

NMXTM

NETWORK MANAGEMENT SYSTEM

Release 8.8.0

Installation Guide

Manual Part No. BookPartNumber
September 2020

Copyright © 2015–2020 Harmonic Inc. All rights reserved. Harmonic, the Harmonic logo, Omneon, the Omneon logo, [all other Harmonic products mentioned] are trademarks, registered trademarks or service marks of Harmonic Inc. in the United States and other countries. Dolby, Dolby Digital, Dolby Digital Plus and Dolby E are registered trademarks of Dolby Laboratories. Implementations of AAC and HE-AAC by Fraunhofer IIS. Other company, product and service names mentioned herein may be trademarks or service marks of their respective owners. All product and application features and specifications are subject to change at Harmonic's sole discretion at any time and without notice.

Disclaimer

Harmonic® reserves the right to alter the product specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty. The information contained herein is merely descriptive in nature, and does not constitute a binding offer for sale of the product described herein. Harmonic assumes no responsibility or liability arising from the use of the products described herein, except as expressly agreed to in writing by Harmonic. The use and purchase of this product does not convey a license under any patent rights, copyrights, trademark rights, or any intellectual property rights of Harmonic. Nothing hereunder constitutes a representation or warranty that using any product in the manner described herein will not infringe any patents of third parties.

Third-party product trademarks

Adobe® After Effects®, Photoshop®, Flash® Professional, Premiere®
Avid® Media Composer®
Jünger Audio™
Apple® QuickTime®
Microsoft® Mediaroom®
Microsoft PlayReady®
DOCSIS® 3.0
Start Over® TV

CentOS 7™

Dolby is a registered trademark of Dolby Laboratories.

Dolby Digital, Dolby Digital Plus, Dolby Pulse, aacPlus, AC-3, and Dolby® E are trademarks of Dolby Laboratories.

Level Magic and Jünger are trademarks of Jünger Audio Studioteknik GmbH.

MPEG Audio technology licensed from Fraunhofer IIS <http://www.iis.fraunhofer.de/amm/>.

PitchBlue® is a registered trademark of Vigor Systems.

QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom.

Third-party copyright notes

Harmonic software uses version 3.15.4 of the FreeImage open source image library under FreeImage Public License (FIPL). See <http://freeimage.sourceforge.net> for details. The product may include implementations of AAC and HE-AAC by Fraunhofer IIS; and MPEG Audio technology licensed from Fraunhofer IIS.

The software described in this publication may use version 2.8 of FFmpeg open source package under Lesser General Public License (LGPL).



The software described in this publication is furnished under a nondisclosure agreement, or the License Agreement and Limited Warranty stated below, and the end user license agreement (which is furnished with the software), which may have additional terms. The software may be used or copied only in accordance with the terms of those agreements. By using the software, you acknowledge you have read the end user license agreement and the License Agreement and Limited Warranty provision.

The product described in this publication maybe covered by one or more of U.S. Patents, their foreign counterparts and pending patent applications.

The product is distributed with certain other software that may require disclosure or distribution of licenses, copyright notices, conditions of use, disclaimers and/or other matter. Use of this product or otherwise fulfilling their conditions constitutes your acceptance of it, as necessary. Copies of such licenses, notices, conditions, disclaimers and/or other matter are available in any one of the following locations: the LEGAL NOTICES AND LICENSES section of the documentation directory of the product, user guide, or by contacting us at support@harmonicinc.com.

Notice

Information contained in this publication is subject to change without notice or obligation. While every effort has been made to ensure that the information is accurate as of the publication date, Harmonic, Inc. assumes no liability for errors or omissions. In addition, Harmonic, Inc. assumes no responsibility for damages resulting from the use of this guide.

License agreement and limited warranty

1. AGREEMENT: This is a legal agreement ("Agreement") between you ("you" or "your") and Harmonic, or its appropriate local affiliate ("Harmonic", "we", "us" or "our"). Use of our product(s) and any updates thereto purchased or validly obtained by you (the "Products"), and/or the Software (as defined below) (collectively, the "System"), constitutes your acceptance of this Agreement. "Use" includes opening or breaking the seal on the packet containing this Agreement, installing or downloading the Software as defined below or using the Software preloaded or embedded in your

-
- System. As used herein, the term "Software" means the Harmonic owned software and/or firmware used in or with the Products and embedded into, provided with or loaded onto the Products in object code format, but does not include, and this Agreement does not address, any third-party or free or open source software separately licensed to you ("Third Party Software"). If you do not agree to this Agreement, you shall promptly return the System with a dated receipt to the seller for a full refund.
2. **LICENSE:** Subject to the terms and conditions of this Agreement (including payment), we hereby grant you a nonexclusive, nontransferable license to use the object code version of the Software embedded into, provided solely for use with or loaded onto the Product, and the accompanying documentation ("Documentation") for your internal business purposes. The Software and any authorized copies are owned by us or our suppliers, and are protected by law, including without limitation the copyright laws and treaties of the U.S.A. and other countries. Evaluation versions of the Software may be subject to a time-limited license key.
 3. **RESTRICTIONS:** You (and your employees and contractors) shall not attempt to reverse engineer, disassemble, modify, translate, create derivative works of, rent, lease (including use on a timesharing, applications service provider, service bureau or similar basis), loan, distribute, sublicense or otherwise transfer the System, in whole or part except to the extent otherwise permitted by law. The Software may be operated on a network only if and as permitted by its Documentation. You may make one (1) back up copy of the object code of the Software for archival purposes only. Evaluation Software will be run in a lab, nonproductive environment. Results of any benchmark or other performance tests may not be disclosed to any third party without our prior written consent. Title to and ownership of the Software and Documentation, and all copyright, patent, trade secret, trademark, and other intellectual property rights in the System, shall remain our or our licensors' property. You shall not remove or alter any copyright or other proprietary rights notice on the System. We reserve all rights not expressly granted.
 4. **LIMITED WARRANTY:** (a) Limited Warranty. We warrant to you that, commencing on your receipt of a Product and terminating 1 year thereafter, the System will perform substantially in accordance with its then-current appropriate Documentation. The Product (including replacements) may consist of new, used or previously-installed components. (b) Remedies. If the System fails to comply with such warranty during such period, as your sole remedy, you must return the same in compliance with our product return policy, and we shall, at our option, repair or replace the System, provide a workaround, or refund the fees you paid. Replacement Systems are warranted for the original System's remaining warranty period. (c) Exclusions. EVALUATION SOFTWARE IS LICENSED ON AS-IS BASIS AND SUBJECT TO 4(d). We will have no obligation under this limited warranty due to: (i) negligence, misuse or abuse of the System, such as unusual physical or electrical stress, misuse or accidents; (ii) use of the System other than in accordance with the Documentation; (iii) modifications, alterations or repairs to the System made by a party other than us or our representative; (iv) the combination, operation or use of the System with equipment, devices, software or data not supplied by us; (v) any third party hardware or Third Party Software, whether or not provided by us; (vi) any failure other than by us to comply with handling, operating, environmental, storage or maintenance requirements for the System in the Documentation, including, without limitation, temperature or humidity ranges. (d) Disclaimers. We are not responsible for your software, firmware, information, or data contained in, stored on, or integrated with any Product returned to us for repair or replacement. SUCH LIMITED WARRANTY IS IN LIEU OF, AND WE SPECIFICALLY DISCLAIM, ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. WE DO NOT WARRANT THAT THE SYSTEM WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED OR ERROR-FREE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM US OR ELSEWHERE, WILL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so such exclusions may not apply to you. In that event, such implied warranties or limitations are limited to 60 days from the date you purchased the System or the shortest period permitted by applicable law, if longer. This warranty gives you specific legal rights and you may have other rights which vary from state to state or country to country.
 5. **LIMITATION OF LIABILITY:** WE AND OUR AFFILIATES, SUPPLIERS, LICENSORS, OR SALES CHANNELS ("REPRESENTATIVES") SHALL NOT BE LIABLE TO YOU FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO LOST REVENUES, PROFITS OR SAVINGS, OR THE COST OF SUBSTITUTE GOODS, HOWEVER CAUSED, UNDER CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, EVEN IF WE WERE ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. NOTWITHSTANDING ANY OTHER PROVISIONS OF THIS AGREEMENT, WE AND OUR REPRESENTATIVES' TOTAL LIABILITY TO YOU ARISING FROM OR RELATING TO THIS AGREEMENT OR THE SYSTEM SHALL BE LIMITED TO THE TOTAL PAYMENTS TO US UNDER THIS AGREEMENT FOR THE SYSTEM. THE FOREGOING LIMITATIONS SHALL NOT APPLY TO DEATH OR PERSONAL INJURY TO PERSONS OR TANGIBLE PROPERTY IN ANY JURISDICTION WHERE APPLICABLE LAW PROHIBITS SUCH LIMITATION. YOU ARE SOLELY RESPONSIBLE FOR BACKING UP YOUR DATA AND FILES, AND HEREBY RELEASE US AND OUR REPRESENTATIVES FROM ANY LIABILITY OR DAMAGES DUE TO THE LOSS OF ANY SUCH DATA OR FILES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO SUCH EXCLUSIONS MAY NOT APPLY TO YOU.
 6. **CONFIDENTIALITY:** Information in the System and the associated media, as well as the structure, organization and code of the Software, are proprietary to us and contain valuable trade secrets developed or acquired at great expense to us or our suppliers. You shall not disclose to others or utilize any such information except as expressly provided herein, except for information (i) lawfully received by the user from a third party which is not subject to confidentiality obligations; (ii) generally available to the public without breach of this Agreement; (iii) lawfully known to the user prior to its receipt of the System; or (iv) required by law to be disclosed.
 7. **SUPPORT:** Updates, upgrades, fixes, maintenance or support for the System (an "Upgrade") after the limited warranty period may be available at separate terms and fees from us. Any Upgrades shall be subject to this Agreement, except for additional or inconsistent terms we specify. Upgrades do not extend the limited warranty period.
 8. **TERM; TERMINATION:** The term of this Agreement shall continue unless terminated in accordance with this Section. We may terminate this Agreement at any time upon default by you of the license provisions of this Agreement, or any other material default by you of this Agreement not cured with thirty (30) days after written notice thereof. You may terminate this Agreement any time by terminating use of the System. Except for the first sentence of Section 2 ("License") and for Section 4(a) ("Limited Warranty"), all provisions of this Agreement shall survive termination of this Agreement. Upon any such termination, you shall certify in writing such termination and non-use to us.
 9. **EXPORT CONTROL:** You agree that the Products and Software will not be shipped, transferred, or exported into any country or used in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions, or regulations (the "Export Laws"). You will indemnify, defend and hold us harmless from any and all claims arising therefrom or relating thereto. In addition, if the Products or Software are identified as export controlled items under the Export Laws, you represent and warrant that you are not a citizen, or otherwise located within, an embargoed nation (including without limitation Iran, Iraq, Syria, Sudan, Libya, Cuba, North Korea, and Serbia) and that you are not otherwise prohibited under the Export Laws from receiving the Software. All rights to the Products and Software are granted on condition that such rights are forfeited if you fail to comply with the terms of this Agreement.
 10. **U.S. GOVERNMENT RIGHTS:** The Software and the documentation which accompanies the Software are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such

terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government as end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Harmonic, 2590 Orchard Parkway, San Jose, CA 95131, U.S.A.

11. **GENERAL:** You shall not assign, delegate or sublicense your rights or obligations under this Agreement, by operation of law or otherwise, without our prior written consent, and any attempt without such consent shall be void. Subject to the preceding sentence, this Agreement binds and benefits permitted successors and assigns. This Agreement is governed by California law, without regard to its conflicts of law principles. The U.N. Convention on Contracts for the International Sale of Goods is disclaimed. If any claim arises out of this Agreement, the parties hereby submit to the exclusive jurisdiction and venue of the federal and state courts located in Santa Clara County, California. In addition to any other rights or remedies, we shall be entitled to injunctive and other equitable relief, without posting bond or other security, to prevent any material breach of this Agreement. We may change the terms, conditions and pricing relating to the future licensing of our Systems and other intellectual property rights, including this Agreement, from time to time. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, the remaining parts will be enforced to the maximum extent permitted. There are no third-party beneficiaries to this Agreement. We are not bound by additional and/or conflicting provisions in any order, acceptance, or other correspondence unless we expressly agree in writing. This Agreement is the complete and exclusive statement of agreement between the parties as to its subject matter and supersedes all proposals or prior agreements, verbal or written, advertising, representations or communications concerning the System.

Every reasonable attempt has been made to comply with all licensing requirements for all components used in the system. Any oversight is unintentional and will be remedied if brought to the attention of Harmonic at support@harmonicinc.com.

Documentation conventions

In Harmonic documents, special symbols and fonts call your attention to important information.

-  **DANGER:** The Danger symbol indicates information that, if ignored, can cause physical harm to you.
-  **CAUTION:** The Caution symbol indicates information that, if ignored, can adversely affect the performance of your Harmonic product, or that can make a procedure needlessly difficult.
-  **NOTE:** The Note symbol indicates especially important information you need, or it may provide additional information that applies in only some carefully delineated circumstances.
-  **IMPORTANT:** The Important symbol indicates information that should stand out when you are reading product details and procedural information.
-  **TIP:** The Tip symbol indicates parenthetical information that is not necessary for performing a given procedure, but which, if followed, makes the procedure easier, smoother, or more efficient.

In addition to these symbols, this guide may use the following text conventions:

Convention	Explanation
Typed Command	Indicates the text that you type in at the keyboard prompt.
Ctrl, Ctrl + Shift	A key or key sequence to press.
http://www.harmonicinc.com	The italics in blue text to indicate Cross-references, and hyperlinked cross-references in online documents.
Bold	Indicates a button to click, or a menu item to select.
Screen Output	The text that is displayed on a computer screen.
<i>Emphasis</i>	The italics text used for emphasis and document references.

Table of Contents

Chapter 1: Introduction.....	8
NMX Architecture.....	8
NMX Server.....	9
NMX Client.....	9
NMX Database.....	9
NMX Rear Panels.....	10
Intel Wildcat Server.....	10
HPE ProLiant DL 360 Gen 10 Server.....	11
NMX Licensing support.....	11
Viewing license names and descriptions.....	12
Viewing time remaining on your NMX license.....	12
NMX Delivery Package.....	13
Accessing NMX documentation.....	14
Supported languages and keyboards.....	15
Chapter 2: Installing NMX Server on Win 2019/SQL 2017.....	16
NMX Server 8.5.x and later system requirements.....	16
Supported hardware and software platforms.....	18
Supported recovery images.....	19
About antivirus definition files.....	19
Installing NMX Server for the first-time overview.....	19
Deploying the recovery image overview.....	19
Logging in to Windows 2019 Server.....	21
Offline Windows Server 2019 license activation.....	22
Changing the NMX Server name and Domain.....	23
Assigning NMX Server IP addresses.....	23
Assigning NMX Server IP addresses with no DNS server.....	24
Downloading the NMX installation package.....	25
Installing a new version of NMX Server software.....	25
Logging in to NMX Domain Manager.....	31
Creating a new database catalog.....	32
Starting the NMX Server.....	32
Installing NMX Client only overview.....	33
NMX Client system requirements.....	33
Installing NMX Client software.....	34
Installing NMX VM overview.....	35
NMX VM system requirements.....	35
Deploying the NMX VM .OVA template.....	36
Deploying multiple instances of NMX .OVA overview.....	38
Logging in to NMX VM.....	40
About certificates.....	40

Installing a certificate in Trusted Root Authorities directory.....	40
Configuring custom SSL certificates for REST API.....	41
Enabling SSL encryption for SQL Server.....	42
Chapter 3: Converting a Windows Server 2019 machine to an NMX server.....	43
Required software for conversion.....	43
Installing SQL Server 2017.....	43
Launching SQL Server Management Studio 18.....	45
Launching the SQL Server Configuration Manager.....	45
Installing the SNMP service.....	46
Installing the IIS Web Server.....	47
Adding Server Manager Features.....	50
Configuring DCOM settings.....	50
Configuring TCP/IP parameters.....	50
Configuring Local Security Policy.....	51
Completing the conversion.....	53
Chapter 4: Migrating a Windows 2012 Server to a Windows 2019 Server for NMX.....	54
Method 1: Using the Domain Manager.....	54
Method 2: Using PowerShell scripts.....	55
Chapter 5: Upgrading NMX Server.....	57
Upgrading NMX overview.....	58
Backing up catalogs.....	61
Uninstalling NMX.....	62
Downloading the NMX installation package.....	62
Upgrading the NMX Server software.....	62
Logging in to Windows 2019 Server.....	63
Upgrading the NMX catalog.....	64
Upgrading NMX Client software.....	65
Device end of service information for NMX 8.5.x and later.....	65
Upgrading to NMX 8.4 and later.....	65
Device end of service information for NMX 8.x and later.....	66
Upgrading from NMX 6.x to NMX 7.x (catalog sync IDs).....	66
Upgrading NMX catalogs.....	66
Upgrading catalogs after first-time NMX installation.....	67
Activating catalogs.....	68
Starting the NMX Server.....	69
Upgrading Java JRE.....	69
Upgrading the JRE.....	70
Upgrading Apache Tomcat.....	70
Chapter 6: Monitoring HPE Server Alarms.....	73
Enabling the iLO interface.....	73
Configuring the static IP address.....	73
Configuring the Alarms Options.....	74
Chapter 7: Troubleshooting NMX.....	75
Connecting NMX to VOS after upgrade.....	75
NMX redundancy.....	75

NMX Bootp process and Cisco switches.....	76
SNMP reset.....	76
Getting device logs.....	77
Sending log files to Harmonic Technical Support.....	77
 Appendix A: Harmonic Technical Assistance Center contact information.....	 78
Harmonic corporate contact information.....	79

Chapter 1

Introduction

NMX is a video network management tool built on a scalable client/server architecture that runs on Microsoft Windows Server® 2019 with SQL Server® 2017.

Review the NMX Server system requirements to accurately plan for your installation or upgrade.

- [NMX Architecture](#)
- [NMX Server](#)
- [NMX Client](#)
- [NMX Database](#)
- [NMX Rear Panels](#)
- [NMX Licensing support](#)
- [NMX Delivery Package](#)
- [Supported languages and keyboards](#)

NMX Architecture

The NMX layered software architecture includes client/server applications, and embedded hardware and software applications.

NMX saves device and service configurations to the ORS (Object Repository/SQL Server database) and interfaces with Element Managers to control devices.

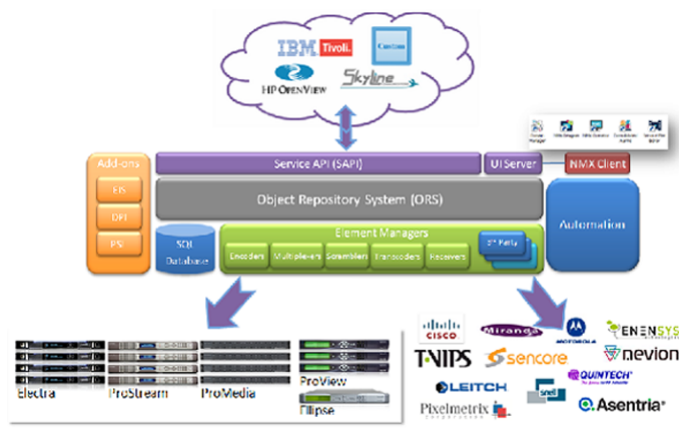


Figure 1-1: NMX architecture

NMX Server

NMX Server is a PC-based computer running Microsoft SQL Server 2017. It can be provided by Harmonic with a pre-configured Operating System (OS), database server and NMX Software, or the server can be a custom hardware platform provided by customer. In the latter case, the platform and OS must comply to minimum requirements described in the “NMX Server 8.5.x and later system requirements” section of the NMX Installation Guide.

All internal and network communication between NMX applications, processes, and configurations is through the ORS.

-  **IMPORTANT:** Installing the NMX Client will install the GUI application software and associated documentation, but not the NMX Server or NMX Daemons.
-  **Attention:** It is recommended that after installing the NMX server to change the default password using SQL Server Management Studio.

NMX Client

The NMX Client software comprises the GUI applications that are the interface to the NMX Server.

