DeskAlerts 9 Installation Guide

Copyright Notice

ToolbarStudio, Inc.
815 North Royal St,
STE 202 Alexandria,
VA 22314 United States

Email: sales@deskalerts.com
Tel: +1-703-881-3166 fax: +1-801-457-8820

Contents

DeskAlerts software supported platforms and pre-requirements

DeskAlerts software requires a Windows-based server to operate.

The client applications are available for:

- Windows 7 (SP1) / 8.1 / 10 with IE 11 installed
- OS X 10.12 (Sierra) or higher
- Android 4.1 or higher
- iOS 8.0 or newer

DeskAlerts Application server requirements

DeskAlerts Application server must be hosted on Windows Server, unless it's serving a rather small audience (below 100 end users), in which case it can be installed on a generic Windows box, with IIS installed on top.

Software requirements include:

- IIS (Internet Information Services) 7.5 or higher
- Windows Server 2012 or newer (2019 is supported)
- ASP.NET 4.8

Hardware requirements depend on the number of end users connected to the system. Note that for each number of users, there's a recommended polling period value, i.e. how often the desktop client apps will connect to the server and check for new content. If you wish to further decrease the polling period, the server specs will have to be scaled up accordingly. If you wish to use non-recommended values – contact DeskAlerts support for advice on scaling.

The default values can be found in a table below:

DeskAlerts Application server requirements

Number of users	1-600	600-2000	2000-10000	10000-20000+*
CPU speed	2GHz (2 core or higher)	3GHz (2 core or higher)	3GHz (4 core or higher)	3GHz or higher (8 core or higher)
RAM volume	1GB	2GB or higher	4GB or higher	8GB or higher
Hard disk space	200 MB for installation files + 1-2GB for log files	200 MB for installation files + 2-4GB for log files	200 MB for installation files + 4-8GB for log files	200 MB for installation files + 8-20 GB for logs
Client poll frequency	60 seconds	60 seconds	120 seconds	120-300 seconds
Network speed	80 Mbps	100 Mbps	150 Mbps	200mbps

*It’s advised to perform the cluster server setup if the product audience exceeds 20.000 people.

DeskAlerts server application can share a single virtual or physical box with other applications. If you plan to host the system in such shared environment – consult DeskAlerts Support regarding the resource scaling.

DeskAlerts Database server requirements

DeskAlerts Server application stores all its data in Microsoft SQL Server database, which can be hosted on a dedicated or shared instance of MS SQL.

For smaller audiences (below 600 end users), SQL Express can be used, while Standard or Enterprise edition is required for larger companies.

DeskAlerts software can operate with both Windows authentication to SQL Server and SQL Server's own (mixed) authentication. However, if you do plan to set up Single Sign On authentication for content creators at a later point, SQL Server own account MUST be used.

For the purpose of installing a new DeskAlerts server or applying server updates, this account must be granted db_owner rights. In between such maintenance works, the elevated access can be revoked and limited to db_datareader + db_datawriter.

Recommended hardware requirements for different audience sizes can be found below:

Number of users	1-600	600-2000	2000-10000	10000-20000+*
CPU speed	1GHz	3GHz or higher	3GHz or higher	3GHz or higher
RAM volume	2GB	2GB min, 4GB recommended	4GB min, 6GB recommended	6GB min, 8GB recommended
Hard disk space	1-5 GB	5-10 GB	10-20 GB	20-50 GB
Hard disk speed	7200 RPM	7200 RPM	10000 RPM	10000 RPM
SQL Server Version	Express/Standard	Express/Standard	Standard	Standard

* For audiences above 20.000 end users, consult DeskAlerts support for scaling advice

Step by step installation

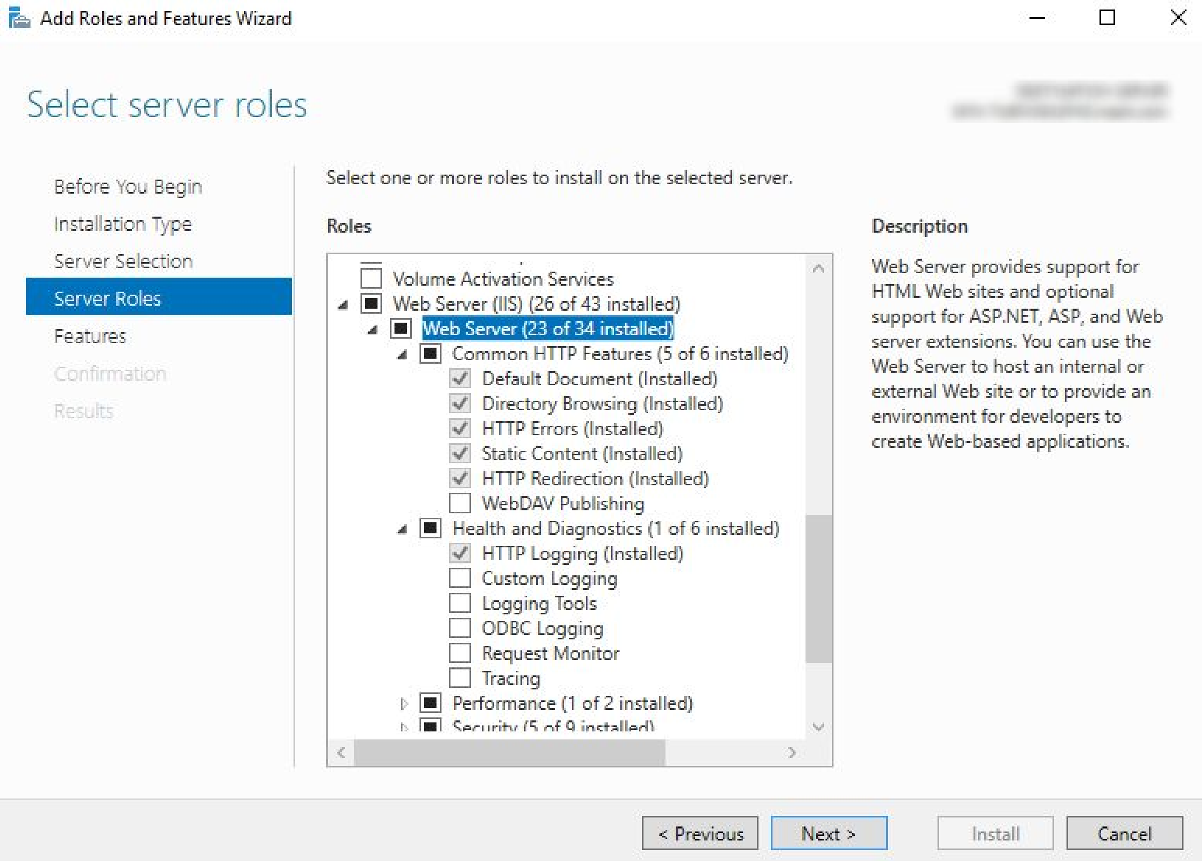
Basic installation and configuration of DeskAlerts server usually takes a few hours – the time depends on the specific environment configuration (proxies, firewalls, Active Directory policies)

Pre-installation steps

Before launching the DeskAlers Server installation script, you must ensure, that you have all necessary accounts to perform the installation, and that your server has all necessary IIS components installed. If you are installing a trial version, make sure that you got a valid trial key from DeskAlerts Support.

IIS components required to run DeskAlerts server

To successfully run DeskAlerts Server application on IIS, the following items will have to be enabled (through Server Manager "add roles and features" wizard):



Add Roles and Features Wizard

Select server roles

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

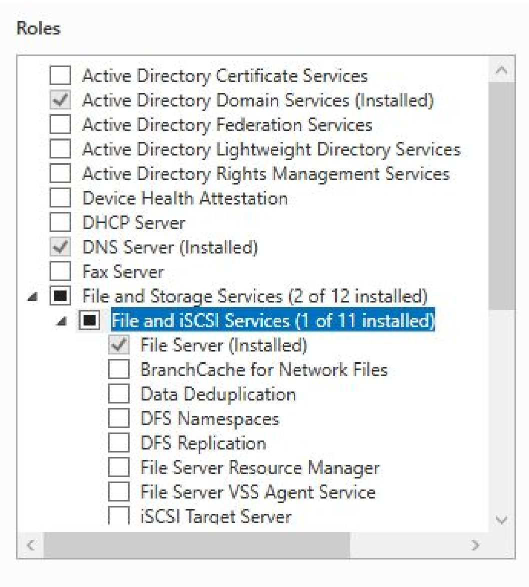
Select one or more roles to install on the selected server.

