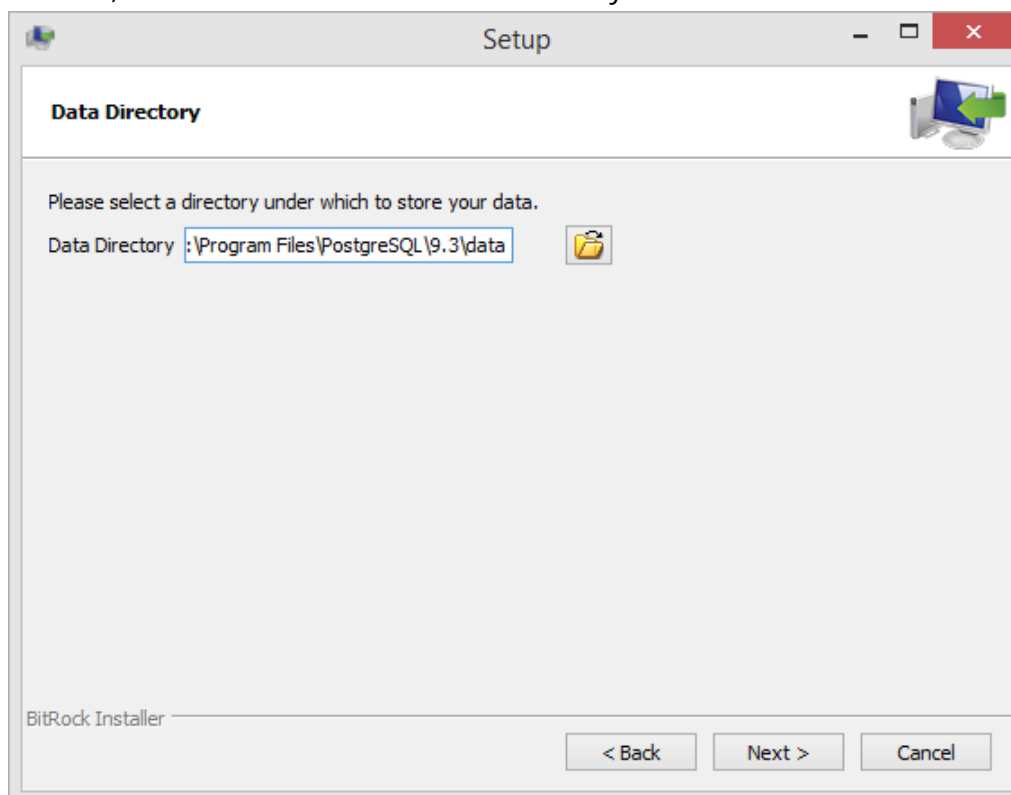
3. Start the PostgreSQL installation program (for example, postgresql-10.6-1-windows-x64.exe) with Administrator's privileges by right clicking the PostgreSQL installation file in Windows Explorer and selecting 'Run as Administrator' from the context menu..
4. The Setup dialog displays. Click **Next** to continue with the installation.



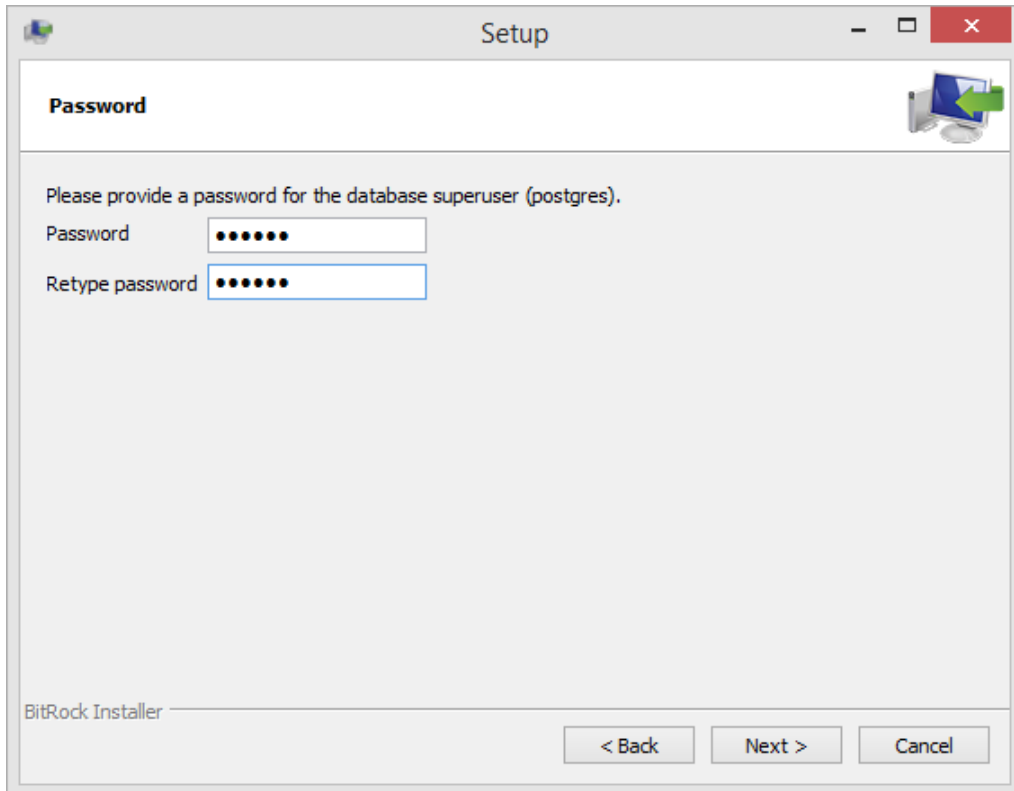
5. In the Installation Directory dialog select the PostgreSQL installation folder, if the default install location does not suit you. Click **Next** to continue.



6. In the Data Directory dialog select the folder where PostgreSQL databases should be created, if the default location does not suit you. Click **Next** to continue.

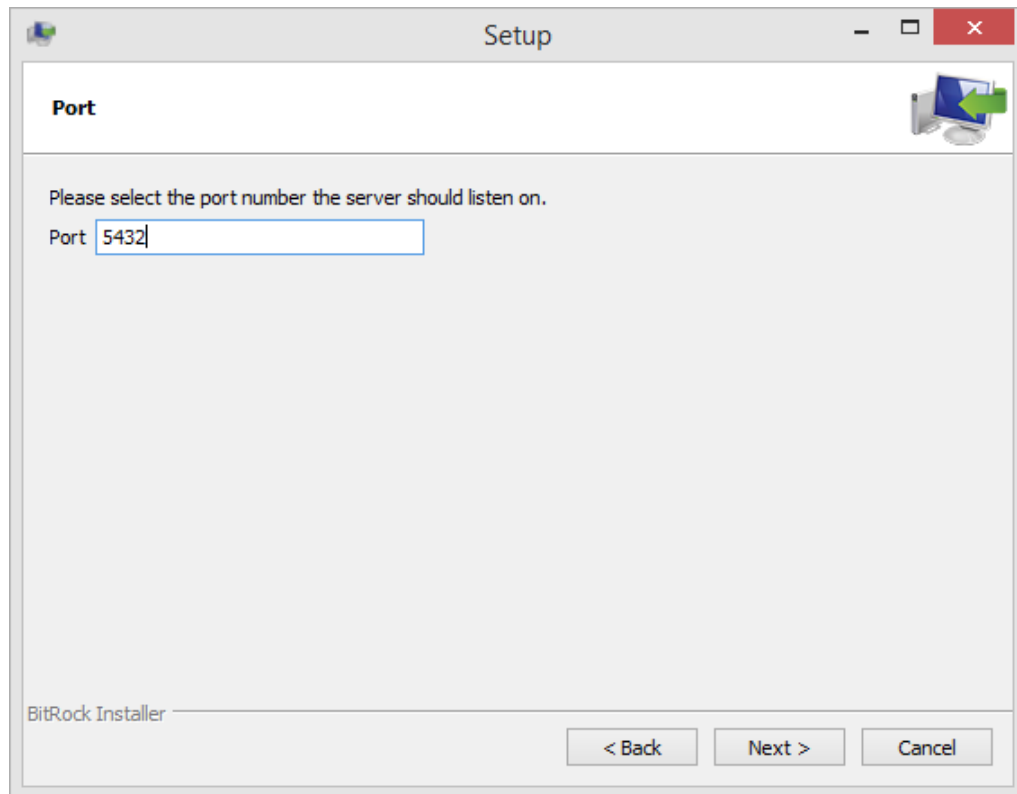


7. In the Password dialog enter the password for both the database superuser (the account name is postgres) and the PostgreSQL service account. Please check your corporate password policy before entering the password. If you do not comply with the password policies, the installation can fail. Click **Next**.