When you install NMX Server, the NMX Client is installed, but you can install up to 25 stand-alone NMX Client instances on remote computers. Selecting to install only the NMX Client will install all NMX applications except the NMX Server and the NMX Daemons application (which reports BootIP Server, TFTP Server, and DPI Server messages and performance).

Multiple NMX Client instances can be placed anywhere on the network and you can access any system function on any network group, regardless of its geographical location. NMX supports the client on Windows 10 without needing Administrator permissions.

The Harmonic NMX Client applications are:

- NMX Domain Manager for setting global options, alarms, redundancy, and managing user accounts and database catalogs.
- NMX Designer for designing, configuring, and provisioning network, device, and video/audio services.
- NMX Operator for monitoring networks and scheduling batch services.
- NMX Service Plan Editor for making network changes offline.
- NMX Consolidated Alarms for viewing all network alarms in one place.

NMX Database

NMX uses Microsoft SQL Server 2017 as its relational database, where all NMX network, devices, and service configuration information is stored in database catalogs. You create and manage catalogs through NMX Domain Manager.

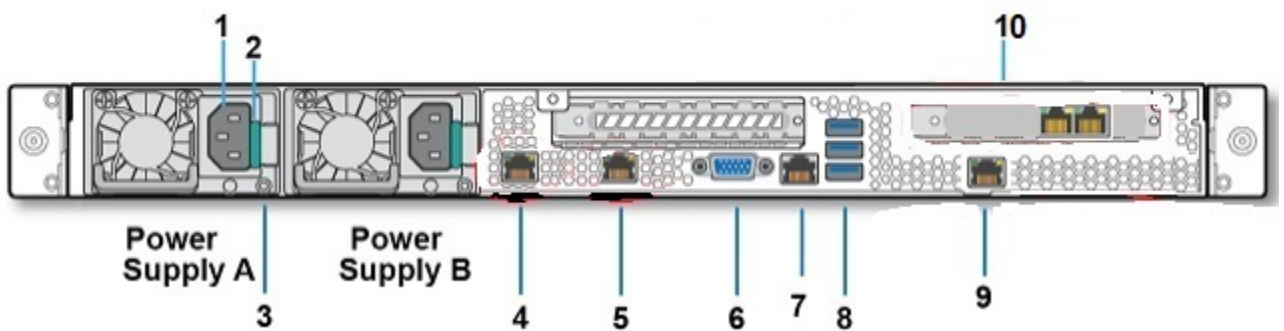
-  **IMPORTANT:** The SQL Server is installed on the same computer as the NMX Server.

NMX Rear Panels

A diagram of the NMX rear panel components, for Intel Wildcat server (NMX-HWP-3F-xx reference) and the HPE ProLiant DL 360 Gen 10 (NMX-HWP-3G-A-xx reference).

Intel Wildcat Server

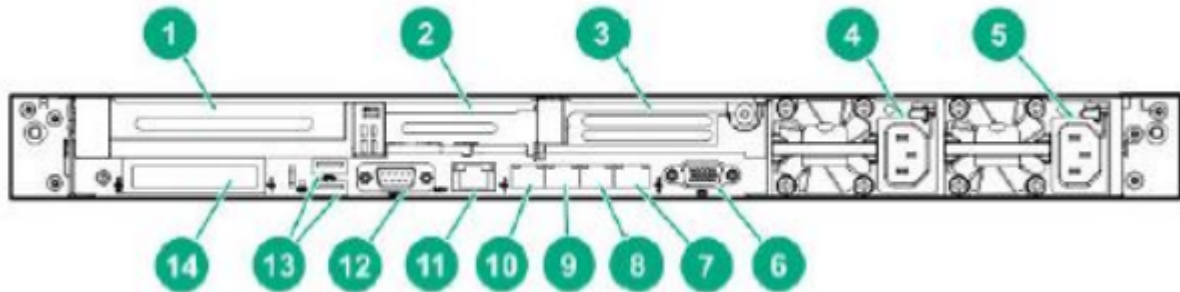
The back panel of the Intel Wildcat server (NMX-HWP-3F-xx reference) is displayed below, along with descriptions of its components.



Key	Component	Description
1.	AC Power connector	
2.	Release Lever	Secures power supply module to the chassis.
3.	Power supply LED	Dual redundant power supplies.
4.	Ethernet port 1	Gigabit Ethernet port, typically used for Management network.
5.	Ethernet port 2	Gigabit Ethernet port, typically used for CAS network if isolated from Management network.
6.	VGA port	Video port connects NMX to a monitor.
7.	Serial over LAN	Unused.
8.	USB ports	Port connects NMX to a keyboard or mouse.
9.	BMC	Baseboard Management Controller.
10.	Dual Port RJ-45 Ethernet Card	Other Gigabit Ethernet ports.

HPE ProLiant DL 360 Gen 10 Server

The back panel of the HPE ProLiant DL 360 Gen 10 Server (NMX-HWP-3G-A-xx reference) is displayed below, along with descriptions of its components.



Key	Component	Description
1.	Slot 1 PCIe 3.0	A high-speed serial computer expansion bus.
2.	Slot 2 PCIe 3.0	A high-speed serial computer expansion bus.
3.	Slot 3 PCIe 3.0	A high-speed serial computer expansion bus. Optional: requires a second processor.
4.	Power Supply 2	PS2
5.	Power Supply 1	PS1
6.	VGA port	Video port connects NMX to a monitor.
7.	NIC Port 4	Network Interface Controller port.
8.	NIC Port 3	Network Interface Controller port.
9.	NIC Port 2	Network Interface Controller port.
10.	NIC Port 1	Network Interface Controller port.
11.	iLO Management Port	Port for access to HP Integrated Lights-Out management.
12.	Serial Port	Optional
13.	USB 3.0 Ports	USB 3.0 ports.
14.	FlexibleLOM	Optional NIC card.

NMX Licensing support

Licenses for supported NMX and device features, such as the DPI (Digital Program Insertion) feature, can be added using the Harmonic License Manager. Refer to NMX Release Notes, “NMX and Device Licenses”, for the list of available licenses with their name and description.



IMPORTANT: License Manager requires a user account; please contact Harmonic Technical Support if you need a License Manager user account.

You can add and remove licenses to your system using the Harmonic License Manager. Most licenses are permanent. Once enabled, the feature will continue to function without raising license-related alarms. In specific cases (e.g. trial period), temporary licenses can be delivered.

Licenses are required for some NMX features, and you cannot enable those features without the appropriate license. However, some licensed features, for example, SAPI, DPI, and ESI, can be enabled for the 45-day grace period, and then require licenses.

Licenses are required for the NMX Base software and for some NMX features (refer to the NMX Release Notes for the complete list). You cannot enable those features without the appropriate license. However, a 45-day grace period is used when the NMX Base software license is not installed yet. It enables the base software and all of the NMX licensed features. There is no grace period for licensed features when the NMX Base software license is installed.

License alarm and expiration behavior includes:

- Streams that include features under license will raise alarms when their licensing expires (whether due to end of the grace period or due to end of a temporary license).
- When licenses expire, streams will continue to flow as configured, but will stop flowing if modified, or disabled then re-enabled.
- If any changes are made after a license expires, service may be affected, and other operations, such as redundancy, may not function properly.
- If a license is not installed for a feature that is enabled, a grace period will allow that function to operate fully for 45 days. Alarms will issue each day to advise you that licensing is required for a given feature.
- If the 45-day grace period has been used for less than 45 days, the remaining days are saved and can be used later (if the NMX Base license is returned).

 **IMPORTANT:** Temporary licenses included with NMX or supported devices are provided for Demo purposes, and not intended for production systems. Contact Harmonic Technical Support if you want to remove temporary licenses.

Viewing license names and descriptions

View available license names and descriptions from the NMX Release Notes.

- To view NMX and device license names and descriptions, open the NMX Release Notes to the device's New Features section whose licenses you want to review. For example: NMX Release Notes > New Features > Electra X New Features > Electra X Firmware Licenses.

Viewing time remaining on your NMX license

View the time remaining on your NMX features' licenses from any NMX application. NMX supported device feature licenses will raise an alarm on the device when the license is nearing expiration.

- At the upper right of the NMX **Ribbon bar**, click the "play" button. The **NMX version**, build number, **Unique ID**, **Active Licenses** name, and **Remaining Days** for the license display.

Remaining Days value is displayed for temporary licenses and for grace period. When the NMX license is nearing expiration, the lower right of any NMX application will flash red.

- When the grace period is used, it appears as a specific internal license named **ECL-INTERNAL-GRACE-LIC**, along with the associated Remaining Days.

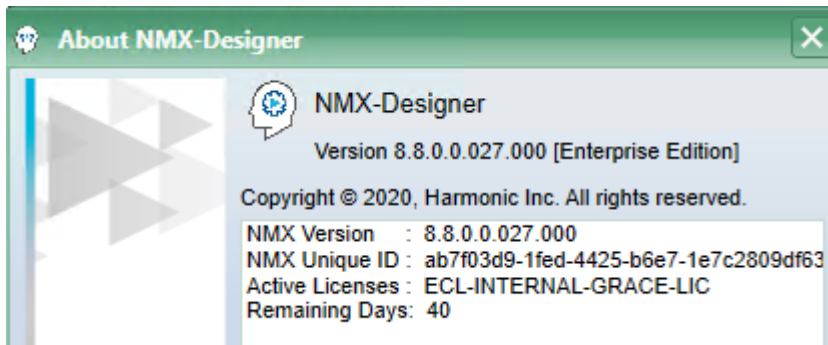


Figure 1-2: NMX Grace Period License

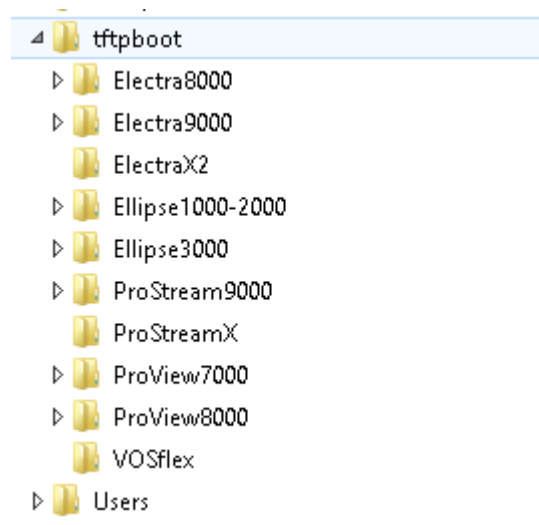
NMX Delivery Package

The NMX delivery package installs the NMX Server and NMX Client software, embedded device software, and third-party software packages. **Desktop** shortcuts provide links to the **Documents** and **Technical Notes** product documentation folders.

 **NOTE:** Contact your Harmonic representative if you are interested in Harmonic's non-embedded device software, such as Electra X, Electra™ XVM, and XVM.

	Name	Size
	Documents/	
	Devices.zip	2.6 kB
	Install_NMX_8.2.0.0-eng.3-A.exe	1.3 GB
	Install_NMX_Validator_8.2.0.0-eng.3-A.msi	499 kB
	manifest.txt	402 B
	NMX_8_2.pdf	573 kB

After installation, the tftp embedded device directory names appear in the C:\tftpboot directory. Embedded device folders contain the device release software supported by this NMX release. Non-embedded device folders can appear, but will not contain software until you install the software.



If you are upgrading NMX, and had installed EOS (End of Service) devices in previous releases, the EOS device directories may still appear in the tftp directory in the new installation.

Accessing NMX documentation

After installing NMX, view documentation on configuring applications, supported devices, creating and configuring network groups, and creating, configuring, connecting, and activating services.

Table 1-1: Documentation

To view:	Go to:
<i>NMX Installation Guide</i>	Desktop > Documents > NMX > Product_Guides Install the NMX recovery image before installing or upgrading, then upgrade your catalogs and maps.
<i>NMX User Guide</i>	Desktop > Documents > NMX > Product_Guides Configure NMX Server and users, build a network from a template, create a service plan and connect/activate services, and monitor your network.
<i>NMX Technical Notes</i>	Desktop > Technical Notes View common task workflows such as configuring splicing or VBR-CBR services.
Supported device guides	Desktop > Documents > Device_Guides Installation and user guides for supported devices.
<i>NMX Release Notes</i>	Desktop > Release Notes

To view:	Go to:
Earlier/archived release notes	Desktop > Documents > Archive_Release_Notes
<i>NMX Online Help</i>	View context-sensitive help with detailed workflows, and supported devices' network and service field descriptions.
NMX REST API Getting Started Guide	Desktop > Documents > NMX > REST_API How to set-up control of an NMX-managed system from the RESTful API.

To access the *NMX Online Help*:

1. Open any of the NMX applications.
2. Navigate to the dialog where you would like assistance.
3. Click the area or component in question, then click the **Help** button or icon.

Example: To see help for a device in the **Network** map, select the device, then click the **Help** button at the bottom of the device's **Properties** page.

Example: To see help for a service on the **Service** tab, select the service, then click the **Help** icon at the top of the **Properties** page. The **Properties** page shows the help for both the **Input** and the **Output**.

Result: The **Help** dialog opens, displaying help for the selected component.
4. To search for additional information about the component, click the **Search** tab.
5. Type the information you're searching for in the **Type in the Word(s) to Search for** field, then click **List Topics**.
6. Double-click a topic in the list to open it.

Supported languages and keyboards

The NMX server and client applications now support the French language setting in Windows and the Azerty keyboard. You can set both of these properties through the Windows settings (see Microsoft documentation and help for more information).

The following characters cannot be used with the Azerty keyboard:

§ é è ç à ù £ ° ³ ´ ² # * ; ' " | \ ? < >

Installing NMX Server on Win 2019/SQL 2017

A first-time manual NMX software installation involves validating your system requirements, downloading an NMX recovery image, preparing a bootable USB flash drive, deploying the recovery image onto your platform, and finally downloading and installing the NMX software.

Contact your Harmonic representative to purchase an NMX device that includes the recommended Operating System (OS) and database prerequisites, based on the software you purchased.

- [NMX Server 8.5.x and later system requirements](#)
- [Installing NMX Server for the first-time overview](#)
- [Installing NMX Client only overview](#)
- [Installing NMX VM overview](#)
- [About certificates](#)

NMX Server 8.5.x and later system requirements

NMX Server software can run on preconfigured, Harmonic-approved platforms. These platforms come with a pre-configured Operating System (OS), database server and NMX Software. Or it can run on a custom hardware platform provided by customer. In the latter case, the platform and OS must comply to minimum requirements described in Table 2-1.

NMX can be upgraded to Microsoft Windows Server 2019/SQL Server 2017 on Harmonic-approved platforms. The platform must meet specific system requirements.

Table 2-1: NMX 8.5.x and later System Requirements

Item	Requirement
NMX Server operating system/SQL Server release (version)	Microsoft Windows Server 2019/SQL 2017 required
NMX Client operating system	Microsoft Windows 10 client, 64-bit required (US English language only) required. Non-administrator access allowed.
Storage	480 GB minimum

Item	Requirement
Recovery image version	v1.1 or later. Recovery images available from: https://harmonic.force.com/SWAccess/SWDownloadLogin. Install any Windows updates to the image before installing NMX.  NOTE: We strongly recommend using the latest NMX Recovery Image.
Recovery image defaults	The NMX recovery image is shipped with these features turned off or disabled: • Windows Firewall and notifications • Internet Explorer Pop-up Blocker • Windows Updates and notifications • No antivirus software and notifications. If you use antivirus software, it is your responsibility to configure the proper settings, and install the most recent updates and virus definition files to protect your system, especially if you have Internet access. • The recovery image includes the latest Harmonic tested Windows updates. Periodically, Harmonic delivers additional tested Windows updates. Ensure your recovery image has the latest Harmonic tested Windows updates.
RAM	32GB RAM minimum
Processor	Minimum 2 Intel Xeon E5-2620 or better, 6 cores and 15MB cache
Browser	Google Chrome (required)
Ports	2 x GbE ports or more
Windows Server 2019 license	After installing the recovery image, you will enter your Windows license.
SQL Server 2017 license	You must have an SQL Server license.
Cloning NMX	Acronis Backup software, release 11.5 (build 11.5.4.43800) is recommended. Visit http://www.acronis.com/en-us/business/overview/ for more information.
Remote access	Remote users must log in with administrative permissions: <code>mstsc /admin</code>

Item	Requirement
Client applications installation	If you are installing NMX client applications on your own computer, you must install vcredist_x86.exe, which is required for the NMX installation process to succeed (Win32 Cabinet Self-Extractor). Go to Microsoft.com to search for, and download, the vcredist_x86.exe file.
NMX location	NMX should be installed on a system rack or in another appropriate location.
Network connections	NMX should be connected to the network with a standard Ethernet cable, and connected to any other required network devices.
Other software	NMX supports the latest versions of Symantec Endpoint Protection and McAfee® VirusScan Enterprise antivirus SW that are available at the NMX release date. Do not install or run any software on the NMX Server or NMX Client that does not come with your Harmonic software package.
Installing or upgrading NMX	To install or upgrade NMX yourself, comply with the system requirements, and follow the installation and upgrade procedures. Always install recently delivered Windows updates to the image before installing NMX.
Windows updates	Periodically, Harmonic will make tested Windows updates available for your system. If you are upgrading, install recently delivered Windows updates to the image before installing NMX. Protect your system by always installing the latest Windows security updates.

Supported hardware and software platforms

The following Harmonic-approved platforms can run NMX server software:

- HPE DL360 Gen10 running Windows Server 2019 and SQL Server 2017
- Intel® Wildcat Pass running Windows Server 2019 and SQL Server 2017
- Dell PowerEdge R230 running Windows Server 2019 and SQL Server 2017

The NMX platforms are delivered with:

- Microsoft Windows Server® 2019 Standard Edition (English language only)
- Microsoft SQL Server® 2017 Standard Edition



NOTE: The installation of third party software is not recommended and shall be done at the customer's own risk. Contact Harmonic Technical Assistance for advice and/or specific testing request.

Supported recovery images

NMX recovery image files include the supported Windows operating system, and support for specific system fixes and security updates. For a complete listing of these recovery image files, refer to the "NMX Recovery Image Versions and Compatibility" section of the NMX Release Notes.



NOTE: Download the latest recovery image by logging in to: <https://harmonic.force.com/SWAccess/SWDownloadLogin>. Install any Windows updates to the image before installing NMX.



NOTE: Every NMX recovery image comes with the User Account Control (UAC) enabled by default for increased security. Since NMX client applications, like NMX Operator, require Windows Administrator privileges, this can cause the appearance of warning messages each time you launch these applications on the NMX server. To prevent these messages from being generated, you must change the Windows UAC setting. Consult the Windows Server documentation for details.

About antivirus definition files

Antivirus software protects your NMX network from malicious software.

If you use antivirus software, it is your responsibility to configure the proper settings, and install the most recent updates and virus definition files. See your antivirus software manufacturer's website for the most current files.

NMX supports the latest versions of Symantec Endpoint Protection and McAfee® VirusScan Enterprise antivirus SW that are available at the NMX release date. Exclusion of NMX files or folders from antivirus scan is not required with Symantec and McAfee software.

Installing NMX Server for the first-time overview

Installing NMX Server for the first-time involves deploying the recovery image, logging in to Windows on the NMX Server device, changing the NMX Server name, assigning IP addresses, downloading the NMX installation package, and installing NMX Server and/or NMX Client.

Deploying the recovery image overview

After validating your system requirements, NMX recovery image deployment involves downloading the image, creating a bootable USB Flash Drive, and deploying the image.

After installation, you can check your recovery image release number here: `C:\Utilities\Version.txt`. The release number appears as a Version 2019_1.1 (date) or similar number at the top of the file.

Downloading the NMX recovery image

Download the NMX recovery image onto a PC with ~150 GB of free disk space.

Before you begin

The de-compile/compile process to create the bootable drive requires ~150 GB of free disk space.

1. On a PC with Windows 10, or Windows Server 2019, ensure that `C:\Temp` is created.

2. Log in to <https://harmonic.force.com/SWAccess/SWDownloadLogin>. Contact Harmonic Technical Support if you do not have access.
3. Navigate to: **Home > Service & Support > Software Downloads > Authorized Products > NMX Recovery Image**.
4. Open the correct recovery image directory for your system.
5. Download all the files in the directory to C:\Temp.