Roles

- □ Volume Activation Services
- ■ Web Server (IIS) (26 of 43 installed)
  - ■ Web Server (23 of 34 installed)
    - ■ Common HTTP Features (5 of 6 installed)
      - ☑ Default Document (Installed)
      - ☑ Directory Browsing (Installed)
      - ☑ HTTP Errors (Installed)
      - ☑ Static Content (Installed)
      - ☑ HTTP Redirection (Installed)
      - □ WebDAV Publishing
    - ■ Health and Diagnostics (1 of 6 installed)
      - ☑ HTTP Logging (Installed)
      - □ Custom Logging
      - □ Logging Tools
      - □ ODBC Logging
      - □ Request Monitor
      - □ Tracing
    - ■ Performance (1 of 2 installed)
    - ■ Security (5 of 9 installed)

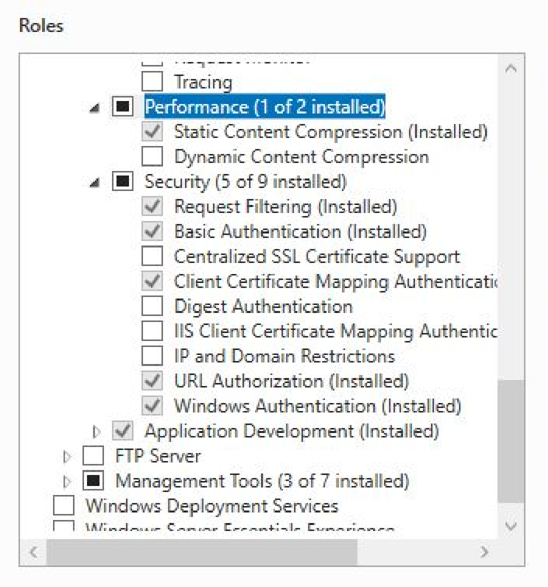
Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.



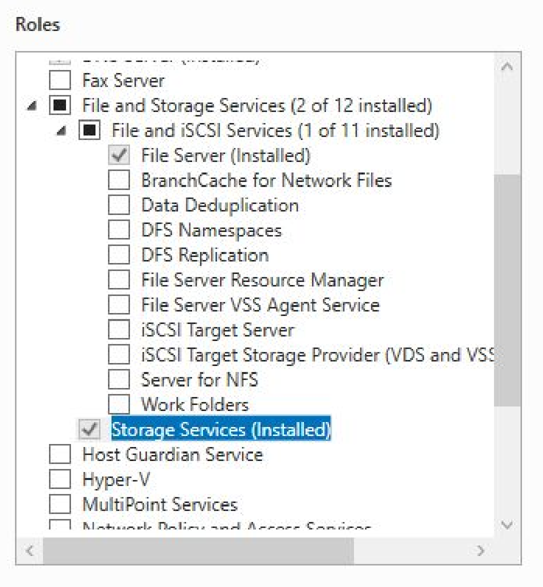
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
  - ■ File and iSCSI Services (1 of 11 installed)
    - ☑ File Server (Installed)
    - □ BranchCache for Network Files
    - □ Data Deduplication
    - □ DFS Namespaces
    - □ DFS Replication
    - □ File Server Resource Manager
    - □ File Server VSS Agent Service
    - □ iSCSI Target Server



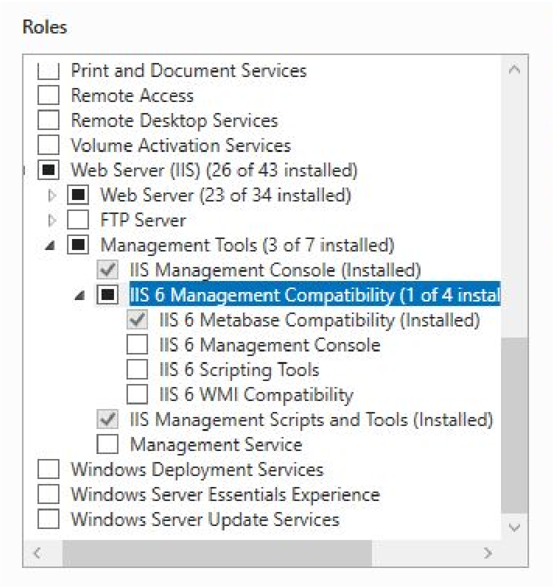
Roles

- □ Tracing
- ■ Performance (1 of 2 installed)
  - ☑ Static Content Compression (Installed)
  - □ Dynamic Content Compression
- ■ Security (5 of 9 installed)
  - ☑ Request Filtering (Installed)
  - ☑ Basic Authentication (Installed)
  - □ Centralized SSL Certificate Support
  - ☑ Client Certificate Mapping Authenticati
  - □ Digest Authentication
  - □ IIS Client Certificate Mapping Authentic
  - □ IP and Domain Restrictions
  - ☑ URL Authorization (Installed)
  - ☑ Windows Authentication (Installed)
- ☑ Application Development (Installed)
- □ FTP Server
- ■ Management Tools (3 of 7 installed)
- □ Windows Deployment Services



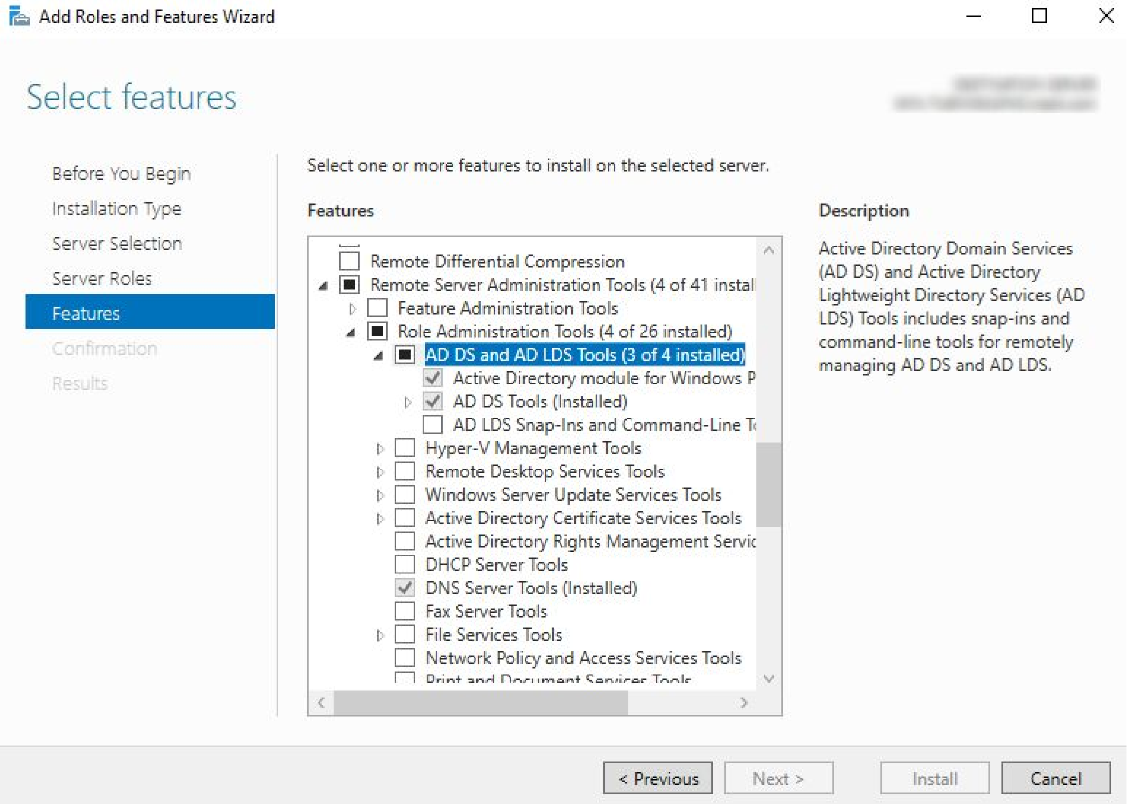
Roles

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



Roles

- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (26 of 43 installed)
  - ■ Web Server (23 of 34 installed)
  - □ FTP Server
  - ■ Management Tools (3 of 7 installed)
    - ☑ IIS Management Console (Installed)
    - ■ IIS 6 Management Compatibility (1 of 4 instal
      - ☑ IIS 6 Metabase Compatibility (Installed)
      - □ IIS 6 Management Console
      - □ IIS 6 Scripting Tools
      - □ IIS 6 WMI Compatibility
    - ☑ IIS Management Scripts and Tools (Installed)
    - □ Management Service
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services



