

# Vitreau® Advanced Visualization

## Enterprise Upgrade Supplemental Information Guide



VPMC-17431 B

# Legal and Regulatory Information

Copyright © 1997 -2025 Canon Medical Systems Corporation. All rights reserved. Date of Publication: 2025-04

**REF** VPMC-17431 B Enterprise Upgrade Supplemental Information Guide

This publication is valid for:

**MD** Vitrea® Advanced Visualization and **#** 7.16.2.SU01 and later software versions.

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system without permission in writing from Canon Medical.

## Trademarks

Vitrea is a registered trademark in the United States and may have protection in other countries. All other marks are property of their respective owners.

## Restricted Rights Legend

If this software or documentation is delivered to the Department of Defense (DoD) of the U.S. Government, it is delivered with Restricted Rights as follows: Use, duplication or disclosure of the software by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

If this software or documentation is delivered to any unit or agency of the U.S. Government other than DoD, it is delivered with Restricted Rights and use, duplication or disclosure by the U.S. Government is subject to the restrictions as set forth in FAR 52.227-19 (b)(3). If the software or documentation is delivered to NASA, it is delivered with Restricted Rights subject to the restrictions set forth in 18-52.227-86(d) of the NASA FAR Supplement.

## Limits of Liability and Disclaimer of Warranty

CANON MEDICAL SHALL HAVE NO LIABILITY OF ANY KIND FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES BASED ON ANY DEFECT, FAILURE OR MALFUNCTION OF THE SOFTWARE, OR USE OF ANY CANON MEDICAL DOCUMENTATION, WHETHER THE CLAIM IS BASED UPON WARRANTY, CONTRACT, TORT OR OTHERWISE. CANON MEDICAL MAKES NO WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WHETHER ARISING FROM STATUTE, COMMON LAW, CUSTOM OR OTHERWISE.

## Notice of Confidentiality

This software and the information in this software including, but not limited to, the ideas, concepts and know-how are proprietary, confidential and trade secret to Canon Medical, and the information contained therein shall be maintained as proprietary, confidential and trade secret to Canon Medical and shall not be copied or reproduced in any form whatsoever. This software and any information contained therein shall not be disclosed to anyone other than authorized representatives of the user's employer, who is contractually obligated not to disclose same without the express written consent of Canon Medical. The user of this software and any information contained therein shall not attempt to discern Canon Medical's confidential and trade secret information and shall not reverse compile, disassemble, or otherwise reverse engineer this software or any information contained therein.

## Software License Notice

This software is a licensed product of and is distributed by Canon Medical, and may only be used according to the terms of that license on the system identified in the applicable Software License Agreement. In the event of any conflict between these terms and the terms of any written agreement or agreement assented to through electronic means with Canon Medical, the terms of such written or assented agreement shall control.

CE 2797

**EC** **REP**

MDSS GmbH  
Schiffgraben 41  
30175 Hannover, Germany

**Australian Sponsor:**

Canon Medical Systems ANZ Pty Limited  
Unit 1, Building 16, Showground Business Park, 12-20 Anella Avenue, Castle Hill NSW 2154  
Australia

Vitrea: ARTG 466648



Canon Medical Systems ANZ Pty Limited is the authorized sponsor in Australia and acts on behalf of Canon Medical Informatics, Inc. in the communication of safety-related incidents and regulatory matters with Therapeutic Goods Administration in Australia. Distributors are still the first line of communication with their customers regarding service and complaints.