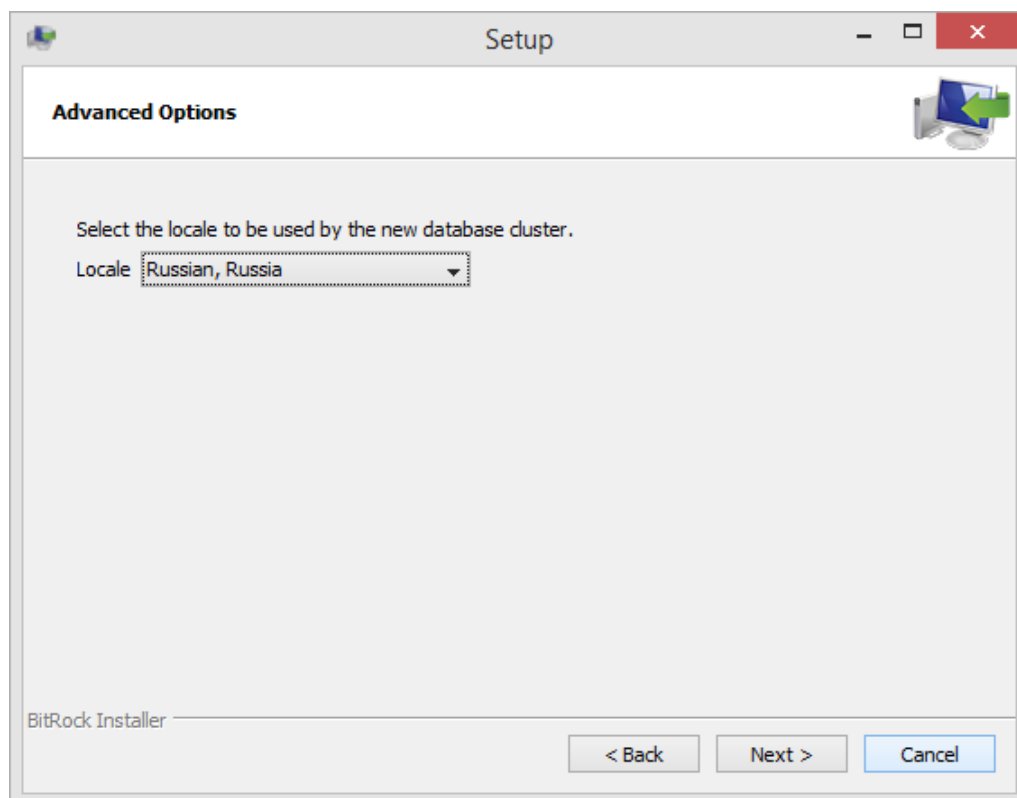


The screenshot shows a Windows-style dialog box titled "Setup". Inside the dialog, the title "Password" is displayed in the top left corner. Below the title, there is a text prompt: "Please provide a password for the database superuser (postgres)." followed by two input fields. The first field is labeled "Password" and the second is labeled "Retype password". Both fields contain masked characters (dots). In the bottom right corner of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a blue border. In the bottom left corner, the text "BitRock Installer" is visible.

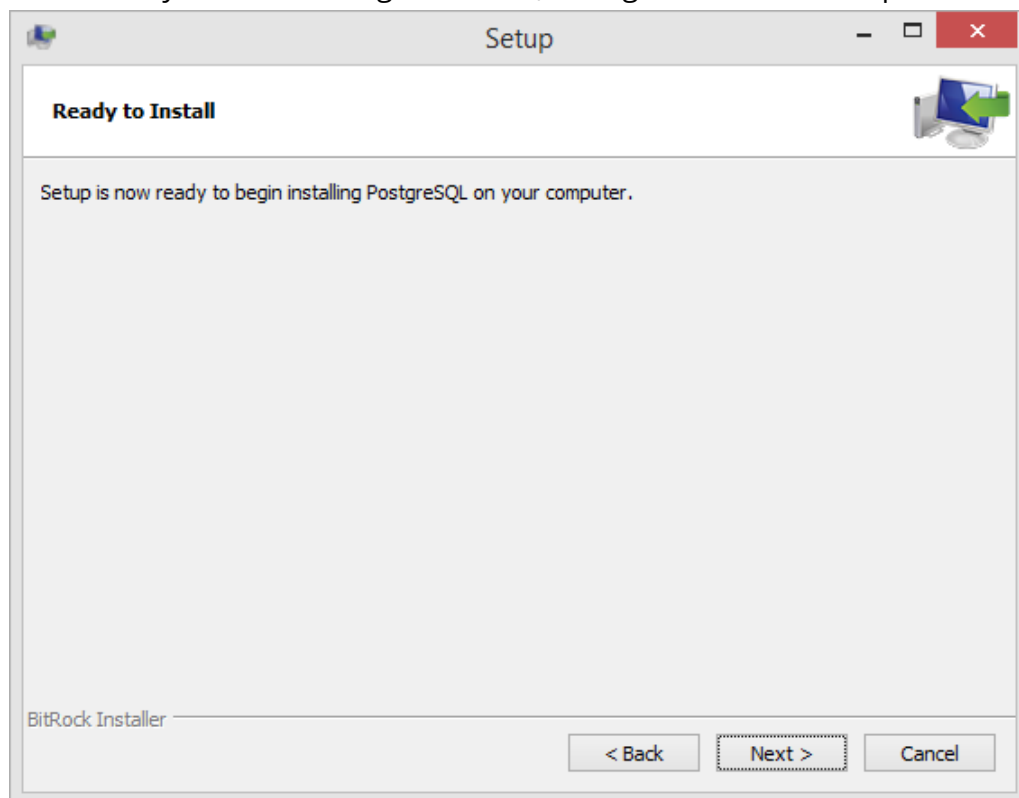
8. In the Port dialog enter the TCP port where PostgreSQL server should be available. Click **Next** to continue.



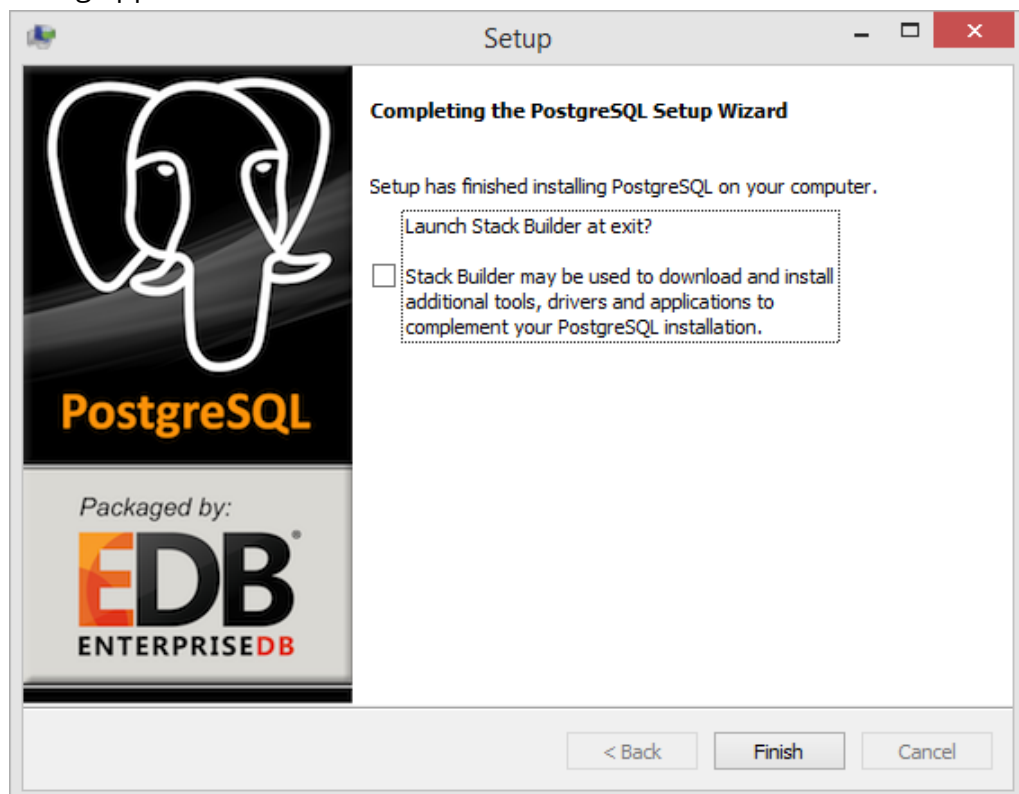
9. In the Advanced Options dialog select the locale supporting your language. Click **Next** to continue.



10. In the Ready to Install dialog click **Next**, to begin the installation process.



11. When PostgreSQL server is installed the Completing the PostgreSQL Setup Wizard dialog appears. **Clear the checkbox** 'Launch Stack Builder at exit' and click **Finish**.



### **4.3.      *Creating the Areashell Database***

After the installing the PostgreSQL server, create the database for Areashell:

1. Start pgAdmin tool by clicking pgAdmin III in Windows Start menu.
2. Right click on the server in the Object browser and select Connect.
3. In the Connect to Server dialog enter the password of the PostgreSQL superuser (the account name is postgres), entered at the time of the installation of the server. Click OK.
4. Right-click Databases in the Object browser and select New Database.
5. Enter the name for new database (for example, areashell). You can change parameters of the new database if you have special requirements or leave default values. It is recommended to leave the encoding of the database on the tab Definition as UTF8. Click OK.

