Periscope for SQL Server

Installation Guide

Copyright 2006
Highwire Development, LLC

System Requirements *3*
Periscope Management Console and Monitoring Services Server **3**
Periscope Repository Database Server **3**
Periscope Reports Server **3**
Installation Overview *4*
Typical Installation **4**
Alternative Installation **5**
Detailed Installation Steps *6*
Create Periscope Repository Database **6**
Run Periscope Management Console Setup **6**
Configure Periscope Repository Database **6**
Configure Periscope Monitoring Services **7**
Install Periscope Reports **12**
Trouble Shooting *13*
Uninstall *13*

System Requirements

Periscope Management Console and Monitoring Services Server

Operating System	Windows XP, 2000, or 2003 Any edition, any service pack
Framework	.NET 2.0 framework MDAC 2.8
CPU	500 MHz or higher
Memory	15 MB per monitored instance
Disk	25 MB

Periscope Repository Database Server

Operating System	Windows XP, 2000, or 2003 Any edition, any service pack
Framework	SQL 2000 or 2005 Any edition, SP2 or higher
CPU	500 MHz or higher
Memory	256 MB
Disk	1.5 MB per 1000 items of captured data

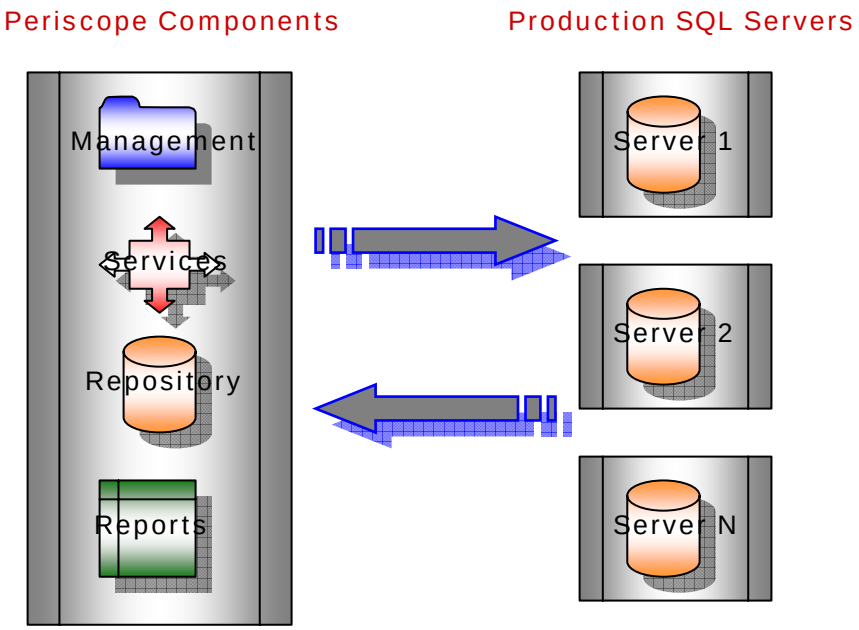
Periscope Reports Server

Operating System	Windows XP, 2000, or 2003 Any edition, any service pack
Framework	IIS 5.0 or higher .NET 1.0 framework
CPU	500 MHz or higher
Memory	256 MB
Disk	25 MB

Installation Overview

Typical Installation

The typical installation involves installing the Periscope Management Console and Services, Periscope Repository Database, and Periscope Reports on one server.

