

86456

VistaNET[®] 5.06 Release Notes

Version: 5.06
Release Date: March 2015
Type of Release: Production Release

Lentronics Multiplexers

JungleMUX SONET Multiplexers,
TN1U and TN1Ue SDH Multiplexers,
T1MX, E1MX and E1MXe Multiplexers



Copyright © GE Multilin 2015, All Rights Reserved

The copyright of this document is the property of GE Multilin. This document must not be copied, reprinted or reproduced in any material form, either wholly or in part, without the written consent of GE Multilin.

GE Multilin reserves the right to make changes and modifications to any part of this document without notice.

GE Multilin is not responsible for any damages or losses incurred as a result of out-of-date or incorrect information contained in this document.



TABLE OF CONTENTS

Table of Contents	2
Release Summary	4
Product/Component	4
Requirements	4
Release Details	5
New Features	5
SNMP Support	5
CSSU (Cyber-Secure Service Unit) Support	9
Activity Log	14
License Expiration Notification.....	16
Important Remarks	17
Management of the VistaNET Services	17
Firewall.....	19
Windows Firewall.....	19
Windows Server 2008 Firewall.....	19
Software Upgrade Procedure.....	22
Required software before upgrade.....	22
Upgrading from VistaNET version 2.25 or lower.....	22
Upgrading from VistaNET version 3.xx.....	22
Steps to upgrade VistaNET from 3.xx to 4.05.....	22
Installing VistaNET version 5.06 or Upgrading from VistaNET version 4.xx	23
Steps to INSTALL VISTANET 5.06 or upgrade VistaNET from 4.xx.....	23
Upgrading IPSU.....	24
Licensing and Activating VistaNET 5.0x	25
License File (*.lic)	25
Licensing VistaNET.....	26
Activation PIN	27
Activating VistaNET	27
Activation via a PIN	27
Activation via Synchronization	28
Activation via secure .db3	29
Licensing and Activation Notes	29
Replacing an Administrator Account.....	29
Expiration of License or Activation PIN	30



Impact of expiration	30
Replacing an Expried License File or Add a new License	31
User Authentication	32
Administrating Users	32
Domain Selection	35
Limitations.....	36
Non-VistaNET issues.....	37
Known Deficiencies	38
Fixed Deficiencies	42
Fixed Deficiencies - VERIFYING.....	42



RELEASE SUMMARY

PRODUCT/COMPONENT

- VistaNET version 5.06.15800

REQUIREMENTS

VistaNET version 5.06 requires the following components to be installed:

- Microsoft .NET Framework 4

VistaNET version 5.06 may be installed on to any of the following operating systems

- Windows 7 OS (recommended)
- Windows Server 2008 and Windows Vista are also supported¹

Note: Windows XP Service Pack 3 is NOT Supported.

¹ For install procedure please contact Customer Support or refer to Windows Server 2008 or Windows Vista / Windows 7 OS installation sections in this document.



RELEASE DETAILS

NEW FEATURES

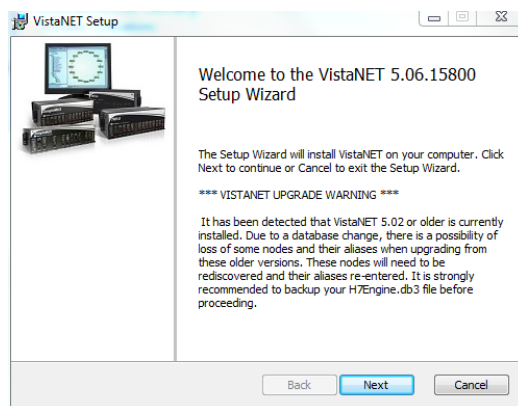
Due to numerous changes in the VistaNET database, a rediscovery is needed after the upgrade is complete. A message has been added into the VistaNET install shield to notify users of this requirement. The text states

“It has been detected that VistaNET 5.02 or older is currently installed. Due to a database change, there is a possibility of loss of some nodes and their aliases when upgrading from these older versions. These nodes will need to be rediscovered and their aliases re-entered. It is strongly recommended to backup your H7Engine.db3 file before proceeding.”

The new system features present in this software release version are:

SNMP SUPPORT

Expanded SNMP functionality is included in version 5.06 for Alarms (now supporting RFC 3877) and unique object identifiers, GET Performance Monitoring (PM), and fully supporting Entity MIBs for T1/E1 MX and SDH product lines. SNMP SET functionality now available to initiate extended rediscovery of selected nodes.



New MIBs now available via www.jmux.com include (prefixed with LENTRONICS-JMNUXTN1U-):

- ALARMSTATUS-TC: contains unit alarm status definitions
- COMMON-TC, COMMON: data-points common to all units (i.e., temp)
- CHANNEL-TC, CHANNEL: channel unit data-points
- ETHER-TC, ETHER: Ethernet unit data-points (performance only)
- JIFTIF-TC, JIFTIF: JIF/TIF unit data-points (performance only)
- OPTIC-TC, OPTIC: Optic unit data-points (performance only)
- SU-TC, SU: Service unit data-points (performance only)



All SNMP functionality is licensed through vSNMP (p/n 86456-51, for system-wide TRAPS and SNMP Alarm GETs), and SNMP-Traffic-Monitoring (p/n 86456-21, per node) for all physical and logical entity information and now performance monitoring data.

NEW ALARM MIB (RFC 3877) AND JMUX EXTENSIONS

The new alarm MIB files have been added for monitoring alarms. It includes the following tables:

- 1. **Alarm Model** (*alarmModelTable*) – represents a list of all potential alarms in the system

Instance	alarmModelName	alarmModelStatus	alarmModelSeverity	alarmModelPriority	alarmModelDescription	alarmModelSpecificPointer	alarmModelStatus	alarmModelPriority	alarmModelActive
0.1.1	Not accessible	Not accessible	zeroDotZero	0	No Alarm	ituAlarmEventType.0.1.1	zeroDotZero	zeroDotZero	active(1)
0.1.2	Not accessible	Not accessible	zeroDotZero	0	Alarm	ituAlarmEventType.0.1.2	zeroDotZero	zeroDotZero	active(1)
0.1.3	Not accessible	Not accessible	zeroDotZero	0	Alert	ituAlarmEventType.0.1.6	zeroDotZero	zeroDotZero	active(1)
0.1.5	Not accessible	Not accessible	zeroDotZero	0	Alarm	ituAlarmEventType.0.1.4	zeroDotZero	zeroDotZero	active(1)
0.1.6	Not accessible	Not accessible	zeroDotZero	0	Alarm	ituAlarmEventType.0.1.3	zeroDotZero	zeroDotZero	active(1)
0.2.1	Not accessible	Not accessible	zeroDotZero	0	Address Mismatch Cleared	ituAlarmEventType.0.2.1	zeroDotZero	zeroDotZero	active(1)
0.2.2	Not accessible	Not accessible	zeroDotZero	0	Address Mismatch	ituAlarmEventType.0.2.2	zeroDotZero	zeroDotZero	active(1)
0.3.1	Not accessible	Not accessible	zeroDotZero	0	Channel Mismatch Cleared	ituAlarmEventType.0.3.1	zeroDotZero	zeroDotZero	active(1)
0.3.2	Not accessible	Not accessible	zeroDotZero	0	Channel Mismatch	ituAlarmEventType.0.3.2	zeroDotZero	zeroDotZero	active(1)
0.4.1	Not accessible	Not accessible	zeroDotZero	0	FPGA Loaded Successfully	ituAlarmEventType.0.4.1	zeroDotZero	zeroDotZero	active(1)
0.4.6	Not accessible	Not accessible	zeroDotZero	0	FPGA Failed to Load	ituAlarmEventType.0.4.3	zeroDotZero	zeroDotZero	active(1)
0.5.1	Not accessible	Not accessible	zeroDotZero	0	Clock Restored	ituAlarmEventType.0.5.1	zeroDotZero	zeroDotZero	active(1)
0.5.2	Not accessible	Not accessible	zeroDotZero	0	Clock Loss	ituAlarmEventType.0.5.2	zeroDotZero	zeroDotZero	active(1)
0.6.1	Not accessible	Not accessible	zeroDotZero	0	Jumpers Configured Correctly	ituAlarmEventType.0.6.1	zeroDotZero	zeroDotZero	active(1)
0.6.2	Not accessible	Not accessible	zeroDotZero	0	Jumper Mismatch	ituAlarmEventType.0.6.2	zeroDotZero	zeroDotZero	active(1)
0.7.1	Not accessible	Not accessible	zeroDotZero	0	Data Rate Corrected	ituAlarmEventType.0.7.1	zeroDotZero	zeroDotZero	active(1)
0.7.2	Not accessible	Not accessible	zeroDotZero	0	Data Rate Mismatch	ituAlarmEventType.0.7.2	zeroDotZero	zeroDotZero	active(1)
0.8.1	Not accessible	Not accessible	zeroDotZero	0	Main Loop is Good	ituAlarmEventType.0.8.1	zeroDotZero	zeroDotZero	active(1)
0.8.2	Not accessible	Not accessible	zeroDotZero	0	Main Loop is Bad	ituAlarmEventType.0.8.2	zeroDotZero	zeroDotZero	active(1)
0.9.1	Not accessible	Not accessible	zeroDotZero	0	Auxiliary Loop is Good	ituAlarmEventType.0.9.1	zeroDotZero	zeroDotZero	active(1)
0.9.2	Not accessible	Not accessible	zeroDotZero	0	Auxiliary Loop is Bad	ituAlarmEventType.0.9.2	zeroDotZero	zeroDotZero	active(1)

A JMUX specific extension table (*lenAlarmModelTable*) also allows an external manager to access priority of each alarm.

- 2. **Active Alarm** (*alarmActiveTable*) – represents the current alarms (alarms currently active in the system); synonymous to *lenMuxActiveAlarmTable* from old MIB.

The new table now contains all of the alarms over VSA.

alarmActiveName	alarmActiveEngineID	alarmActiveSeverity	alarmActivePriority	alarmActiveDescription	alarmActiveResourceID	alarmActiveDescription	alarmActiveModelPointer	alarmActiveStatus	
Not accessible	80.00.1F.88.80.E0...	ipv4(1)	10.13.255.3	(zero-length)	0	zeroDotZero entPhysicalDescr.1561	Dead Channel [S] CH10	zeroDotZero alarmModelNotificationId.0.50.6	zeroDotZero
Not accessible	80.00.1F.88.80.E0...	ipv4(1)	10.13.255.3	(zero-length)	0	zeroDotZero entPhysicalDescr.1561	Dead Channel [S] CH10	zeroDotZero alarmModelNotificationId.0.50.6	zeroDotZero

The existing active alarm table (*lenMuxActiveAlarmTable*) and SNMP trap have also been extended to include:

- The alarm priority
- A pointer to the resource in question in the Entity MIB physical table
- A pointer to the item in the alarm model table.



A JMUX/TN1U/Ue specific extension table (*lenAlarmActiveTable*) includes the following information:

- The unit path
- The alarm value
- A special “key” value for identifying rows of the same alarm with different paths.

3. Clear Alarms (*alarmClearTable*) – represents cleared alarms, up to the last 7 days; synonymous to *lenMuxClearedAlarmTable* from old MIB.

Instance	alarmClearIn...	alarmClearDa...	alarmClear...	alarm...	alarmClear...	alarmClear...	alarmClear...	alarmClearResourceld	alarmClear...	alarmClearModelPointer
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.4...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1561	zeroDoZero	alarmModelNotificationId.0.50.6
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1570	zeroDoZero	alarmModelNotificationId.0.46.6
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1570	zeroDoZero	alarmModelNotificationId.0.46.6
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1570	zeroDoZero	alarmModelNotificationId.0.46.6
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1570	zeroDoZero	alarmModelNotificationId.0.148.2
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1570	zeroDoZero	alarmModelNotificationId.0.148.2
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1570	zeroDoZero	alarmModelNotificationId.0.148.2
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1596	zeroDoZero	alarmModelNotificationId.0.148.2
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1596	zeroDoZero	alarmModelNotificationId.0.148.2
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1573	zeroDoZero	alarmModelNotificationId.0.50.2
0.11.7.222.12.5...	Not accessible	Not accessible	80.00.1F....	ipv4(1)	10.13.255.3	[zero-length]	zeroDoZero	entPhysicalDescr.1573	zeroDoZero	alarmModelNotificationId.0.50.2

The existing active alarm table (*lenMuxClearedAlarmTable*) and SNMP trap modified in the same way as the active table.

JMUX specific extension table (*lenAlarmClearTable*) includes the following information:

- the alarm description,
- unit type
- serial number (in case unit is no longer in inventory).