**Brazil Importer and Distributor:**

Canon Medical System do Brasil  
Avenida Ceci, 328, Tamboré,  
Barueri/SP  
Brasil

ANVISA registration number: 10295030090



**Canada Importer and Distributor:**

Canon Medical Systems Canada LTD  
75 Tiverton Court  
Markham, ON Canada L3R 4M8



**European Importer and Distributor:**

Canon Medical Systems Europe B.V.  
Bovenkerkerweg 59, 1185 XB Amstelveen  
The Netherlands



**Ukraine Authorized Representative:**

Representative office Canon Medical Systems B.V.  
Mechnikova str.2. Letter A, Kyiv, 01601, Ukraine



**UK Responsible Person:**

Canon Medical Systems Limited  
Boundary Court, Gatwick Road  
Crawley, RH10 9AX United Kingdom



## India:

Imported by: M/s. Erbis Engineering Co. Ltd., 39, Second Main Road, Raja Annamalaipuram, Chennai-600028  
Name of Manufacturer & ADDRESS: Canon Medical Informatics, Inc.; 5850 Opus Parkway, Suite 300; Minnetonka, MN, US; 55343

Manufacturing Date: see "Date of Publication"

Expiry Date: N.A.

Voluntary Registration No: M/s. C-USA/I/MD/007892

Batch No: N.A.



## Switzerland:



Canon Medical Systems AG/SA  
Richtistrasse 9, 8304 Wallisellen  
Switzerland



## Contact Us:

Any serious incident that has occurred in relation to the device should be reported to Canon Medical at 1.800.208.3005 and the competent authority of the Member State in which the user and/or patient is established. See [mi.medical.canon/contact-us](https://mi.medical.canon/contact-us) for more detailed contact information.



Manufactured by: Canon Medical Informatics, Inc.; 5850 Opus Parkway, Suite 300; Minnetonka, MN, USA; 55343; Phone 866.433.4624

# Safety and Regulatory Considerations

PLEASE REFER TO THE *ABOUT VITREA MEDICAL IMAGING SOFTWARE* DOCUMENT BEFORE USING THIS PRODUCT. This document includes important information regarding general Vitrea Safety and Regulatory considerations.



## CAUTION

Federal law restricts this device to sale by or on the order of a physician, as directed by 21 CFR 801.109(b)(1).



## NOTE


While every effort has been made to ensure the accuracy of the content in this document, you may notice slight differences between screen captures and the actual software interface.

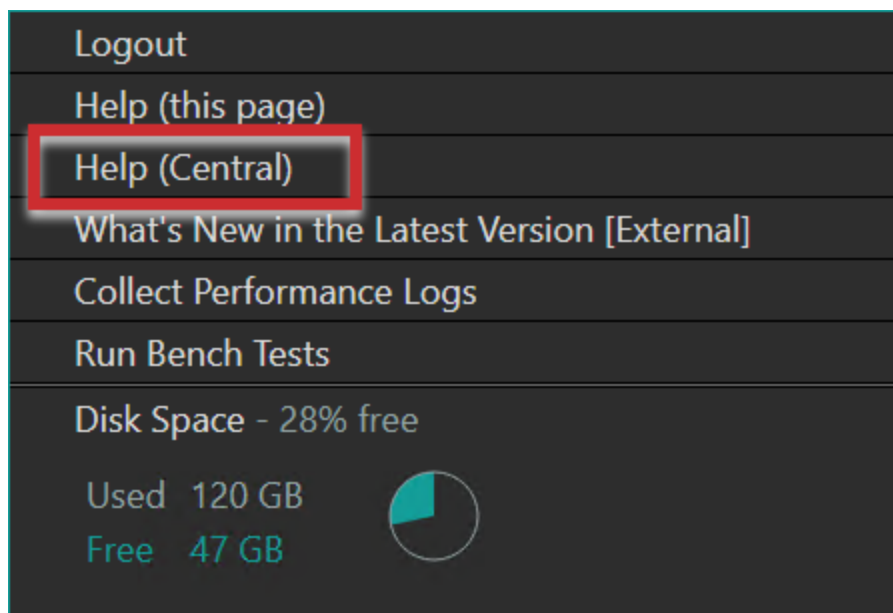
# Contact Us

- For general, non-technical support questions, contact us through our website: [mi.medical.canon](https://mi.medical.canon).
- For customer technical support, contact us:
  - In the U.S., call the Customer Support line at 1.800.208.3005.
  - Outside the U.S., contact your distributor.
  - Send an email to [support@mi.medical.canon](mailto:support@mi.medical.canon).
- For a printed version of the Release Notes, Education and Reference Guide, or Installation Guides, contact Customer Support at 1.800.208.3005.