### **4.4.      *Installing Areashell AM with WildFly Application Server***

Areashell Access Management can be installed manually on existing Java EE 7 Full Platform compatible application server or can be installed and configured by the installation program, containing WildFly 14 application server, Areashell server components, database access and other components required for Areashell Access Management.

Download the latest version of the Areashell installation program from the Areashell web site:

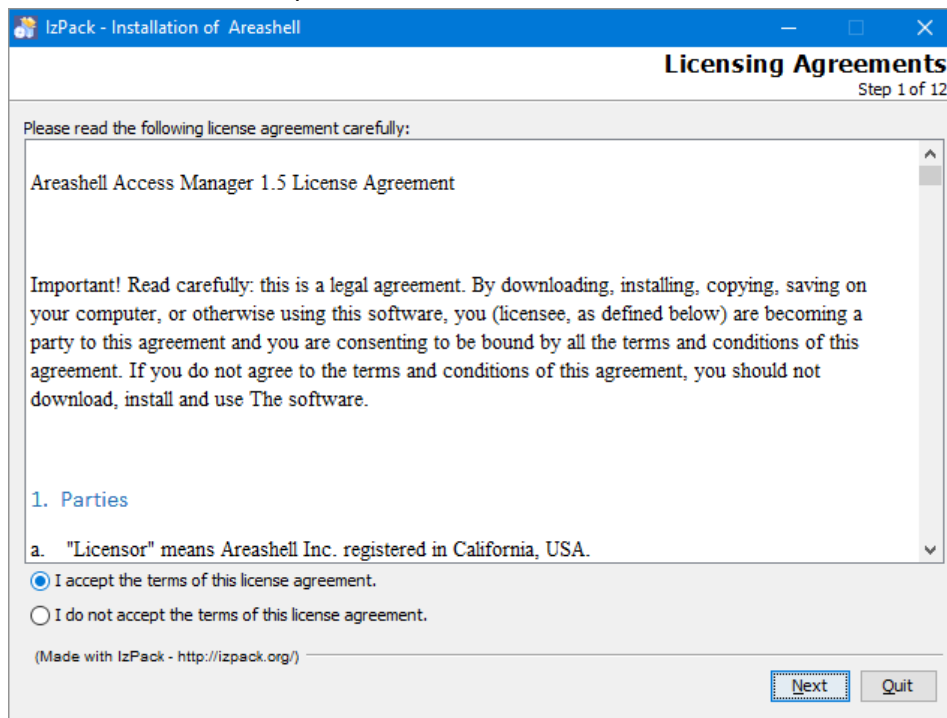
<http://www.areashell.com/download>

#### **4.4.1. Installing Areashell AM with WildFly Application Server by the installation program in GUI Mode**

This section of the installation guide covers the default installation of Areashell AM together with WildFly 14 application server by the Areashell installation program with using of graphic user interface (GUI).

1. Download Areashell installation program from Areashell web site:  
<http://www.areashell.com/download>
2. Start the installation program by entering the next command in the command line:  
`java -jar areashell-1.7-install.jar`  
or right click the install.jar in Windows Explorer and select Open with / Java (TM) Platform SE binary.

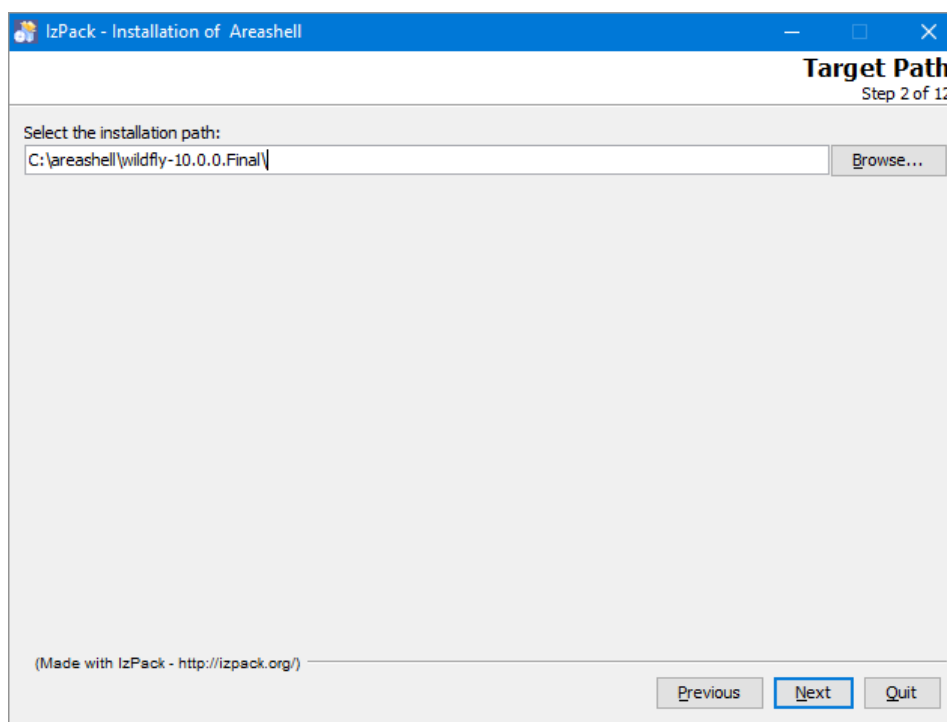
- The License Agreements panel of the Installation of Areashell wizard will appear. You have to select the item "I accept the terms of this license agreement" to continue installation process. Click **Next** to continue.



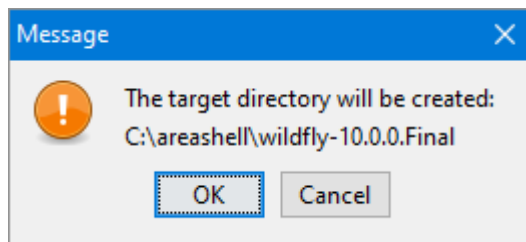
- The Target Path panel of the Installation of Areashell wizard will appear. Select the folder where WildFly application server should be installed, if the default location does not suit you.

**Note:** Do not select folder, containing spaces.

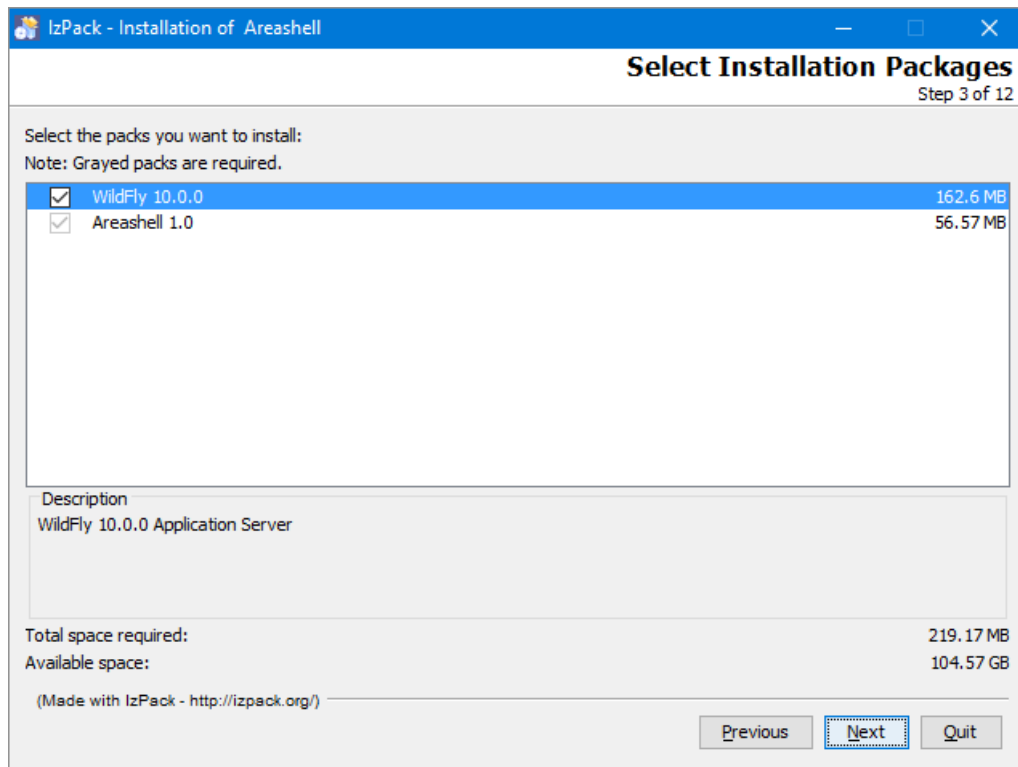
Click **Next** to continue.



