
REM Deployment Guide

The Security Integrator Reference Guide

Deploying REM within your Enterprise

eEye Digital Security



eEye Digital Security®

Warranty

This document is supplied on an "as is" basis with no warranty and no support.

Limitations of Liability

In no event shall eEye Digital Security be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this user guide.

Disclaimer

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. eEye Digital Security is not associated with any other vendors or products mentioned in this document.

This document contains information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of eEye Digital Security.



Contents

System Requirements	1
Minimum System Requirements	1
REM Server Machine	1
Recommended System Requirements	1
REM Server Machine	1
Installation Summary	2
Installation Order	2
Approximate Installation Time	2
REM Events Server Installation	3
File Installation	3
Licensing	5
Configuration	5
Changing the Replication Configuration	13
REM to REM Replication	14
REM:ES Master	14
REM:ES Slave	15
Manual Database Preparation	16
REM Events Manager Installation	17
File Installation	17
Licensing	19
Configuration	20
Configuring REM Events Server SQL Security	21
Accessing the REM Events Manager	23



System Requirements

Minimum System Requirements

REM Server Machine

- Microsoft Windows 2000 (SP3) or Microsoft Windows 2003
- Microsoft IIS 5.0 or above
- Microsoft .NET Framework version 1.1
- Intel Pentium IV 2GHz CPU (or equivalent)
- 1 gigabyte (GB) of RAM
- 100 MB of free hard disk space required for installation
- 1 gigabyte (GB) of free hard disk space recommended for event storage
- Microsoft SQL Server 2000 Desktop Engine (SP3)
- Microsoft Internet Explorer version 5.0 or higher

Recommended System Requirements

REM Server Machine

- Microsoft Windows 2000 (SP3) or Microsoft Windows 2003
- Microsoft IIS 5.0 or above
- Microsoft .NET Framework version 1.1
- Intel Pentium IV 2GHz CPU (or equivalent) dual processor
- 2 gigabytes (GB) of RAM
- 10 MB of free harddisk space required for installation
- 10 GB of free hard disk space recommended for event storage
- Microsoft SQL Server 2000 (SP3)

- Microsoft Internet Explorer version 6.0 or higher



Specific configuration will depend on expected product usage (for example, scanned network size, number of scanners, frequency of scanning, events data retention requirements, and so on).

Installation Summary

Installation Order

It is recommended that you install REM in the following order:

1. REM Events Server
2. REM Events Manager

Approximate Installation Time

Approximate installation times are based on a machine meeting the minimum system requirements.

REM Events Server	30 Minutes *
REM Events Manager	15 Minutes
Total	45 Minutes



The estimated REM Events Server installation time does not include installation of MS-SQL database server (if necessary).



REM Events Server Installation

The REM Events Server functions as a hub between the REM database and REM Event Clients. Each event created by an REM Event Client application is sent to the REM Events Server, which in turn processes the event and inserts it into the REM database.

Perform the installation as an Administrator on the local machine.

File Installation

Follow these steps to install the REM Events Server:

1. Download the program from the eEye web site at <http://www.eeye.com/clients/>, using your user name and password.
2. When the setup program starts, the installation welcome screen displays. This screen serves as an introduction for the installation program. Click **Next** to continue.
3. The *License Agreement* screen displays. Review the End User License Agreement, and then click **Yes** to accept the terms of the license agreement.



License Agreement screen

4. The *Select Destination Folder* screen displays. You have the option of installing the REM Events Server to a different location than the default of C:\Program Files\eEye Digital Security\REM Events Server. Once you have selected a destination, click **Next** to continue.
5. The *Ready to Install the Application* screen displays. Click **Next** to begin copying files.
6. If you have a previous version of REM Events Server installed on your machine, you will be prompted to delete your configuration files during the install (for example, the database selection, the DSN, and so on). If you would like to keep the same configuration in the new version, click **No**.



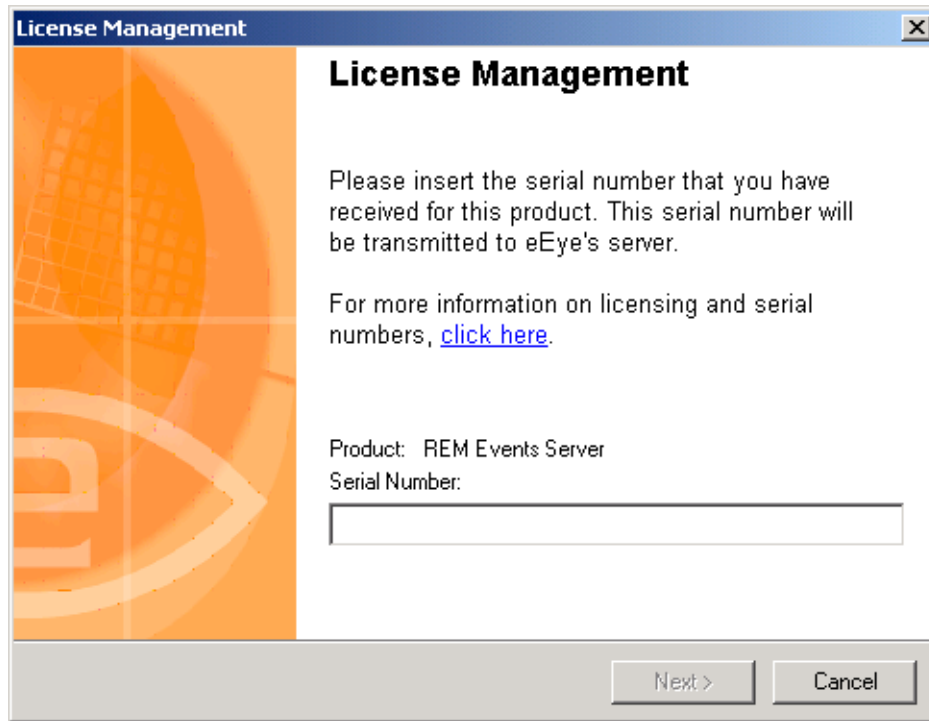
If you have a previous version of REM Events Server on your machine, the uninstallation of REM Events Server begins automatically. If you would like to keep the same configuration in the new version, click **No** when it prompts you to delete your configuration files defining the connection settings. You should also click **No** when prompted to delete any associated certificates. The uninstall process may also prompt you to remove shared files. If this occurs, click **No to All**.

7. Once all the necessary files are copied to your computer, the *Installation Complete* screen displays. Click **Finish** to exit the installation. If it is necessary to reboot the machine to complete the installation, you will be prompted to do so.

