ARGENT
ENCYCLOPEDIA

Reducing Network Utilization When Consolidating Log Events

Reducing Network Utilization When Consolidating Log Events

Customers using Argent Data Consolidator or Argent for Security may notice a lot of WAN bandwidth utilization while consolidating logs from servers located in remote offices.

The default Argent services used for log collection do not compress the collected logs when forwarding them from an Argent Engine located in a remote office to the central Argent database.

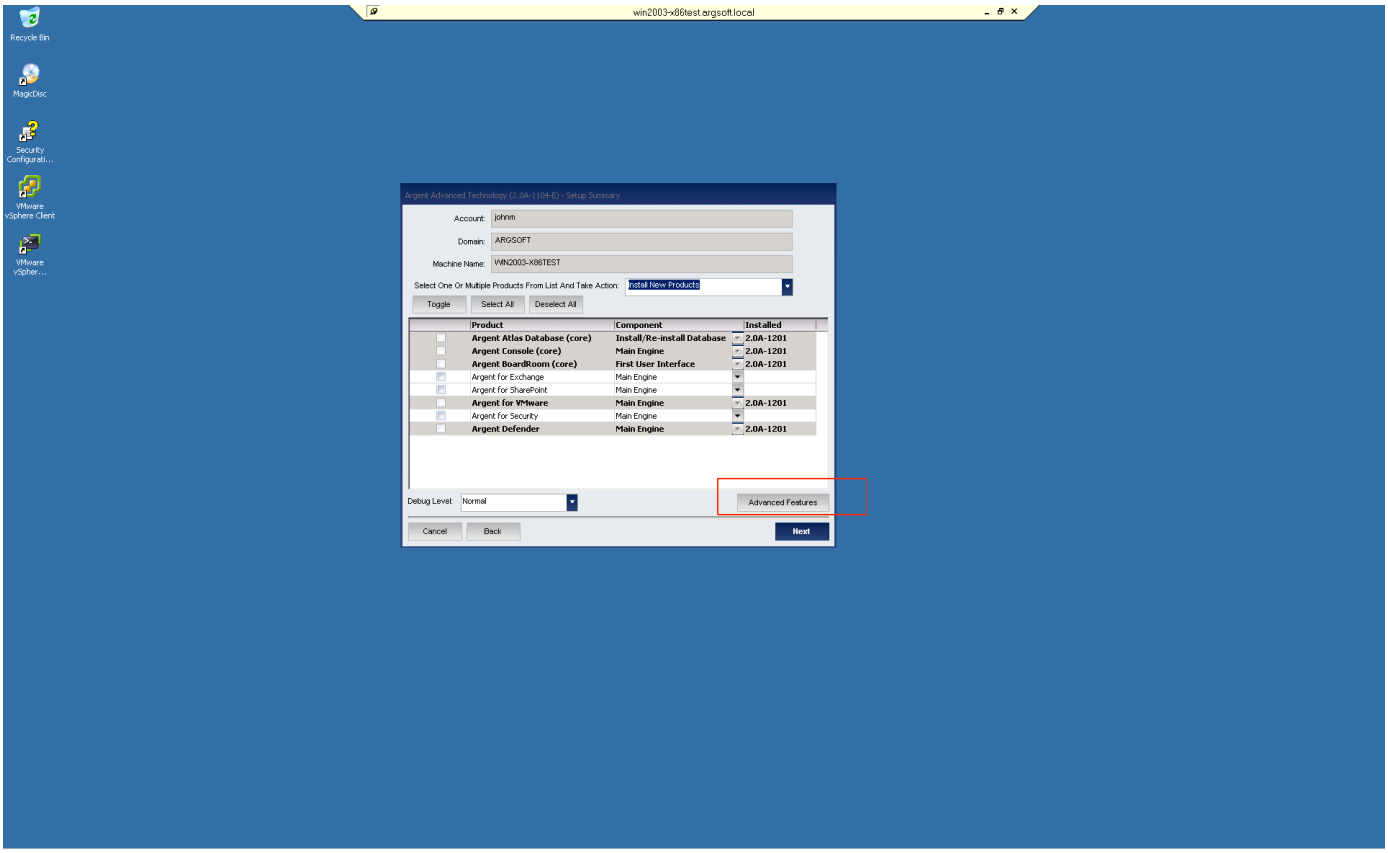
If this is a concern, then customers have the alternative option of using the Argent Event Log Reader service, which compresses the collected logs prior to forwarding them from a remote Engine server to the central Argent database.

