



GATEKEEPER

GateKeeper Hub

Version 3.6.12

Installation Guide

Untethered Labs, Inc.
support@gkaccess.com

Contents

1	GateKeeper Hub Installation.....	2
2	Configuring GateKeeper Hub	5
3	Application Setup	6
3.1	SQL Server Connection.....	6
3.1.1	Create New SQL Database	6
3.1.2	Edit Existing SQL Server Connection	8
3.1.3	Synchronize GateKeeper Database.....	8
3.2	Active Directory Access.....	9
3.2.1	Create an Active Directory Account.....	9
3.2.2	Assign an Existing Active Directory Account	10
3.3	Windows Management Service	10
3.3.1	Select Active Directory Account to Run the Windows Management Service.....	10
3.3.2	Start or Stop the GateKeeper Windows Management Service	11
3.4	Broadcast GateKeeper Hub Server Address	11
3.5	SysLog Server Connection	11
3.6	IP Restrictions	12
3.6.1	Allowed IP Addresses	12
4	IIS Setup	13
4.1	GateKeeper Hub Website	13
4.2	Port Bindings	13
4.3	Application Pool	14
4.3.1	Application Pool Recycling	15
4.4	IIS Logging	15
5	Off-Site Access	16
5.1	Setup Tunneling Service.....	17
6	Troubleshoot.....	18
7	Logs	19
8	Other Technical Aspects	20
8.1	Enabling TCP/IP Protocol for SQL Server	20
8.2	Unable to connect to the SQL Server?.....	20
9	Contact Support	21

1 GateKeeper Hub Installation

Download the latest version of the GateKeeper Hub installer from the GateKeeper Customer Portal website (<https://gkchain.com/portal/login>).

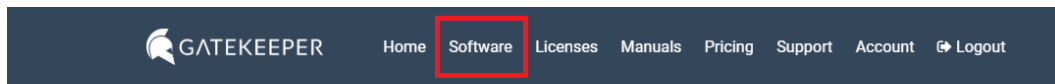
Operating System requirements:

- Windows 7 and Windows 10, only
- Mac on Sierra and Mojave, only

SQL requirements:

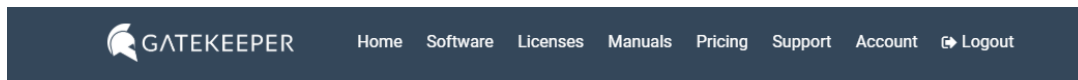
- GateKeeper software supports SQL 2012 and up
- Express is a great option for certain users
- 10 gb is enough for less than 50 users

First, download the GateKeeper Hub from the [GateKeeper Customer Portal](#) under the **Software** tab.



Welcome to the GateKeeper Enterprise Portal

Click **Software**.



Welcome to the GateKeeper Enterprise Portal

Please use the following sections to access GateKeeper Enterprise resources.

LIVE DEMO OF GATEKEEPER ENTERPRISE

Enterprise Software

Get the latest versions of the GateKeeper client and server software.

Licenses

Download your server license.

SOFTWARE

LICENSES

Scroll down to "**GateKeeper Server Hub Application**" and click "**Download Web-Installer**".

GateKeeper Hub Server Application

Version: (3.5.25)

Download
Web-Installer

Download
Offline-Installer

Requirements

Change log

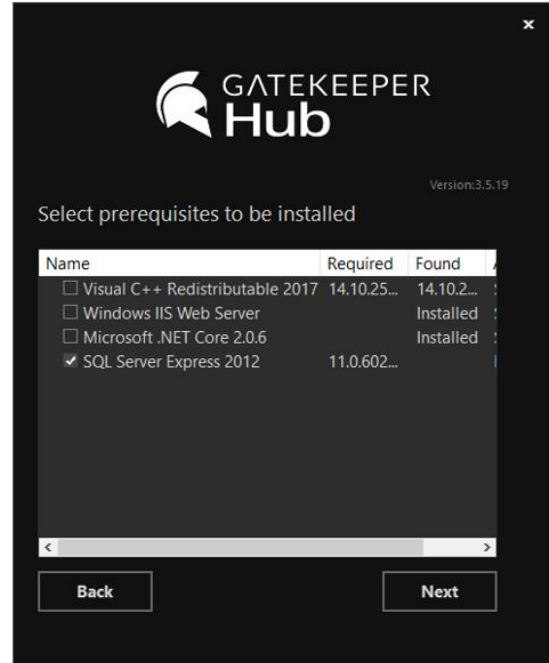
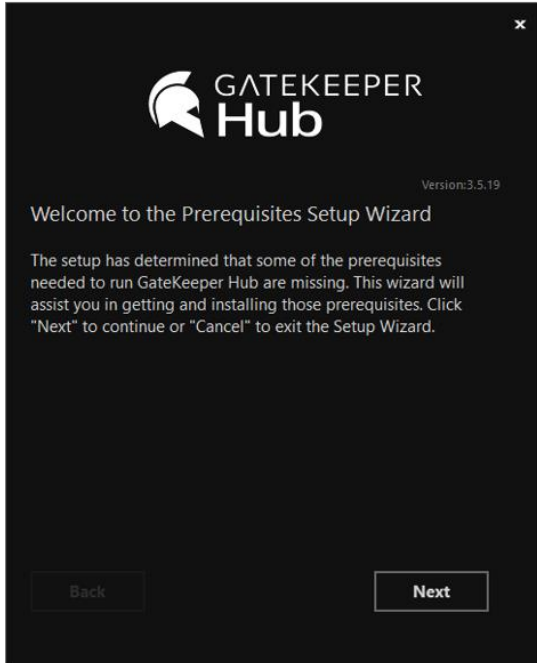
- SQL Server to store GateKeeper database. If a SQL server is not available, SQL Express can be downloaded and installed for no cost from this [link](#).
NOTE: SQL Express 2012 can be installed later through GateKeeper Hub Installer UI for version **3.5.10**.
- Windows Server platform (2012 or 2016). If Windows Server is not available, a Win 10 machine can be configured to run the server application.
- At least 10GB of free space on the computer.
- Administrator rights to install and configure the server application.

The current version of our server application is 3.5.25. The release date is 11/15/2019.

Click [here](#) for the list of updates to our software.

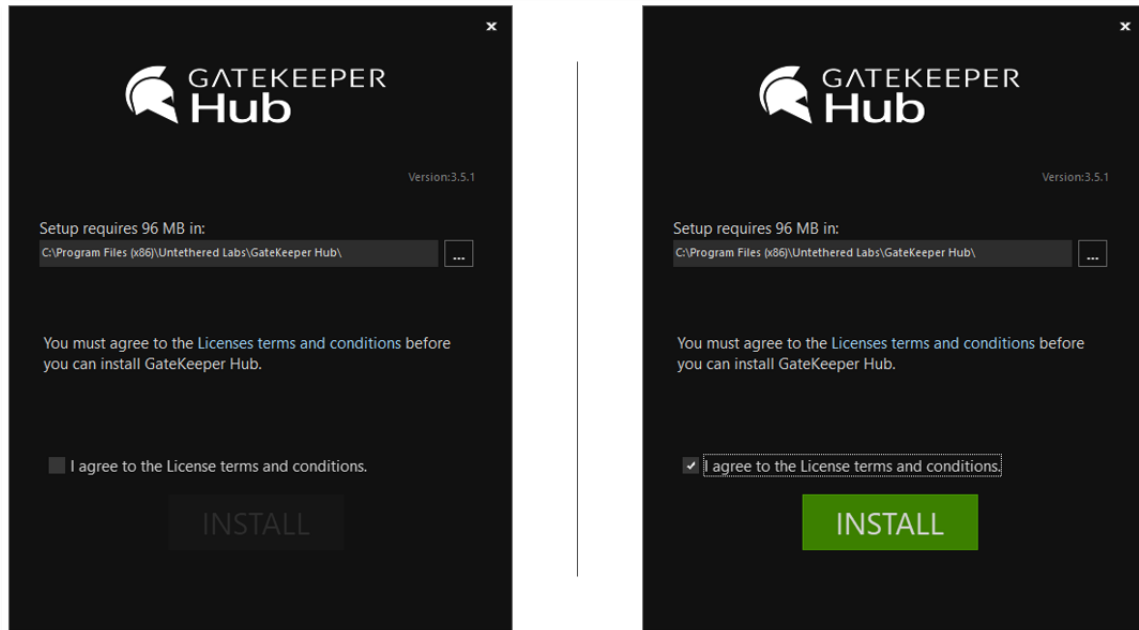
Step 1: After download, run the GateKeeper Hub installer.