Licensing

Follow these instructions to license the REM Events Server:

1. If no reboot is required, you will be prompted for a serial number at the end of the installation. Type the serial number that you received for the REM Events Server. If your machine needs to be rebooted, you will be prompted for your serial number when you begin configuring the REM Events Server. *(If you are reinstalling REM Events Server on a machine that already has a valid serial number, you will not be prompted to re-enter it.)*



License Management screen

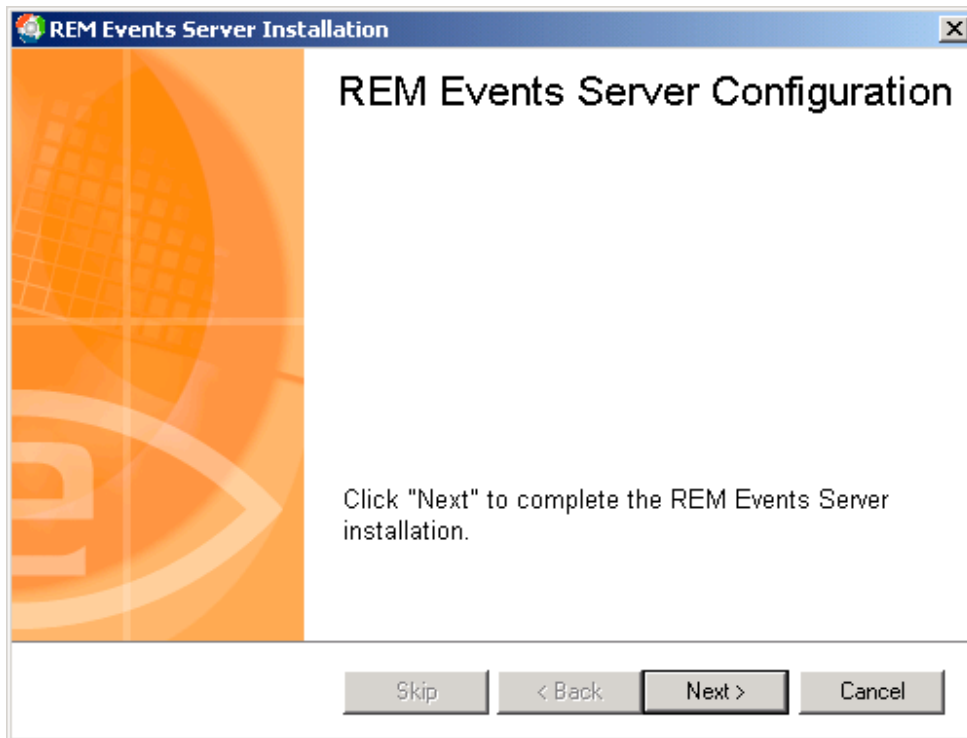
2. After you have entered the serial number, click **Set**.

Configuration

Follow these instructions to configure the REM Events Server:

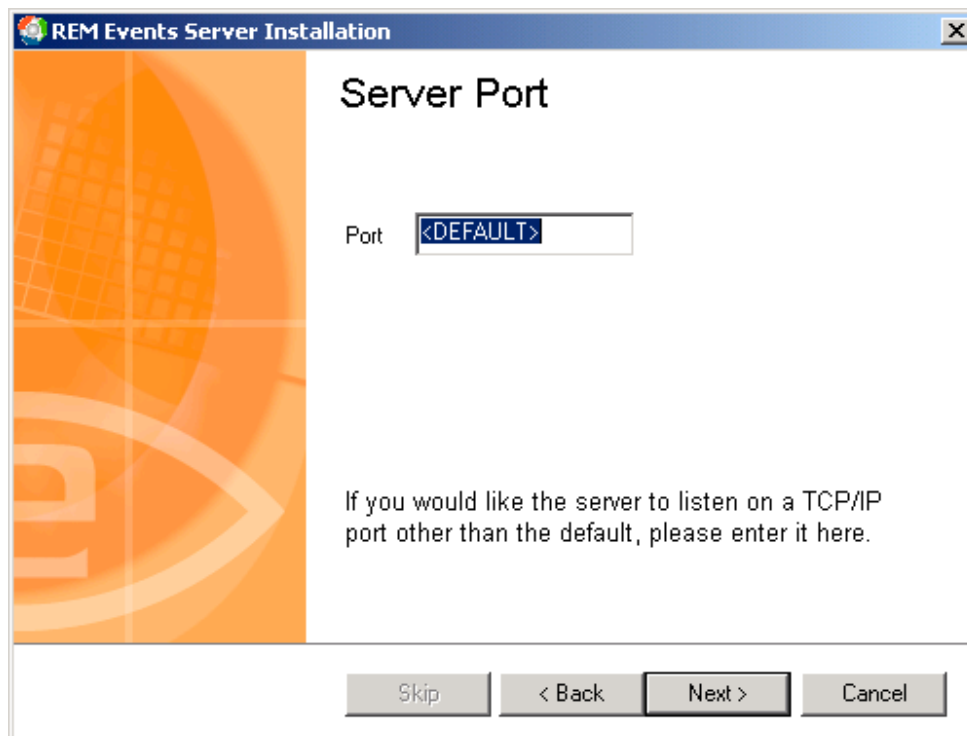
1. After you have licensed the product, the REM Events Server configuration wizard should start automatically. If it does not start automatically, you can manually launch it by clicking *Start > Programs > eEye Digital Security > REM Events Server > Server Configuration*. If you performed this installation by upgrading from a previous version of REM Events Server and you chose not to delete the existing configuration during the server uninstall, the settings will default to the previous configuration.

- The *REM Events Server Configuration* screen displays. Click **Next**.



REM Events Server Configuration screen

- The *Server Port* screen displays. Specify a port for the REM Events Server, or leave the value at <DEFAULT>. (The default port is 21690.) This port will be used to communicate with the applications (for example, Retina, Blink). Click **Next**.



Server Port screen

4. The *Configure Database* screen displays. This screen contains options for configuring the SQL Database.
 - **Create database** check box — Select this check box to create a SQL Server database with the specified information. By default, the Database Name is assigned the label: REM.
 - **Automatically create DSN** check box — Select this check box to create an ODBC Data Source Name with the specified information to be used by REM Events Server.



If an upgrade is being performed and the database and DSN already exist, both options will likely be unnecessary; therefore, uncheck either or both as appropriate. Attempts to recreate the database will generate an error that the “Database already exists”, and the user will be forced to revisit this page to modify the selection.

