

# Vocera Alarm Analytics Configuration Guide

Version 2.2.4



# Notice

---

Copyright © 2002-2018 Vocera Communications, Inc. All rights reserved.

Vocera® is a registered trademark of Vocera Communications, Inc.

This software is licensed, not sold, by Vocera Communications, Inc. ("Vocera"). The reference text of the license governing this software can be found at <http://www.vocera.com/legal/>. The version legally binding on you (which includes limitations of warranty, limitations of remedy and liability, and other provisions) is as agreed between Vocera and the reseller from whom your system was acquired and is available from that reseller.

Certain portions of Vocera's product are derived from software licensed by the third parties as described at <http://www.vocera.com/legal/>.

Microsoft®, Windows®, Windows Server®, Internet Explorer®, Excel®, and Active Directory® are registered trademarks of Microsoft Corporation in the United States and other countries.

Java® is a registered trademark of Oracle Corporation and/or its affiliates.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owner/s. All other brands and/or product names are the trademarks (or registered trademarks) and property of their respective owner/s.

Vocera Communications, Inc.

[www.vocera.com](http://www.vocera.com)

tel :: +1 408 882 5100

fax :: +1 408 882 5101

**Last modified:** 2018-11-27 07:49

VAM-225-Docs build 26



# Contents

---

<b>About Vocera Alarm Analytics.....</b>	<b>4</b>
<b>Prerequisites.....</b>	<b>5</b>
Software and Server Prerequisites.....	5
Verifying the SQL Username and Password.....	5
Verifying the SQL Driver.....	5
Verifying Database Privileges.....	5
Verifying the Features Installed in IIS 7.....	7
Verifying .NET Framework 4.5.....	8
Verifying IIS Operation.....	8
Verifying ASP.NET.....	9
Additional Server Requirements.....	10
<b>Installation.....</b>	<b>11</b>
<b>SSL Configuration for Analytics.....</b>	<b>15</b>
<b>Configuring Vocera Alarm Analytics.....</b>	<b>16</b>
Logging into the Configuration Screen.....	16
Configuring the Servers.....	16
Configuring the Alarm Colors.....	17
Configuring the Outset Values.....	18
Logging out of the Configuration Screen.....	18
<b>Shutdown and Disaster Recovery.....</b>	<b>19</b>
Prerequisites.....	19
Shutdown.....	19
Steps for Backup.....	20
Backing up the SQL Server Database.....	20
Backing Up Components.....	22
Restoring and Verification.....	23
Remarks.....	26
<b>Technical Information.....</b>	<b>27</b>
Vocera Analytics Service.....	27
Vocera Dashboard Rest API.....	27
Vocera Analytics Configuration.....	27
Vocera Admin Rest API.....	27
Analytics Database.....	27
<b>Appendix A: Installed Services.....</b>	<b>28</b>

## About Vocera Alarm Analytics

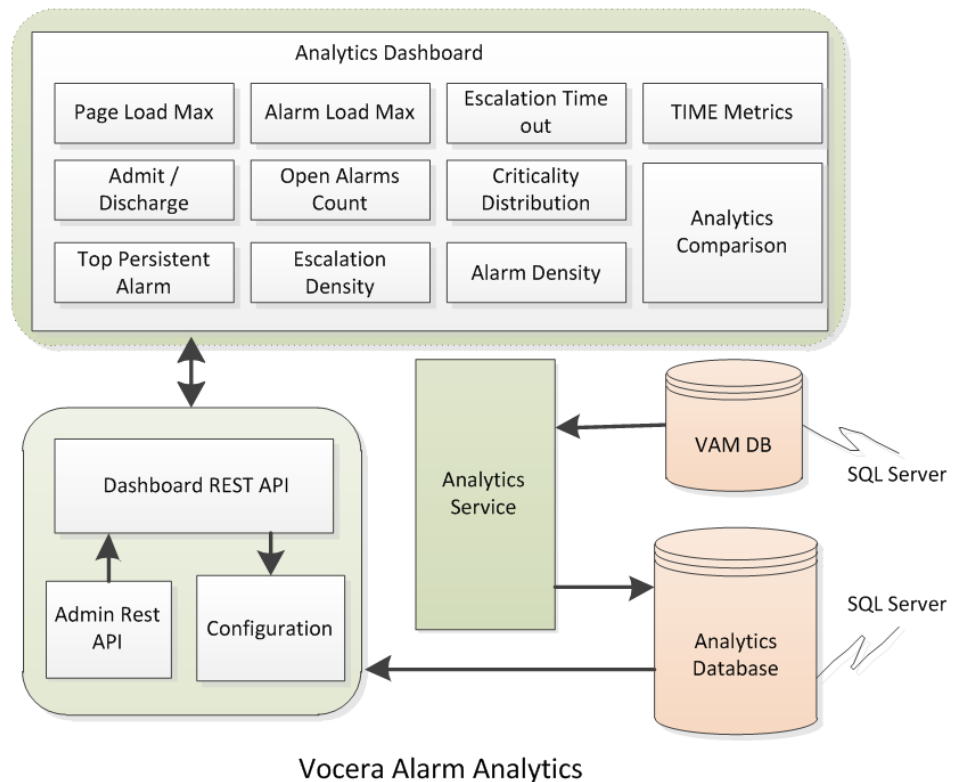
Vocera Alarm Analytics is a tool that works in conjunction with the Vocera Alarm Management system, providing hospitals with the evidence needed to improve their alarm management strategy.

Vocera Alarm Analytics:

- Allows refinement of alarm filtering and escalation
- Allows monitoring and measurement of clinical workflow effectiveness
- Provides a real-time dashboard to monitor operations against benchmarks
- Provides data aggregation and reporting to support safety, regulatory, and quality requirements

When Vocera Alarm Management is optimized with the Vocera Alarm Analytics solution, the number of alarms that will be sent to each nurse can be drastically reduced, reducing alarm fatigue, increasing patient safety and satisfaction, and improving care team efficiency.

The diagram shown here displays the Vocera Alarm Analytics architecture.





## Prerequisites

---

These sections describe the prerequisites required to install Vocera Alarm Analytics.

---

### Software and Server Prerequisites

The following software and servers must be in place before you can install Vocera Alarm Analytics.

- Microsoft SQL Server 2008 R2 and above
  - IIS 7 or above
  - Microsoft .NET Framework 3.5 and 4.5
  - MS SQL CMD and ODBC driver. This needs to be installed when the SQL server database is in a different server.
- 

### Verifying the SQL Username and Password

To verify the SQL username and password, log into the SQL server from the SQL Server Management Studio.

If needed, create a new user with the relevant roles and verify whether this user is able to log in. This new user may need to change the password on the first login, which may create problems.

Ensure that the password is not expired or disabled.

---

### Verifying the SQL Driver

To verify that you have the correct SQL driver, type `sqlcmd -?` in the Command Prompt window.

This displays the following result:

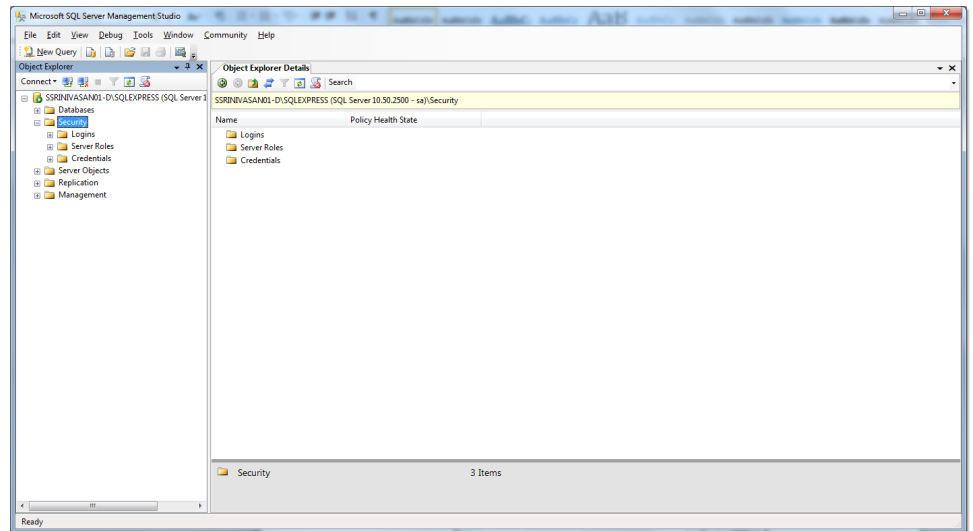
```
C:\>sqlcmd -?  
Microsoft (R) SQL Server Command Line Tool  
Version 11.0.2100.60 NT x64  
Copyright (c) 2012 Microsoft. All rights reserved.
```