Add Roles and Features Wizard

Select features

[redacted]

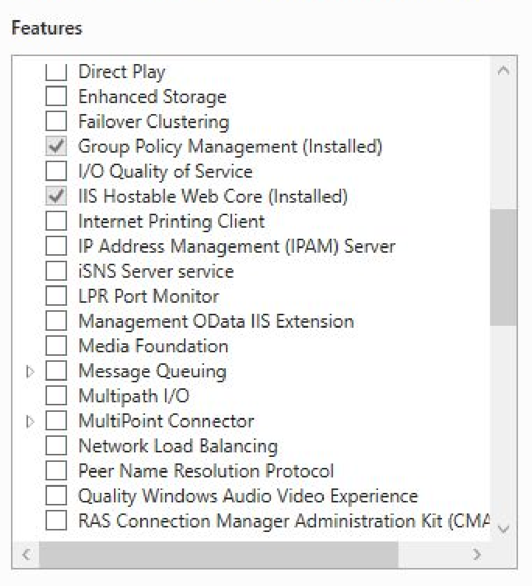
Select one or more features to install on the selected server.

Features

- ☐ Remote Differential Compression
- ■ Remote Server Administration Tools (4 of 41 instal
  - ☐ Feature Administration Tools
  - ■ Role Administration Tools (4 of 26 installed)
    - ■ AD DS and AD LDS Tools (3 of 4 installed)
      - ☑ Active Directory module for Windows P
      - ☑ AD DS Tools (Installed)
      - ☐ AD LDS Snap-Ins and Command-Line T
    - ☐ Hyper-V Management Tools
    - ☐ Remote Desktop Services Tools
    - ☐ Windows Server Update Services Tools
    - ☐ Active Directory Certificate Services Tools
    - ☐ Active Directory Rights Management Servic
    - ☐ DHCP Server Tools
    - ☑ DNS Server Tools (Installed)
    - ☐ Fax Server Tools
    - ☐ File Services Tools
    - ☐ Network Policy and Access Services Tools
    - ☐ Print and Document Services Tools

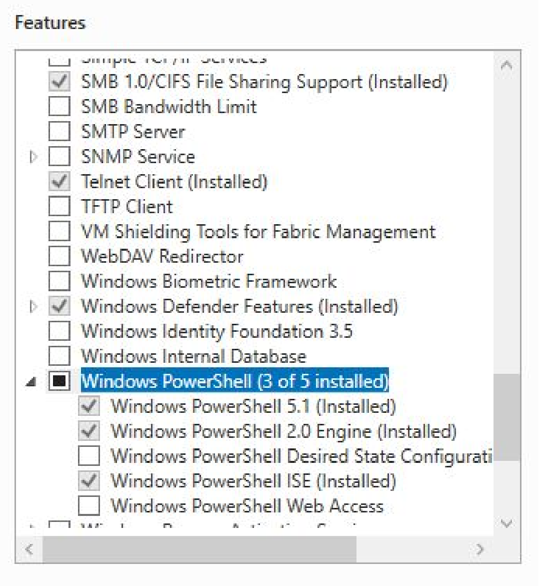
Description

Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS) Tools includes snap-ins and command-line tools for remotely managing AD DS and AD LDS.



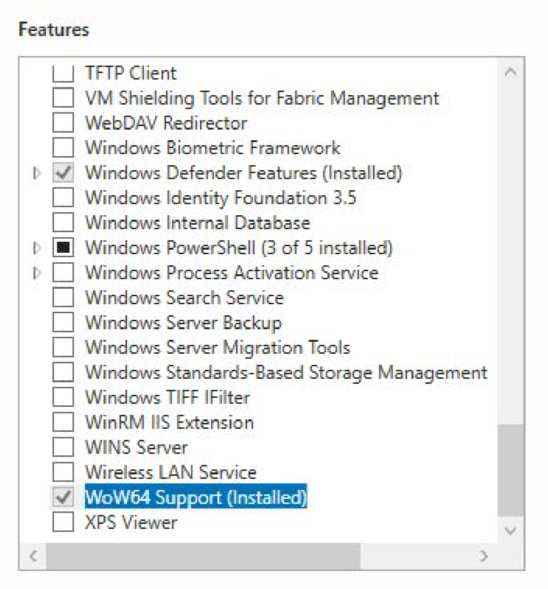
Features

- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☑ Group Policy Management (Installed)
- ☐ I/O Quality of Service
- ☑ IIS Hostable Web Core (Installed)
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ iSNS Server service
- ☐ LPR Port Monitor
- ☐ Management OData IIS Extension
- ☐ Media Foundation
- ☐ Message Queuing
- ☐ Multipath I/O
- ☐ MultiPoint Connector
- ☐ Network Load Balancing
- ☐ Peer Name Resolution Protocol
- ☐ Quality Windows Audio Video Experience
- ☐ RAS Connection Manager Administration Kit (CMA



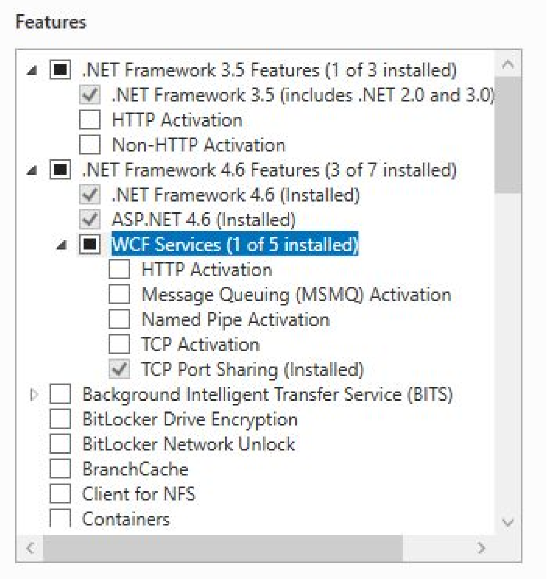
Features

- ☐ Simple TCP/IP Services
- ☑ SMB 1.0/CIFS File Sharing Support (Installed)
- ☐ SMB Bandwidth Limit
- ☐ SMTP Server
- ☐ SNMP Service
- ☑ Telnet Client (Installed)
- ☐ TFTP Client
- ☐ VM Shielding Tools for Fabric Management
- ☐ WebDAV Redirector
- ☐ Windows Biometric Framework
- ☑ Windows Defender Features (Installed)
- ☐ Windows Identity Foundation 3.5
- ☐ Windows Internal Database
- ■ Windows PowerShell (3 of 5 installed)
  - ☑ Windows PowerShell 5.1 (Installed)
  - ☑ Windows PowerShell 2.0 Engine (Installed)
  - ☐ Windows PowerShell Desired State Configurati
  - ☑ Windows PowerShell ISE (Installed)
  - ☐ Windows PowerShell Web Access
- ☐ Windows Process Activation Servic