DISCOVERY TABLE (VISTANET MIB)

New discovery table (*vnDiscoveryTable*) contains current discoveries and discoveries completed within last 5 minutes. This table allows:

- remote SNMP manager to initiate a new discovery
- to add T1/E1 discoveries

vnDiscoveryRange	vnDiscoveryUnits	vnDiscoveryActiveNodes	vnDiscoveryCompletedNodes	vnDiscoveryFailedNodes	vnDiscoveryProgress	vnDiscoveryAdded	vnDiscoveryStarted	vnt
R152	24	0	2	0	100	2014-12-9:2:4:44...	2014-12-9:2:4:44...	26
R156	15	2	0	0	70	2014-12-9:2:5:46...	2014-12-9:2:5:46...	0



PERFORMANCE AND UNIT SPECIFIC DATA

Unit specific MIB files are available and contain data similar to unit GUI in VistaNET. These MIB files provide most of the channels units' information, unit status, location, temperature, and performance counters for most of the JMUX units. Use of SNMP v3 is required to access a specific unit.

The image shows a configuration window for a 'Data-G703 Unit (86466-01)'. The 'Unit Monitor' section shows 'Unit Status' as 'OK' and 'Temperature' as '37 °C'. A blue arrow points to a 'Query results' window displaying the following SNMP query output:

```

***** SNMP QUERY STARTED *****
1: sysUpTime.0 (TimeTicks) 0 days 00h:19m:58s.00th (119800)
2: lenComLocationRack.0 (Integer32) 1
3: lenComLocationShelf.0 (Integer32) 1
4: lenComLocationSlot.0 (Integer32) 1
5: lenComLoopbackSetting.1 (LoopbackSettings) none(1)
6: lenComSlotAssignmentSetting.1 (Integer32) 5
7: lenComTemperature.0 (Integer32) 37
8: lenComUnitStatus.0 (UnitAlarmStatus) ok(0)
9: lenComUnitSeverity.0 (UnitAlarmSeverity) ok(3)
10: lenChanAIS.0 (TruthValue) false(2)
11: lenChanCircuitAddressEnable.0 (TruthValue) true(1)
12: lenChanCircuitTransmitAddress.0 (Integer32) 5
13: lenChanCircuitExpectedAddress.0 (Integer32) 6
14: lenChanCircuitReceivedAddress.0 (Integer32) 6
15: lenChanChannelMismatchEnable.0 (TruthValue) false(2)
16: lenChanDataPRBSGenerator.0 (ChannelPRBSGeneratorState) disabled(0)
17: lenChanDataPRBSAnalyzer.0 (ChannelPRBSAnalyzerState) disabled(0)
18: lenChanDataPRBSResult.0 (SnmpAdminString) : 2D (hex)
19: lenChanDataPortTransmitActive.1 (ChannelActivityStatus) false(2)
20: lenChanDataPortReceiveActive.1 (ChannelActivityStatus) false(2)
Start time : 08/12/2014 6:08:39 PM
End time : 08/12/2014 6:08:39 PM
Duration : 730ms
***** SNMP QUERY FINISHED *****

```

SNMP PHYSICAL ENTITY AND TRAFFIC: ADDED SUPPORT FOR SDH AND T1/E1 SPUR TRAFFIC

In addition to supporting an 'Extended Discovery' in VistaNET 5.04 for SONET and T1 networks, support to SDH and E1 networks and T1/E1 spurs has been added in VistaNET 5.06.

TIE TABLE

CBW Tie table is replaced with generic Tie Table. The new tie table stores CBW and VT ties. This data is used by SNMP Traffic table. The information is stored using serial number and tie connections must be re-created after upgrading and if units are changed.

Tie Table for a tie connection between R151N1 and R152N2

Ring	Node	Unit	Port	Tie Ring	Tie Node	Tie Unit	Tie Port
151	1	JIF-Share (Right, [04-13-1595])	S	152	2	CDAX (Left, [05-16-1543])	S
151	1	OC-12 (Left, [05-17-0791])	CBW-A	152	2	OC-3 (Right, [05-34-1844 (Unit), 05-34-1855 (SFP)])	CBW-A

Buttons: Add, Delete, Properties, Cancel, Apply, OK



CSSU (CYBER-SECURE SERVICE UNIT) SUPPORT

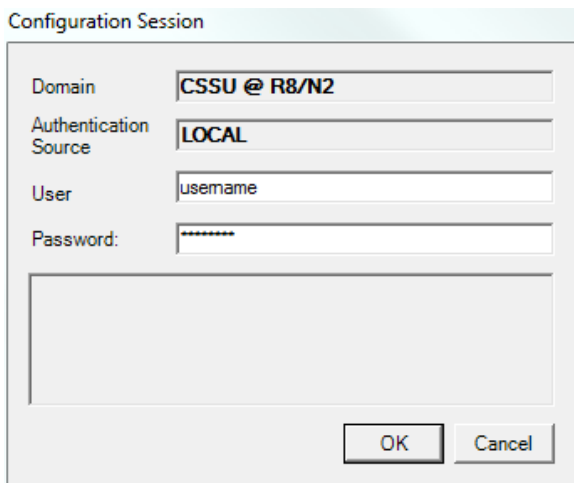
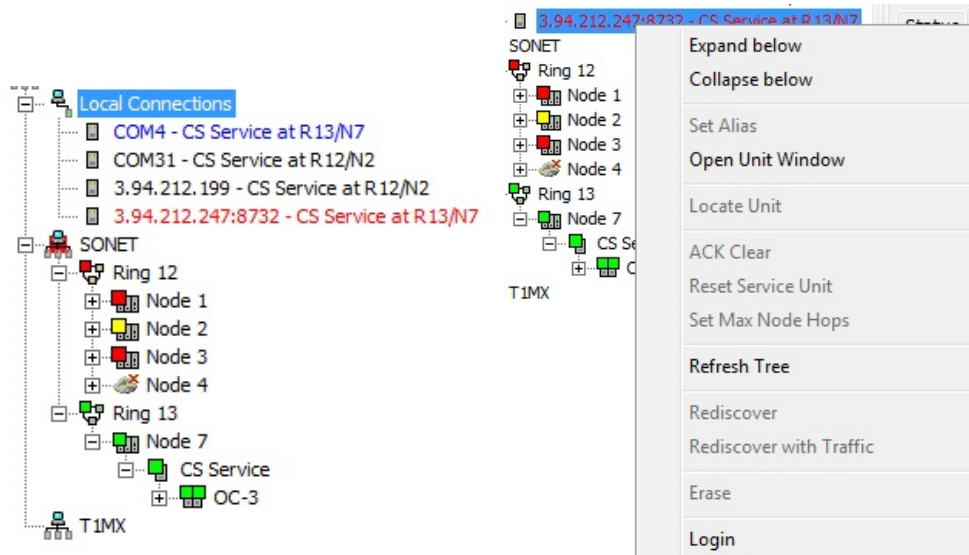
VistaNET 5.06 contains additional support for CS Service Unit Firmware version 2.x. The graphical user interface for CS Service Unit has been revised to show and configure the new features.

TREE VIEW

Locally connected CS Service Units running in Secure mode will be shown in either red text (unauthenticated) or blue text (authenticated). New context-sensitive menu items have been added to allow you to login and logout to/from the unit.

To login to CS Service Unit running in Secure mode, right click on the locally connected unit and select the Login menu item. On the login dialog, enter the RADIUS/LOCAL username (depending on the Authentication Source) and password.

There are two modes available on this latest version of the firmware: Legacy and Secure. If users have activated the license for Secure mode, the mode can be toggled in the Firmware tab.





STATUS TAB

The Status tab shows the Security Configurations, primary and secondary RADIUS Servers status, the date and time (in local time) of the unit, and Communications Monitor for NMS and Maintenance channels.

CS Service Unit (86434-11)

Status | Basic Setup | Network Setup | NMS Tie | Firmware

CS Service Unit

Unit Mode	Secure	Temperature	39 °C
Node Status	OK	Power Bus Voltage	5.2 V
Sentinel	-	Security Configurations	Synchronized
Unit Status	OK	RADIUS Status (Pri / Sec)	N/A N/A

Communications Monitor

NMS | Maintenance

	Left	Right	NMS-Tie (M)	NMS-Tie (S)
Packets XMT	0	0	0	0
Packets RCV	0	0	0	0
Receive Errors	9	8	0	0
Packet Rate	0	0	0	0
PBOC	0	0	0	0

Clear Counters

Alarm Summary

	Left	Right
Sync	-	-
JMUX	Normal	Normal
JIF/SPE/CBW	Normal	Normal
Channel	Normal	Normal

Power Units: OK

Date & Time

Date: 1970-01-01

Time: 09:37:42

Source: Internal



BASIC SETUP TAB

The Basic Setup tab provide configuration to Overhead Allocation and the NMS, OrderWire and Maintenance channels.

CS Service Unit (86434-11)

Status Basic Setup Network Setup NMS Tie Firmware

Overhead Allocation

Overhead Use TOH (NMS+OW+Mnt)

DCC1	N	E1	O1	R1	R18
DCC2	N	E2	-	R2	R17
DCC3	N	DCC8	-	R3	R16
DCC9	M	DCC7	-	R4	R15
DCC10	M	DCC6	-	R5	R14
DCC11	M	DCC5	-	R6	R13
DCC12	M	DCC4	-	R7	R12
				R8	R11
				R9	R10

CS Service Unit

Node Name Unit no. 0019

Ring 13

Node 7

Max Node Hops 14

Optic Rate OC-3

Sentinel Mode -

Input Contacts

	Alias	Ext. Input	Invert	Declared State	NMS Alert
#1	CONTACTIN1	Open	<input type="checkbox"/>	Idle	<input type="checkbox"/>
#2	CONTACTIN2	Open	<input type="checkbox"/>	Idle	<input type="checkbox"/>
#3	CONTACTIN3	Open	<input type="checkbox"/>	Idle	<input type="checkbox"/>
#4	CONTACTIN4	Open	<input type="checkbox"/>	Idle	<input type="checkbox"/>

Security Configurations

Sync security configurations from adjacent CSSUs

Unit Location

Latitude 0.00000 Longitude 0.00000 Building 24 Rack 8 Shelf 24

When the CSSU is running in secure mode and first inserted into a ring containing CSSU-S units, the local unit must receive it security profile from a trustworthy remote CSSU-S. A request from the local CSSU-S unit must be made to initiate this trusted source to 'push' out security profile onto the network. A VistaNET button called the Sync security configuration from adjacent CSSUs has been added to the GUI to perform this task.

At the conclusion of this process, the newly inserted CSSU will have the same security settings as stored in remote CSSUs.



NETWORK SETUP TAB

The Network Setup tab shows the Master CSSUs ring and node numbers for the primary and secondary masters.

The Craft Interface is not available for use on the CS Service Unit firmware version 2.00, therefore it is important that at least one of the Ethernet port is enabled, specifically one with the network connection.

CS Service Unit (86434-11)

Status | Basic Setup | Network Setup | NMS Tie | Firmware

Front Ethernet Port		Rear Ethernet Port	
Port Enable / Status	<input checked="" type="checkbox"/> No Link	Port Enable / Status	<input checked="" type="checkbox"/> OK
DHCP	Client	DHCP	Client
Local IP	0.0.0.0	Local IP	255.255.255.0
Subnet Mask	0.0.0.0	Subnet Mask	255.255.255.0
Gateway IP	0.0.0.0	Gateway IP	0.0.0.0
DNS Server IP	0.0.0.0	DNS Server IP	0.0.0.0
MAC Address	00:00:00:00:00:00	MAC Address	00:00:00:00:00:00

Listening Port		Master CSSUs	
NMS Data (TCP)	8732	Ring #	Node #
		Primary Master	12 2
		Secondary Master	12 4

NMS TIE TAB

The NMS Tie tab is new in this release. It provides a way to configure the NMS Tie settings, however this release only supports enabling/disabling NMS Tie Port.

CS Service Unit (86434-11)

Status | Basic Setup | Network Setup | NMS Tie | Firmware

NMS Tie Port

Enable NMS Tie Port

Block egress of:

- Read/Discover requests
- Alarm notifications
- Configuration change commands

Block ingress of:

- Read/Discover requests
- Alarm notifications
- Configuration change commands

Block security maintenance traffic



FIRMWARE TAB

The Unit Mode can be changed in the Firmware tab. Changing the mode from Secure to Legacy requires user with VistaNET Administrator privilege. This operation will remove existing Overhead Allocation settings and will load default settings applicable to Legacy mode.