5. If selected folder does not exist, the warning window appears. Click **OK**.



6. Select Installation Packages panel appears.  
Leave all components selected. Click **Next** to continue.



7. Database connection parameters panel appears.

Enter the following parameters:

- a. Database host name – the name of the server where the database is located
- b. Database port – TCP port of the database server  
(by default PostgreSQL uses 5432 or 5433)
- c. Database user name
- d. Database user password
- e. Database name – the name of the database (the database should be created before the installation of the Areashell AM server)

Click **Next** to continue.

The screenshot shows a window titled 'IzPack - Installation of Areashell' with a blue header. The main content area is titled 'User Data' and 'Step 4 of 12'. Below this, the section 'Database connection parameters' is displayed. It contains six input fields with labels on the left: 'Database host name or IP address' (value: localhost), 'Database port' (value: 5432), 'Database user name' (value: postgres), 'Database user password' (masked with dots), 'Retype database user password' (masked with dots), and 'Database name' (value: areashell). At the bottom left, there is a small text: '(Made with IzPack - http://izpack.org/)'. At the bottom right, there are three buttons: 'Previous', 'Next' (highlighted with a blue border), and 'Quit'.

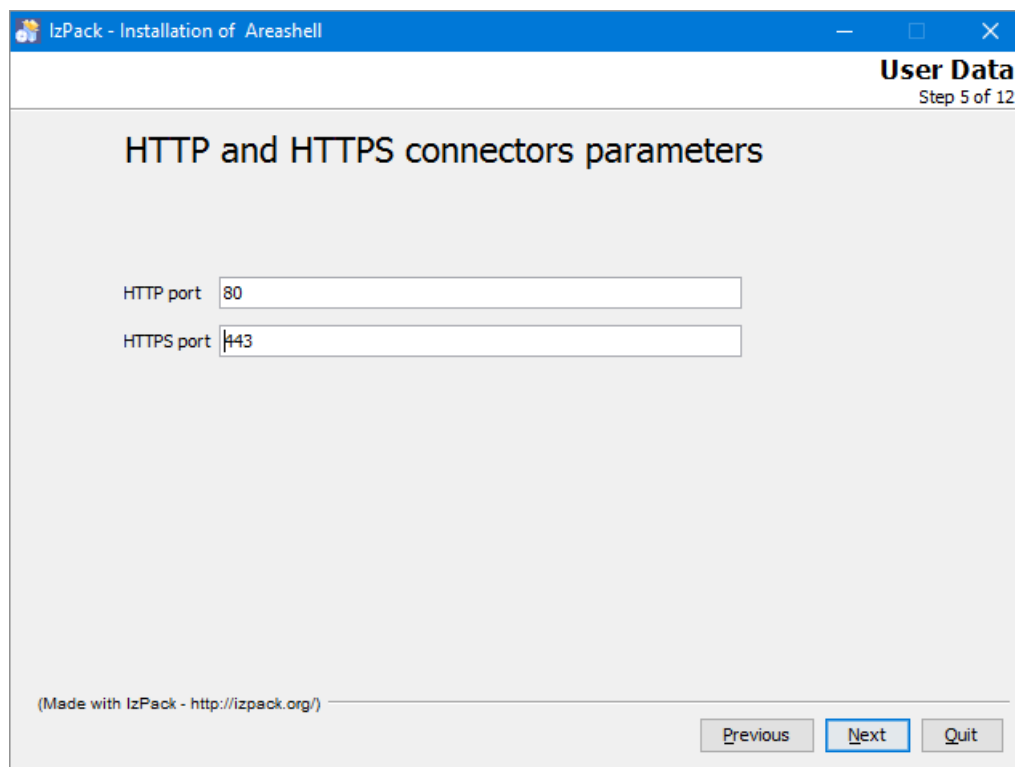
8. HTTP and HTTPS connectors parameters panel appears.

Enter TCP ports for HTTP and secure HTTPS connections, that will be used to connect to the Areashell AM Management Console.

By default, all browsers use ports 80 for HTTP and 443 for HTTPS protocols. If you enter any other values, console users will need to enter these numbers as a part of the connection URL, for example: <https://<full.server.name>:8443/areashell/login> instead of:

<https://<full.server.name>/areashell/login>

Click **Next** to continue.



9. HTTP parameters panel appears.

Enter the following parameters:

- a. Keystore password – The password which is used to protect the integrity of the keystore. Be sure to write down the keystore password and save in a safe location. Password is case sensitive.
- b. FQDN or IP address – a fully qualified domain name or IP address of Areashell AM server, that will be used by users of Areashell AM web console as a part of URL of the console.
- c. Organizational Unit – a value typically given to the entity or group that has management authority over the certificate
- d. Organization – a value typically given to the entity or company that is an owner of the certificate

Click **Next** to continue.

The screenshot shows the 'User Data' window at Step 6 of 12. The title bar reads 'IzPack - Installation of Areashell'. The main heading is 'HTTPS parameters'. Below it, a text block states: 'This step will create self-signed certificate for HTTPS usage. Common name must be the fully qualified domain name (FQDN) or IP address of your server (for example: pacs.mycompany.com)'. There are five input fields: 'Keystore password' and 'Retype keystore password' (both masked with dots), 'FQDN or IP address' (containing 'pacs.areashell.com'), 'Organizational unit' (containing 'Security'), and 'Organization' (containing 'Areashell'). At the bottom, there is a footer '(Made with IzPack - http://izpack.org/)' and three buttons: 'Previous', 'Next' (highlighted with a blue border), and 'Quit'.

10. Authentication Realm Type panel appears.

Select required authentication mechanism and click **Next** to continue.

The screenshot shows the 'User Data' window at Step 7 of 12. The title bar reads 'IzPack - Installation of Areashell'. The main heading is 'Authentication Realm Type'. Below it, the text says 'Select authentication realm type:' and 'Select authentication domain type'. There are two radio button options: 'Active Directory' (which is selected) and 'Areashell Database'. At the bottom, there is a footer '(Made with IzPack - http://izpack.org/)' and three buttons: 'Previous', 'Next' (highlighted with a blue border), and 'Quit'.

11. If you have selected Active Directory authentication mechanism, then Active Directory Connection Settings panel appears. Enter parameters of the connection to the corporate Active Directory and click **Next** to continue.

This panel will not appear if you select Areashell Database authentication mechanism.

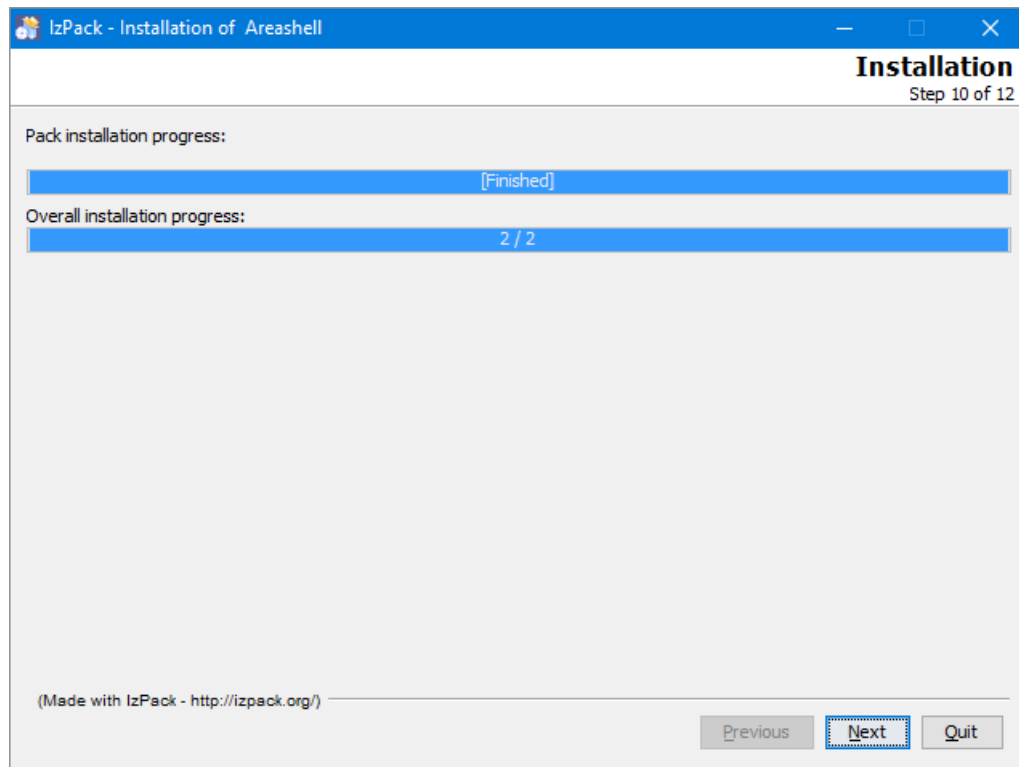
The screenshot shows a window titled "IzPack - Installation of Areashell" with a subtitle "User Data Step 8 of 12". The main heading is "Active Directory Connection Settings". It contains several input fields: "Address or name of the Active Directory server" with the value "pdc.areashell.com", "Port of the Active Directory service (usually 389, 3268)" with the value "389", "Base distinguished name" with the value "cn=Users,dc=areashell,dc=com", "Active Directory binding user name" with the value "searchuser@areashell.com", "Active Directory binding user password" with masked characters "•••••", and "Retype database user password" with masked characters "•••••". At the bottom, there is a footer "(Made with IzPack - <http://izpack.org/>)" and three buttons: "Previous", "Next" (highlighted with a blue border), and "Quit".