---

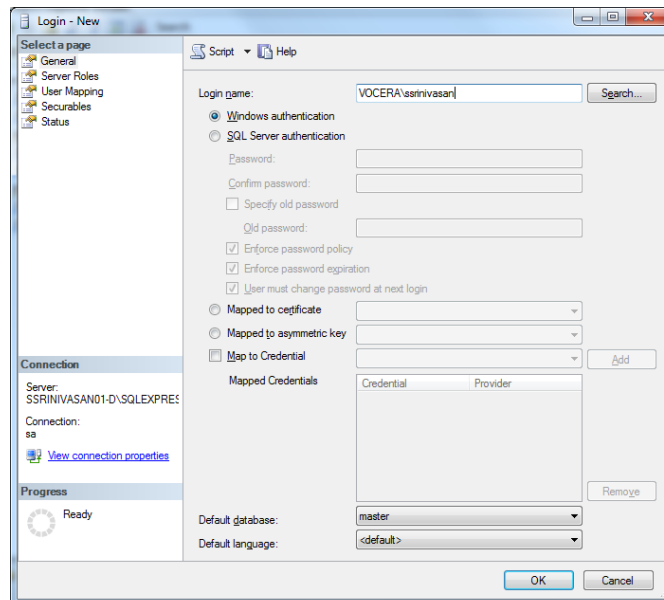
### Verifying Database Privileges

Follow these steps to verify the database privileges in the SQL Server.

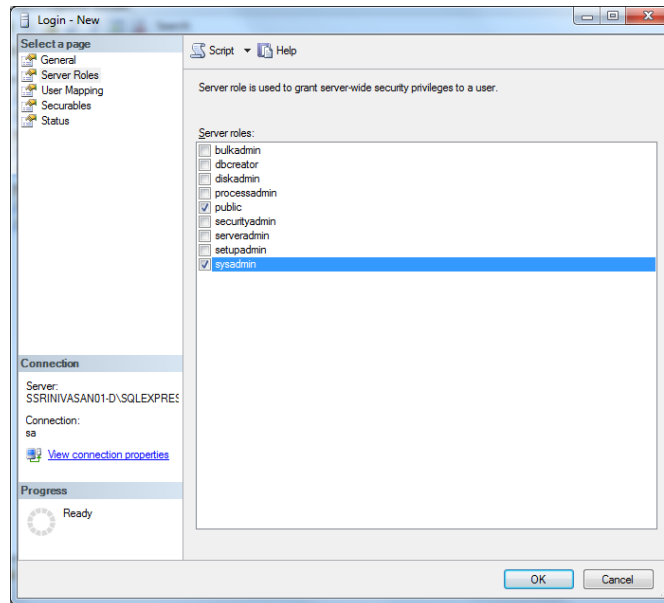
1. Log into the SQL Server with valid credentials.
2. In Object Explorer, expand Security and Logins.



3. If you have previously set up a user with the necessary database privileges:
  - a. Right-click on the user's name and select Properties.
  - b. Select Server Roles.
  - c. Ensure that public and sysadmin have been selected.
4. If you need to set up a user with database privileges:
  - a. Right-click Logins > New Login.
  - b. Type the login name of the user that is to be granted database privileges. Select the Windows authentication radio button.



- c. In the left pane, select Server Roles. Select the checkboxes as shown below, and click OK.



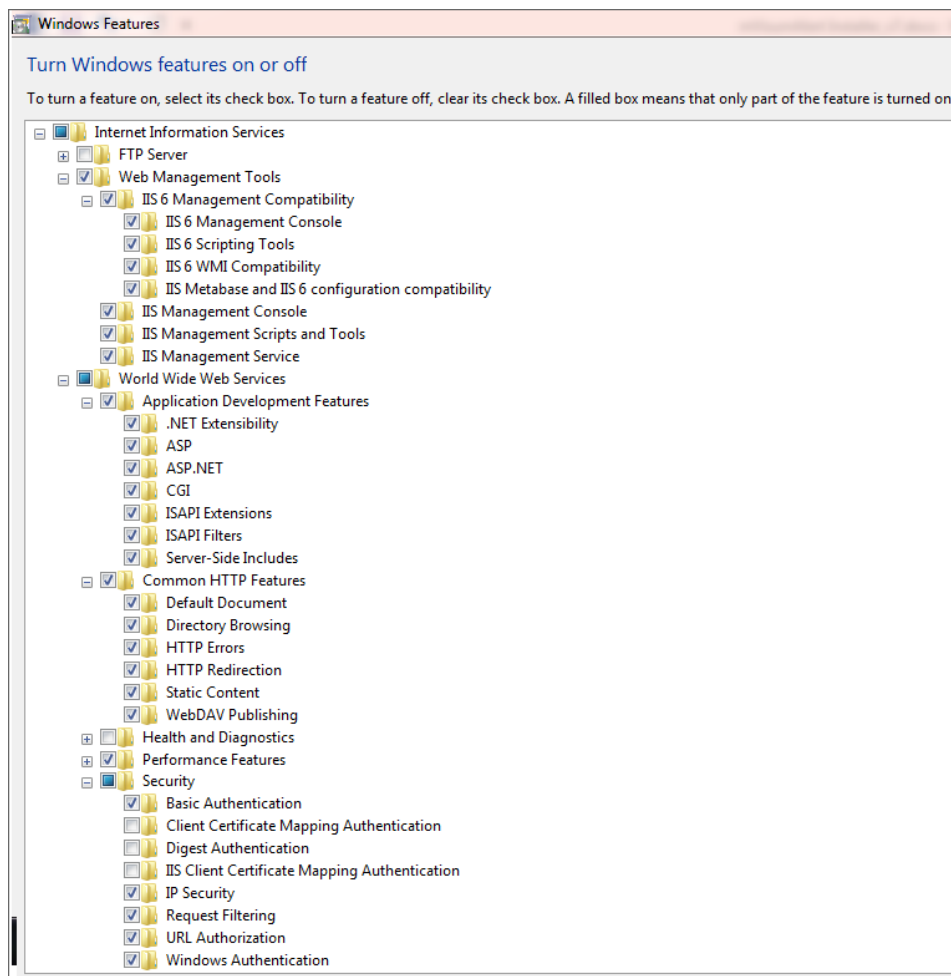
## Verifying the Features Installed in IIS 7

Follow these steps to verify that the IIS 7 feature installation is correct.



**Note:** IIS 7 is a prerequisite for Vocera Alarm Analytics.

1. Start the Microsoft Windows Control Panel.
2. Select Programs and Features.
3. Select Turn Windows features on or off.
4. Verify that the following features are selected.



## Verifying .NET Framework 4.5

If .NET Framework 4.5 is installed after IIS has been set up, you must register ASP.NET separately.

To register ASP.NET, use one of the following commands, depending on your Windows operating system:

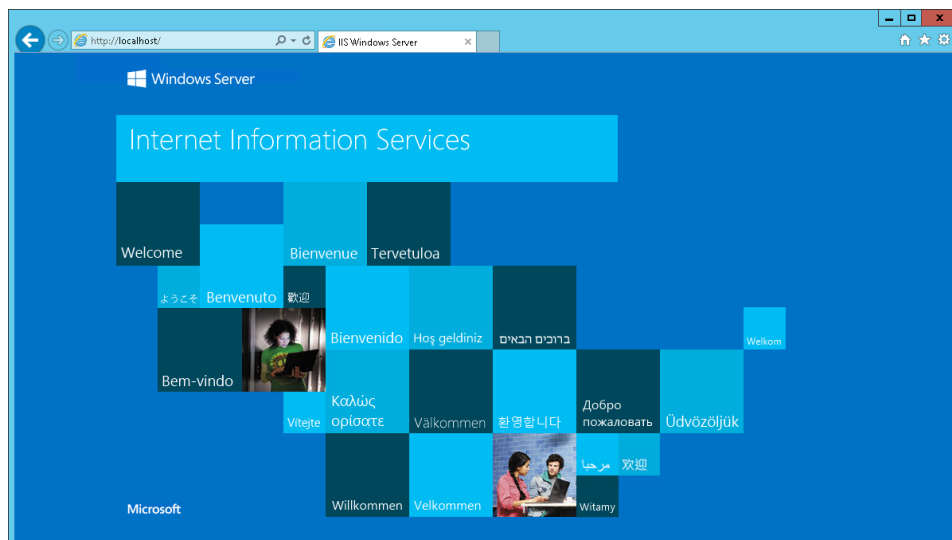
```
command%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe /i
command%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe /i
```

## Verifying IIS Operation

To verify that IIS is working, type `http://localhost` in your browser.