Features

- □ TFTP Client
- □ VM Shielding Tools for Fabric Management
- □ WebDAV Redirector
- □ Windows Biometric Framework
- ☑ Windows Defender Features (Installed)
- □ Windows Identity Foundation 3.5
- □ Windows Internal Database
- ■ Windows PowerShell (3 of 5 installed)
- □ Windows Process Activation Service
- □ Windows Search Service
- □ Windows Server Backup
- □ Windows Server Migration Tools
- □ Windows Standards-Based Storage Management
- □ Windows TIFF IFilter
- □ WinRM IIS Extension
- □ WINS Server
- □ Wireless LAN Service
- ☑ WoW64 Support (Installed)
- □ XPS Viewer



Features

- ■ .NET Framework 3.5 Features (1 of 3 installed)
  - ☑ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - □ HTTP Activation
  - □ Non-HTTP Activation
- ■ .NET Framework 4.6 Features (3 of 7 installed)
  - ☑ .NET Framework 4.6 (Installed)
  - ☑ ASP.NET 4.6 (Installed)
  - ■ WCF Services (1 of 5 installed)
    - □ HTTP Activation
    - □ Message Queuing (MSMQ) Activation
    - □ Named Pipe Activation
    - □ TCP Activation
    - ☑ TCP Port Sharing (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers

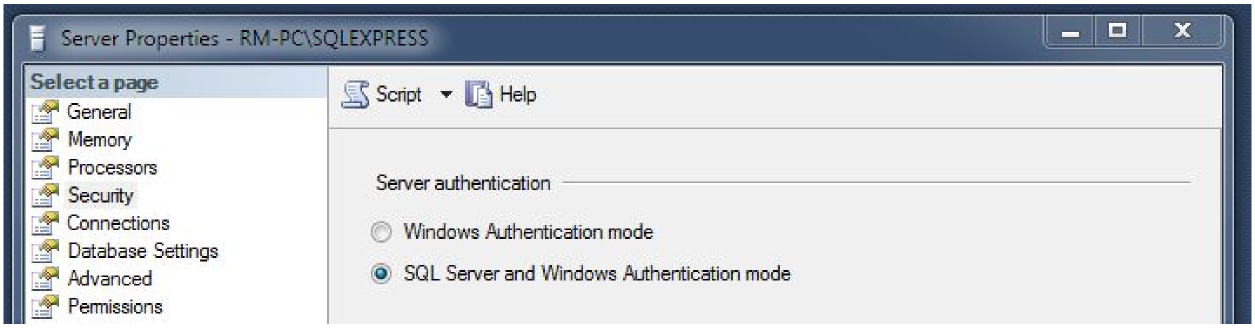
Another important pre-requirement is having **.NET Framework 4.8** installed to support all latest DeskAlerts features.

Accounts required to run DeskAlerts server installation

To run DeskAlerts server application you will require two main accounts - the one which will be used as IIS application pool identity, and the one used for database connections. Here, you have two options, depending on whether you're planning on setting Single Sign On access for content creators.

Option 1. Single Sign On required

To set up DeskAlerts Single Sign On, you will need a separate SQL Server login to access DeskAlerts database. For this, your MSSQL instance should support mixed authentication:



Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Once the mixed authentication is enabled, create an empty database for DeskAlerts data, and a new SQL login with db_owner access to it - this is sufficient to alter the database structure and fill it with information.

Write down the access credentials for this newly created SQL login - it will be used during the installation

The second account you'll need is a service account with non-expiring password and local admin rights on DeskAlerts Application server. It will be used in Application Pool Identity configuration later on.

Option 2. Single Sign On not required

If SSO is not required, you may use Windows account to connect to DeskAlerts database. It is advised that the account you're using to connect to database has local admin rights on DeskAlerts Application server and a password that won't expire.

Once you have such service account, go to your MSSQL instance and create a new database for DeskAlerts. Then, add the service account to the list of valid SQL Logins for this instance, with the db_owner rights for the DeskAlerts database.

Later on, after running DeskAlerts Server installation package, you will also need to assign this account as an IIS Application Pool Identity for the pool hosting DeskAlerts server application.

Some extra requirements for additional modules setup

Some of the DeskAlerts solution modules may have additional requirements, please check the table below and verify if you may be missing something for one of the purchased modules:

Module	**Requirements**
SMS Module	SMS gateway you'll be using should be accessible from DA server via the TCP port required by its documentation – some firewall configuration may be required
Screensaver Module	Employees' screensavers must not be managed by Group Policy (it will override any DeskAlerts changes)
Wallpaper Module	Employees' wallpapers must not be managed by Group Policy (it will override any DeskAlerts changes)

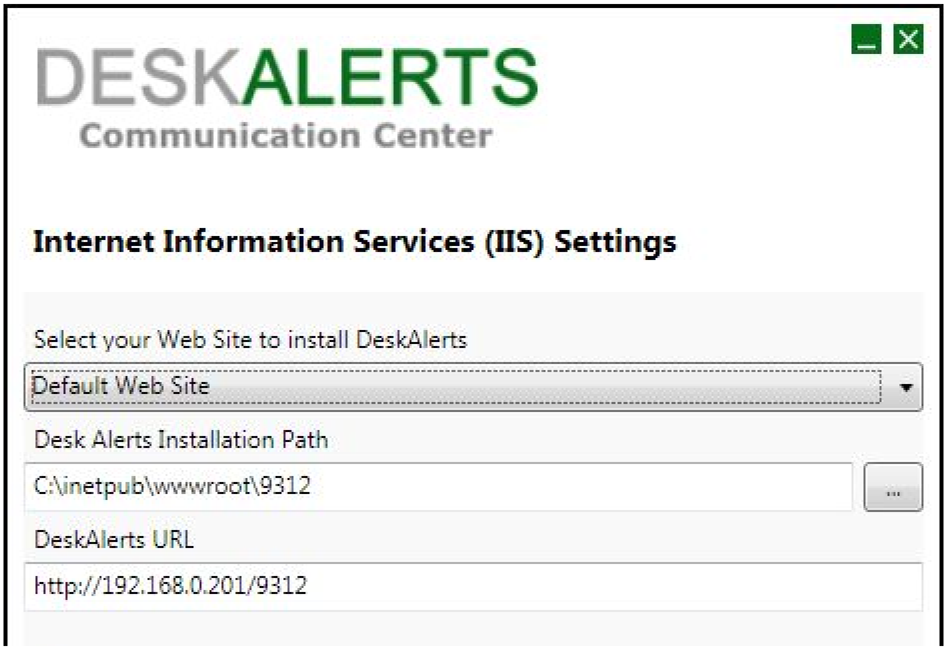
RSS Module	The RSS feeds used need to be accessible from the Application server, since the RSS reader is the part of server application
Active Directory module	The AD domain controller should be accessible for LDAP requests via port 389 or 636 if LDAPS is used
Mobile alerts module	Push notification services of Apple and Google must be accessible via ports 2195 and 443 respectively

Deploying DeskAlerts server

The package you received from DeskAlerts contains the installation package for DA server and the DeskAlerts client builder. The server installer executable is named **DeskAlerts.Server.vx.x.x.x.x.exe**, where x.x.x.x is a version number. To start the installation, copy the file to Application server and launch it as Administrator.

As first two steps, you will be presented with the EULA and the form to enter your trial key if you're installing a trial version. If you don't have a trial key yet, request it from DeskAlerts Support or sales representative.

Next two steps after requirements verification prompt you to enter the IIS options and database connection parameters. The IIS options include the DeskAlerts installation path (actual directory where the software will be installed) and DeskAlerts URL (the link the publishers and client applications will use to access the server dashboard). To avoid firewall and DNS-related issues, it usually a good idea to check whether the server name automatically supplied here is accessible from one of the potential employee workstations.