Configuring the Argent Event Log Reader

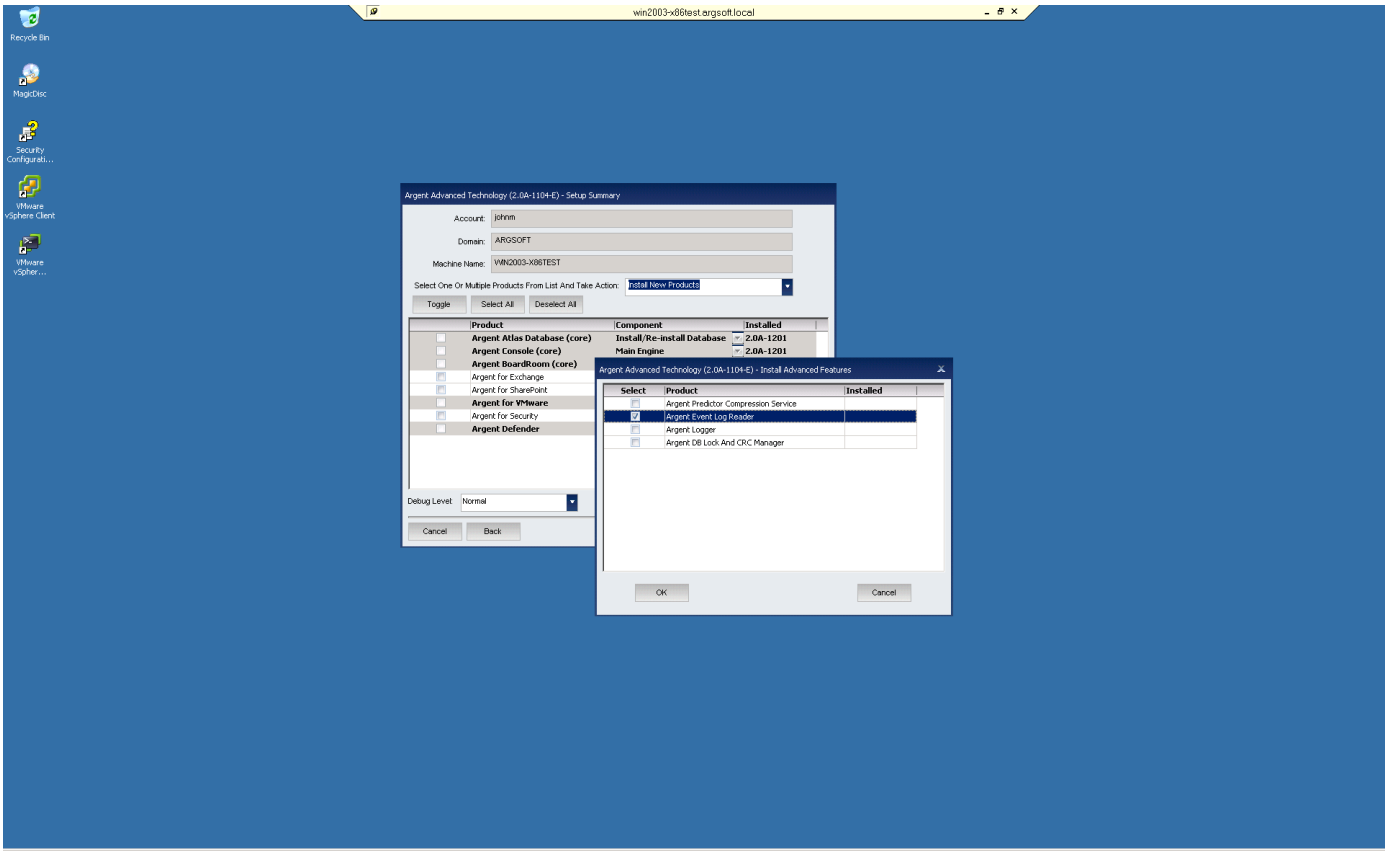
The Argent Event Log Reader service is installed from the Argent AT setup files, however it can be used by both the Argent XT Argent Data Consolidator product or the Argent AT Argent for Security product.

The first step is to launch the Argent AT setup.exe file and install the Argent Event Log Reader service on a remote site server being used to collect logs from servers in that remote office location.

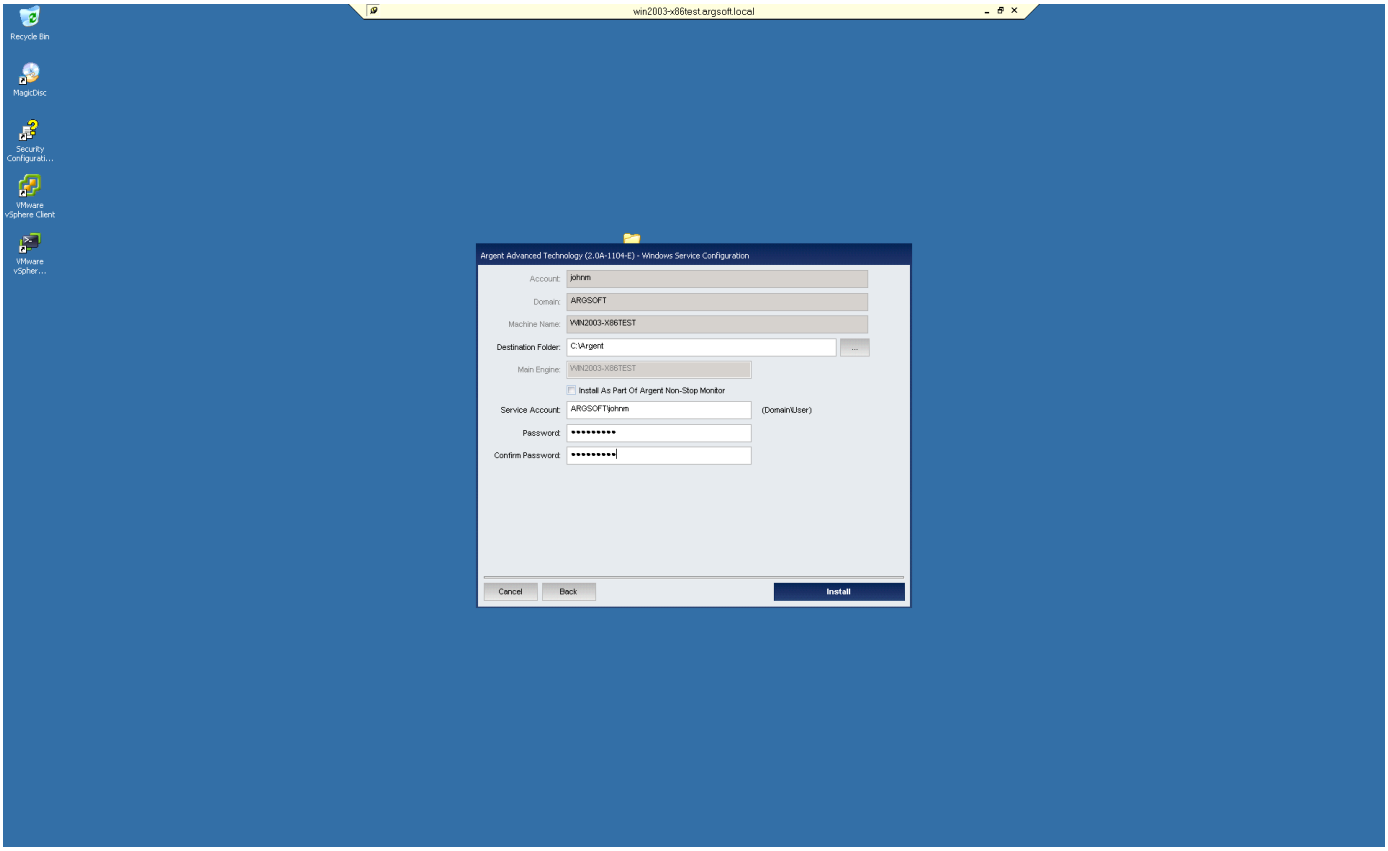
Select the following 'Advanced Feature' button option during the installation wizards:



Select the checkbox for 'Argent Event Log Reader' and click OK:



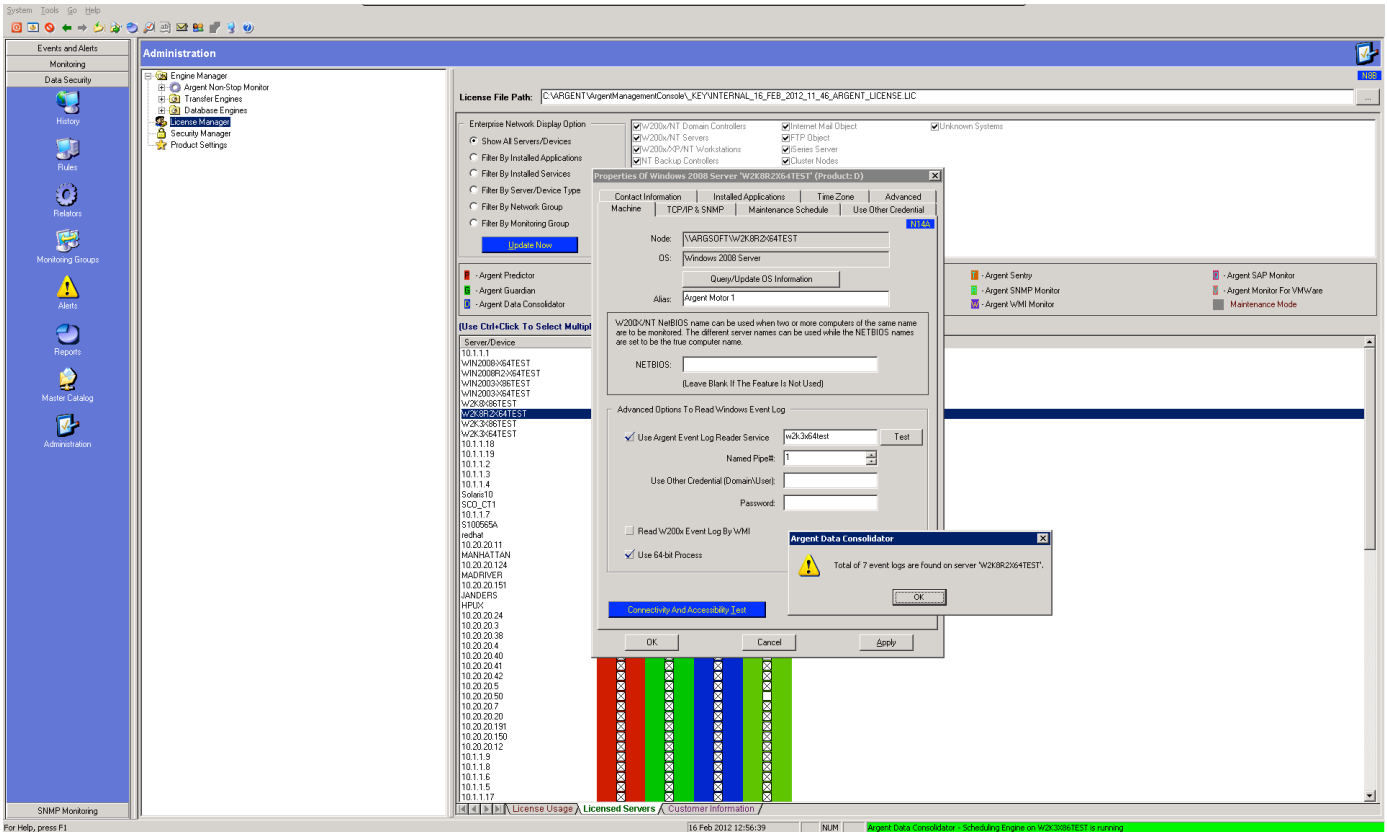
Enter the service account credentials to run the Argent Event Log Reader service.