Switching from Legacy to Secure mode can be done by any VistaNET user, however it is important to note that because the Craft Interface is not available in Secure mode, ensure that there is a connection to at least one of the Ethernet port.

The screenshot shows the 'Firmware' tab in the VistaNET configuration interface. At the top, there are navigation tabs: Status, Basic Setup, Network Setup, NMS Tie, and Firmware. The 'Firmware' section contains two columns for 'Package 1' and 'Package 2'. Package 1 has a Version of 2.01d, a Checksum of DEA241CF, and a Status of Active (highlighted in green). Package 2 has a Version of -, a Checksum of -, and a Status of -. Below these packages is a 'Unit Mode' dropdown menu currently set to 'Secure'. At the bottom, the 'OS Image' section shows 'Active Version' as 1.00 and 'Inactive Version' as 1.00. Buttons for 'Reboot' and 'Reboot with this package' are present under each package.

Package	Version	Checksum	Status
Package 1	2.01d	DEA241CF	Active
Package 2	-	-	-

Unit Mode: Secure

OS Image: Active Version 1.00, Inactive Version 1.00



ACTIVITY LOG

VistaNET 5.06 provides more activity logging information. The following events are now being logged into the Activity Log:

1. Adding, deleting and updating user information,
2. Adding and deleting groups, enabling/disabling discovery for a specific group of users, adding and deleting configuration restrictions,
3. Starting and canceling discovery,
4. Erasing the inventory,
5. Configuring data points in the units GUI,
6. Users logging in/out of VistaNET,
7. User logging in/out of CSSUs,
8. Registering the License PIN,
9. Starting/shutting down the service,
10. Connecting/disconnecting the client (starting and stopping the GUI)
11. Resetting the Service Unit,
12. Resetting / rebooting the any unit,
13. Changing the MAXHops value

In addition, the Activity Log tab has been changed to provide the following functionality:

- Activity events are sorted by Time (default),
- Events show start time and duration of the event instead of start/end time,
- 'Details' box below the data grid provides additional parameters for the event, results of an action, and relevant error messages,
- Filtering by activity log columns is possible by clicking on the column headers, as well as search through actions by text (select 'show filters>> button).



VistaNET: ES-T20015525 (Debug Build)

Alarms View Inventory Activity Log

Tree Filter: ON 25 From Nov 6 1 day

Time	User	Description	Path	Unit	Loc/NMS	Result	IP	Category	Duration
11/6/2014 3:33:16 PM	VistaNET	Set "MaxHops" to "16"	R1/N2	SERVICE	NMS	Success	3.94.212.205	Unit Config	0 sec
11/6/2014 3:33:15 PM	VistaNET	Set "MaxHops" to "16"	R1/N1	SERVICE	NMS	Success	3.94.212.205	Unit Config	0 sec
11/6/2014 3:32:31 PM	VistaNET	Set "MaxHops" to "15"	R1/N2	SERVICE	NMS	Success	3.94.212.205	Unit Config	0 sec
11/6/2014 3:32:30 PM	VistaNET	Login			Local	Success	3.94.212.205	Log In/Out	0 sec
11/6/2014 3:32:17 PM	VistaNET	Logout			Local	Success	3.94.212.205	Log In/Out	0 sec
11/6/2014 3:32:12 PM	VistaNET	Modify NMS Write Restriction			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:32:07 PM	VistaNET	Modify NMS Write Restriction			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:32:07 PM	VistaNET	Modify NMS Write Restriction			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:32:01 PM	VistaNET	Delete User Group			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:31:58 PM	VistaNET	Add User Group			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:31:52 PM	VistaNET	Modify Group Permissions			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:31:24 PM	VistaNET	Delete User			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:31:16 PM	VistaNET	Add User			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:31:16 PM	VistaNET	Add User Group			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 3:30:48 PM	VistaNET	Login			Local	Success	3.94.212.205	Log In/Out	0 sec
11/6/2014 3:29:05 PM	VistaNET	Logout			Local	Success	3.94.212.205	Log In/Out	0 sec
11/6/2014 3:16:25 PM	VistaNET	Start Discovery			Local	Success	3.94.212.205	Discovery	0 sec
11/6/2014 3:16:25 PM	VistaNET	Start Discovery			Local	Success	3.94.212.205	Discovery	0 sec
11/6/2014 3:16:20 PM	VistaNET	Login			Local	Success	3.94.212.205	Log In/Out	0 sec
11/6/2014 3:16:20 PM	VistaNET	Start Discovery			Local	Success	3.94.212.205	Discovery	0 sec
11/6/2014 12:02:46 PM	VistaNET	Login			Local	Success	3.94.212.205	Log In/Out	0 sec
11/6/2014 12:02:36 PM	(unknown)	Add User			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 12:02:21 PM		Register Licence PIN			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 12:02:08 PM		Register Licence PIN			Local	Success	3.94.212.205	User Config	0 sec
11/6/2014 12:01:43 PM		Register Licence PIN			Local	Fail	3.94.212.205	User Config	0 sec

Erase=No
Rediscover=Yes
Traffic=Yes
Range=SONET

User: VistaNET Company: GE Multilin

Alarms View Inventory Activity Log

<< Show History 3 entries From Jan 28 1 day

Show only selected node
Tree Filter: ON

Action category filters

- Startup
- Log In/Out
- Unit Config
- Discovery
- Erase
- Unit Reset
- User Config

Text Searches (partial matches accepted)

User

Unit

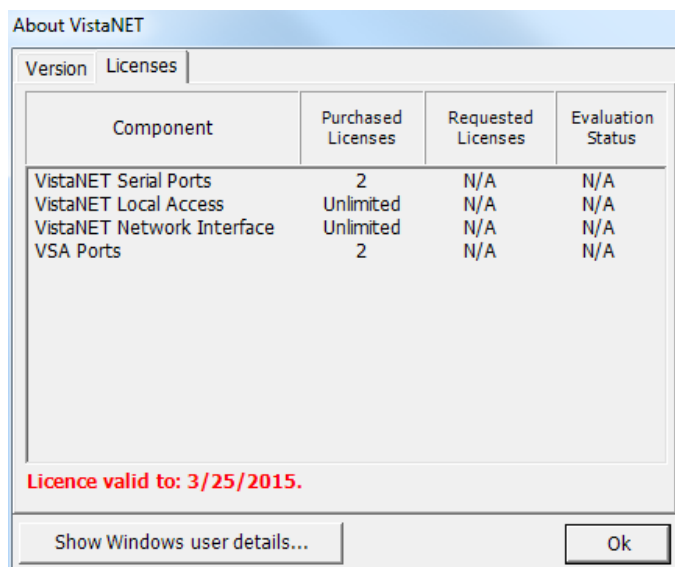
Description

Details

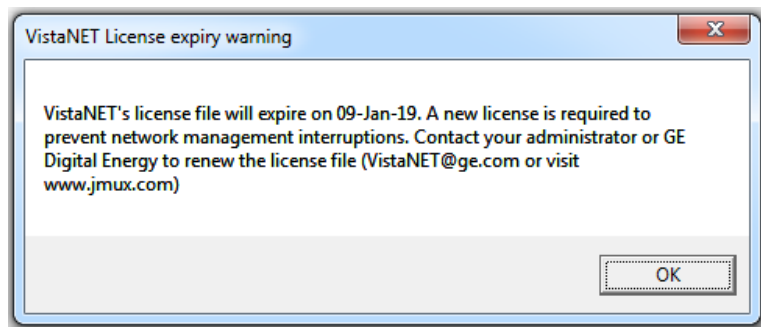


LICENSE EXPIRATION NOTIFICATION

VistaNET notifies users when the digital certificate associated with the License file is about to expire. Each license file will expire within a 36 month period after it has been created. Each organization will need to contact GE and request a new license file. Users can also see the expiry date through the About dialog box (accessed through the 'Information' icon)



VistaNET will give a maximum of 1 warning / 24 hours when there is 14-60 days remaining, and maximum of 1 warning / 6 hours when there is less than 14 days.





IMPORTANT REMARKS

MANAGEMENT OF THE VISTANET SERVICES

The VistaNetService.exe has to be stopped / restarted whenever:

- A new passport/license file has been synchronized.
- There were changes in Administrative & Startup Options.
- Whenever prompted to restart VistaNET.
- When removing/upgrading VistaNET.

VistaNET.exe will start VistaNetService.exe but it will not stop it on exit. On the other hand VistaNetService.exe will close VistaNET.exe when stopped.

VistaNetService.exe has default startup option set to Manual. The PC administrators may choose to change this to Automatic (recommended for 24/7 PC used to manage the Lentrionics Multiplexer system).

If a VistaNET service fails to start or if the service fails to install, reboot the computer and attempt the request again.

If VistaNetServices fails to stop from Services snap-in, at least one of the following two procedures should be able to stop it. Please use these as a last resort, since you may lose data when abruptly killing the service. A restart of the PC is then recommended.

1. End VistaNetService process, which runs as SYSTEM user, from the Task Manager (running as Administrator on W7, make sure to Show processes from all users).

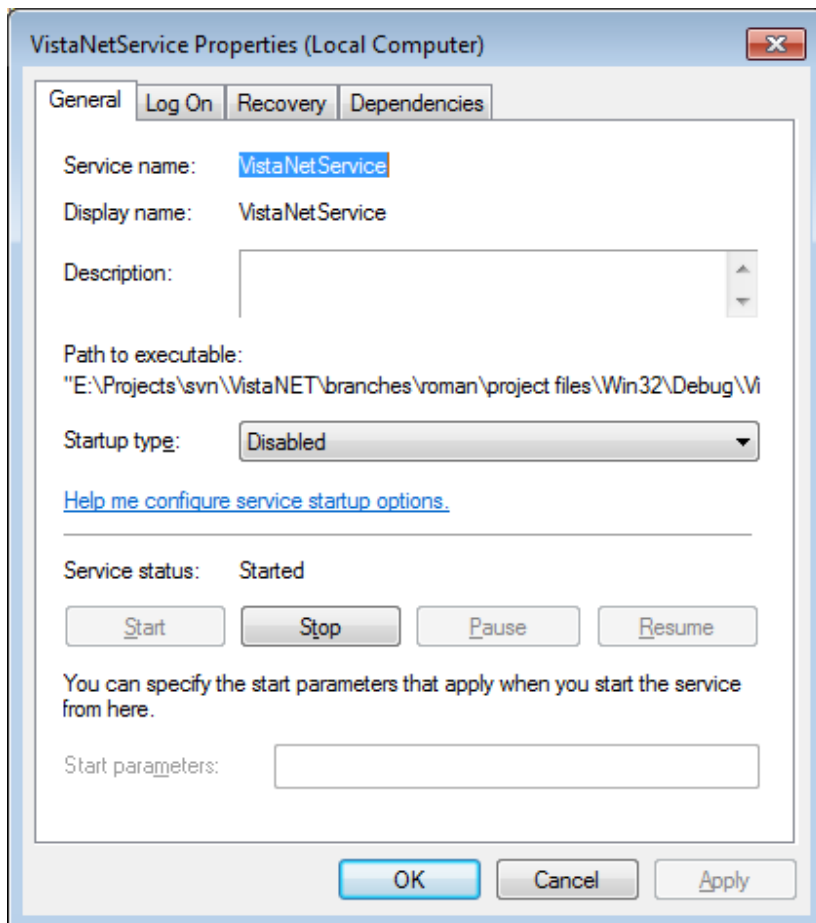
Image Name	PID	User Name	CPU	CPU Time	Working Set (Memory)	Memory (Private Working Set)	Page Faults	Handles	Threads	USE
wmpnetwk.exe	3636	NETWORK SERVICE	00	0:00:09	5,444 K	2,640 K	41,919	272	9	
WmiPrvSE.exe	4424	LOCAL SERVICE	00	0:00:00	5,080 K	1,640 K	1,465	123	8	
winlogon.exe	572	SYSTEM	00	0:00:00	1,464 K	600 K	5,456	130	3	
wininit.exe	444	SYSTEM	00	0:00:00	160 K	112 K	1,280	79	3	
vmware-vmx.exe	5856	Roman	00	0:30:26	261,352 K	11,108 K	873,928	440	9	
vmware-tray.exe	3148	Roman	00	0:00:01	1,016 K	516 K	39,829	286	6	
vmware-authd.exe	1980	SYSTEM	00	0:02:49	1,576 K	868 K	6,674	242	7	
vmware.exe	692	Roman	00	0:00:08	3,288 K	2,064 K	45,747	371	7	
vmnetdhcp.exe	2028	SYSTEM	00	0:00:00	564 K	192 K	1,489	45	3	
vmnat.exe	1948	SYSTEM	00	0:00:00	588 K	212 K	1,414	67	5	
VistaNetService.exe	4584	SYSTEM	00	0:11:55	68,396 K	45,284 K	63,702	503	44	
VistaNET.exe	1828	Roman	00	0:03:29	125,592 K	92,396 K	909,228	575	13	2
taskmgr.exe	5092	Roman	00	0:00:21	10,516 K	2,240 K	3,091	129	5	
taskhost.exe	2492	Roman	00	0:00:02	3,004 K	1,136 K	8,933	208	8	

Show processes from all users

Processes: 59 CPU Usage: 0% Physical Memory: 74%



2. Disable the service from Services MMC plug-in (change Manual or Automatic Startup Type option to Disabled), and reboot the computer.