Step 2: Certain mandatory pre-requisites that are required for running the GateKeeper Hub website on the computer will be preselected. If you wish to install SQL Server on the same computer, you can select the SQL Server Express 2012 pre-requisite from the menu. If you want to use an SQL server that is already installed on your network, then **uncheck this option**. Please see the screenshots provided below. After selecting prerequisites, click **Next**.

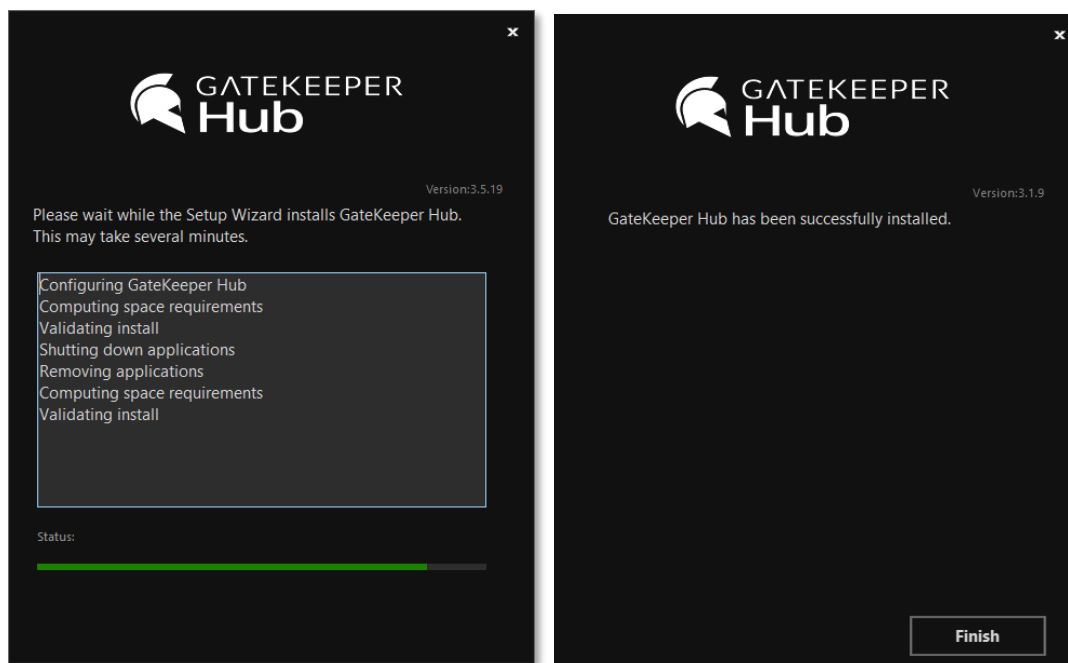


Step 3: Confirm the location for the GateKeeper Hub installation. The installer will also show the storage space needed. Acknowledge agreement to the license terms and conditions to enable the **INSTALL** button.

Step 4: Click **INSTALL** to begin the installation. It will take a few minutes, depending on all the prerequisites selected, to finish installing the GateKeeper Hub server.



Step 5: Click **Finish** to launch the **GateKeeper Hub Manager**. You do not have to restart the computer immediately. However, it is highly recommended that a reboot is performed when the GateKeeper Hub application is finished being set up.



2 Configuring GateKeeper Hub

The **GateKeeper Hub Manager** connects the **GateKeeper Hub** to an SQL Server and sets up various features of the Hub as necessary. The **GateKeeper Hub Manager** has the following sections:

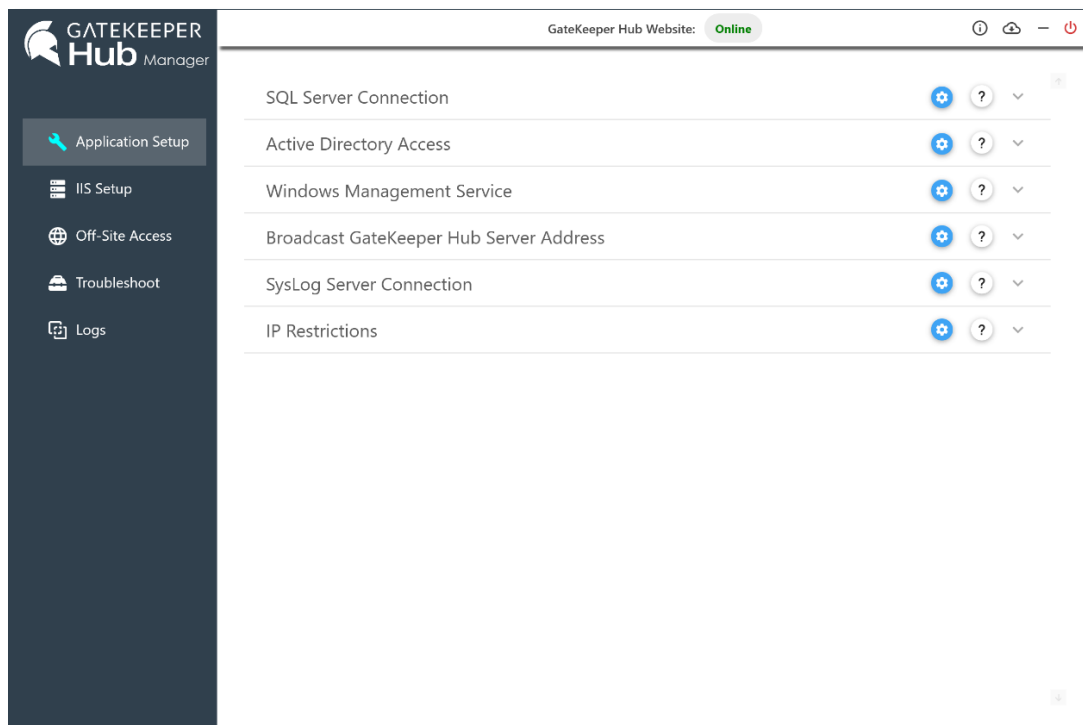
1) Application Setup: The Application Setup page allows for SQL Server connection, Active Directory access, management of Windows computers through the Windows Management service, ability to broadcast the Hub IP and port number, connecting the Hub to a Syslog server for logging, and setting up restrictions on IP addresses that can connect to the Hub.

2) IIS Setup: The IIS Setup page allows you to choose different settings for the GateKeeper Hub website running in Internet Information Services (IIS). These include the ability to start, stop, or restart the Hub website, port bindings, application pool settings, and IIS logs.

3) Off-Site Access: The Off-Site Access page allows you to set up a publicly available URL to access the GateKeeper Hub website over the Internet. Off-site access is only available if you have the appropriate license which can be obtained by contacting the company at support@gkaccess.com.

4) Troubleshoot: The Troubleshoot page runs automated tests on the GateKeeper Hub installation. The automatic tests validate various pre-requisites, SQL Server connection, IIS setup, and other aspects of the GateKeeper Hub server and reports on any errors that may be present.

5) Logs: The Logs page shows all error logs collected by GateKeeper Hub and stored locally on the computer. These logs can be examined to manage any issues that might be reported during the operation of the GateKeeper Hub website.



3 Application Setup

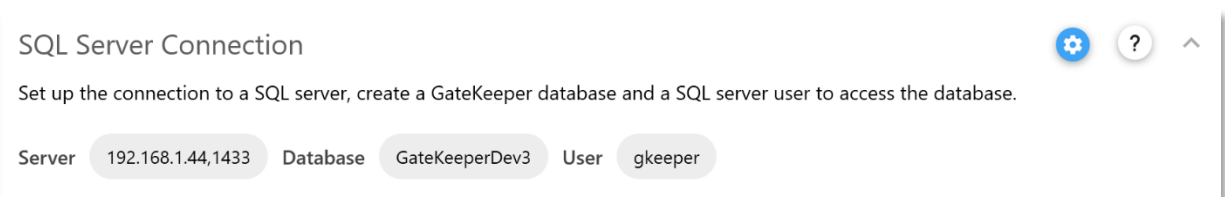
Application Setup

The Application Setup page allows for




- SQL Server connection
- Active Directory access
- management of Windows computers through the Windows Management service
- ability to broadcast the Hub IP and port number
- connecting the Hub to a Syslog server for logging
- setting up restrictions on IP addresses that can connect to the Hub

3.1 SQL Server Connection


The first task is to connect the GateKeeper Hub server application to an SQL Server to create and manage a database to be used by the Hub. GateKeeper Hub requires an SQL database to store data regarding users, computers, logs, etc. This database is part of an SQL Server instance that is running on your network. The SQL Server can be running locally on this computer, or any other computer on your network. All the data is stored on your network and not shared with anyone else.



