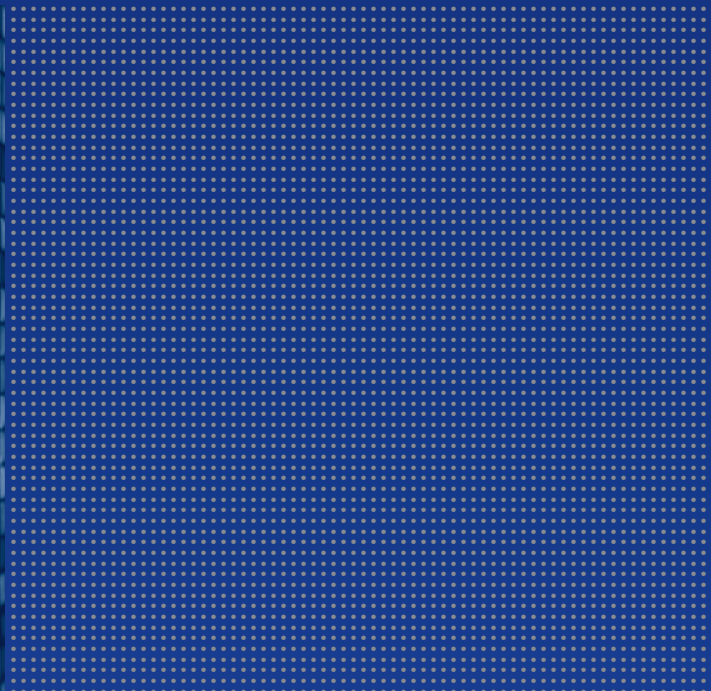


# Reducing Network Utilization When Consolidating Log Events

**A R G E N T**  
ENCYCLOPEDIA



## 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.

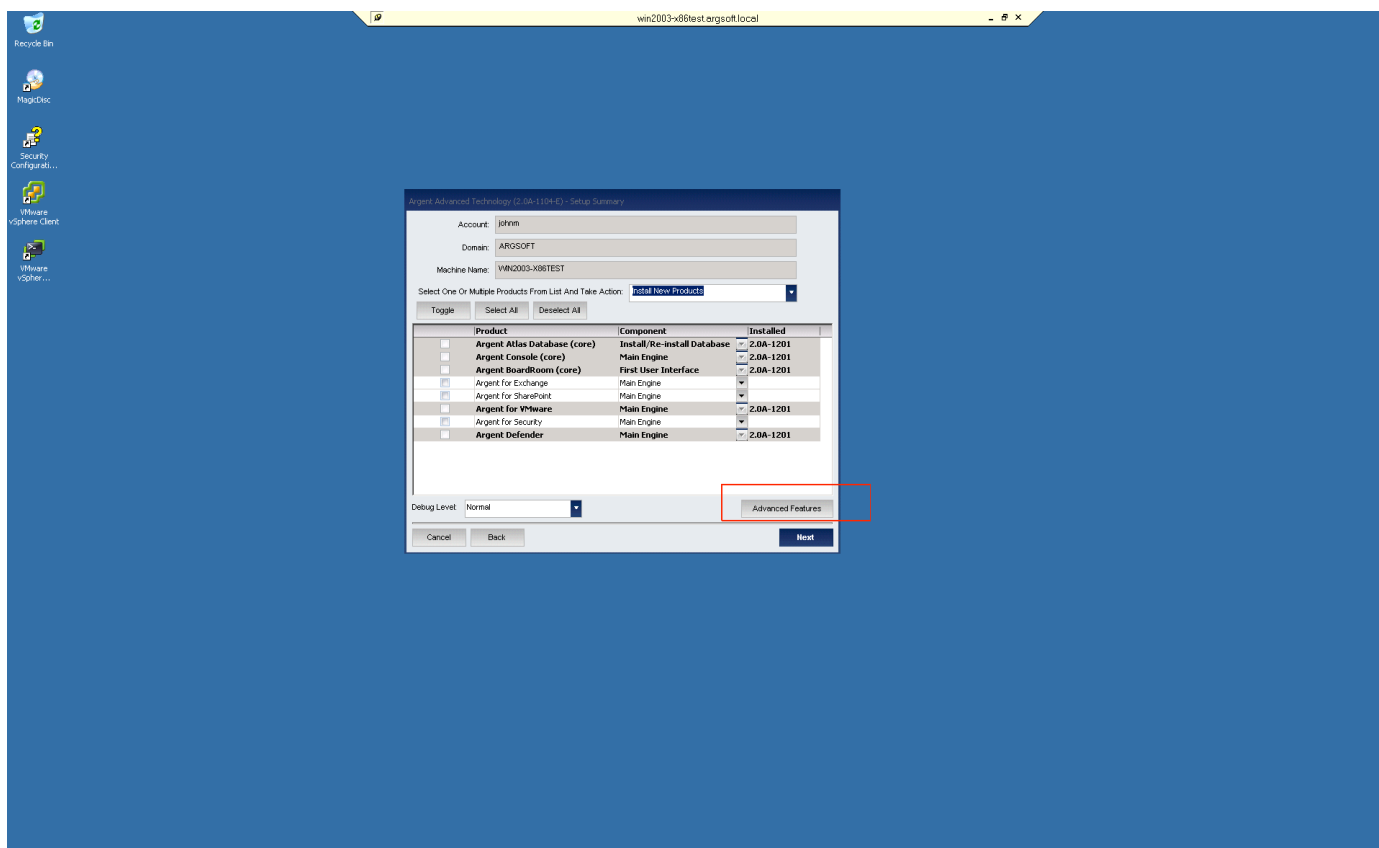
If this is a concern, then customers have the alternative option of using the Argent Event Log Reader service, which compresses the collected logs prior to forwarding them from a remote Engine server to the central Argent database.

