

Installing SentryOne for use on AWS EC2

A user guide compiled by James Holden, Technical Training Specialist, SentryOne

As more and more businesses move their database servers to the cloud, we have seen an increase in customers interested in hosting SentryOne on and monitoring EC2 instances.

To address the growing need to provide assistance in getting monitoring up and running successfully, I put together the following step by step guide.

The guide is divided into several parts:

Part 1: Spinning up your EC2 instances

Part 2: Preparing for installation of SentryOne

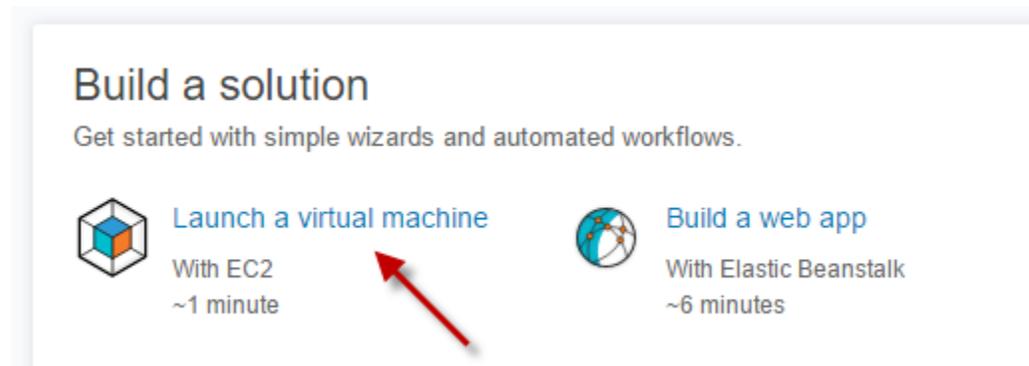
Part 3: Completing the SentryOne installation

Part 4: Successfully monitoring additional EC2 instances

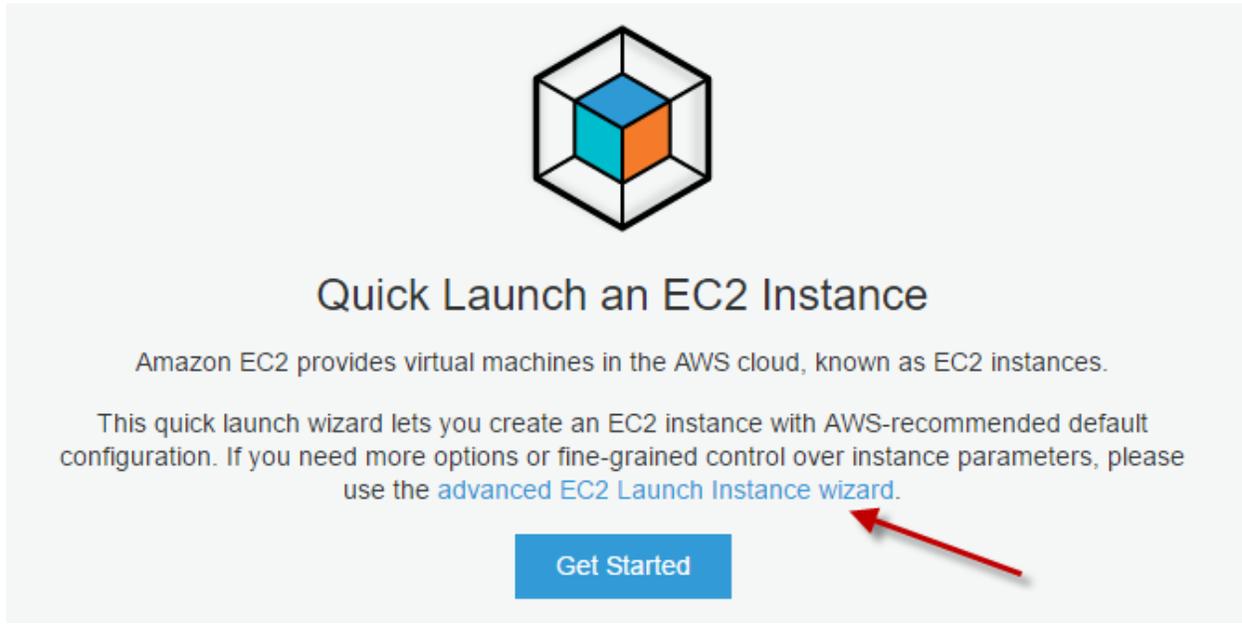
Let's begin with Part 1:

Part 1: Spin up an instance that will be hosting the SentryOne components and a target instance to monitor:

- a. Click on 'Launch a virtual machine' with EC2



- b. Click on the 'advanced EC2 Launch Instance wizard' link



Quick Launch an EC2 Instance

Amazon EC2 provides virtual machines in the AWS cloud, known as EC2 instances.

This quick launch wizard lets you create an EC2 instance with AWS-recommended default configuration. If you need more options or fine-grained control over instance parameters, please use the [advanced EC2 Launch Instance wizard](#).

[Get Started](#)

- c. Select an Amazon Machine Image (AMI)



	Microsoft Windows Server 2016 with SQL Server Standard - ami-37e16957 Microsoft Windows 2016 Datacenter edition, Microsoft SQL Server 2016 Standard, [English]	Select
---	--	------------------------

Root device type: ebs Virtualization type: hvm

- d. Select your instance type then click 'Review and Launch'

	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate
<input checked="" type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
<input type="checkbox"/>	General purpose	m4.16xlarge	64	256	EBS only	Yes	20 Gigabit
<input type="checkbox"/>	General purpose	m5.medium	4	8	EBS only	Yes	Moderate

e. Edit the security group as follows, select 'Review and Launch', and then 'Launch'

Assign a security group: Create a new security group
 Select an existing security group

Security group name:

Description:

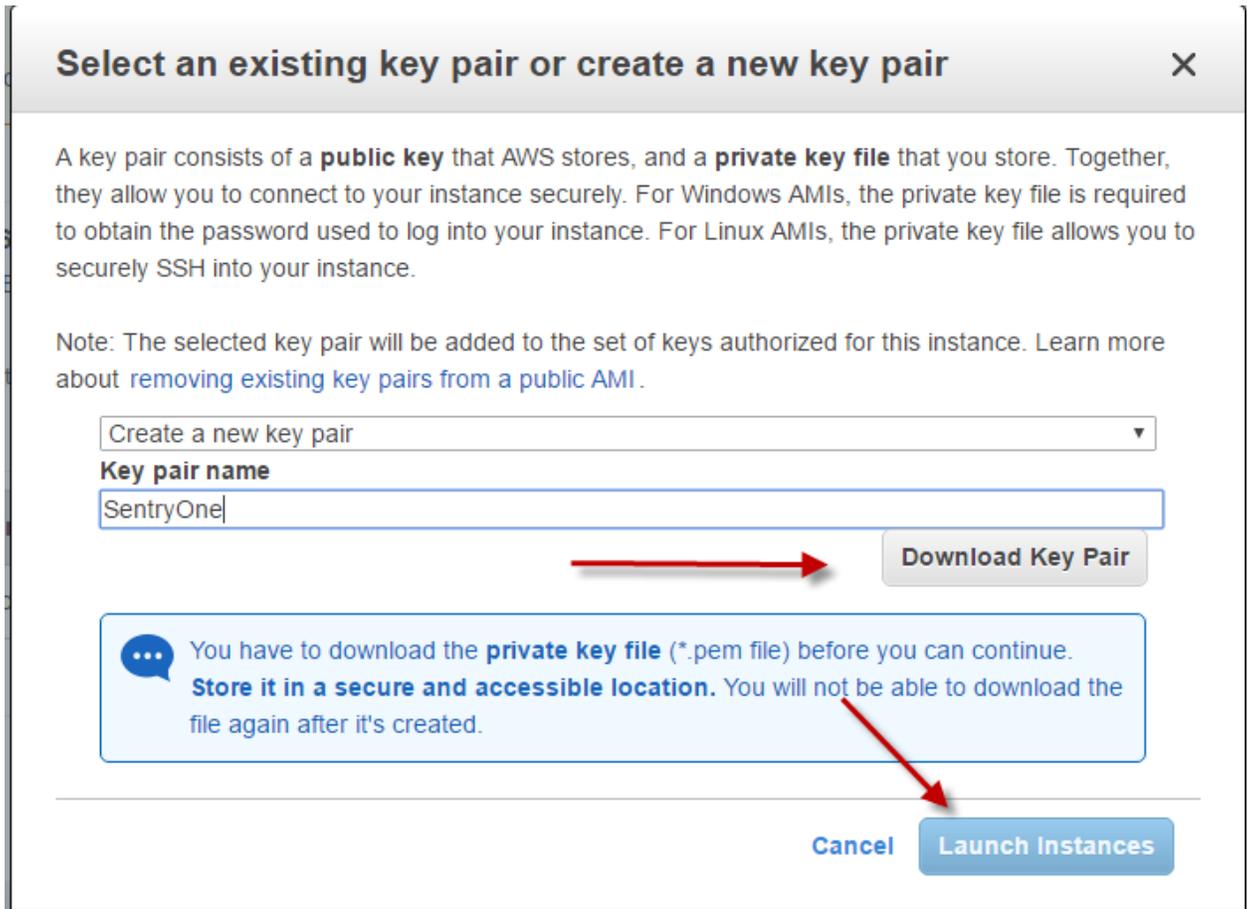
You can restrict access later

Type	Protocol	Port Range	Source
MS SQL	TCP	1433	SQL Server
RDP	TCP	3389	Remote Desktop
Custom TCP Rule	TCP	135	WMI
Custom TCP Rule	TCP	445	Windows Performance Counter Access
Custom TCP Rule	TCP	49152-65535	Dynamic Ports for use with WMI

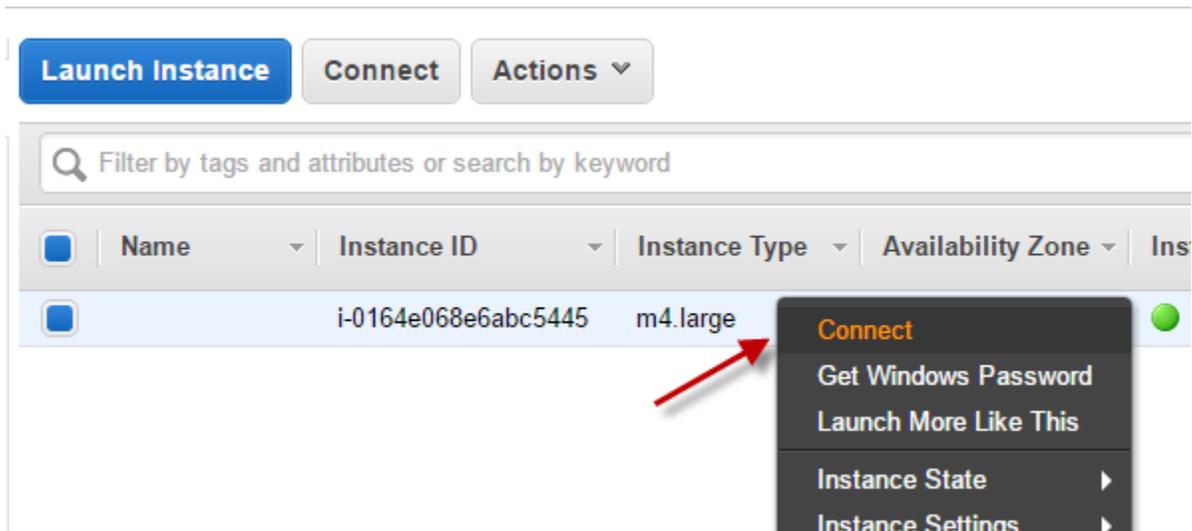
Warning
 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Please note that you can edit this security group later to lock down access by specific IP addresses.