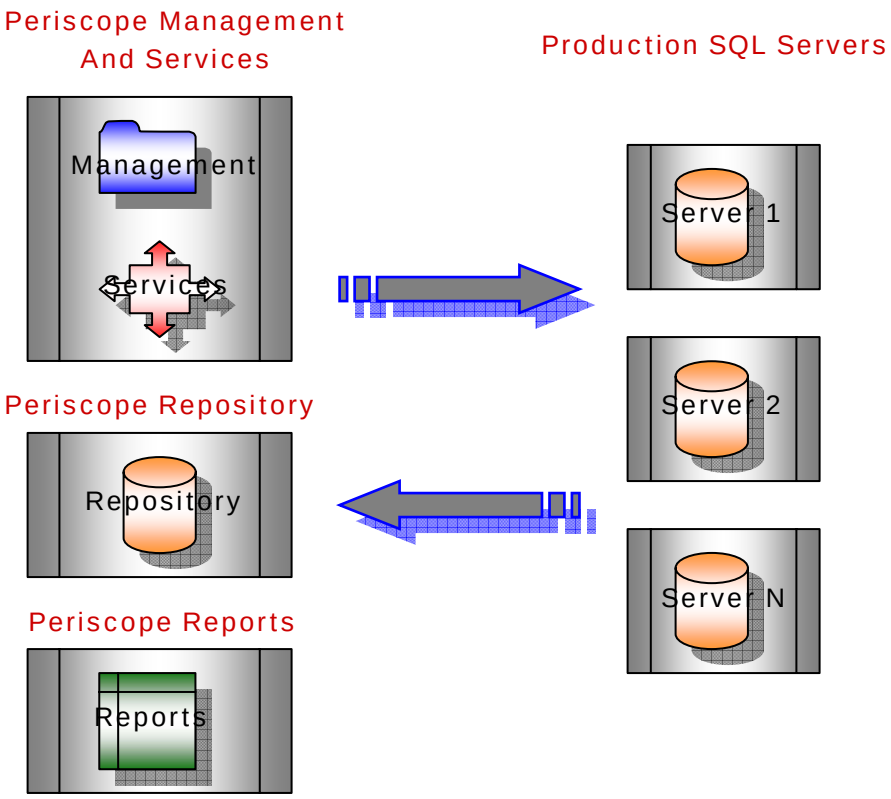


Installation steps are as follows:

- Create Periscope Repository Database on a SQL server
- Run Periscope Management Console setup on the same machine where the Periscope Monitoring Services will run
- Launch the Periscope Management Console and configure the Periscope Repository Database connection information
- Launch the Periscope Management Console and configure Periscope Monitoring Services
- Install Periscope Reports

Alternative Installation

An alternative installation option is to install the Periscope Management Console and Services, Periscope Repository Database, and Periscope Reports on two or more servers.



Installation steps are as follows:

- Create Periscope Repository Database on a SQL server
- Run Periscope Management Console setup on the same machine where the Periscope Monitoring Services will run
- Launch the Periscope Management Console and configure the Periscope Repository Database connection information
- Launch the Periscope Management Console and configure Periscope Monitoring Services
- Install Periscope Reports

Detailed Installation Steps

Create Periscope Repository Database

1. Create a blank database on your Periscope Repository server. The initial size can be determined through the system requirements section. The name may be whatever you wish.

2. If you want the Periscope Monitoring Services to connect to the Repository Database using Windows Authentication, add the appropriate domain user to the db_owner group in the Repository Database.
    - **NOTE**: If you wish to use Windows Authentication, the same domain user must also be used for the service startup account for the Periscope Monitoring Services you will configure later in the installation process.

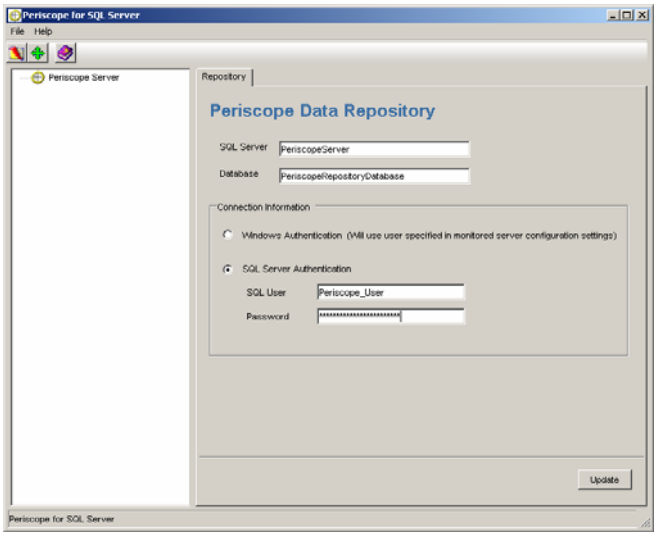
3. If you want the Periscope Monitoring Services to use SQL Authentication to access the Repository Database, create a SQL login and add that login to the db_owner group in the Repository Database.

Run Periscope Management Console Setup

1. Run Periscope Installation.msi from Management Console folder in the installation directory.
2. Click through the installation wizard, then click finish.