Creating the bootable USB flash drive

Create the bootable flash drive on a 16 GB or larger flash drive.

1. Download the latest Recovery Image (ISO) provided by Harmonic.
2. Launch the **Rufus** tool provided with the image (run as **Administrator**).
3. Insert an empty USB flash drive. All the existing data will be deleted from the flash drive.
4. Select that USB drive as **Device** in Rufus.
5. Locate and select the ISO image file using the **SELECT** option under the **Boot** selection.
6. Set the **Partition** scheme as **MBR** and the **File** system as **NTFS**.
7. Set an appropriate **Volume** label for the USB drive and keep all other settings as **Default**.
8. Click **START**.
9. Click **OK** on the warning message.
Note:The process takes 20-25 minutes to complete, depending on the operating system and USB brand.
10. After the process is completed, close Rufus and unplug the drive.
11. Use this USB drive to deploy the image for upgrades or recovery, when needed.

Deploying the recovery image

Deploy the recovery image on to your NMX Server.

Before you begin

You will need to enter your Windows OS product key at the end of this procedure.

1. Ensure that the NMX Server is shut down.
2. Insert the USB flash drive into the NMX Server.
3. Power up the system.
4. Press **F11** to view the **BIOS Boot Manager** menu.
5. In the **Boot Manager**, select to boot from the USB flash drive.
A message displays: **The hard disk will be reformatted. Are you sure you want to continue?**
 **CAUTION:** Upgrading the operating system with the USB drive will erase all data on your system.
6. Click **Yes** to continue.

7. Click **Yes** when the second message displays: **All the data on the hard disk will be deleted. Please backup your data before continuing. Are you sure you want to continue?**

The recovery image installation process takes about 15 minutes.

8. After deployment completes, remove the USB flash drive and click **OK** to reboot the system.
The default login user name and password for systems upgrade or recovery is Administrator / Harmonic2008 (case sensitive) and for SQL server is sa/harmonic. You will be forced to change the password on your first login to the system.

9. If you do not have access to the Internet, when the OS boots up, open a command prompt.

- a. Open **Activate Windows** from **System Properties**.
- b. Click **Enter Key**, then enter the new product key. But the new key gets applied internally in the system. Can be verified by running `slmgr.vbs /dlv` command

Result: Because the internet is not accessible, the **This key didn't work** message opens, but the new key is applied internally in the system.

- c. Call Microsoft to activate the key.
- d. To verify the key, run the `slmgr.vbs /dlv` command.

10. If you do have access to the Internet, when the OS boots up, open a command prompt.

- a. Type `slmgr.vbs /upk` to remove the current product key.
- b. Type `slmgr.vbs /ipk {product key}` Include the dashes in the product key.

Example: `slmgr.vbs /ipk {3JDKG-F7N3X-WJHD2-Q6T4X-KP9CB}`

- c. Open a browser and activate the key.

Installing Windows Security updates

Windows Security updates must be installed on the recovery image before NMX.

Install Windows Security updates as you normally would. This procedure is a workaround in case you installed NMX on the recovery image before installing Windows Security updates.

1. Open the **Run** window (Windows key + R).
2. Type `dcomcnfg.exe` and click **OK**.
3. In the console tree on the left, expand **Component Services**.
4. Expand **Computers**.
5. Right-click **My Computer**, select **Properties**, then navigate to the default **Properties** tab.
6. Change the **Default Authentication Level** from **None** to **Connect**.
7. Choose **Identify** in the **Default Impersonation Level** list (from the original **Impersonate** entry).
8. Click **OK**, then click **Yes** to confirm the selection.
9. Close the **Component Services** console.
10. After installing the Windows Security updates, revert back to the above setting.

Logging in to Windows 2019 Server

Log in to Windows.

1. Start the Windows 2019 computer.

2. Log in:

User: Administrator

Password: Harmonic2008

You must log in to Windows as a user with administrator permissions to run the NMX Server software. The server must have a password set up for access from Windows 10 clients. The administrator can add other users, if necessary.

3. Click **OK**.

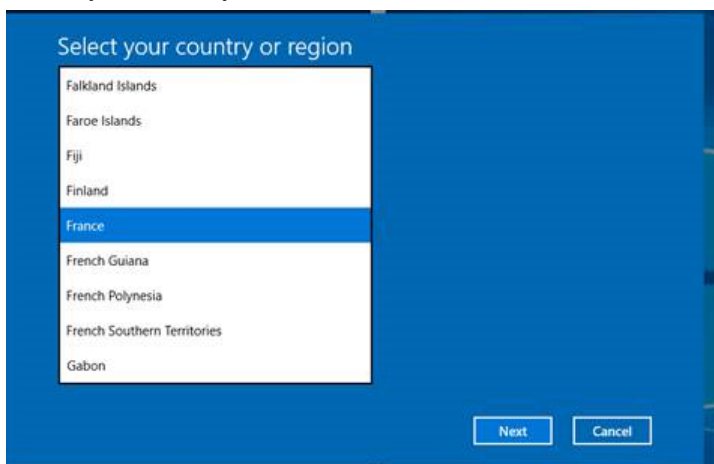
Result: The NMX applications, documentation folders appear on the desktop.

Offline Windows Server 2019 license activation

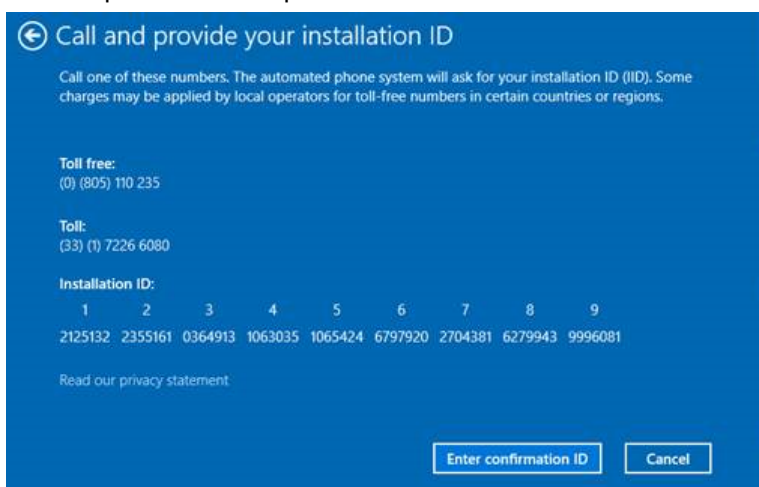
If the machine you are installing Windows Server 2019 is not connected to the Internet, you must contact Microsoft by telephone to activate your license.

Context for the current task

1. Open a PowerShell session as an administrator and run the command `slui 4`.
2. Select your country from the list and click **Next**.



3. Call the phone number provided and follow instructions to activate your license.



4. Enter the Installation ID and then click **Enter confirmation ID**.
5. Enter the confirmation ID indicated by the vocal server.

Changing the NMX Server name and Domain

Each NMX Server must have a unique name. Systems with only one NMX can keep the assigned default name.

1. If it is running, stop NMX Domain Manager.
2. On the NMX Server, go to **Control Panel > System > Change Settings**.
3. Click **Change**.
4. Type the new server name in **Computer Name** field, then click OK.
5. Click **Apply**.
6. At the prompt, click **Yes** to restart the computer.

NMX Server Membership

By default, the NMX Windows Server is configured as a Member of a Workgroup in the System Properties. You can move it to be a Member of a Domain, but this requires you to reinstall the NMX software release immediately afterwards. Otherwise the NMX applications will be unable to connect to the server.

Assigning NMX Server IP addresses

Assign the NMX Server IP addresses and add the server to your network.

 **NOTE:** Most Electra X2S installations will not need to change the preassigned addresses. Changing the IP address of the interface on which the Remote Desktop connection is active will result in disconnecting the current Remote Desktop session. Make sure you can continue to access the system with the Remote Desktop console.

 **NOTE:** NMX ports can be configured in NIC teaming (Windows setting) and this configuration is compatible with NMX server redundancy. When NIC teaming is used with NMX server redundancy, the MAC address of the primary NIC must be manually set in the NIC properties: **NICTeam > Properties > Configure > Advanced > MAC Address > Value**. Also applicable to NMX VM.

1. Log in to NMX Server.
2. Go to **Network and Internet > Network Sharing Center**, then click the link displayed next to **Connections**.
3. On the link's status dialog, click **Properties**.
4. On the link's properties page, click **Internet Protocol Version 4 (TCP/IPv4) > Properties**.
5. On the **General** tab, enter the **IP address**, **Subnet Mask**, **Default Gateway**, and **Preferred** and **Alternate DNS** server addresses for your system.
6. Click the **Advanced...** button.
7. Uncheck the **Automatic Metric** checkbox.

8. Enter a value in the **Interface metric** field. This determines the order of the connections.
9. Click **OK > Close > Close**.
10. Add the server to your network.

Assigning NMX Server IP addresses with no DNS server

If the NMX Server is not connected on a network with a DNS Server, the host name/IP address association must be done using the Windows configuration file named **hosts**. This is **mandatory** for the management of some devices like Electra XT, Electra VS, Spectrum XE, CP9000/RD9000, Newtec MCX7000/M6100/USS2x2, Cisco switch, and MIT-xperts. This is not a complete list.

1. Make sure you have full Administrator rights to the NMX Server.
2. Log in to NMX Server.
3. Go to **Control Panel > All Control Pannel > System**.
4. Verify the **Full computer name**.

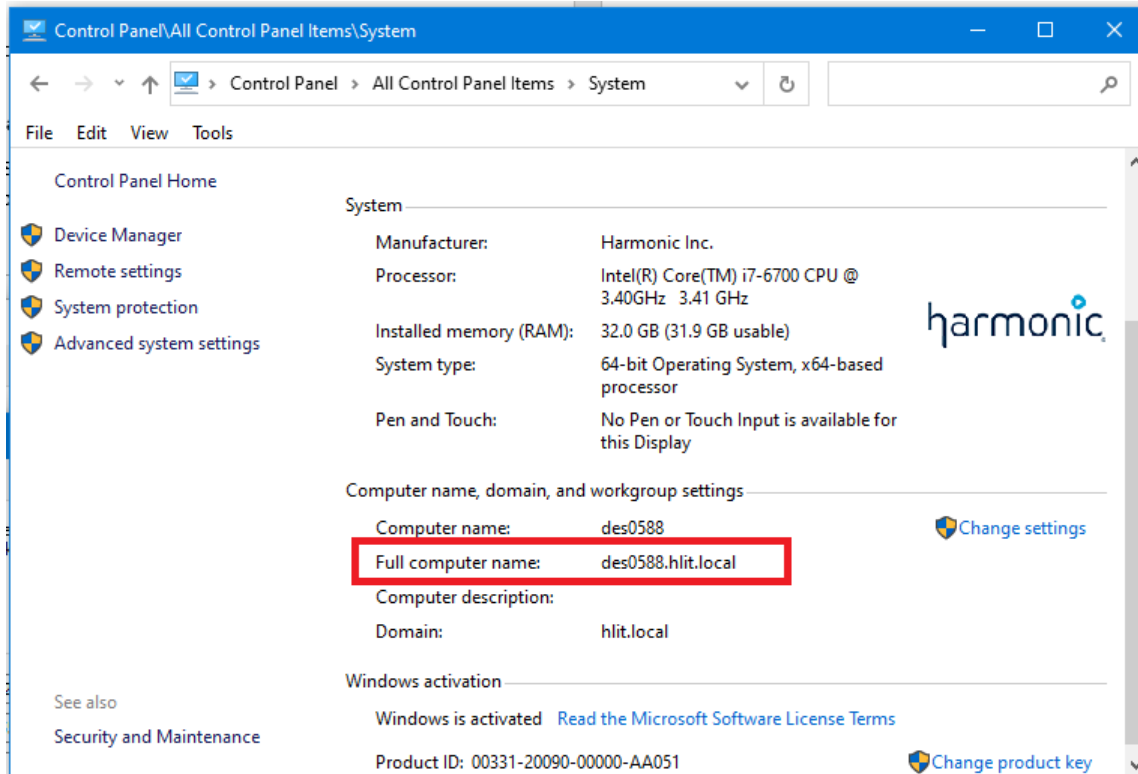


Figure 2-1: NMX Server Control Panel

5. Exit the **Control Panel**.
6. Open the **C:\Windows\System32\drivers\etc\hosts** file in Notepad with **Administrator** privileges. Right-click the Notepad application icon and select **Run as Administrator**; click **Yes** to the security warning.



NOTE: This file must be opened with **Administrator** privileges even if you have Administrator rights. Otherwise Windows will not be able to save the updated hosts file.

7. Add a line with the IP address and host name at the end of the file.

```

1  # Copyright (c) 1993-2009 Microsoft Corp.
2  #
3  # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4  #
5  # This file contains the mappings of IP addresses to host names. Each
6  # entry should be kept on an individual line. The IP address should
7  # be placed in the first column followed by the corresponding host name.
8  # The IP address and the host name should be separated by at least one
9  # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #       102.54.94.97       rhino.acme.com       # source server
17 #       38.25.63.10       x.acme.com           # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 #   127.0.0.1       localhost
21 #   ::1             localhost
22
23 127.0.0.1       localhost
24
25 10.1.62.64      DES0588.hlit.local
26

```

Figure 2-2: NMX Server Hosts File



NOTE: If the NMX Server is in a Workgroup, and not in a Domain, the computer name and the full computer name are identical. In this case the line to add would be:
10.1.62.64 DES0588.

8. Save your changes and close the file.
9. Add the server to your network.

Downloading the NMX installation package

Download the NMX installation software onto the NMX Server.

1. From your NMX Server, log in to <https://harmonic.force.com/SWAccess/SWDownloadLogin>.
2. Navigate to: **Home > Service & Support > Software Downloads > Authorized Products > \NMX 8.x Application**.
3. Open the correct NMX directory for your installation.
4. Download all the files in the directory to NMX Server **Desktop**.

Installing a new version of NMX Server software

Install the NMX software onto the NMX Server.

Before you begin

Install any Windows security updates before installing NMX.

1. Open the NMX installation directory on the desktop and double-click the Install_NMX_<BuildNo>.exe file.

2. Click **Next** in the **Setup - NMX** dialog.

- a. In the **NMX Registration** dialog, enter your user name and company name, and click **Next**.
- b. In the **License Agreement** dialog, select to accept the license agreement and click **Next**.
- c. In the **Select Components** drop-down, select **Client and Server**, and click **Next**.
- d. Complete the fields in the **Server Settings** dialog.

Site ID	Enter a unique identifier for the Site ID . You can enter any number from 11–2000. This number must be unique for all NMX Server instances on the network.
SQL Server Name	Confirm or edit the host name of the computer where the SQL Server database will be installed.
SQL Catalog Name	Enter a name for the SQL Server catalog you will use. The name must start with an alphabetic character. In this step, you're just naming the catalog. You must create the catalog in NMX Domain Manager after installation finishes. The default catalog name is NMXDB.
Backup Directory Path	Accept the default for the Backup Directory Path . This is the full path to a directory on the SQL Server computer where you want to save NMX database backups.

3. Click **Next**.



NOTE: If your server does not have enough memory for the SQL database, click **Yes** if you are prompted to modify the SQL memory size (selecting yes sets the memory size to 50% of available RAM).

- a. On the **Ready to Install** dialog, click **Install**.
Installation begins.
 - b. Documentation requires Adobe Reader. Click **Install** and follow any onscreen steps to install Adobe Reader. If Adobe prompts you to restart the system, select to **Restart later**, and let installation complete.
 - c. On the **Setup - NMX** dialog, select **Yes** to install the **Meinberg NTP** and **Meinberg Time Server Monitor**.
 - d. Click the **I Agree** button on the **Network Time Protocol Setup** dialog.
 - e. On the next dialog, accept the **Destination Folder** default location and click **Next**.
 - f. On the **Choose Components** dialog, and click **Next**.
4. On the **Files Have Been Installed** dialog, ensure that **Create an initial configuration file with the following settings:** is selected.
5. Select your nearest country or region from the drop-down list., then click **Next**.
Result: NTP creates a conf file for the selected servers.
6. On the **Network Time Protocol Setup** dialog, click **Yes** to use the default configuration.
7. On the next dialog, click **No** to review the generated config file.
You will complete NMX installation first, then configure the Meinberg NTP Server.
8. On the **Network Time Protocol Setup: NTP Service Options** dialog, accept the defaults and click **Next**.
9. Click **Next** in the **Setup - NMX** dialog.

10. When the installation completes, click **Finish** to restart the computer.

Restarting ensures proper performance.

11. Log in to Windows after the restart completes.

Result: The NMX applications, documentation folders, and the NTP Time Server Monitor icons appear on the desktop.

What to do next

Configure the Meinberg NTP Server, log in to NMX Domain Manager, create a new database catalog (or restore/upgrade your backed up catalog), and start the NMX Server.

About configuring the Meinberg NTP Server

Configuring the Meinberg NTP Server involves disabling the default time setting, checking the server's status, and assigning its IP addresses in NMX **Options**.

The Meinberg NTP Server synchronizes NMX clients or servers time to another server or reference time source, such as a radio or satellite receiver or modem, for accurate time synchronization and stable reference timing.

Disabling the default time settings

Disable the NMX Server **Internet Time Settings** and check the Meinberg NTP Server status to ensure NMX devices and services will have accurate time synchronization and stable reference timing .

1. If your NMX Servers have enabled **Synchronize with an Internet time server**, disable it.

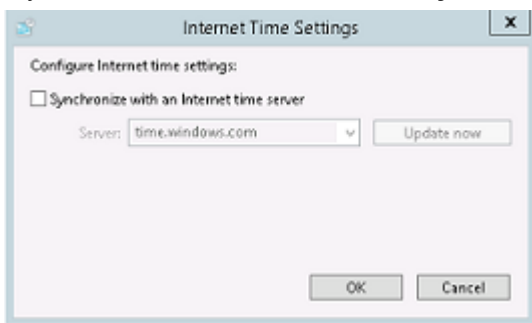


Figure 2-3: Internet Time Settings

- When you installed NMX, the Meinberg NTP service was installed and started. Check that it is running from **Administrative Services > Services > Network Time Protocol Daemon**.

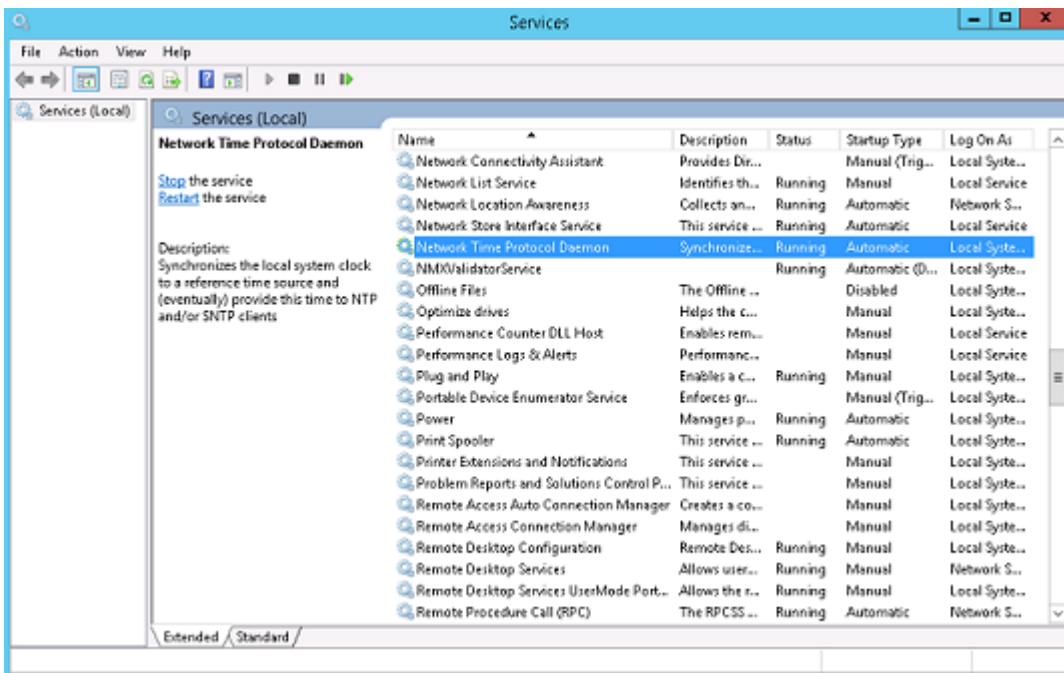


Figure 2-4: NTP Service Running

- Check the NTP status by opening the **Quick NTP Status** shortcut at C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Meinberg\Network Time Protocol.