- f. Choose to create a new key pair, give it a name, click on 'Download Key Pair', click 'Launch Instances', and then click 'View Instances' on the next screen.



- g. Right click on your instance and click 'Connect'



- h. Click on 'Get Password'

Connect To Your Instance ✕

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download Remote Desktop File](#)

When prompted, connect to your instance using the following details:

Public DNS	ec2-54-191-94-246.us-west-2.compute.amazonaws.com
User name	Administrator
Password	Get Password 

If you've joined your instance to a directory, you can use your directory credentials to connect to your

- i. Find your Key Pair that you downloaded earlier and select 'Decrypt Password'

Connect To Your Instance > Get Password ✕

The following Key Pair was associated with this instance when it was created.

Key Name SentryOne.pem

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

Key Pair Path No file chosen

Or you can copy and paste the contents of the Key Pair below:

j. Copy your Password and click 'Download Remote Desktop File'

Connect To Your Instance ✕

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

Public DNS ec2-54-191-94-246.us-west-2.compute.amazonaws.com

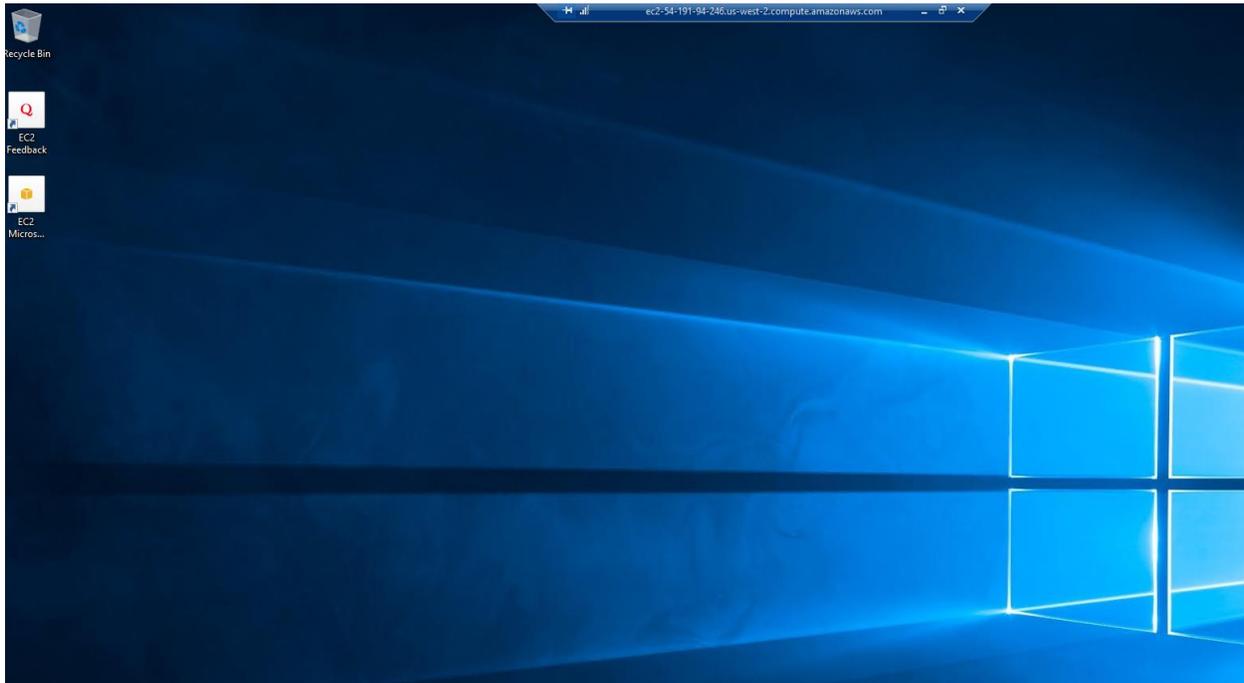
User name Administrator

Password UAgRI=v)IWQTQSlptf@zl=2%y34%INT

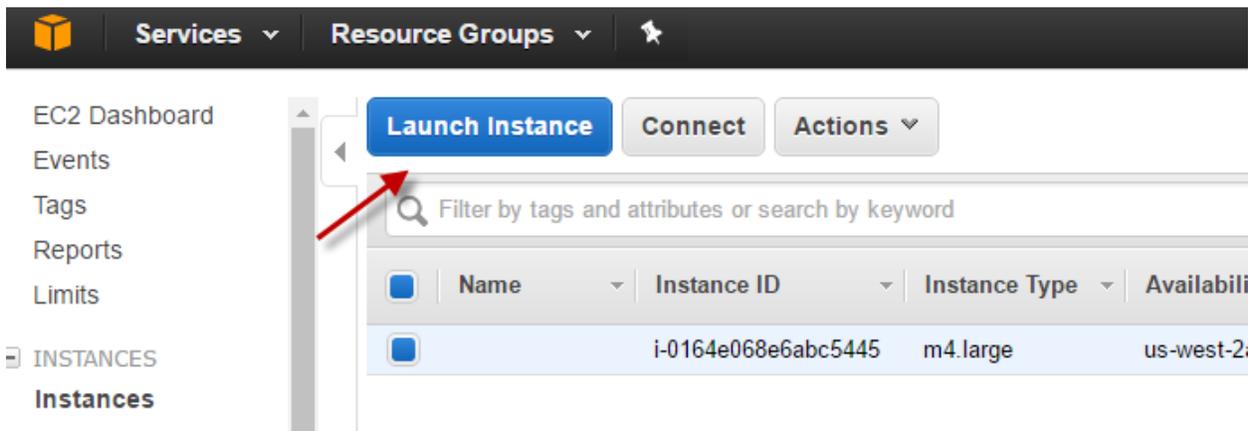
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

k. Connect and log into your new instance



l. To launch an EC2 instance to be monitored, Just click on 'Launch Instance' from the EC2 screen



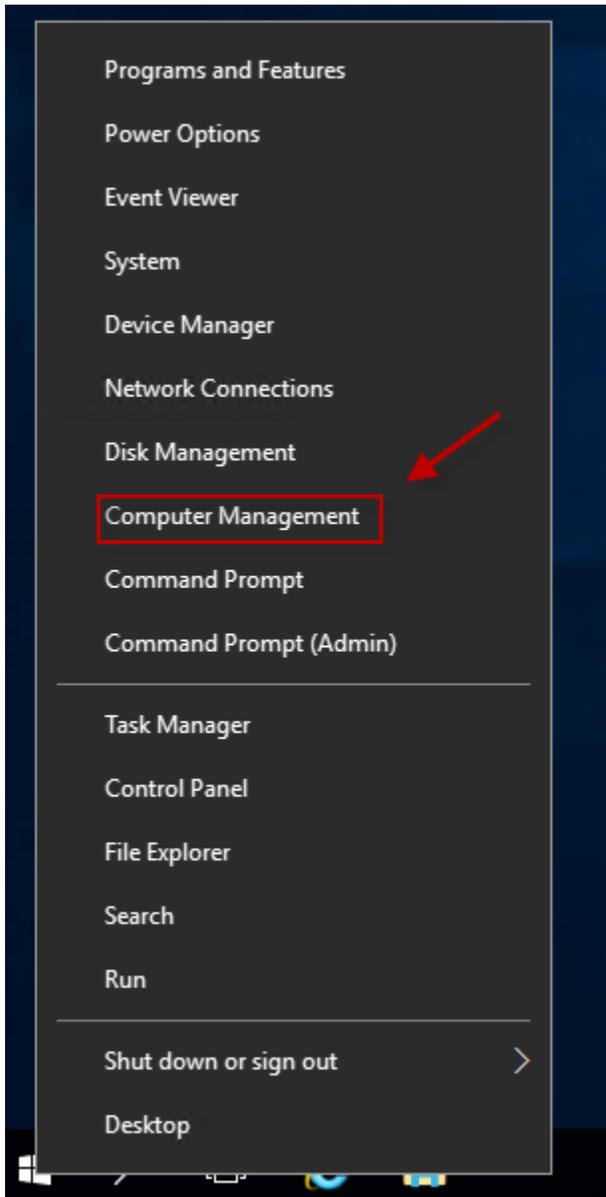
You can now follow the same steps above with one exception. When it comes to Part 1 – e above, you can just choose to use an existing security group and choose the one we created initially then click 'Review and Launch' and 'Launch'.

Assign a security group: Create a new security group
 Select an existing security group

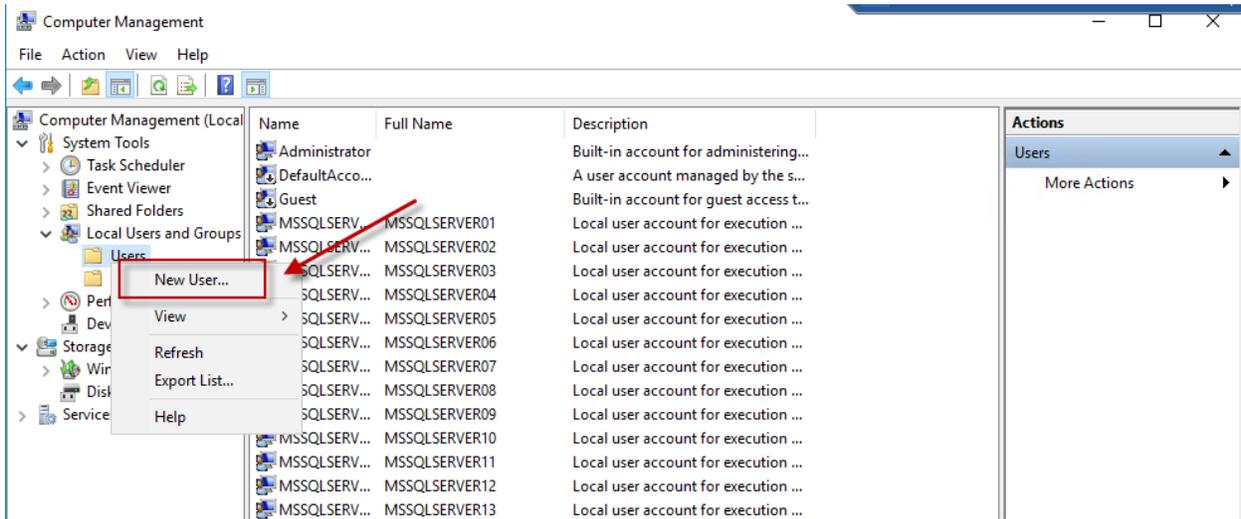
Security Group ID	Name	Description
<input type="radio"/> sg-ce6626ab	default	default VPC security group
<input checked="" type="radio"/> sg-0324d478	SentryOne SG	SentryOne