# UDI

Locate the Vitrea unique device identifier (UDI) on the Help Central page. This identifier contains the software version information and manufacture date.

1. Click  at the top of the window to display the Global Options menu.
2. Select **Help (Central)**.



The UDI is displayed under the **Version Info** section.

## Release Notes

Vitrear Release Notes contain late-breaking information not available at the time the Education and Reference Guide was released. This document is available from your system administrator or from Canon Medical.

Canon Medical offers a full range of diagnostic medical imaging solutions including CT, X-Ray, Ultrasound, Vascular and MR, as well as a full suite of Healthcare IT solutions, across the globe. To support a unified business approach, Vital Images has adopted the Canon Medical brand, and will leverage Canon Medical's global infrastructure and broaden its capabilities to accelerate the delivery of a full range of Enterprise, AI, and Collaborative imaging solutions. In line with our continued Made for Life philosophy, patients are at the heart of everything we do. Our mission is to provide medical professionals with solutions that support their efforts in contributing to the health and wellbeing of patients worldwide. Our goal is to deliver optimum health opportunities for patients through uncompromised performance, comfort and safety features.

Canon Medical Informatics, Inc.

5850 Opus Parkway, Suite 300 | Minnetonka, MN 55343, USA | + 1 866.433.4624

# Contents

Legal and Regulatory Information .....	2
Safety and Regulatory Considerations .....	5
Contact Us .....	5
UDI .....	5
Release Notes .....	6
Overview .....	8
Intended Audience .....	8
Appendix A: TLS Digital Certificate Request details .....	9
Review IIS Settings on the Management Server .....	14
Appendix B: Configure Group Policy Object Settings .....	16
Review Group Policy .....	22
Appendix C: Graphics Card Drivers and Windows Updates .....	23
Install Video Drivers - all video cards .....	23
Install Video Drivers for vGPU-driven Application Servers .....	31
Verify GPU Data Center Graphics Cards .....	31
Install Microsoft Windows Updates .....	34
Appendix D: Specific Antivirus exclusions .....	35
Anti malware Exclusions .....	39
Appendix E: Run the System Hardening Script .....	41
Run the System Hardening Script on the Management Server .....	41
Run the System Hardening Script on the Application Server .....	43
System Hardening Script Settings .....	44
Vitrear System Checker Script and Reporting .....	48
Appendix F: VMware Procedures .....	50
Verify EVC is enabled .....	50
Configure the vCPU cores on the system .....	51

# Overview

This document describes supplemental information you may need to complete a Vitrea Enterprise upgrade at a customer site location. This document is designed to be used with the Enterprise Deployment Upgrade Spreadsheet by Canon Medical Professional Services personnel and by customer site personnel.

The content included in this document has been leveraged from other existing planning, setup and upgrade guides. The source guide will be noted within each appendix.

# Intended Audience

This document is intended for people who want to complete an Enterprise deployment upgrade. Canon Medical assumes you know how to complete a standard installation process and have a basic understanding of Windows Operating Systems.



# Appendix A: TLS Digital Certificate Request details



## NOTE

The content listed below is part of the **Enterprise Deployment Active Directory Planning Guide**.

This appendix explains information about digital certificate requirements.