12. Summary Configuration Data panel appears.  
Click **Next** to begin the installation process.

The screenshot shows a window titled "IzPack - Installation of Areashell" with a subtitle "Summary Configuration Data Step 9 of 12". The main heading is "Summary Configuration Data". Below the heading, it says "Installation will proceed with the following settings. Press Next to continue." The content area lists the following information: "Installation Path" with the value "C:\areashell\wildfly-10.0.0.Final", "Chosen Installation Packs" with the values "WildFly 10.0.0" and "Areashell 1.0". At the bottom, there is a footer "(Made with IzPack - <http://izpack.org/>)" and three buttons: "Previous", "Next" (highlighted with a blue border), and "Quit".

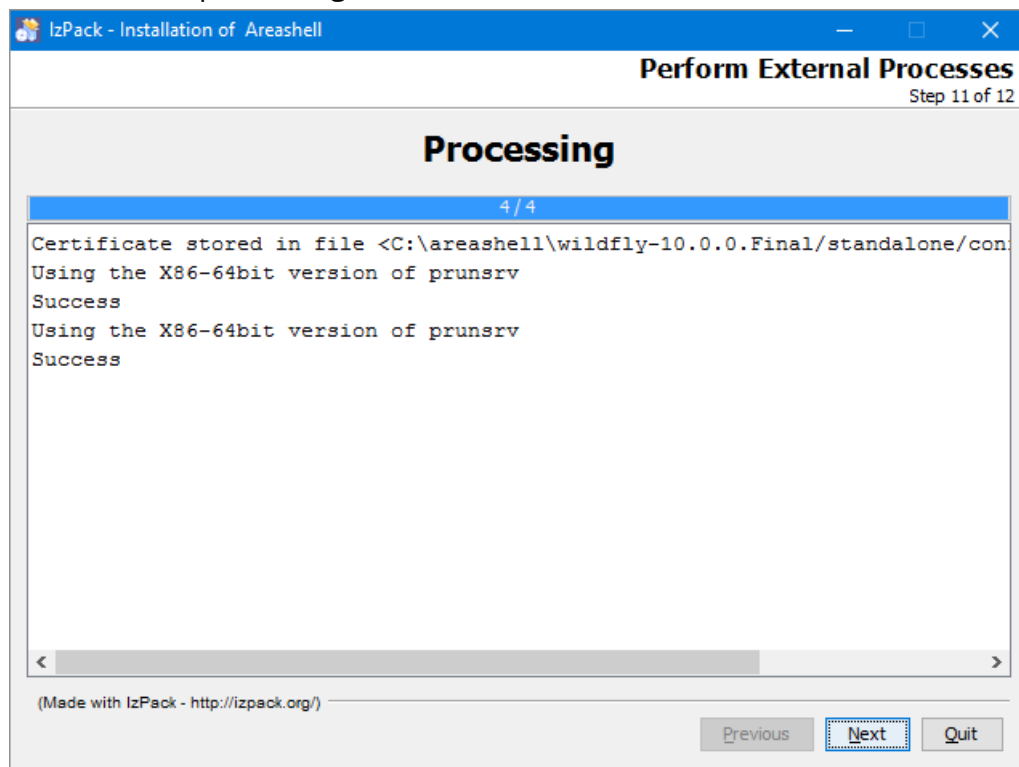
## 13. Installation panel appears.

Wait until the installation finished and click **Next** to continue.

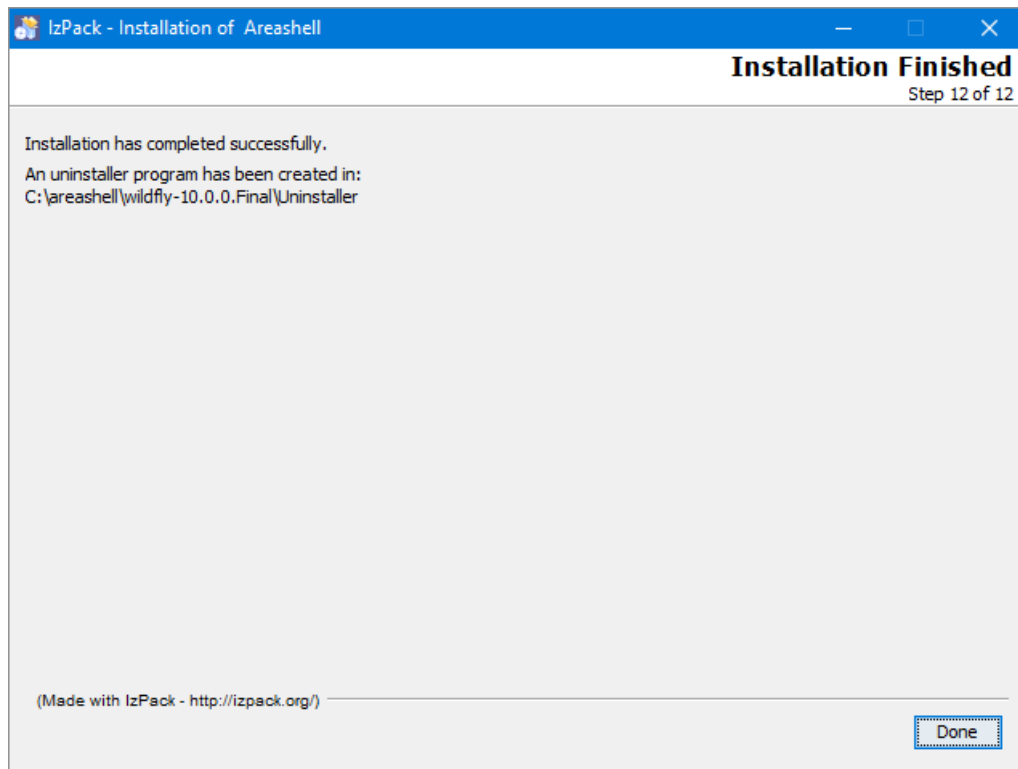


## 14. Processing panel appears.

Wait until the processing finished and click **Next** to continue.



15. Installation Finished panel appears.  
Click **Done** to finish the installation process.



### 4.4.2. Installing Areashell AM with WildFly 14 application server by the installation program in Console Mode

This section of the installation guide covers the default installation of Areashell AM together with WildFly 14 application server by the Areashell installation program in console mode.

1. Download Areashell installation program from Areashell web site:  
<http://www.areashell.com/download>
2. Start the installation program by entering the next command in the command line:  
`java -jar areashell-1.7-install.jar -console`
3. The prompt of the Areashell installation program to select target path will appear. Enter the path where WildFly application server should be installed.

**Note:** Do not enter name, containing spaces.

If the default location does suit you, just press Enter.

```
Nov 19, 2014 1:35:24 PM INFO: Logging initialized at level 'INFO'
Nov 19, 2014 1:35:24 PM INFO: Commandline arguments: -console
Nov 19, 2014 1:35:24 PM INFO: Detected platform:
windows,version=6.3,arch=x64,symbolicName=null,javaVersion=1.8.0_45
Select target path [C:\areashell\wildfly-14.0.1.Final\]
```

1. The prompt to accept Areashell License Agreement and continue will appear. Press Enter to continue.

```
Areashell Access Manager 1.7 License Agreement
Important! Read carefully: this is a legal agreement. By
downloading, installing, copying, saving on your computer, or otherwise using
this software, you (licensee, as defined below) are becoming a party to this
...
Press Enter to continue, X to exit
```

2. The prompt to continue will appear. Enter '1' and press Enter.

```
Press 1 to continue, 2 to quit, 3 to redisplay
1
```

3. If selected path does not exist, the prompt to create it appears. Enter 'Y' and press Enter.

```
WildFly 14.0.1
Enter Y for Yes, N for No: Y
```

4. The prompt to continue will appear. Enter '1' and press Enter.

```
Areashell 1.7 required
Done!
Press 1 to continue, 2 to quit, 3 to redisplay
1
```

5. The set of prompts to set database connection parameters appears.

Enter the following parameters:

- a. Database host name or IP address – the name of the server where the database is located
- b. Database port – TCP port of the database server  
(by default PostgreSQL uses 5432 or 5433)
- c. Database user name
- d. Database user password
- e. Database name – the name of the database (the database should be created before the installation of the Areashell AM server)

Enter '1' and press Enter to continue.

```
Database connection parameters

Database host name or IP address [localhost]

Database port [5432]

Database user name [postgres]

Database user password123456
Retype database user password123456

Database name [areashell]

Press 1 to continue, 2 to quit, 3 to redisplay
1
```

6. The set of prompts to set HTTP and HTTPS connectors parameters appears.

Enter TCP ports for HTTP and secure HTTPS connections, that will be used to connect to the Areashell AM Management Console.