Part 2: Preparing for installation of SentryOne

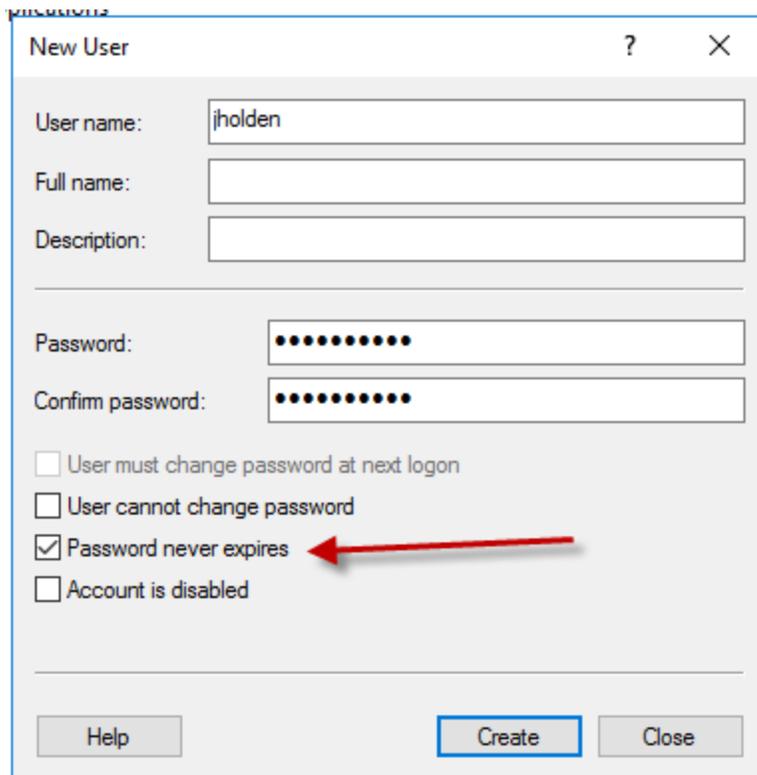
- a. Right click on the Windows button and select 'Computer Management'



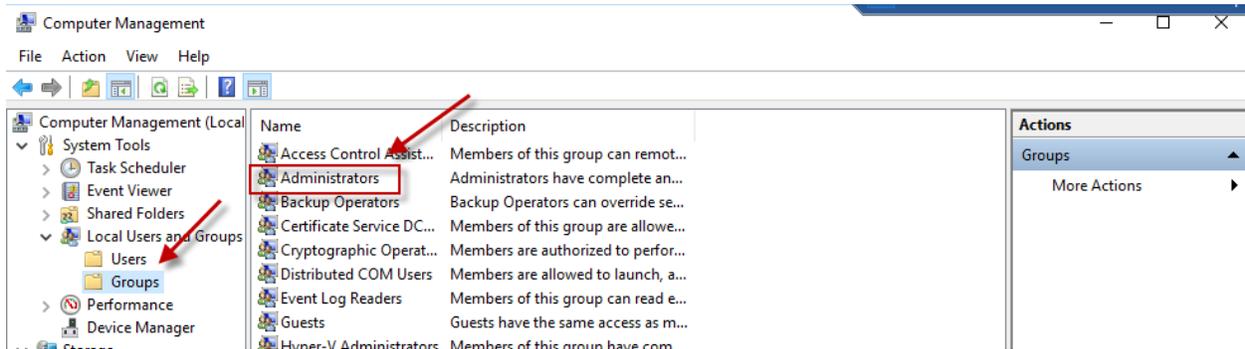
b. Add new user (we will be setting up the monitoring service account here)



c. Make sure that the Password never expires (unless your policy's dictate otherwise)

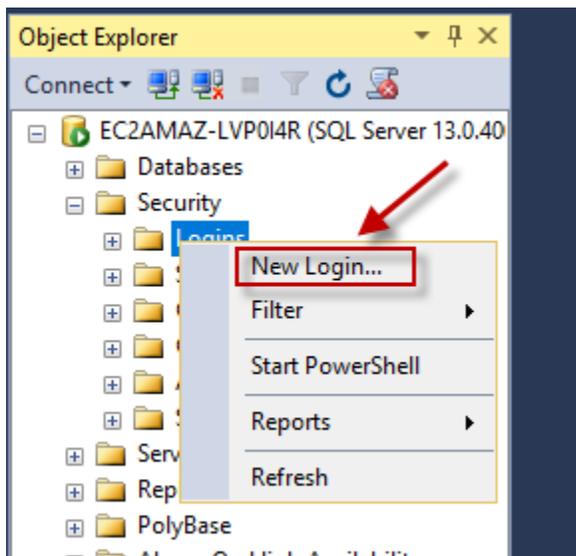


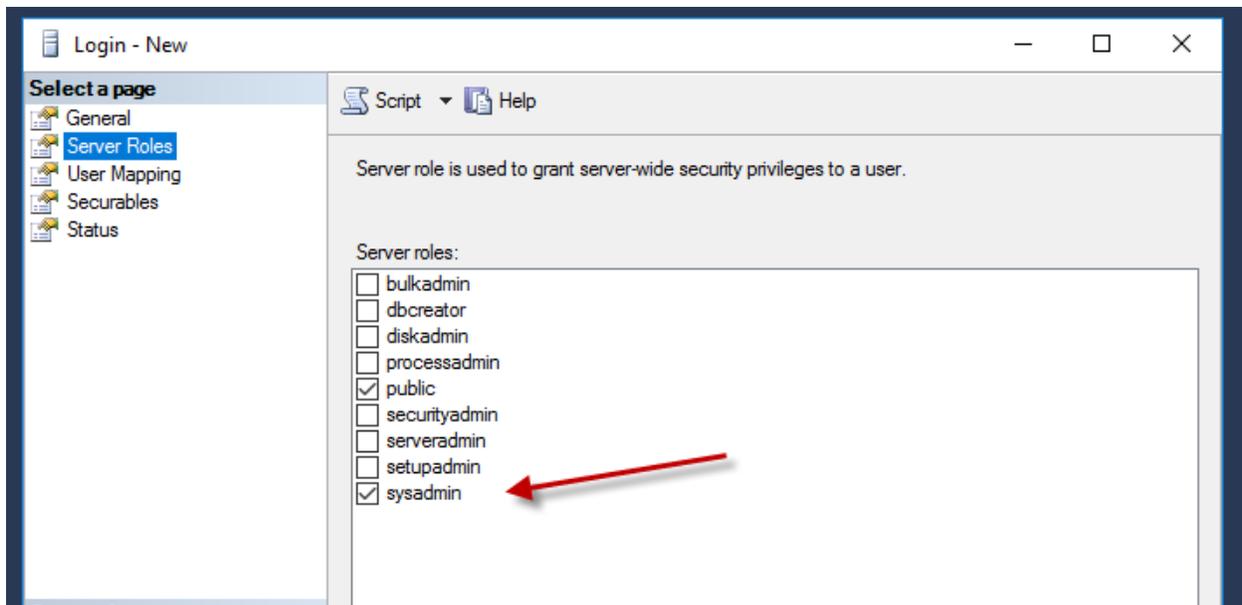
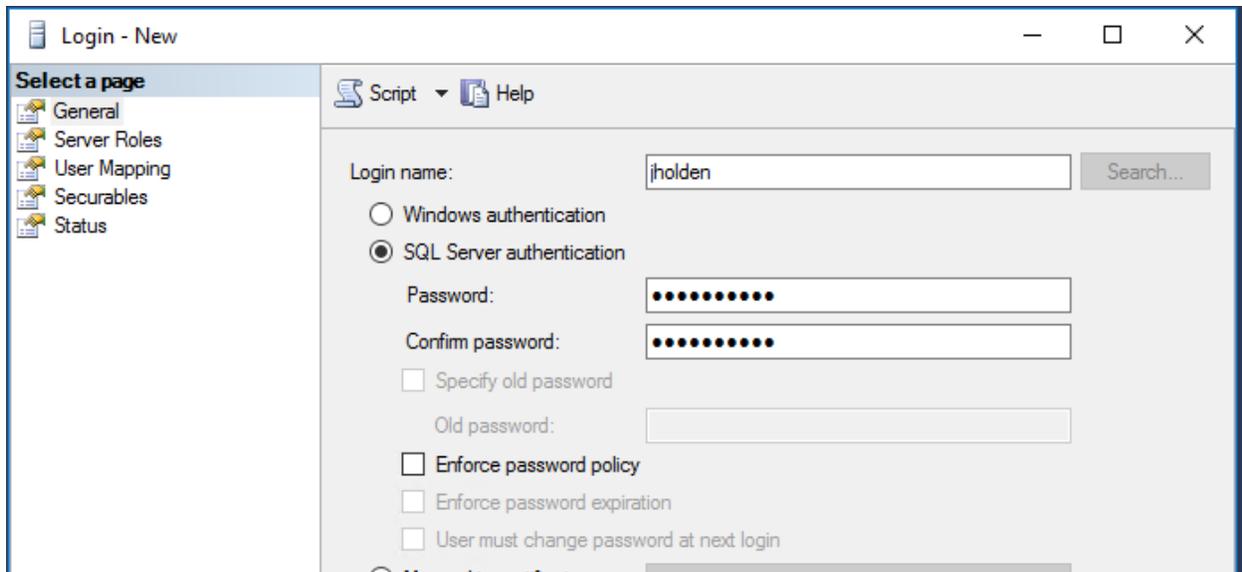
d. Add the account as a member of the Windows Administrators Group



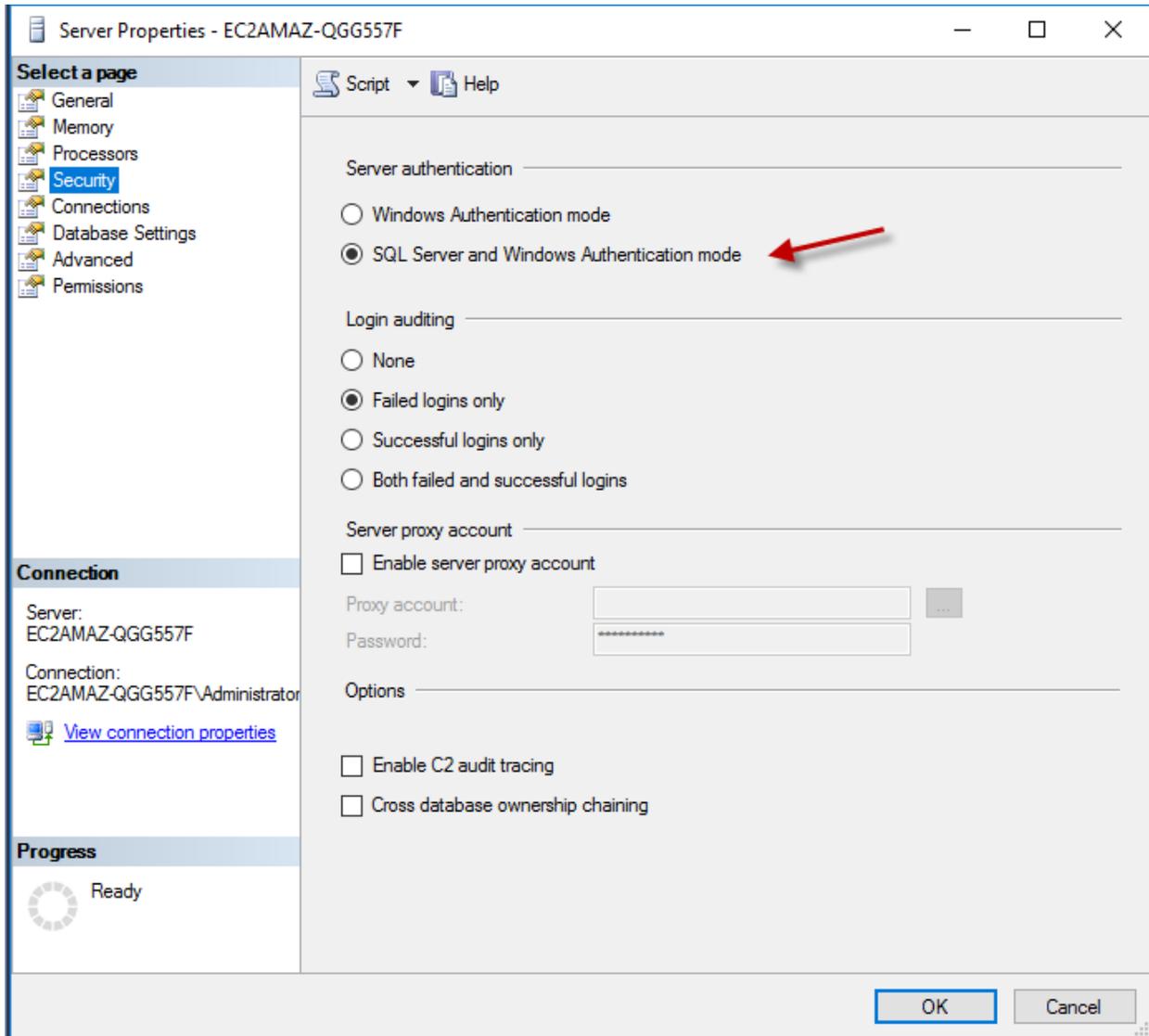
e. Add the account as a sysadmin for the SQL Server instance (dbcreator role if you are not going to be monitoring the SentryOne host server – Not Recommended).