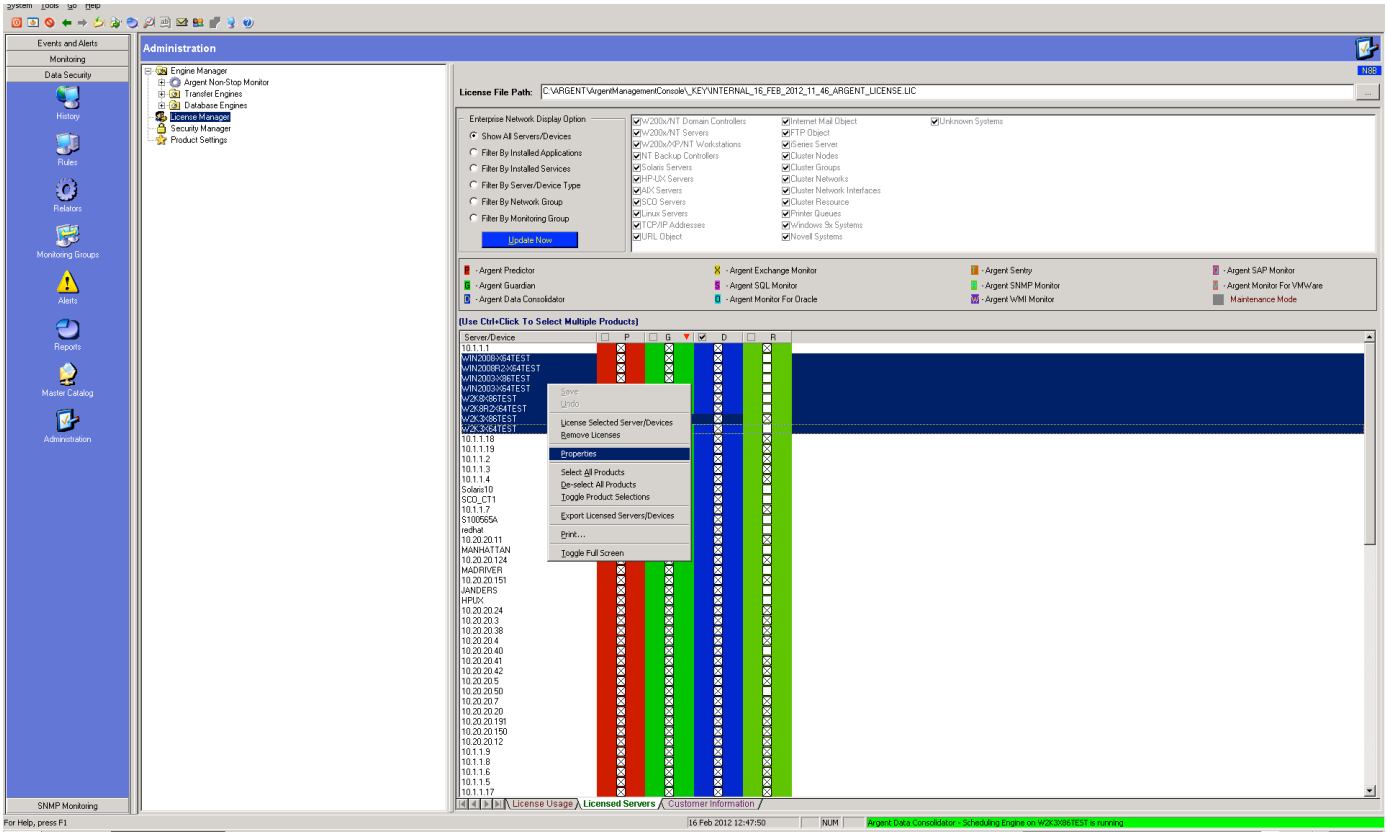
To configure Argent XT Argent Data Consolidator, go to the Node Properties of the monitored servers located in the remote site location.

Select the checkbox option to 'Use Argent Event log Reader Service', and specify the server that you installed the Event Log Reader service on.