By default, all browsers use ports 80 for HTTP and 443 for HTTPS protocols. If you enter any other values, console users will need to enter these numbers as a part of the connection URL, for example: <https://<full.server.name>:8443/areashell/login> instead of:

<https://<full.server.name>/areashell/login>

Enter '1' and press Enter to continue.

```
HTTP and HTTPS connectors parameters

HTTP port [8080]80

HTTPS port [8443]443
```

```
Press 1 to continue, 2 to quit, 3 to redisplay
```

```
1
```

7. The set of prompts to set HTTP parameters appears.

Enter the following parameters:

- f. Keystore password – The password which is used to protect the integrity of the keystore. Be sure to write down the keystore password and save in a safe location. Password is case sensitive.
- g. FQDN or IP address – a fully qualified domain name or IP address of Areashell AM server, that will be used by users of Areashell AM web console as a part of URL of the console.
- h. Organizational Unit – a value typically given to the entity or group that has management authority over the certificate
- i. Organization – a value typically given to the entity or company that is an owner of the certificate

Enter '1' and press Enter to continue.

```
This step will create self-signed certificate for HTTPS usage. Common name must be the fully qualified domain name (FQDN) or IP address of your server (for example: pacs.mycompany.com)
```

```
FQDN or IP address [pacs.mycompany.com] pacs.mycompany.com
```

```
Organizational unit [] Security
```

```
Organization [] MyCompany
```

```
Press 1 to continue, 2 to quit, 3 to redisplay
```

```
1
```

8. The prompt to set Authentication Realm Type appears.

Select required authentication mechanism by entering '0' or '1' and press Enter.

Enter '0' to use database-based authentication and press Enter to continue.

```
Authentication Realm Type
```

```
Select authentication realm type:
```

```
Select authentication domain type
```

```
0 [] Areashell Database
```

```
1 [] Active Directory
```

```
input selection:
```

```
0
```

```
Press 1 to continue, 2 to quit, 3 to redisplay
```

```
1
```

9. If you have selected Active Directory authentication mechanism, then Active Directory Connection Settings prompt appears. Enter parameters of the connection to the corporate Active Directory and press Enter.  
Enter '1' and press Enter to continue.

```
Active Directory Connection Settings

Address or name of the Active Directory server [pdc.demo.domain.com] pdc.mycompany.com
Port of the Active Directory service (usually 389, 3268) [389]

Base distinguished name [cn=Users,dc=demo,dc=domain,dc=com] cn=Users,dc=mycompany,dc=com

Active Directory binding user name [searchuser@demo.domain.com] areashell@mycompany.com

Active Directory binding user password123456
Retype database user password123456

Press 1 to continue, 2 to quit, 3 to redisplay
1
```

10. Wait until the installation finished and click **Next** to continue.

```
[ Starting to unpack ]
[ Processing package: WildFly 14.0.1 (1/2) ]
[ Processing package: Areashell 1.7 (2/2) ]
[ Unpacking finished ]
[ Starting processing ]
Starting process Generate keystore file (1/3)
Starting process Install service (2/3)
Using the X86-64bit version of prunsrv
Success
Starting process Start service (3/3)
Using the X86-64bit version of prunsrv
Success
Installation was successful
application installed on C:\areashell\wildfly-14.0.1.Final\
[ Writing the uninstaller data ... ]
[ Console installation done ]
```

## 4.5. Installation Summary

If the installation process has completed successfully, the WildFly 14 application server is installed in the next configuration:

- PostgreSQL module is deployed
- EclipseLink is integrated into WildFly server
- Areashell database is registered in the server's configuration
- Keystore with self-signed SSL certificate is created for HTTPS protocol support
- WildFly management user is created with next parameters:
  - o Logon name: admin
  - o Password: admin

**Note:** For security reasons it is recommended to change the password of this user.
- WildFly is integrated with Active Directory (only if this option was selected at the time of installation)
- All modules of the Areashell AM are deployed as a Java EE application and set of JCE resource adapters.
- WildFly is registered as a Windows service and started (in the case of installation on Windows).

## 5. Starting Areashell Access Management server

To start Areashell Access Management server you need to start WildFly application server.

To do this open Windows Services and start service 'Wildfly'.

It is recommended to set automatic startup type for this service to start it automatically after restarting of the server.

If you need to use command prompt to start WildFly application server, it could be started by the next command:

```
standalone.bat -c standalone-full.xml
```

or

```
standalone.sh -c standalone-full.xml
```

Please note that '-c *standalone-full.xml*' parameters should be added.

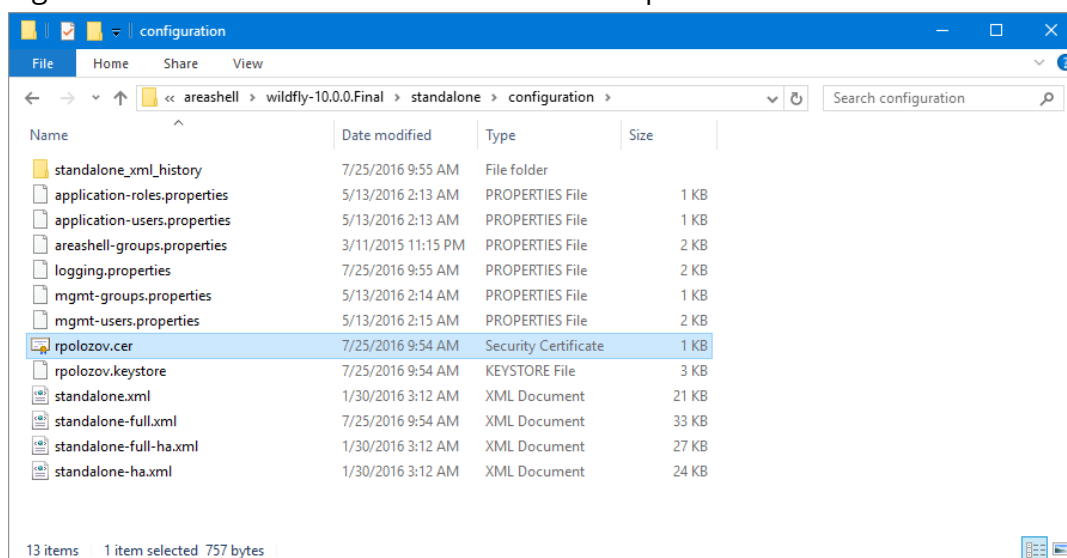
## 6. Installing Server Certificate

To prevent displaying “Your connection is not private” message in web browser it is recommended to install sever certificate to client computers as trusted. Areashell AM Installation Program creates and deploys to WildFly application server self-signed SSL certificate. If you have not changed the installation directory at the time of installation, the certificate is stored in file

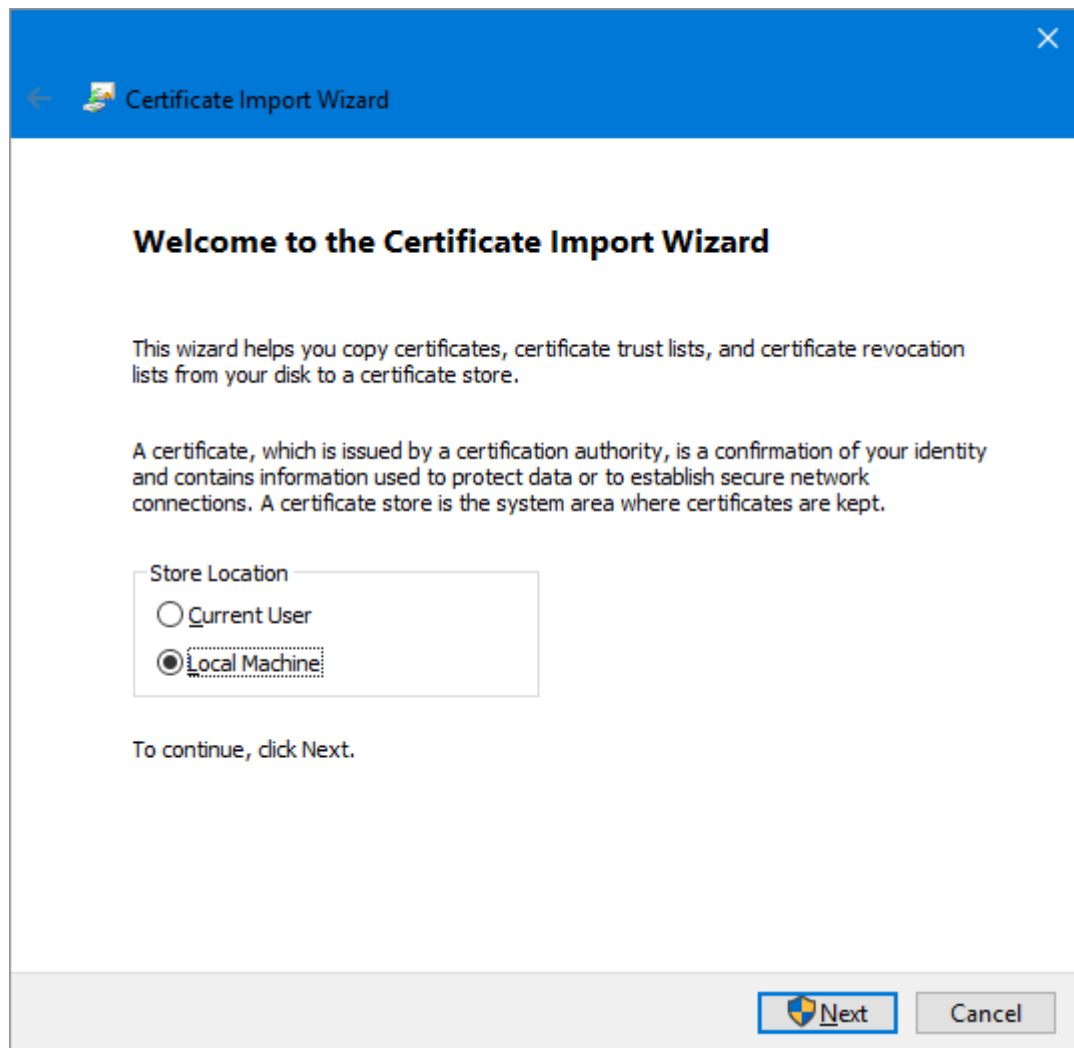
C:\areashell\wildfly-14.0.1.Final\standalone\configuration\<server\_name>.cer