Click on the **Settings** () button to bring up three options:

-  **Create a new database for Hub** (create new SQL database)
-  **Edit existing connection** (edit SQL connection)
-  **Update connected database** (synchronize existing SQL database)

3.1.1 Create New SQL Database

 Clicking on the button to create a new database will bring up a sidebar with options to log in to an SQL Server and create a new user and database for the Hub to utilize. A new database must be created the first time the Hub is installed. You will need the instance name of the SQL Server and administrative rights to create databases in the SQL Server instance. While creating the new database, a new GateKeeper Hub user is also added to the SQL Server with ownership rights to the newly created database.

Enter the location of the SQL Server. If the SQL Server is on the same machine as the Hub, then the SQL Server address will be of the form: **(local)\INSTANCENAME**

Typical instance names for SQL Servers are **SQLEXPRESS** or **MSSQLSERVER**.

If the SQL Server is on a different computer on the network, then the SQL Server address will be of the form: **IPADDRESS,PORT\INSTANCEN**

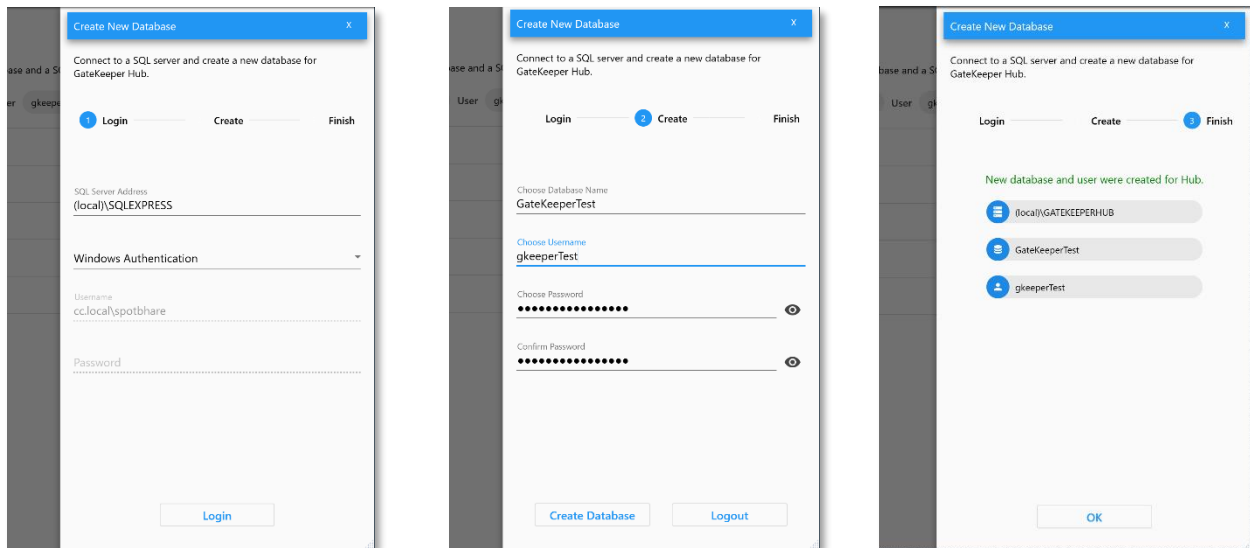
The SQL Server will have to be configured to communicate over Internet Protocol (IP). Typical port number for the SQL Server is **1433**, and the instance name is whatever the SQL instance you want to connect to. For example, the SQL address can be written as: **192.168.1.44,1433\SQLEXPRES**

Next, you will select the authentication mode to log on to the SQL Server. This login account must have privileges to create new users and databases in the SQL Server instance.


Select **Windows Authentication**, from the **Authentication Type** drop down menu, if your credentials have access to create a database on the SQL Server. If not, select **SQL Server Authentication** to sign in with credentials that have access to create a database and enter a login username and password.

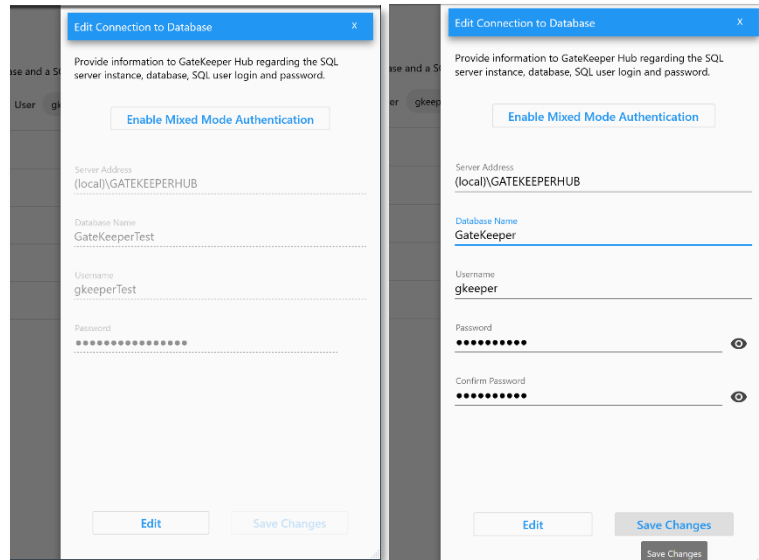
The next step is to create the GateKeeper Hub database. Default values for the database name, database user, and database password are auto filled. These can be changed as required. Once the values are filled in, click on **Create Database** to create the new user and database.

Once the database has been successfully created, a notification will confirm it and the sidebar will show the database and user created for use with GateKeeper Hub.



3.1.2 Edit Existing SQL Server Connection

 A SQL Server database connected to the GateKeeper Hub database can be changed at any time. You can edit the SQL connection information using the **Edit existing connection** (edit SQL Server) option. This is useful if there are multiple GateKeeper Hub databases on the network, and you want to switch the Hub server from one to another. This is also useful if the SQL Server user assigned to GateKeeper Hub has to be changed. This may occur if the database administrator has changed the password for the GateKeeper database user. If the GateKeeper database user has changed, then the Hub will no longer be able to communicate with the SQL Server and must be updated by editing the SQL Server connection.




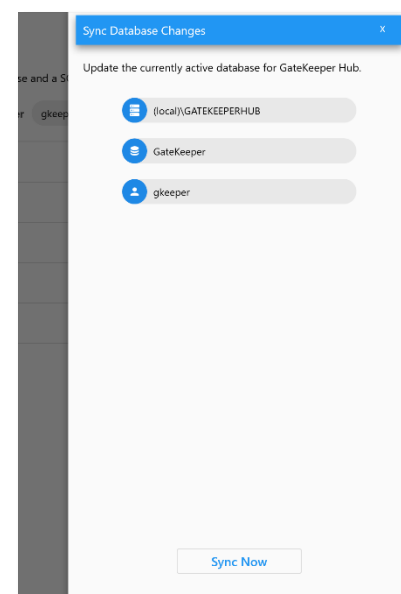
The currently connected SQL Server and database will be displayed when the side panel is first opened. Click **Edit** to make changes to the SQL connection.

Once you have updated the various fields, click **Save Changes** to save your edits. This will then verify all changes including the connection to the SQL Server, validity of the database, accessibility by the user, and the tables inside the database. If everything is verified, then the new settings will be saved, and the GateKeeper Hub website will be restarted.

Additionally, there's a button to ensure that the SQL Server has mixed mode authentication enabled. Clicking on the **Enable Mixed Mode Authentication** button will enable SQL authentication on the SQL Server if it was not already enabled. This is important because the GateKeeper Hub server can only use SQL Authentication to access the SQL Server.


3.1.3 Synchronize GateKeeper Database


 Whenever a new instance of the GateKeeper Hub is installed, it modifies the tables in the GateKeeper database associated with the Hub to ensure that all database changes are incorporated properly. In order to make sure that the database has been successfully updated, a backup button to synchronize all tables in the GateKeeper database is provided. Click this button to run an SQL script to update the tables in the GateKeeper database as needed.