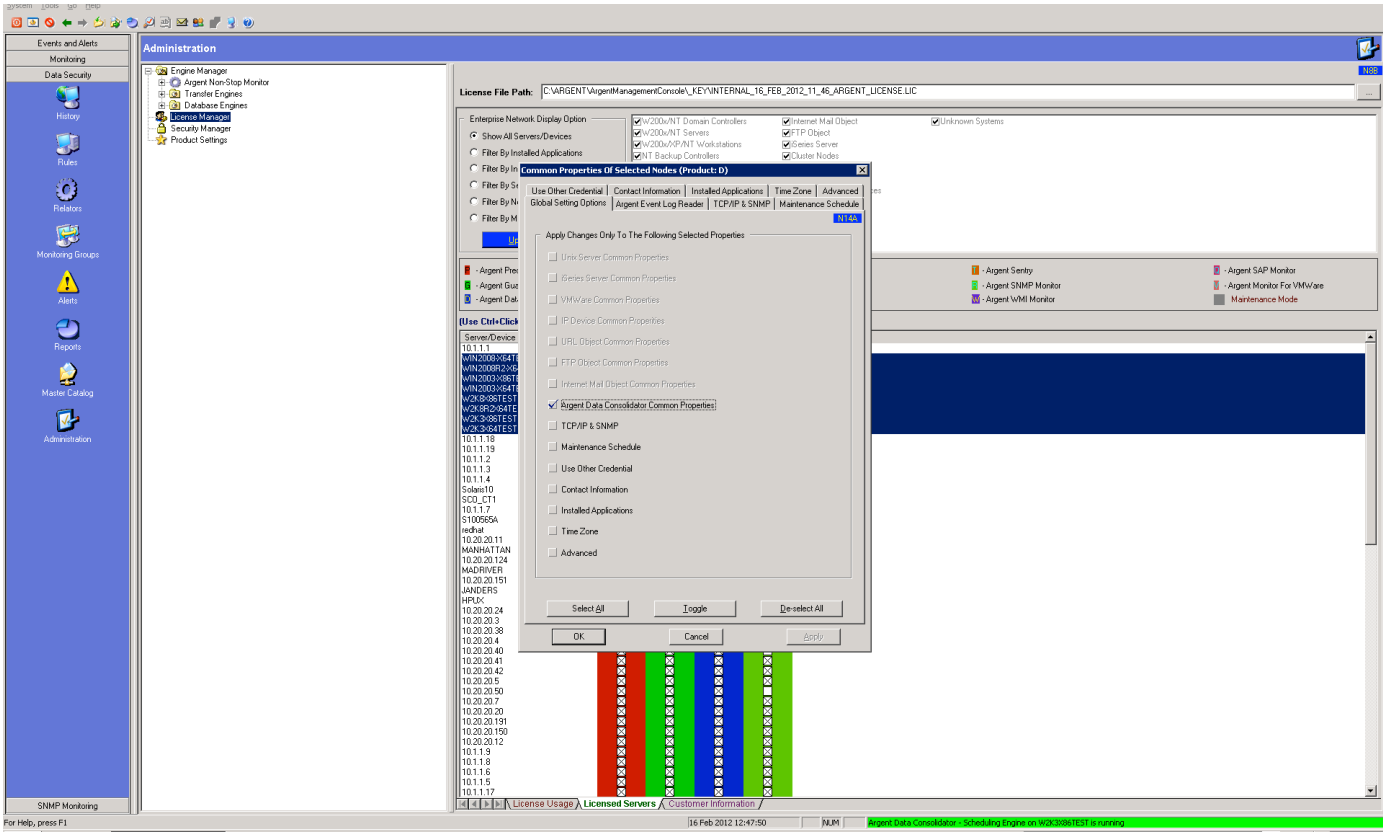
If any of the monitored servers are 64-bit, then it is recommended to install the Argent Event Log Reader service on a 64-bit server. The checkbox option for 'Use 64-bit Process' can then be used, which allows Windows 64-bit Event Log descriptions to be read by the Argent service.



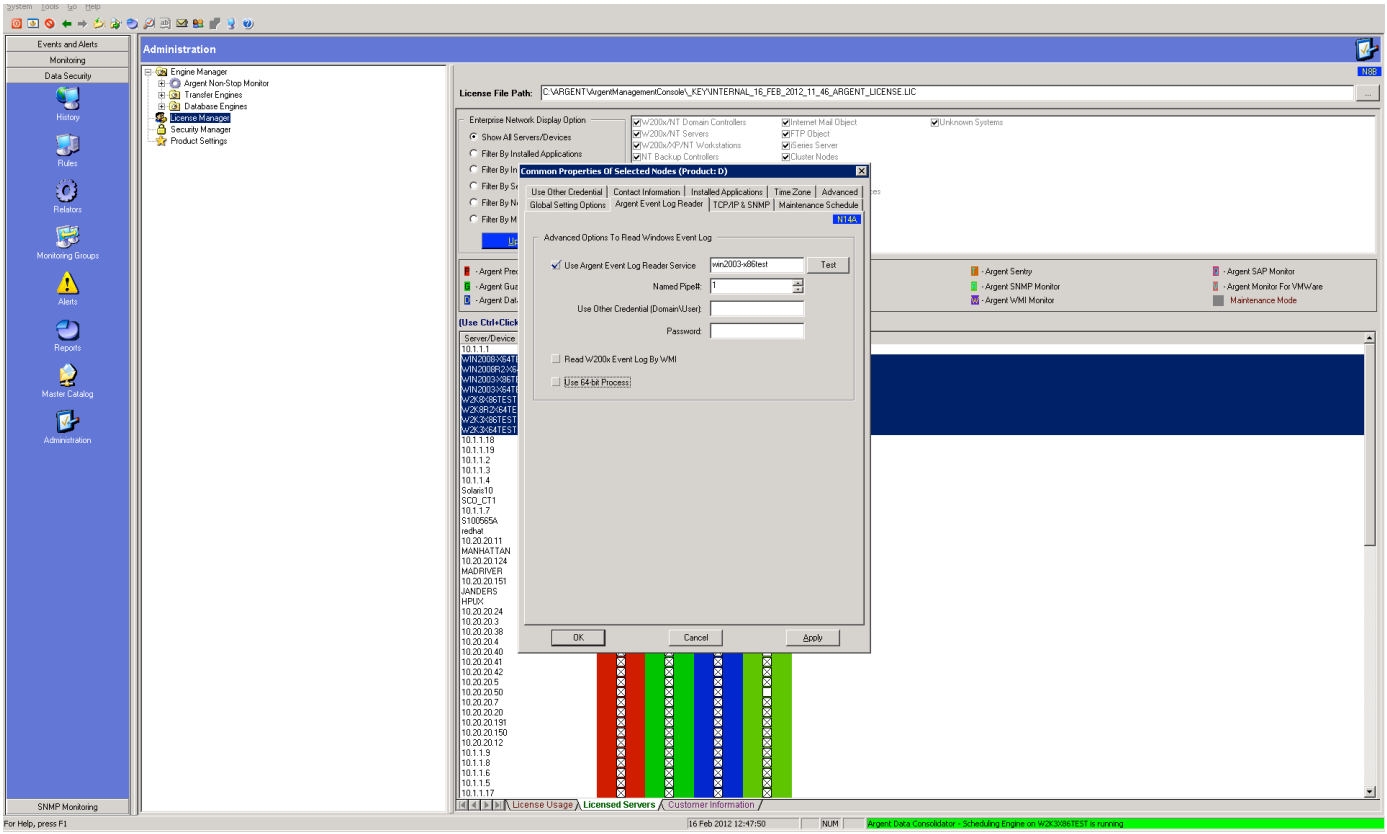
To configure these settings against multiple monitored servers, right-click the select servers and choose the ‘Properties’ option:



Select the checkbox for ‘Argent Data Consolidator Common Properties’:

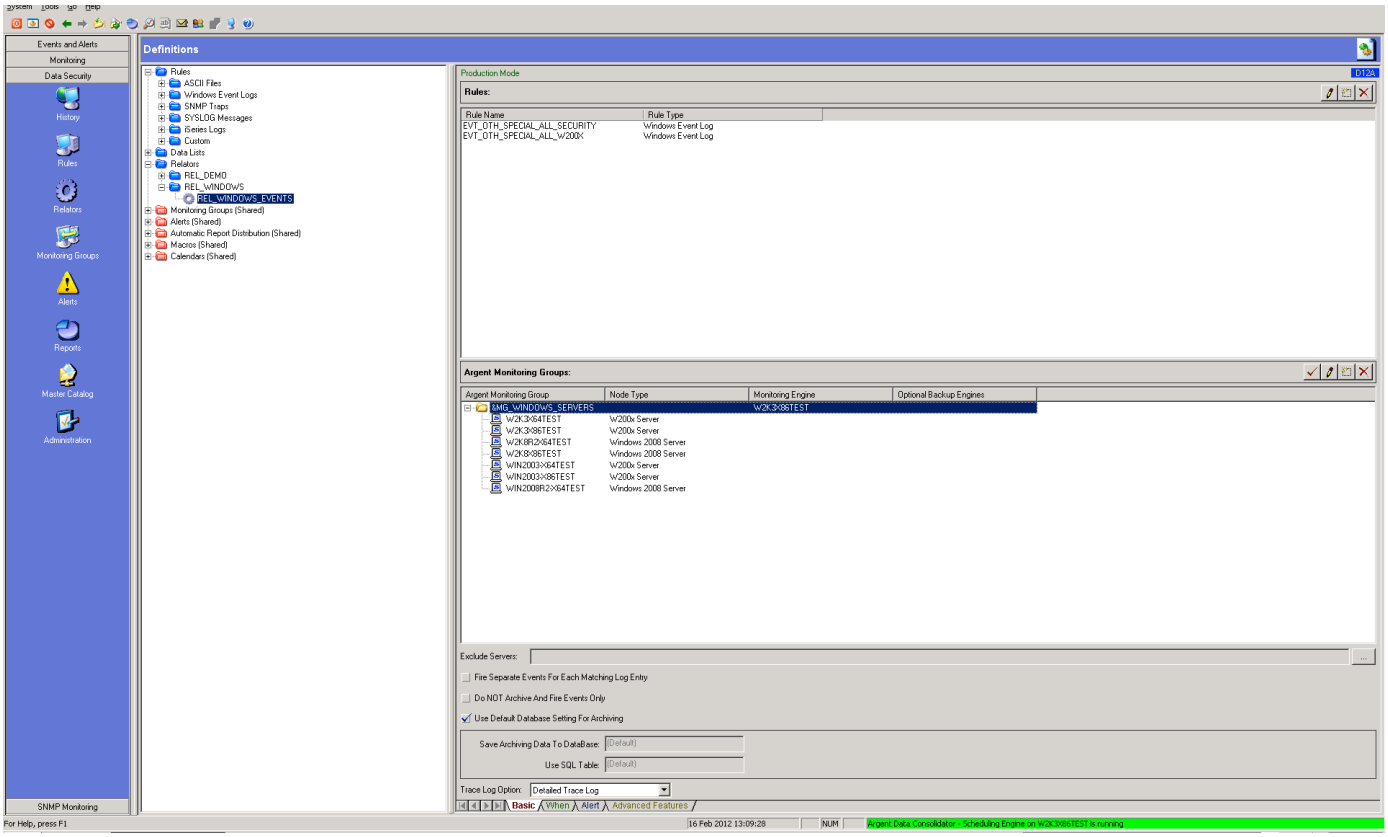


Next use the 'Argent Event Log Reader' tab to specify connectivity to the server running the Event Log Reader service:



Log Rules and Relators can then be executed against the remote site servers.