FIREWALL

WINDOWS FIREWALL

If used, the first time that VistaNetService is started, a Windows Firewall message may be generated. Ensure that the 'Private Networks' checkbox is checked and press 'Allow Access'. Active Services will now be allowed through the Windows Firewall.

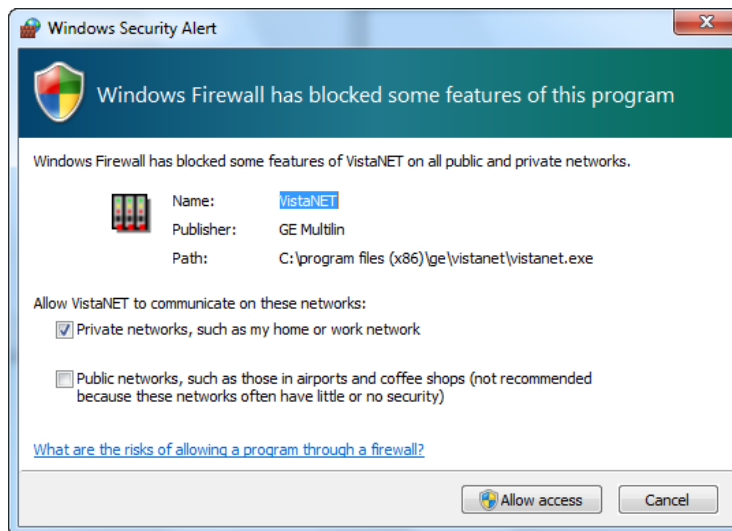


Figure: Windows Firewall

WINDOWS SERVER 2008 FIREWALL

Unlike the Windows 7 firewall setting, which prompts the user to allow VistaNetService through the firewall, in Windows Server 2008 an inbound firewall rule must explicitly be set. By default, all applications are blocked by the firewall. An inbound rule must be created to open the firewall for the specified application.

Open the Server Manager and navigate to the 'Configuration – Windows Firewall with Advanced Security – Inbound Rules.

In the Actions panel, select 'New Rule'. This will walk the user through creating a new rule using a new rule wizard.

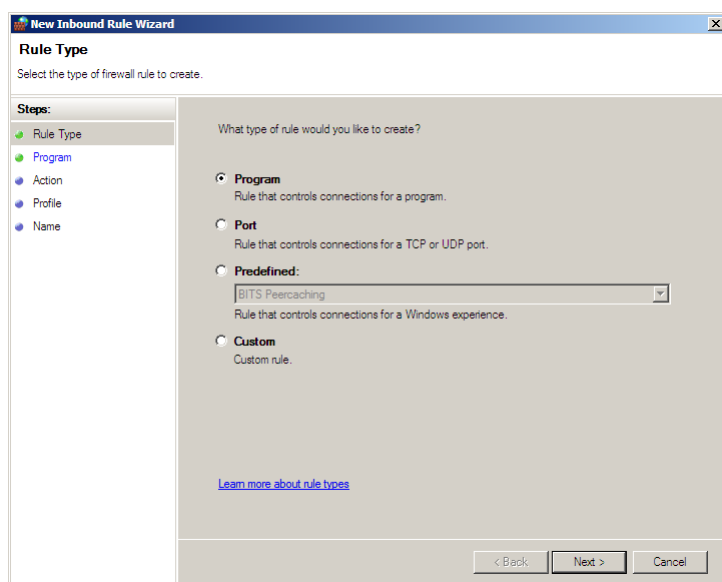


Figure: 2008 Server New Inbound Rule Wizard – Step #1 – Rule Type

Select the 'Program' option. This will allow all IP ports that are used by VistaNetService to be passed through the firewall. Press the 'Next' button.

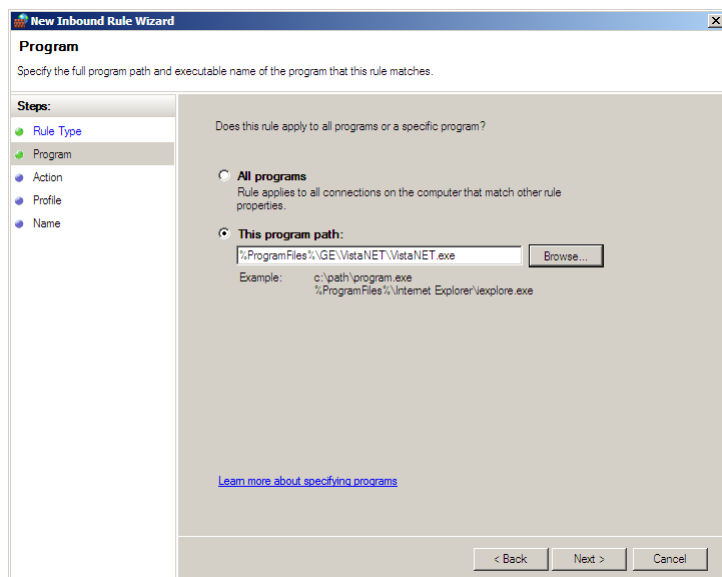


Figure: Program Path

Using the 'Browse' button navigate to the 'C:\Program Files\GE\VistaNET\VistaNetService.exe' application (32-bit) or 'C:\Program Files (x86)\GE\VistaNET\VistaNET.exe' (64-bit). Press the 'Next' button.

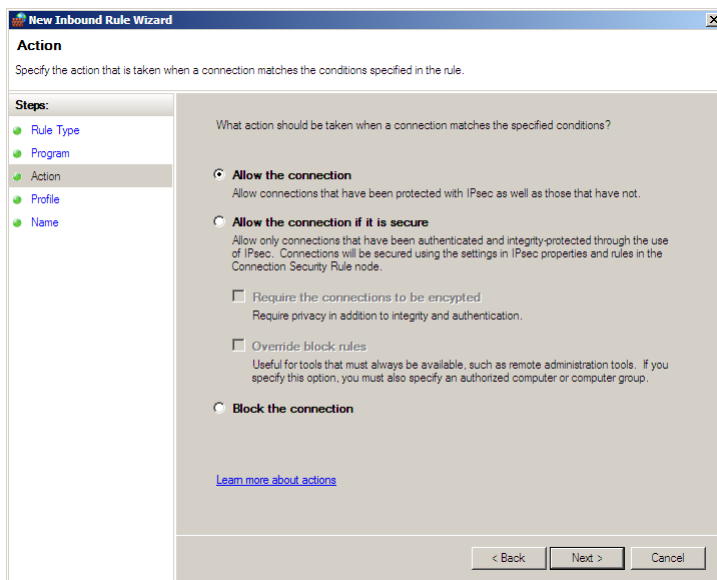


Figure: Action

Select the 'Allow the connection' option to allow the VistaNetService ports through the firewall. Press the 'Next' button.

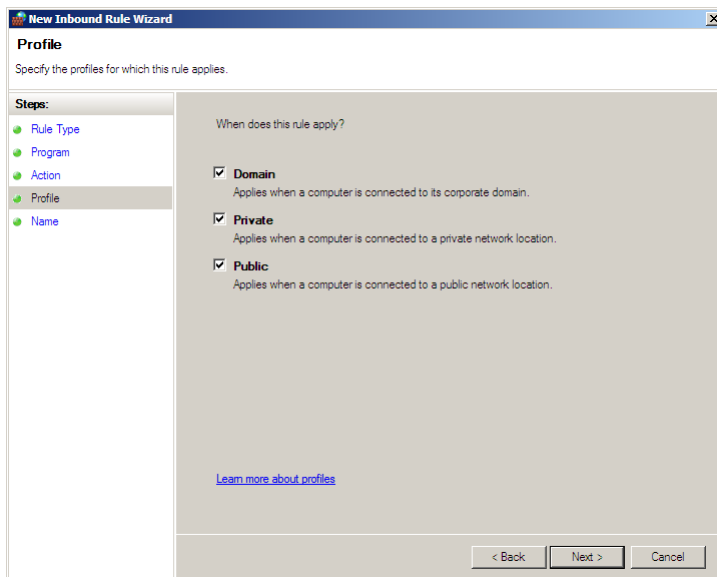


Figure: Profile

Determine on which networks the rule will apply. This rule must be applied to allow connections to any VistaNetService session used on the network.

Press the 'Next' button. The user will be requested to give the rule a name (typically VistaNET).

Press the 'Next' button to complete the rule.

The firewall rule will now apply to all users of the Windows 2008 Server. There will not be a requirement to change rules for other users (such as Standard users).



SOFTWARE UPGRADE PROCEDURE

This section focuses on upgrading your PC with VistaNET 5.06 Software.

REQUIRED SOFTWARE BEFORE UPGRADE

VistaNET version 5.06 requires the following components to be installed:

- Microsoft .NET Framework 4

UPGRADING FROM VISTANET VERSION 2.25 OR LOWER

- If you are upgrading from VistaNET versions 2.25 and below, you must uninstall the old version using **Add/Remove Programs** before installing VistaNET version 5.0x.
 - **Uninstall** is required due to the change in the installer software used.
- You must upgrade the H7Engine.dat with VistaNET4.xx before VistaNET version 5.0x will be installed, since running it will not update the H7Engine.dat file to a new format. As a result of this new install, you will not be able to revert to any previous versions of VistaNET unless you also revert to the saved version of the H7Engine.dat file by manually copying it in the corresponding VistaNET file folder.

RECOMMENDATION: GE recommends that the old database files (H7engine.dat) be removed from the program files directory after a backup is securely saved.

- After installing VistaNET version 5.0x, you must rediscover the existing network in order to populate the database with required data. This discovery is required for the nodes containing CDAX cards, to properly obtain and store CDAX Left/Right information. Also, the discovery is needed in order to obtain and store the units' Serial Number, and data used to properly refresh the tree view of your network.
- After installing VistaNET version 5.0x and connecting various VNI/VSA computers in your management network, you must let it run for at least one hour before performing any tasks. This approach will allow VistaNET to resynchronize all the JMUX/TN1U network data between the networked VistaNET computers.
- VistaNET 5.0x will not start properly if in earlier VistaNET versions you had the modem connection name or telephone number containing an ampersand (&). In this case please make sure that there are no '&' characters in the modem name(s) or numbers before installing.

UPGRADING FROM VISTANET VERSION 3.XX

If you are upgrading from VistaNET versions 3.xx, uninstalling the previous version is NOT required, but you are required to upgrade your database with VistaNET 4.xx before proceeding with the installation of VistaNET version 5.06.

STEPS TO UPGRADE VISTANET FROM 3.XX TO 4.05

- Stop any previous versions of VistaNET
- Using Windows Explorer, go to the "C:\Program Files\GE\VistaNET\H7Engine" folder and make a backup copy of the H7Engine.dat file.



-
- Using a Web-browser, open <http://www.JMUX.com>
 - Click on the *Existing Customers Login* button.
This is a protected site, a username and password is required
 - Select the 'Software' web link
 - Select 'VistaNET Software Download'
 - Download the *VistaNETsetup_405.msi* file to the PC's hard drive
 - Run the *VistaNETsetup_405.msi* file
 - Follow the Install Shield installation instructions
 - Repeat on all PC's running VistaNET

Note: There is no need to start VistaNET 4.05. Proceed to upgrade to VistaNET 5.0x.

INSTALLING VISTANET VERSION 5.06 OR UPGRADING FROM VISTANET VERSION 4.XX

If you are upgrading from VistaNET versions 4.xx, uninstalling the previous version is NOT required.