If IIS is working properly, the IIS page is displayed:





In the `C:\Windows\Microsoft.NET\Framework64` folder, ensure that subfolders are defined for v2.0 and v4.0. These subfolder names may include more complete version information that includes the build number - for example, v2.0 may be indicated by the folder name `v2.0.50727`.

## Verifying ASP.NET

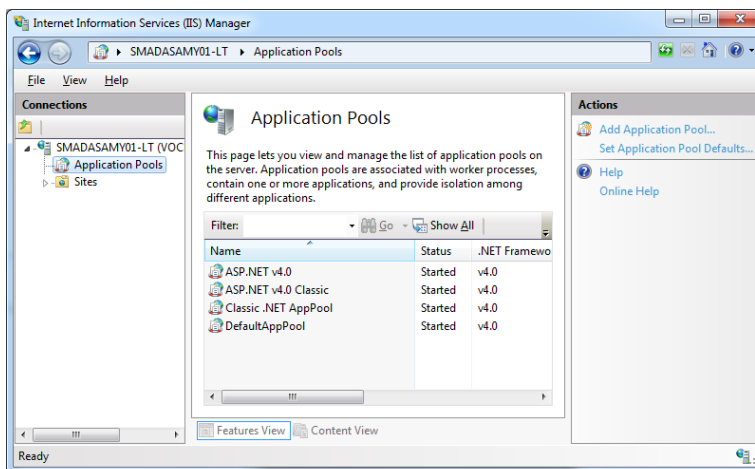
Follow these steps to ensure that ASP.NET is working properly.

First, in the Windows registry, search for the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InetStp\Components` registry key. This is the IIS Setup key that contains the components that have been enabled in IIS.

- Click the Windows Start key and click Run. In the Run window, type `regedit.exe` and click OK. This displays the Windows registry.
- Locate the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InetStp\Components` registry key.
- If you are using ASP.NET 4.5, ensure that `ASPNET45` and `NetFxExtensibility45` have been set to 1.
- If you are using an older version, ensure that `ASPNET`, `NetFxEnvironment`, and `NetFxExtensibility` have been set to 1.

Next, check whether the current .NET Framework version is 4.0. To do this on Windows Server 2008:

- Go to IIS Manager.  
Click Start > Administrative Tools > Internet Information Services (IIS) Manager.
- Click on the name of your server to display the Actions Panel.  
If a dialog box appears asking you whether you want to get started with Microsoft Web Platform, click No.
- In the Actions Panel, click `Change .NET Framework Version`. A dialog box appears, displaying the version of .NET Framework that is currently in use.
- Verify that the version starts with 4.0, and click OK to close the dialog box.
- In the Actions Panel, click `View Application Pools` to check whether the application pools .NET Framework version is 4.0:



- If you can't find ASP.NET or .NET, open a Command Prompt window in administrator mode and run the following command from the folder in which you have installed .NET Framework:  
`C:\Windows\Microsoft.NET\Framework\v4.0.30319>aspnet_regiis -I`  
 Replace `v4.0.30319` with your version of .NET Framework. Restart your server after completing this command.

If you are using Windows Server 2012, see [IIS 8.0 Using ASP.NET 3.5 and ASP.NET 4.5](#) for details on how to verify that .NET Framework 4.0 is installed on your server.

## Additional Server Requirements

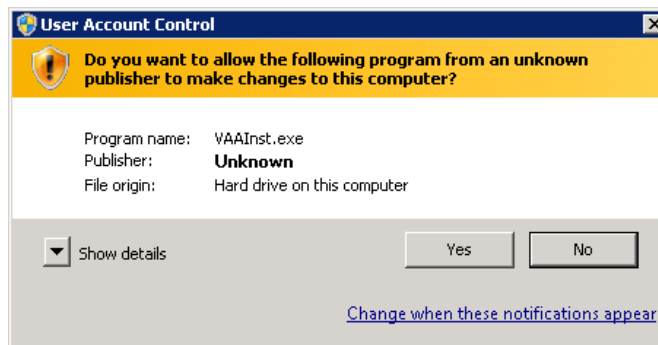
To install Vocera Alarm Analytics, your server must meet the additional requirements shown here.

- The time zone of the Vocera Alarm Analytics server must match that of the Vocera Alarm Management server that it is analyzing. If you must change the time zone, you must restart the server.
- The Vocera Alarm Analytics server must have a static IP Address.

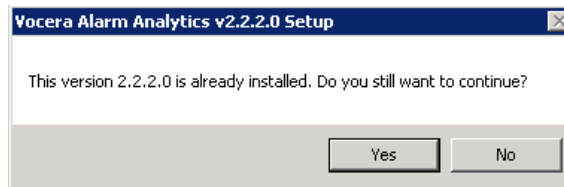
## Installation

Follow these steps to install Vocera Alarm Analytics.

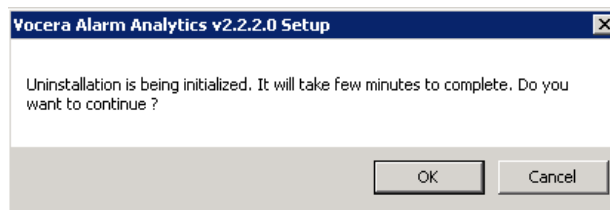
1. Double-click the `VoceraAnalytics.exe` installation file to launch the installer.
2. In the Access Control dialog box, click Yes.



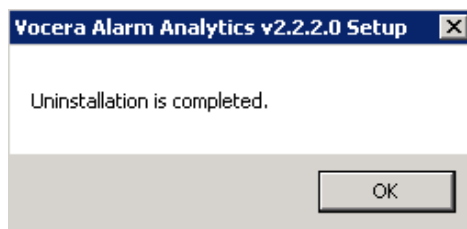
3. If Vocera Alarm Analytics is already installed, the screen shown below appears. Click Yes.



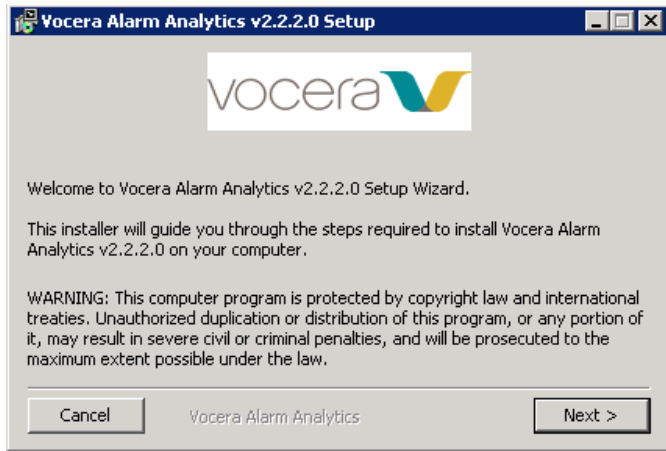
4. Click OK.



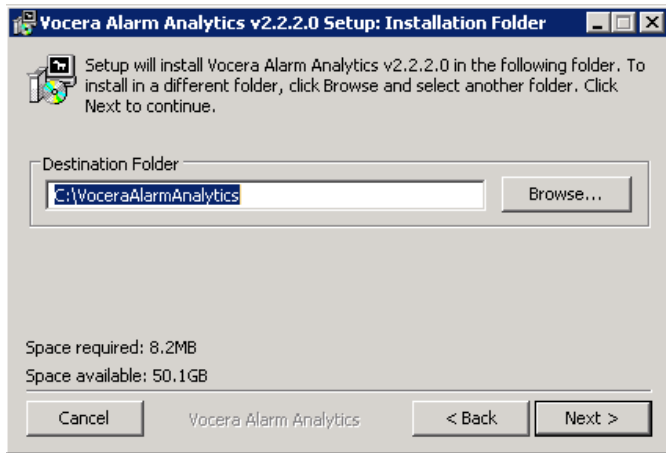
5. Wait for the uninstallation process to complete. This happens in the background. When the screen shown below appears, click OK.