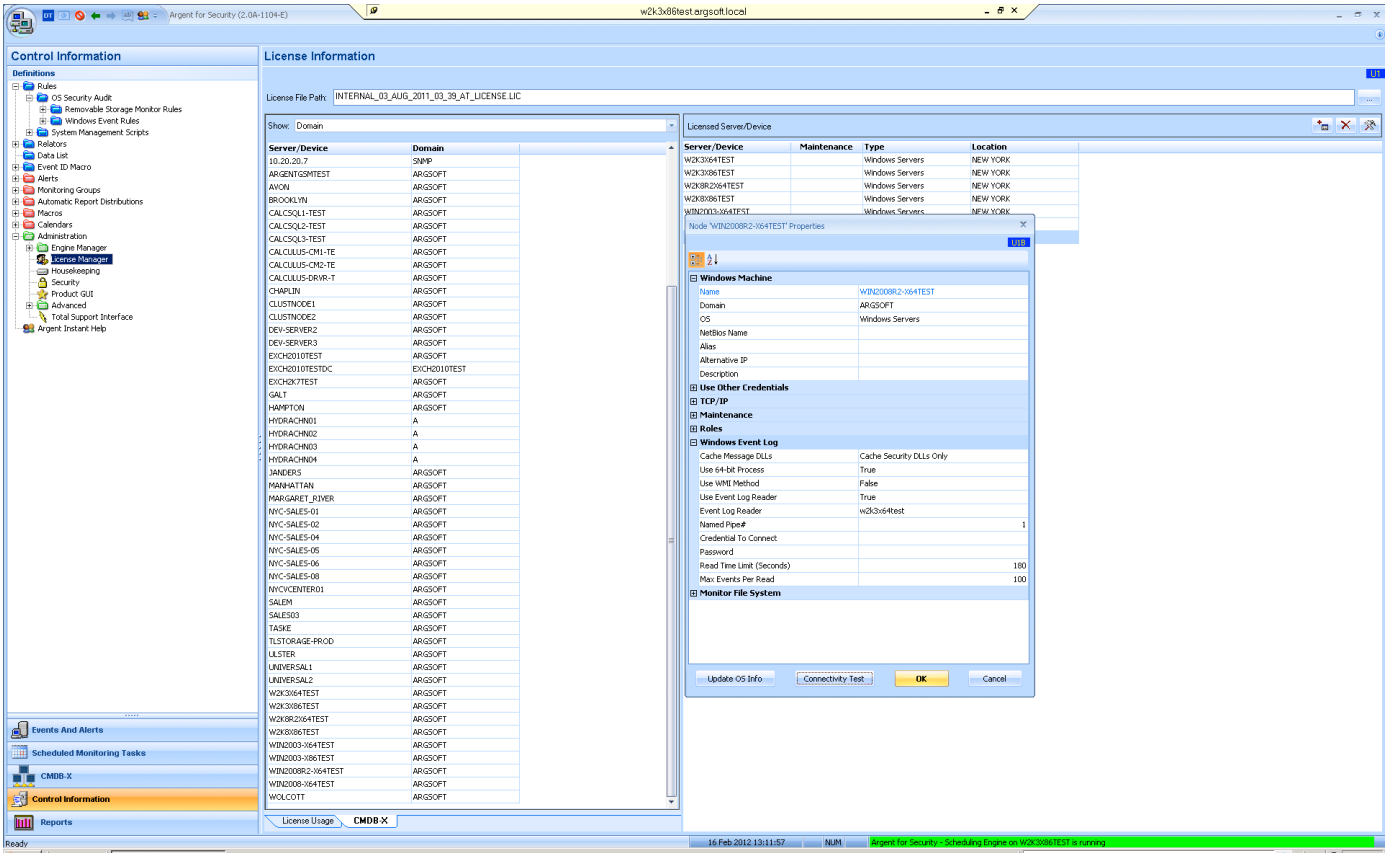
The Event Log Reader server defined in the Node Properties of the servers will collect and compress the logs prior to forwarding them to the central SQL database at the main site location.



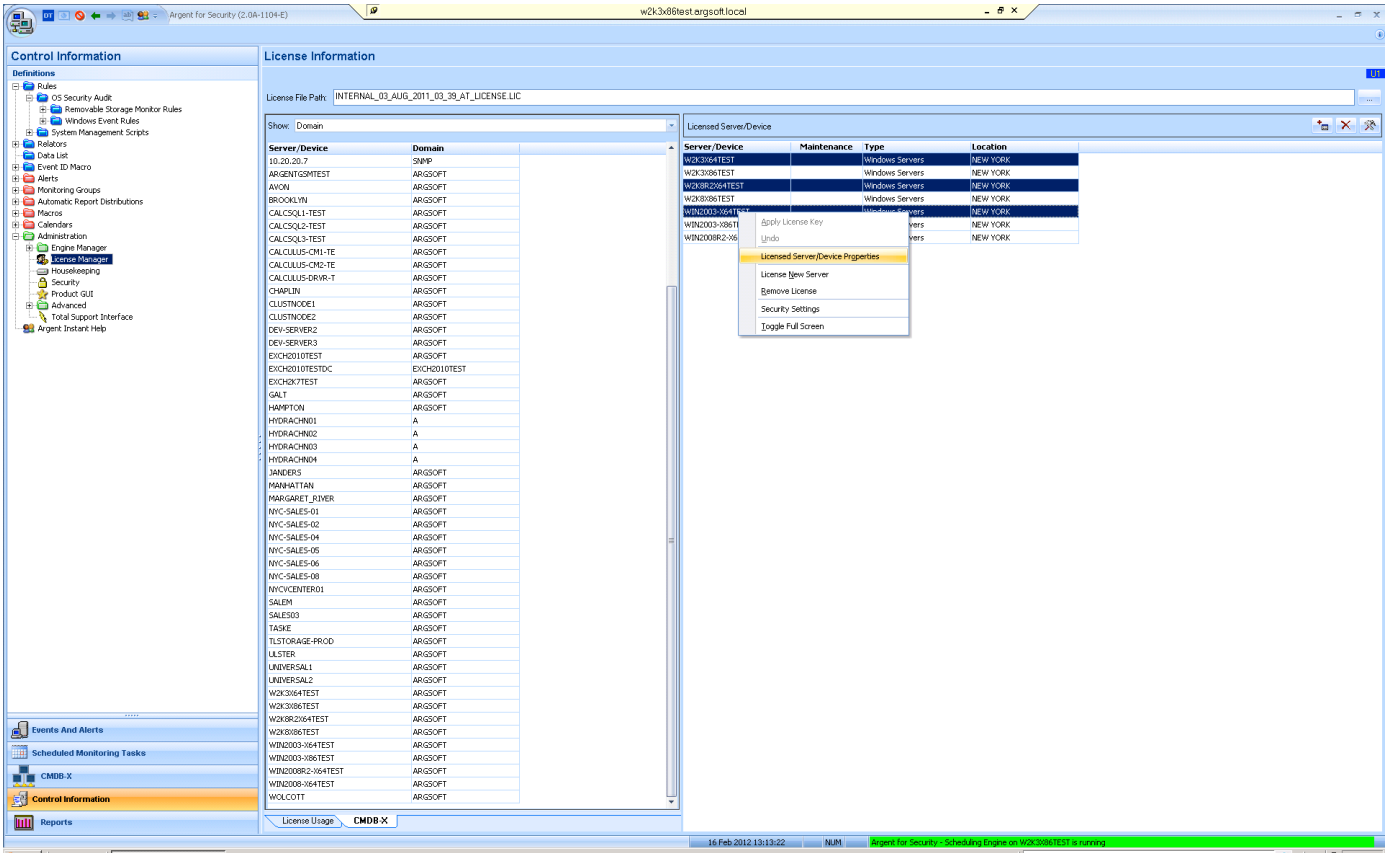
To configure Argent AT Argent for Security, go to the Node Properties of the monitored servers located in the remote site location.