Configure Periscope Repository Database

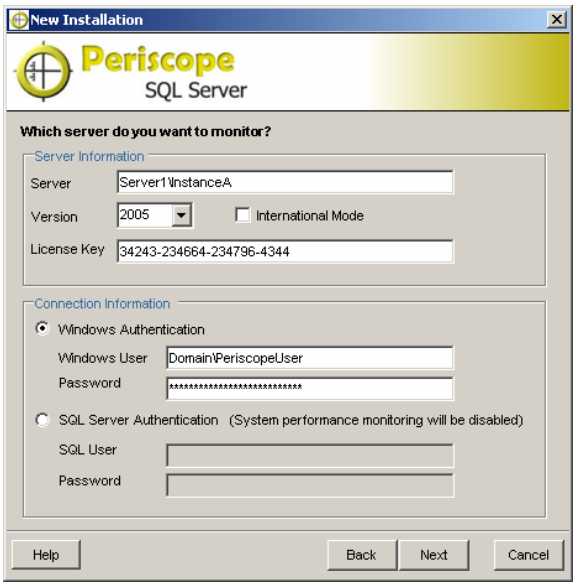
1. The Management Console installation will have created a Periscope for SQL Server start menu group. Find that group and click Periscope Management Console.
2. Click Configure Repository Database.
3. Enter the proper information for the database you created in the first section.
    - **NOTE**: If you wish to use Windows Authentication, the same domain user must also be used for the service startup account for the Periscope Monitoring Services you will configure later in the installation process.



Configure Periscope Monitoring Services

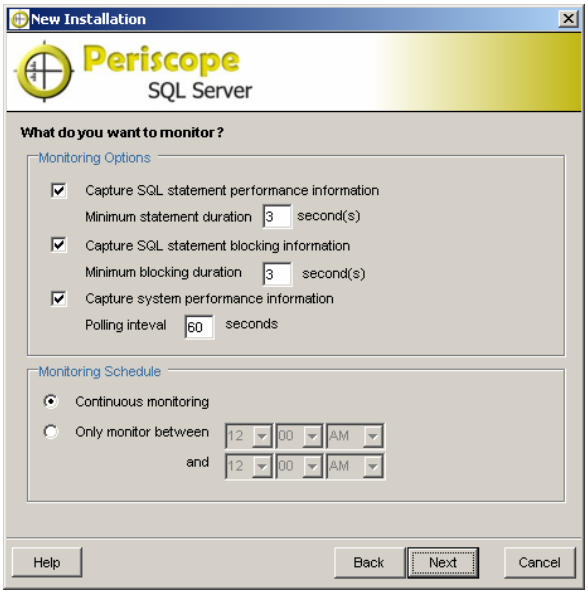
1. Launch the Periscope Management Console from the Start menu.
2. Choose “Install new service” from the File menu, from the main screen, by right clicking on the Periscope Server icon, or click the database shortcut icon.

Connection Tab



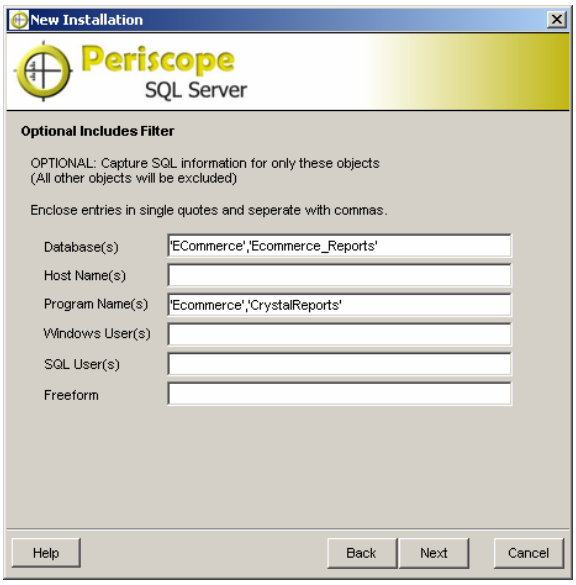
- **New SQL Server**: Enter the name of the SQL server you wish to monitor, and specify the version.
- **Version**: Choose the appropriate SQL server version
- **International Mode**: This will affect date formats (mm/dd/yyyy in the US, dd/mm/yyyy in most other countries). Check this box if either the default language for your SQL server is not English, or the operating system on the Periscope Monitoring Services server or SQL server is not US.
- **License Key**: Enter the key supplied by Highwire Development.
- **Authentication**: Enter the authentication mode for the SQL server to be monitored. The user requires SA privileges on the monitored server in order to capture SQL command text.
    - **NOTE**: If you choose Windows Authentication, the same domain user will be used to connect to the Periscope Repository database, if that is also configured to use Windows Authentication.
    - **NOTE**: If you choose SQL Server Authentication then system performance information such as CPU utilization, Pages/sec, etc. will not be captured.