## Configuring the Argent Event Log Reader

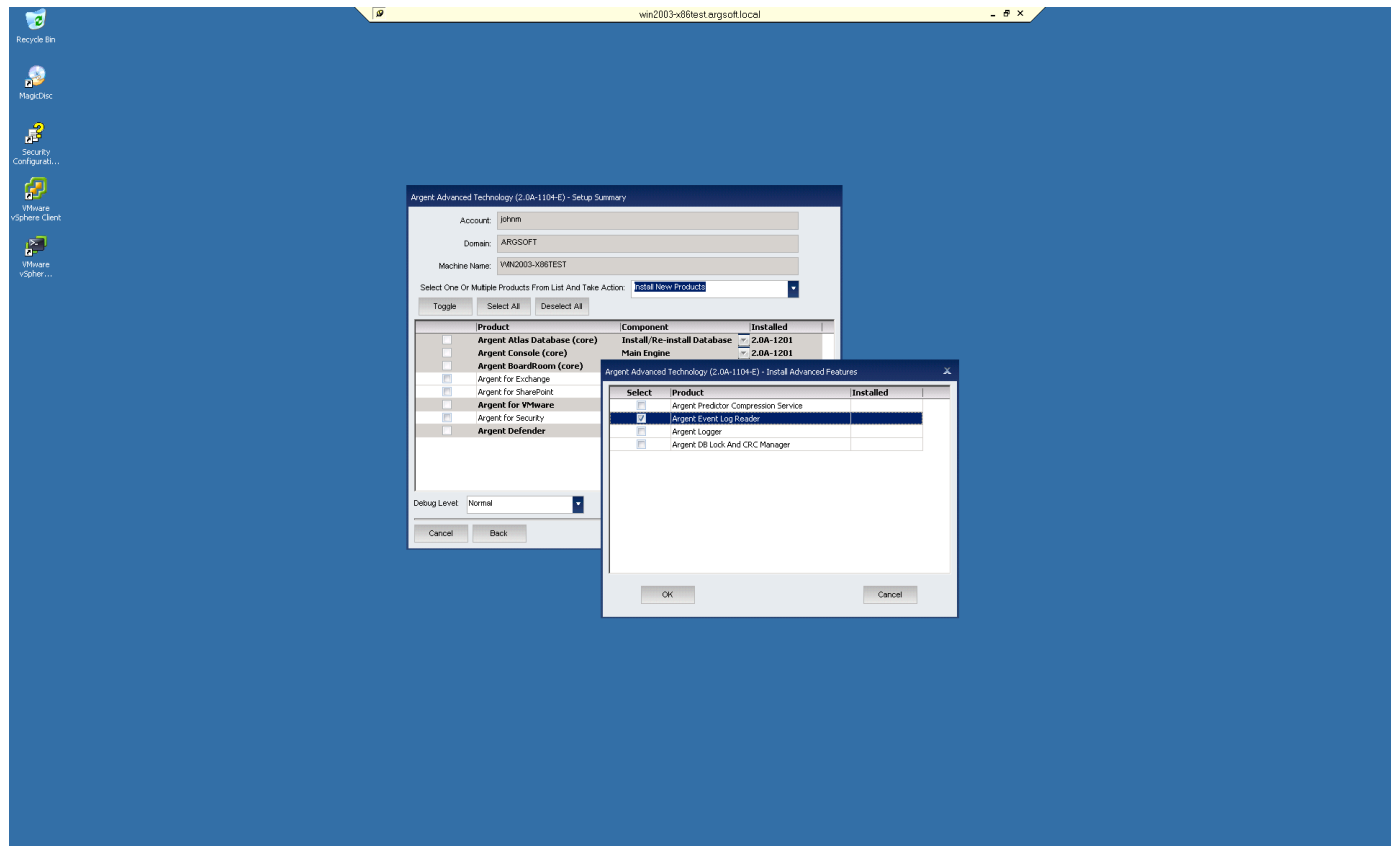
The Argent Event Log Reader service is installed from the Argent AT setup files, however it can be used by both the Argent XT Argent Data Consolidator product or the Argent AT Argent for Security product.

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.