STEPS TO INSTALL VISTANET 5.06 OR UPGRADE VISTANET FROM 4.XX

For new installation of VistaNET version 5.06 or when upgrading from VistaNET version 5.00, 5.02 or 4.xx:

- If you are upgrading from VistaNET 2.xx or 3.xx, please read above for additional upgrade instructions
- Stop any previous versions of VistaNET (GUI and Service) before performing this upgrade
- Using Windows Explorer, go to the "C:\Program Files\GE\VistaNET\H7Engine" folder and make a backup copy of the H7Engine.db3 file. If you are upgrading from version 4.00, the location of the database is in "%APPDATA%\GE\VistaNET\H7Engine".
- Using a Web-browser, open <http://www.JMUX.com>
- Click on the *Existing Customers Login* button.
This is a protected site, a username and password is required
- Select the 'Software' web link
- Select 'VistaNET Software Download'
- Download the *VistaNETsetup_50x.msi* file to the PC's hard drive

NOTES and RECOMMENDATIONS

1. **NOTE 1:** After installing VistaNET version 5.06, you must rediscover the existing network in order to populate the database with required data. This discovery is required for all nodes due to significant changes with SNMP-based Entity, Traffic and Performance MIBs.
2. **NOTE 2:** All of the information contained in the .db3 file prior to the upgrade will be available after the upgrade*.



3. **NOTE 3:** * Occasionally, JIF-Share and CMUX unit aliases are not restored. Refer to the workaround in **TRAC # xxxx** to resolve this issue.
 - Run the *VistaNETsetup_50x.msi* file
 - Follow the Install Shield installation instructions
 - License and Activate the VistaNET software
 - see *License File and Licensing VistaNET, and Activation PIN and Activating VistaNET*
 - Repeat on all PC's running VistaNET
4. **RECOMMENDATION:** GE recommends that the old database files (H7engine.dat and H7engine.db3) be removed (from "C:\Program Files\GE\VistaNET\H7Engine" and "APPDATA\GE\VistaNET\H7Engine" directory's respectively) after a backup is securely saved.

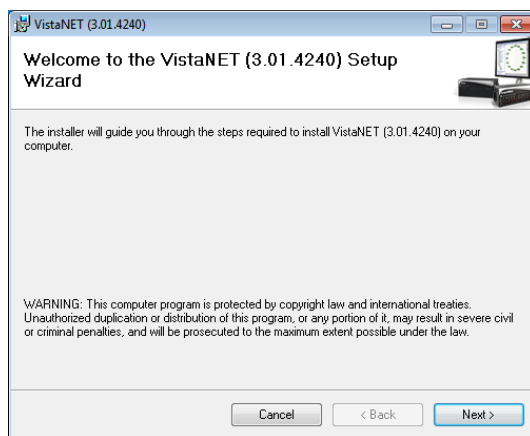


Figure: Welcome Screen

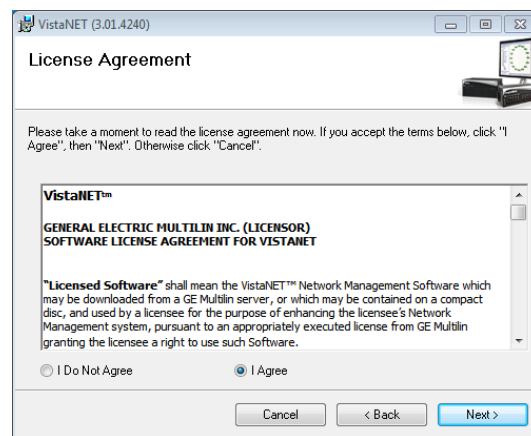


Figure: License Agreement

INSTALLATION NOTES

1. If a Windows generated User Account Control warning is seen, select 'Allow'. The installation will then complete.
2. VistaNET will be installed in the C:\Program Files\GE\VistaNET folder (32-bit) or the C:\Program Files(x86)\GE\VistaNET folder (64-bit).

UPGRADING IPSU

VistaNET 5.06 is not supported for IPSU's. GE recommends the use of 86456-51 vSNMP (a VistaNET SNMP license) where SNMP functionality is required for Lentrionics Multiplexers), and/or the new B86434-11 Cyber Secured Service Unit (for IP connectivity to Lentrionics Multiplexers).



LICENSING AND ACTIVATING VISTANET 5.0X

LICENSE FILE (*.LIC)

The VistaNET license file used to activate and control licensed features has been changed for VistaNET version 5.0x. A new license file (issued by GE Digital Energy) will facilitate improved security for VistaNET administrators and users in the following ways:

1. VistaNET activation requires two security factors, a license file (*.lic) and activation PIN.
2. Previous copies of the VistaNET passport (company_name.psr, .dat or .db3 files) will not successfully activate VistaNET version 5.0x.
3. The new license file contains no default username or password. Distribution of this license file is recommended and will successfully start VistaNET, but prevents equipment configuration because it contains no users or user privileges.
 - a. An Activation PIN is required to add users and privileges (typically performed on a 24/7 VistaNET service by the VistaNET administrator).
 - b. Successful synchronization to a VistaNET service containing users and user privileges is another acceptable method of activating remote VistaNET instances.
4. The license file is digitally signed, and as such, authentication is verifiable.
5. The license file also contains an expiry date (36 months by default, but configurable from 1 month to 60 months), preventing activation of VistaNET with the underlying base code, and preventing normal VistaNET operation. This will ensure that uncontrolled copies of the license file are (in time) rendered inoperable.
6. An activation PIN used to activate VistaNET expires after a defined period, preventing activation of VistaNET with the license file (3 months by default, but configurable from 1 month to 60 months).

A representative (VistaNET administrator) from each organization will need to register for a new VistaNET License file. This file is in an XML format following this naming convention "company_name.lic".

Obtaining a .LIC file: Each VistaNET administrators should register for the license file by visiting the Lentrionics Multiplexer website <http://www.JMUX.com> (recommended)

- Click on the Existing Customers Login button. This is a protected site, a username and password is required
- Select the 'Software' web link
- Select 'VistaNET Passport Registration Form'
- Complete and submit the registration form
 - Please specify desired PIN and LICENSE file expiration dates.

Alternatively, contact our customer support team at VistaNET@GE.com



GE Lentrionics will create the license file (company_name.lic). A notification will be e-mailed to each VistaNET administrator indicating the passport location and integration instructions. A second factor, a security PIN, required to fully activate VistaNET version 5.0x, will be independently supplied to each primary VistaNET administrator.

Distribute the LICENSE file:

This license file can be safely distributed (recommended) to all VistaNET users that require VistaNET version 5.0x.

See 'Licensing VistaNET' below for more details on activating VistaNET.

LICENSING VISTANET

VistaNET is licensed to a company using the new license file ("company_name.lic"). After installation of VistaNET is complete, running VistaNET will prompt each user for a license file. Start VistaNET, then Browse for and Synchronize to the supplied license file.

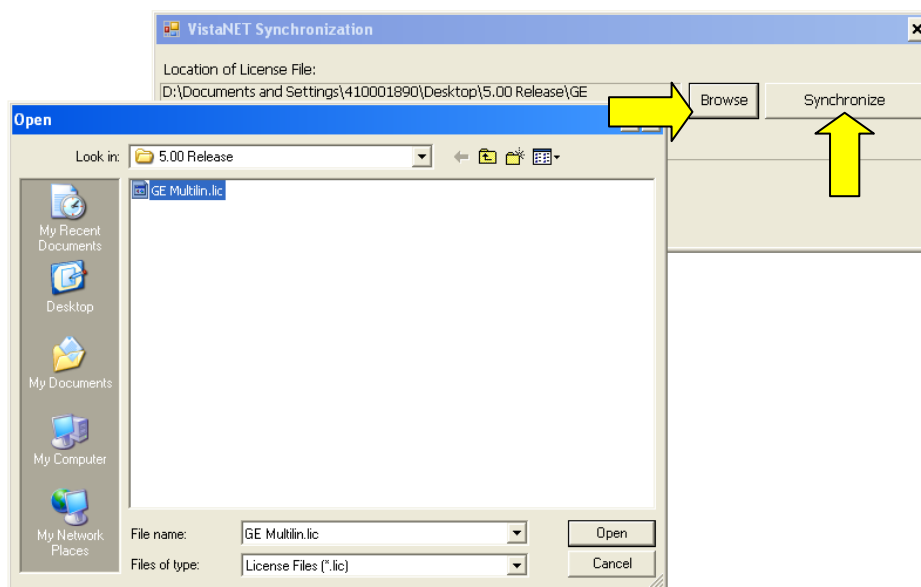


Figure: Open license file

Figure: Synchronization

After synchronization is successful, an encrypted (secure) database file (.db3) will be created and stored on C:\Program Files\GE\VistaNET\H7engine\ folder (32-bit) or the C:\Program Files(x86)\GE\VistaNET\H7engine folder (64-bit).

VistaNET can now be successfully started; however, VistaNET 5.0x is not fully operational. No equipment configuration is permitted until a second security factory is applied.



This second security factor can be applied in one of three ways

1. Activation PIN
 - Reserved to VistaNET Administrators
2. Synchronization with an activated version of VistaNET
 - Recommended for general VistaNET users
3. Supply remote VistaNET instances with a secure db3 file
 - Recommended for remote VistaNET users without network access to a centralized VistaNET service. Windows™ administrative privileges are required.

ACTIVATION PIN

VistaNET version 5.0x requires two factors before the product is successfully activated and ready for use. The license file is the 1st factor, generated by GE and sent to a designated VistaNET administrator, then distributed internally within each organization, while the 2nd factor, an activation PIN, is also required.

While VistaNET appears to be operable without this second security factor, any attempt to configure equipment will prompt the user for this PIN.

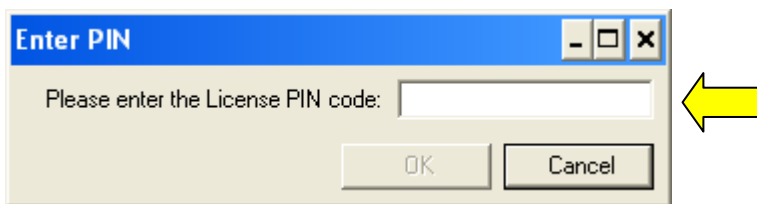


Figure: Enter Activation PIN

This activation PIN is married to the supplied license file (paired keys). Both factors are needed to successfully license and activate VistaNET 5.0x. Additionally, the license file and activation PIN are both designed to expire, protecting companies who lose control of their security keys.

RECOMMENDATION: GE strongly recommends that the activation PIN be protected, and NOT distributed.

ACTIVATING VISTANET

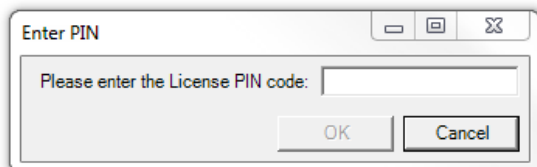
Activating VistaNET 5.0x can be achieved in one of three ways,

1. Apply an Activation PIN (reserved for VistaNET Administrators)
2. Synchronization VistaNET with a previously activated version of VistaNET 5.0x (recommended for general VistaNET users)
3. Supply remote VistaNET instances with a secure db3 file.

ACTIVATION VIA A PIN




A VistaNET administrator who has been supplied with both security keys, can pair the license file and activation PIN to activate VistaNET 5.0x. Essentially, the pairing will permit this administrator to create an administrative user within the software. This action is performed typically once by the VistaNET administrator on a centralized 24/7 PC where the primary VistaNET service runs. The newly created administrative account has a default user name of 'administrator' and password equal to the *activation pin*. VistaNET 5.04 will then prompt the administrator to replace this account with one picked from Active Directory or from a Windows Local Account. This step must be performed before the software activation process is successful.



ACTIVATION VIA SYNCHRONIZATION

Remote VistaNET instances may also be activated by an administrator using the activation PIN (as described above); however, this would require an administrator to apply the pin locally on every VistaNET PC. A more convenient method is recommended. Remote VistaNET instances can instead synchronize to a centralized 24/7 VistaNET instance, previously activated by the administrator.

In this case, instruct each remote user to

- Install VistaNET (provide a link to the downloaded VistaNET 5.0x installation executable),
- License VistaNET (provide a link to the company-wide license file)
- Instruct each user to press the login icon  and select "No" to "Is this the first VistaNET PC to be upgraded". This action will both activate remote VistaNET instances, and synchronize an active control list (ACL).



Configuring this IP/Hostname of a centralized VistaNET service (and/or Backup service) is an allowed setting without an activation pin. Once the remote VistaNET service connects with the centralized service, the 2nd security factor will be learned, along with the complete list of usernames, and associated access control credentials.

Please note. The communications link between VistaNET 5.0x services is completely encrypted, mitigating man-in-the-middle attacks.

Remote instances of VistaNET 5.0x are now fully operational.



ACTIVATION VIA SECURE .DB3

Remote VistaNET instances may be optionally activated by supplying users with a copy of a secure .db3 file. This activation method is not typical, but suitable none-the-less when a remote user cannot synchronize with a centralized 24/7 VistaNET instance.