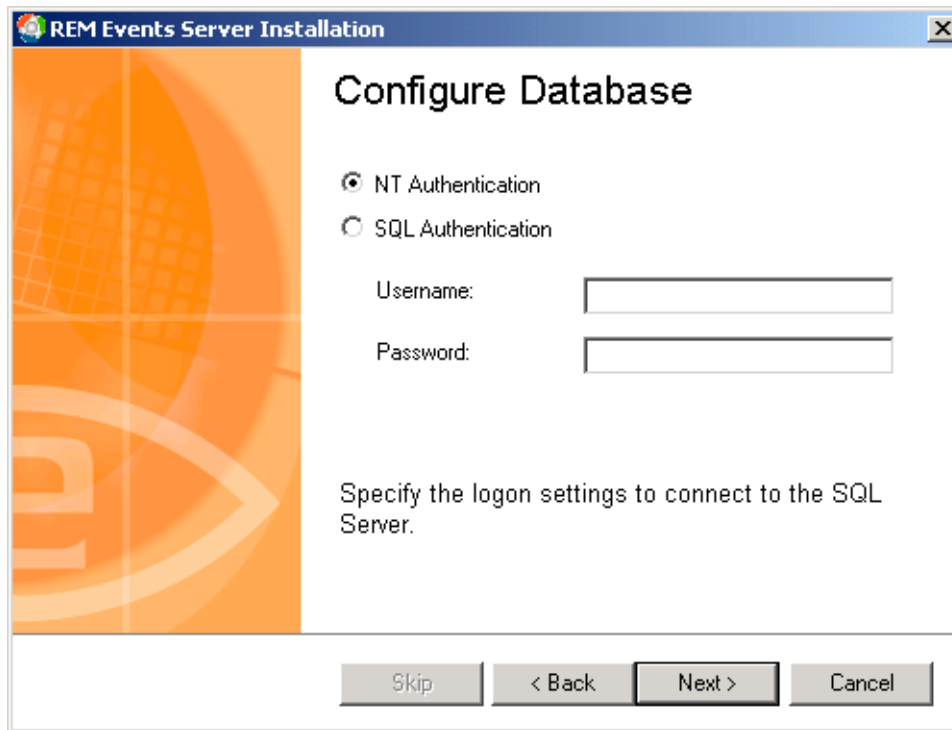
A screenshot of the 'Configure Database' window in the REM Events Server Installation process. The window has a blue title bar with the text 'REM Events Server Installation' and a close button. The main area has an orange background on the left and a white area on the right. The title 'Configure Database' is centered at the top. Below the title are two checked checkboxes: 'Create database' and 'Automatically create DSN'. Below these are two text input fields: 'SQL Server name:' with the value 'CSMITH\ENG' and 'Database Name:' with the value 'REM'. Below the input fields is a paragraph of text: 'To automatically create the REM Events Server database and/or DSN, specify the SQL Server settings.' At the bottom of the window are four buttons: 'Skip', '< Back', 'Next >', and 'Cancel'.

Configure Database screen

5. If either the **Create database** or **Automatically create DSN** check boxes are selected, you will be prompted to specify the credentials for the database connection.

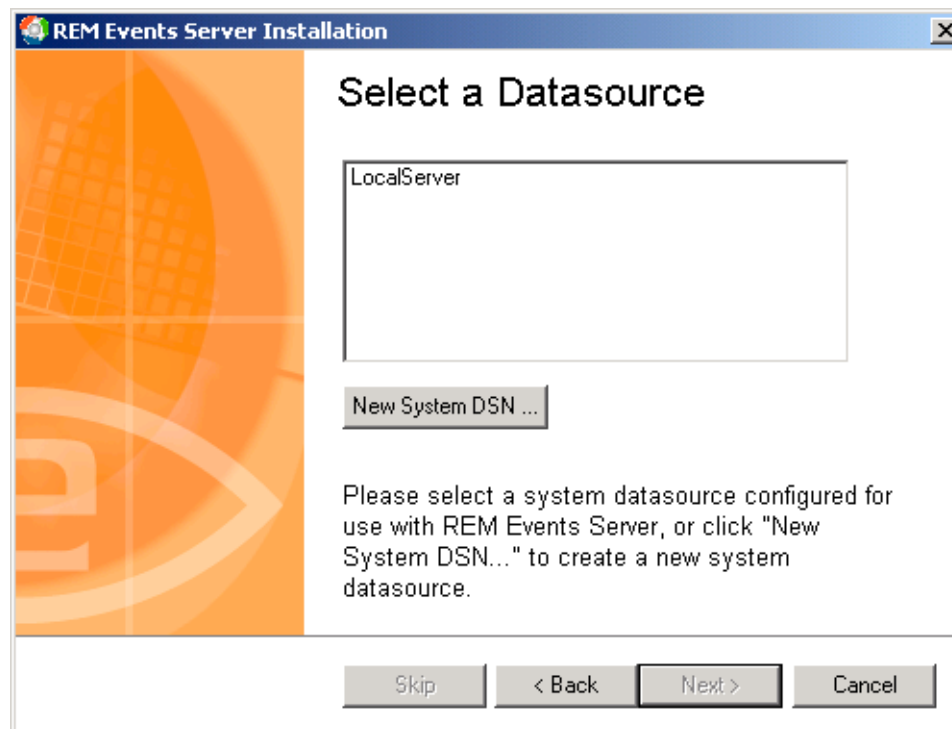


NT Authentication requires the local IUSR account, and that user be assigned to the database with access to the REM tables.



Specifying authentication

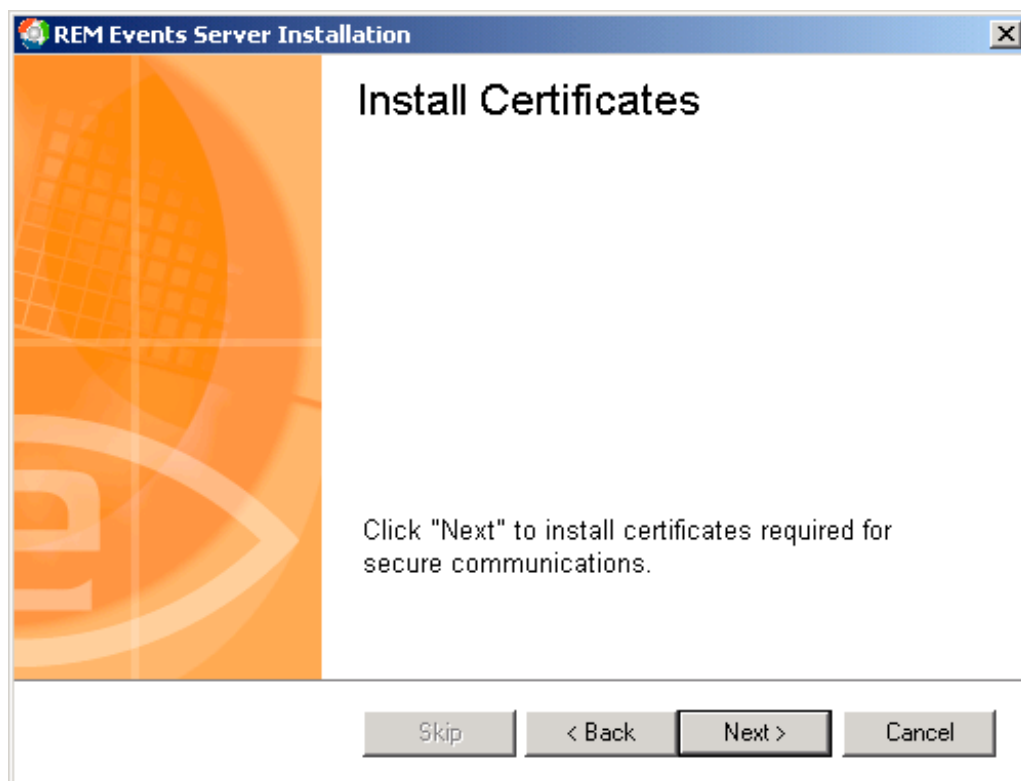
6. The *Select A Datasource* screen will display if you did not choose to automatically create it. Click **New System DSN** to start the *Microsoft Create New Data Source* wizard.