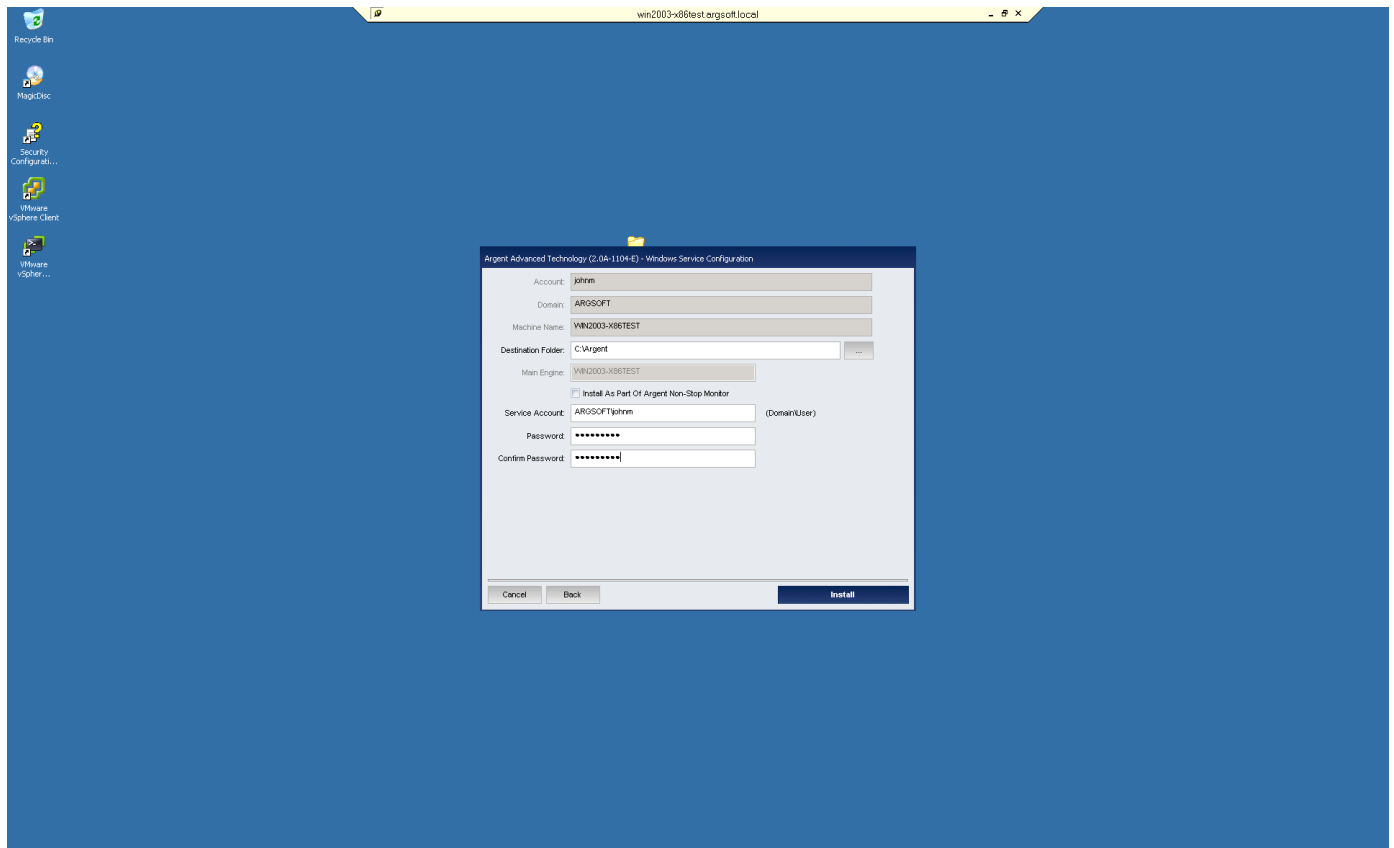
Select the following 'Advanced Feature' button option during the installation wizards:



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



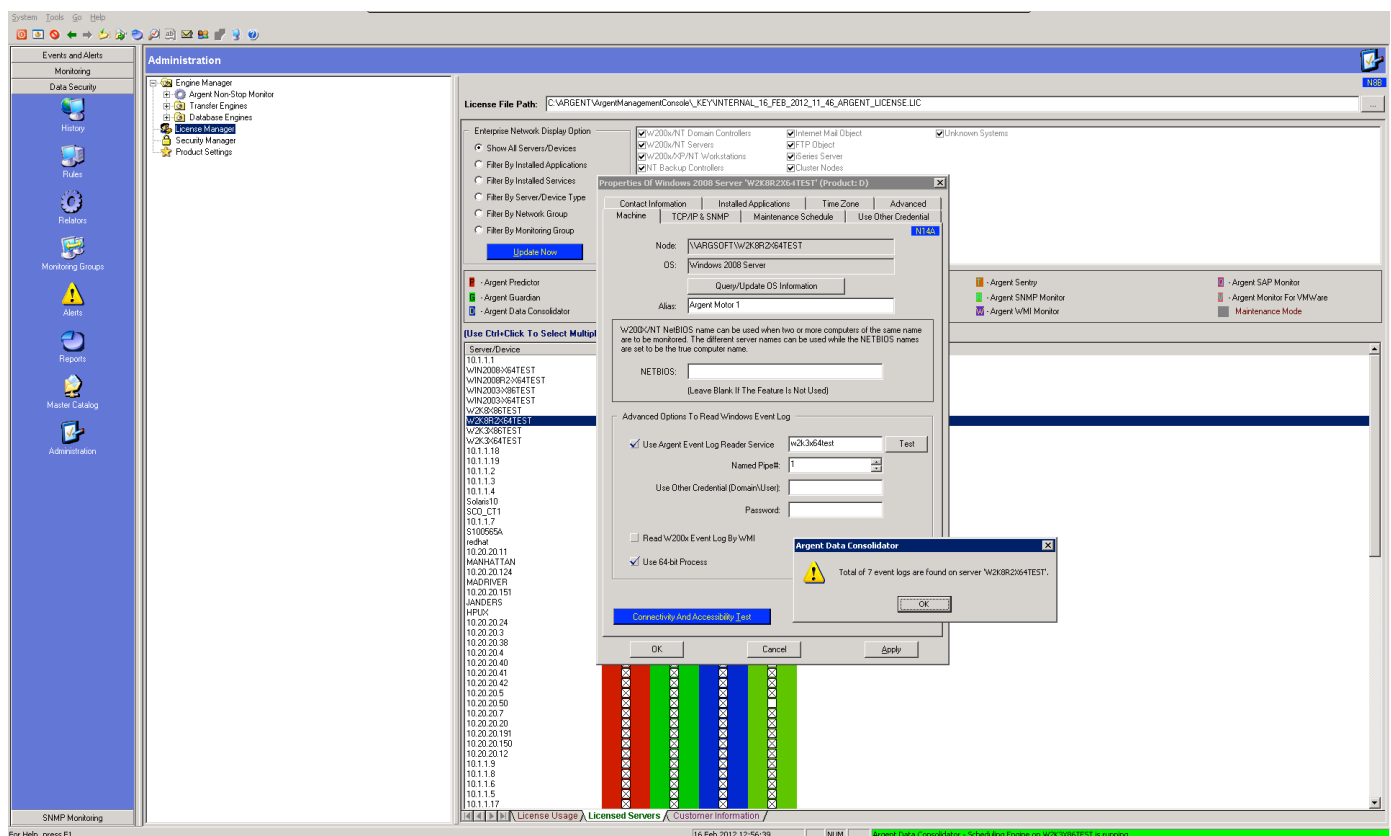
Enter the service account credentials to run the Argent Event Log Reader service.



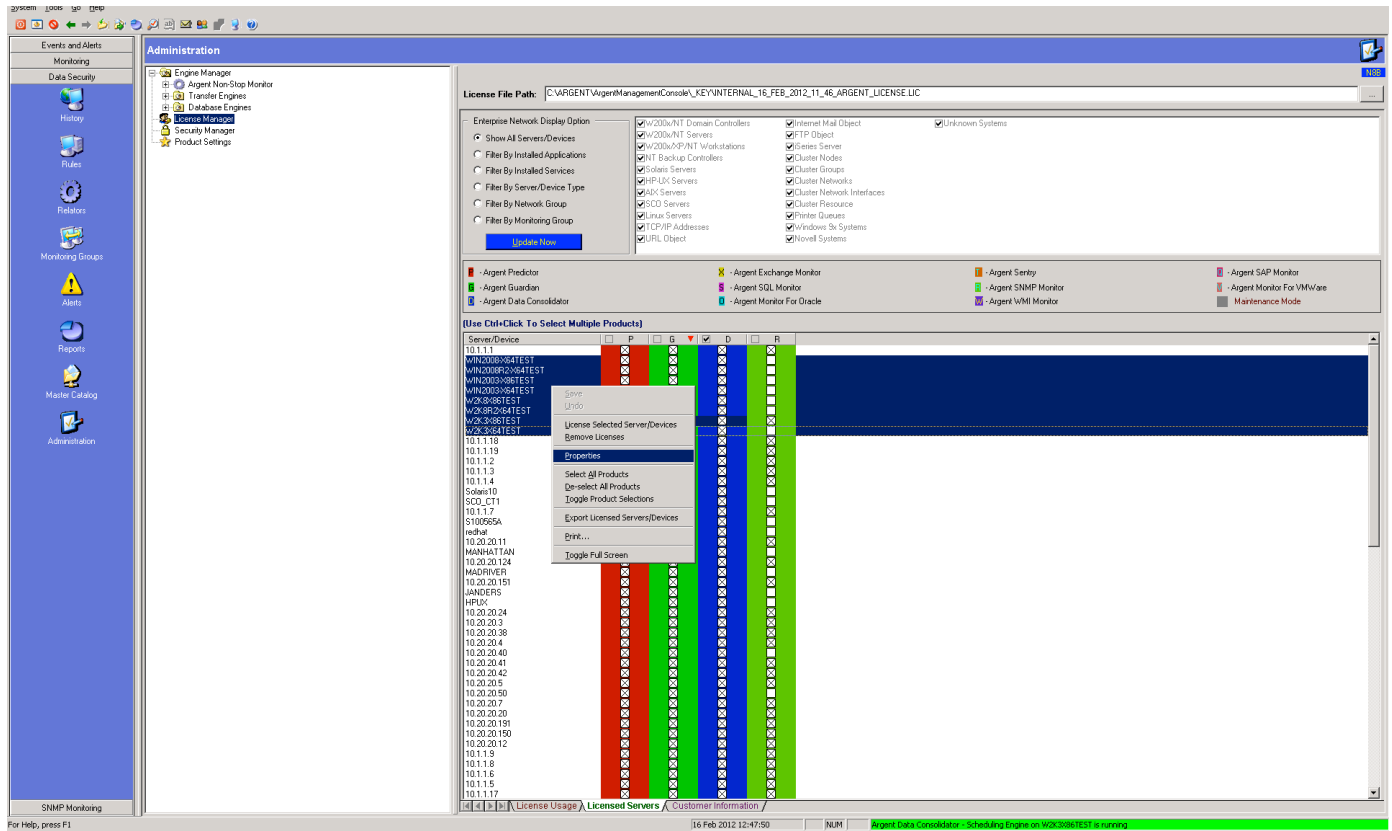
To configure Argent XT Argent Data Consolidator, go to the Node Properties of the monitored servers located in the remote site location.