Monitoring Tab



- **Capture statement performance information**: Check if wish to capture this information, and choose the minimum duration in seconds you wish to capture.
- **Capture statement blocking information**: Check if you wish to capture this information, and choose the minimum duration in seconds you wish to capture.
- **Capture system performance information**: This includes CPU, memory, disk, and network subsystems, as well as SQL specific information such as connections, active transactions, etc. Check if you wish to capture this information, and choose how often you want to collect data.
- **Continuous or Scheduled monitoring**: Choose if you wish to monitor your SQL Server continuously, or only during certain hours.

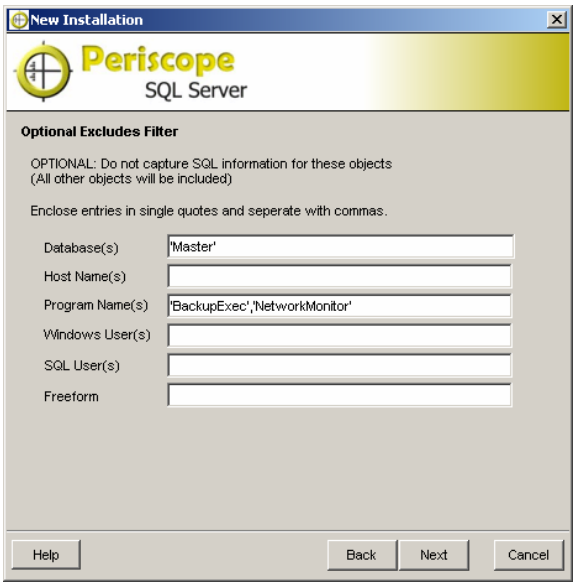
Includes Tab



This tab is optional

- Enter any objects for which you wish to explicitly capture information. This includes data for both statement performance monitoring and blocking monitoring.
    - All entries must be surrounded by single tics – ‘ – and must be separated by commas. Ex. ‘Object1’,’Object2’ or ‘UserABC’.
    - A percent symbol - % - may be used as a wildcard
    - Freeform: any column that exists in the Master..Sysprocesses table in SQL 2000 may be entered here. Ex. Net_library = ‘TCP/IP’ or Net_address = ‘000F1F6F8D10’ and Open_tran = 1
- If any fields are filled in, all other objects in that category will be excluded. Ex. ‘Computer10’ is entered for Host Name(s), all other hosts will be excluded from performance and blocking monitoring.