3.2 Active Directory Access






GateKeeper Hub can manage your Active Directory users. You can change Active Directory passwords, deactivate accounts, and much more directly from the GateKeeper Hub web interface. In order to do this, the Hub requires **WRITE ACCESS** to Active Directory. The Hub Manager can be used to add a new account in Active Directory for GateKeeper Hub to use, or you can assign an existing account to GateKeeper Hub as well. Make sure that this account has permissions to **WRITE** to Active Directory.

Clicking **Settings** () will expand two more buttons:

+  Create new AD Account

 Edit AD Account

Active Directory Access



Set up an Active Directory account for GateKeeper Hub to manage AD users. This AD account should have write privileges to active directory.

Domain

cc.local


Username

adtestuser

AD Server

COOLCAD-SERVER.cc.local

3.2.1 Create an Active Directory Account

+  The Hub Manager can create a new user account in your Active Directory with the appropriate permissions to make changes to user accounts in AD. You can either create a new account yourself or let the Hub Manager automatically create one for you.

It is important that the account that is created have **WRITE access** to Active Directory. This will allow the GateKeeper Hub website to be used for managing passwords and other aspects of AD accounts.

Enter the domain, username, and password in the appropriate text boxes. In the **Select Active Directory Group** dropdown menu, please select a group that has **WRITE access** to Active Directory. Typically this group will be the **Domain Admins** group.

Click **Save Changes** to finish setting up the AD account for GateKeeper Hub to use.

Create Account in AD for GateKeeper Hub

Create a new user in with permissions to write to the Active Directory.

Active Directory Domain

cc.local

Choose Username

GK553971

Choose Password

.....

Confirm Password


.....

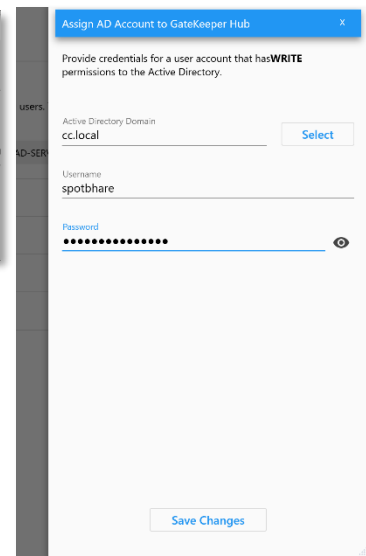
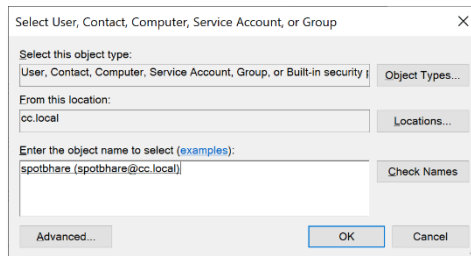
Select Active Directory Group

Domain Admins

Save Changes

3.2.2 Assign an Existing Active Directory Account

 You can also select an existing user account from your Active Directory. Make sure the selected account has the correct permissions to make changes to the Active Directory.



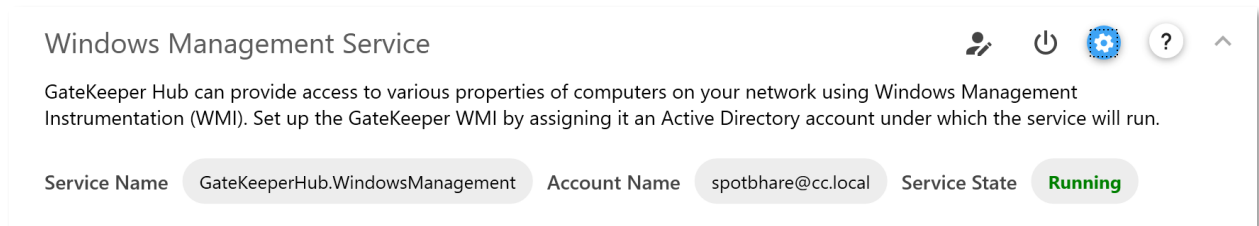
Click **Select** to show the Windows **Select User or Group** screen. Search for AD accounts and then type in the password for the chosen account.

Make sure to pick an account that has **WRITE** access to Active Directory.


Click **Save Changes** to finish setting up the AD account for GateKeeper Hub to use.

3.3 Windows Management Service

GateKeeper Hub provides admins access to many properties of all GateKeeper-enabled computers on your network including CPU usage, memory, disk space, network adapters, processes, services, and others. In order to access these properties, the Hub server needs to install and run the **GateKeeperHub.WindowsManagement** service. This service must run under an Active Directory account which has the capability to access processes on all computers on your network.




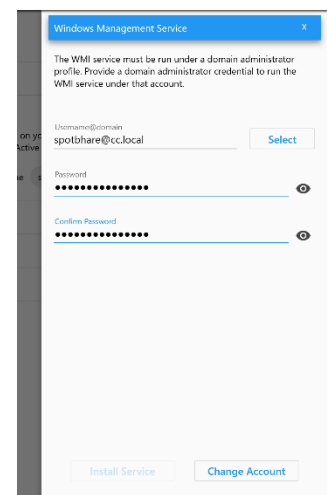
Click **Settings** () to expand two options for setting up GateKeeper Windows Management service.

 Select AD Account for WMI Service

 Start or Stop the GateKeeper Windows Management Service

3.3.1 Select Active Directory Account to Run the Windows Management Service

 Please select an Active Directory account and assign it to the GateKeeper Hub's Windows Management service to run using that account. Please make sure to select an Active Directory account that has permissions to access processes on all computers of your network. We recommend choosing a Domain Admin account for this purpose.




Click **Select** to show the Windows user picker tool. You can search for AD accounts there and then type in the password for the chosen account. The account must have the following form:

username@domain

Make sure to pick an account that has rights to access processes on all computers on your network.

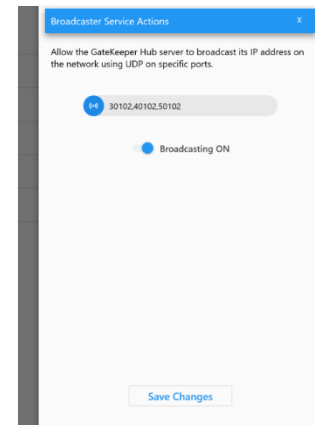
Click **Change Account** to finish setting up the AD account for GateKeeper Hub to use.

3.3.2 Start or Stop the GateKeeper Windows Management Service

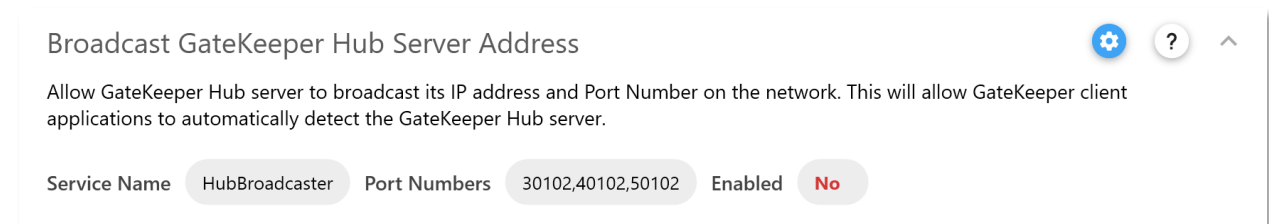
 The other option in the GateKeeper Windows Management Service menu is to start or stop the service. Clicking on that button will bring up a sidebar that shows the current status of the service and buttons to either **Start** or **Stop** it.

3.4 Broadcast GateKeeper Hub Server Address

The GateKeeper Hub Broadcaster service broadcasts the IP address and port number of the Hub website using UDP transport on the local network. This allows the GateKeeper Client applications on the computers in the network to automatically detect the Hub and connect to it in order to sync information. While this service is not necessary for client-server communication, you can use it to make sure that Client applications are always connected to the correct Hub IP address. Click **Settings (Gear)** to open a sidebar menu where you can enable Hub Broadcasting.

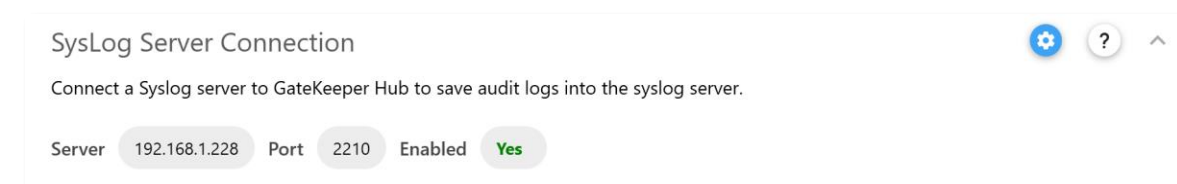



The broadcaster service sends out the IP address and port number on specific UDP ports which should be opened in the firewalls of the GateKeeper-enabled computers on the network.