Selecting a datasource

7. From the Microsoft wizard, select **System Data Source** and click **Next**.
8. From the driver list, select **SQL Server** and click **Next**.

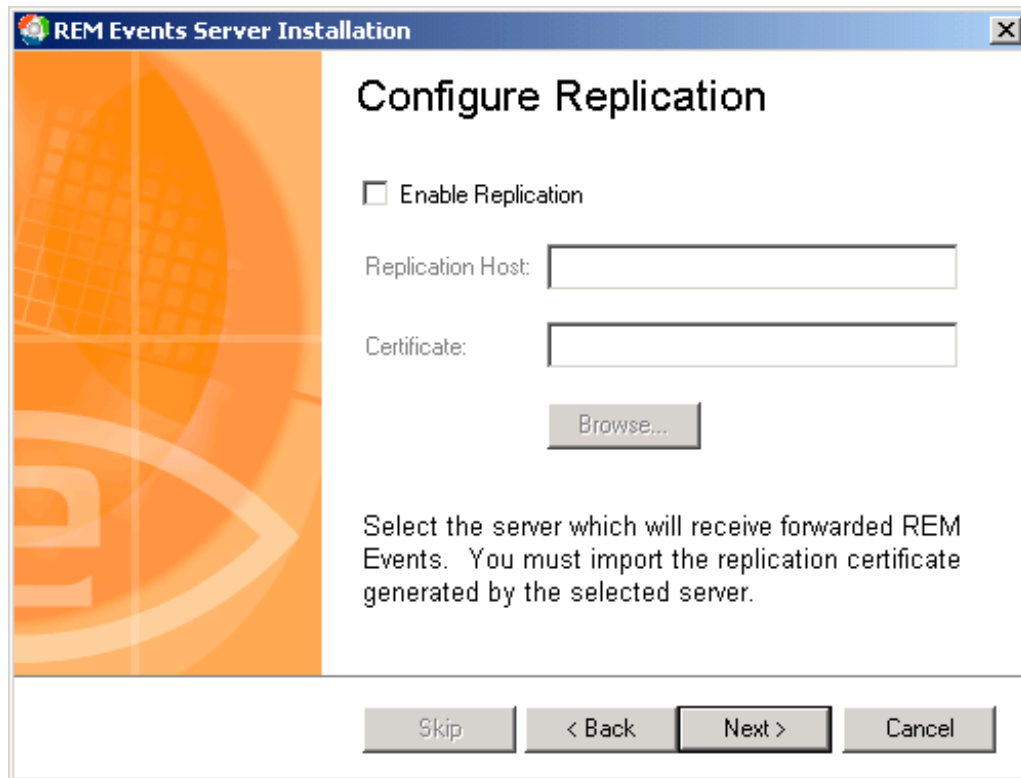
9. Click **Finish**. The *Create a New Data Source to SQL Server* wizard begins. Type eEye REM DataSource in the *Name* and *Description* fields. In the *Server* field, select your SQL server and click **Next**.
10. Select **With Windows NT authentication using the network login ID** and click **Next**.
11. A screen displays that allows you to change the default database for the data source. Select *Change the default database to:* and type the name you selected during database preparation (for example, "REM"). Click **Next**, and then click **Finish**.
12. You can now test your data source to verify connectivity. After testing your data source, exit the Microsoft wizard, and select your newly created *REM* data source from the REM Events Server configuration wizard list. Click **Next**.
13. Choose the *REM* Datasource and click **Next**. Now it's time to generate and install your certificates.
14. The *Install Certificates* screen displays. In order for the REM Events Server and REM Event Client to communicate in a secure manner, they each must have a valid certificate. Click **Next** to have the configuration wizard generate the necessary certificates.



Installing certificates for secure communication

15. After the certificates are generated, click **Next** to continue.
16. The *Configure Replication* screen displays. If replication is desired, select the **Enable Replication** check box. This enables this REM Events Server machine to forward all events to the specified Replication Host. The Replication Host must be a REM Events Server configured to accept replicated events, and the Certificate must be the exported replication certificate from that host.

To select the Certificate, click the **Browse** button, locate the exported certificate file, and then click **OK**. You will be prompted for the password for the certificate. Once the host and certificate have been configured, click **Next** to continue. (For information on REM to REM Replication, see **“REM to REM Replication” on page 14.**)



Configuring replication

17. The *Export Client Certificate* screen displays. Select a destination for the client certificate. This certificate will be needed on all REM Event Client machines on your network. The certificate will be exported and enable the REM Events Server to accept replicated events. It is recommended that you store this certificate in a secure location that can be accessed later by a remote node. (Clicking **Skip** will not export the certificate and disable accepting replicated events.) Click **Next**.



CAUTION: Store this Certificate in a secure location. If an attacker can access this certificate, they may be able to intercept REM security events.



Exporting the Client Certificate

18. The *Client Certificate Password* screen displays. Select a password to protect your REM Event Client Certificate. We recommend choosing a password that is at least eight characters in length, contains numbers and letters, varying from uppercase and lowercase. Confirm your password by typing it again in the confirmation box, and then click **Next**. You will receive a notification message that your certificate has been exported correctly to the location that you specified previously.



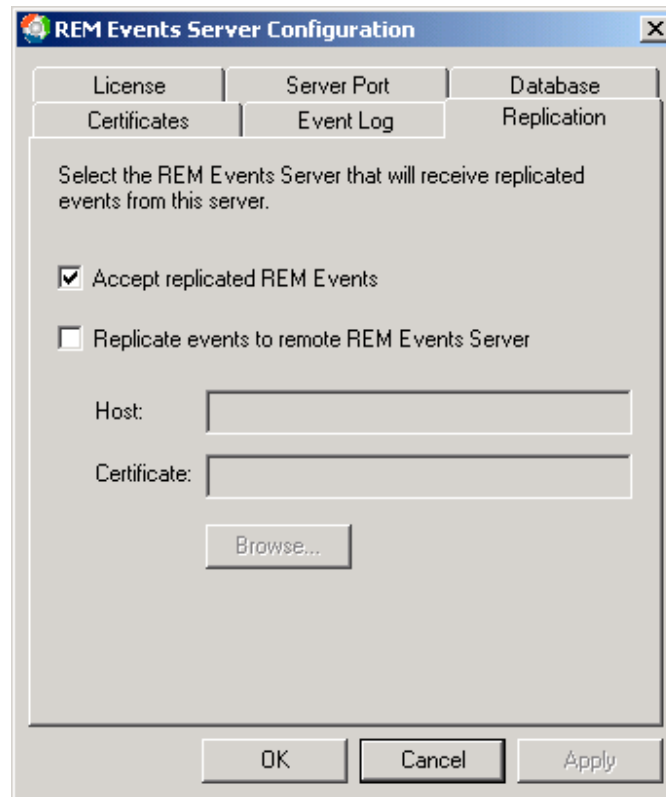
Specifying a password for the client certificate

19. Click **Finish**. Your REM Events Server has now been configured.

Changing the Replication Configuration

To make changes to the replication configuration after running the wizard, you must use the *REM Events Server Configuration* dialog box.