Note: The SQL Server and Agent services must be started prior to this.





- f. Make sure to change the server properties to set security to SQL Server and Windows Authentication mode and restart the SQL Server Service.



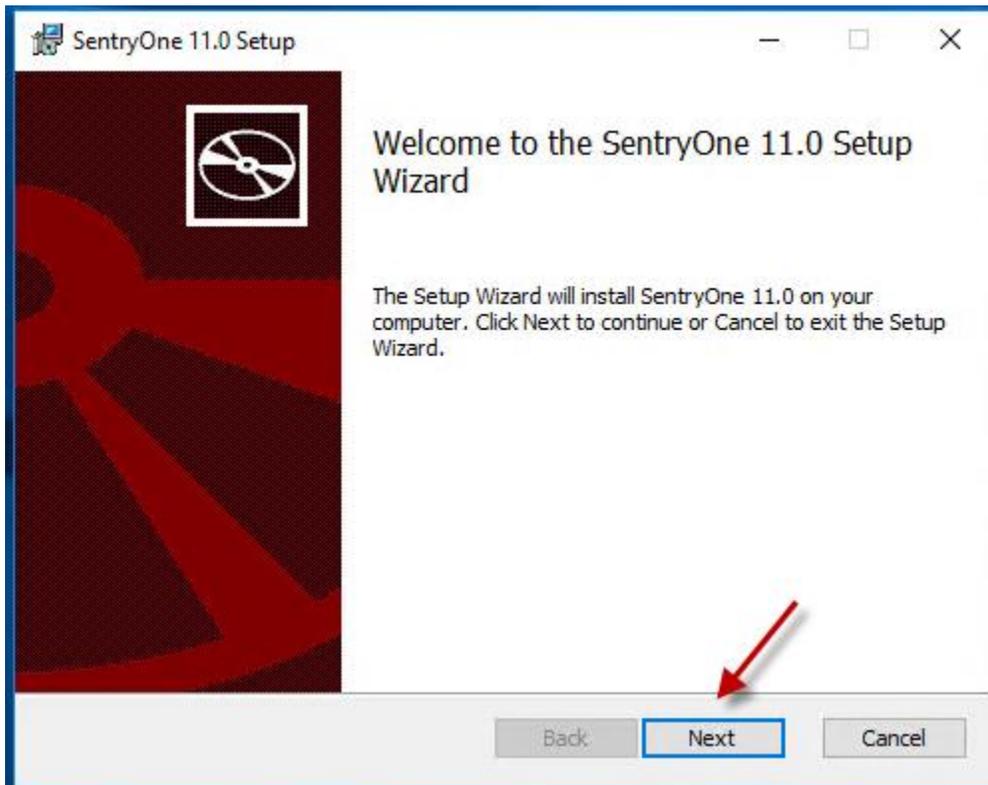
Part 3: Completing the SentryOne installation

- a. Download the installation package from your portal account (<https://sentryone.com/myaccount/login>)

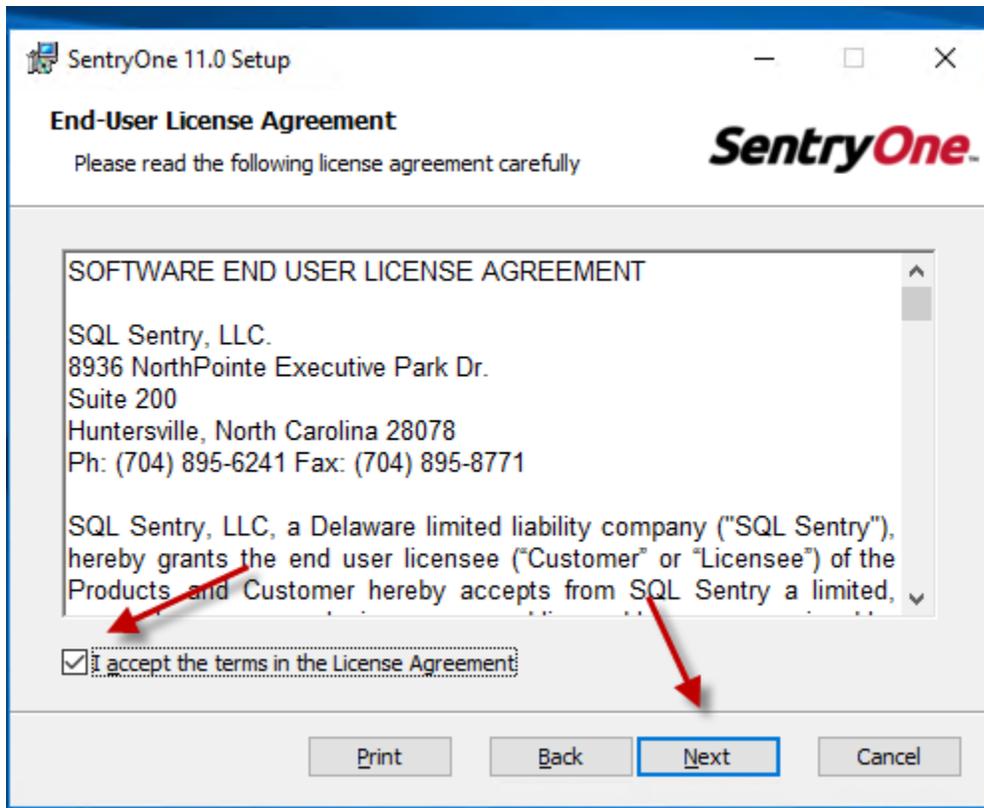
Downloads

Product	Version	Build	Released	Size	Links
SentryOne Unified Setup	11.0	11.0.87.0	03/02/2017	142 MB	x86 x64 Change List
Plan Explorer	3	11.0.84.0	01/16/2017	20 MB	x86 x64 Change List

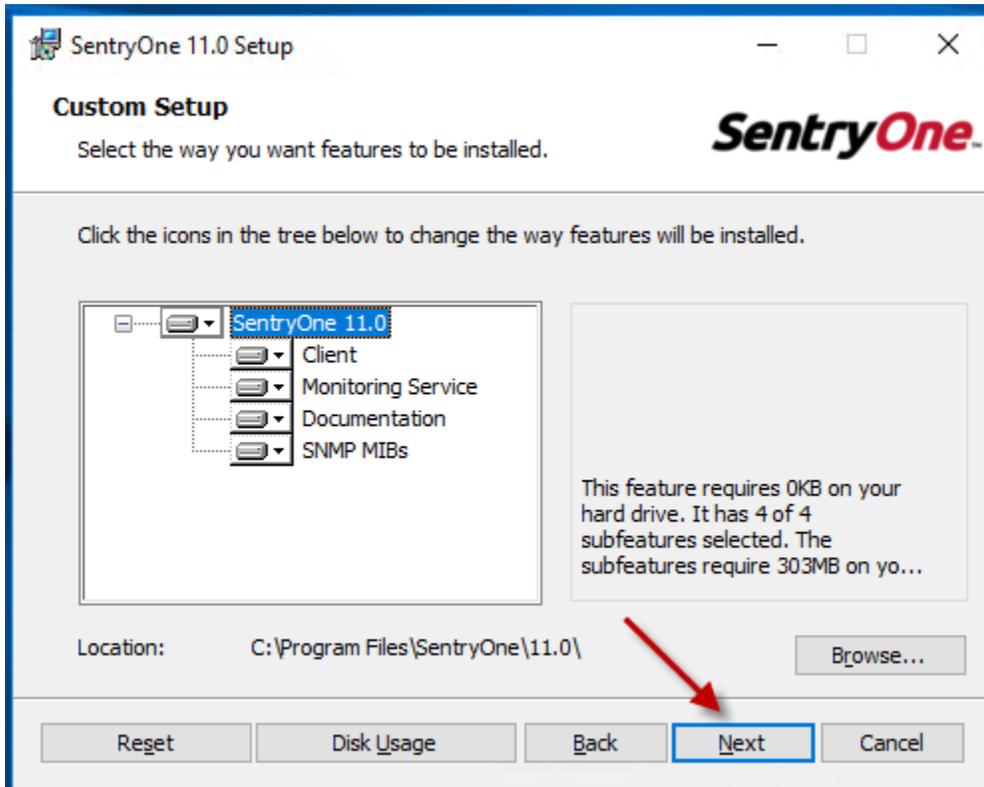
- b. Launch the setup and select 'Next'



- c. Accept the license terms and click Next



- d. Since we are choosing to add all of the components of SentryOne on this server, we can just select the Next button



- e. Here we will enter the server name, the name we want the database to be called, and we will click the Test button

SentryOne 11.0 Setup [Close]

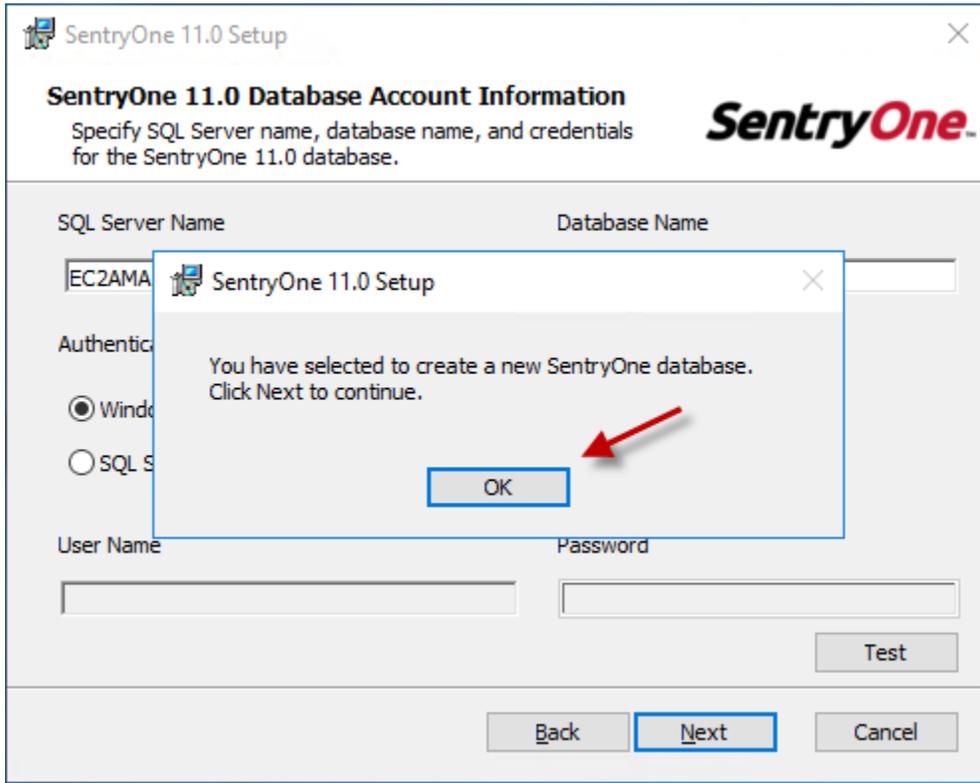
SentryOne 11.0 Database Account Information *SentryOne*
Specify SQL Server name, database name, and credentials for the SentryOne 11.0 database.