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.



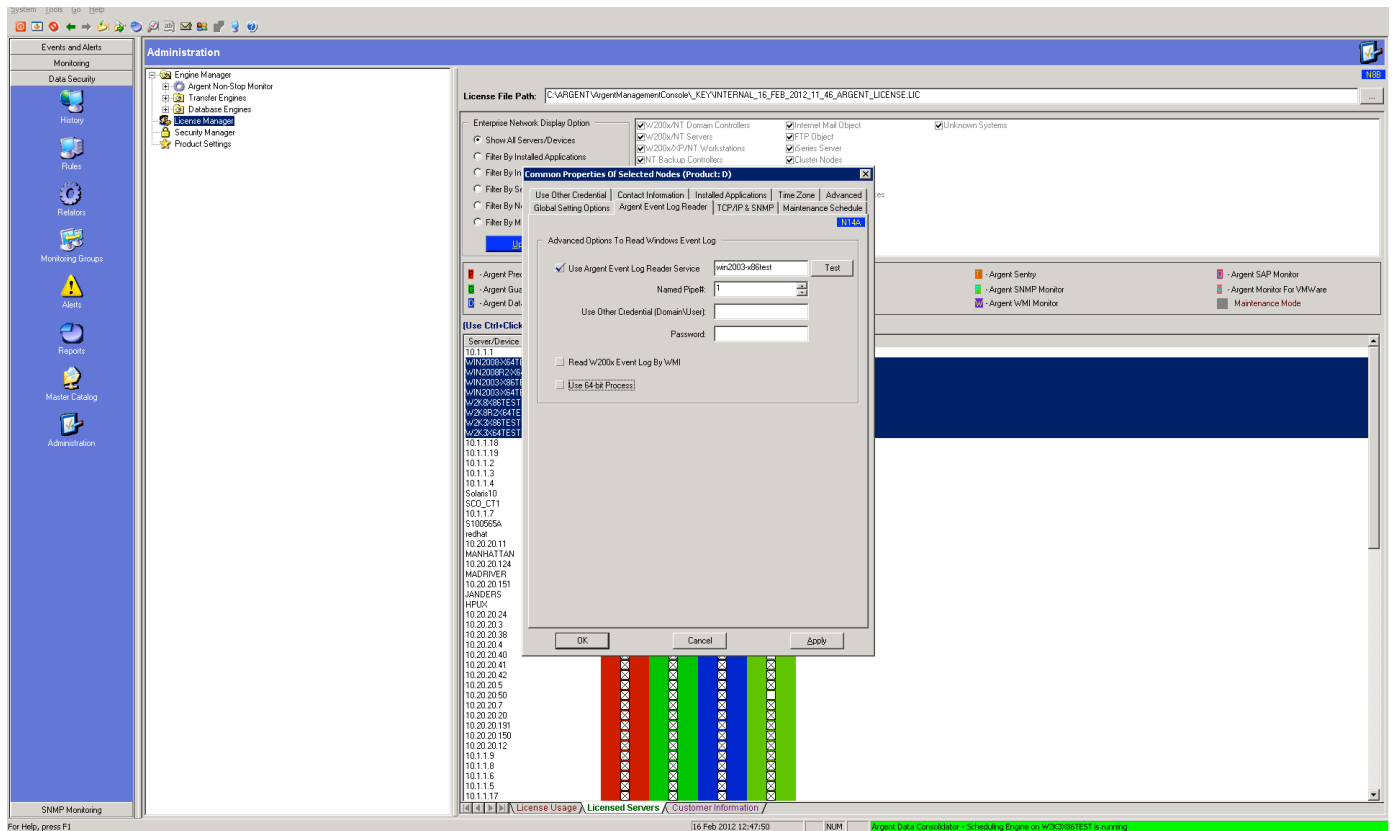
To configure these settings against multiple monitored servers, right-click the select servers and choose the 'Properties' option:



The screenshot displays the Argent Management Console (AMC) interface. The main window is titled 'Administration' and shows a list of servers/devices. A dialog box titled 'Common Properties Of Selected Nodes (ProductID)' is open, displaying a list of properties for the selected nodes. The 'License File Path' is set to 'C:\ARGENT\ArgentManagementConsole\KEY\INTERNAL\_16\_FEB\_2012\_11\_46\_ARGENT\_LICENSE.LIC'. The status bar at the bottom indicates 'Argent Data Consolidator - Scheduling Engine on W2K3-98TEST is running'.