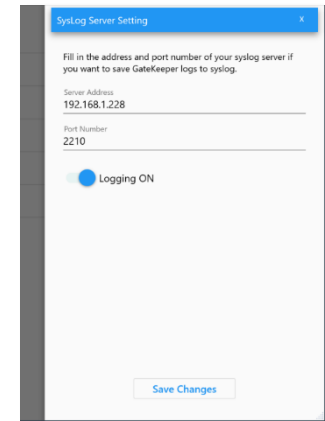


3.5 SysLog Server Connection

Logs from the GateKeeper Client applications sent to the Hub are uploaded to your Syslog server. Add the address and port number of the Syslog server to the Hub application settings to enable this feature.



Click **Settings** () to bring up a sidebar where you can put in the address and port number of your SysLog server. Then, click the switch to enable “**Logging ON**” and click **Save Changes** to save the SysLog server information for the GateKeeper Hub to use.

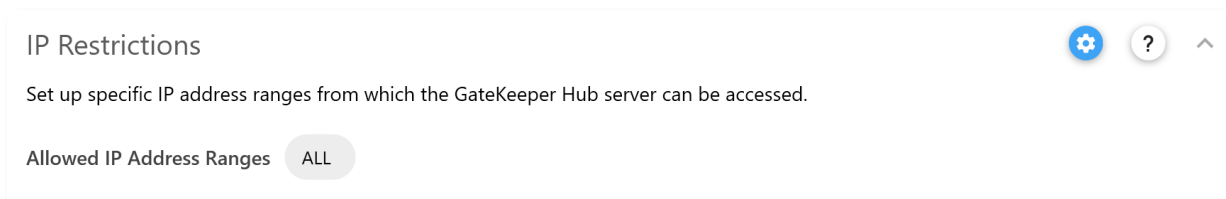


The dialog box titled "SysLog Server Setting" contains the following fields and controls:

- Instruction: "Fill in the address and port number of your syslog server if you want to save GateKeeper logs to syslog."
- Server Address: Input field with "192.168.1.228" entered.
- Port Number: Input field with "2210" entered.
- Logging ON: A toggle switch that is currently turned on.
- Save Changes: A button at the bottom right.

3.6 IP Restrictions

The GateKeeper Hub website is accessible from all computers on the local network. If the local network is set up using non-traditional network addresses and subnet configurations, you can restrict access to the Hub from specific IP addresses if you so desire. This setting allows network administrators to control access to the GateKeeper Hub website from certain IP addresses.

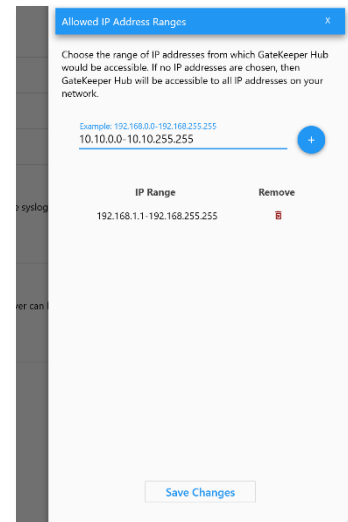


The sidebar titled "IP Restrictions" includes the following elements:

- Settings icon (gear) and a question mark icon.
- Description: "Set up specific IP address ranges from which the GateKeeper Hub server can be accessed."
- Allowed IP Address Ranges: A section with a button labeled "ALL".


3.6.1 Allowed IP Addresses

If no IP addresses are chosen, then all possible IP addresses on the local network will have access to the Hub website. Click **Settings** to expand the sidebar where you can set ranges of IP addresses from which the Hub website can be accessed. For example, a typical IP address range for a local network is 192.168.1.1-192.168.255.255.



The dialog box titled "Allowed IP Address Ranges" contains the following elements:

- Instruction: "Choose the range of IP addresses from which GateKeeper Hub would be accessible. If no IP addresses are chosen, then GateKeeper Hub will be accessible to all IP addresses on your network."
- Example: "192.168.0.0-192.168.255.255" and "10.10.0.0-10.10.255.255" with a plus icon to add more.
- Table of IP Ranges:

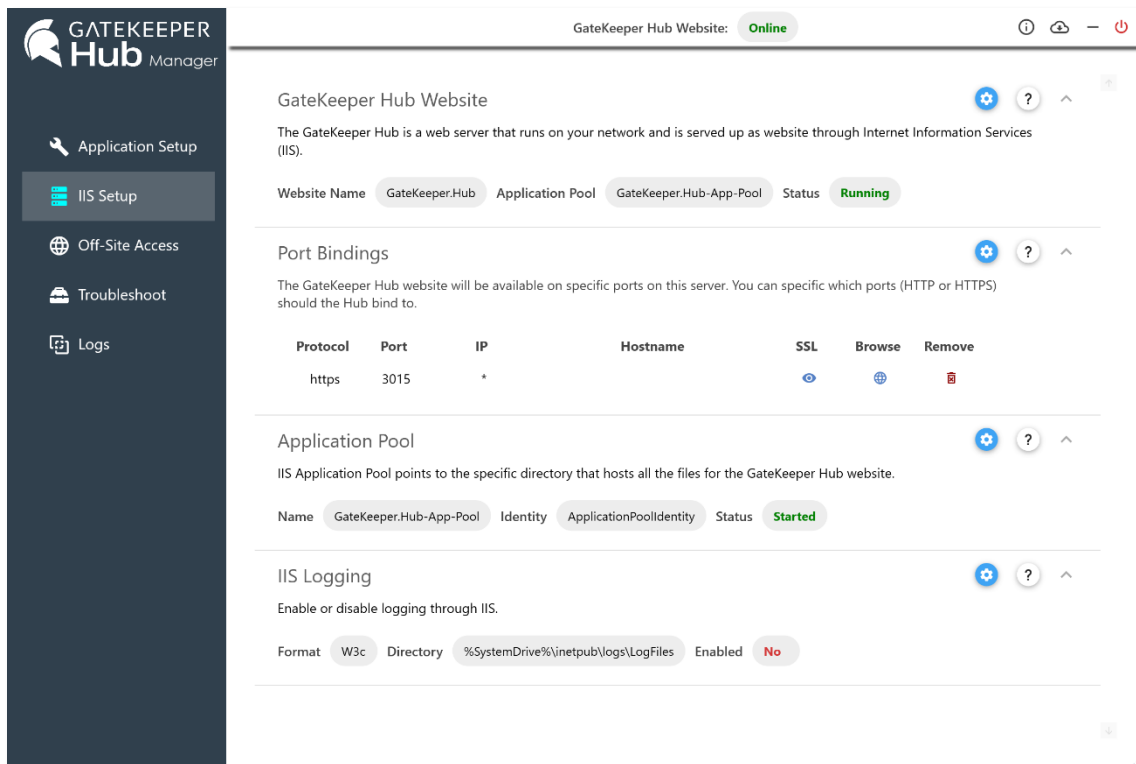
IP Range	Remove
192.168.1.1-192.168.255.255	

- Save Changes: A button at the bottom right.

4 IIS Setup


IIS Setup

The IIS setup page allows you to choose different settings for the GateKeeper Hub website running in Internet Information Services (IIS). These include the ability to start, stop, or restart the Hub website, port bindings, application pool settings, and IIS logs.



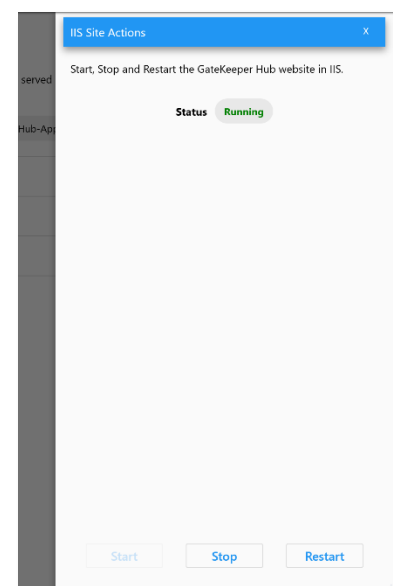
4.1 GateKeeper Hub Website

GateKeeper Hub runs as a website using Internet Information Services (IIS). The website is accessible from all computers on the local network. Every GateKeeper Client application connects to this website to synchronize users, credentials, tokens, and audit logs. The Hub website uses an SQL database for storing all data. The website is automatically set up in IIS after the installation process and must not be modified.