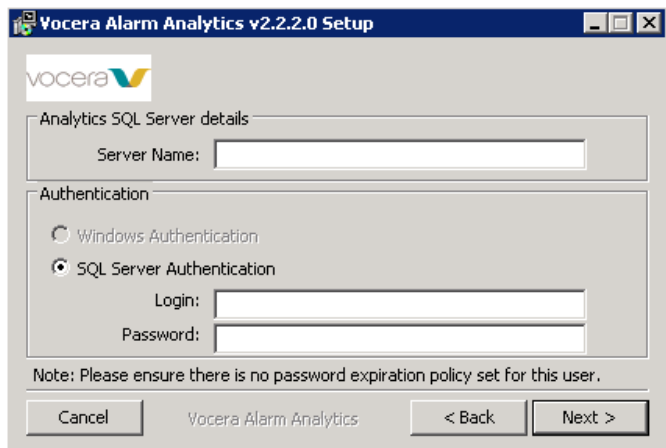
6. Click Next.



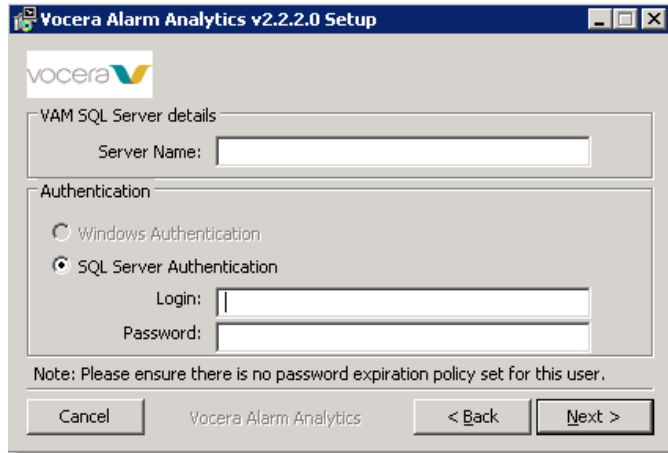
- Specify the installation directory. The default installation directory is C:\VoceraAlarmAnalytics. You can use the file browser to select another directory. Click Next.



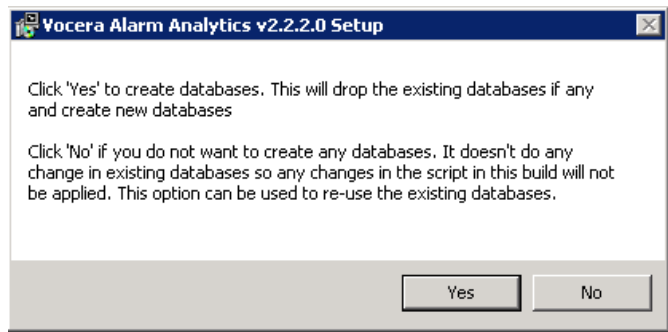
- Specify the server name and authentication credentials for the Analytics SQL server. Click Next.



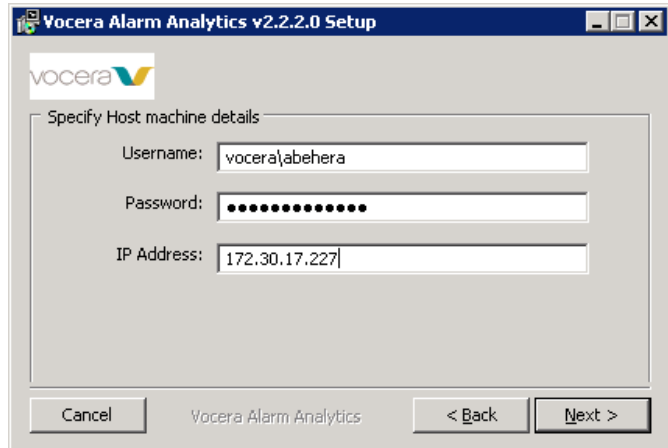
- Specify the server name and authentication credentials for the VAM SQL server. Click Next.



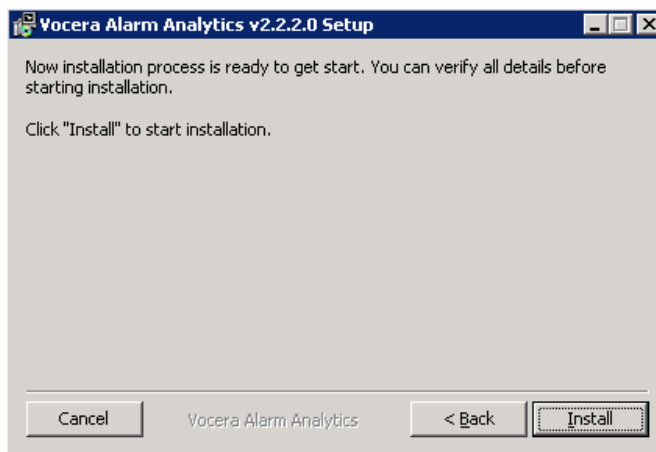
10. Click Yes to create the databases. This erases any existing data in these databases. Click No to reuse the existing databases.



11. Provide the credentials and the static IP address for your host machine. Click Next.



12. Click Install to start the installation.



13. During installation, do not close any windows that appear.

## SSL Configuration for Analytics

---

To configure Vocera Alarm Analytics for SSL, you must change its configuration as described in these steps.



**Note:** Your IIS settings must be updated to provide SSL support.

1. In the folder in which you have installed Vocera Alarm Analytics, go to the **Vocera Analytics/VAAConfiguration** subfolder, and open the file **web.config**.
2. In the **Configuration/AppSettings** section, locate the **RestService** tag, and replace **http** with **https**. Save the file.
3. In the folder in which you have installed Vocera Alarm Analytics, go to the **Vocera Analytics/AnalyticsDashBoard** subfolder, and open the file **web.config**.
4. In the **Configuration/AppSettings** section, locate the **RestService** tag, and replace **http** with **https**. Save the file.
5. In the folder in which you have installed Vocera Alarm Analytics, go to the **Vocera Analytics/VoceraDashboardRestAPI** subfolder, and open the file **web.config**.
6. In the **Configuration/AppSettings** section, locate the **SSLEnabled** tag, and set its value to **True**.
7. In the **configuration/system.serviceModel/bindings/webHttpBinding/binding** section, change the security mode to **Transport**.
8. In the **configuration/system.serviceModel/bindings/basicHttpBinding/secureHttpBinding** section, change the security mode to **Transport**. Save the file.
9. In the folder in which you have installed Vocera Alarm Analytics, go to the **Vocera Analytics/VoceraAnalyticsAdminRestAPI** subfolder, and open the file **web.config**.
10. In the **configuration/system.serviceModel/bindings/basicHttpBinding/secureHttpBinding** section, change the security mode to **Transport**. Save the file.



## Configuring Vocera Alarm Analytics

---

You can use the configuration console to configure Vocera Alarm Analytics.

You can:

- Specify the Vocera Alarm Management servers to analyze.
- Specify the colors to use for alarm levels.
- Specify the outset values.



**Note:** After installing Vocera Alarm Analytics, you must clear your browser cache before starting configuration.

---

### Logging into the Configuration Screen

Follow these steps to log into the Vocera Alarm Analytics configuration screen.

1. In your web browser, type `http://hostname/VAAConfiguration/`, where **hostname** is the IP address or domain name of your Vocera Alarm Analytics server. The login screen appears.
2. In the `UserName` field, enter your user name. The default is `admin`.
3. In the `Password` field, enter the password for your user name. The default is `admin`.
4. Click `Login`. The list of configured Vocera Alarm Management servers appears. See [Configuring the Servers](#) on page 16 for more details on server configuration.

---

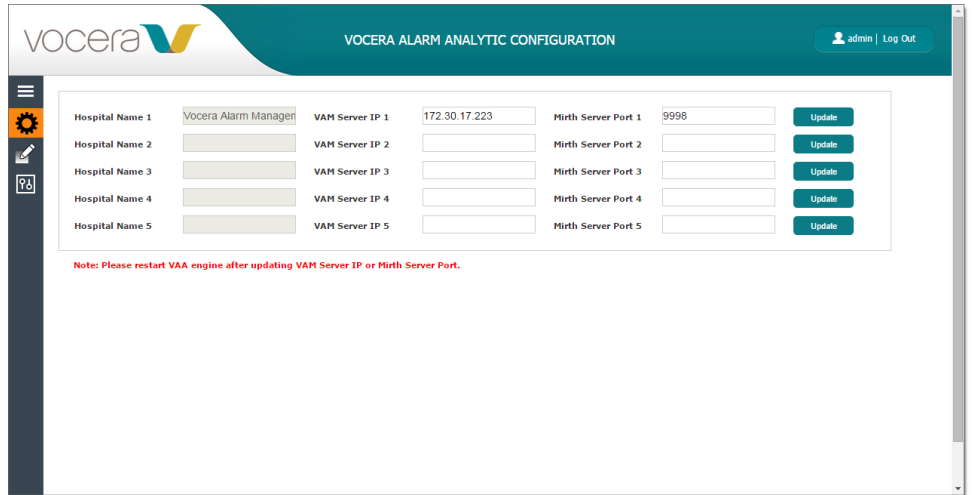
### Configuring the Servers

From the configuration screen, you can specify the Vocera Alarm Management servers that Vocera Alarm Analytics is to analyze.