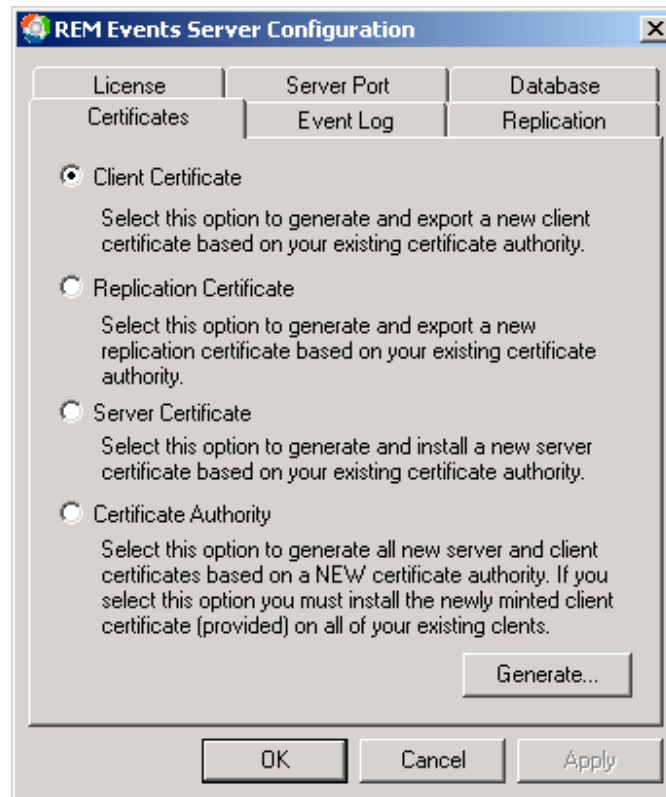
To open the *REM Events Server Configuration* dialog box, click the **Start** button, and then point to **Programs**. Point to the **eEye Digital Security** folder, point to **REM Events Server**, and then click **Server Configuration**. Click the **Replication** tab.



Changing the replication configuration

- **Accept replicated REM Events** — Allows incoming replicated REM Events from other REM Events Servers
- **Replicate events to remove REM Events Server** — Enables REM Events to be forwarded to the specified Host using the certificate from that REM Events Server
- **Host** — Name or IP of the REM Events Server to send the replicated events
- **Certificate** — Path to the certificate file to import. This field will be blank if the certificate was previously imported.

To enable replicated events to be received by this REM Events Server, you can export another Replication Certificate by clicking the *Certificates* tab, selecting the desired Certificate, and then clicking **Generate**. Make sure the *Accept replicated REM Events* option is selected on the *Replication* tab.



Selecting a certificate

REM to REM Replication

The REM Events Server has the ability to replicate the events it receives to another REM Events Server. This allows for high scalability during the installation of the REM solution, and ensures a secure way to replicate the information from REM to REM.

This section discusses the concept of the REM Events Server Master (REM:ES Master) and the REM Events Server Slave (REM:ES Slave). The REM:ES Slave forwards the events, while the REM:ES Master receives the events using the default port TCP/21692.

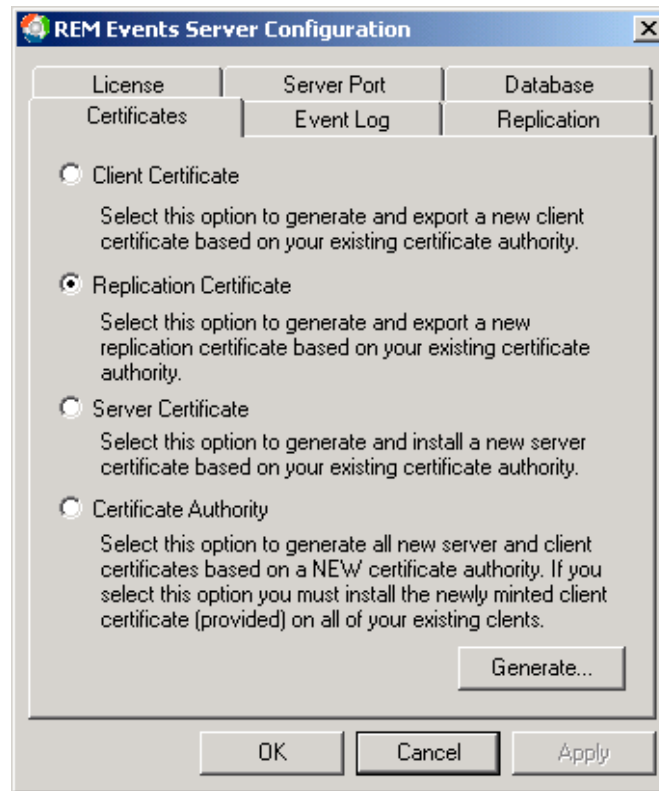
Store and forward technology has been implemented in the replication system to ensure that if the REM:ES Master is not available to the slave, the information will get stored locally and sent to the REM:ES Master at a later point, when communication is resumed.



The default port TCP/21692 used for replication can be redefined by modifying the registry keys in the following path: `HKLM\SOFTWARE\eEye\EMS\Server`. As it relates to the traffic direction of the replicated data, enter a decimal value for **Port** in both: **CommIn** and **CommOut**

REM:ES Master

While installing the REM Events Server, you will be prompted to generate a Replication certificate. This certificate will be used to secure the communication between the two REM Events Servers. Make sure to protect this certificate with a strong password. You will be able to generate a new Replication Certificate later if you skipped this step during the installation process by using the *Certificates* tab in the *REM Events Server Configuration* dialog box. Make sure the **Accept replicated REM Events** check box is selected on the *Replication* tab. (See **“Changing the Replication Configuration”** on page 13 for more information.)



When using REM to REM replication, make sure the **Enable Replication** check box in the *Configure Replication* screen is selected.

REM:ES Slave

The REM Events Server Slave does not need to generate the Replication Certificate, therefore, you can skip this step during the installation process. However, you will need to import the REM:ES Master Replication certificate generated in the previous step into the REM:ES Slave so that they are both able to establish a secure tunnel for communication.