A digital certificate is required for your deployment. Based on the numbers of servers in your deployment, you will need at least one of the following certificate types:

- a digital certificate
  - for a single server deployment
  - for each individual server in a small Enterprise deployments
- A SAN certificate. This is a certificate with the Fully Qualified Domain Name (FQDN) for all the Vitrea servers (and the SQL Server if remote) listed in the Subject Alternative Name. **NOTE:** A SAN certificate can only be utilized if the following specific conditions are true:
  - If SQL communications are encrypted, the certificate being used by SQL (which may be running on a Vitrea server) must have a Common Name (CN) that matches the FQDN of the machine where SQL is running. For more information, refer to the [Certificate requirements for SQL Server](#) article. Specific guidance is listed below.
  - The Subject property of the certificate must indicate that the common name (CN) is the same as the host name or fully qualified domain name (FQDN) of the server computer. When you use the host name, the DNS suffix must be specified in the certificate. If SQL Server is running on a failover cluster, the common name must match the host name or FQDN of the virtual server, and the certificates must be provisioned on all nodes in the failover cluster. For example, if you have a two-node cluster, with nodes named test1.<your company>.com and test2.<your company>.com, and you have a virtual server named virtsql, you need to install a certificate for virtsql.<your company>.com on both nodes.
- a wild card certificate (for unlimited hosts or for large customer deployments). For more information about using a wildcard certificate thumbprint with SQL Server, refer to the following article: <https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-ver16>

## Deployment Examples

- Scenario One - one Management Server, remote SQL Server, and 10 Application Servers, you could have one wildcard certificate that is used for the Vitrea Servers and the SQL Server (if using Server 2019). If the SQL Server is older than 2019, you would use a second digital certificate with the **At\_KEYEXCHANGE** property.
- Scenario Two - one Management Server, on-box SQL Server, less than five Application Servers, you could have one SAN certificate for all machines.
- Scenario Three - one Management Server, on-box SQL Server, and one Application Server, you could have one digital certificate for the Management Server and one digital certificate for the Application Server.
- Scenario Four - one Enterprise Single Server with PACS integration, you could have one digital certificate.

Listed below are the digital certificates you may need for an Enterprise deployment.

Digital Certificate	Description
SQL Communication	<p>This digital certificate is used for encrypting SQL communication between the SQL Server database and the Application Servers.</p> <p>Review the following articles to learn how to set up SQL with a certificate:</p> <ul style="list-style-type: none"> <li>• <a href="https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/ad-fs-and-keyspec-property">https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/ad-fs-and-keyspec-property</a>.</li> <li>• <a href="https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-ver16">https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-ver16</a></li> </ul> <p>For SQL Server 2017, you need to create a digital certificate with the <b>At_KEYEXCHANGE</b> property. SQL Server 2019 or newer does not require the <b>At_KEYEXCHANGE</b> property.</p> <p>You will need to create a .PFX file from your original digital certificate and then run the following command to add the <b>At_KEYEXCHANGE</b> property to the certificate.</p> <pre>certutil -importpfx certfile.pfx AT_KEYEXCHANGE</pre> <p>When creating a CA certificate:</p> <ul style="list-style-type: none"> <li>• If you have issues in adding the <b>At_KEYEXCHANGE</b> property, you must set the template compatibility to Windows 2003.</li> <li>• When you request a certificate, select the key exchange.</li> </ul> <p>If you need to add the key exchange to the certificate:</p> <ul style="list-style-type: none"> <li>• You must add <b>-KeySpec KeyExchange</b> in the PowerShell command.</li> <li>• The Subject Alternate Name should include all the names of your Management Server and Vitrea Application Servers or Multi Modality Viewer Servers used to connect to a SQL Server instance.</li> </ul>
PACS Integration	<p>This digital certificate on the Management Server is used for PACS-integrated launches.</p>
Vitrear Application Communication	<p>This digital certificate on the Vitrea servers is used for IIS/APIs.</p>
Remote Desktop/RDWeb/Remote Desktop Connection Broker	<p>If the customer wants to replace the digital certificate Microsoft creates when loading the Windows Remote Feature, they must provide another digital certificate or the certificate for the Management Server can be used by exporting to a .PFX file..</p>
Mevis LungCAD	<p>If Mevis LungCAD is installed on the Management Server, an additional certificate is not required. If the Mevis LungCAD product is installed on a separate server you need a digital certificate for the Mevis LungCAD product.</p>