To specify servers:

1. Click  to display the server pane. If this icon has an orange background, this pane is already displayed.





2. For each hospital server to be analyzed:
  - a. In the Hospital Name field, enter the name of the Vocera Alarm Management server.
  - b. In the VAM Server IP field, enter the IP address of the server.
  - c. In the Mirth Server Port field, enter the port of the Mirth server that the Vocera Alarm Management server uses. The default is 9997.
  - d. Click Update to update the server information. Each server setting is updated separately.



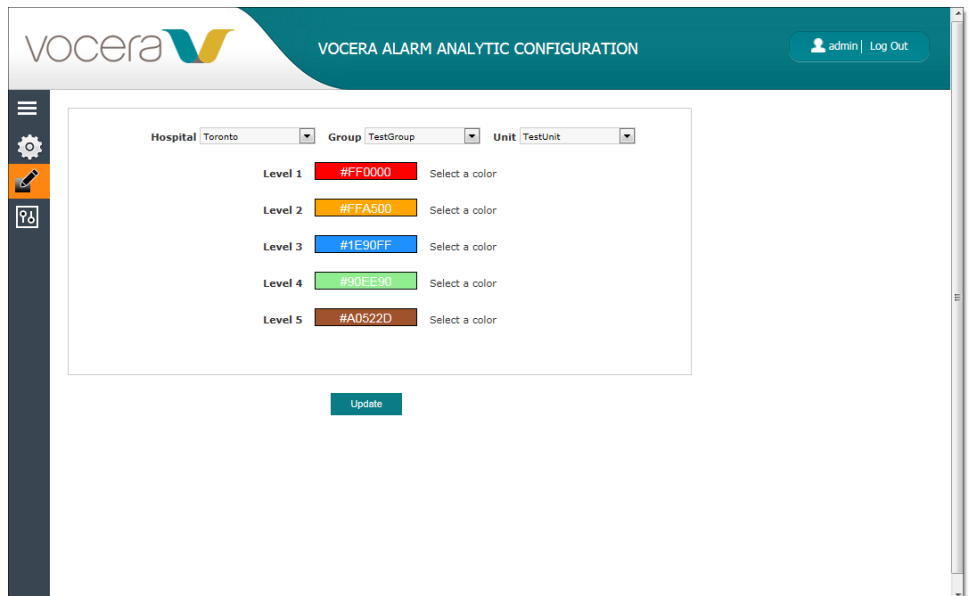
**Note:** You must restart Vocera Alarm Analytics after reconfiguring these servers.

## Configuring the Alarm Colors

From the configuration screen, you can specify the colors to use to display alarms in Vocera Alarm Analytics. These colors can be specified on a unit-specific basis.

To specify alarm colors:

1. Click  to display the color pane. If this icon has an orange background, this pane is already displayed.




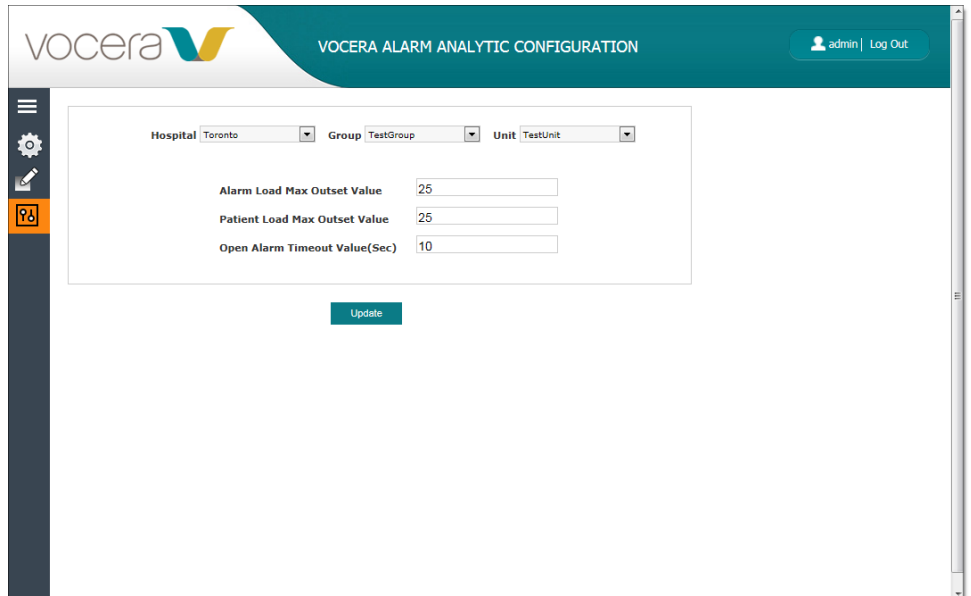
2. From the Hospital, Group, and Unit dropdown lists, select the affected hospital, group, and unit.

- To select a color for an alarm level, click its current color. In the collection of color swatches that appears, select a color. Repeat this step for other alarm levels as needed.
- Click *Update* to update the alarm colors. If the Vocera Alarm Analytics dashboard is being displayed, you must refresh the dashboard to display it in the new colors.

## Configuring the Outset Values

From the configuration screen, you can specify the maximum outset values and the open alarm timeout value.

- Click  to display the outset pane. If this icon has an orange background, this pane is already displayed.



The screenshot shows the 'VOCERA ALARM ANALYTIC CONFIGURATION' interface. At the top, there is a header with the Vocera logo and the title. On the right, it shows 'admin | Log Out'. On the left, there is a sidebar with several icons, including one with a question mark and a plus sign, which is highlighted in orange. The main content area contains three dropdown menus for 'Hospital' (Toronto), 'Group' (TestGroup), and 'Unit' (TestUnit). Below these are three input fields: 'Alarm Load Max Outset Value' with the value 25, 'Patient Load Max Outset Value' with the value 25, and 'Open Alarm Timeout Value(Sec)' with the value 10. At the bottom center, there is a blue 'Update' button.

- In the *Alarm Load Max Outset Value* field, specify the threshold value for the number of alarms for a nurse. If the number crosses this threshold, the nurse is included in the *Alarm Load Max* pane in the dashboard.
- In the *Patient Load Max Outset Value* field, specify the threshold value for the number of alarms for a patient. If the number crosses this threshold, the patient is included in the *Patient Load Max* pane in the dashboard.
- In the *Open Alarm Timeout Value*, specify the number of seconds before an alarm is considered open. Open alarms are included in the *Open Alarms Counts* pane in the dashboard.
- Click *Update* to update the outset values.

## Logging out of the Configuration Screen

To log out of the Configuration Screen, click the *Log Out* button, which is located at the top right of the screen.

# Shutdown and Disaster Recovery

Learn how to shut down the Vocera Alarm Analytics application server and how to perform a back up and restore. These processes can help with disaster recovery.

## Prerequisites

The following prerequisites must be in place before backup.

- Vocera Alarm Analytics must have been installed, and must be up and running.
- The necessary systems and software must have been installed to enable restoring and verification of Vocera Alarm Analytics.

The following table lists the Vocera Alarm Analytics prerequisites.

Hardware	Software
Intel Xeon Dual-Core or equivalent	Windows 2008 R2 and above
8 GB RAM	Microsoft SQL Server 2008 R2 and above
500 GB HDD	IIS 7 or above
	.NET framework 3.5, 4.5

## Shutdown

Vocera Alarm Analytics includes one Windows service and several web services for communicating with different devices and applications. Follow these steps to shut down these services and the Vocera Alarm Analytics application server.



**Note:** You must shut down or log out from all VAA dashboard or Analytics configuration websites that are connected to the Vocera Alarm Analytics application server before shutting it down. If you do not do this, the current operations in the browsers will be terminated abruptly and users will be logged out. The Windows service that must be stopped is Vocera Analytics Service.

The simplest shutdown procedure is the following:

- The easiest way to shut down the Vocera Alarm Analytics application is to shut down the application and database servers by powering off the systems (unless other services are being used).
- The easiest way to restart the Vocera Alarm Analytics application is to restart the application and database servers (unless other services are being used).