DESKALERTS
Communication Center

Internet Information Services (IIS) Settings

Select your Web Site to install DeskAlerts: Default Web Site

Desk Alerts Installation Path: C:\inetpub\wwwroot\9312

DeskAlerts URL: http://192.168.0.201/9312

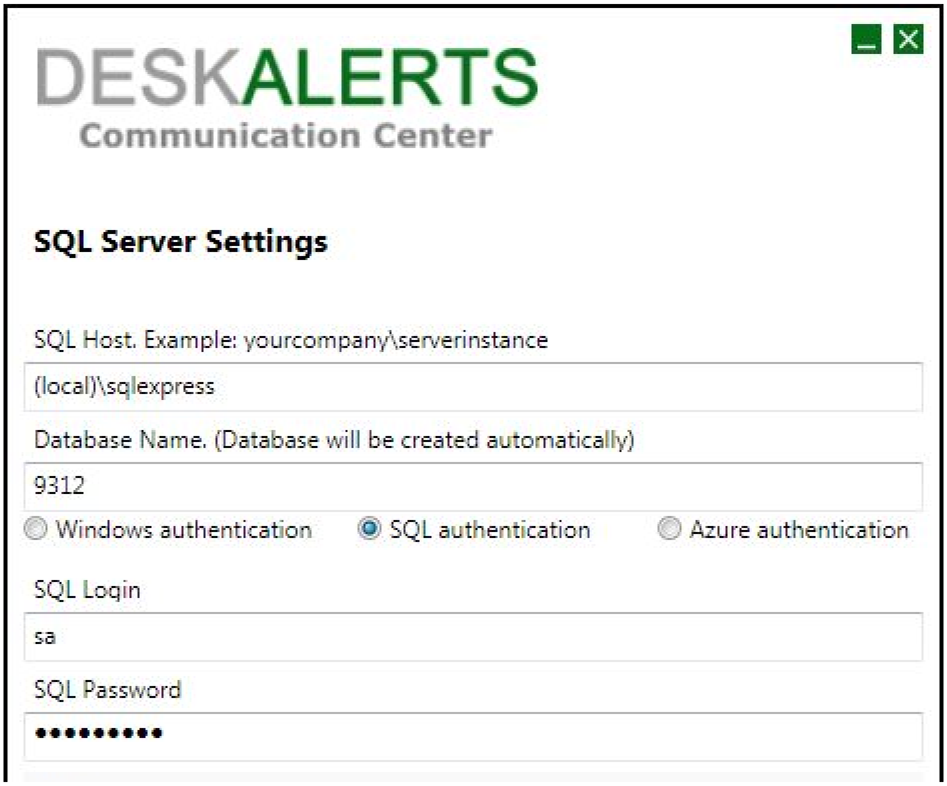
The SQL server settings step will also perform a validation of all information entered. If you encounter errors – check "Help" section in the installer window for hints.

On the database configuration stage, select a proper authentication type. Windows authentication can only be used if you're not planning to set up SSO authentication for content creators.

Azure authentication should only be used if you’re using MSSQL instance in the cloud, provided by MS Azure as a service.

If you’re using SQL authentication, use the login and password you created in Accounts required to run DeskAlerts server installation

If you are performing a server update (database already exists), you will be prompted whether you need to update the data in existing database, or drop it and create a new one. Click “Yes” to keep all existing data, including messages history, user information etc.



DESKALERTS
Communication Center

SQL Server Settings

SQL Host. Example: yourcompany\serverinstance

(local)\sqlexpress

Database Name. (Database will be created automatically)

9312

○ Windows authentication ● SQL authentication ○ Azure authentication

SQL Login

sa

SQL Password

●●●●●●●●●●

Next steps allow you to select the modules to install. Some of these modules also have installer steps for additional configuration, but the module configuration can also be performed later, from the web UI.

After clicking through module configuration steps (if any of these were necessary), you will be presented with the final step – click “Install” to launch the installation process. Depending on your server performance and existing database size, the process might take up to 10-20 minutes.

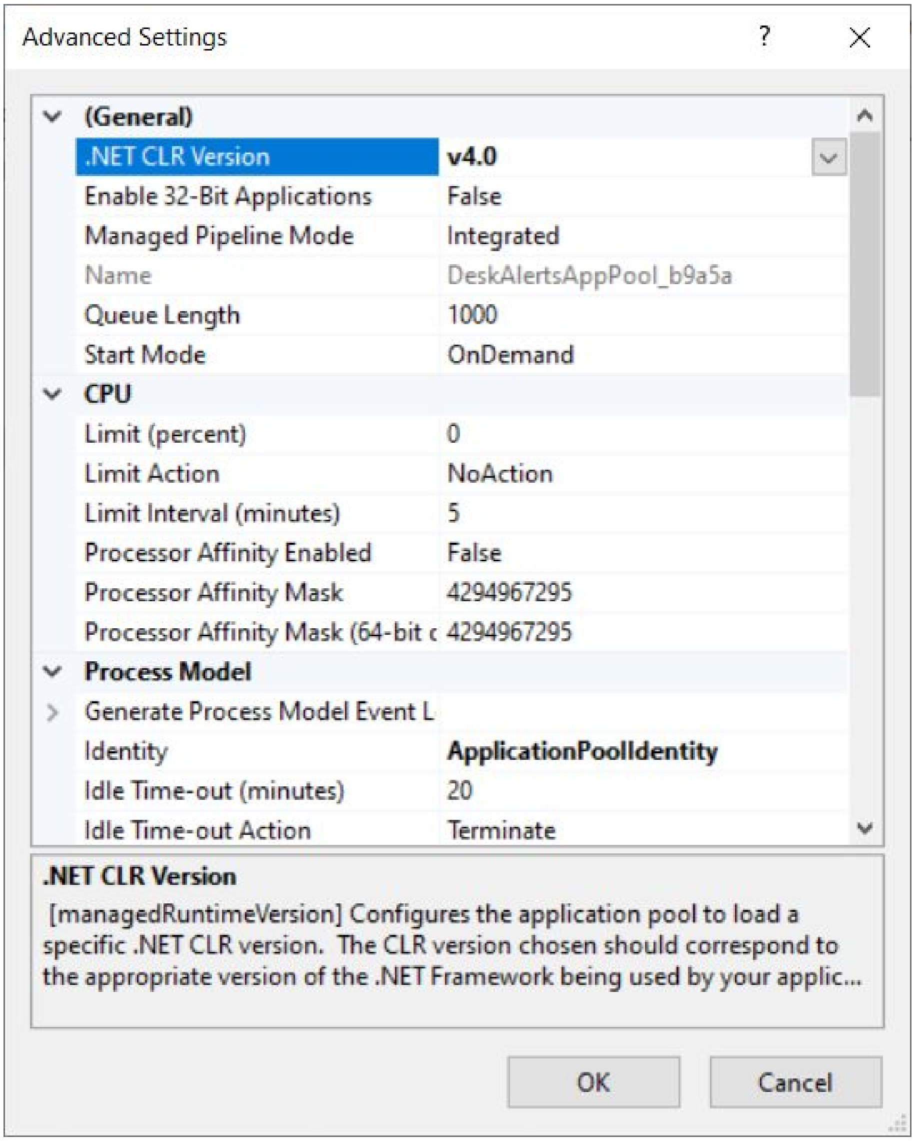
If any errors occur during the installation, you will be presented with the installation log. Please save this file and send it to DeskAlerts support using support@deskalerts.com

If the installation completes successfully, you will be presented with a corresponding notification. If this is a first installation on a clean database, you can use the default “admin” user with the “admin” password to log in the product dashboard.

DeskAlerts Application Pool configuration

When installed, DeskAlerts Server Application will create a new Application Pool in IIS, effectively isolating itself from other application that may be running on the same application server. However, the application pool requires some configuration before the software is fully functional.

First of all, set the “.NET CLR Version” setting to the highest available in your edition of IIS.