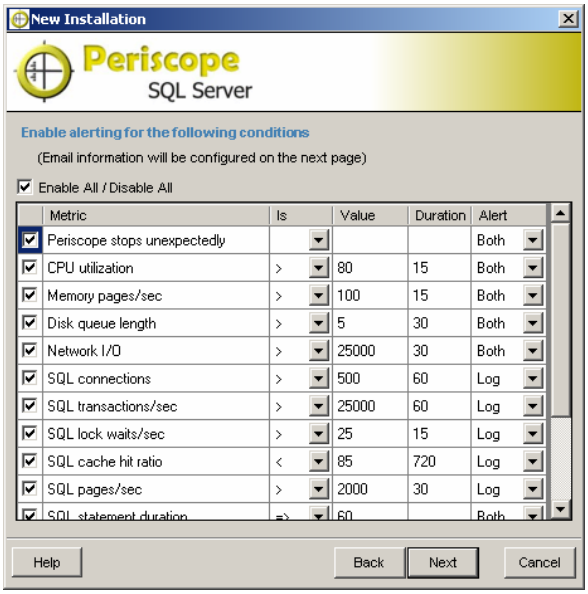
Excludes Tab



This tab is optional

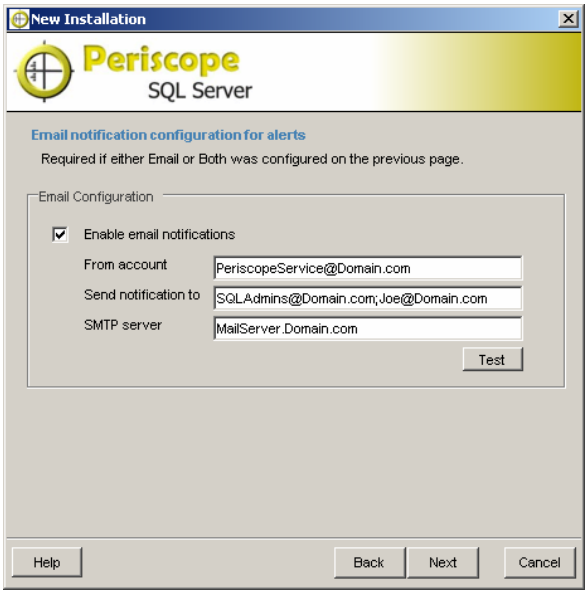
- Enter any objects for which you wish to explicitly not capture information. This includes data for both statement performance monitoring and blocking monitoring.
    - All entries must be surrounded by single tics – ‘ – and must be separated by commas. Ex. ‘Object1’,’Object2’ or ‘UserABC’.
    - A percent symbol - % - may be used as a wildcard
    - Freeform: any column that exists in the Master..Sysprocesses table in SQL 2000 may be entered here. Ex. Net_library = ‘TCP/IP’ or Net_address = ‘000F1F6F8D10’ and Open_tran = 1
- If any fields are filled in, all other objects in that category will still be included. Ex. ‘Computer10’ is entered for Host Name(s), all other hosts will still be included in performance and blocking monitoring.

Alerts Tab



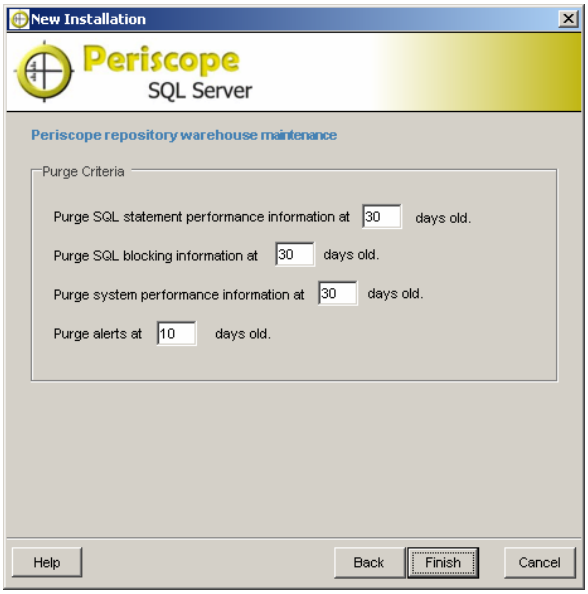
- Check the checkbox next to any alerts you would like to enable.
  - **Metric:** The monitored metric for which you would like to receive alerts. Important – if you did not enable the type of monitoring required for a specific metric, you will not receive alerts for that metric. For example, if you did not enable “Capture System Performance Information” earlier in the new service wizard, you will not receive alerts for the “CPU utilization” metric.
  - **Is:** Comparison to use.
  - **Value:** The threshold which must be met for a particular metric. Measurement may be in milliseconds, seconds, or actual count, depending on the metric.
  - **Duration:** The number of minutes the threshold must be met in order for the alert to fire.
  - **Alert:** Type of alert to raise when a threshold is met.
    - **Email:** An alert will be emailed to the address configured on the next tab
    - **Log:** An alert will be written to the Periscope Repository Database and will be viewable through Periscope Reports
    - **Both:** An Email will be sent and the log will be updated

Notification Tab



- Send email alerts via the configured settings. Required if either “Email” or “Both” alert types were configured on the previous tab.
    - **From account**: A valid email account on the SMTP server
    - **Send notification to**: Valid email account(s) on the SMTP server. Multiple accounts should be separated with your email server separator, generally a semicolon.
    - **SMTP server**: You corporate mail server. Can be MS Exchange or any other SMTP server

Warehouse Tab



- **Purge Repository Database Data**: Performance and alert data held in the Repository Database for this particular instance will be purged and not be available for future reporting.