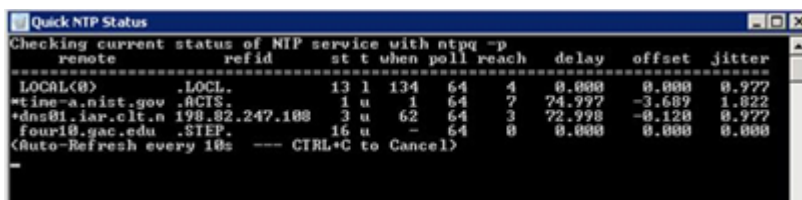


Figure 2-5: NTP Status Check

Configuring the Meinberg NTP Server

Configure the NTP Server IP addresses from **Options > External Servers** so that the NTP Server can run with NMX.

- From NMX Domain Manager, stop the NMX Server, if it is running.
- Click **Options > External Servers**.

3. Select the **Use NTP Server** check box.

Example: The NTP Server 1 might be the local master NTP server 1, such as GPS receiver NTP server 1.

The screenshot shows the 'Options' dialog box with the 'External Servers' tab selected. The 'Use NTP Server' checkbox is checked. The configuration for three NTP servers is as follows:

Server	IP Address	Port	Request Interval (sec)
NTP Server 1	172.19.161.143	123	30
NTP Server 2	172.19.161.144	123	30
NTP Server 3	0.0.0.0	123	30

Additional settings shown include a GPS UTC Offset of 16 seconds, a Playout Pre-fetch Cache of 10 seconds, and a Time Zone of (GMT-08:00) Pacific Time (US & Canada).

4. Click **OK**.
5. From NMX Domain Manager, start the NMX Server.
The NTP services are ready for the video system. All devices provisioned under NMX will get accurate, synchronized, and stable NTP timing from the NTP servers.

Meinberg NTP Server recommended configuration

Harmonic recommends a Meinberg NTP Server installation where NMX Server instances are installed with the Meinberg NTP client, and synchronize with the local NTP servers as master NTP servers.

Network Time Protocol (NTP) time synchronization is a critical part of video networks. NTP provides common accuracy and stable reference timing for all the devices in the video network, and allows synchronizing all StatMux, DPI, automation, and NMX redundancy control messages across devices in the network. As unstable timing systems cause issues for video processing, video delivery, and system management, Harmonic recommends using the Meinberg NTP Server.

The recommended Meinberg NTP Server architecture includes NMX Server instances installed with the Meinberg NTP client, where the NMX Server instances synchronize with the local NTP servers as master NTP servers. All the other devices in the video network synchronize with the local master NTP servers through direct NTP connections between the master NTP servers and the devices. With accurate and stable master NTP servers, a common shared and synchronized timing is achieved with low delay and low jitter for all devices.

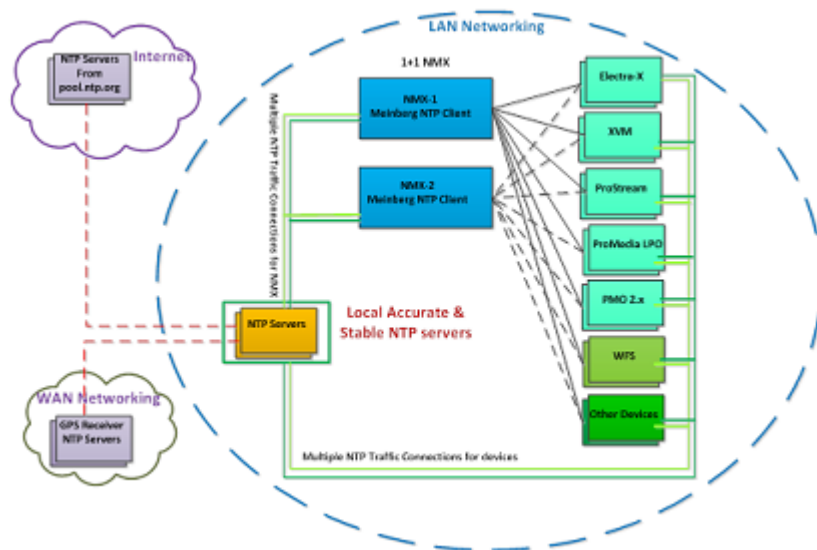


Figure 2-6: Harmonic Recommended NTP Configuration

Meinberg NTP Server alternative configuration

When local accurate and stable master NTP servers are not available, Harmonic recommends alternative configuration options.

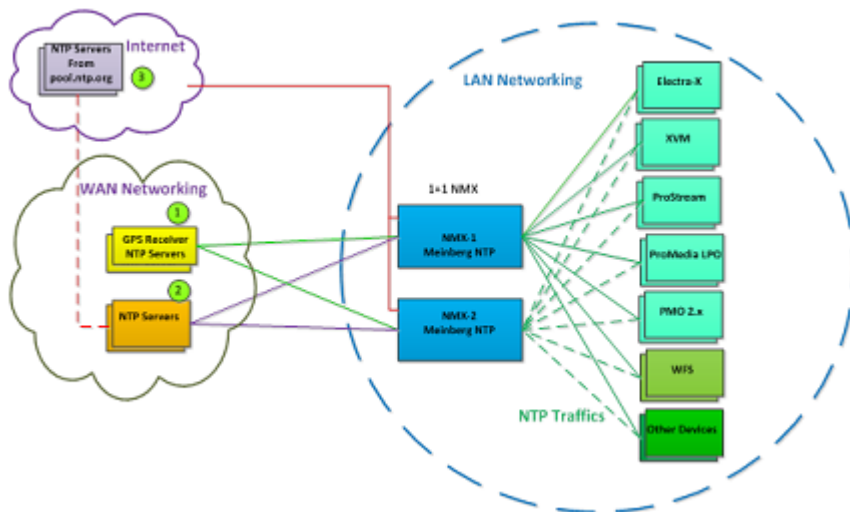


Figure 2-7: Harmonic Recommended Alternative NTP Configuration

Option 1

In the configuration for Option 1, there are two NMX Server instances clustered together in a 1+1 redundancy scheme. Each NMX server is installed with Meinberg NTP software. The Meinberg NTP, as NTP clients on the NMX Server instances, should synchronize with external accuracy and as stable master NTP servers. The Meinberg NTP as NTP servers on the NMX Server instances should provide accuracy and stable timing for all the devices in the video solution system. The Meinberg NTP on the NMX Server needs to synchronize with the external master NTP servers. The GPS receiver NTP servers are the best external master NTP servers (option 1).

Option 2

Normally, the GPS Receiver NTP server provides the best accuracy and stability network time. If the GPS receiver NTP server is not available, then other external master NTP servers in the WAN networks (Option 2) can be used.

Option 3

If Options 1 and 2 are not available, the Meinberg NTP should be connected to the Internet NTP Pool as provided by pool.ntp.org, highlighted as Option 3. Synchronization with the NTP pool over the Internet normally degrades the NTP time accuracy and stability slightly. In many applications, the NMX Server, may not have access to the Internet for the connection with NTP pool. It is not recommended that you use the NMX PC's free running clock local time as the reference timing for the NTP services. With this NTP architecture, all the Harmonic devices and third-party devices in the video network can be connected with the Meinberg NTP services on the NMX Server instances. The NTP services on the two NMX Server instances Servers also provide redundant NTP services (connected through separate physical IPs, not the single Virtual IP) to the video processing and delivery devices in the network.

Logging in to NMX Domain Manager

Log in to NMX Domain Manager.

1. Log in to the device on which you installed NMX Domain Manager with your **User Name** and **Password**.
2. Double-click the **NMX Domain Manager** icon.



3. Complete the login information on the **Domain Manager Login** dialog box.

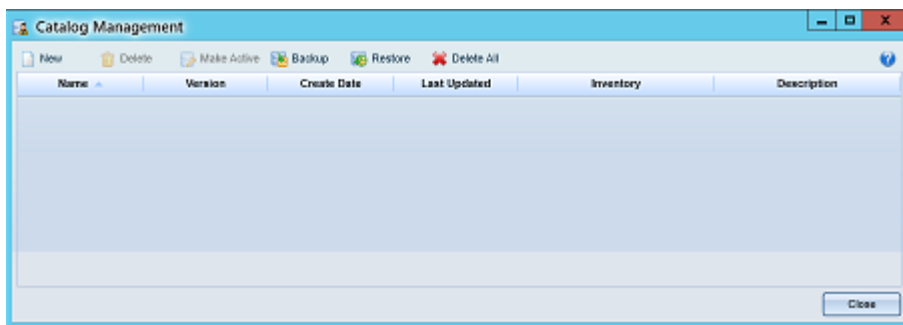
Server Name/IP	The NMXmanagement IP used for the network.
User Name	Administrator is the default.
Password	harmonic is the default.

4. Click **OK**.

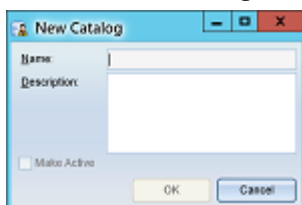
Creating a new database catalog

Create a database catalog in which to save network groups and service plans, or to which you can restore previous catalogs when you upgrade.

1. From **NMX Domain Manager > Database** tab, click the **Catalog Management** tab.
2. Enter **sa** in the **User Name** field.
3. Enter **harmonic** in the **Password** field.
4. Select the **Remember Login Information** check box for NMX Domain Manager to remember your login credentials while you are working in NMX Domain Manager, then click **OK**.
5. On the **Catalog Management** dialog, click **New**.



6. On the **New Catalog** dialog, enter a **Name** and a **Description**.



7. Click **OK**.

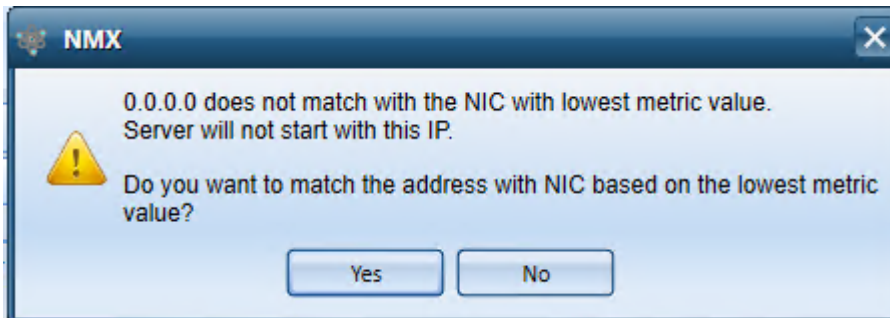
Result: The catalog appears on the **Catalog Management** dialog box.

Starting the NMX Server

Start NMX Server before opening NMX applications.

1. From the **NMX Domain Manager > Home** tab, click **Start Server**.

- On the message confirming if you want the IP address to match the highest NIC, click **OK**. This message appears only for first-time NMX installations, when you start NMX Server for the first time.



NMX Server processes are started when the toolbar **Status** displays **Server Started**.

What to do next

Harmonic recommends backing up your NMX map as soon as you have a working version completed. Back up the C:\database\backup file to another location, away from the local disks of the Electra X2S platform, using FTP or Remote Desktop copy-and-paste. This protects against a storage medium failure and allows you to quickly restore service if the hardware requires replacement.

Installing NMX Client only overview

After you have installed the NMX Server, you can install standalone NMX Client instances on other Windows Server 2019 or Windows 10 computer platforms.

NMX Client system requirements

The NMX Client software runs on Harmonic-approved platforms.

NMX Client applications (the NMX Client, NMX Service Plan Editor, and NMX Consolidated Alarms), can be installed on a local or remote NMX Server, or on your own local or remote computer. Installing the NMX Client installs all the NMX GUI applications. You can also install only NMX Service Plan Editor or NMX Consolidated Alarms. For remote NMX Server instances, you must specify the IP address of the NMX Server computer when you start NMX Client application(s).

Table 2-2: NMX Client System Requirements

Item	Requirement
NMX Client operating system	- Microsoft Windows 2019, Windows10 clients, 64-bit required (US English language only) required. - Non-administrator access allowed after the first administrator login post-installation.
Disk size	20 GB minimum
RAM	16 GB recommended, 8 GB minimum
Processor	i3 Dual Core processor or better

Item	Requirement
Browser	Google Chrome recommended
Firewall	Disable the Internet Explorer Pop-up Blocker and Microsoft Windows Firewall features.
Cloning NMX	Acronis Backup software, release 11.5 (build 11.5.4.43800) is recommended. Visit http://www.acronis.com/en-us/business/overview/ for more information.
Remote access	Remote users must log in with administrative permissions: mstsc /admin
Client applications installation	If you are installing NMX Client applications on your own computer, you must install vcredist_x86.exe, which is required for the NMX installation process to succeed (Win32 Cabinet Self-Extractor). Go to Microsoft.com to search for, and download, the vcredist_x86.exe file. You can install up to 25 stand-alone NMX Client instances on remote computers.
Upgrading the client	To upgrade a standalone NMX Client instance, upgrade the NMX Server first, then, uninstall the existing client, and install the new client.

Installing NMX Client software

Install the NMX Client as a standalone application on a supported platform after you have installed NMX Server on another computer.

Before you begin

Make sure the NMX Client computer is connected to your network.

1. Copy the NMX installation directory to your client computer.
2. Open the directory and double-click the Install_NMX_<BuildNo>.exe file.
3. Click **Next** in the **Setup - NMX** dialog.
4. In the **NMX Registration** dialog, enter your user name and company name, then click **Next**.
5. In the **License Agreement** dialog, select to accept the license agreement, then click **Next**.
6. In the **Select Components** drop-down, select **Client only**, and click **Next**.
7. On the **Ready to Install** dialog, click **Install**.
NMX begins installing files.
8. On the **Setup - NMX** dialog, click **Finish** to restart the computer.
9. Log in as Administrator to Windows after the restart completes so that NMX can complete post-installation tasks.
After Administrator login, non-Administrator users can log in.

What to do next

With the NMX Server installed, connected to the network, and started, you can access NMX Server from the NMX Client applications to create, configure, and manage your video network.

Installing NMX VM overview

Installing NMX VM software involves validating your system requirements, installing the VMware vSphere® (ESXi) 5.5, 6.0, 6.5, or 6.7 Hypervisor and vSphere client, deploying the NMX VM .OVA, and finally installing NMX.

NMX VM system requirements

The NMX VM runs on Harmonic-approved platforms with the recommended hardware requirements for optimum performance. Hardware that meets minimum requirements may affect performance on some systems.

Before deploying the NMX VM, review the important notes and system requirements.



IMPORTANT:

- Do not install or run any software on the NMX VM Server or NMX VM Client that does not come with your Harmonic software package. Consult your Harmonic representative for more information.
- If you start a second VM on a server, you will get warning message. It is your responsibility to monitor your resource utilization and increase your resources as required.
- Creating and using an .OVA file different from the supported license-enabled Windows OS may be in breach of Microsoft's license agreement.
- VMware vSphere® must be installed before deploying the Harmonic .OVA.
- For redundancy purposes, an NMX VM must be backed up with another NMX VM. Backing up an NMX VM to an NMX installation on an appliance is not supported.

Table 2-3: NMX VM System Requirements

Item	Minimum Requirements	Recommended Requirements
Virtual CPU	4 cores CPU (Intel Xeon processor E3-1220 equivalent)	16 cores CPU (2 Intel Xeon processor E5-2620 equivalent)
Memory	16 GB RAM	32 GB RAM or higher
Disk size	120 GB (10000 rpm) or higher hard disk	160 GB (10000 rpm) or higher hard disk
GbE Base-T Ports	2	4
Browser	N/A	Google Chrome recommended

Item	Minimum Requirements	Recommended Requirements
Firewall	N/A	- The Windows firewall must be enabled. - Disable Symantec Endpoint Protection Firewall.
Harmonic .OVA	N/A	Harmonic .OVA template is stored in a single Open Virtualization Format (.OVF) file available from Harmonic. The .OVA includes the Windows 2019/SQL 2017 software. No other .OVA template is supported or recommended.
VM Server	N/A	VMware vSphere (ESXi) 5.5, 6.0, 6.5, or 6.7. Hypervisor and vSphere client) Hypervisor (host NMX VM on a virtual server).
VM Client	N/A	VMware vSphere Client (to remotely control ESXi).

Deploying the NMX VM .OVA template

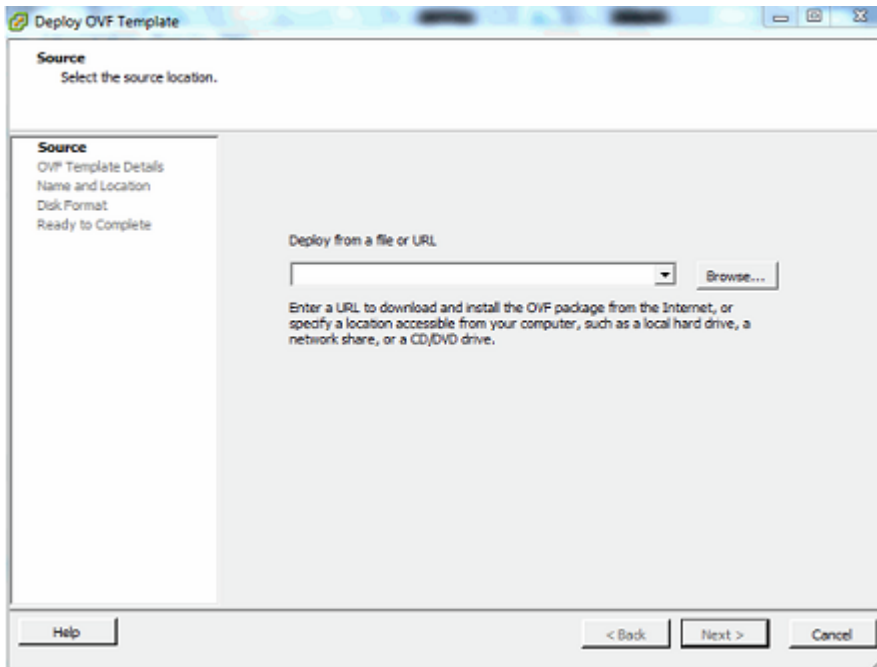
Deploy the NMX VM .OVA template on a system where the supported VMware vSphere (ESXi) Hypervisor and vSphere client are installed.

Before you begin

You must have validated your system requirements before deploying the NMX VM .OVA.

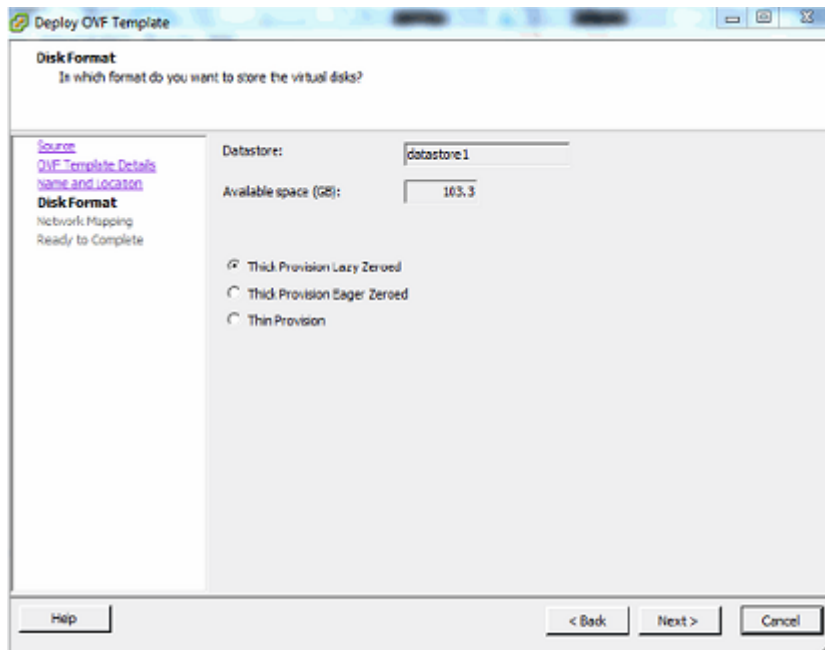
1. Log in to the vSphere client with:
root / <password>
<IP address>
2. Click **Login**.
3. Respond to the security warning.
4. Click **Inventory**.
The ESXi server IP address appears in the left column.
5. Click the **Summary** tab in the right column and confirm that the server resources meet the hardware requirements.
6. Select the ESXi server IP address.