Change the 'Use Argent Event log Reader Service' option to 'True' and specify the server that you installed the Event Log Reader service on.

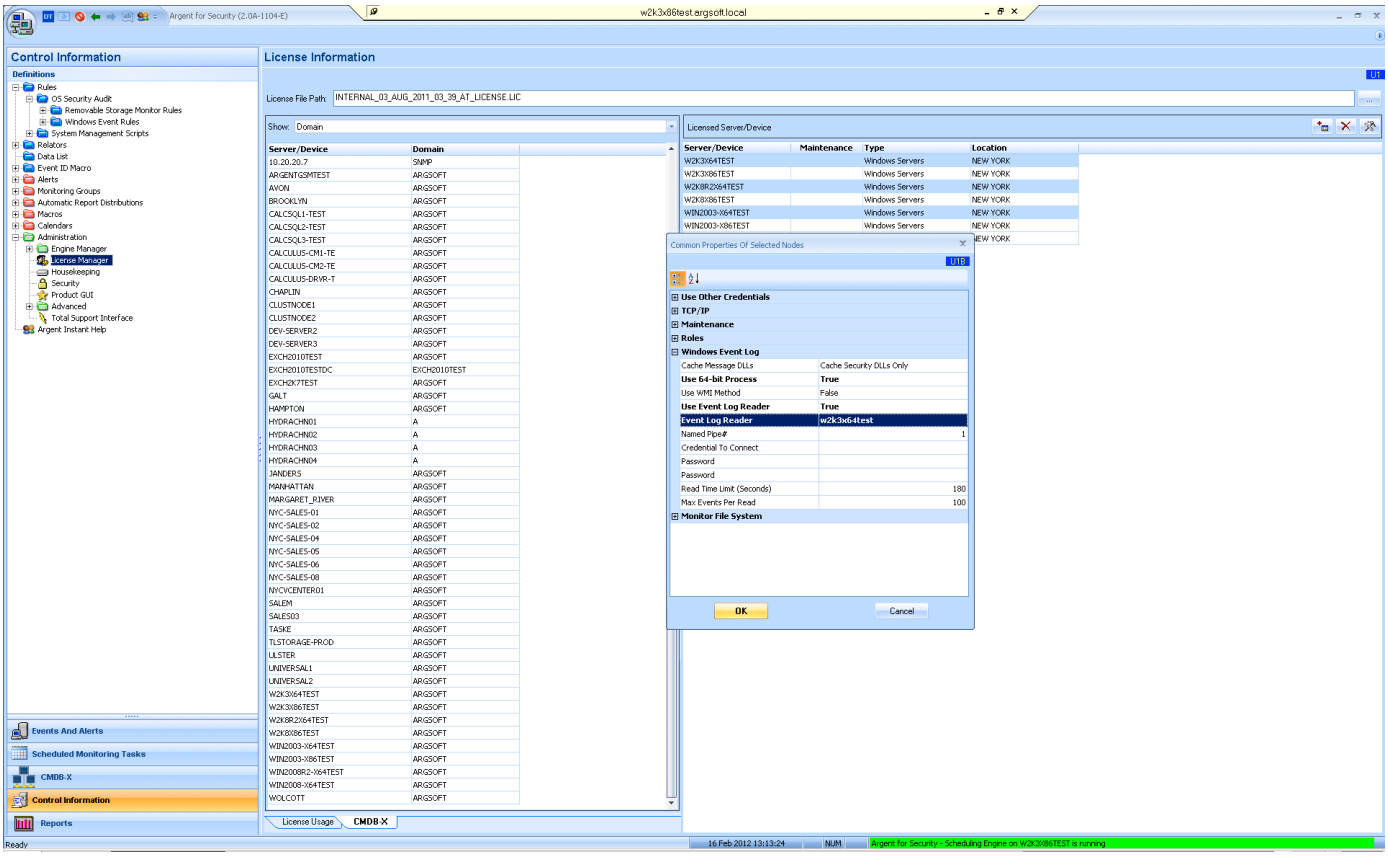
If any of the monitored servers are 64-bit, then it is recommended to install the Argent Event Log Reader service on a 64-bit server. The option for 'Use 64-bit Process' can then be used, which allows Windows 64-bit Event Log descriptions to be read by the Argent service.



To configure these settings against multiple monitored servers, right-click the select servers and choose the 'Licensed Server/ Device Properties' option:



Change the 'Use Argent Event log Reader Service' option to 'True' and specify the server that you installed the Event Log Reader service on.



Log Rules and Relators can then be executed against the remote site servers.

The Event Log Reader server defined in the Node Properties of the servers will collect and compress the logs prior to forwarding them to the central SQL database at the main site location.