Click **Settings** () to open the sidebar where you can start, stop or restart the GateKeeper Hub website in IIS.

4.2 Port Bindings







The GateKeeper Hub website runs on specific ports in IIS. These ports can be set using the IIS Port Bindings setting. By default, the website runs on port **3015** using the HTTPS protocol. A self-signed certificate is



Port Bindings






The GateKeeper Hub website will be available on specific ports on this server. You can specify which ports (HTTP or HTTPS) should the Hub bind to.

Protocol	Port	IP	Hostname	SSL	Browse	Remove
https	3015	*				
http	3016	*				

automatically generated and added to IIS to enable secure data communication using the HTTPS protocol. Other ports can be added to run the website on, and other SSL certificates can be added to the website if required.

The Port Bindings table shows the ports currently bound to the GateKeeper Hub website. If the website is running on HTTPS, then you can view details of the SSL certificate from the table as well. The website can be browsed by clicking on the Browse Website button in the Port Bindings table.

Click **Settings** () to open a sidebar where new port bindings can be set up. Choose the transport method (HTTP or HTTPS) and a port number to associate with the website. You can also optionally choose a hostname for the website. If you choose a hostname, then you will have to edit the DNS for your network to make sure that the hostname is properly pointed to this computer. If you choose the HTTPS protocol, then you must also choose an SSL certificate to associate with the GateKeeper Hub website. All available certificates can be seen in the drop-down menu in the sidebar.

GateKeeper Hub Website Bindings

Setup HTTP or HTTPS ports for GateKeeper Hub website.

Protocol Type	IP Address	Port
https	All Unassigned	3017

Hostname (Optional)

Select SSL Certificate




GateKeeper.Hub

Save Changes

4.3 Application Pool

The Application Pool manages the location of the files used in running the GateKeeper Hub website in IIS. These files are installed during the Hub installation process and the identity of the application pool is automatically created according to appropriate rules in IIS. The Application Pool can be further configured to optimize the website performance on your network based on the capacity of the computer running the website. Click **Settings** to expand buttons for setting up recycling options for the application pool, and to restart the application pool.

Application Pool

IIS Application Pool points to the specific directory that hosts all the files for the GateKeeper Hub website.

Name	GateKeeper.Hub-App-Pool	Identity	ApplicationPoolIdentity	Status	Started
------	-------------------------	----------	-------------------------	--------	---------

4.3.1 Application Pool Recycling

IIS can be configured to periodically recycle the memory used by the Application Pool. This recycling allows for stale data to be cleared from the computer's memory and can optimize the performance of the website. This is especially important if there is a significant amount of network traffic on the GateKeeper Hub website - for example, when many computers are running the GateKeeper Client application.

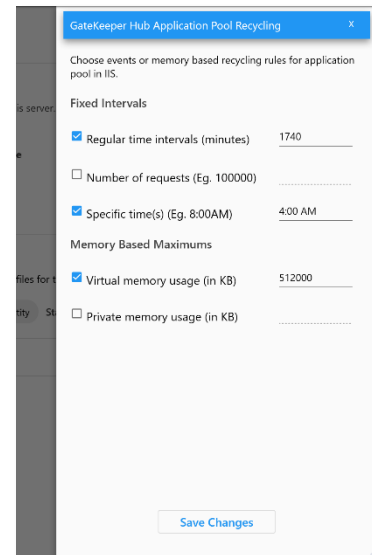
The recycling rules can be set based on number of requests being made to the website, on a periodic time basis, or based on amount of memory used by the website.

Click **Save Changes** once you have chosen your recycling options.

4.4 IIS Logging

IIS can collect logs related to requests made to the GateKeeper Hub website from all the computers on your network. These logs are useful in diagnosing errors in connectivity, database, and access to the GateKeeper Hub website. However, if there are a large number of computers connected to the GateKeeper Hub website, then these IIS logs can grow very quickly in size. Enable IIS logging if you experience any issues while accessing the GateKeeper Hub website. Please share these logs with the GateKeeper technical support team for troubleshooting if required.

Clicking **Settings** (⚙️) will open a sidebar to reveal options to enable or disable IIS logging.



GateKeeper Hub Application Pool Recycling

Choose events or memory based recycling rules for application pool in IIS.

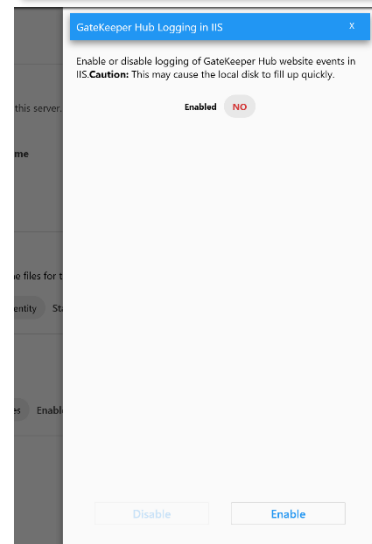
Fixed Intervals

- ☒ Regular time intervals (minutes) 1740
- ☐ Number of requests (Eg. 100000)
- ☒ Specific time(s) (Eg. 8:00AM) 4:00 AM

Memory Based Maximums

- ☒ Virtual memory usage (in KB) 512000
- ☐ Private memory usage (in KB)

Save Changes



GateKeeper Hub Logging in IIS

Enable or disable logging of GateKeeper Hub website events in IIS. **Caution:** This may cause the local disk to fill up quickly.

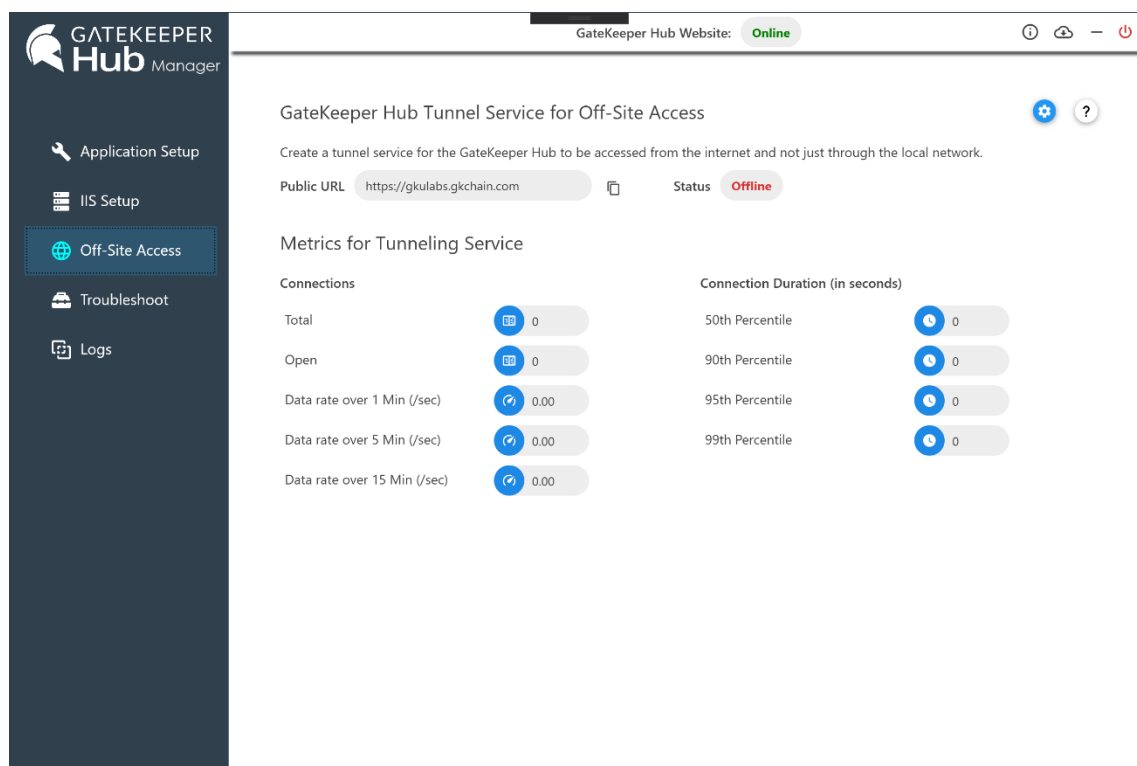
Enabled NO

Disable Enable

5 Off-Site Access

Off-Site Access

The GateKeeper Hub website is accessible only on the local network. This means that when a computer is not on the network, the GateKeeper Client application is unable to communicate with the Hub server, unless there is a VPN connection. Furthermore, Hub administrators cannot access the website over the Internet, unless they are using a VPN connection. However, it is possible to set up off-network access to the GateKeeper Hub website using a tunneling service managed through the GateKeeper Hub Manager. If you want the GateKeeper Hub website accessible over the Internet, you can set up a unique URL for the Hub and set up the tunneling service using this setting on the manager.