SQL Server Name: Database Name:

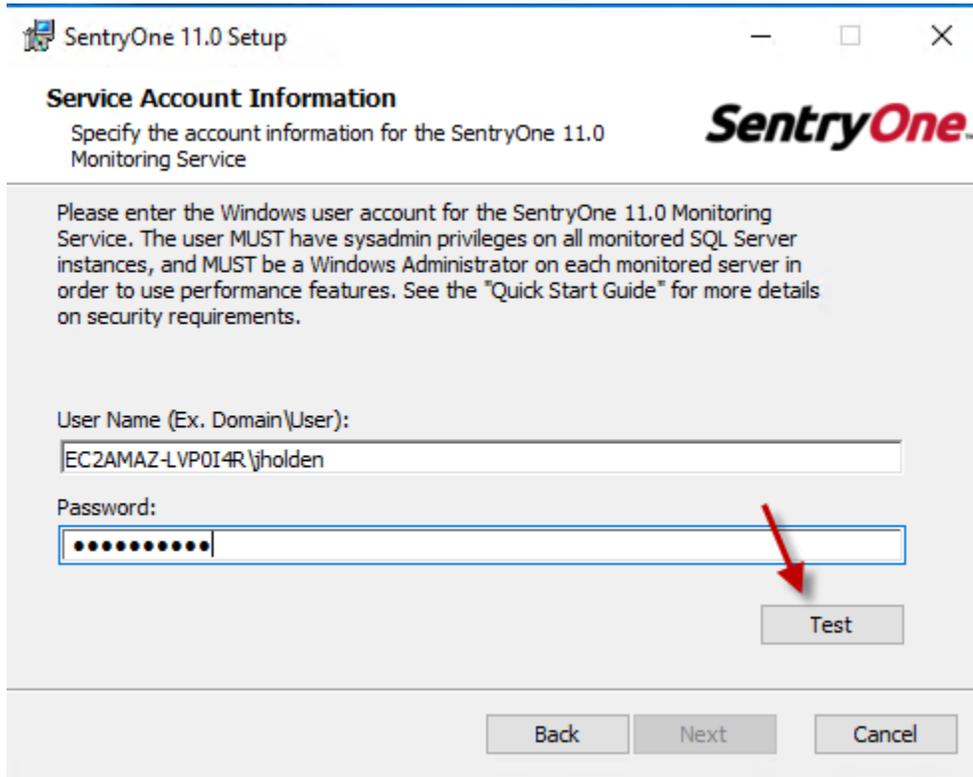
Authentication Mode:
 Windows Authentication
 SQL Server Authentication

User Name: Password:

- f. Once successfully connected, we can click the 'OK' button and then the 'Next' button to proceed



- g. Here we enter the monitoring service account we created in Part 2 above and click the 'Test' button



SentryOne 11.0 Setup

Service Account Information

Specify the account information for the SentryOne 11.0 Monitoring Service

Please enter the Windows user account for the SentryOne 11.0 Monitoring Service. The user MUST have sysadmin privileges on all monitored SQL Server instances, and MUST be a Windows Administrator on each monitored server in order to use performance features. See the "Quick Start Guide" for more details on security requirements.

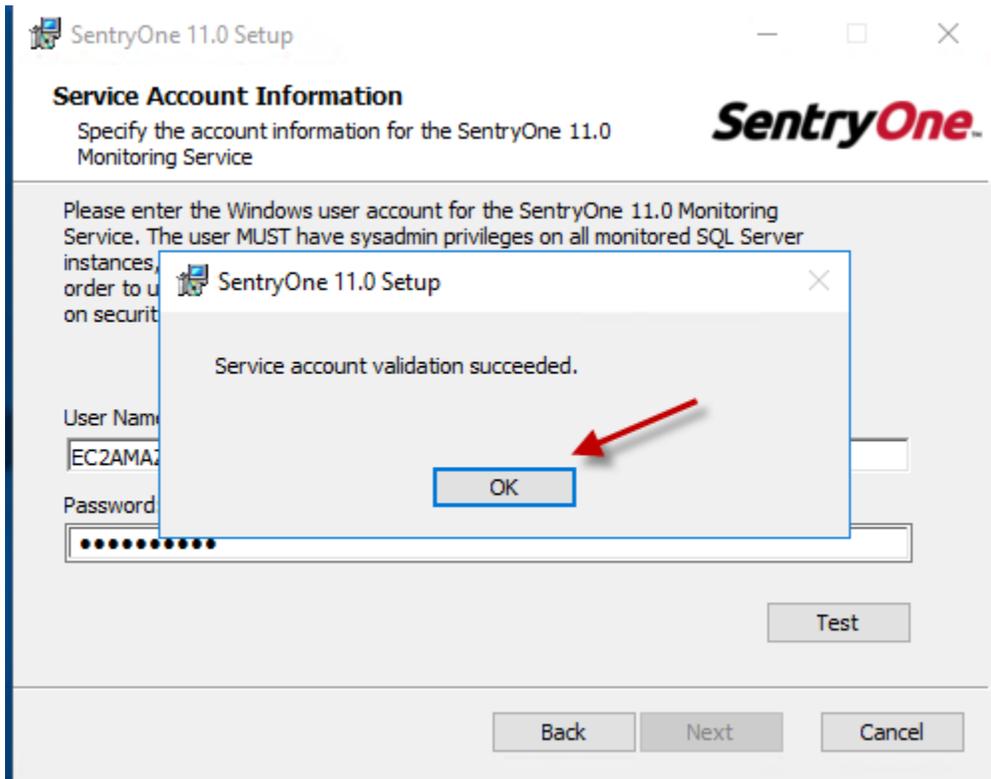
User Name (Ex. Domain\User):

Password:

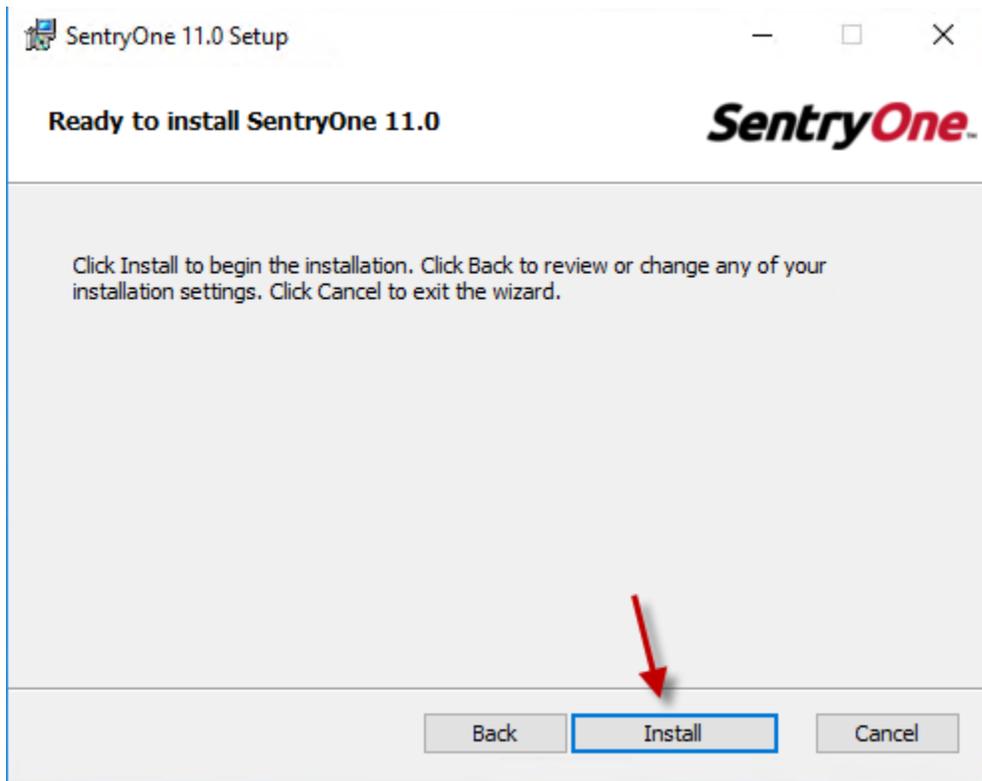
Test

Back **Next** **Cancel**

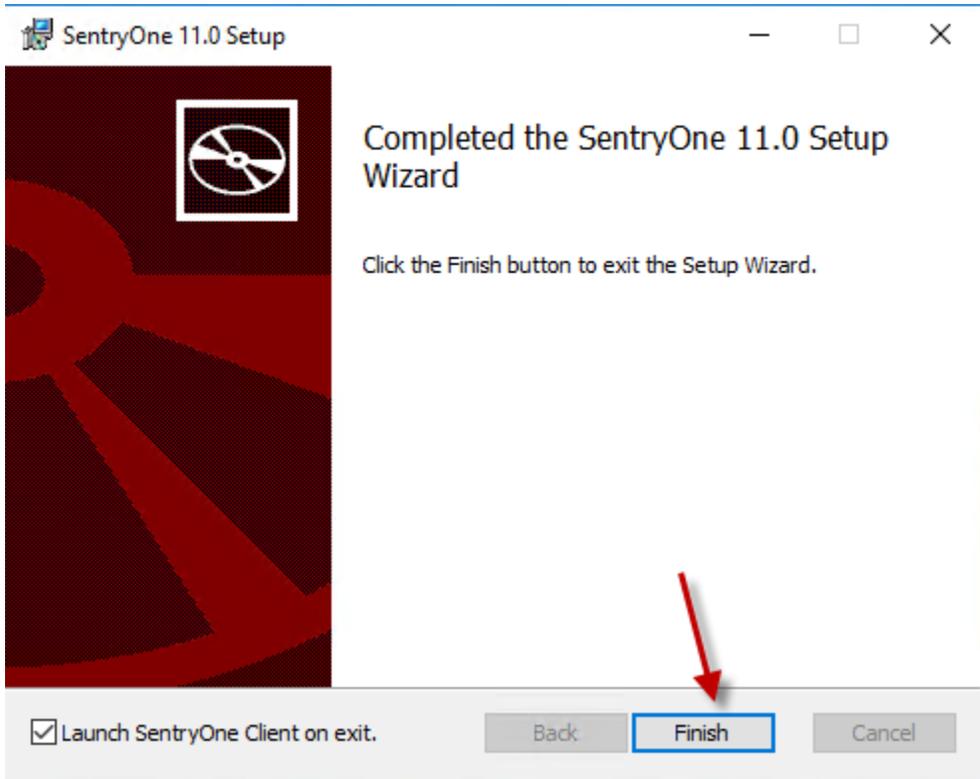
- h. Once the validation has succeeded, we can click the 'OK' and 'Next' buttons



- i. We can now click the 'Install' button to finish the installation



- j. Once the installation finishes, we can select the 'Finish' button to open up the SentryOne client and finish the Setup Wizard



- k. Click the 'Continue' button



- I. Click the 'Paste license' button and paste in the license that should have been sent to you and click 'Save'

License Configuration

It looks like a license is not configured. Please provide a valid license by pasting or loading it from a file.

Paste license

Load from file

Please provide a valid license. If you need a license for evaluation, or to purchase the full product, contact sales@sentryone.com.