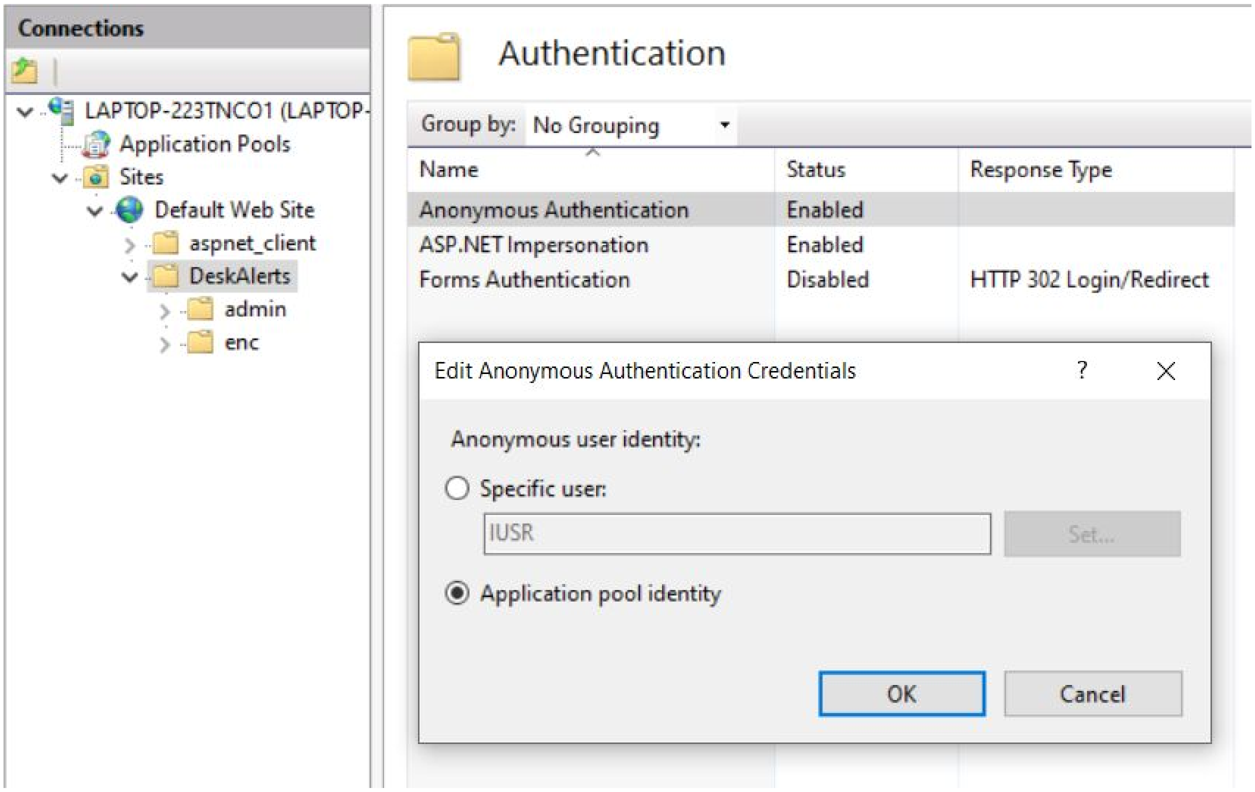
(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Name	DeskAlertsAppPool_b9a5a
Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate

.NET CLR Version

[managedRuntimeVersion] Configures the application pool to load a specific .NET CLR version. The CLR version chosen should correspond to the appropriate version of the .NET Framework being used by your applic...

Second, change the “Identity” parameter to the specific user, possessing local admin rights and non-expiring password. If you’re using Windows authentication to connect to DeskAlerts database - it should be the same account which you’ve set up as a db_owner.

One the application pool identity is set to the local admin user, go to DeskAlerts sub-site Authentication feature in IIS manager, edit the Anonymous authentication settings and set it to “application pool identity”



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Enabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect

Edit Anonymous Authentication Credentials

Anonymous user identity:

○ Specific user:

IUSR

● Application pool identity

Multi-server configuration

For audiences over 20.000 end users, it is advised to set your servers up in a cluster configuration to balance the load.

Alternatively, DeskAlerts can be set up in a multi-server configuration if you’re looking for some extra redundancy or setting up a high availability environment.

DeskAlerts multi-server configuration is currently being reworked and therefore can be set up only in presence of DeskAlerts Support engineer.

Desktop client applications configuration

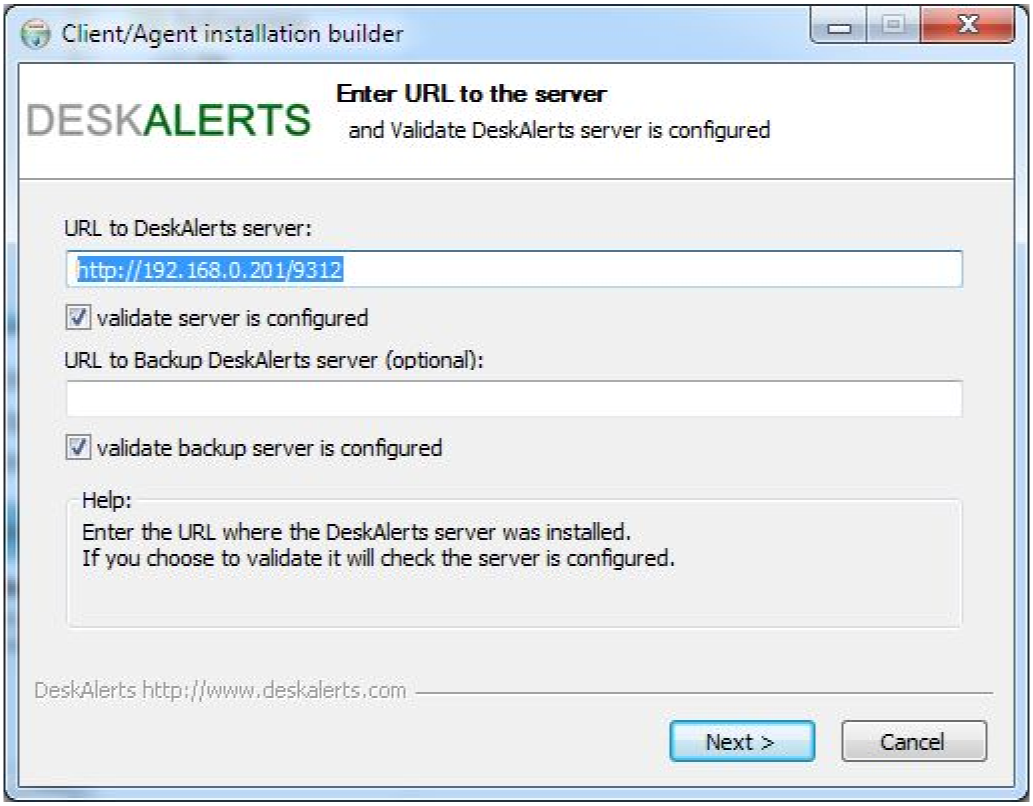
DeskAlerts package contains a client application builder for Windows workstations, that enables you to configure some options and choose which features will be available to the end users. You can also build several versions of client applications with different sets of features available and deliver them to different audiences (e.g. allow upper management to use “do not disturb” mode, while leaving this option off for everyone else).

The client builder files are contained in archive named **DeskAlerts.Client.vx.x.x.x.zip** and must be extracted before use.

Running the builder on the Application server running DeskAlerts is recommended, because this way builder will store your choices for future use.

Run the file named **ClientInstallation.exe** to begin.

On the first step, put in your DeskAlerts URL (same as the one used during the server installation):



Client/Agent installation builder

DESKALERTS

Enter URL to the server
and Validate DeskAlerts server is configured

URL to DeskAlerts server: http://192.168.0.201/9312

☑ validate server is configured

URL to Backup DeskAlerts server (optional):

☑ validate backup server is configured

Help:
Enter the URL where the DeskAlerts server was installed.
If you choose to validate it will check the server is configured.