You must obtain an offsite access license from the GateKeeper support team in order to enable this feature. If you do not have an offsite access license, then you will not be able to setup the tunneling service. Please contact support@gkaccess.com if you would like to obtain the offsite access license.

A tunneling service provides secure access to the GateKeeper Hub website from outside of the local network. This service needs to be installed on the server and set up using a unique URL for your Hub website. Once set up, this service can be started or stopped on demand. By using this service, your GateKeeper Hub website will be visible on the Internet. Please ensure that you have ample network monitoring and threat detection services installed on your network to mitigate any attacks on the website.

During the installation of the tunneling service, you will be asked to choose a unique URL as your public website for GateKeeper Hub. Each URL must be a subdomain of gkchain.com. For example, you can choose the URL as **COMPANYNAME.GKCHAIN.COM**. Make sure to select a URL that cannot be easily replicated.

Once the tunneling service has been set up, you will be able to see properties such as total number of connections, average data rates, as well as time spent on an open connection. These metrics are useful in validating the performance of the tunnel.

5.1 Set up Tunneling Service

Click **Settings** () to open a sidebar to set up the Tunneling Service.

Step 1: Install the tunneling service by clicking **Install**.

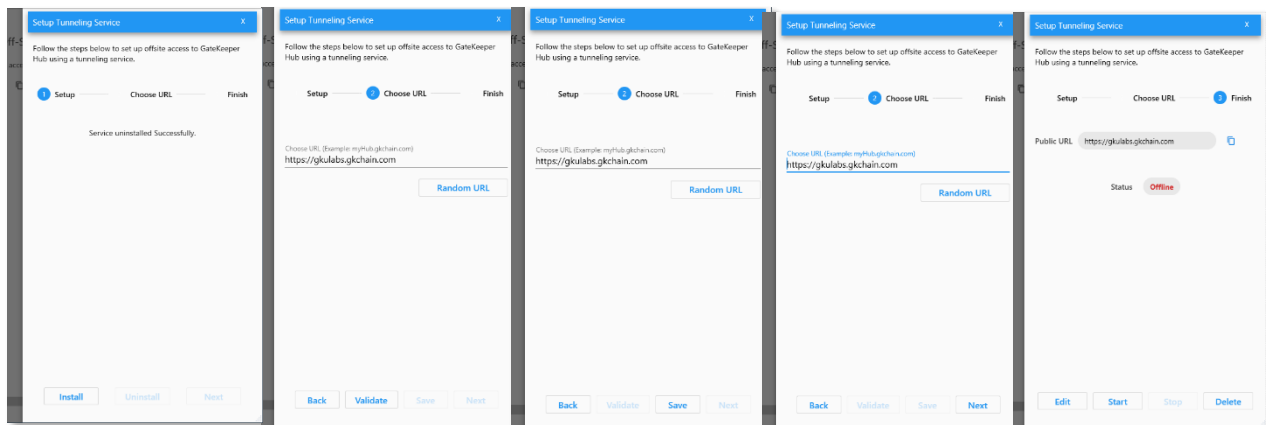
Step 2: **Choose a URL** for the GateKeeper Hub website. This URL will be accessible over the internet. Make sure to choose a unique sub-domain name. You can also click on the Random URL button to randomly choose a URL for your website.

Step 3: Click **Validate** to make sure that the URL is available for use.

Step 4: Once the URL has been validated, click **Save** to save the tunnel service settings.

Step 5: The Hub Manager will validate your license before saving the setting. Click **Next**.

Step 6: Click **Start** to start the tunneling service. Once the service has been started, you can go to a web browser and type in the full URL (including https://) to access the GateKeeper Hub website.

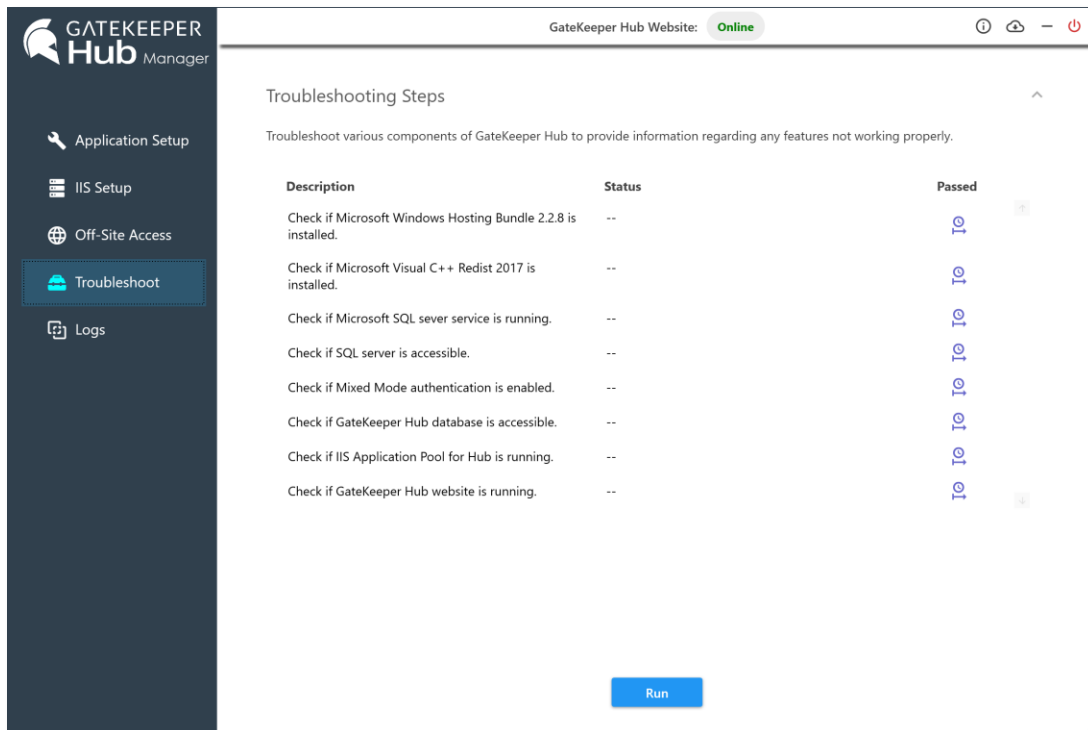


6 Troubleshoot

Troubleshoot

The troubleshooting page allows you to run automated tests on the GateKeeper Hub installation. The automatic tests validate various pre-requisites, SQL Server connection, IIS setup, and other aspects of the GateKeeper Hub server and reports on any errors that may be present.

Click **Run** to start the troubleshooting diagnosis. It will check all possible points of error and report results. If any step fails, please contact GateKeeper Support at support@gkaccess.com to resolve the issue.