License Configuration

Please paste the license into the space below and click Save.

```
<Type="System.Int32"><Custom><LicenseUnits Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedApsApplianceConnections><WatchedAzureSqlDbConnections Value="0"
Type="System.Int32"><Custom><LicenseUnits Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedAzureSqlDbConnections><WatchedOracleConnections Value="0"
Type="System.Int32"><Custom><LicenseUnits Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedOracleConnections><WatchedSharePointConnections Value="0"
Type="System.Int32"><Custom><LicenseUnits Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedSharePointConnections><WatchedSqlDataWarehouseConnections Value="0"
Type="System.Int32"><Custom><LicenseUnits Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedSqlDataWarehouseConnections><WatchedSqlServerConnections Value="5"
Type="System.Int32"><Custom><LicenseUnits Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedSqlServerConnections><WatchedSsasConnections Value="0" Type="System.Int32"><Custom><LicenseUnits
Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedSsasConnections><WatchedTaskSchedulerConnections Value="0"
Type="System.Int32"><Custom><LicenseUnits Value="0" Type="System.String" ></LicenseUnits></Custom></
WatchedTaskSchedulerConnections><IsSubscriptionLicense Value="False" Type="System.Boolean" >></
IsSubscriptionLicense></Custom><StandbyHardwareKeys xmlns="" ></StandbyHardwareKeys></Object></
Signature></LicenseFile>
```

Save

- m. Enter in your user information and click the 'Save' button

Tell Us More About Yourself

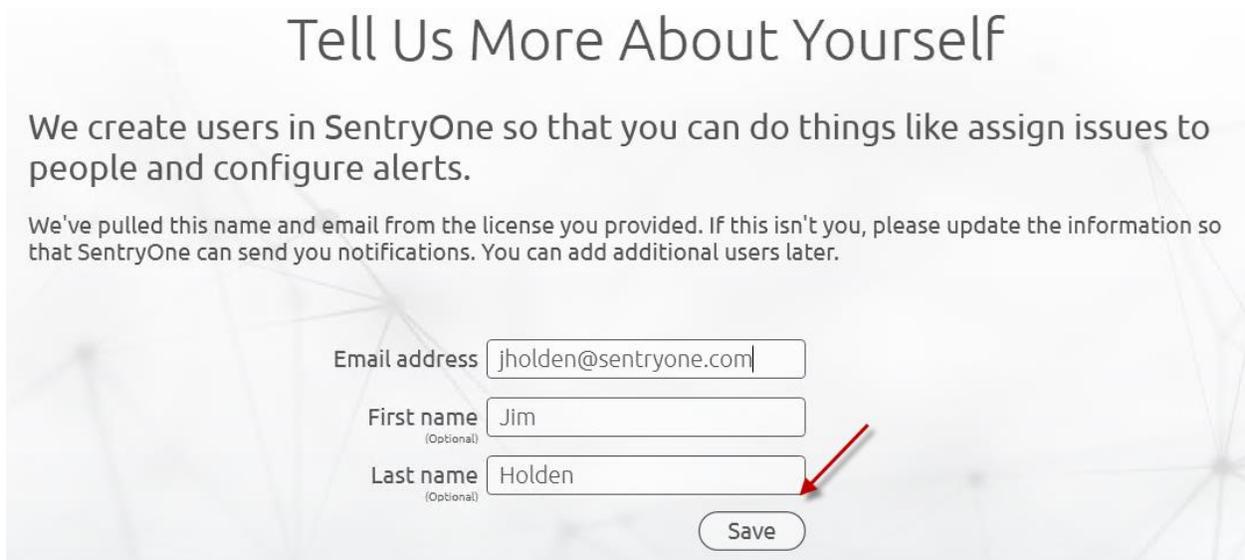
We create users in SentryOne so that you can do things like assign issues to people and configure alerts.

We've pulled this name and email from the license you provided. If this isn't you, please update the information so that SentryOne can send you notifications. You can add additional users later.

Email address

First name
(Optional)

Last name
(Optional)



- n. Configure your SMTP Server (check the radio button and select the 'Save' Button)

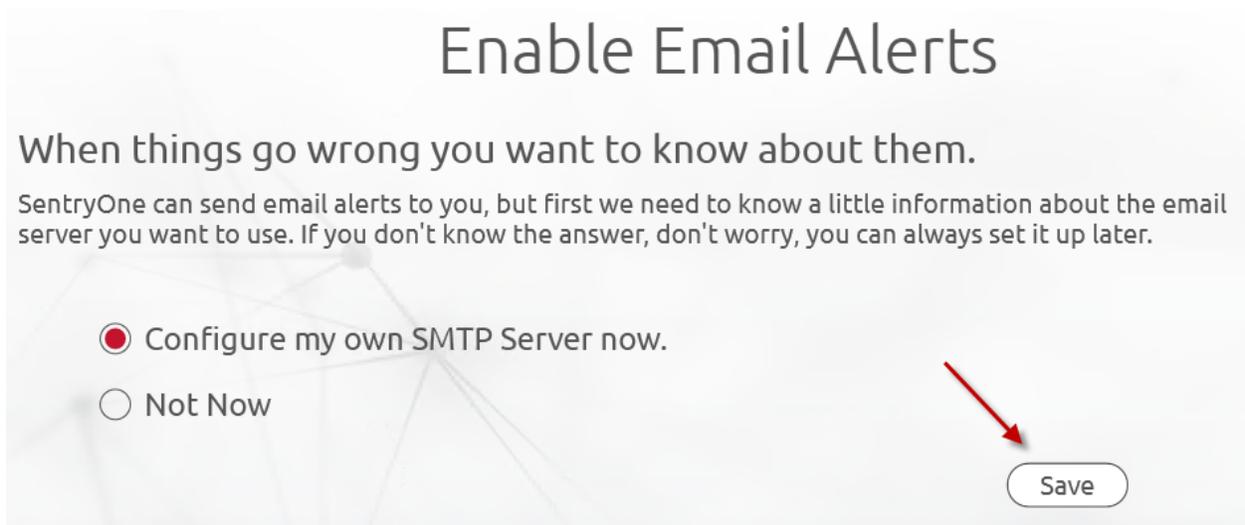
Enable Email Alerts

When things go wrong you want to know about them.

SentryOne can send email alerts to you, but first we need to know a little information about the email server you want to use. If you don't know the answer, don't worry, you can always set it up later.

Configure my own SMTP Server now.

Not Now



- o. Enter your information and click on the 'Save' button

Enable Email Alerts

Please provide the address of your SMTP server and the "from address" you'd like to use for the alert emails. You can always set this up at a later time, but skipping this step means that no alerts will be emailed.

SMTP Server address <input type="text" value="123@sentryone.com"/>	<div style="border: 1px solid #ccc; padding: 5px;"><p style="margin: 0;">Security (Optional)</p><p>User name <input type="text" value="stuff&things"/></p><p>Password <input type="password" value="●●●●●●●●●●"/></p><p style="font-size: small;">If your SMTP Server is security enabled we'll need some credentials. (Optional)</p></div>
Email from address <input type="text" value="Alerts@sentryone.com"/>	
<input checked="" type="checkbox"/> Enable SSL	
Custom port number <input type="text" value="587"/> <small>(Optional)</small>	

- p. Select the severity level for your Advisory Conditions to be emailed to you and click the 'Save' button

Advisory Conditions

Advisory Conditions is a powerful feature of SentryOne that allows you to define scenarios for which you want to be alerted, or execute an automated action.

You can create just about any condition you can think of, completely tailored to your environment! We've included a great selection of **default Advisory Conditions** to get you started.

We've categorized the **default Advisory Conditions** based on severity.

Which severity conditions would you like emailed to you?

Critical High Medium Low

- q. If you have a cloud.sentryone.com account you can enter it here, or create a new one by choosing the options below (I will skip this for now).



cloud.sentryone.com

cloud.sentryone.com provides secure access to your performance data from anywhere in the world using a browser or mobile device.

You can use this feature to share your performance data with consultants, partners, or just other members of your team who may not have access to the SentryOne Client.

Through cloud.sentryone.com, you can also download additional advisory conditions via the Condition Exchange, and even share your own creations.

To get started, you need a SentryOne Cloud account. This only records your cloud configuration, and synchronizes your advisory conditions so you can share them across installations.

It will not synchronize any performance data or events without your permission.

[Create account](#) [Sign into existing account](#)

- r. Click on the 'Let's Go!' button here



Welcome!

Give us a few seconds to get everything configured.

The information you have provided will help give you the best user experience.

Once everything is configured, we'll start off by helping you add your first target.

SentryOne™
Monitor • Diagnose • Optimize

[Let's Go!](#)

- s. Now it is time to add our first target to be monitored. I'm going to choose our SentryOne server here

S1 Add Target

Please select the type of target
SQL Server

Please enter the name of the target
EC2AMAZ-LVP0I4R

Instance Name (leave blank for default instance)

Port

Use Integrated Authentication

Credentials

User Name

Password

>> Advanced Options

Feature Availability

Feature	Results	Details
Monitoring Service: Default Site: EC2AMAZ-LVP0I4R		
Monitoring Service Available	●	OK
Windows Dashboard	?	Unknown
Windows Processes	?	Unknown
Disk Activity	?	Unknown
Disk Space	?	Unknown
Windows Performance Counters	?	Unknown
Validate Core-Based License	?	Unknown
VMware Site Compliance	?	Unknown

Click "Connect" to find the feature availability.

Connect Next Cancel

Click the 'Next' button here

SI Add Target

Please select the type of target
SQL Server

Please enter the name of the target
EC2AMAZ-LVP0I4R

Instance Name (leave blank for default instance)

Port

Use Integrated Authentication

Credentials
User Name
Password

» Advanced Options

Feature Availability

Feature	Results	Details
Monitoring Service: Default Site: EC2AMAZ-LVP0I4R		
Monitoring Service Available	●	OK
Windows Dashboard	●	OK
Windows Processes	●	OK
Disk Activity	●	OK
Disk Space	●	OK
Windows Performance Counters	●	OK
Validate Core-Based License	●	N/A
VMware Site Compliance	●	N/A

Select Site
Default Site (Full Access)

Click "Next" to add this target with full feature availability.

Retry Next Cancel

The server is now being added

The screenshot shows a window titled "Watch Status for 2 Instances" with a table of tasks. The tasks are grouped under "EC2AMAZ-LVP014R". The "Event Manager W..." and "Performance Advis..." tasks are in a "Running" state with a message "Attempting to connect". The "Performance Advisor ..." and "Initialize Target" tasks are in an "Idle" state and have completed.

Task	Description	Duration	% Complete	State	Message	Last Result	Last Success Time
EC2AMAZ-LVP014R	2 Running, 0 Errors, 0 Cancelled						
EC2AMAZ-LVP014R	2 Running, 0 Errors, 0 Cancelled						
Event Manager W...	Tracks phases for newly watche...	00:00:21.203		Running	Attempting to connect		
Performance Advis...	Tracks phases for newly watche...	00:00:21.193		Running	Attempting to connect		
Performance Advisor ...	Tracks phases for newly watche...	00:00:14.750		Idle		Completed	2017-03-31 14:20:03
Initialize Target	Initializes and collects data for t...	00:00:10.770		Idle		Completed	2017-03-31 14:20:00

Message: Attempting to connect

Buttons: Export, Open, OK

Initialization has been completed and the server can now be monitored

The screenshot shows the same window as above, but now all tasks are in a "Completed" state. The "Event Manager W..." and "Performance Advis..." tasks are now "Completed" with a "Last Success Time" of 2017-03-31 14:20:14 and 2017-03-31 14:20:19 respectively. A red arrow points to the "Open" button at the bottom right.