SAN Certificate	Description
SQL Communication	<ul style="list-style-type: none"> <li>If SQL is Local on the Management Server, the same digital certificate can be used for SQL. For SQL Server 2017, you need to create a digital certificate with the <b>At_KEYEXCHANGE</b> property.</li> <li>If SQL is Remote a separate digital certificate is required. For SQL Server 2017, you need to create a digital certificate with the <b>At_KEYEXCHANGE</b> property.</li> </ul> <p>Follow the Microsoft SQL Certificate requirements as described in this article: <a href="https://learn.microsoft.com/en-us/sql/database-">https://learn.microsoft.com/en-us/sql/database-</a></p> <p>The Subject Alternate Name should include all the names of your Management Server and Vitrea Application Servers or Multi Modality Viewer Servers used to connect to a SQL Server instance.</p>
PACS Integration	<p>The FQDN of the Management Server and the Subject Alternative Name of the Application Servers or Multi Modality Viewer Servers.</p> <p><b>NOTE:</b> SAN Certificates can be multi-domain. example.com and example.net</p>
Vitrear Application Communication	The certificate with the FQDN of the Management Server and the Subject Alternative Name of the Application Servers or Multi Modality Viewer Servers is applied.
Remote Desktop/RDWeb/Remote Desktop Connection Broker	If the customer wants to replace the digital certificate Microsoft creates when loading the Windows Remote Feature, they must provide another digital certificate or the certificate for the Management Server can be used by exporting to a .PFX file.
Mevis LungCAD	If Mevis LungCAD is installed on the Management Server, an additional certificate is not required. If the Mevis LungCAD product is installed on a separate server you need a digital certificate for the Mevis LungCAD product.
Wildcard Certificate	Description
SQL Communication	<ul style="list-style-type: none"> <li>For SQL Server 2019 or higher the same wild card certificate can be used for SQL.</li> <li>For SQL Server 2017, a separate digital certificate with the <b>At_KEYEXCHANGE</b> property is required.</li> </ul> <p>Follow the Microsoft SQL Certificate requirements as described in this article: <a href="https://learn.microsoft.com/en-us/sql/database-">https://learn.microsoft.com/en-us/sql/database-</a></p>
PACS Integration	<p>The FQDN of the Management Server and the Subject Alternative Name of the Application Servers or Multi Modality Viewer Servers.</p> <p><b>NOTE:</b> SAN Certificates can be multi-domain. example.com and example.net</p>

Wildcard Certificate	Description
Vitrear Application Communication	The wild card certificate can be used for the Management Server, Application Servers, and Multi Modality Viewer Servers.
Remote Desktop/RDWeb/Remote Desktop Connection Broker	If the customer wants to replace the digital certificate Microsoft creates when loading the Windows Remote Feature, they must provide another digital certificate or the certificate for the Management Server can be used by exporting to a .PFX file.
Mevis LungCAD	If Mevis LungCAD is installed on the Management Server, an additional certificate is not required. If the Mevis LungCAD product is installed on a separate server you need a digital certificate for the Mevis LungCAD product.