- In the installation wizard, you must specify the IP address of the REM:ES Master you want to forward the events to, and then specify the certificate for the REM:ES Master.
- You will be prompted for the password you defined for the REM:ES Master Replication Certificate.

Next, open the *REM Events Server Configuration* dialog box.

1. Click the *Replication* tab.
2. Select the **Replicate events to remote RM Events Server** check box.
3. Specify the REM:ES Master IP address in the *Host* field.
4. Click the **Browse** button to import the REM:ES Master Replication Certificate. You will be prompted for the password of this certificate.

Manual Database Preparation

The Server Configuration Wizard performs these steps for you automatically if you are using Microsoft SQL Server 2000 when the wizard is run. If you choose to manually configure a database, follow these instructions to configure the database with the REM Event tables.

1. Start your database management software. You can do this by clicking *Start > Programs > Microsoft SQL Server > Enterprise Manager*.
2. Once the Enterprise Manager is started, locate your server from the tree view in the left window pane and select *Databases*.
3. Click the **Action** menu, and then select **New Database**.
4. A dialog box opens. Type a name for the database (for example, "REM"). If desired, use the *Data Files* and *Transaction Logs* tabs to change the location of the database files. Click **OK**.
5. Close the SQL Server Enterprise Manager. Your REM database has now been created.
6. Next, launch your database querying client software. You can do this by clicking *Start > Programs > Microsoft SQL Server > Query Analyzer*.
7. Once the application launches, select your database server from the *Connect To SQL Server* screen, and then click **OK**.
8. Click the **Query** menu, and then select **Change Database**.
9. Select the database that you previously created, and then click **OK**.
10. Click the **File** menu, and then select **Open**.
11. Included with the REM Events Server installation is an SQL script to create tables that your REM Events Server will use in the future. When the *Open query file* screen displays, you will need to navigate to the REM Events Server installation directory and choose the SQL script `create_script (install).sql`. Click **OK** once to select the script.
12. Click the **Query** menu, and then select **Execute**. This will run the script and create the REM tables.
13. When the SQL script is finished running, the "The command(s) completed successfully" message displays. Close the SQL Query Analyzer. The REM database is now ready for the REM Events Server.



REM Events Manager Installation

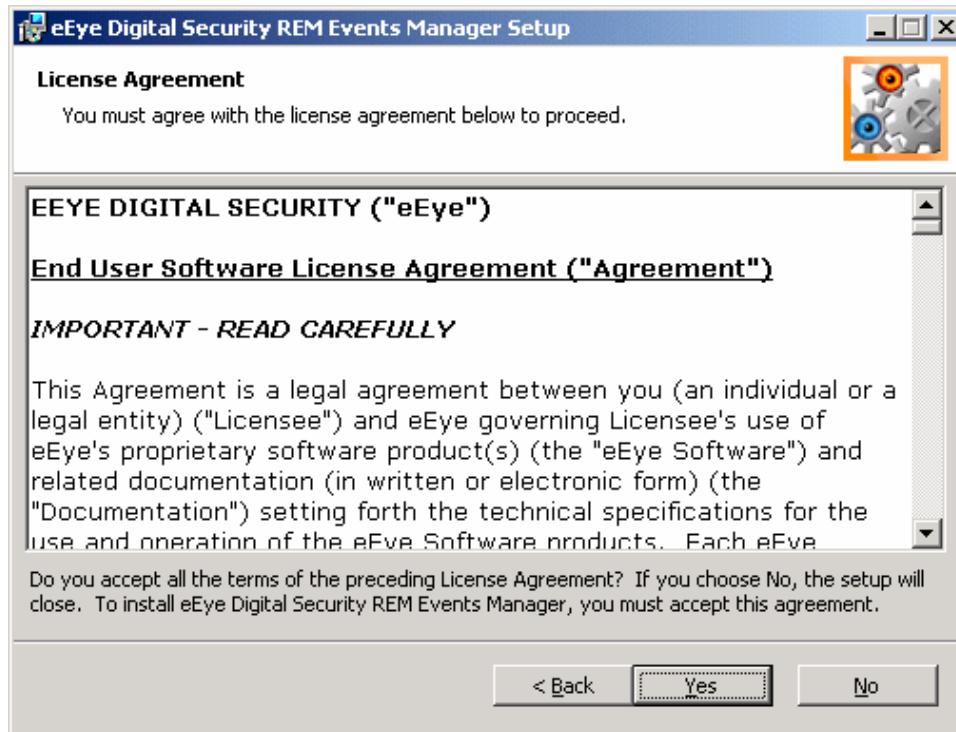
The REM Events Manager allows you to administer all of the REM events from a centralized web interface. You can delegate events to users, assign tasks and priorities, as well as generate detailed reports.

Perform the installation as an Administrator on the local machine.

File Installation

Follow these steps to install REM Events Manager:

1. Download the program from the eEye web site at <http://www.eeye.com/clients/>, using your username and password to enter.
2. When the setup program launches, the installation welcome screen displays. This screen serves as an introduction into the installation program. Click **Next** to continue.
3. The *License Agreement* screen displays. Review the End User License Agreement and click **Yes** to accept the terms of the license agreement.



License Management screen

4. The *Select Destination Folder* screen displays. You have the option of installing the REM Events Manager to a different location than the default of C:\Program Files\eEye Digital Security\REM Events Manager. Once you have selected a destination, click **Next** to continue.
5. The *Start Installation* screen displays. Click **Next** to begin copying files.



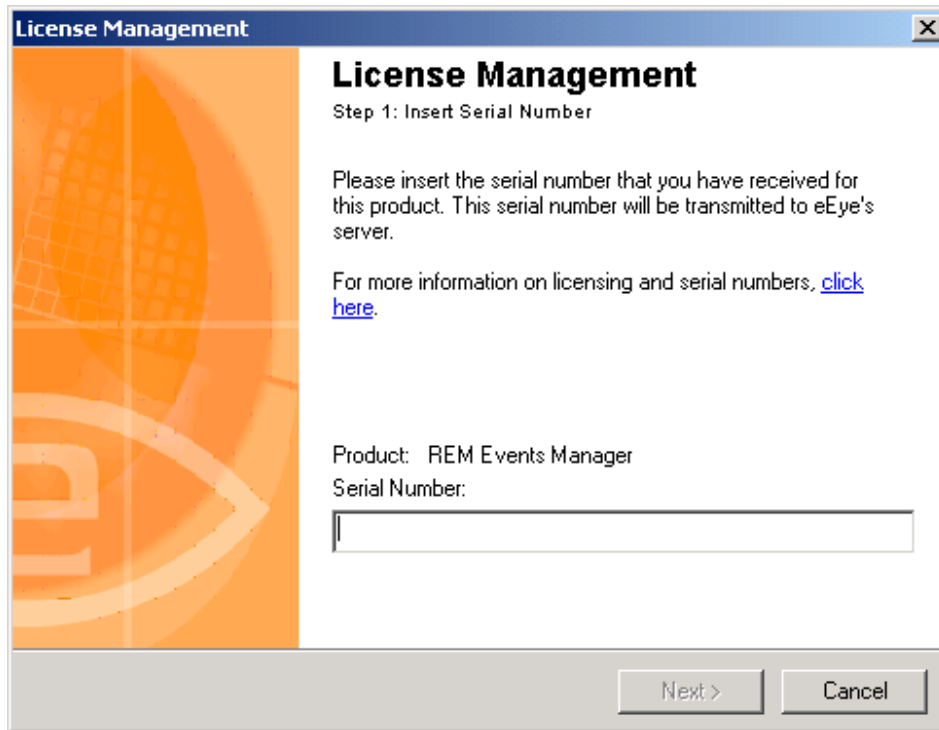
If you have a previous version of REM Events Manager on your machine, you may be prompted to remove your License during the installation. If you would like to keep the same license, make sure the check box to remove the license is not selected. Click **Next**, and then click **Finish**.