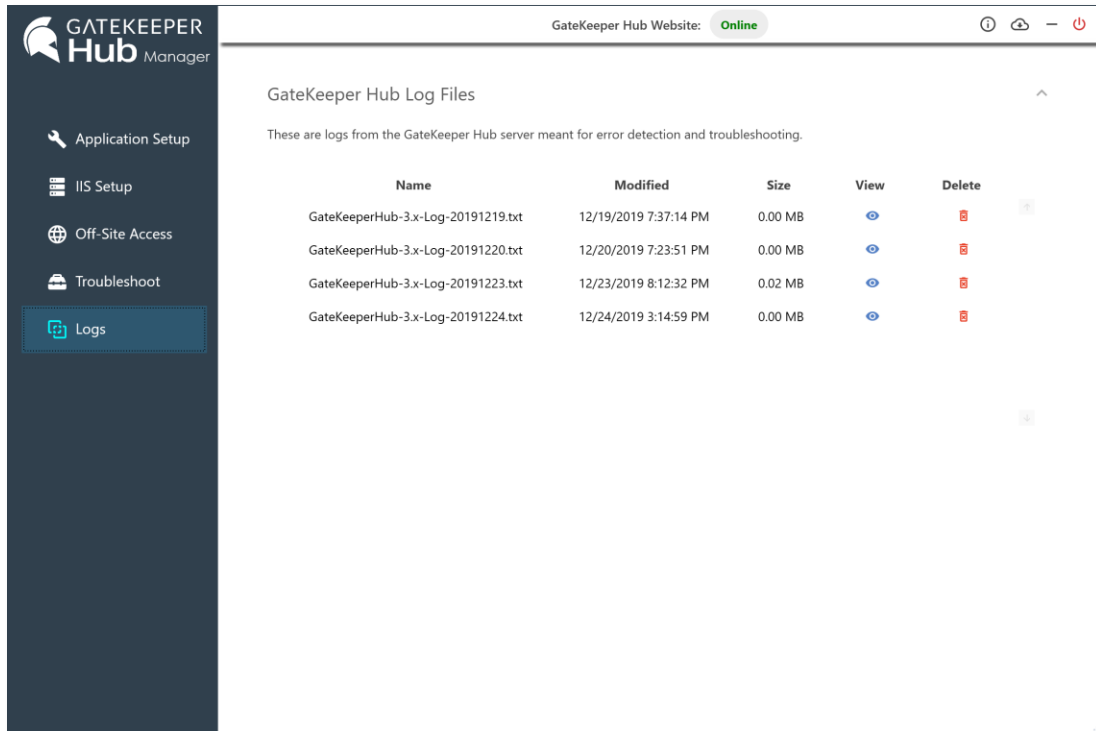
The screenshot shows the GateKeeper Hub Manager interface. On the left is a dark sidebar with navigation links: Application Setup, IIS Setup, Off-Site Access, Troubleshoot (highlighted), and Logs. The main content area is titled 'GateKeeper Hub Website: Online'. Below this is the 'Troubleshooting Steps' section, which includes a description of the process and a table of checks. The table has three columns: Description, Status, and Passed. The Status column shows '--' for all items. The Passed column shows a series of blue 'I' icons, indicating that the tests have passed. A 'Run' button is located at the bottom right of the table.

Description	Status	Passed
Check if Microsoft Windows Hosting Bundle 2.2.8 is installed.	--	I
Check if Microsoft Visual C++ Redist 2017 is installed.	--	I
Check if Microsoft SQL server service is running.	--	I
Check if SQL server is accessible.	--	I
Check if Mixed Mode authentication is enabled.	--	I
Check if GateKeeper Hub database is accessible.	--	I
Check if IIS Application Pool for Hub is running.	--	I
Check if GateKeeper Hub website is running.	--	I

7 Logs



The logs page shows all the error logs that are collected by GateKeeper Hub and stored locally on the computer. These logs can be examined to manage any issues that might be reported during the operation of the GateKeeper Hub website. The logs can be viewed by clicking the  button and deleted by clicking on the  button. In case of any issues with the performance of the GateKeeper Hub server, please send the latest log to GateKeeper Support at support@gkaccess.com to aid in diagnosis.











GateKeeper Hub Manager

GateKeeper Hub Website: Online

GateKeeper Hub Log Files

These are logs from the GateKeeper Hub server meant for error detection and troubleshooting.

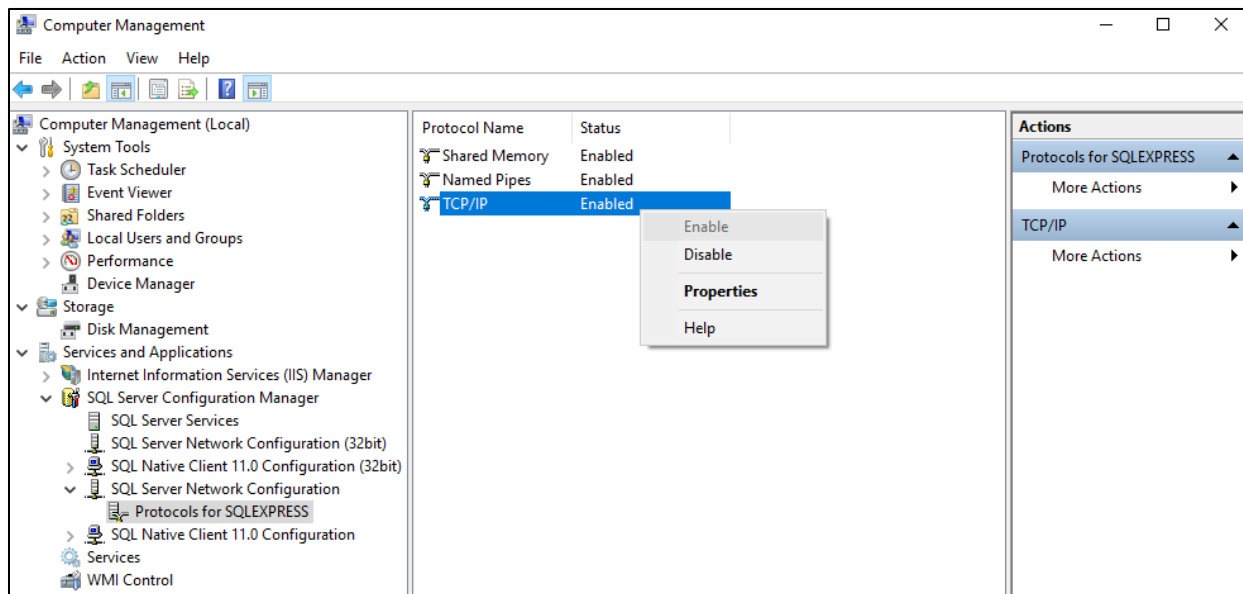
Name	Modified	Size	View	Delete
GateKeeperHub-3.x-Log-20191219.txt	12/19/2019 7:37:14 PM	0.00 MB		
GateKeeperHub-3.x-Log-20191220.txt	12/20/2019 7:23:51 PM	0.00 MB		
GateKeeperHub-3.x-Log-20191223.txt	12/23/2019 8:12:32 PM	0.02 MB		
GateKeeperHub-3.x-Log-20191224.txt	12/24/2019 3:14:59 PM	0.00 MB		

8 Other Technical Aspects

8.1 Enabling TCP/IP Protocol for SQL Server

If the SQL Server is not on the same computer as the GateKeeper Hub server, then you may need to enable the TCP/IP communication with the SQL Server.

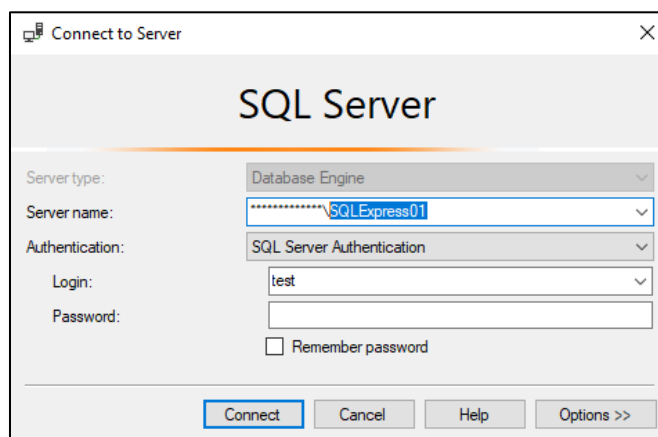
Log in to the computer with the SQL Server and from the **Start Menu**, open **Computer Management**. Expand **Services and Applications**, expand **SQL Server Configuration Manager**, expand **SQL Server Network Configuration**, and click **Protocols for SQLEXPRESS (or whatever the name of your SQL Server is)**. On the right side of the window, right-click on **TCP/IP** under **Protocol Name** and **Enable** it.



8.2 Unable to connect to the SQL Server?

Verify the IP address of the computer where the SQL Server is installed. If it is on the same machine just enter '**(local)**'. If it is on a different machine, log on to that machine. Open the **Command Prompt**, type '**ipconfig**', and note the IP address of the machine.

To check the instance name of the SQL Server, open **SQL Server Management Studio** and verify the instance name by clicking **Connect** to log in. The instance name is mentioned under '**Server name**'.



9 Contact Support

Untethered Labs, Inc.

5000 College Avenue, College Park, MD 20740 USA

www.gkaccess.com

Email: support@gkaccess.com

Phone: 240-547-5446