In this case, instruct each remote user to

- ***Install*** VistaNET (provide a link to the downloaded VistaNET 5.0x installation executable),
- ***Instruct*** each user to save a secure .db3 file into C:\Program Files\GE\VistaNET\H7engine\ folder (32-bit) or the C:\Program Files(x86)\GE\VistaNET\H7engine folder (64-bit).

Note: Providing users with this secure (encrypted) .db3 file provides them with an exact copy from the source database. Saving this file into the specified location will require Windows™ administrative privileges by the user logged into this remote PC.

Remote instances of VistaNET 5.0x are now fully operational.

LICENSING AND ACTIVATION NOTES

1. The database (*.db3 file) is additionally encrypted during the upgrade to version 5.0x. Ensure a copy of the original (version 4.xx) db3 file is retained before the upgrade is performed.
2. All of the information contained in the .db3 file prior to the upgrade will be available after the upgrade.
3. GE strongly recommends that the VistaNET administrator protect the activation pin.
4. After the license file has expired, VistaNET will not be able to synchronize with its local license file (synchronization error). A new VistaNET license file is required from GE Digital Energy. See "[Obtaining a .LIC file](#)"

REPLACING AN ADMINISTRATOR ACCOUNT

Starting from VistaNET version 5.04, all user accounts are picked from Active Directory or from a Windows Local Account. Forgetting a username / password will therefore impact a user's ability to login to their PC's Windows user account.

Occasionally an administrator needs to be replaced. If no other users had been assigned administrator group privileges, then the encrypted VistaNET database and associated users access control list cannot be modified. The administrator will need to contact GE for a new *.lic file and activation pin.

The administrator should follow these steps to regain access control

1. Contact GE Customer Service (VistaNET@ge.com) or 604-421-8610 to request a renewal of the VistaNET passport



- a. Note: GE will send the renewed License file and Activation PIN only to the original VistaNET administrator. If requested recipient is different, GE will insist that this request be made in writing, and approved by a manager.
2. From a centrally connected VistaNET service (VNET_24/7), shut down the VistaNET application (GUI and Service).
3. Locate a remote VistaNET PC (VNET_remote) that's able to connect over IP to the production / operational VistaNET PC from step 2 above.
4. From the VNET_remote PC, open Windows Explorer, locate then rename the local database (i.e. from H7engine.db3 to H7enginedb3.old)
 - a. Start VistaNET
 - b. VistaNET will ask for a new license file. Browse for then synchronize to the new license file supplied by GE
 - c. Press the "Key" Icon (from VistaNET's top-level icons) and enter the Activation PIN
 - d. Pick a new administrator from Active Directory or from a Windows Local Account
 - e. Connect this remote VistaNET PC onto the production / operational network and enter the IP address of a known VistaNET service.

Note: Synchronization of the two services will take place. The new "administrator" created in step 4d will be added to the active control list, and available from both sessions.

5. Consider creating administrative designates.

EXPIRATION OF LICENSE OR ACTIVATION PIN

After a prescribed period of time, each company's LICENSE file and ACTIVATION PIN will EXPIRE. By default, the license file expiration is set to 36 months, while the activation PIN default expiration is 3 months.

A company may specify the expiration duration when GE creates these security factors. In both cases, the security key expiration can be set between 1 and 60 months.

IMPACT OF EXPIRATION

The impact of expiring license and PIN differs:

1. Expired License File

When a license file expires, activation of VistaNET via the license file is no longer permitted. Additionally, existing instances of VistaNET will require a new license file before it continues to operate normally.

A user or administrators should apply for a new license file well in advance of the license file expiry date. Please refer to *License File > Obtaining a new license* for instructions on requesting a new license file.

2. Expired PIN

When the activation PIN expires, administrators will not be able to activate the VistaNET software via the first activation method described herein.

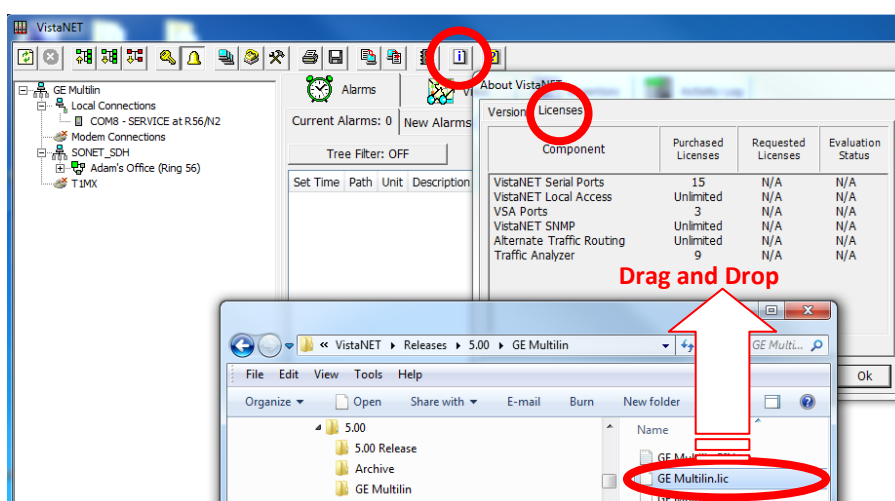


However, the activation PIN is typically needed just once, during the initial activation of VistaNET 5.00. The VistaNET administration team can administer users and user privileges via a valid VistaNET administrative login.

A new pin is only typically needed if an administrator loses their access password. See *'Forgot your administrative account credentials?'*

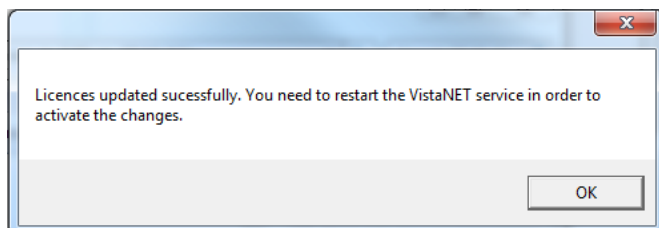
REPLACING AN EXPIRED LICENSE FILE OR ADD A NEW LICENSE

If a license file has expired, VistaNET will prompt the user to Synchronize with a valid license file. Users must request a new license file from GE, and then drag the new license file into the VistaNET Licenses tab. Please refer to *License File > Obtaining a new license* for instructions on requesting a new license file.



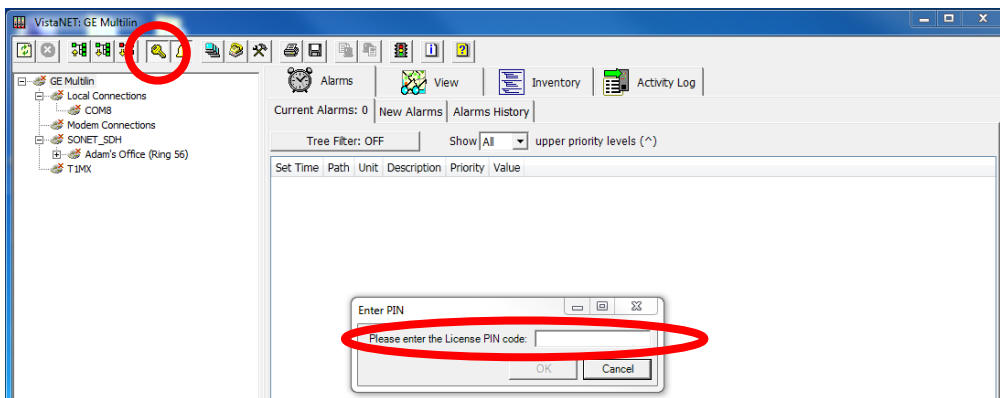
Drag the new license file into the VistaNET Licenses tab.

If the license file is valid, users will be asked to restart the VistaNET service in order to activate the changes.



After restarting the VistaNET service and the VistaNET GUI, the new license file has been successfully integrated, but will require a second security factor to activate it. VistaNET will appear inactive and completely disconnected from the equipment hardware until activation is complete.

This is the same process a customer would follow if a new license feature has been purchased. GE will deliver this new license via the .LIC file. Users need to drag this license file over the VistaNET licenses tab to integrate the new license.



Entering the activation pin is one of three methods described above (see *Activating VistaNET*). The primary VistaNET administrator will receive a corresponding activation PIN to enable the first instance of this new license file.

USER AUTHENTICATION

Starting from version 5.04, VistaNET employs Microsoft Active Directory (AD) and Windows™ Local Accounts to authenticate users. All users previously stored in the VistaNET database will be disabled after migrating to VistaNET 5.04 or higher versions. These disabled accounts are still visible to the user with the “Show Obsolete Accounts” checkbox. A VistaNET administrator must select users from either an AD server, or locally from a pre-defined Windows™ local account. Users added from AD must now login to VistaNET with their network credentials, which are often the same login credentials used to log into their Windows Operating system.

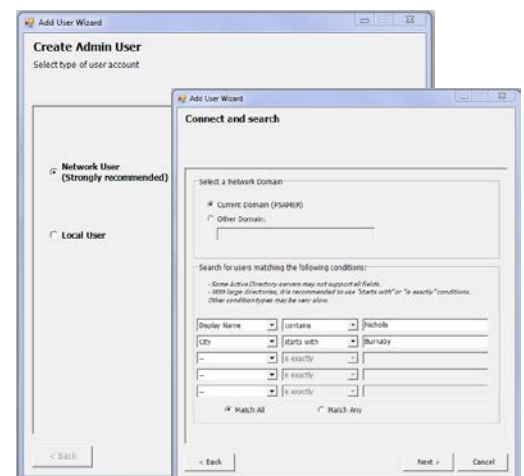
IMPORTANT NOTE: All users stored in the VistaNET database before VistaNET version 5.04 will be deleted after migrating to VistaNET 5.04 or higher. User credential will no longer be stored in the VistaNET database.

ADMINISTRATING USERS

After installing VistaNET 5.04 (or higher) for the first time or upgrading from VistaNET 5.03 (or lower), administrators will be prompted to create an administrator account with one picked from a Network or a Windows Local Account:

1. for new installations of VistaNET, administrators will login with ‘administrator’ as the username and use the ‘PIN’ for the password.
2. for customers upgrading VistaNET, administrators will login with their previous administrative account credentials.

An ‘Add User Wizard’ is included to help administrators add users. After selecting the source from which a user will be added, “Network” or “Local”, the wizard then helps narrow the search criteria when picking from large network domains. A list of users that match the defined search parameters will be available for





selection. After selection, a new administrator account is added into the VistaNET database, and locked to prevent accidental deletion. Adding a second administrative account would permit editing or deletion of the first. Non-administrative user accounts are added the same way, but a GROUP (other than administrator) must be defined.

Each user account stored in VistaNET contains a 'Display name' and a 'Security ID' (SID) value. This Microsoft generated value is uniquely assigned to each user based on their assigned username and domain. This SID is used to securely identify users. A user belonging to different domains would be assigned a different SID, and hence would require a VistaNET account to access each domain controller.

For users not contained in Active Directory VistaNET service would require a Windows Local Account to access VistaNET. Please contact your IT administrator to help set one up. The VistaNET administrator will then require specific Windows account information to create this local user account, which can be extracted automatically by VistaNET.

Typically, adding/editing or deleting user accounts (either network or local) are performed from a central location. This allows the resulting account changes to be distributed via VistaNET synchronization to all remote VistaNET instances. To ensure synchronization is effective to remote users, Administrators must securely communicate the following to all remote users:

- An IP address or host name of the centralized VistaNET service where the user accounts are stored
- User's login instructions
 - For Active Directory: Domain name and reuse of users AD login credentials
 - For Local Windows Account: Host PC name, and reuse of users Window Local Account login credentials

Note: *If firewalls are employed between central and remote VistaNET instances, please refer to the firewall section contained within these release notes.*


Note: *To avoid service interruptions, administrators should work with their IT departments when migration to a new domain is required. Users that are migrating to a new network domain will require a new VistaNET account linked to that domain (a new SID is needed to help authenticate users within VistaNET).*

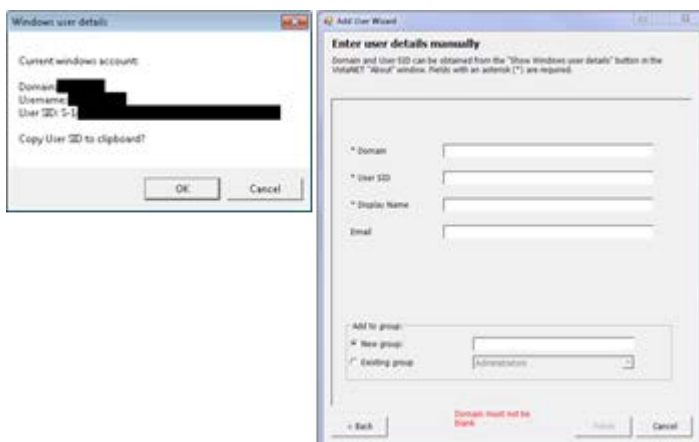
Note: *All users, with Network or Local Windows accounts, require a valid user password. The password field cannot be kept blank.*

ADMINISTRATING LOCAL USERS

To add a local VistaNET user account, an administrator will need to know the user's domain and SID.