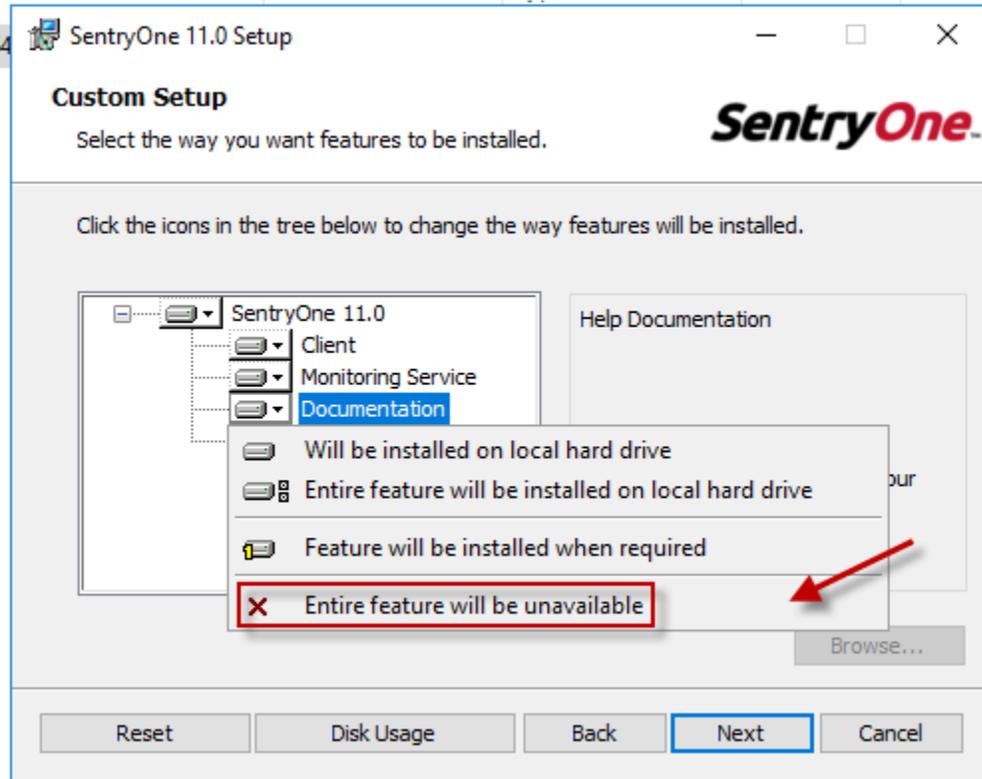
Task	Description	Duration	% Complete	State	Message	Last Result	Last Success Time
EC2AMAZ-LVP014R	0 Running, 0 Errors, 0 Cancelled						
EC2AMAZ-LVP014R	0 Running, 0 Errors, 0 Cancelled						
Event Manager W...	Tracks phases for newly watche...	00:00:25.483		Idle		Completed	2017-03-31 14:20:14
Performance Advis...	Tracks phases for newly watche...	00:00:30.257		Completed		Completed	2017-03-31 14:20:19
Performance Advisor ...	Tracks phases for newly watche...	00:00:14.750		Idle		Completed	2017-03-31 14:20:03
Initialize Target	Initializes and collects data for t...	00:00:10.770		Idle		Completed	2017-03-31 14:20:00

Message:

Buttons: Export, Open, OK

Part 4: Successfully monitoring additional EC2 instances

- a. Because I am monitoring an EC2 Instance that is a Workgroup, I will install a monitoring service and client on the target server. The process of installation is the same as Part 3 above with a couple of exceptions
 1. In the custom setup screen, I will only select the Client and the monitoring service from the list by choosing to disable the Documentation and the SNMP MIBs



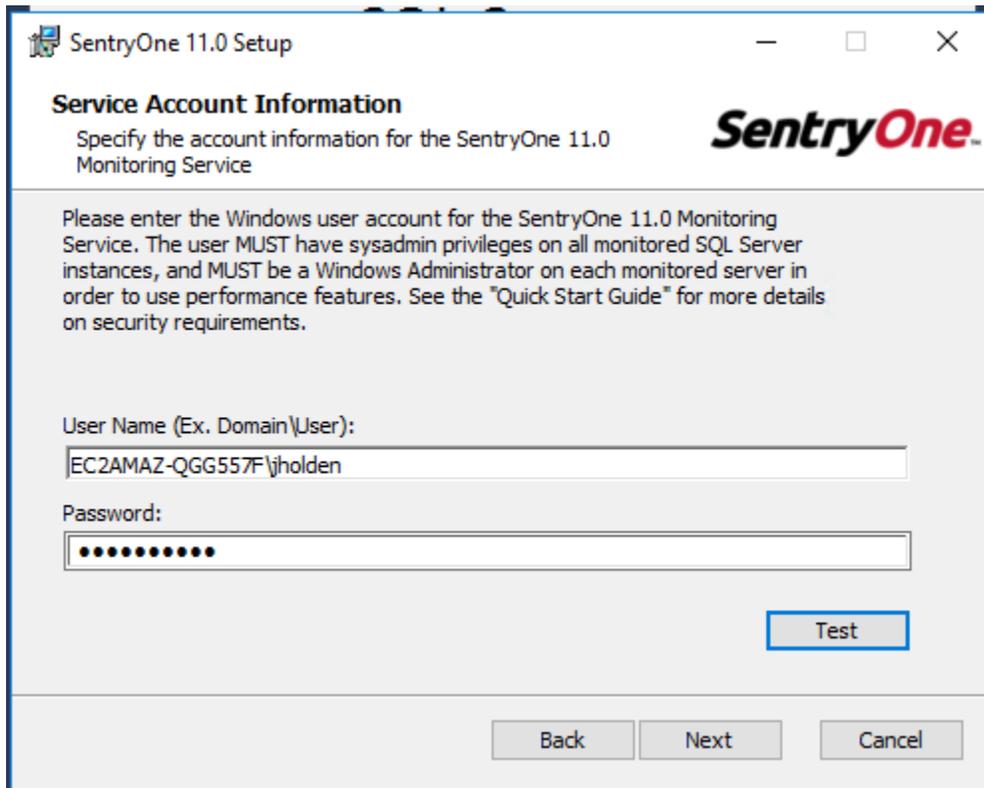
2. In the database account information screen, I will use the public DNS name for the workgroup and use SQL Authentication to connect to the SentryOne database

The screenshot shows the 'SentryOne 11.0 Setup' dialog box, specifically the 'Database Account Information' screen. The window title is 'SentryOne 11.0 Setup' with a close button (X) in the top right corner. The main heading is 'SentryOne 11.0 Database Account Information' followed by the instruction: 'Specify SQL Server name, database name, and credentials for the SentryOne 11.0 database.' The SentryOne logo is visible in the top right. The form contains the following fields and options:

- SQL Server Name:** A text box containing the value 'i?-148-34.us-west-2.compute.amazonaws.com'.
- Database Name:** A text box containing the value 'SentryOne'.
- Authentication Mode:** Two radio button options: 'Windows Authentication' (unselected) and 'SQL Server Authentication' (selected).
- User Name:** A text box containing the value 'jholden'.
- Password:** A text box containing ten black dots, indicating a masked password.

At the bottom right of the form area is a 'Test' button. At the bottom of the dialog box are three buttons: 'Back', 'Next', and 'Cancel'.

3. In the service account information screen, I will use the local account that we created for the SentryOne monitoring service to use



The screenshot shows a Windows dialog box titled "SentryOne 11.0 Setup". The main heading is "Service Account Information" with the subtext "Specify the account information for the SentryOne 11.0 Monitoring Service". The SentryOne logo is in the top right corner. Below the heading, there is a paragraph of instructions: "Please enter the Windows user account for the SentryOne 11.0 Monitoring Service. The user MUST have sysadmin privileges on all monitored SQL Server instances, and MUST be a Windows Administrator on each monitored server in order to use performance features. See the 'Quick Start Guide' for more details on security requirements." There are two input fields: "User Name (Ex. Domain\User):" containing "EC2AMAZ-QGG557F\jholden" and "Password:" with masked characters. A "Test" button is located to the right of the password field. At the bottom, there are "Back", "Next", and "Cancel" buttons.

SentryOne 11.0 Setup

Service Account Information
Specify the account information for the SentryOne 11.0 Monitoring Service

Please enter the Windows user account for the SentryOne 11.0 Monitoring Service. The user MUST have sysadmin privileges on all monitored SQL Server instances, and MUST be a Windows Administrator on each monitored server in order to use performance features. See the "Quick Start Guide" for more details on security requirements.

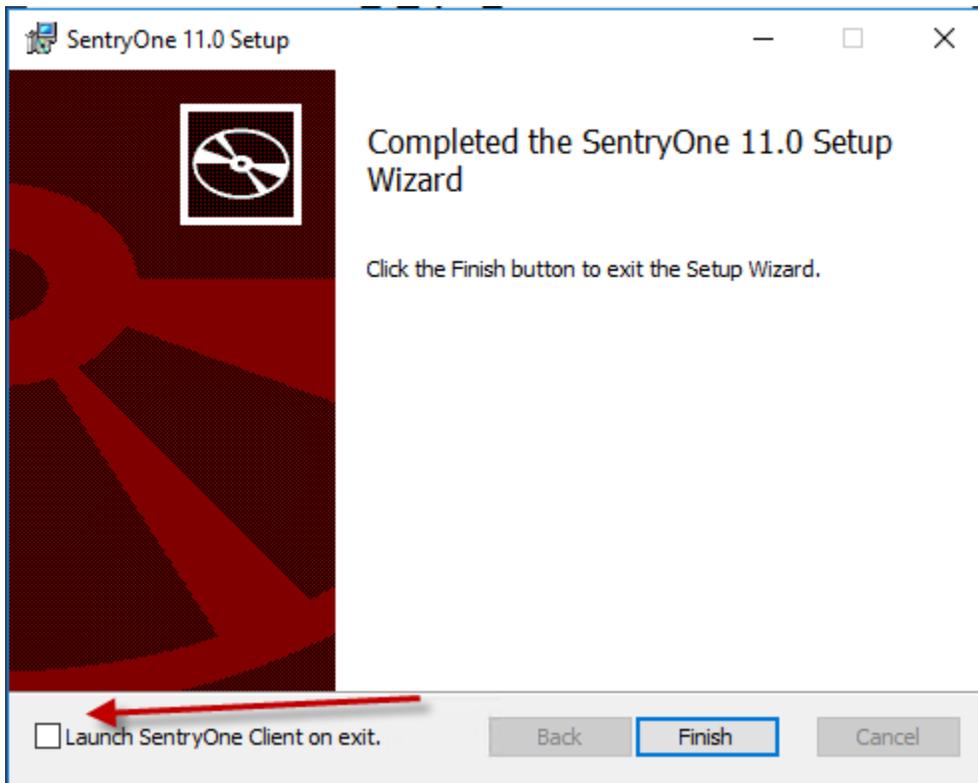
User Name (Ex. Domain\User):
EC2AMAZ-QGG557F\jholden

Password:
●●●●●●●●

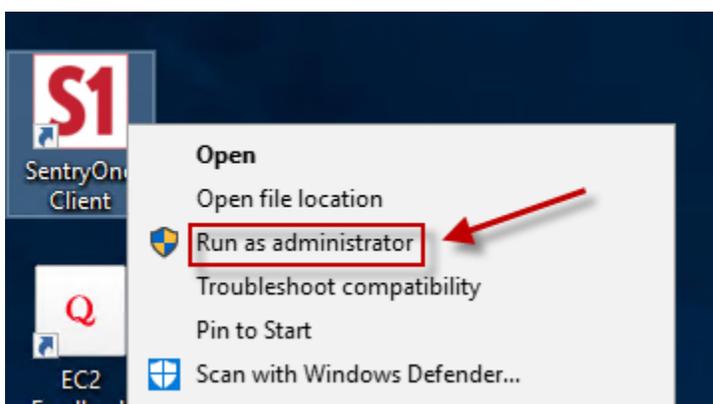
Test

Back Next Cancel

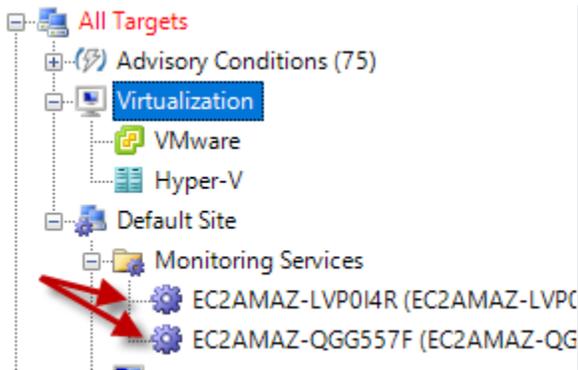
4. Once the installation completes, I have unchecked the box marked 'Launch SentryOne Client on exit', and then clicked 'Finish'. The reason for this is that we need to run the client as Administrator when we first connect to the server where the client is running.