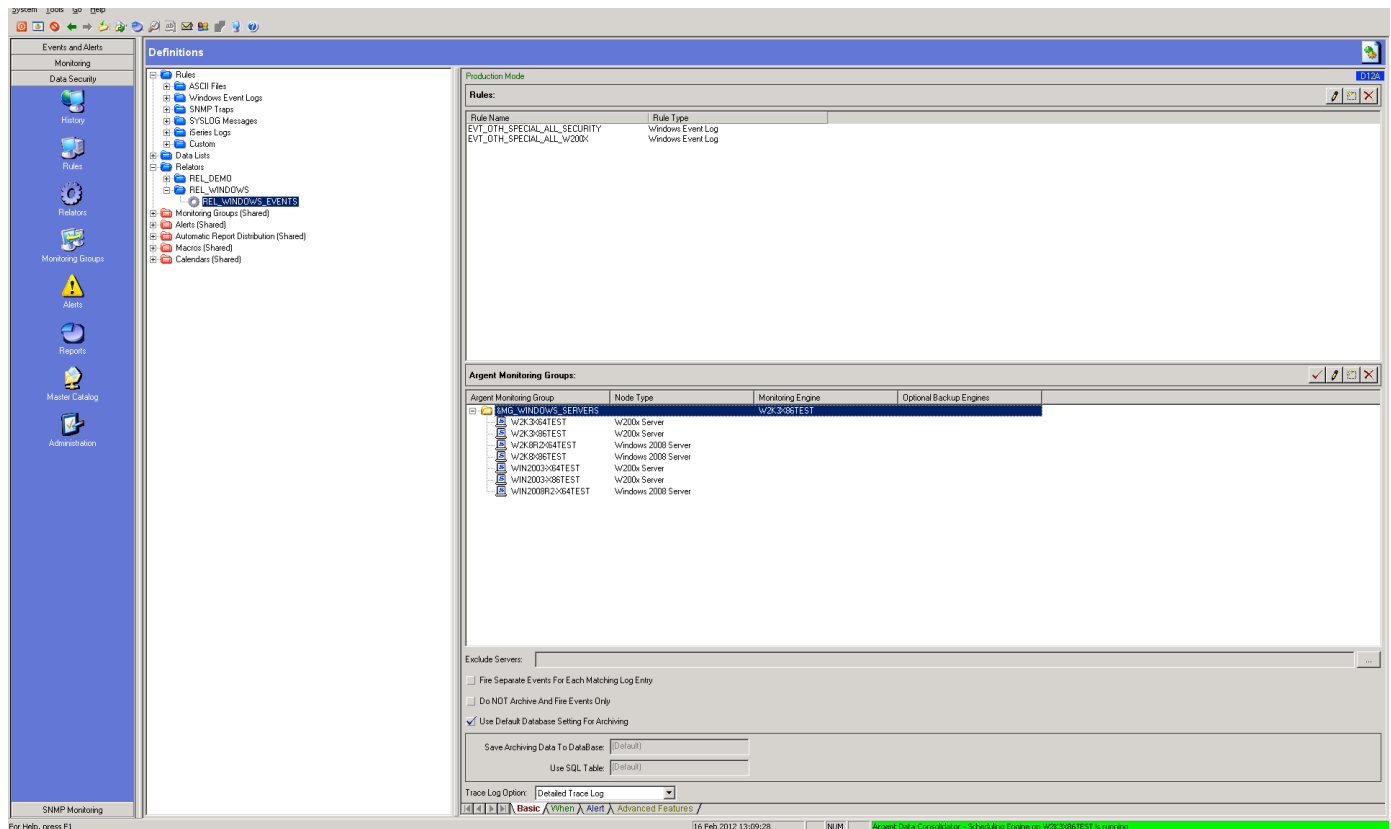


Next use the 'Argent Event Log Reader' tab to specify connectivity to the server running the Event Log Reader service:



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

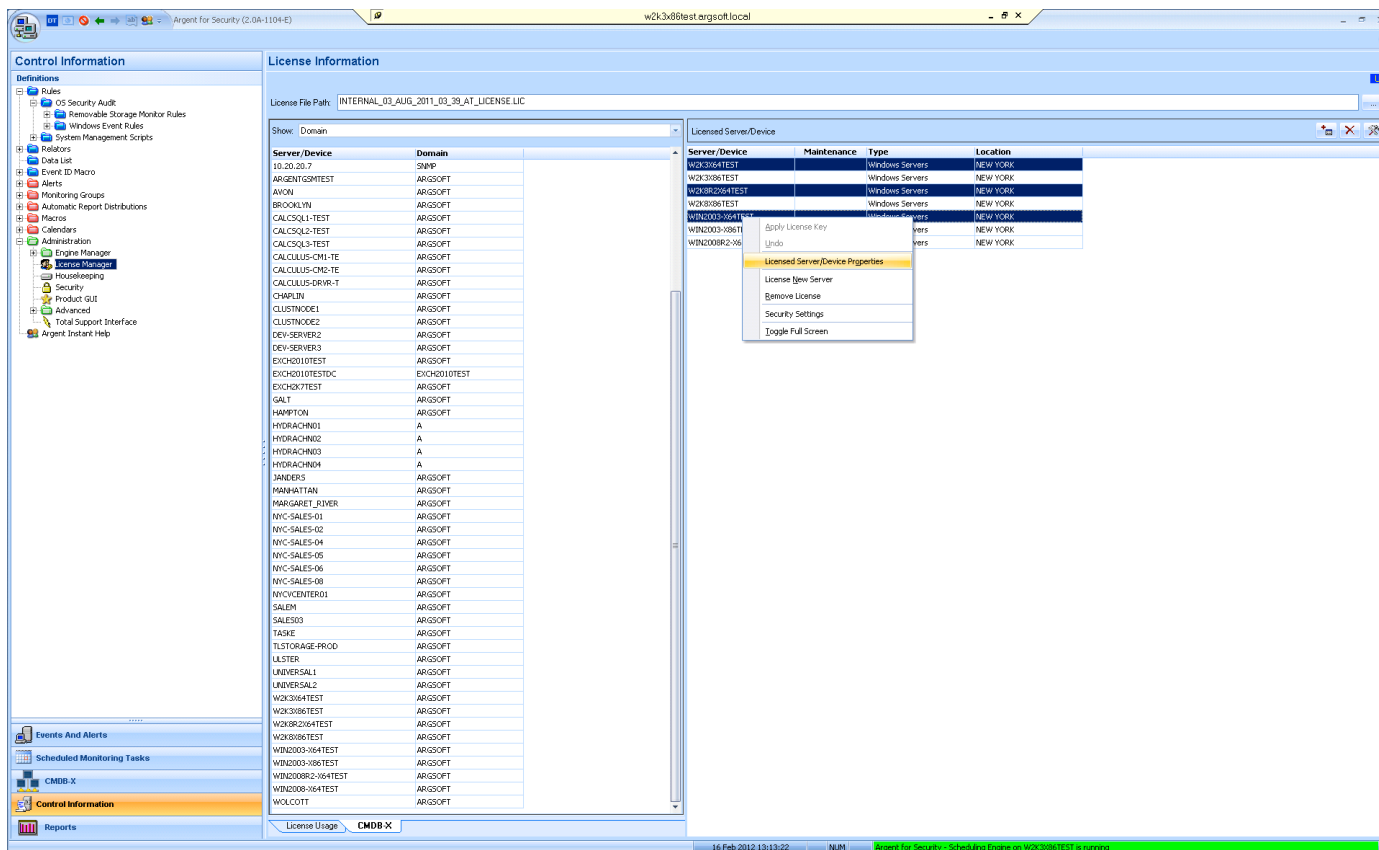
The Event Log Reader server defined in the Node Properties of the servers will collect and compress the logs prior to forwarding them to the central SQL database at the main site location.



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.

The screenshot shows the Argent For Security (2.0A-1104-E) interface. The main window is titled 'w2k3x86test argsoft.local'. The 'License Information' tab is active, displaying a list of servers and their domains. The 'License File Path' is set to 'INTERNAL\_03\_AUG\_2011\_03\_39\_AT\_LICENSE.LIC'. A dialog box titled 'Common Properties Of Selected Nodes' is open, showing the 'Use Event Log Reader' option set to 'True' and the 'Event Log Reader' server set to 'w2k3x86test'.

Server/Device	Domain	Location
10.20.20.7	SNIP	
ARGENTGSMTEST	ARGSOFT	
AVON	ARGSOFT	
BROOKLYN	ARGSOFT	
CALCSQL1-TEST	ARGSOFT	
CALCSQL2-TEST	ARGSOFT	
CALCSQL3-TEST	ARGSOFT	
CALCULUS-CH1-TE	ARGSOFT	
CALCULUS-CH2-TE	ARGSOFT	
CALCULUS-DRW-1	ARGSOFT	
CHARLIN	ARGSOFT	
CLUSTNODE1	ARGSOFT	
CLUSTNODE2	ARGSOFT	
DEV-SERVER2	ARGSOFT	
DEV-SERVER3	ARGSOFT	
EXCH010TEST	ARGSOFT	
EXCH010TESTDC	EXCH010TEST	
EXCH07TEST	ARGSOFT	
GALT	ARGSOFT	
HAPPYON	ARGSOFT	
HYDRACHN01	A	
HYDRACHN02	A	
HYDRACHN03	A	
HYDRACHN04	A	
JANDERS	ARGSOFT	
MANHATTAN	ARGSOFT	
MARGARET_RIVER	ARGSOFT	
NYC-SALES-01	ARGSOFT	
NYC-SALES-02	ARGSOFT	
NYC-SALES-04	ARGSOFT	
NYC-SALES-05	ARGSOFT	
NYC-SALES-06	ARGSOFT	
NYC-SALES-08	ARGSOFT	
NYCVCENTER01	ARGSOFT	
SALEM	ARGSOFT	
SALES03	ARGSOFT	
TASKE	ARGSOFT	
TLSTORAGE-PROD	ARGSOFT	
ULSTER	ARGSOFT	
UNIVERSAL1	ARGSOFT	
UNIVERSAL2	ARGSOFT	
W2K3x64TEST	ARGSOFT	
W2K3x86TEST	ARGSOFT	
W2K3x86TEST	ARGSOFT	
W2K3x86TEST	ARGSOFT	
W2K3x86TEST	ARGSOFT	
WIN2003-x64TEST	ARGSOFT	
WIN2003-x86TEST	ARGSOFT	
WIN2008R2-x64TEST	ARGSOFT	
WIN2008-x64TEST	ARGSOFT	
WOLCOTT	ARGSOFT	