If the SQL database server is restarted, the Vocera Analytics Windows service must be restarted. This is not likely to result in major issues, but a user might become logged out, or an error, exception, or web portal crash might occur, depending on the currently running operation.

If the server has to be restarted because of maintenance, such as for a Windows update, it is advisable to restart at midnight or on the weekend when the load is smaller.

## Steps for Backup

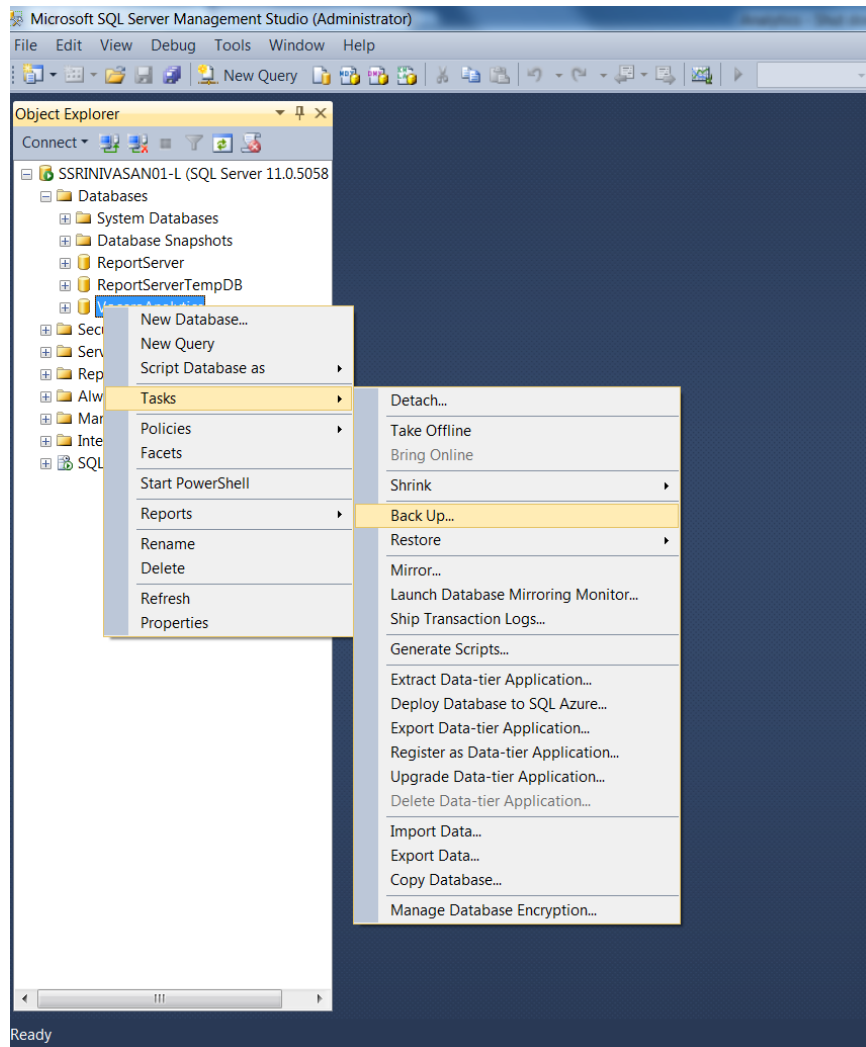
To back up Vocera Alarm Analytics, you must perform the steps shown here.

- Back up the SQL server database
- Back up the components

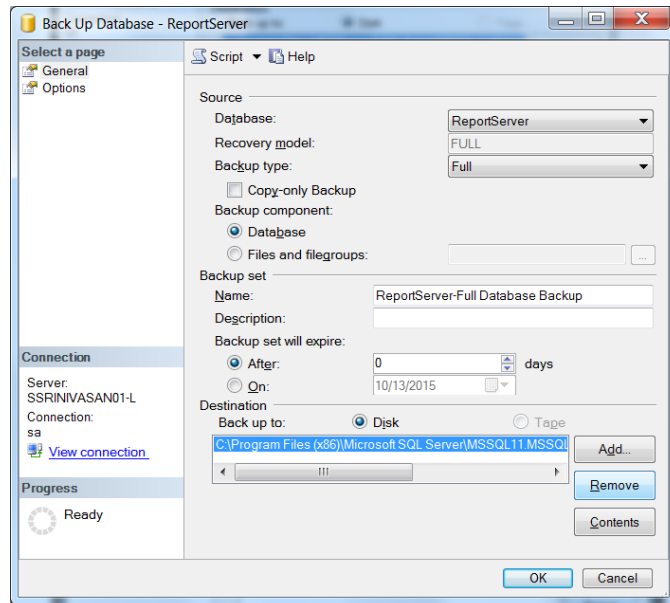
### Backing up the SQL Server Database

The following are the steps to be used to make a backup of the Vocera Alarm Analytics database so that it can be recovered if the database server crashes.

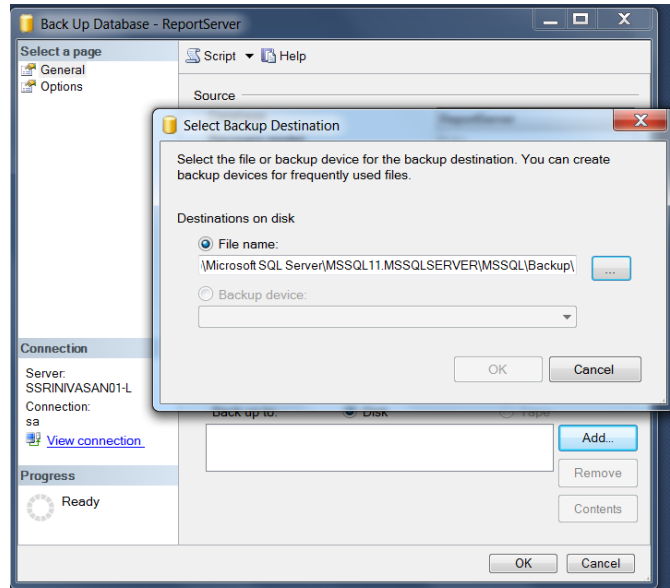
1. Launch the management console and login with valid credentials.
2. Right click on the database.
3. Go to Tasks > Back Up.



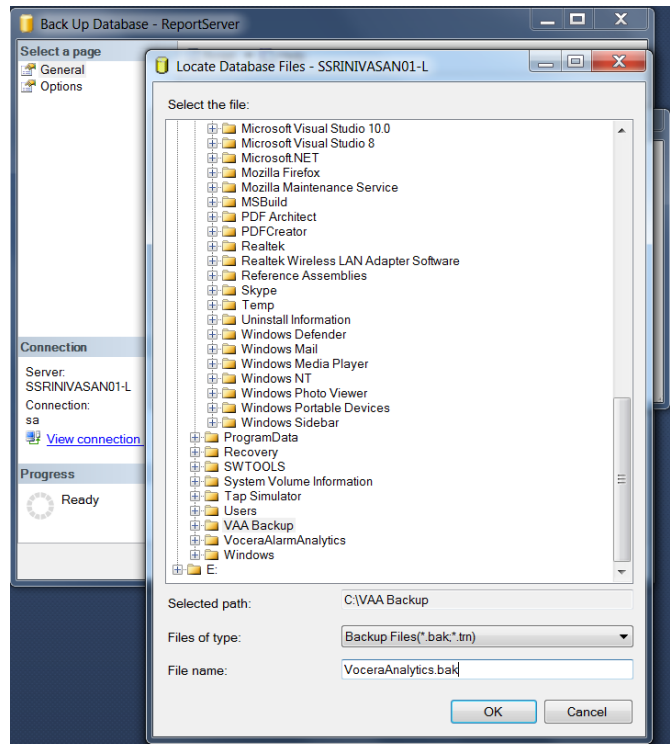
4. Remove the existing path using the Remove option and select the desired location.