To install this certificate as trusted on a Windows-client:

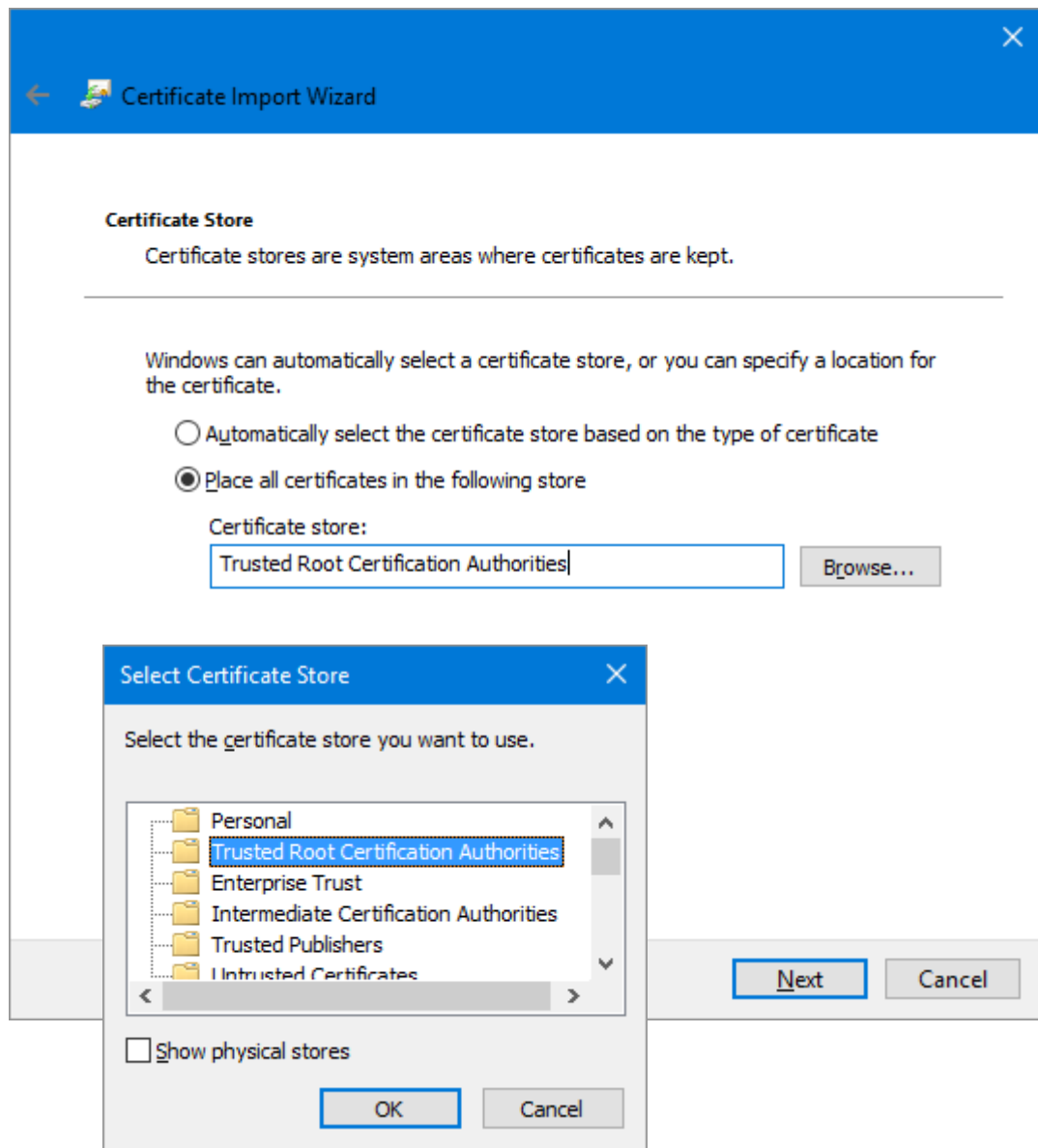
1. Right-click on certificate file in Windows Explorer and select Install Certificate.



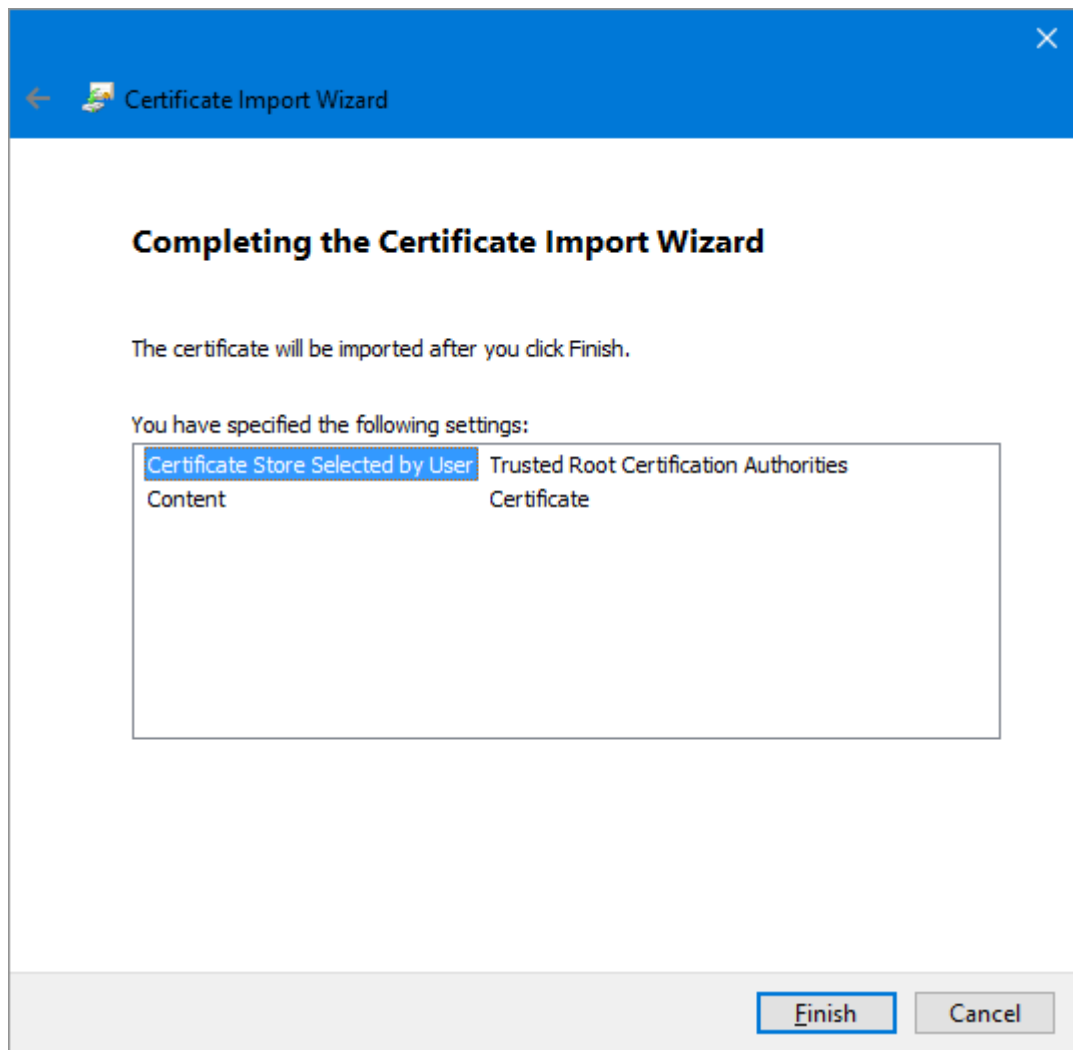
2. Select "Local Machine" and click **Next** to continue.