To locate this information, administrator will need to ask a user to perform the following actions from the PC where the local user will be logging into VistaNET:

1. login to user's Windows account via their Windows Local Account credentials
2. select the information icon  in VistaNET, running on user's PC
3. select the "Show Windows user details..." button. After pressing this button, the necessary Windows user details are copied to the clipboard which can be emailed off to the VistaNET administrator.



Administrator can complete the 'Enter user details manually' for remote user account when user's domain and SID are provided.

Note: Alternatively, from a command prompt, users can enter in "whoami /user" to obtain the same information.

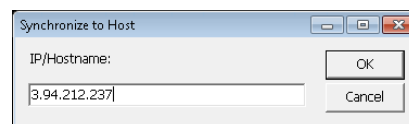
ENABLING REMOTE USERS


Remote VistaNET users upgrading from VistaNET 5.03 or lower versions will not be able to use their previous usernames and passwords to login to VistaNET after the upgrade is complete. Depending on the new user type defined for each individual, remote users will login to VistaNET either by their company assigned network credentials (authenticated by active directory) or their windows local account credentials (authenticated by Windows™). These new user accounts must first be added into VistaNET by the VistaNET administrator.

Typically, adding the new user accounts is performed on a centralized 24/7 instance of VistaNET, and distributed to all remote users via Synchronization. In addition to communicating the type of user account defined for each user, administrators must also provide the IP address or host name of the PC where the new remote user accounts are stored. Synchronization of the data must occur to distribute the access control list to remote users.

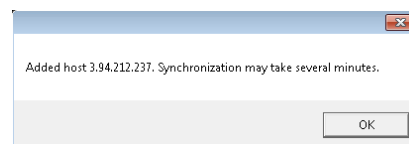
Note: VistaNET does not store user credentials, but does contain a list of 'Display names' and 'Security Identifiers' (SID). Either Microsoft's Active Directory or the local Windows Operating System will authenticate users against their supplied username and passwords.

After installing or upgrading to VistaNET 5.04 or higher version, remote users can quickly synchronize to a targeted 24/7 VistaNET service containing remote user account listings and SIDs through a new "Synchronize to Host" prompt.



Remote users should press the login icon  and select "No" to "Is this the first VistaNET PC to be upgraded". This action will both activate remote VistaNET instances, and synchronize an active control list (ACL).

After a few moments, remote users can now login to VistaNET.



The IP address used to synchronize to Host will be automatically added to the list of unicast IP addresses, contained in the *Administration and Startup Options*, which VistaNET uses periodically (and upon startup) to connect with 24/7 VistaNET instances.

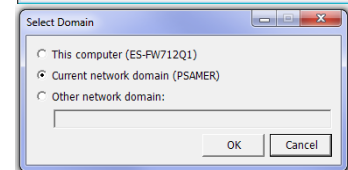
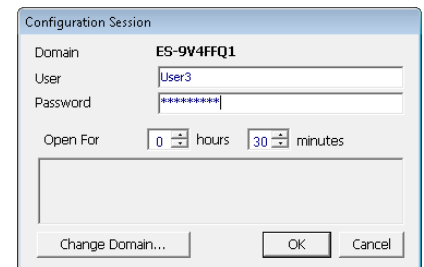


DOMAIN SELECTION

VistaNET 5.04 (or higher) authenticates users against Network or Local Windows accounts. These accounts are aligned with Microsoft's Active Directory or within Windows Local Accounts. VistaNET needs to know which domain the user is attempting to authenticate against. The user login prompt has been modified to allow users to toggle between:

- Network domain preconfigured on their PC,
- Local Host name of their PC, or
- Another domain that can be manually defined by the user

The selected Domain is presented to the user in bold text at the top of the Configuration Session dialog box. A '*Change Domain*' button has been added to this same dialog box to change the selected domain.





LIMITATIONS

The following is a list of known limitations related to VistaNET 5.00. A workaround was provided where applicable. Please note that these items are listed in conjunction to our tracking system ticket number.

- In VNI/VSA networks, restart VistaNET anytime the IP address of the VSA machine changes (for example, from 127.0.0.1 to the external address). Failure to do so may cause some nodes to appear as if they are visible, even if they are not, due to the node controllers for the port not being updated properly in the database. *Workaround:* Restart VistaNET after the IP address changes [ticket #269].
- After upgrading to VistaNET 3.01 and newer, it can be observed that right button in the unit view does not get selected for the pair of units. *Workaround:* Rediscover the node containing the unit. The discovery will update unit side information in the database and resolve the issue [ticket #383].
- It is not allowed to have XPort connection and Craft Interface connection to the same Service unit. If attempted, VistaNET will become unresponsive and the results might be unpredictable [ticket #322]. *Workaround:* First, remove J10 and J11 jumpers on XPort paddleboard to open serial connection to XPort, before connecting to Craft Interface. Then, replace jumpers upon CI disconnect to resume Service Unit to XPort communications.
- When using the Craft Interface to connect to units, it may be observed that Serial Number is not updated properly in the Unit Info box. If serial connection from one unit is quickly switched to another unit with similar unit type and unit option (for example, CDAX option 01) the serial number of the first one will still be shown in the Unit Info box. *Workaround:* When working the units of the same type and option, wait for the COM connection to drop before connecting to another unit or connect to a different unit type first (for example, Service unit) [ticket #293].
- When Rack/Shelf/Slot information changes through local unit configuration, the unit configuration for this unit through NMS will fail if the unit is not rediscovered to apply local changes. *Workaround:* Rediscover the unit every time its Rack/Shelf/Slot information was changed through local configuration [ticket #381].
- In a JIFshare, after physically adding a new DS-0 unit or clearing the DS-0 channel table, allow a couple minutes before initiating discovery on the node this JIFshare belongs to. The JIFshare requires some time to obtain DS-0 unit information required for discovery. If discovery is performed too fast, JIFshare may return incorrect discovery results: presents non-existing units or misses existing units. *Workaround:* If first discovery is incorrect, do rediscover to correct the issue. Or, wait for up to 1 minute before initiating discovery after making changes to JIFshare DS-0 channel table [ticket #23, #321, #345].
- For Windows 2000 users, after upgrading to VistaNET 3.01 and newer, it may be observed that the tree is empty and all previously discovered inventory, by older version of VistaNET, is missing. *Workaround:* Rediscover the entire network. Note that all aliases will be preserved and rediscovery is needed only once after upgrade [ticket #386].
- Rebooting an IPSU without a LAN connection, allowing it to finish discovery and then applying the LAN connection causes the IPSU to not obtain an IP address in DHCP mode. *Workaround:* Reboot IPSU after applying LAN connection [ticket #825].
- If ntp server time is changed abruptly, IPSU needs to be restarted [ticket #826].



NON-VISTANET ISSUES

On occasions, issues that appear to be VistaNET problems are in fact limitations associated with individual units. In some cases, the limitation may be solved with future unit firmware updates. To help users differentiate between unit firmware and VistaNET issues, the following is a list of known unit limitations that have been reported as VistaNET problems.

- 4W unit cannot copy/paste between unit firmware version 2.07 and 2.05. The paste option is reported to be not shown
Response: Copy/paste was removed by design. Significant unit firmware changes made to version 2.06 prevent copy/paste of data between units running these firmware versions
- VistaNET Map view is not clearing alarms and test indications after the L/R optics units are disabled (unchecked) from the Service Unit's GUI
Response: The Service Unit continues to respond to optical issues (alarms and tests) even after the optics units have been disabled.
- The CV count in the OC-3 Error tab does not clear the (section CV) count when Clear counter is selected to be "CV". [ticket#418]
- The VistaNET map (Ring view) shows unexpected alarms on the L/R optics units when AIS-L(T) and AIS-P(R) are enabled [ticket#339]
- Optics units that support SFP transceivers equipped with 'colored' xWDM options shall report their wavelength [ticket#618]

**KNOWN DEFICIENCIES**

The following is a list of known deficiencies related to this VistaNET release. The [ticket number] reflected in the GE Lentrionics deficiency tracking system precedes each deficiency. Note that these deficiencies are worked upon based on a schedule that permits the release of new and awaited features in parallel with improved and correct functionality of the VistaNET NMS system.

Ticket	Summary	Component
<u>#111</u>	<u>VNET-871: OC-XX: JIF Port tabs->Multiple JIFshares in one JIFport/slot assignment</u>	<u>OpticUnits</u>
<u>#161</u>	<u>Sometimes Configure and Cancel Buttons do not get enabled when a configuration is desired [Workaround: Restart or just close and re-open VistaNET and re-select the unit]</u>	<u>Other</u>
<u>#306</u>	<u>Modem Lockout jumper is not functional [Workaround: None]</u>	<u>Security</u>
<u>#425</u>	<u>J-Sync shows incorrect ssm information in some cases</u>	<u>GUI</u>
<u>#426</u>	<u>Occasionally an alarm status in the main tab of OC-3 is not properly refreshed</u>	<u>GUI</u>
<u>#483</u>	<u>STM-16: Discovered node not accurately shown when asymmetrical configurations exist on the node.</u>	<u>Discovery</u>
<u>#500</u>	<u>When selecting a COM port item in local connections, the "open unit window" option opens an empty GUI</u>	<u>GUI</u>
<u>#522</u>	<u>In T1MX Spur, Multiple T1MX trees painted when the group value at L0 is changed</u>	<u>T1MX/E1MX</u>
<u>#523</u>	<u>CDAXs that have their group and node number changed are not accessible anymore</u>	<u>T1MX/E1MX</u>
<u>#524</u>	<u>Discovery fails Intermittently after one or more nodes deleted from the discovered ring</u>	<u>Discovery</u>
<u>#526</u>	<u>T1MX discovery incorrectly show L0 CDAX that doesn't support T1 Spur</u>	<u>Discovery</u>
<u>#533</u>	<u>Audible alarm button is non functional</u>	<u>Alarms</u>
<u>#538</u>	<u>Ring and node number for level 0 CDAX still shows on the unit after it is relocated</u>	<u>T1MX/E1MX</u>
<u>#539</u>	<u>The new setting of a moved CDAX from level 0 to a level N location still accessible from L0 icon</u>	<u>GUI</u>
<u>#545</u>	<u>In T1MX, the Data unit path identifier at Level 0 does not meet the requirement</u>	<u>T1MX/E1MX</u>
<u>#549</u>	<u>Aliases are not shown in the alarm engine "Unit path" field</u>	<u>Alarms</u>
<u>#578</u>	<u>Inconsistent alarm information on tree view</u>	<u>GUI</u>
<u>#579</u>	<u>Tree does not paint correct information on JIF-Share under OC-12</u>	<u>GUI</u>
<u>#583</u>	<u>VistaNET freezes during configuration when unit changes rack shelf slot info</u>	<u>DataAccess</u>
<u>#598</u>	<u>STM-16: Connecting TU12-structured TUG-3s to Bulk TUG-3 slots on CBW ports</u>	<u>GUI</u>
<u>#640</u>	<u>SRP - Alias for DS0 circuit in alarm history</u>	<u>Alarms</u>
<u>#691</u>	<u>Multiple unit user controls are displayed on top of each other when clicking around on the tree quickly</u>	<u>GUI</u>
<u>#697</u>	<u>Date drop down and "next" (>>) button are not updated when VistaNET is running for more than 1 day</u>	<u>GUI</u>
<u>#705</u>	<u>Order of units in Inventory XML file does not reflect the parent/child relationship of the network</u>	<u>GUI</u>
<u>#716</u>	<u>Nodes controlled by IPSU are not released during firmware upgrade using the Craft</u>	<u>IPSU</u>