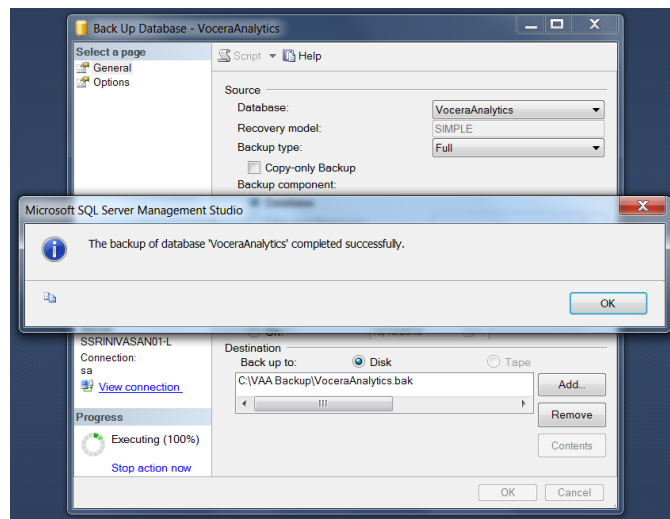
5. Click Add. The screen shown below appears. Click the Browse button .



6. Locate the desired directory and provide the name of the backup file as `[DatabaseName].bak`. For example, the name of the database backup file for the Vocera Analytics database is `VoceraAnalytics.bak`.



7. Click OK to complete the backup process. If it is successful, the message shown below is displayed.



If an error message appears, change the file path, as this might be due to a permission issue.

## Backing Up Components

Vocera recommends that you make a backup of the component configuration files.

The following are the configuration files that need to be backed up.

- [VAM Analytics Installation directory]\Vocera Analytics\AnalyticsDashBoard\web.config
- [VAM Analytics Installation directory]\Vocera Analytics\VAAConfiguration\web.config
- [VAM Analytics Installation directory]\Vocera Analytics\VoceraAnalyticsAdminRestAPI\web.config
- [VAM Analytics Installation directory]\Vocera Analytics\VoceraAnalyticsService\VoceraAnalyticsService.exe.config
- [VAM Analytics Installation directory]\Vocera Analytics\VoceraDashboardRestAPI\web.config

## Restoring and Verification

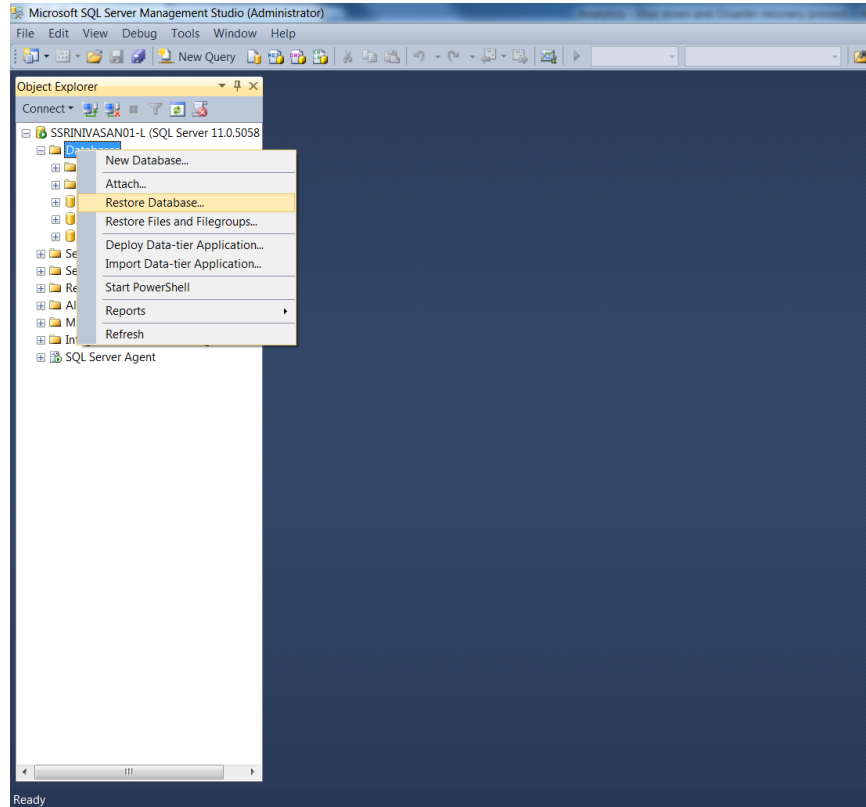
To restore Vocera Alarm Analytics, you must restore the databases that you have previously backed up.

The following are the steps to be followed to recover the VoceraAnalytics database using SQL Server Management Studio.

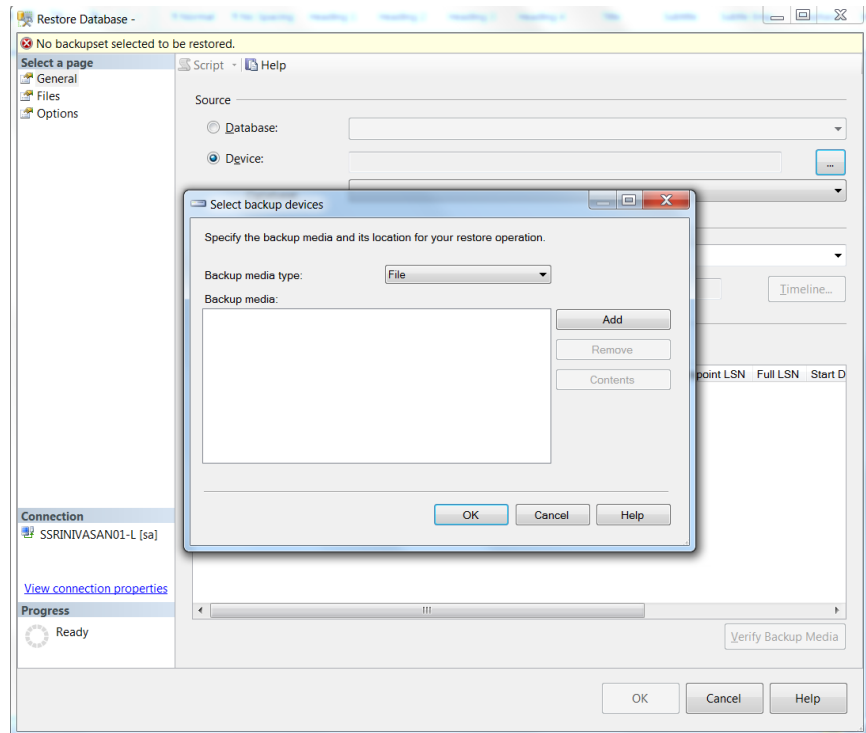
1. On the machine where Vocera Alarm Analytics is installed, stop all Vocera Alarm Analytics Windows services and IIS. To stop IIS, run following command from the Command Prompt window:

```
iisreset /stop
```

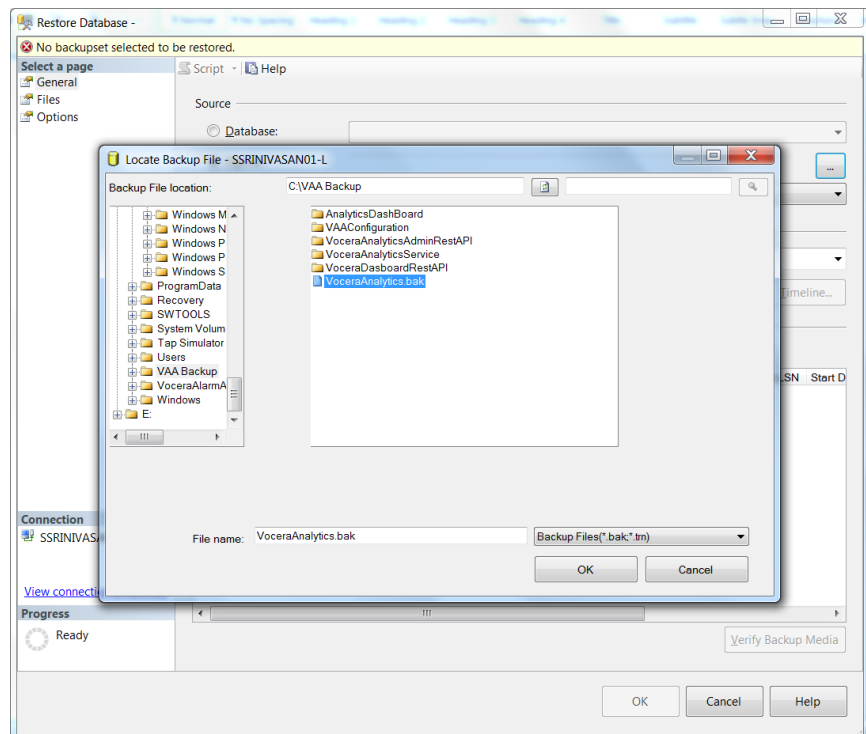
2. Right click on the database and select Restore Database.