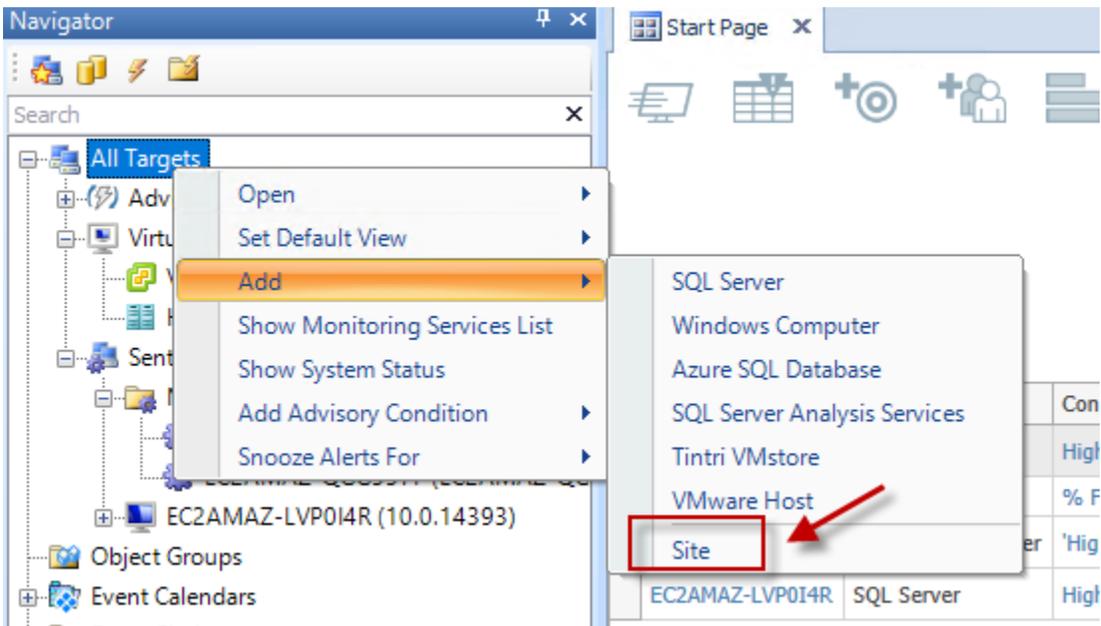
- b. We will now want to right click on the SentryOne client icon and choose the 'Run as administrator option'



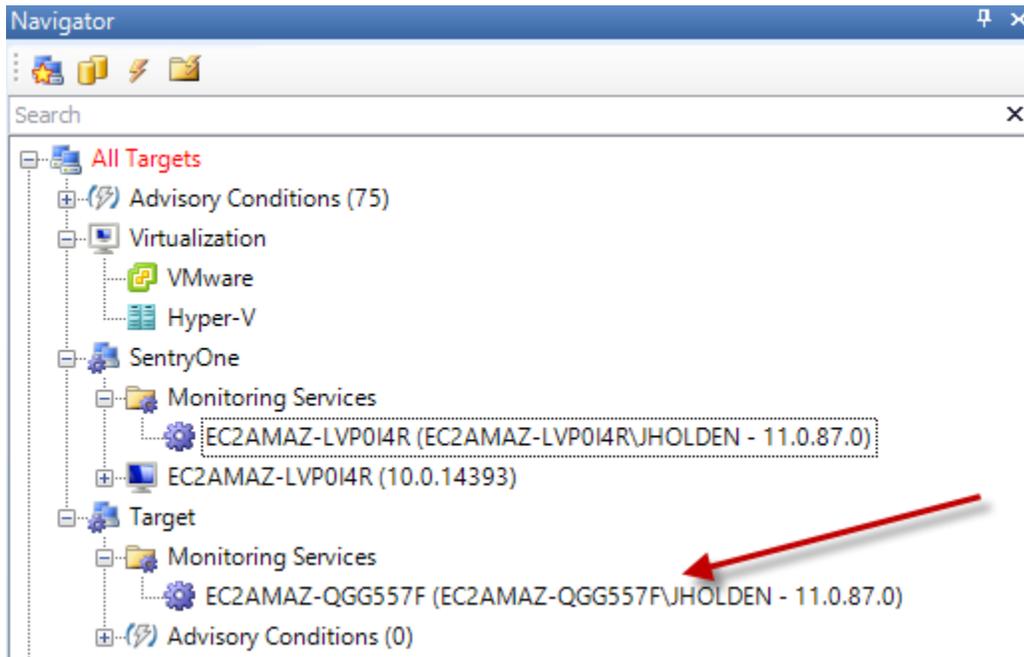
- c. Once the client opens, we can expand the Monitoring Services folder under the Default Site in the Navigator pane and we will see both of our monitoring services



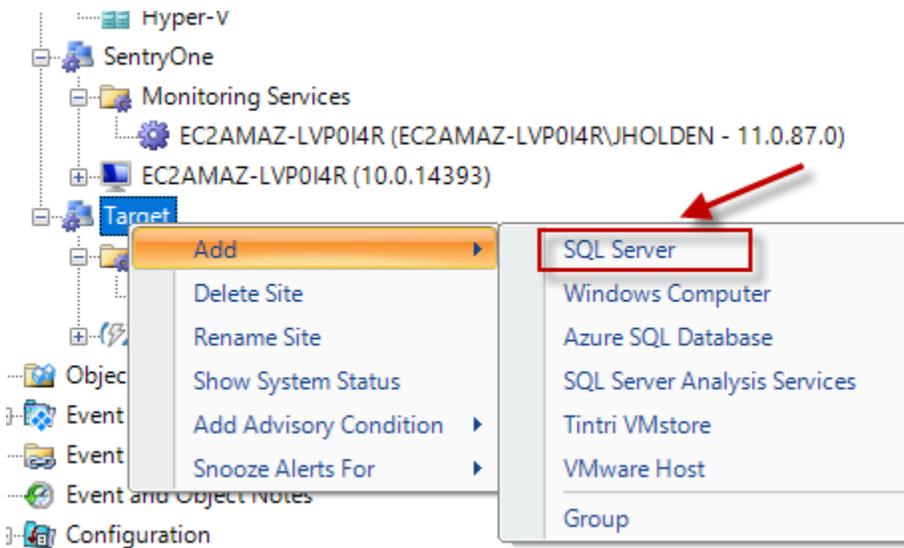
- d. We can now create a separate site for our target to keep it separated from our SentryOne site (I right click and renamed from Default Site to SentryOne). I will call this new site Target.



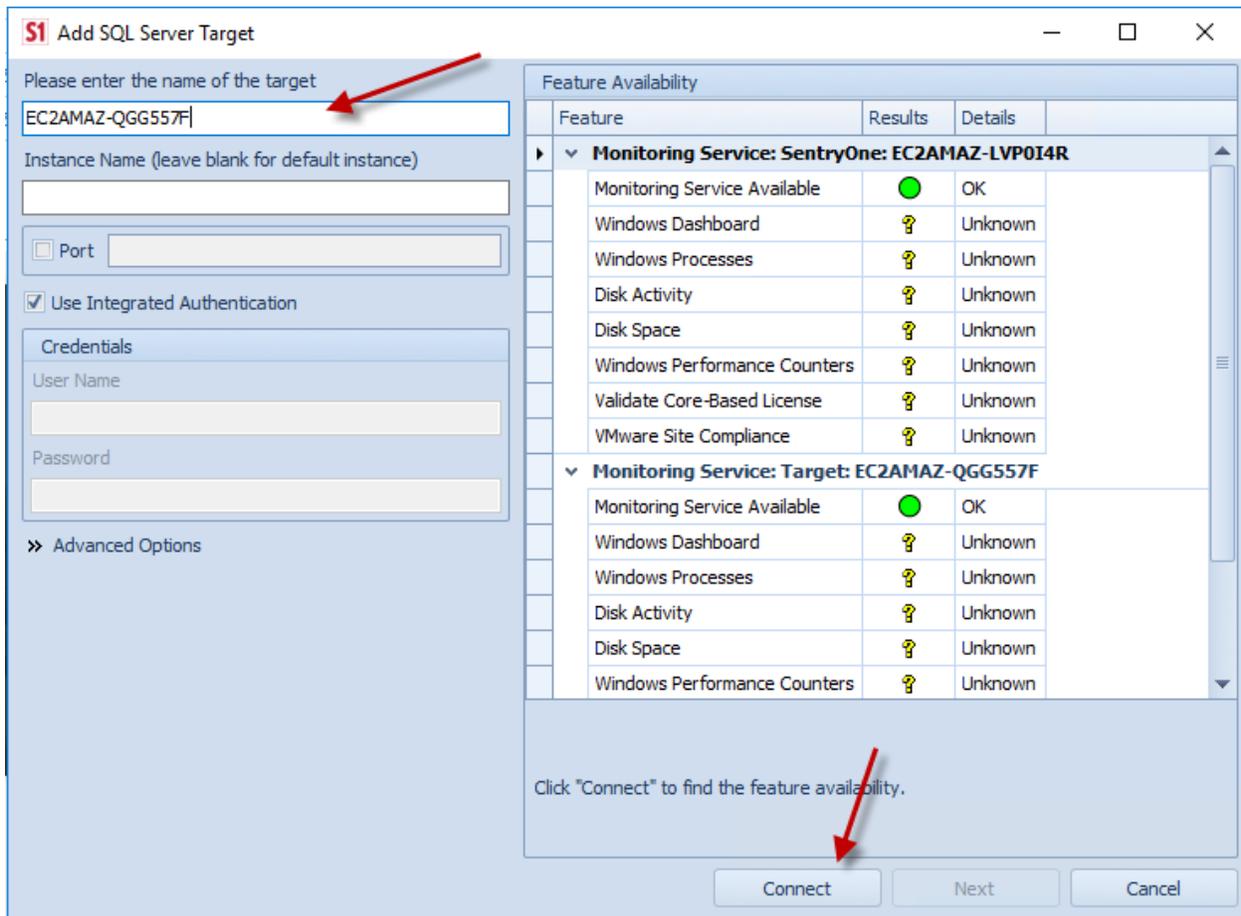
- e. Now I can click and drag the monitoring service that we added on our target and drop it into the new site



- f. From here, we can add our new target by right clicking on the Target site and choosing to Add SQL Server.



g. We can now add the new server (same process as Part 3 – s above)



I hope that you have found this useful.

Happy monitoring!