Ticket	Summary	Component
	<u>Interface</u>	
<u>#717</u>	<u>VistaNET Local IP display in Status Tab Does Not UPdate With A Change in IP address</u>	<u>GUI</u>
<u>#730</u>	<u>IPSU GUI: Disable fields associated with new IPSU when connected to old IPSU</u>	<u>GUI</u>
<u>#733</u>	<u>VSA enable/disable should be available to administrators only</u>	<u>GUI</u>
<u>#779</u>	<u>VistaNET does not show correct option numbers for certain TN1U/TN1Ue units</u>	<u>GUI</u>
<u>#780</u>	<u>4W VF Unit Loopback field not coloured in blue</u>	<u>GUI</u>
<u>#785</u>	<u>Dead JIF-DS1 causes bogus DS0 alarm and VT test</u>	<u>GUI</u>
<u>#791</u>	<u>A 4W single channel unit sometimes is displayed with left and right sides</u>	<u>Discovery</u>
<u>#796</u>	<u>Terminal Window does not get displayed after Modem has connected</u>	<u>DataAccess</u>
<u>#799</u>	<u>CDAX T1 port LOS alarm is displayed when alarm is disabled and multiple alarms exist</u>	<u>DataAccess</u>
<u>#803</u>	<u>Yellow text box on L0 CDAX does not appear if the unit is set as G0N0</u>	<u>GUI</u>
<u>#813</u>	<u>IPSU sometimes does not reset correctly when issued RESET command from VistaNET</u>	<u>GUI</u>
<u>#815</u>	<u>Simultaneous and differing configurations to the same JIFPort slot can corrupt optical units and hang VistaNET displays</u>	<u>GUI</u>
<u>#820</u>	<u>Menu bar dialog box has inconsistent behaviour</u>	<u>GUI</u>
<u>#821</u>	<u>Passport file company name too long for IPSU "Company Name" field</u>	<u>GUI</u>
<u>#827</u>	<u>VistaNET sometimes displays an exception when selecting the unit of an alarm</u>	<u>GUI</u>
<u>#832</u>	<u>Wrong error message for Serial-over-IP link to NMX unit</u>	<u>GUI</u>
<u>#833</u>	<u>VSA license checkbox is N/A to Serial-over-IP links to NMX unit</u>	<u>GUI</u>
<u>#839</u>	<u>Strong Arm IPSU shows wrong Processor Info</u>	<u>GUI</u>
<u>#846</u>	<u>Unknown publisher, VistaNET code is not signed</u>	<u>GUI</u>
<u>#850</u>	<u>Traffic Manager does not display E100 under OC-3</u>	<u>GUI</u>
<u>#852</u>	<u>VistaNET 4.00 Performance</u>	<u>GUI</u>
<u>#870</u>	<u>OC48 Sometimes displays "VT" in the CBW cross connect</u>	<u>GUI</u>
<u>#872</u>	<u>VistaNET show invalid argument during discovery</u>	<u>GUI</u>
<u>#885</u>	<u>CDAX reset returns (expected?) exception with hresult = 0x80591099</u>	<u>GUI</u>
<u>#897</u>	<u>VistaNET 4.06: IPSU GUI: Software Licensing frame always reports as IPSU0406</u>	<u>GUI</u>
<u>#901</u>	<u>Cannot shutdown VistaNET gracefully per services.msc method</u>	<u>GUI</u>
<u>#923</u>	<u>Synchronized VistaNET PC services only forward alarms from the locally monitored network and not from synchronized services, even though synchronized alarms are in the alarm engine</u>	<u>VSNMP</u>
<u>#926</u>	<u>Unplug CI cable while discovering a network will cause VistaNetService crash</u>	<u>Discovery</u>
<u>#927</u>	<u>VistaNET does not check in the background if a unit has been put to sleep.</u>	<u>DataAccess</u>
<u>#938</u>	<u>Alias disappearing on G703 circuits</u>	<u>GUI</u>
<u>#940</u>	<u>Potential race condition when attempting to add Redirected Serial over IP connections</u>	<u>GUI</u>
<u>#950</u>	<u>Bogus NMS alarms when simultaneous Alarm, Alert (and Test) are reported from DS0 level unit</u>	<u>GUI</u>
<u>#954</u>	<u>VistaNET should display a more meaningful error message instead of</u>	<u>GUI</u>



Ticket	Summary	Component
<u>#956</u>	<u>DISP_E_TYPEREMISMATCH when the company id does not match</u> <u>Nx64F is shown as Nx64 in the SNMP entry</u>	<u>VSNMP</u>
<u>#959</u>	<u>Expired License + PIN number license file can be made to work again by changing the time and date on the local PC</u>	<u>Security</u>
<u>#962</u>	<u>Unit view doesn't appear when connected to CI although unit is detected and displayed in tree</u>	<u>GUI</u>
<u>#967</u>	<u>Inconsistency when adding Group Name between the Users and Groups Tab of the Administration & Startup Options window</u>	<u>GUI</u>
<u>#970</u>	<u>Treeview not loading after improper server shutdown</u>	<u>GUI</u>
<u>#977</u>	<u>Alarm engine description incorrect for STS level alarms</u>	<u>GUI</u>
<u>#978</u>	<u>VNI client not shutting synchronization when another VNI client service is shutdown</u>	<u>GUI</u>
<u>#980</u>	<u>VistaNET synced with another *.lic file on network</u>	<u>GUI</u>
<u>#984</u>	<u>Ring Icon shows erroneous JMUX alarm status for non-existent side of linear system in System/Network Map View</u>	<u>DataAccess</u>
<u>#1021</u>	<u>Restart of VistaNET service required when PC comes back from standby or hibernation</u>	<u>Other</u>
<u>#1023</u>	<u>STM-16 Unit Fibre View does not display Unit and FOT Temperatures</u>	<u>GUI</u>
<u>#1024</u>	<u>STM-16: NMS Location cannot be properly set</u>	<u>GUI</u>
<u>#1025</u>	<u>STM-16: Individual VC-4 loopbacks available when AUG-4 is set for VC-4-4c mode</u>	<u>GUI</u>
<u>#1026</u>	<u>System Tree Labels incorrect (shows SONET & T1MX for SDH .lic file)</u>	<u>GUI</u>
<u>#1027</u>	<u>Multiple CBW Tie Links can be entered in Network Map View</u>	<u>GUI</u>
<u>#1034</u>	<u>CDAX Spur links are not present in Traffic table</u>	<u>Discovery</u>
<u>#1038</u>	<u>Modem connections are displayed on the Local Connections tree</u>	<u>Discovery</u>
<u>#1043</u>	<u>Service locks up when trying to shut down while modem is connected</u>	<u>DataAccess</u>
<u>#1047</u>	<u>Node View does not update when status changes</u>	<u>GUI</u>
<u>#1049</u>	<u>GUI does not switch properly when craft interface cable is moved to a different unit</u>	<u>GUI</u>
<u>#1055</u>	<u>Active Directory sometimes times out when attempting search by employee ID</u>	<u>Security</u>
<u>#1057</u>	<u>Removing a JVT TIE in map view</u>	<u>GUI</u>
<u>#1059</u>	<u>"Open Unit Window" shows invalid data when the CI connection is changed to different unit</u>	<u>GUI</u>
<u>#1060</u>	<u>DTT-RCV (86442-01) shows an invalid channel number in the tree and path elements</u>	<u>GUI</u>
<u>#1062</u>	<u>Tree shows unit as dead instead of in alarm when one or more but not all VTs/Channels are dead</u>	<u>DataAccess</u>
<u>#1063</u>	<u>right unit in connected CDAX pair shows as serial number for first 5 minutes after power cycling node</u>	<u>DataAccess</u>
<u>#1064</u>	<u>Contact I/O woken up from sleep mode displays "Invalid" channel</u>	<u>GUI</u>
<u>#1066</u>	<u>Orderwire unit configuration issue</u>	<u>GUI</u>
<u>#1067</u>	<u>External Sync Units must appear above aggregate units in System Tree</u>	<u>GUI</u>
<u>#1068</u>	<u>Any remote change in CDAX CC tab for a T1/Optic port sets its 'Alarm Enable' to enabled</u>	<u>GUI</u>
<u>#1069</u>	<u>Clearing red fields on the Node Icon upon reestablishing communication to its Service</u>	<u>GUI</u>



Ticket	Summary	Component
	<u>Unit</u>	
<u>#1070</u>	<u>86486-21 E1CDAX Ring GUI Support</u>	<u>GUI</u>
<u>#1071</u>	<u>VistaNET 5.04 Log In Problem</u>	<u>GUI</u>
<u>#1073</u>	<u>Invalid IP Address '127.0.0.1' gets stuck in database</u>	<u>DataAccess</u>
<u>#1074</u>	<u>Save Unit Data to File on Unit with Multiple Channels or VTs sometimes fails if not all elements are configured</u>	<u>DataAccess</u>
<u>#1078</u>	<u>The "Locate Unit" menu option does not display "in T1MX" or "in SONET"</u>	<u>GUI</u>
<u>#1079</u>	<u>"Grey Box" in status bar does not display 3D relief</u>	<u>GUI</u>
<u>#1083</u>	<u>Setting all channels to "Thru" and then attempting to change a single channel back does not work on JIF-Share-02/CMUX-22</u>	<u>GUI</u>
<u>#1084</u>	<u>T1/E1 Unit does not display alarms under certain conditions</u>	<u>Alarms</u>
<u>#1087</u>	<u>VistaNET believes that it is still connected to a USB to RS232 Converter when the USB to RS232 Converter is disconnected from the USB Port</u>	<u>GUI</u>
<u>#1088</u>	<u>VistaNET Current Alarms count is erroneous when VSA'ed and there is time difference between the VistaNETs.</u>	<u>GUI</u>
<u>#1096</u>	<u>VistaNET GUI Does Not Exit Gracefully when VistaNET Service Stops</u>	<u>GUI</u>
<u>#1097</u>	<u>Active Services May Not Display Peer IP</u>	<u>GUI</u>
<u>#1100</u>	<u>Inconsistent Inventory Counts for CDAXes in SONET and T1MX Spurs</u>	<u>GUI</u>
<u>#1102</u>	<u>Local connection to a CSSU continually drops out and takes a very long time to stabilize.</u>	<u>GUI</u>
<u>#1103</u>	<u>Tie Info Tab on the TIE unit GUI does not refresh</u>	<u>GUI</u>
<u>#1104</u>	<u>TIE Unit Bad Tie Cable Alarm does not show on the tree view</u>	<u>GUI</u>
<u>#1105</u>	<u>Serial Connection Drop-off</u>	<u>GUI</u>
<u>#1106</u>	<u>Cannot Remotely Configure NMS Channel at Level 0 T1/ E1 CDAX</u>	<u>GUI</u>
<u>#1108</u>	<u>"Launch VistaNET" checkbox not working in installer</u>	<u>GUI</u>
<u>#1113</u>	<u>Data-Nx64F: Mistakenly exposed Transmit and Expected Circuit Addresses</u>	<u>GUI</u>
<u>#1114</u>	<u>E1 CDAX: problem pasting the hairpins on the E1 port</u>	<u>GUI</u>
<u>#1116</u>	<u>JIF-Share/CMUX/CDAX Channel Force Offline feature should be designated 'RS' rather than 'RW'</u>	<u>JIF/TIFUnits</u>
<u>#1118</u>	<u>OC-48 GUI Exception when toggling between right and left units if backup tab was selected</u>	<u>GUI</u>
<u>#1119</u>	<u>Ether-1000: Doesn't allow configuring SPE Slots by non-admin users in High Security Mode</u>	<u>GUI</u>
<u>#1120</u>	<u>Upgrading from VistaNET 5.02 or earlier to 5.04 or 5.06 may remove some DS0 alias</u>	<u>GUI</u>

**FIXED DEFICIENCIES**

The following deficiencies were identified corrected and validated prior to this release at GE Lenronics. They are listed here as a reference to your reported earlier problems and also as a record of the shared knowledge base with the VistaNET user base:

Ticket	Summary	Component
<u>#1081</u>	<u>JIF-Share-02: GUI Minor issues</u>	<u>GUI</u>

FIXED DEFICIENCIES - VERIFYING

The following deficiencies were identified and corrected prior to this release at GE Lenronics but validation of the issue continues. These issues remain open. They are listed here as a reference to your reported earlier problems and also as a record of the shared knowledge base with the VistaNET user base:

Ticket	Summary	Component
<u>#1076</u>	<u>Add "Enable Channel Mismatch Check" to Nx64F</u>	<u>GUI</u>
<u>#1094</u>	<u>Add New Tie Connection Exhibits Erratic Behaviour</u>	<u>GUI</u>
<u>#1098</u>	<u>Tie Connections Are Not Synchronized Correctly in the Map View</u>	<u>GUI</u>
<u>#1109</u>	<u>VistaNET not fully installed after upgrading</u>	<u>GUI</u>
<u>#1117</u>	<u>AD Login requires "Access this computer from the network" right</u>	<u>Security</u>