3. Select Device. Click the Browse button to select the backup file.

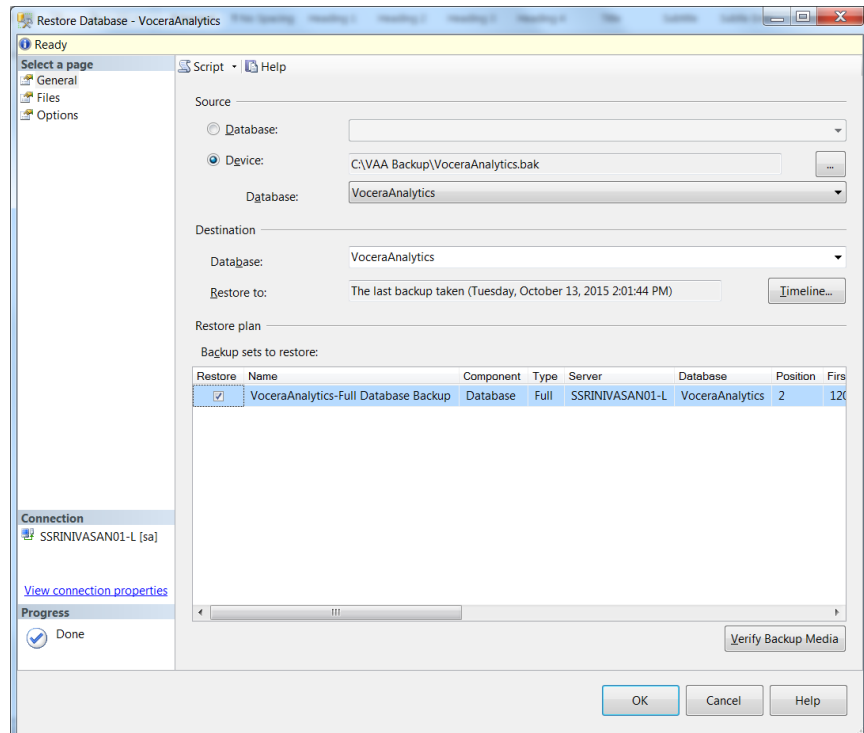


4. Click Add.
5. Locate the .bak file, which is the backup of the database that was taken from the original server.

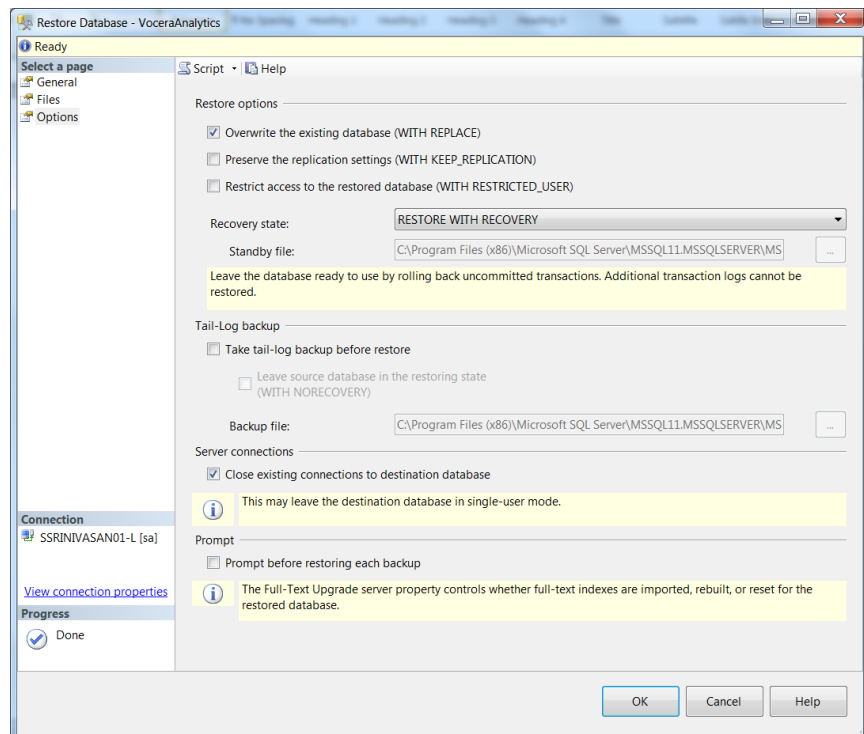


6. Click OK. Click OK.
7. Select the checkbox in the Restore column.

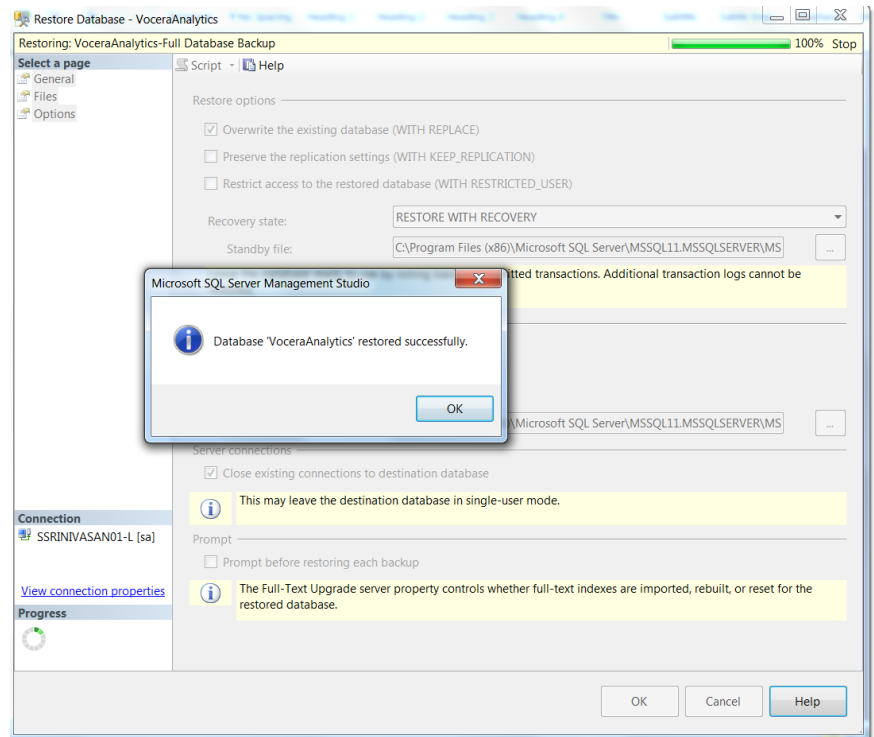




8. Go to the Options page and select Overwrite the existing database.
9. For SQL Server 2012 and above, clear Take tail-log backup before restore and select Close existing connections to destination database.



10. Click OK. If the restore operation is successful, you will see the dialog box shown below.



## Remarks

The steps for database backup and restore that are described here can be replaced with other approaches, such as replication or automatic backup using a third-party application.

Using this approach, the backup server can be set up and tested by switching off the main server and moving to the backup server.



## Technical Information

---

These sections provide technical background information on the features and capabilities of Vocera Alarm Analytics.

Vocera Alarm Analytics can be divided into the following components:

- Vocera Analytics Service
- Vocera Dashboard Rest API
- Vocera Analytics Configuration
- Vocera Admin Rest API
- Analytics Database

---

### Vocera Analytics Service

The Vocera Analytics Service is responsible for fetching the alarm data from the VAM database. It also synchronizes the alarm status, hospital settings, and group, unit, and bed information from the VAM database.

---

### Vocera Dashboard Rest API

This service is responsible for accessing data from the analytics database and providing the data to the Vocera Alarm Analytics dashboard.

This service consists of a business layer and a data access layer.

---

### Vocera Analytics Configuration

This service is responsible for the configuration of the VAM server IP address.

This service also sets the colors for each alarm level.

---

### Vocera Admin Rest API

This service is responsible for logging into and authentication to the VAM database.

Active Directory users that have been imported into the VAM database are able to log into Vocera Alarm Analytics.

---

### Analytics Database

The analytics service is responsible for inserting data into the analytics database and synchronizing it with the VAM database.

The analytics database is deployed on a SQL server.



## Appendix A: Installed Services

---

This appendix lists the services that are installed with the Vocera Alarm Analytics server.

Windows services installed with the Vocera Alarm Analytics server:

- Vocera Analytics Service

IIS services installed with the Vocera Alarm Analytics server:

- VoceraAlarmAnalytics
- VoceraDashboardRestAPI
- VoceraAnalyticsAdminRestAPI
- VAAConfiguration