7. From the **File** menu, select **Deploy OVF Template**.
The Deploy OVF Template wizard opens.



8. Click **Browse**, then locate and select the NMX VM .OVA file.

9. Click **Next** and complete the steps in the wizard.
 - a. If desired, give the .OVA file a different name, such as NMX VM, then click **Next**.
 - b. On the **Disk Format** dialog, keep the default **Thick Provision Lazy Zeroed** selection, then click **Next**.



- c. On the **Ready to Complete** dialog, click **Finish**.
The NMX VM begins deploying. On successful deployment, the **Deployment Completed Successfully** dialog opens
10. Use the **Edit Settings** option for the newly created VM and update the settings to meet the NMX VM System Requirements as specified in [Table 2-3](#).

Deploying multiple instances of NMX .OVA overview

To deploy multiple instances of the NMX .OVA, for each instance, you must deploy the .OVA image, change the server name, set the network connections, create a catalog, and set a unique Site ID.

Deploying multiple instances of NMX .OVA

For each NMX .OVA instance, change the server name, set the network connections, and re-boot the computer.

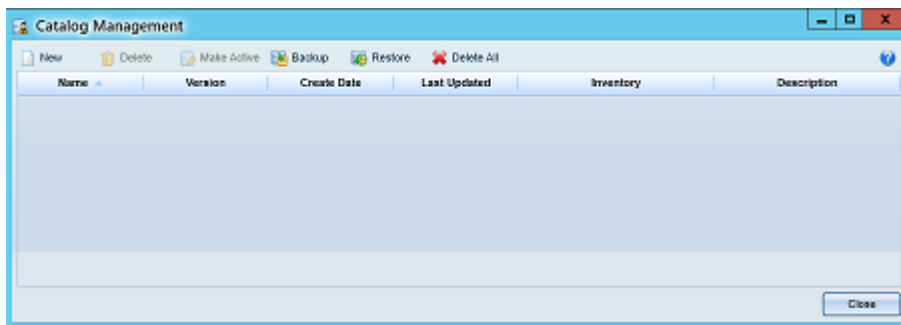
Follow this procedure for each VM instance on which you will install the NMX .OVA.

1. Deploy the NMX .OVA on a VM.
2. Change the server PC name.
3. Go to **Network and Sharing Center > Connections: J_ETH2 > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties > J_ETH2 Status** and set the IP and DNS connections.
4. Click **OK > Close > Close**.
5. Reboot the computer.

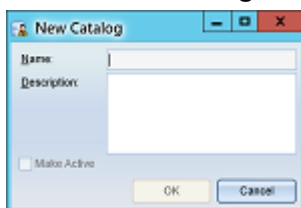
Creating a new database catalog

Create a database catalog in which to save network groups and service plans, or to which you can restore previous catalogs when you upgrade.

1. From **NMX Domain Manager > Database** tab, click the **Catalog Management** tab.
2. Enter **sa** in the **User Name** field.
3. Enter **harmonic** in the **Password** field.
4. Select the **Remember Login Information** check box for NMX Domain Manager to remember your login credentials while you are working in NMX Domain Manager, then click **OK**.
5. On the **Catalog Management** dialog, click **New**.



6. On the **New Catalog** dialog, enter a **Name** and a **Description**.



7. Click **OK**.

Result: The catalog appears on the **Catalog Management** dialog box.

Setting the NMX site ID

Set a unique site ID for each NMX .OVA instance. Systems with only one NMX can keep the assigned default site ID.

Follow this procedure for each VM instance on which you will install the NMX .OVA.

Before you begin

IMPORTANT: Each NMX .OVA instance must have a unique server name, correct network connections, a catalog, and a unique Site ID.

1. Go to **Domain Manager > Options > General** and set a unique Site ID.
2. Click **OK**.

Logging in to NMX VM

Power on and log in to NMX VM.

1. On the vSphere client, click the **Virtual Machines** tab.
2. Right-click the <NMX VM> and **Power > Power On**.
The **State** notes **Powered On**.
3. Right-click <NMX VM> and select **Open Console**.
4. Select to **Start Windows Normally**.
5. At the Windows login dialog, type **Alt + Ctrl + Insert**, then enter: Administrator as the user name and Harmonic2008 as the password.
The Windows 2019 **Desktop** opens.

Alternately, you can connect with Remote Desktop protocol to the symbolic name "x2s-nmx" on the network connected to GbE8. This provides a larger available screen area than the VMware console, and allows easy copy/paste of files to the NMX desktop.

About certificates

One Harmonic self-signed certificate is included with the NMX installation; it works with the REST API.

This certificate is installed so that the use of REST API is not blocked after NMX installation.



NOTE: If required for security reasons, a customer certificate can be installed by customer IT support with the required server name present in the certificate's SAN.



NOTE: The certificate installed with the NMX installation is for **localhost** only.

If you intend to use LDAPS protocol, you must install your LDAPS server certificate on the NMX server.



NOTE: For information about NMX and LDAPS, refer to "Configuring LDAP Authentication for NMX" in the NMX User Guide.

Installing a certificate in Trusted Root Authorities directory

Follow these steps to install a certificate in the **Trusted Root Authorities** directory.

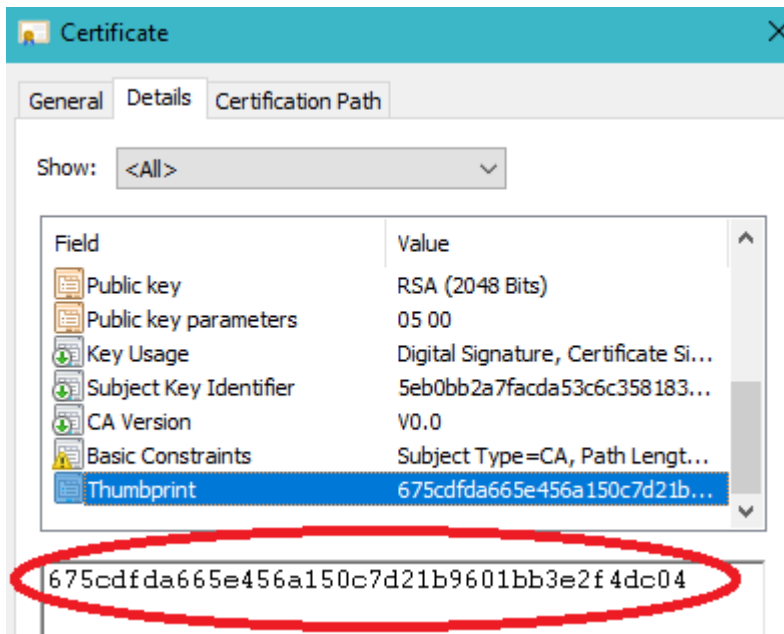
1. Get the certificate from the Domain Administrator of ITSupport and place it on your machine.
2. Double-click the certificate.
3. Select **Local Machine as the Store Location** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Select **Trusted Root Certificate Authorities** from the list and click **OK**.
6. Click **Next**.
7. Click **Finish**.

Configuring custom SSL certificates for REST API

An SSL certificate enables the use of the NMX REST API.

Before following these steps, complete the procedure outlined in [Installing a certificate in Trusted Root Certification Authorities](#).

1. Open the certificate manager on your local machine by using the **certlm.msc** command.
2. Locate the **Trusted Root Certification** and open its properties.
3. Click the **Details** tab and locate the **Thumbprint** field.
4. Copy the Thumbprint entry, as shown in the field below.



5. Close the window.
6. Open an Administrator command prompt.
7. Remove the existing binding of the certificate to the SSL port by entering the following command:

```
netsh http delete sslcert ipport=0.0.0.0:443
```
8. Add the new SSL port binding by entering the following command: `netsh http add sslcert ipport=0.0.0.0:443 certhash=675cdfda665e456a150c7d21b9601bb3e2f4dc04 appid={7CE058D3-892A-4318-9D3C-41FA3D8C6CE2}`
Note: The commands described in steps 7 and 8 are examples. The fixed appid of the NMX REST API is as follows: {7CE058D3-892A-4318-9D3C-41FA3D8C6CE2}
9. The new certificate is now bound to the NMS REST API and is ready to use.

Enabling SSL encryption for SQL Server

This procedure describes how to install a certificate to enable SSL encryption at the SQL Server. This encryption is useful in defending against various security threats.

Once you install SSL certificates on your SQL Server, then you can use following procedure to configure those SSL certificates for encryption.



NOTE: For more information on SSL encryption for SQL Server, including troubleshooting information, please consult the following article on the Microsoft Support site: "How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console".

To enable encryption at the server, open the SQL Server Configuration Manager and do the following:

1. Expand the SQL Server Network Configuration, right-click **Protocols** for your <server instance>, and then select **Properties**.
2. Click the **Certificate** tab, then select the desired certificate from the **Certificate** drop-down menu, and then click **OK**.
3. Click the **Flags** tab, select **Yes** in the **ForceEncryption** box, and then click **OK**.
4. Restart your SQL Server.

Chapter 3

Converting a Windows Server 2019 machine to an NMX server

This section describes how a Windows Server 2019 OS only machine can be converted into an NMX server.

- [Required software for conversion](#)
- [Installing SQL Server 2017](#)
- [Launching SQL Server Management Studio 18](#)
- [Launching the SQL Server Configuration Manager](#)
- [Installing the SNMP service](#)
- [Installing the IIS Web Server](#)
- [Adding Server Manager Features](#)
- [Configuring DCOM settings](#)
- [Configuring TCP/IP parameters](#)
- [Configuring Local Security Policy](#)
- [Completing the conversion](#)

Required software for conversion

he following software must be installed on the machine to be converted:

Table 3-1: Required Software

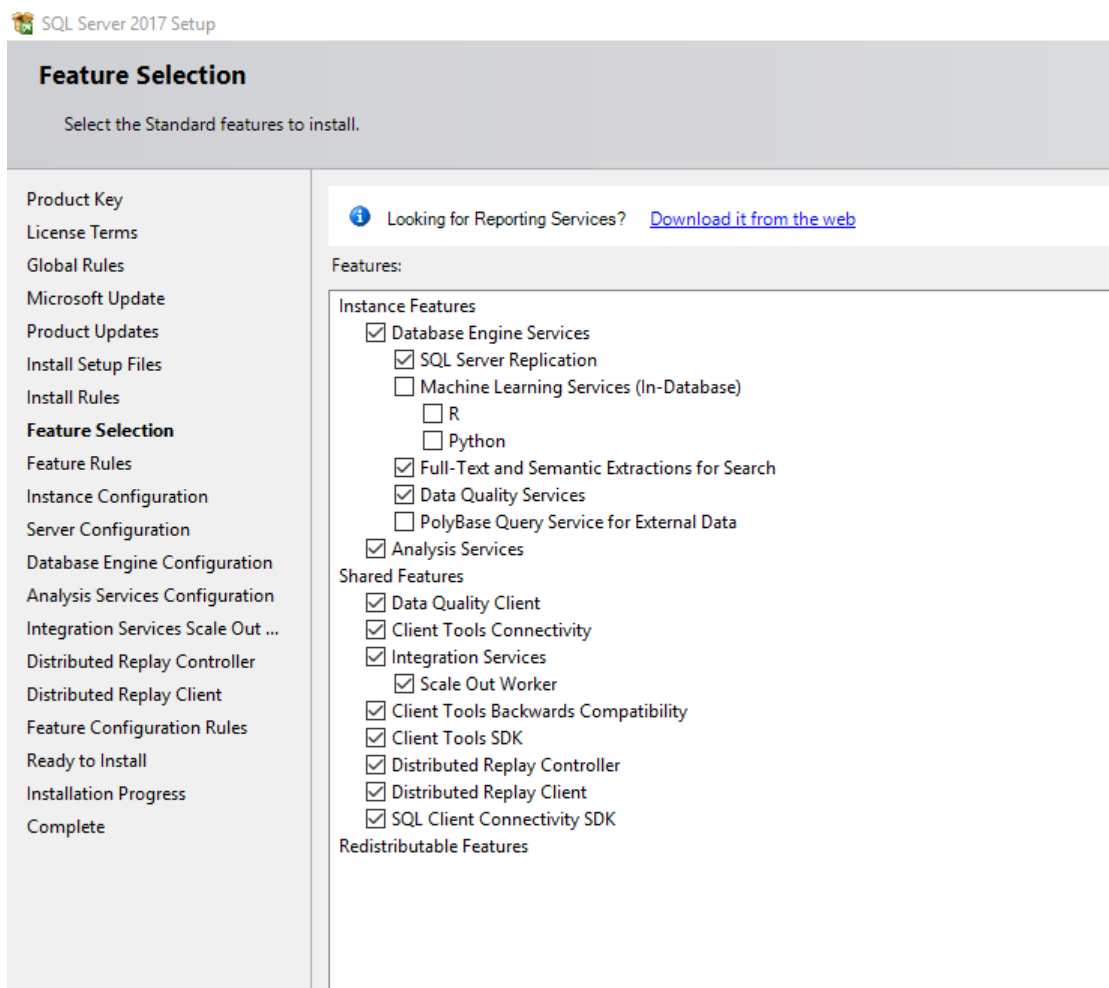
Software	File Name
SQL Server 2017 - For Windows Server 2019	en_sql_server_2017_standard_x64_dvd_11294407.iso
Microsoft SQL Server Management Studio 18 - For Windows Server 2019	SSMS-Setup-ENU.exe
Google Chrome	Latest version from Google

Installing SQL Server 2017

Step one is installing SQL Server 2017 on the machine to be converted.

1. Download and mount the SQL Server installer.

2. Launch the SQL Server installer using the setup file in the mounted directory.
3. Click on **Installation** and then **New SQL Server stand-alone installation or add features to an existing installation** and, until and unless specified, use the default configurations provided by the installer.
4. Select **Setup Role** as **All Features with Defaults**.
5. Verify that the following **Prerequisites** are already installed. Make selections as necessary.



Result:

6. Click **Instance Configuration**, then select **Default Instance** and verify that the **Instance ID** is **MSSQLSERVER**.
7. Click **Server Configuration** and set the **Startup Type for SQL Server Agent** to **Automatic**.
8. Click **Database Engine Configuration**, then click the **Server Configuration** tab, and then select **Mixed Mode**.
9. Enter any password for the **sa** account, such as "harmonic@123".
Note: Later, once the SQL Server is installed, you must set the **sa** password as "harmonic".
10. Click **Next**, and select the **Add Current User** on any subsequent windows if that option is present. This provides permissions to the current user for different SQL services.

11. The SQL Server installation will start and you will see the message, **“Your SQL Server 2014/2017 installation completed successfully”** when the installation is complete.
12. Close the setup window.
13. Eject the drive on which you mounted the installer.

Launching SQL Server Management Studio 18

Step two is launching the SQL Server Management Studio 18 for Windows 2019.

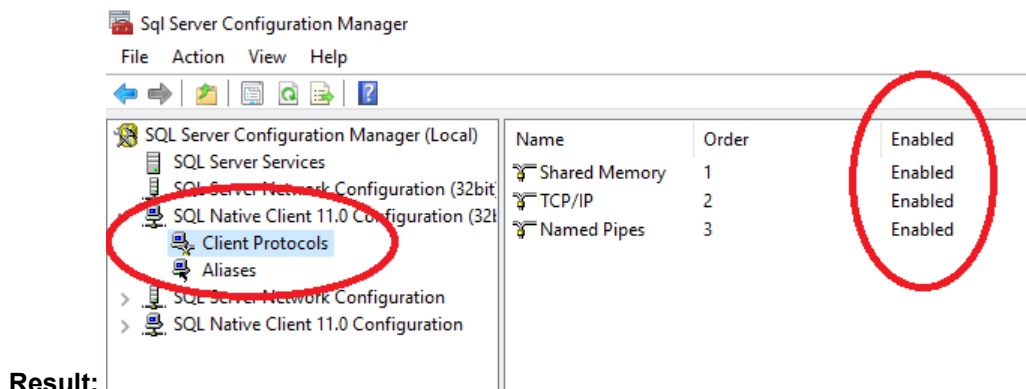
Launch and login to the SQL Server Management Studio and perform the following steps:

1. Navigate to **Security > Logins** and change the password for the **sa** account to “harmonic”.
2. Uncheck the **Enforce password policy** option and click **OK**.
3. Go to **Security > Logins** and open the properties for **NT_Authority/System**.
4. Select the **public** and **sysadmin** roles on the **Server Roles** page.
5. Add a new login with the name “NMXUser” and SQL Server authentication with the Password and Confirm Password fields left blank.
6. Uncheck the **Enforce password policy** option.
7. Select the **public** and **sysadmin** check boxes on the **Server Roles** page.
8. Open the **Facets** options by right-clicking on the **SQL Server instance name** and make the following changes:
 - a. Select the facet **Server Security** and set **XPCmdShellEnabled** as **True**.
 - b. Select the facet **Server Configuration** and set **OleAutomationEnabled** as **True**.
9. Close the Security window to save your changes.