## SSL/TLS Certificate Requirements

Canon Medical recommends digital certificates adhere to the following requirements:

- If a .pfx file is used, it is required that the private key be set
- The certificate must be signed using a SHA256 or better signature hash algorithm
- 2048-bit or greater RSA key or a 256-bit or greater Elliptic Curve Cryptography (ECC) key
- The server must support TLS version 1.2
- The certificate's Subject Alternative Name(s) include(s) the Vitrear server(s) unless a Wild Card cert is used.
- A 1-year digital certificate
- For deployments with Test environments, Disaster Recovery environments, etc., each deployment must have its own digital certificate
- Wildcard digital certificates are acceptable; these currently cannot be used for SQL Server 2017
- Self-signed certificates are not supported. Canon Medical requires a digital certificate generated by an internal CA (Certificate Authority), or from a third party (such as Digicert, Thawte, etc.)
- If users from greater than one Active Directory Domain need to authenticate to the system, a SAN digital certificate is required and any domains must be listed in the Subject Alternative Name field

## Obtain an SSL/TLS Certificate - COMPLETED BY CUSTOMER

You must obtain a valid SSL/TLS certificate. If this is a public facing device for use on the Internet, a certificate from Thawte or Verisign is recommended; otherwise, manually install the certificate in the client browser.

### 1. Choose a Certificate Authority (CA)

Thawte and VeriSign are commonly used vendors of SSL/TLS certificates. If your company has its own Certificate Authority, that can be used as well.

## 2. Generate a Server Key

The server key is required to generate the Certificate Signing Request that is submitted to the Certificate Authority. Each server key generated is unique. The key should be backed up to a secure location. If the key is lost a new certificate will have to be obtained. This key must be kept private. When generating a Server key from your company Certificate Authority, the certificate should have the Intended Purpose of Server Authentication. If this is not included, the digital certificate will not function.

## 3. Generate a Certificate Signing Request (CSR)

Generate a Certificate Signing Request (CSR) using the server on which the SSL/TLS certificate will be installed. The contents of the CSR file are needed when applying for the SSL/TLS certificate. It is critical that the information in the CSR exactly matches the information in the Proof of Right. The most common Proof of Right document is the Articles of Incorporation. As part of the CSR, the server's "Common Name" (CN) must be entered. The CN is the fully qualified hostname of the server.

For instance:

<https://vitrea.myhospital.com>, the Common Name will be [vitrea.myhospital.com](https://vitrea.myhospital.com)



### NOTE

- Do **not** include the <https://> at the beginning of the Common Name.
- As part of the certificate request, you should include any Subject Alternative Name for the Management Server and the Application Servers.

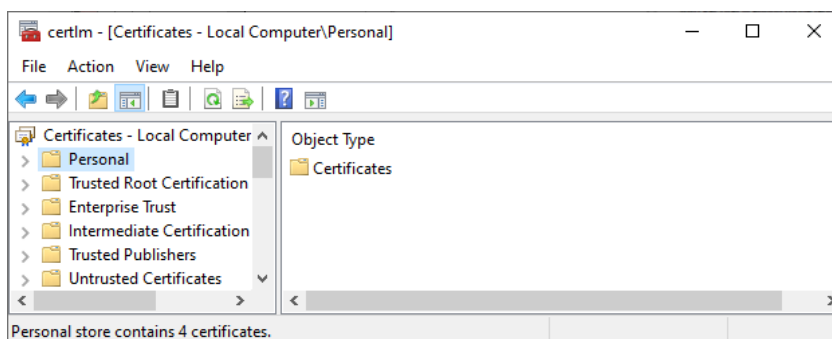
## 4. Purchase your digital certificate from an authorized vendor or generate your certificates from your private CA and include the certificate authority trust chain.

## 5. Apply for the SSL/TLS Certificate

Follow the instructions on the vendor's website to apply for the SSL/TLS certificate. Canon Medical recommends purchasing a 1-year certificate. Information on certificate renewal is provided by the Certificate Authority.

## 6. Install the SSL/TLS Certificate

Install the SSL/TLS certificate on the Management Server, Application Server(s), and SQL Server in the **Personal Digital Repository** location. Perform tests to verify that a user outside the enterprise network can access the Vitrea software.