6. Once all the necessary files are copied to your computer, the *Installation Complete* screen displays. Click **Finish** to exit the installation. If it is necessary to reboot the machine to complete the installation, you will be prompted to do so.

Licensing

Follow these instructions to license REM Events Manager:

1. At the end of the installation, you will be prompted for a serial number. Type the serial number that you received for REM Events Manager. If you are reinstalling REM Events Manager on a machine that already has a valid serial number, you will not be prompted to re-enter it.



License Management screen

2. After you have entered the serial number, click **Next** to activate the license.

Configuration

Follow these instructions to configure REM Events Manager:

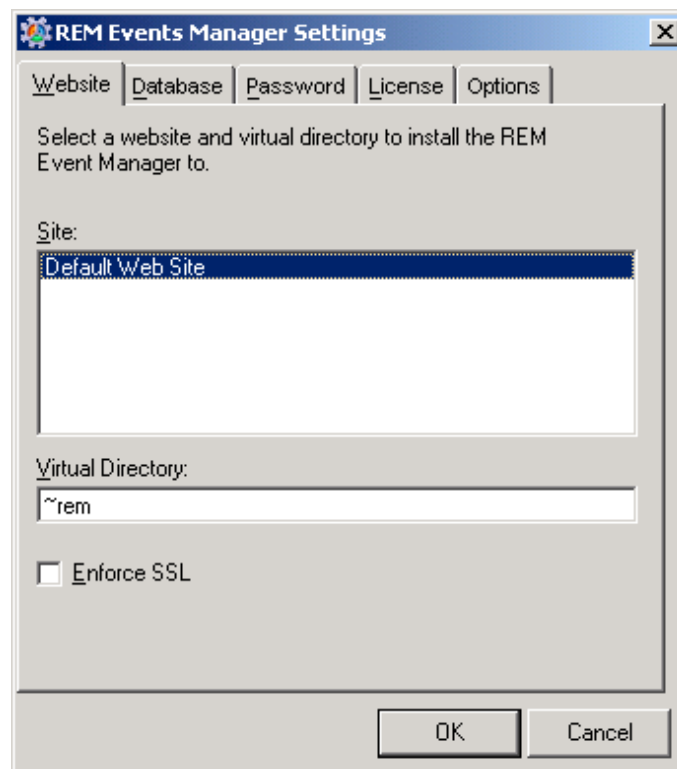
1. After you have completed licensing, the *REM Events Manager* dialog box opens. You are now ready to configure the REM Events Manager.



If the program does not launch automatically, it can be started by doing the following:

Start > Programs > eEye Digital Security > REM Events Manager > Configuration

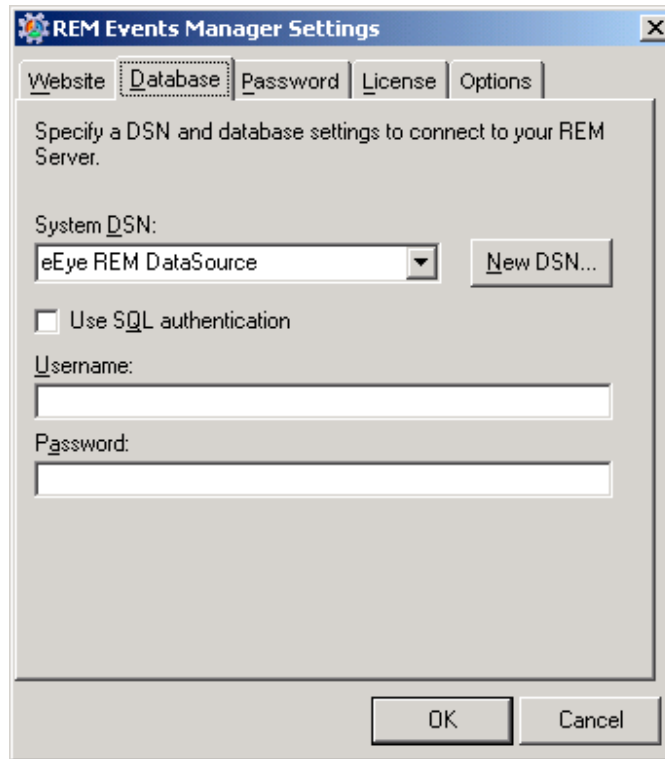
If you performed this installation by upgrading a previous version of REM Events Manager, the settings will default to the previous configuration.



Configuring REM Events Manager

2. In the *Site* list box, select a web site to be used to host the REM Events Manager. This list contains all web sites configured on your machine. The *Default* web site is selected by default.
3. Type a virtual directory name for your REM Events Manager files. The default name is `~rem`.
4. If the web server is configured to take advantage of SSL, the secure HTTPS protocol, enable **Enforce SSL**. Should a web server certificate be installed and the option not checked, after clicking **OK**, the configuration utility will prompt you that an SSL certificate has been detected and ask if you would like to enforce it.

- Click the *Database* tab.



Specifying the system DSN

- Select the name of a System DSN that points to the REM database. The System DSN created by the REM Events Server configuration wizard will be selected by default. If you do not already have a DSN, then you need to create one by clicking the **New DSN** button and following the wizard.
- Type and confirm a password for the *Administrator* account. This password will be used to access the REM Events Manager web interface.



By default the password is set to blank and can be saved as such; however, after logging into the Events Manager web interface for the first time, the *Administrator* will be prompted immediately to supply a new password.