DeskAlerts http://www.deskalerts.com

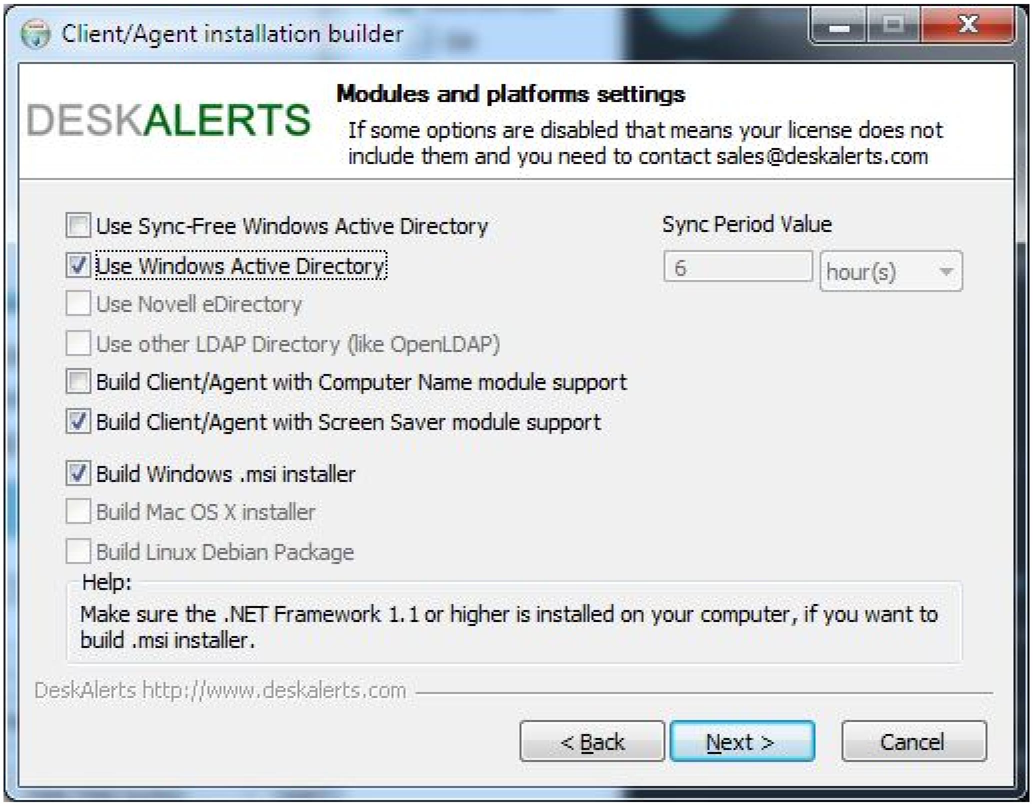
The builder will check if DeskAlerts server exists at this URL before proceeding. The Backup DeskAlerts Server URL can only be applied in Multi-server configuration

The next step contains several options related to different configuration - most of the time, some settings will be disabled because no company needs them all. Disabled options are simply not included in the package you've been provided.

This step give you an option to turn screensaver management feature on or off, as well as letting you determine how this client application will handle end user registration:

1. If your end users have accounts in your AD - check the "Use Active Directory" box
2. If you checked previous option and the DeskAlerts Application Server cannot access your AD domain (common for cloud-hosted DeskAlerts instances) - check "Use Sync-Free Windows Active Directory" and set the sync period value (how often the information about end user group membership has to be updated with DeskAlerts system)
3. If your end users don't have accounts in your AD, but you still want to register them with the system automatically - check "Build Client/Agent with Computer Name module support" - this will ensure that no end user interaction is required after client app is installed, and you'll be able to target them by workstation network name.

Make sure that the "Build Windows .msi installer" box is checked.



Client/Agent installation builder

DESKALERTS

Modules and platforms settings

If some options are disabled that means your license does not include them and you need to contact sales@deskalerts.com

☐ Use Sync-Free Windows Active Directory

☑ Use Windows Active Directory

☐ Use Novell eDirectory

☐ Use other LDAP Directory (like OpenLDAP)

☐ Build Client/Agent with Computer Name module support

☑ Build Client/Agent with Screen Saver module support

☑ Build Windows .msi installer

☐ Build Mac OS X installer

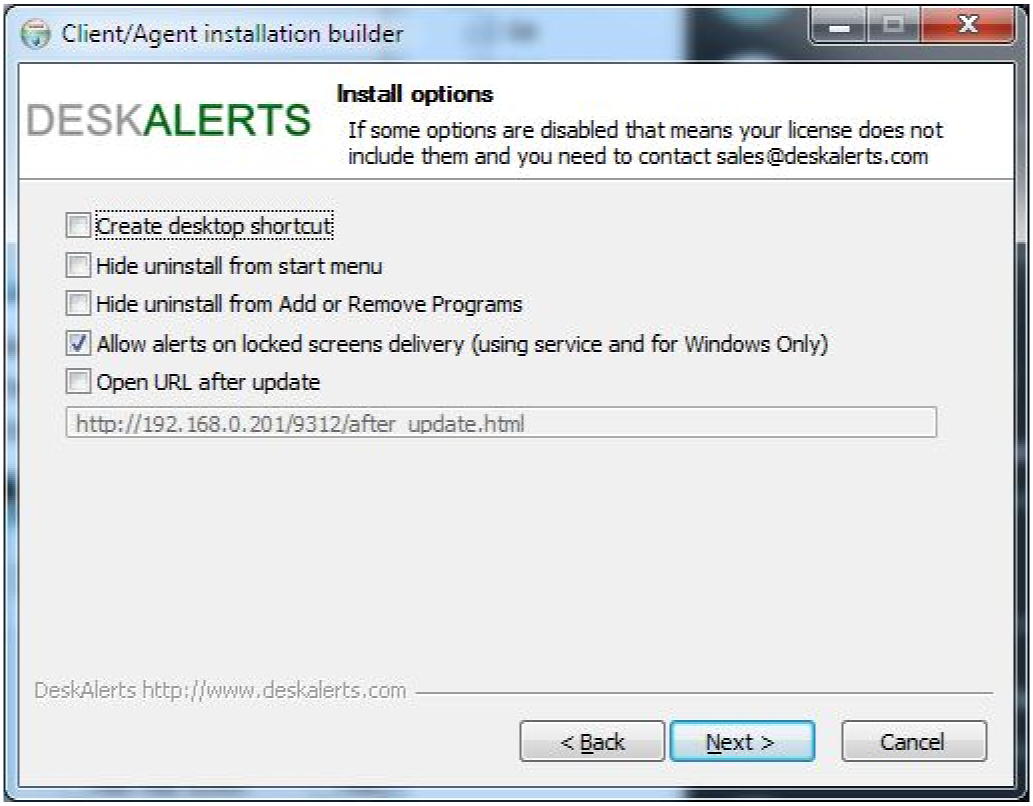
☐ Build Linux Debian Package

Sync Period Value: 6 hour(s)

Help:
Make sure the .NET Framework 1.1 or higher is installed on your computer, if you want to build .msi installer.

DeskAlerts http://www.deskalerts.com

The next step, Installation options, allows you to select a few more options related to the client presence in the end user's system. It also allows you to specify some URL that will be opened after the installation if you want to provide employees with some instructions or informational message about their DeskAlerts client.