Install Periscope Reports

Wizard Based Installation

1. Launch PSReportsInstall.msi from the Periscope Reports folder. Follow through the steps and click Finish.
2. At the end of the installation the wizard will open the Web.Config file. Modify the database connection section as follows:

   If using **SQL Authentication** to connect to the Periscope Repository Database, enter the appropriate information like this:

```
<appSettings>
   <add key="dbconnection" value="server=???;user id=???;password=???;database=???" />
</appSettings>
```

   The SQL user used to connect to the Repository Database must have data_reader and ddl_admin permissions in the database at a minimum.

   If using **Windows Authentication** to connect to the Periscope Repository Database, enter the appropriate information in the web.config file like this:

```
<appSettings>
   <add key="dbconnection" value="server=???;database=???;Trusted_Connection=true" />
</appSettings>
```

   In order to use Windows Authentication, the IIS login account must be mapped to the Periscope Repository Database:

   2.1 If Periscope Reports is installed on the same server running the Periscope Repository SQL database AND you are using IIS 6.0, you can add the local IIS_WPG group as a user in the Periscope database
   2.2 If Periscope Reports is installed on the same server running the Periscope Repository SQL database AND you are using IIS 5.1 or below, you can add the local ASPNET account as a user in the Periscope database
   2.3 If Periscope Reports is installed on a different server than the Periscope Repository SQL database, impersonation must be used as detailed below:

   In the web.config file, add the following: <identity impersonate="true" />

   Then, from IIS Manager, right click on the virtual directory assigned to your application and select “Properties”. Click on the “Directory Security” tab, then under “Anonymous access and authentication control” click “Edit”. If you are going to allow anonymous access to the application (not requiring users to login with windows authentication each time they access this web application), make sure “Anonymous access” checkbox IS checked. Then uncheck “Allow IIS to control password”. In the “User Name” field, type in (or you can browse to) the domain account (domain\user) and type in the password for the domain account in the “Password” field (By default IIS uses IUSR_machinename for the anonymous account, you can refer to this page if you would like to find its default password in case you want to change it back later for some reason) . Then under “Authenticated Access”, make sure NONE of the boxes are checked. Press “OK” and “OK” to save the settings and exit IIS.

   In any of the above scenarios, the user used to connect to the Repository Database must have data_reader and ddl_admin permissions in the database at a minimum.

   Save and close the web.config file.

3. To view reports, point your web browser to http://IIS_Server/Periscope , or http://IIS_Server/PeriscopeInstallationDirectory if you changed from the default.

Trouble Shooting

Monitoring

If you believe you have a correct Periscope license key – either trial or production – and you receive “invalid license” or “license expired”, try checking the “International Mode” check box. This is for dd/mm/yy date formats (as opposed to the US date format which is mm/dd/yy).

The Periscope Monitoring Services are configured to write to the Event Viewer – Application Log on the computer where they are running.

If your service stops or doesn’t appear to be capturing data correctly, check the Event Viewer for error events for Periscope or Periscope *SERVERNAME.* Generally the first couple of errors after the service is started will contain the most useful information.

Reports

If you receive error code 2755 during the PSReportsInstall wizard, try copying the .msi to a local disk on the web server and rerun the setup. This is a known issue that occurs on occasion with Microsoft web deployment applications.

If you attempt to run Periscope Reports and you appear to be missing web page objects – drop down menus, buttons, etc., there is most likely an ASP.NET to IIS mapping issue on your web server. This is a common issue with IIS 5.1 and below installations, which are not .NET native. This can occur if IIS is installed after .NET, for example.

The simplest way to resolve this issue is to recreate the ASP.NET to IIS mappings by running the following command at a command prompt:

aspnet_regiis –i

Uninstall

To uninstall Periscope for SQL Server, perform the following steps:

1. Launch the Periscope Management Console and uninstall each Periscope Service instance. It is not necessary to choose the uninstall database option since the Periscope Repository Database will be dropped.
2. Uninstall the Periscope Management Console through Control Panel – Add/Remove Programs on the Management server.
3. Drop the Periscope Repository Database on the SQL Server.
4. Delete the Periscope Reports virtual directory and files through the IIS Administrator.