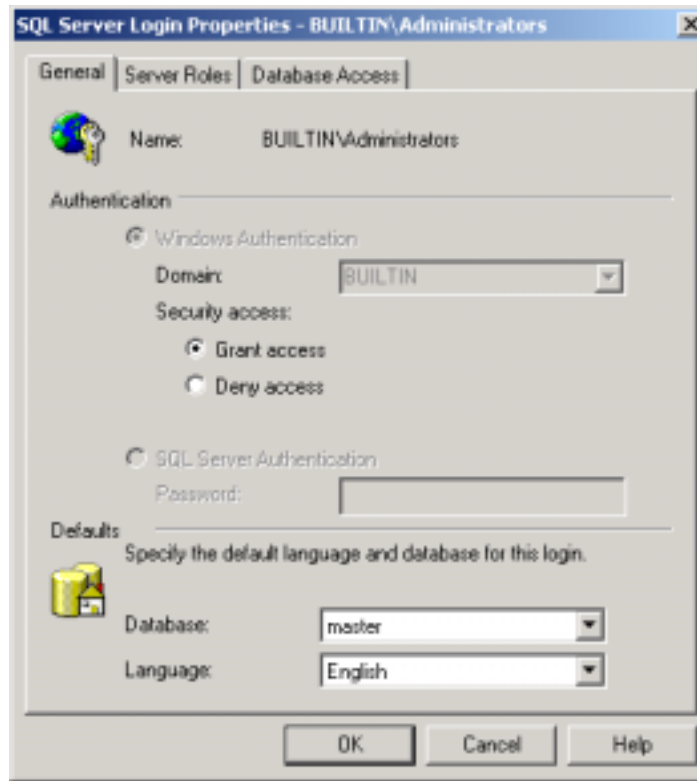
- Click **OK** to exit.

Configuring REM Events Server SQL Security

If the REM Events Manager is configured to use a NT Authentication DSN, then the IIS process user must be given permissions to the database in order to work with the REM Events Manager. In order for NT Authentication to work, REM Events Server must be installed on the same machine as the database.

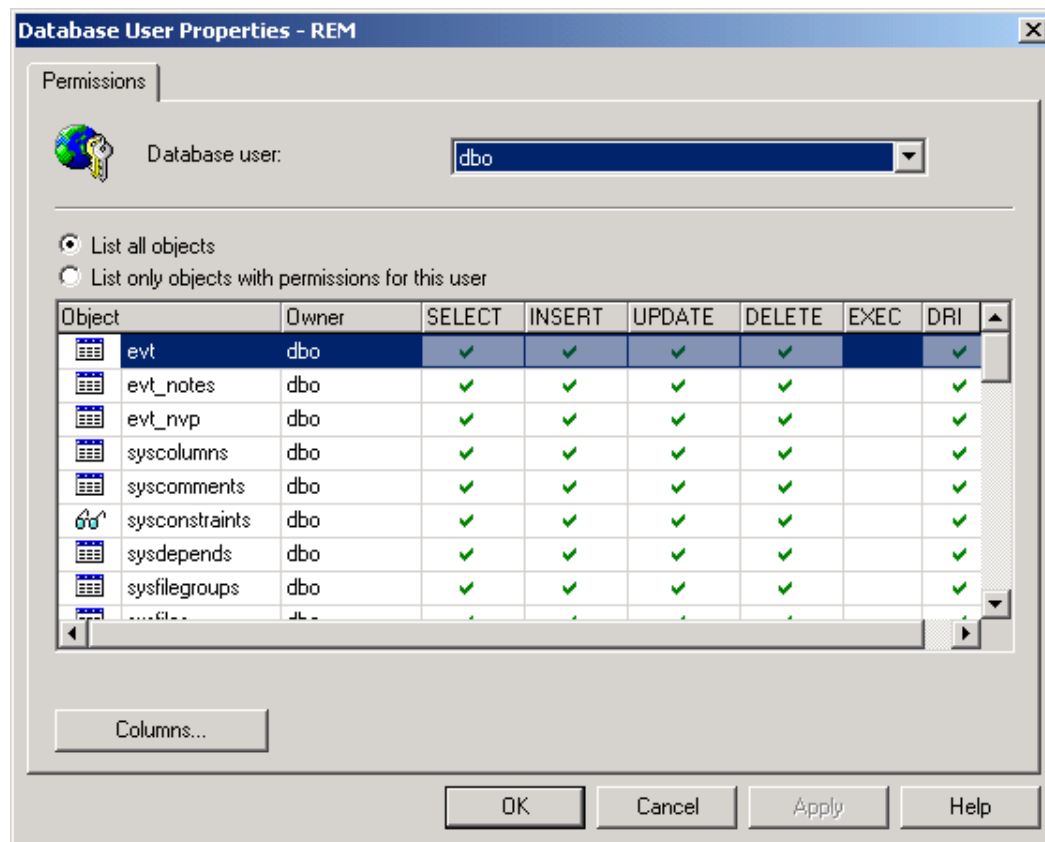
- Open the SQL Enterprise Manager.
- Under *Console Root*, go to *Microsoft SQL Servers > SQL Server Group > (local) (Windows NT) > Security > Logins*.
- Right-click the desired user, and then click **Properties**. If the user does not already exist in the list, right-click and select **New Login**.

- The *SQL Server Login Properties* dialog box opens. Specify *Windows Authentication*. In the *Database* drop-down box, choose the name for the REM database.



- Click the *Database Access* tab, and then click the desired user.
- Provide the user access to the REM database with *public* role rights. Click **OK** to create the user. The main screen displays.
- In the left pane under *Databases*, select the REM database, and then select *Users*. Right-click on the user that was just created, and then click **Properties**.

- Click the **Permissions** button. Make sure the *Select*, *Insert*, *Update*, and *Delete* columns for the *evt*, *evt_notes*, and *evt_nvp* rows are checked. If they are not, click them to enable those permissions, click **Apply**, and then click **OK**.



Setting permissions

- Close the SQL Server Enterprise Manager. Your REM database has now been created, and is now ready for the REM Events Server.

Accessing the REM Events Manager

Follow these steps to access the REM Events Manager web interface:

- Open Microsoft Internet Explorer 5.0 (or later), and navigate to `http://myserver/~rem`; if SSL is enabled, instead navigate to `https://myserver/~rem` to take advantage of the secure protocol. Replace *myserver* with the name of the machine hosting REM Events Manager, also substitute */~rem* with the value you entered for the virtual directory during configuration.
- When the *REM Events Manager login* screen displays, type *Administrator* for the user name, and then type the password that you specified during configuration.



Available from the login screen is the version of the product. However, relevant for our support team, is the specific build number can be obtained by viewing the web interface source code available from within the browser. For Internet Explorer, in the File Menu navigate to **View -> Source**. At the top of the display you will see a tag beginning: `<!-- version.` The final digits in the dotted notation that follows denotes the specific build number.

REM Database Maintenance Utility

This utility is provided to help the database administrator to maintain optimum performance in managing events. The operations available include purging events and re-indexing the database.

1. Open the REM Database Maintenance Utility available from
Start -> Programs -> eEye Digital Security -> REM Events Manager -> Clean Events Database.
2. The following options are available:
 - **Delete All Events** check box — purges all entries that match the severity filter.
 - **Delete events older than** check box — purges any entries that match both the number of days specified and the severity filter
 - **Re-index database** check box — updates the database indexes which are used to optimize the access time to the tables