Client/Agent installation builder

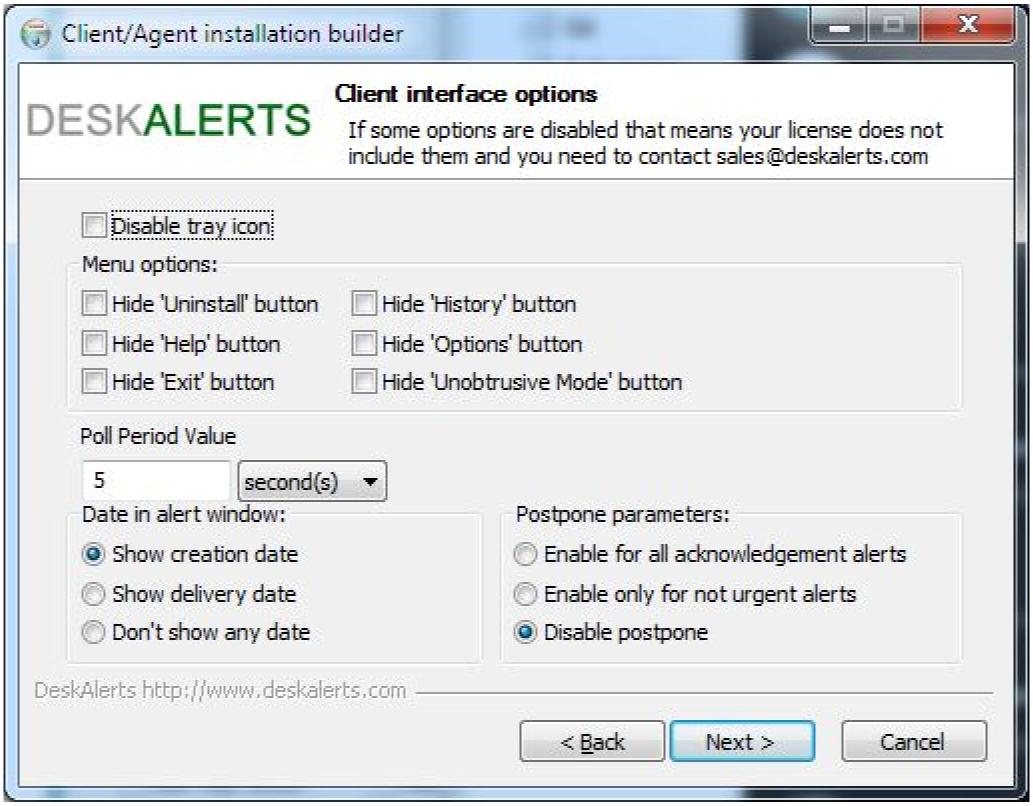
Install options

If some options are disabled that means your license does not include them and you need to contact sales@deskalerts.com

□ Create desktop shortcut
□ Hide uninstall from start menu
□ Hide uninstall from Add or Remove Programs
☑ Allow alerts on locked screens delivery (using service and for Windows Only)
□ Open URL after update

http://192.168.0.201/9312/after_update.html

Next step allows you to configure client interface options – affecting the features employee can use. Usually, the "exit" and "uninstall" options are disabled, as well as "unobtrusive mode" – to prevent the users from closing the app and missing the messages.



Client/Agent installation builder

Client interface options

If some options are disabled that means your license does not include them and you need to contact sales@deskalerts.com

□ Disable tray icon

Menu options:

□ Hide 'Uninstall' button
□ Hide 'Help' button
□ Hide 'Exit' button
□ Hide 'History' button
□ Hide 'Options' button
□ Hide 'Unobtrusive Mode' button

Poll Period Value

5 second(s)

Date in alert window:

● Show creation date
○ Show delivery date
○ Don't show any date

Postpone parameters:

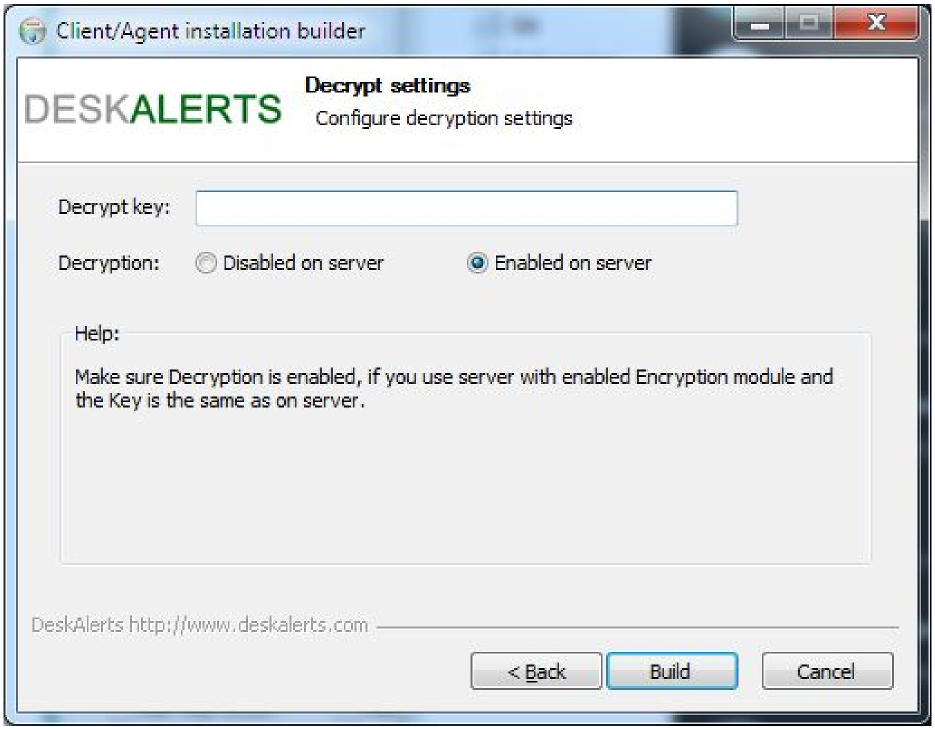
○ Enable for all acknowledgement alerts
○ Enable only for not urgent alerts
● Disable postpone

DeskAlerts http://www.deskalerts.com

The “postpone parameters” setting lets you determine whether people who are receiving alerts with reading confirmation required are able to postpone the reading or have to acknowledge your messages right away.

The “Poll Period Value” setting determines how often the client application checks for new messages being available on the server. Increasing the polling period results in better server performance, lower network traffic, but increased message delivery delay. The recommended polling period values for different audience sizes are listed in DeskAlerts Application server requirements

If you are using DeskAlerts Encryption module to protect your data in transit, you will be presented with a screen to provide your encryption key you’ve earlier set up on DeskAlerts server:



Decrypt settings
Configure decryption settings

Decrypt key:

Decryption: ○ Disabled on server ● Enabled on server

Help:

Make sure Decryption is enabled, if you use server with enabled Encryption module and the Key is the same as on server.

DeskAlerts http://www.deskalerts.com

If the keys on server and client won't match - the alerts will still arrive, but the content will be distorted and unreadable.

After you build the client application installers, click on “Close” and the folder containing the installation files will open automatically.

The MSI file you built is fully compatible with GPO and SCCM deployment. It can be deployed silently using the /quiet or /qn parameter of the msiexec.exe utility. Once the initial deployment has been completed, you can use Desktop clients auto-update feature to deploy client updates without requiring a workstation reboot.

DeskAlerts client for Mac

At the moment, Mac client is not provided along with the Windows client builder and must be assembled separately by DeskAlerts specialists.

In order to request your Mac client installer, you should provide DeskAlerts Support with the configuration file taken from one of your Windows client installations. Once you've determined the optimal client app configuration, retrieve the Windows client configuration file located at *C:\Program Files (x86)\DeskAlerts\conf.xml* and send it over to support so they can assemble Mac client in its likeness.

If your environment doesn't feature any Windows-based installations, just let us know:

1. Your DeskAlerts server URL

2. Your preference regarding the polling period time
3. Your preference regarding tray icon presence and options available to end user
4. Your message postponing policy
5. Your end user registration mechanism (AD synchronization, AD sync-free, Computer name registration or self-registration by the end user)
6. Your encryption key (if used)

Mobile client apps management

DeskAlerts client apps for Android and iOS are available on Play store and Apple App Store, respectively. In order to receive notifications through one of these, the end user must provide two important options - DeskAlerts server URL and their access credentials - this is a one-time process. If you are using AD integration, the app features a one-time association mechanism, effectively binding the device to a certain AD username if the end user provides valid credentials once. The credentials are being securely sent to DeskAlerts server (without storing them here) and validated by making an LDAP(S) request to your AD domain.

If you are managing your employees' devices through some sort of MDM tool, DeskAlerts Support can provide a custom **.apk** or **.ipa** package to be deployed through it. It is recommended to build the Server URL parameter directly into the installation package to minimize the end user error probability.