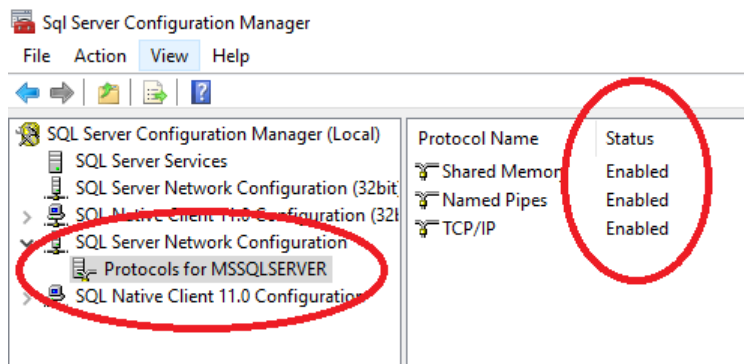
Launching the SQL Server Configuration Manager

Step three is to launch the Microsoft SQL Server Configuration Manager and verify the following settings:

1. Verify that **SQL Native Client 11.0 Configuration(32bit) >Client Protocols > All** are enabled.

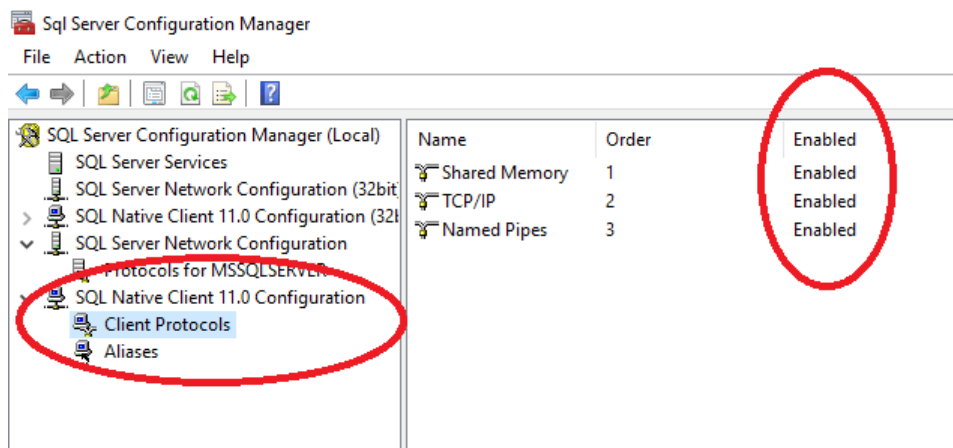


2. Verify that **SQL Server Network Configuration > Protocols for MSSQLSERVER > All** are enabled.



Result:

3. Verify that **SQL Native Client 11.0 Configuration > Client Protocols > All** are enabled.



Result:

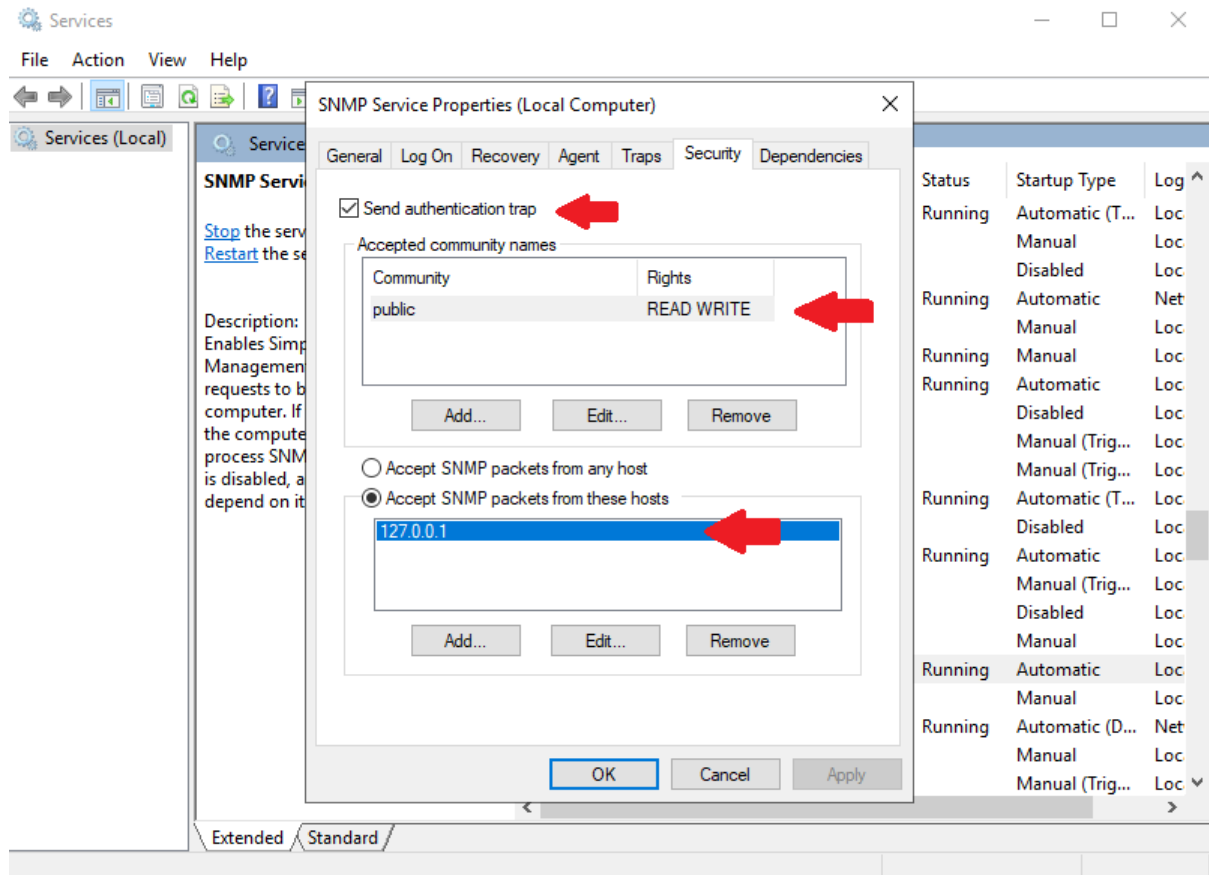
4. Close the Configuration Manager when you are finished.

Installing the SNMP service

Step four is installing the SNMP service.

1. Open the **Server Manager** and go to **Add Roles and Features**.
2. Navigate to **Features > Remote Server Administration Tools > Feature Administration Tools > SNMP Tools**.
3. Select the **SNMP Service > SNMP WMI Provider**. If the SNMP service is already installed, follow the next step.
4. Open a Command prompt in **Administrator** mode.
5. Enter **services.msc** to open the **Services** window and select the **SNMP Service**.

6. Open the **SNMP Service properties**, click the **Security** tab, then make the following changes:
 - a. Make sure **Send authentication trap** is checked.
 - b. In **Accepted community names**, make sure the **public** community is added with **READ WRITE** rights enabled.
 - c. Select **Accept SNMP packets from these hosts** and add **localhost** or **127.0.0.1**.

Result:

7. Click **OK**.
8. Close the Server Manager when you are finished.

Installing the IIS Web Server

Step five is to install the IIS Web Server.

1. Open the **Server Manager** and go to **Add Roles and Features**.
2. Under **File and Storage Services**, select **File and iSCSI Services**.
3. Under **File and iSCSI Services**, select **File Server**.

4. Under **Server Roles**, select **Web Server (IIS)** and the following options:
 - a. **Web Server** and keep all other options which are selected automatically.
 - b. **HTTP Redirection** under **Common HTTP Features**.
 - c. Under **Application Development** select the following options:
 - .NET Extensibility 3.5
 - .NET Extensibility 4.5 (4.7 for Windows 2019)
 - ASP
 - ASP.NET 3.5
 - ASP.NET 4.5 (4.7 for Windows 2019)
 -
 - d. Under **FTP Server** select **FTP Service**.
 - e. Under **Management Tools**, select **IIS 6 Management Compatibility** and **IIS 6 Metabase Compatibility**.
 - f. Install the selected features.

Add Roles and Features Wizard

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- ☐ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☒ Web Server (IIS) (8 of 43 installed)
 - ☒ Web Server (7 of 34 installed)
 - ☒ Common HTTP Features (4 of 6 installed)
 - ☒ Default Document (Installed)
 - ☒ Directory Browsing (Installed)
 - ☒ HTTP Errors (Installed)
 - ☒ Static Content (Installed)
 - ☒ HTTP Redirection
 - ☐ WebDAV Publishing
 - ☐ Health and Diagnostics (1 of 6 installed)
 - ☐ Performance (1 of 2 installed)
 - ☒ Security (1 of 9 installed)
 - ☒ Request Filtering (Installed)
 - ☒ Basic Authentication
 - ☐ Centralized SSL Certificate Support
 - ☐ Client Certificate Mapping Authentication
 - ☐ Digest Authentication
 - ☐ IIS Client Certificate Mapping Authentication
 - ☐ IP and Domain Restrictions
 - ☐ URL Authorization
 - ☐ Windows Authentication
 - ☒ Application Development
 - ☒ .NET Extensibility 3.5
 - ☒ .NET Extensibility 4.7
 - ☐ Application Initialization
 - ☒ ASP
 - ☒ ASP.NET 3.5
 - ☒ ASP.NET 4.7
 - ☐ CGI
 - ☒ ISAPI Extensions
 - ☒ ISAPI Filters
 - ☐ Server Side Includes
 - ☐ WebSocket Protocol
 - ☒ FTP Server
 - ☒ FTP Service
 - ☐ FTPS Service
 - ☒ Management Tools (1 of 7 installed)
 - ☒ IIS Management Console (Installed)
 - ☒ IIS 6 Management Compatibility
 - ☐ IIS Management Scripts and Tools
 - ☐ Management Service
 - ☐ Windows Deployment Services

Result:

5. Open the IIS manager and verify that the following application pools are present:

Result:

Name	Status	.NET CLR V...	Manage...	Identity
 .NET v2.0	Started	v2.0	Integrated	ApplicationPoolIdentity
 .NET v2.0 Classic	Started	v2.0	Classic	ApplicationPoolIdentity
 .NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity
 .NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity
 Classic .NET AppPool	Started	v2.0	Classic	ApplicationPoolIdentity

6. Close the **Server Manager** when you are finished.

Adding Server Manager Features

Step six involves adding features from the Server Manager.

1. Open the **Server Manager** and navigate to **Add Roles and Features**.
2. Select the following features:
 - .NET Framework Features for 3.5 and 4.7
 - Media Foundation
 - Message Queuing Service
 - Remote Server Administration Tools
3. Save and exit the Server Manager.

Configuring DCOM settings

Step seven involves configuring the DCOM settings.

1. Open a Command prompt with **Administrator** authority.
2. Enter **dcomcnfg** to open the **Component Services**.
3. Navigate to **Component Services > Computers > My Computer**.
4. Open the **Properties** and click the **Default Properties** tab.
5. Verify that the **Default Impersonation Level** is set to **Identity**.
6. Click **OK**.

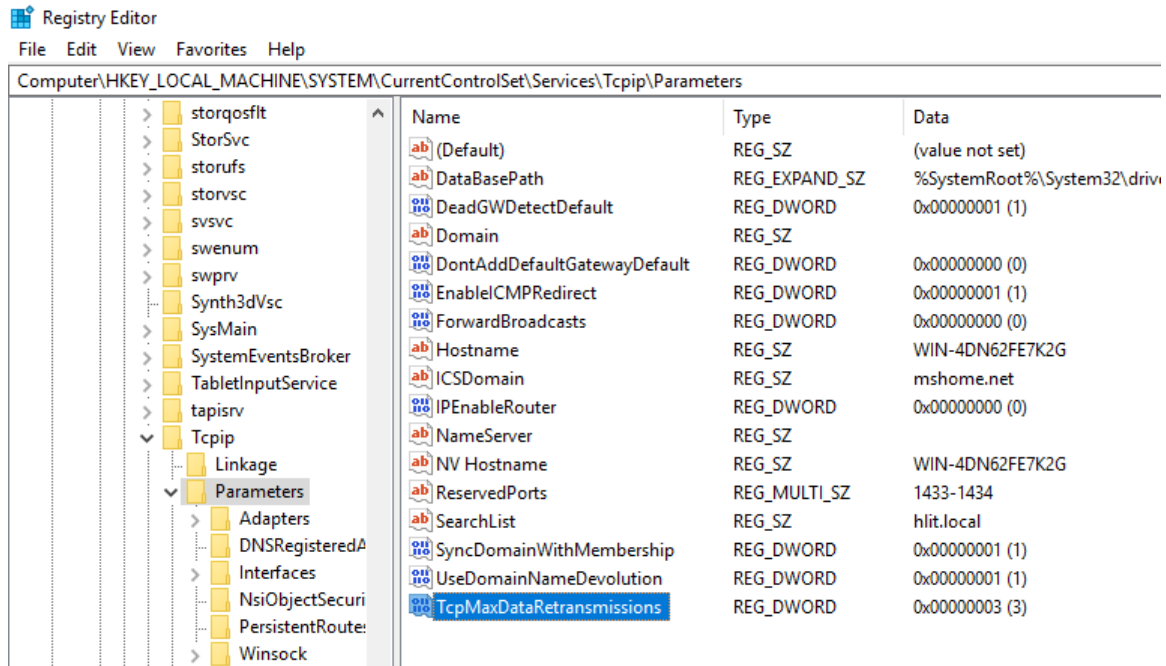
Configuring TCPIP parameters

Step eight involves configuring the TCPIP parameters.

1. Open the **Registry Editor**.
2. Navigate to **Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**.

- Set the value of the **TcpMaxDataRetransmissions** registry key (**DWORD**) to **3**.

Note: This will allow 3 TCP re-transmissions and is useful in case of intermittent network issues.

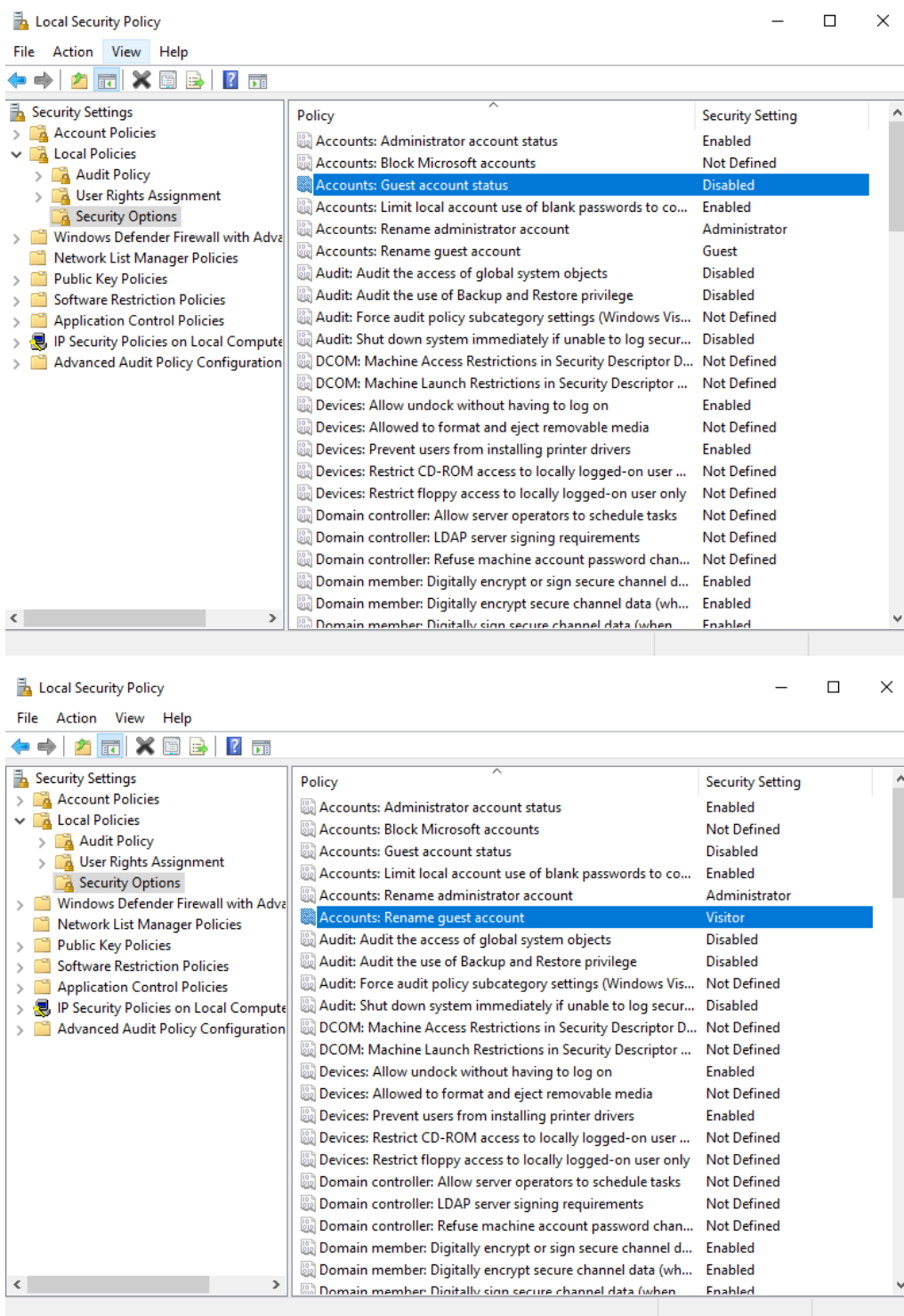


- Save your changes and close the Registry Editor.

Configuring Local Security Policy

Step nine involves configuring the local security policy for your machine.

- Open the Local Security Policy.
- Navigate to **Local Policies > Security Options**.

3. Disable and rename the **Guest** user account for Windows, as shown:

4. Save your work and close Local Security Settings.

Completing the conversion

The tenth and last step to complete the conversion involves running the server hardening scripts (included with NMX) and installing the latest version of Google Chrome.

1. Download the **NMX_Server-HardeningScripts.zip** file and unzip it.
2. Open a Command prompt in **Administrator** mode and go to the **NMX_Server-HardeningScripts** folder.
3. Run **NMX_Server_Hardening.bat**.
4. Download the latest version of the Google Chrome browser and install it.
5. Restart the platform.

Migrating a Windows 2012 Server to a Windows 2019 Server for NMX

There are 2 methods you can use to backup catalogs from a Windows 2012 Server / SQL server 2014 machine and restore them to a Windows 2019 Server / SQL server 2017 machine.

- *Method 1: Using the Domain Manager*
- *Method 2: Using PowerShell scripts*

Method 1: Using the Domain Manager

Using the Domain Manager within NMX is only recommended when there are less than 5 catalogs present on the NMX Server.

1. Open the NMX **Domain Manager** on the Windows 2012 Server.
2. Navigate to **Database tab > Catalog Management**.
3. Select the database you want to backup and click **Backup**.
4. Copy the backed up database file (*.hzb) to the Windows 2019 Server.
5. Using the NMX Domain Manager GUI on the new server, restore the *.hzb file using the **Database tab > Catalog Management** option.

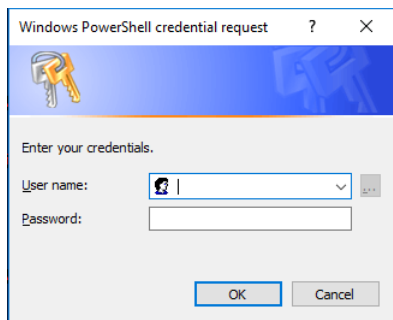
Method 2: Using PowerShell scripts

This method is made up of two steps as follows.

1. **Step One:** Backing up all of the existing catalogs on the Windows 2012 Server/SQL Server 2014 machine.
 - a. Log on to the Windows 2012 machine.
 - b. Create a folder called **C:\NMXDBBackup**.
 - c. Download the PowerShell script **Export-NmxDb.ps1** to the folder you created.
 - d. Open a Command prompt in Administrator mode.
 - e. Navigate to the folder you created and execute **.\Export-NmxDb.ps1 C:\NMXDB**.

```
PS C:\NMXDBBackup> get-help .\Export-NmxDb.ps1
NAME
    C:\NMXDBBackup\Export-NmxDb.ps1
SYNOPSIS
    Exports all user databases to a folder specified by the user
SYNTAX
    C:\NMXDBBackup\Export-NmxDb.ps1 [-BackupPath] <String> [<CommonParameters>]
DESCRIPTION
    The Export-NmxDb backs up databases from 2014 sql server.
RELATED LINKS
REMARKS
    To see the examples, type: "get-help C:\NMXDBBackup\Export-NmxDb.ps1 -examples".
    For more information, type: "get-help C:\NMXDBBackup\Export-NmxDb.ps1 -detailed".
    For technical information, type: "get-help C:\NMXDBBackup\Export-NmxDb.ps1 -full".
```

- f. Enter **sa** for the **User name** and the associated **Password** when prompted.



- g. Copy the backed up catalogs to a thumb drive or disk.

2. **Step Two:** Restoring those catalogs on the Windows 2019 Server/SQL Server 2017 machine.

- a. Log on to the Windows 2019 machine.
- b. Create a folder called **C:\NMXDBBackup**.
- c. Copy the backed up catalogs (*.bak) from the Windows 2012 machine using the **Export-NmxDb.ps1** script into that folder.
- d. Download the PowerShell script **Import-NmxDb.ps1** to the folder you created.
- e. Open a Command prompt in **Administrator** mode.
- f. Navigate to the folder you created and execute **.\Import-NmxDb.ps1 C:\NMXDB**.

```
PS C:\NMXDBBackup> get-help .\Import-NmxDb.ps1

NAME
    C:\NMXDBBackup\Import-NmxDb.ps1

SYNOPSIS
    Imports all user databases to a folder specified by the user

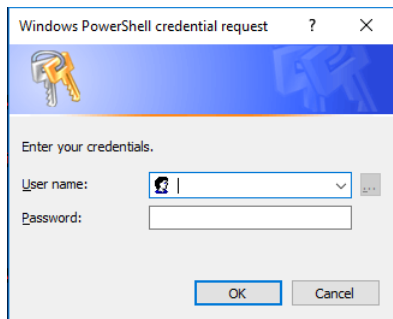
SYNTAX
    C:\NMXDBBackup\Import-NmxDb.ps1 [-BackupPath] <String> [-ReplaceDatabase] [<CommonParameters>]

DESCRIPTION
    The Import-NmxDb restores databases from 2014 sql server to 2017 sql server.

RELATED LINKS

REMARKS
    To see the examples, type: "get-help C:\NMXDBBackup\Import-NmxDb.ps1 -examples".
    For more information, type: "get-help C:\NMXDBBackup\Import-NmxDb.ps1 -detailed".
    For technical information, type: "get-help C:\NMXDBBackup\Import-NmxDb.ps1 -full".
```

- g. Enter **sa** for the **User name** and the associated **Password** when prompted.