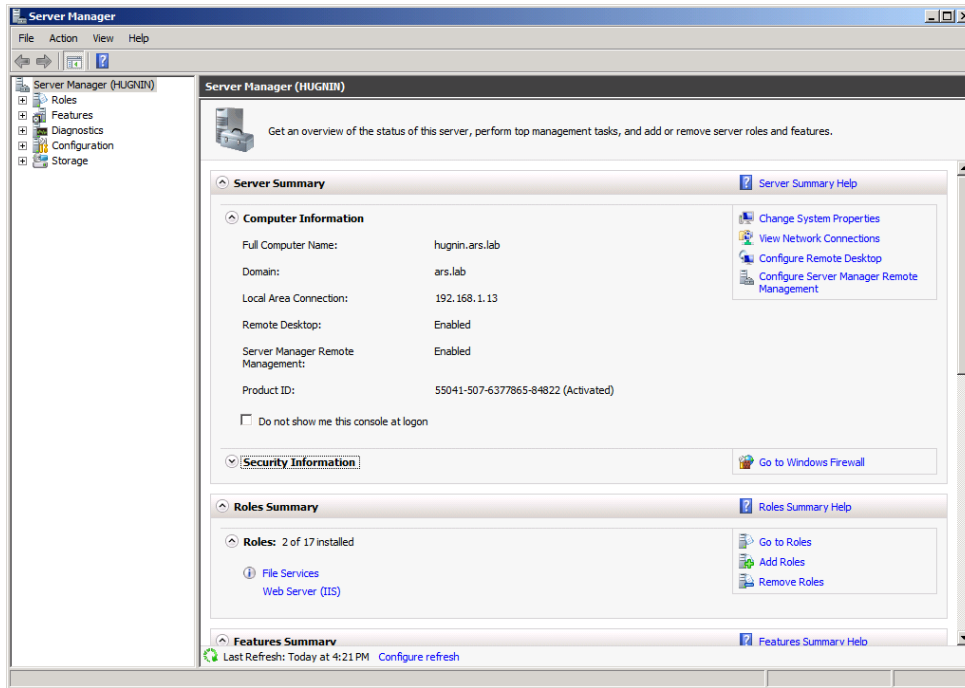


# Review IIS Settings on the Management Server

It has been found that upgrading Vitrea AV can cause Internet Information Services (IIS) certificates and SSL bindings to be removed upon upgrade.

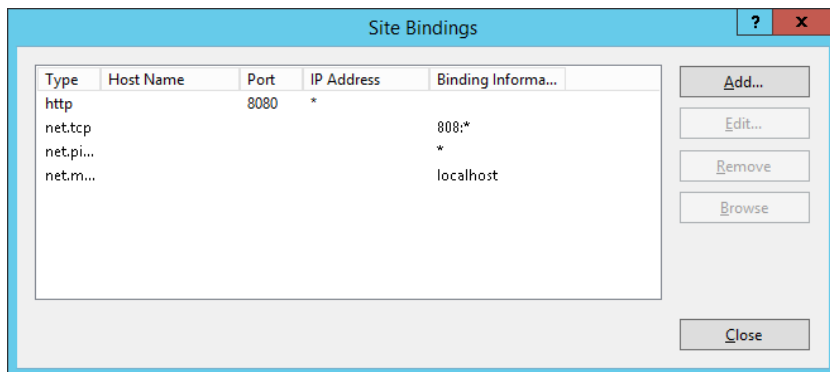
Complete the steps below to review the IIS site bindings for the TLS Digital Certificate being used.

1. Select the **Server Manager** icon on the **Windows Taskbar**.



2. In the left pane, expand **Roles** and **Web Server**.
3. Select **Internet Information Services (IIS) Manager**.
4. Select the server name in the left pane.
5. Expand the **Sites** folder and select the **Default Web Site** option.
6. In the **Actions** pane, select **Bindings**.

The following screen displays.



7. If https is present, select it and click the **Edit** button.
8. Review the certificate being used.
9. Click the **Close** button.
10. Save a copy of the digital certificate to a safe location.