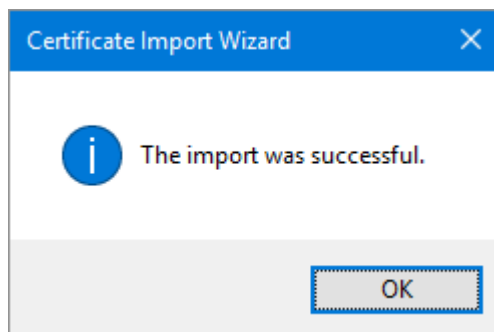
3. Select "Place all certificates in the following store".  
Click **Browse**, select "Trusted Root Certification Authorities", click **OK**.  
Click **Next** to continue.



- Click **Finish** to continue.



- Click **OK**.



- Restart a web browser.

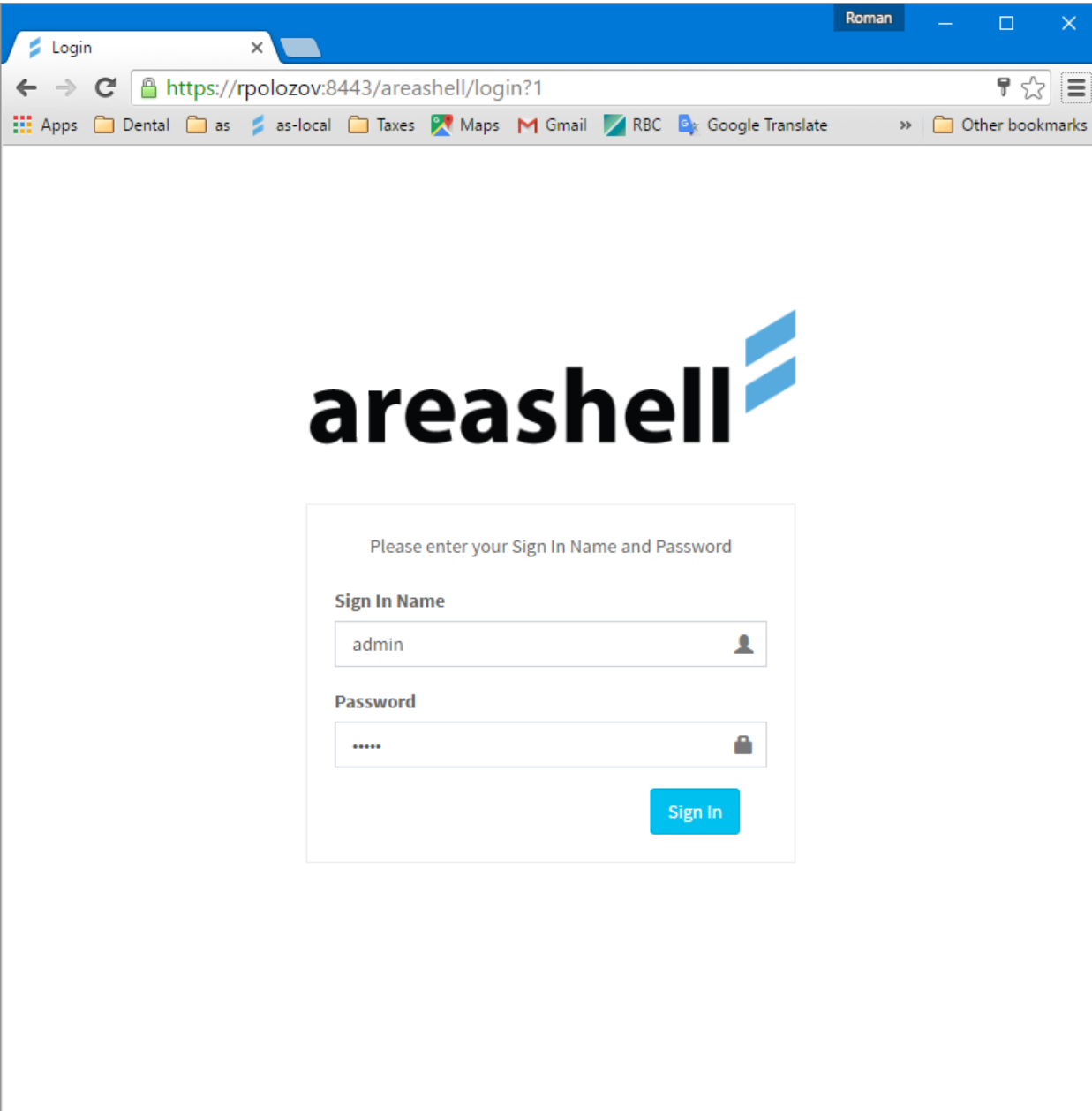
## 7. Launching the Areashell AM Management Console

All functions of Areashell Access Management are available through unified web interface - Areashell Management Console

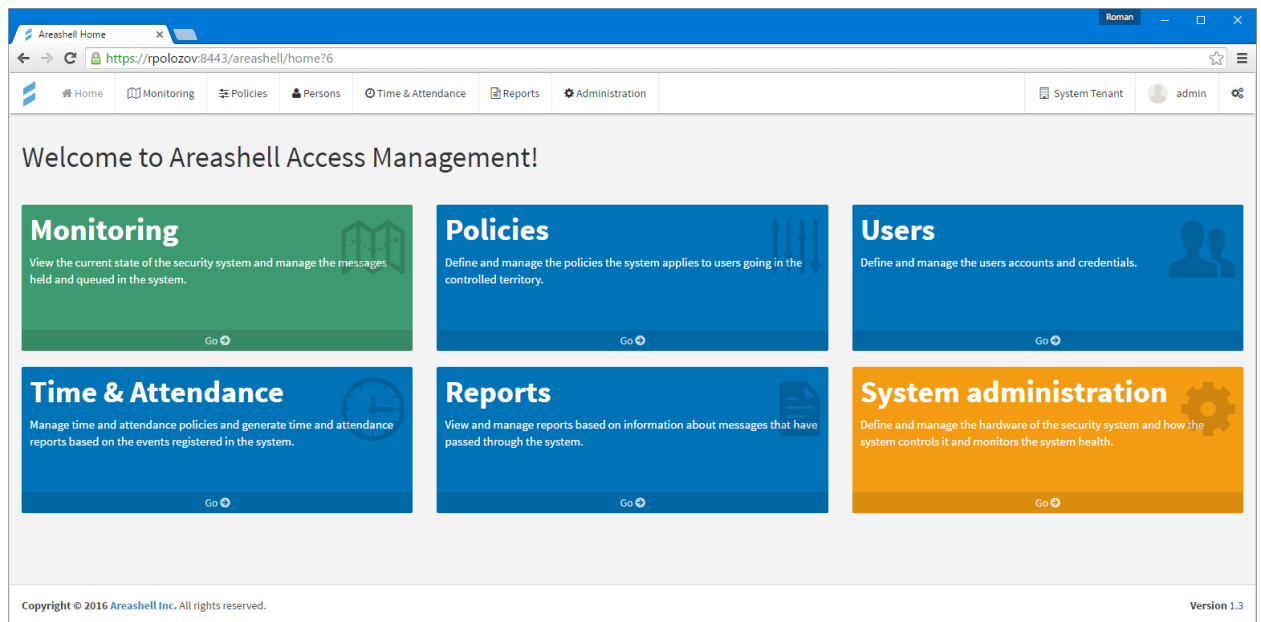
If you have not changed the port for HTTPS protocol at the time of installation, the Management Console is available by the next URL:

<https://<full.server.name>:8443/areashell/login>

To receive access to Areashell Management Console you need to enter user name and password.

A screenshot of a web browser window showing the Areashell login page. The browser's address bar displays the URL 'https://rpolozov:8443/areashell/login?1'. The page features the 'areashell' logo at the top. Below the logo, a login form is centered on the page. The form contains the text 'Please enter your Sign In Name and Password'. It has two input fields: 'Sign In Name' with the value 'admin' and a user icon, and 'Password' with masked characters '\*\*\*\*\*' and a lock icon. A blue 'Sign In' button is positioned at the bottom right of the form. The browser's bookmark bar shows various folders like 'Apps', 'Dental', 'as', 'as-local', 'Taxes', 'Maps', 'Gmail', 'RBC', and 'Google Translate'.

After successful authentication you should see the Home panel of the Areashell Management Console.



## 8. Support

In case of any questions or issues during the installation please contact the Areashell support at [support@areashell.com](mailto:support@areashell.com).