- h. Verify that all the catalogs are present in the folder.

Chapter 5

Upgrading NMX Server

NMX, starting with NMX 8.5, includes new hardware platforms and a new recovery image. Upgrading your NMX software involves working with Harmonic to upgrade or replace existing hardware (depending on your server model), and changes associated with your current NMX release and the release you will upgrade to, before upgrading to NMX 8.5.x or later.

 **IMPORTANT:** Depending upon which NMX release platform you upgrade from, you may complete the recovery image upgrade to NMX 8.5.x process once (from NMX 6.6.8 and later releases), or twice (from NMX 6.4.1 and earlier releases). Whenever you deploy a recovery image the server is reformatted, so your upgrade is really a first-time NMX installation.

 **IMPORTANT:** Whenever you upgrade device hardware that is supported by NMX, you will need to re-create the devices in your NMX network map and service maps. For example, if you upgrade from Electra 8200 to Electra X, or from ProStream® 1000 to ProStream X/XVM, you will need to:

- Delete the old devices from your existing NMX Network map and re-create the devices in the network with the new hardware model.
- Delete services in your service map that are associated with the old devices, and re-create the services associated with the correct device type.

NMX cannot recognize the network or service maps unless the device and service information is correct.

- [Upgrading NMX overview](#)
- [Backing up catalogs](#)
- [Uninstalling NMX](#)
- [Downloading the NMX installation package](#)
- [Upgrading the NMX Server software](#)
- [Logging in to Windows 2019 Server](#)
- [Upgrading the NMX catalog](#)
- [Upgrading NMX Client software](#)
- [Device end of service information for NMX 8.5.x and later](#)
- [Upgrading to NMX 8.4 and later](#)
- [Device end of service information for NMX 8.x and later](#)
- [Upgrading from NMX 6.x to NMX 7.x \(catalog sync IDs\)](#)
- [Upgrading NMX catalogs](#)
- [Upgrading Java JRE](#)

Upgrading NMX overview

Upgrade procedures are dependent upon the release from which you are upgrading. If you purchased your device from Harmonic, it includes the recommended Operating System (OS) and database prerequisites, based on the software you purchased.

Table 5-1: Upgrading NMX

Upgrade from	Running on Windows OS/ SQL Server	To
NMX 7.5.0 and later	Windows Server 2012/SQL Server 2014	NMX 8.5.x and later release running on Windows Server 2019/SQL Server 2017 1. Back up your catalogs. Refer to the Migrating a Windows 2012 Server to a Windows 2019 Server for NMX chapter for more information. 2. Uninstall the current NMX software. 3. Install the new NMX software. 4. Activate/upgrade/back up your catalogs.

Upgrade from	Running on Windows OS/ SQL Server	To
NMX 6.6.8.x GA and later	Windows Server 2008/SQL Server 2008	NMX 7.6.0 running on Windows Server 2012/SQL Server 2014 1. Review/complete "Special system upgrade requirements" in the "Upgrading from NMX 6.6.8 and later to NMX 7.6.x and later" section. 2. Back up your 6.6.8.x catalogs and maps to an external drive. 3. If necessary, upgrade or replace your hardware, then deploy the latest version of the WS2019 recovery image provided for NMX. 4. If necessary, upgrade to new device hardware, then deploy the recovery image for 7.6.x. 5. Install the 7.6.x software and configure the Meinberg NTP Server. 6. Activate/upgrade/back up your catalogs.

Upgrade from	Running on Windows OS/ SQL Server	To
NMX 6.4.1 GA and earlier	Windows Server 2003, SQL Server 2008	NMX 6.6.8 running on Windows Server 2008/SQL Server 2008, and then to Windows Server 2012/SQL Server 2014 in a two-step process. 1. Review/complete "Special system upgrade requirements" in the "Upgrading from NMX 6.4.1 and earlier to NMX 7.6.x and later" section. 2. Back up your 6.4.1 catalogs and maps to an external drive. 3. Upgrade your BIOS and OS to Win 2008/ SQL 2008 as described in "Upgrading from NMX 6.4.1 and earlier to NMX 7.6.x and later." 4. After upgrading the BIOS and OS, install the 6.6.8 software. 5. Review/complete "Special system upgrade requirements" in the "Upgrading Win 2008/SQL 2008 to Win 2012/SQL 2014" section and activate/ upgrade/back up your catalogs to an external drive. 6. If necessary, upgrade to new device hardware, then review/complete "Installing NMX Server for the first-time overview." 7. Activate/upgrade/back up your catalogs and maps.

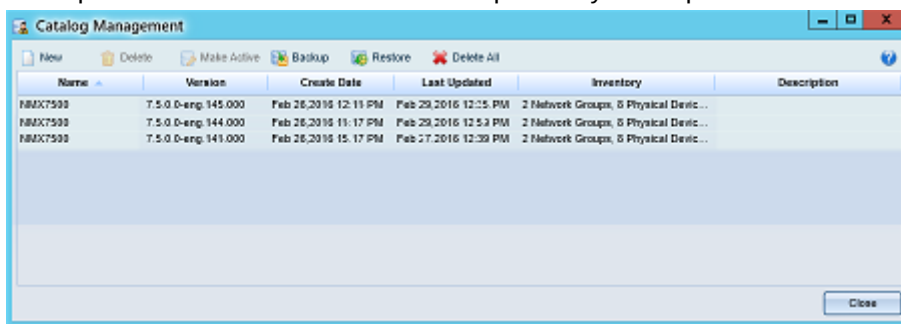
Backing up catalogs

Back up your catalogs frequently as insurance against catalog loss or data corruption, or before upgrading.

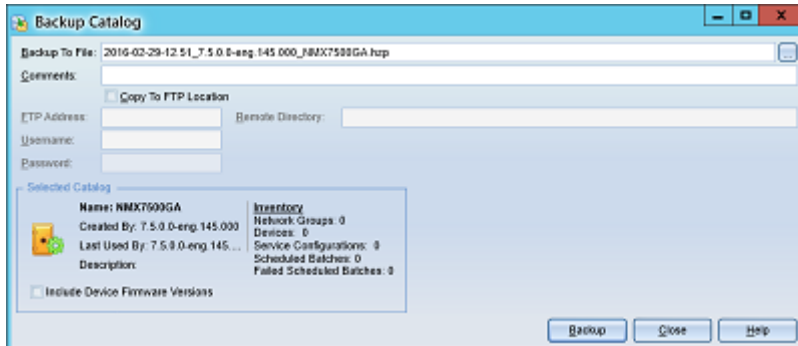
Before you begin

If you are backing up catalogs before upgrading with a recovery image, make sure to copy them to an external drive.

1. From **NMX Domain Manager > Database** tab, click the **Catalog Management** tab.
2. On the **Catalog Management** dialog, select the catalog you want to back up, then click **Backup**.
When you manually back up a catalog, NMX stores it in C:\DatabaseBkup. Automatic daily catalog backups are stored in C:\DatabaseBkup\DailyBackups.



3. Complete the options on the **Backup Catalog** dialog.



- Backup to File** The name of the backup file.
- Comments** Add a description of this file.
- Copy to FTP Location** Copies the catalog to any valid FTP location.



IMPORTANT: For backups to Anonymous FTP sites, the remote directory must exist, and you must have a valid username and password.

FTP Address	Enter the FTP address.
Remote Directory	Enter the name of the FTP remote directory.
Username	Enter the username for the FTP site.
Password	Enter the password for the FTP site.
Include Device Firmware Versions	Copies all managed device firmware versions; takes longer to backup, but includes all your current device firmware.

4. Click **Backup**.

Result: A status dialog notes when the selected catalog is backed up.

Uninstalling NMX

Manually uninstall your existing NMX release before upgrading to the current release.

1. Open NMX Domain Manager and stop the NMX Server.
2. Go to the **Control Panel's Uninstall or Change a Program** dialog to uninstall NMX.
3. Select the NMX release, then click **Uninstall/Change**.
This feature will prompt you to confirm the removal of redundancy and other NMX components. Harmonic recommends that you respond **Yes** or **Remove** to the prompts.
4. Restart the system at the prompt.

Downloading the NMX installation package

Download the NMX installation software onto the NMX Server.

1. From your NMX Server, log in to <https://harmonic.force.com/SWAccess/SWDownloadLogin>.
2. Navigate to: **Home > Service & Support > Software Downloads > Authorized Products > \NMX 8.x Application**.
3. Open the correct NMX directory for your installation.
4. Download all the files in the directory to NMX Server **Desktop**.

Upgrading the NMX Server software

Install the current NMX software onto the NMX Server.

1. Open the installation directory and double-click the Install_NMX_<BuildNo>.exe file.
2. Click **Next** in the **Setup - NMX** dialog.

3. In the **NMX Registration** dialog, enter your user name and company name, if it is not already there, and click **Next**.
4. In the **License Agreement** dialog, select to accept the license agreement and click **Next**.
5. In the **Select Components** drop-down, select **Client and Server**, and click **Next**.
6. Complete the fields in the **Server Settings** dialog.
In most cases, NMX displays the information from your earlier NMX installation.

Site ID	Enter a unique identifier for the Site ID . You can enter any number from 11–2000. This number must be unique for all NMX Server instances on the network.
SQL Server Name	Confirm or edit the host name of the computer where the SQL Server database will be installed.
SQL Catalog Name	Enter a name for the SQL Server catalog you will use. The name must start with an alphabetic character. In this step, you're just naming the catalog. You must create the catalog in NMX Domain Manager after you finish installation. The default catalog name is NMxDB.
Backup Directory Path	Accept the default for the Backup Directory Path . This is the full path to a directory on the SQL Server computer where you want to save database backups.

7. Click **Next**.



NOTE: If your server does not have enough memory for the SQL database, click **Yes** if you are prompted to modify the SQL memory size (selecting yes sets the memory size to 50% of available RAM).

8. On the **Ready to Install** dialog, click **Install**.
Installation begins.
9. Documentation requires Adobe Reader. Click **Install** and follow any onscreen steps to install Adobe Reader.
If Adobe prompts you to restart the system, select to **Restart later**, and complete the installation process first.
10. Click **Next** in the **Setup - NMX** dialog.
11. When the installation finishes, click **Finish** to restart the computer.
Restarting ensures proper performance.

Logging in to Windows 2019 Server

Log in to Windows.

1. Start the Windows 2019 computer.

2. Log in:

User: Administrator

Password: Harmonic2008

You must log in to Windows as a user with administrator permissions to run the NMX Server software. The server must have a password set up for access from Windows 10 clients. The administrator can add other users, if necessary.

3. Click **OK**.

Result: The NMX applications, documentation folders appear on the desktop.

Upgrading the NMX catalog

When you upgrade NMX without installing a recovery image, you can upgrade your catalog after logging in to NMX Domain Manager.

1. Open and log in to NMX Domain Manager.
harmonic is the password.
2. On the **Database Configuration** dialog, enter the SQLServer **User Name** and **Password** to upgrade your older catalog.



User Name is sa and **Password** is harmonic.

3. Immediately after the catalog upgrade, use the **NMX Domain Manager > Home tab > Validate > Validate System** button to check your catalog for duplicate sync IDs. If the test reports failures, please contact Technical Support to manually fix the catalog. Duplicate sync IDs can affect **Site Sync** and lead to service loss.



Upgrading NMX Client software

Upgrade your standalone NMX Client application on a supported platform (Windows 10 clients or Windows 2019 Server) after you have installed or upgraded NMX Server on another computer.

Before you begin

Make sure the NMX Client computer is connected to your network.

1. Uninstall your current NMX Client software and restart the computer.
2. Copy the NMX installation directory to your client computer.
3. Double-click the Install_NMX_<BuildNo>.exe file.
4. Open the NMX installation directory and double-click the Install_NMX_<BuildNo>.exe file.
5. Click **Next** in the **Setup - NMX** dialog.
6. In the **NMX Registration** dialog, enter your user name and company name, then click **Next**.
7. In the **License Agreement** dialog, select to accept the license agreement, then click **Next**.
8. In the **Select Components** drop-down, select **Client only**, and click **Next**.
9. On the **Ready to Install** dialog, click **Install**.
NMX begins installing files.
10. On the **Setup - NMX** dialog, click **Finish** to restart the computer.
11. Log in to Windows after the restart completes.

Device end of service information for NMX 8.5.x and later

Some devices are End of Service (EOS) and are not supported in NMX 8.5.x.

The following devices are EOS and cannot be upgraded to NMX 8.5.x: Electra 8100/8200/8300, Ellipse 1000/2000, Iris, and ProMedia X Origin. You will need to remove or replace EOS devices from the original catalog and maps before upgrading to the current NMX release.

Upgrading to NMX 8.4 and later

To upgrade to NMX 8.4 and later releases requires you to first install SP3 of SQL Server 2014.

This section provides a brief Frequently Asked Questions (FAQ) about this procedure.

Question	Answer
Is it OK to install NMX 8.4.x without SQL 2014 Service Pack 3 if it is not asked by Windows?	No. SQL Service Pack 3 must be installed before installing NMX8.4.x build. First install all windows updates and then install SQL 2014 SP3.
Should we uninstall the old Service Packs in advance?	No. Do not uninstall any Windows/SQL server patch/SP manually.

Question	Answer
Should we make the Windows upgrades offline in advance?	Yes. Install all Windows updates before installing NMX8.4.x build.
When do we recommend to upgrade Windows offline?	If there is no internet connection, then upgrade Windows offline by using the wsusoffline118 tool. Refer to https://www.wsusoffline.net/docs/ for more information.
When is it better to re-image?	Harmonic strongly recommends upgrade using the latest recovery image.
Can we split the SQL-patching from the NMX8.4.1/ PSX-Firmware Upgrade?	Yes. NMX8.3 works with SQL SP3.

Device end of service information for NMX 8.x and later

Some devices are End of Service (EOS) and are not supported in NMX 8.x.

The following devices are EOS and cannot be upgraded to NMX 8.x: Ion Encoder, Audio Encoder, Ion AVC HD, Ion AVC SD, Electra 1000, Electra 5000, Electra 5400, Electra 7000, Proview 2900, ProStream 1000. You will need to remove or replace EOS devices from the original catalog and maps before upgrading to the current NMX release.

Upgrading from NMX 6.x to NMX 7.x (catalog sync IDs)

After upgrading from NMX 6.x to NMX 7.x, run **Validate System** to test your upgraded catalog for duplicate sync IDs, which can affect **Site Sync** and lead to service loss.

- Immediately after the catalog upgrade, use the **NMX Domain Manager > Home tab > Validate > Validate System** button to check your catalog for duplicate sync IDs. If the test reports failures due to sync ID duplication, please contact Technical Support to manually fix the catalog. Duplicate sync IDs can affect **Site Sync** and lead to service loss. You should be able to resolve other types of system failures.

Upgrading NMX catalogs

After first-time NMX installation, upgrading your catalogs involves logging into NMX Domain Manager, creating a new catalog, then restoring, activating, and upgrading your backed up catalog. Upgrading from recent releases involves logging into NMX Domain Manager and activating/upgrading your existing catalog.

If your NMX installation did not include a recovery image, your backed up catalog is upgraded to the new version when you activate it.

All of the NMX network, services, and device configuration information are created, accessed, and stored in SQL Server® database catalog files. NMX requires an active database catalog in which NMX Server can store information. After you have installed or upgraded the NMX Server application, first-time installations must create a catalog for NMX to reference before they begin working. If you are upgrading

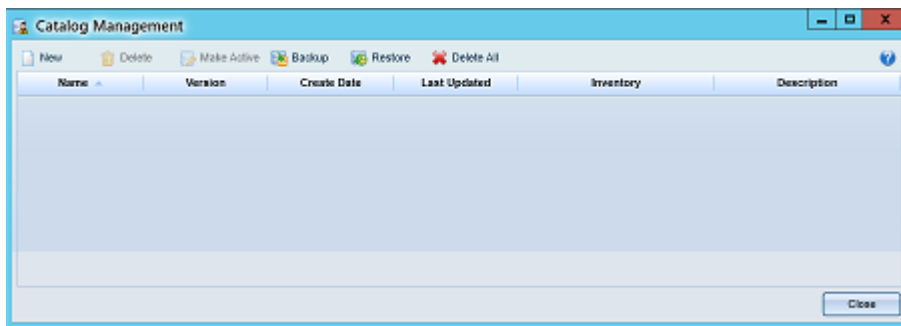
from a recent release, the upgrade occurs automatically when you activate your last catalog. NMX copies, renames, and upgrades the catalog to the current release. The new catalog name is appended with the upgraded version and build number.

Templates created in NMX 7.0 and later releases are supported in this release; templates created in releases before 7.0 are not supported and must be re-created.

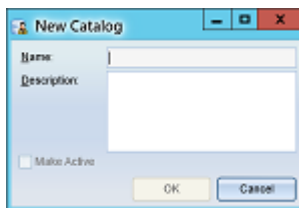
Upgrading catalogs after first-time NMX installation

Create a new catalog so that you can restore your backed up catalog to the new catalog.

1. From **NMX Domain Manager > Database** tab, click the **Catalog Management** tab.
2. Enter **sa** in the **User Name** field and **harmonic** in the **Password** field.
3. Select the **Remember Login Information** check box for NMX Domain Manager to remember your login credentials while you are working in NMX Domain Manager, then click **OK**.
4. On the **Catalog Management** dialog, click **New**.

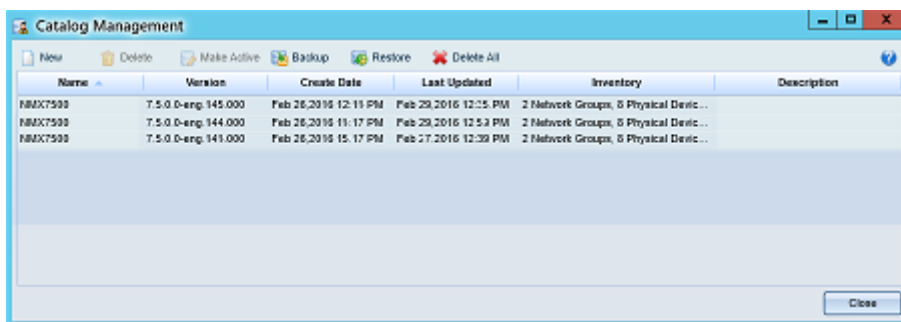


5. On the **New Catalog** dialog, enter a **Name** and a **Description**, then click **OK**.



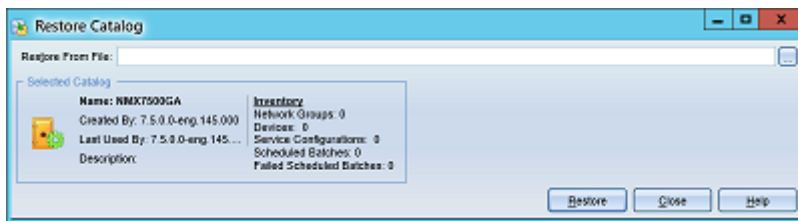
6. Select the catalog you want to restore with another catalog.

 **NOTE:** Restoring a catalog will overwrite the selected catalog.



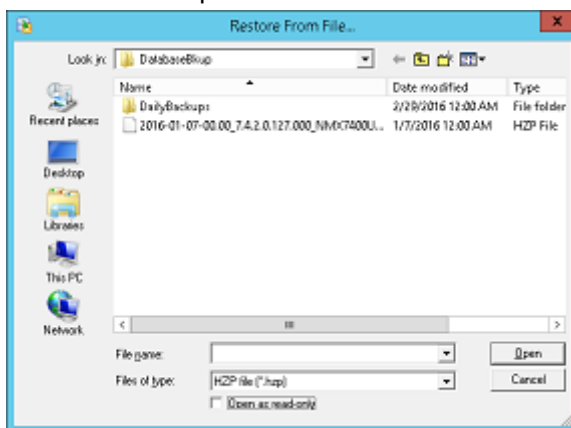
7. Click **Restore**.