Server/Device	Maintenance	Type	Location
W2K3x64TEST		Windows Servers	NEW YORK
W2K3x86TEST		Windows Servers	NEW YORK
W2K3x86TEST		Windows Servers	NEW YORK
W2K3x86TEST		Windows Servers	NEW YORK
WIN2003-x64TEST		Windows Servers	NEW YORK
WIN2003-x86TEST		Windows Servers	NEW YORK

**Common Properties Of Selected Nodes**

- ☐ Use Other Credentials
- ☐ TCP/IP
- ☐ Maintenance
- ☐ Roles
- ☐ Windows Event Log
  - Cache Message DLLs: Cache Security DLLs Only
  - Use 64-bit Process: True
  - Use WRE Method: False
  - Use Event Log Reader: True
  - Event Log Reader: w2k3x86test
  - Named Pipe#: 1
  - Credential To Connect:
  - Password:
  - Read Time Limit (Seconds): 180
  - Max Events Per Read: 100
- ☐ Monitor File System

Buttons: OK, Cancel

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.

**Control Information**

**Definitions**

- Rules
  - OS Security Audit
  - Removable Storage Monitor Rules
  - Windows Event Rules
    - EVT\_APPLICATION\_LOG
    - EVT\_AUDITING\_CLEARED
    - EVT\_AUDITING\_STOPPED
    - EVT\_HACKER\_ATTACK
    - EVT\_RIGHTS\_CHANGE\_LOGON
    - EVT\_RIGHTS\_CHANGE\_USER
    - EVT\_SECURITY\_LOG\_ARCHIVE
  - System Management Scripts
- Relators
  - Data Consolidating
    - REL\_WINDOWS\_SERVERS (Test Mode)**
  - Domain Controller Audit
  - Removable Storage Audits
  - Data List
  - Event ID Macro
  - Alerts
  - Monitoring Groups
    - DEMO\_IS\_SERVERS
    - EXCHANGE
    - LOCAL
      - BMS\_DC
      - BMS\_DEMO
      - BMS\_WINDOWS
      - BMS\_WINDOWS\_SERVERS
    - SHAREPOINT
    - SNMP
    - VMWARE
  - Automatic Report Distributions
  - Macros
  - Calendars
  - Administration
    - Engine Manager
    - License Manager
    - Housekeeping
    - Security
    - Product GUI
    - Advanced
    - Total Support Interface
    - Argent Instant Help

**Relator Definition: REL\_WINDOWS\_SERVERS (Test Mode)**

Relator In Test Mode Will Not Be Scheduled Until Changed To Production Mode

**Prerequisite Rules - All These Rules Must Pass For Main Rules To Run On Mode:**

Rule	Type	Instant Correction	Alert	Root Cause Analysis
EVT_SECURITY_LOG_ARCHIVE	Windows Event		Always	No
EVT_APPLICATION_LOG	Windows Event		Always	No

**Main Rules:**

Rule	Type	Instant Correction	Alert	Root Cause Analysis
EVT_SECURITY_LOG_ARCHIVE	Windows Event		Always	No
EVT_APPLICATION_LOG	Windows Event		Always	No

**Monitoring Group List**

Monitoring Group	Node Type	Excluded	Monitoring Engine	Backup Monitoring Engines	Use Local If Installed
BMS_WINDOWS_SERVERS	Windows Servers	<input checked="" type="checkbox"/>	W2K3/86TEST		<input checked="" type="checkbox"/>
W2K3/64TEST	Windows Servers	<input checked="" type="checkbox"/>			
W2K3/86TEST	Windows Servers	<input checked="" type="checkbox"/>			
WIN2003/64TEST	Windows Servers	<input checked="" type="checkbox"/>			
WIN2003/86TEST	Windows Servers	<input checked="" type="checkbox"/>			
WIN2003/64TEST	NOT Licensed	<input checked="" type="checkbox"/>			
W2K3/86TEST	Windows Servers	<input checked="" type="checkbox"/>			

**How To Run Monitoring Tasks**

☐ Spawn New Monitor Engine Process

☒ Use Shared Monitor Engine Process In Pool : (Dynamic)

**What To Run (Rules)** **When To Run (Schedule)** **What To Do (Alerts)**

Ready 16 Feb 2012 14:05:13 N/A Argent for Security - Scheduling Engine on W2K3/86TEST is running