8. From the **Restore Catalog** dialog box, click



9. Browse to select a catalog to restore.

When you manually back up a catalog, NMX stores it in C:\DatabaseBkup. Automatic daily catalog backups are stored in C:\DatabaseBkup\DailyBackups. The catalog can be restored from either location. If your catalog is on another drive or on the Desktop, move the catalog to C:\DatabaseBkup.



If you will edit the catalog you are restoring, make sure that you clear the **Open as read-only** check box.

10. Select **Open**, then **Restore**.
11. Click **Yes** at the confirmation dialog then Log in to confirm the catalog upgrade: sa/harmonic
12. Click **OK** and then **Close**.

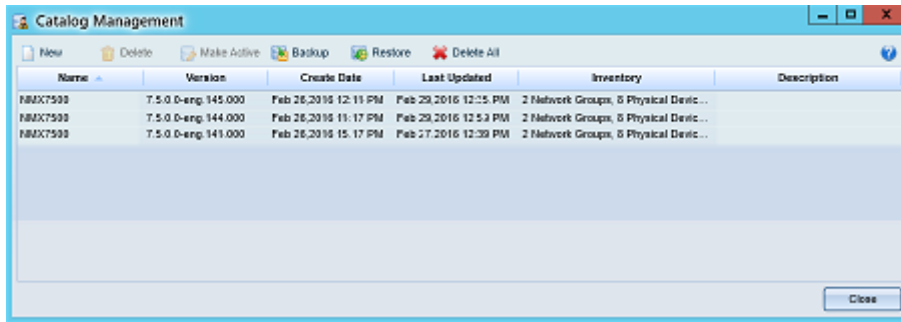
Activating catalogs

Activate a catalog in which to store all NMX network, services, and device configuration information.

If you are upgrading NMX, your catalog is upgraded to the new NMX release when you open NMX Domain Manager or if you select to open and activate a backed up catalog.

1. From **NMX Domain Manager** > **Database** tab, click the **Catalog Management** tab.
2. Enter sa in the **User Name** field.
3. Enter harmonic in the **Password** field.
4. Select the **Remember Login Information** check box for NMX Domain Manager to remember your login credentials while you are working in NMX Domain Manager, then click **OK**.

5. Select a catalog from the list, then click **Make Active**.

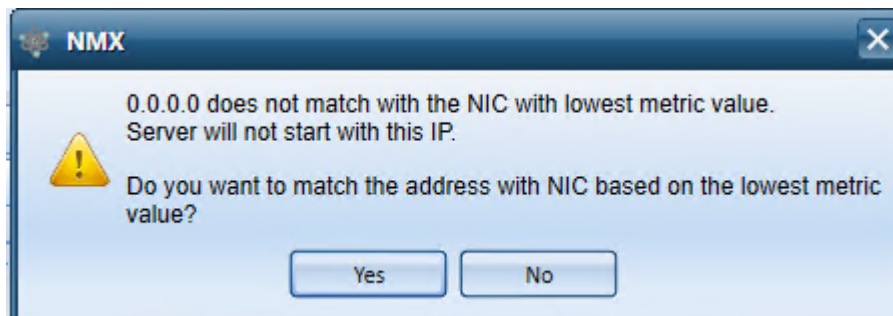


6. Click **Close**.
The catalog is active and ready for when you start the NMX Server.

Starting the NMX Server

Start NMX Server before opening NMX applications.

1. From the **NMX Domain Manager > Home** tab, click **Start Server**.
2. On the message confirming if you want the IP address to match the highest NIC, click **OK**.
This message appears only for first-time NMX installations, when you start NMX Server for the first time.



NMX Server processes are started when the toolbar **Status** displays **Server Started**.

What to do next

Harmonic recommends backing up your NMX map as soon as you have a working version completed. Back up the C:\database\bkup file to another location, away from the local disks of the Electra X2S platform, using FTP or Remote Desktop copy-and-paste. This protects against a storage medium failure and allows you to quickly restore service if the hardware requires replacement.

Upgrading Java JRE

For NMX releases 8.2.0 and higher, the Java JRE (OpenJDK) can be replaced or updated.

When NMX software is installed, the installer checks the JRE version present on the server and replaces it with the version embedded in NMX package if it is more recent. You can also install an up to date JRE version when required when a vulnerability fix is released.

Upgrading the JRE

Follow this procedure to upgrade the Java JRE on your NMX server.

1. Stop the NMX Server.
2. **(For NMX 8.4 or above only)** Navigate to **C:\Program Files\Harmonic\NMX** and execute the following script: **StopWinServicesBeforeJREUpgrade.bat**.
3. Open the Windows Control Panel and uninstall the current version of OpenJDK 8 Amazon Corretto.
4. Make sure folder **C:\Program Files\Harmonic\java** is created and empty.
5. Download and install the latest desired version of OpenJDK 8 Amazon Corretto in this folder: C:\Program Files\Harmonic\java.
Note: This is the download site: <https://aws.amazon.com/corretto/>
WARNING: Only use an *.MSI file, never use a *.ZIP file. The *.MSI file automatically sets the proper registry key that is required for the TOMCAT installation.
6. Verify that this folder exists: **C:\Program Files\Harmonic\java\jre8**.
7. Reboot the machine.
8. Restart the NMX Server.

Upgrading Apache Tomcat

Follow this procedure to upgrade Apache Tomcat in NMX:

When required for security updates, Apache Tomcat can be upgraded to a newer version that has been qualified with NMX by Harmonic. Please contact your Harmonic representative for the latest Tomcat version qualified with NMX.

1. Stop the XMS Gateway and Tomcat services.
On the XServer service, perform a **Stop** command. Wait until the XServer and Tomcat8 are in a Stopped state.
2. Save the following configuration and library files:
From the **C:\Program Files\Apache Software Foundation\Tomcat 8.5\conf** directory, save **server.xml** and **web.xml** in a temp directory.
From the **C:\Program Files\Apache Software Foundation\Tomcat 8.5\lib** directory, save **OrbSaver.jar** and **OrbSaver_XMS_07.00.00.020_RC.sav** in the same temp directory.

3. Uninstall the old Apache Tomcat 8.5 without suppressing the remaining files.

Open the Control Panel and begin the uninstallation process. When the following dialog box appears, click **No** to continue.

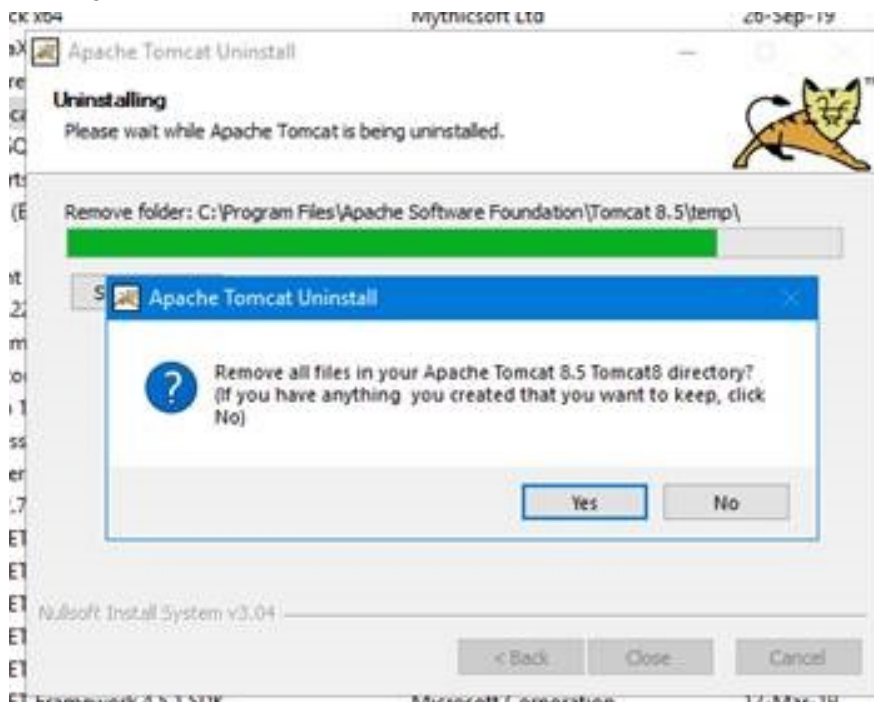


Figure 5-1: Apache Tomcat Uninstallation Warning

4. Install the new Apache Tomcat 8.5.

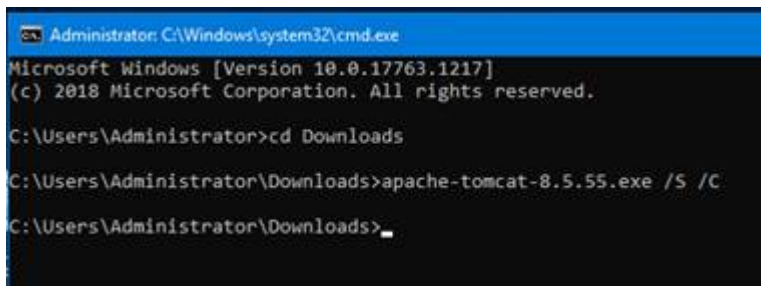


Figure 5-2: Apache Tomcat Installation

5. Copy the files you saved in step 2 to their appropriate folders in the new installation.

6. Reinstall the service with the XMS Gateway scripts.

From the **C:\Harmonic\XMS_Gateway\Scripts\Services** directory, perform the **UninstallAllService.bat** script as Administrator. Then perform the **InstallAllService** script as Administrator.

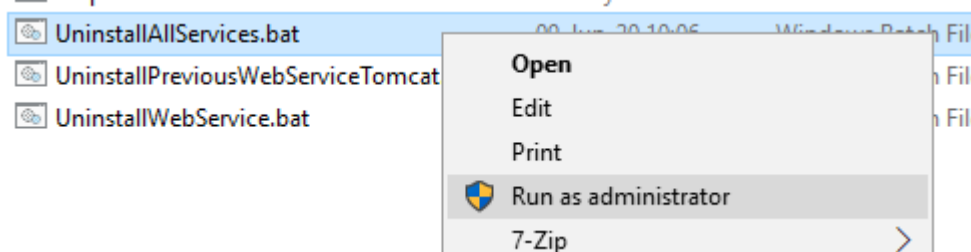


Figure 5-3: XMS Gateway UninstallAllServices.bat Installation

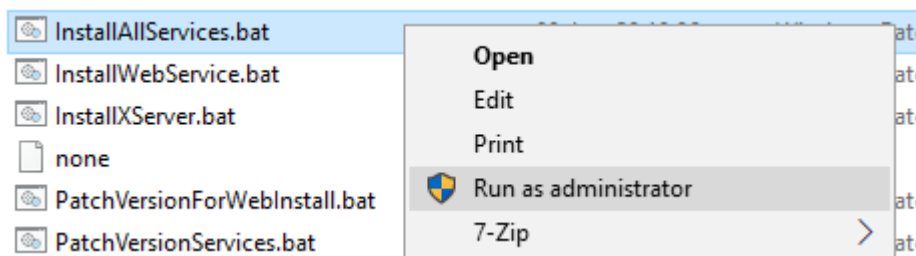


Figure 5-4: XMS Gateway InstallAllServices.bat Installation

7. Restart the XMS Gateway and Tomcat services by starting the Xserver service.

Chapter 6

Monitoring HPE Server Alarms

NMX now supports the HPE ProLiant DL360 Gen 10 server and can monitor its hardware alarms using the Integrated Lights-Out (iLO) server management processor.

The following alarms can be monitored through this configuration:

- Power failure
- Fan failure
- High temperature
- SSD failure

The process to enable HPE server alarm monitoring is made up of the procedures in this section.

- [Enabling the iLO interface](#)
- [Configuring the static IP address](#)
- [Configuring the Alarms Options](#)

Enabling the iLO interface

Follow these steps to enable the Integrated Lights-Out (iLO) server management processor:

1. Ensure that the iLO port is connected to the same switch/router where the highest priority management NIC is connected.
2. Reboot the NMX server.
3. Press **F9** to bring up System Utilities.
4. Navigate as follows: **System Utilities > System Configuration > iLO 5 Configuration Utility > Network Options**.
5. Select **ON** for the **Network Interface Adapter**.
6. Press **F10** to save.

Configuring the static IP address

This process is only required if you want to use a static IP address. Hewlett Packard recommends using dynamic IP addressing.

1. Reboot the NMX server.

2. Press **F9** to bring up System Utilities.
3. Navigate to **System Utilities > System Configuration > iLO 5 Configuration Utility > Network Options**.
4. Disable **DHCP**.
5. Enter values in the **IP Address**, **Subnet Mask**, and **Gateway IP Address** fields.
6. Press **F12** to save your changes and exit.
7. Click **OK**.
8. Start the iLO remote console.
9. Navigate to the System Configuration page.
10. Exit System Utilities and then exit the iLO Configuration Manager to resume the boot process.

Configuring the Alarms Options

Once the iLO has been configured, you can now configure NMX to monitor the HPE alarms. If NMX is running in redundancy mode there will be two sets of fields, one for the primary HPE server and another for the backup.

1. Click the **Options** button on the NMX ribbon.
2. Check the box next to **Monitor Hardware Alarms (HPE Server Only)**.
3. Enter values for the **IP Address**, **Subnet Mask**, and **Default Gateway** in the appropriate fields.
4. Click **OK** to save your changes.

Chapter 7

Troubleshooting NMX

Troubleshoot installation configuration issues, such as NMX redundancy or the NMX Bootp process after you have started the NMX Server .

- [Connecting NMX to VOS after upgrade](#)
- [NMX redundancy](#)
- [NMX Bootp process and Cisco switches](#)
- [SNMP reset](#)
- [Getting device logs](#)
- [Sending log files to Harmonic Technical Support](#)

Connecting NMX to VOS after upgrade

When the upgrade to NMX 8.5.0 is complete, the VOS SW Cluster appears in a Timeout state within the NMX Operator. The alarm "**Device timed out : Unauthorized VOS client credential**" is displayed. This short procedure will connect NMX 8.5.0 to the VOS SW Cluster.

You will need to obtain the **Client ID** and the **Secret ID** for the VOS SW Cluster to perform this procedure. Make sure you obtain them using the **Client Credential mode**; do not use the Authorization Code.

1. Go to the **NMX Designer**.
2. Open the properties for the VOS SW Cluster.
3. Enter the **VOS Client ID** and the **VOS Secret ID** in the appropriate fields.
4. Click **OK**.

NMX redundancy

There are several quick fixes to some common NMX redundancy setup and NIC issues.

- If NMX redundancy setup fails.
 - Check to make sure that the NTP server is running on both primary and backup machines, and that preferably, both machines are pointed to the same NTP server. You can point both the primary and

- backup machines to the Primary NMX IP itself. Check to make sure that **NetTime** is configured with SNTP and port 123, and that the NTP server has a valid server IP.
- Check that both the Primary and Backup server are configured with the same time and time zone; the redundancy wizard does not check for the same time zone.
 - You can save the NMX redundancy validation log files as XML files and send them for further debugging and investigation to Harmonic Technical Support.
 - If the Domain Manager GUI displays a **Replication Failed** alarm after setting up redundancy, then it could be an issue with the Network Interface Card (NIC property). Follow these steps to correct the NIC priority:
 - Change the NIC order by opening the **Control Panel > Network and Sharing Center > Change adapter settings > Connection**.
 - Right click the connection and select **Properties > TCP/IPv4 > Properties > Advanced...**
 - Uncheck the **Automatic metric** box, and then enter the desired number representing the NIC order you want in the **Interface metric** field.
 - Click **OK** to save your changes and then restart the machine.
-  **NOTE:** In Windows 2019, the NIC priority is determined using the metric value in the IPv4 settings of the adapter. NMX uses this metric value to determine the highest priority NIC. You have to configure the lowest metric value to the NMX management NIC.

To help you and Harmonic Technical Support identify any NMX issues, the DomainManager.log file is generated with any critical failures and saved to: C:\ProgramData\Harmonic\NMX\SharedFiles. Send it to Harmonic Technical Support for further debugging and investigation. NMX Bootp Process and Cisco Switches

NMX Bootp process and Cisco switches

Common NMX fixes to the Bootp process and Cisco switches.

For the NMX bootp process to complete on start up, Cisco switch interfaces must have spanning tree portfast enabled on each switch interface to which the encoders are attached.

spanning tree portfast is a command unique to Cisco switches that allows video traffic to flow through the switch first, before performing the spanning tree algorithm. With spanning tree portfast enabled, the switch will forward video traffic immediately, then check for network loops, allowing the bootp process to complete. Otherwise, the switch will check for network loops first and then start forwarding video traffic, by which time the encoder has stopped sending bootp requests.

SNMP reset

The NMX installer will reset the SNMP service permitted managers unless they have been previously configured.

The NMX installer will reset the SNMP service permitted managers to 127.0.0.1 if they are not already configured. This change was necessary to harden the NMX server security by restricting SNMP service exposure. If the SNMP service permitted managers have been reset, you will need to configure the

permitted managers to allow external SNMP managers to communicate with the SNMP service running on the NMX server. The permitted managers can be viewed and/or changed from the following location:

```
services.msc > SNMP Service Properties > Security tab > Accept SNMP packets  
from these hosts
```

Getting device logs

Get devices logs from the shortcut menu in NMX Operator.

1. From the NMX Operator **Home** page, right-click the device and select **Get Device Logs**. It could 1-2 minutes for the logs to generate.
2. Save the logs to your local computer.
3. Send the logs to Harmonic technical support.

Sending log files to Harmonic Technical Support

Export, save, then send log files concerning your network issue to Harmonic Technical Support.

- For critical failures, the DomainManager.log file is generated and saved to: C:\ProgramData\Harmonic\NMX\SharedFiles
- To export and send alarms logs (as .xml files) to Harmonic Technical Support, go to **NMX Operator > Dashboard > Export Logs**. Click **Export Logs**, specify the package type and destination, and click **Generate**.
- If your backup configuration validation fails, go to: **NMX Domain Manager > Server Fail Safe tab > Validate Backup Configuration**. Click **Save** to save the redundancy validation log files as .xml files. Then, send them to NMX Technical Support.
- To view the last 10,000 actions of all users and system operations, go to: **NMX Domain Manager > Home tab > Audit Log > Audit Log View**. Click a column to sort the data, or click **Save** to save the data as a .csv file.

Appendix A

Harmonic Technical Assistance Center contact information

A list of phone numbers, e-mail addresses, and important links for the Harmonic Technical Assistance Center (TAC).

Table A-1: Harmonic Technical Assistance Center phone numbers and email addresses

Region	Telephone Technical Support	Email
Americas	888.673.4896 (888.MPEG.TWO) 408.490.6477	support@harmonicinc.com
Europe, the Middle East and Africa (EMEA)	+44.1252.555.450	emeasupport@harmonicinc.com
India	+91.120.498.3199	apacsupport@harmonicinc.com
Russia	+7.495.926.4608	rusupport@harmonicinc.com
China	+86.10 5798.2626	chinasupport@harmonicinc.com
Japan	+81.3.5614.0524	japansupport@harmonicinc.com
Asia Pacific (APAC) – Other Territories	+852.3184.0045 +65.6542.0050	apacsupport@harmonicinc.com

Support URLs

Report an Issue Online: <https://www.harmonicinc.com/technical-support/report-issue/>

Technical Support: <https://www.harmonicinc.com/technical-support/>

Software download location for Cable Edge products

<ftp://ftp.harmonicinc.com>

Contact Harmonic Technical Publications

techdocs@harmonicinc.com

- [Harmonic corporate contact information](#)

Harmonic corporate contact information

Phone numbers and addresses for the corporate office.

Harmonic corporate address

2590 Orchard Parkway
San Jose, CA 95131
U.S.A.

Harmonic corporate telephone numbers

Tel. 1.800.788.1330 (from the U.S. and Canada)
Tel. +1.408.542.2500 (outside the U.S. and Canada)
Fax. +1.408.542.2511