#### NOTE

- After you complete the upgrade, sites that utilize these IIS settings for functionality such as RDWeb must reestablish their IIS certificates and SSL bindings on the Management Server to reestablish any functionality that relies on IIS. Please plan appropriately to have these settings recreated on the Management Server after you upgrade Vitrea AV.
- After you complete the upgrade, remove the digital certificate from the saved location. Do not leave it in the general file section.

# Appendix B: Configure Group Policy Object Settings



## NOTE

The content listed below is part of the **Enterprise Deployment Active Directory Planning Guide**.

This appendix describes the group policy object settings you will configure at a customer site for Vitrea enterprise deployments.

The policy objects are examples and the underlying policies can be applied in other ways if desired. Apply them to the desired domain in your organization.

## Apply Group Policy Object for the Vitrea Application Servers

Described below are two methods you can perform to apply the server role-specific VitreaAppGPO Group Policy Object required for Application Servers.

Method One: Active Directory Integration for the Application Server policy

Domain Administrators complete the steps below to retrieve the Application Server GPO templates from the Vitrea installation media.

1. Navigate to the **Vitrea\_Resources \{media content\}Utilities\OS Configuration Scripts\GPOs\Application** directory location.
2. Import the contents of the **VitreaAppGPO** folder and link the Group Policy Object to the OU governing the Vitrea Application Servers.
3. Restart the member servers corresponding to the Vitrea Application Servers' OU.

Method Two: Locally import the Application Server policy

Server Administrators complete the steps below to manually import the **VitreaAppGPO** via the **Vitrea\_ImportGPOScript.ps1** script.

1. Click the **Start** button and type `PowerShell`.
2. Right-click **Windows PowerShell** and select **Run as administrator**.
3. Change your directory prompt to the **Vitrea\_Resources\{media content\}Utilities\OS Configuration Scripts\GPOs** folder.
4. Type `".\Vitrea_ImportGPOScript.ps1"` and press **Enter**.

```
PS C:\> cd "E:\Vitrea_Resources\Vitrea-7.x.x.x\Utilities\OS Configuration Scripts\GPOs"
PS E:\Vitrea_Resources\Vitrea-7.x.x.x\Utilities\OS Configuration Scripts\GPOs> .\Vitrea_GPOImportScript.ps1
```

5. Type `"L"` (this selects the LocalServerRoleGPO) and press **Enter**.



```
Type of installation
FOR THIS RELEASE, USE ONLY THE [R]Reset GPO OR [L]Local Server Role GPO OPTIONS WHEN MANUALLY EXECUTING THIS SCRIPT
[E] Extend [M] Management [A] Application [G] GovernmentDeployment [S] EnterpriseSingleServer [R] ResetGPO
[L] LocalServerRoleGPO[?] Help (default is "L"): L
```

- Type "A" (this selects the ApplicationLocal) and press **Enter**.

```
Type of Server Role GPO
Select a specific Server Role GPO
[E] ExtendLocal [M] ManagementLocal [A] ApplicationLocal [S] EnterpriseSingleServerLocal [?] Help
(default is "S"):A
```

The **Vitrear\_ImportGPOScript.ps1** script executes successfully importing the server role Group Policy Object and prompts you to restart.

```
Confirm
Are you sure you want to perform this action?
Performing the operation "Enable the Local shutdown access rights and restart the computer." on target "localhost
(TEST--2019-MGT2)".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

- Type "Y" and press **Enter**.

The system restarts and you return to the OS login entry.

## Reset server role Group Policy Object - Optional Procedure

Troubleshooting Vitrea may require resetting the local server role policies. The method described below resets all local policies configured by the Vitrea installation except the Common local policies.

Complete the steps below to manually reset the local server role policies via the **Vitrear\_ImportGPOScript.ps1**.

- Click the **Start** button and type PowerShell.
- Right-click **Windows PowerShell** and select **Run as administrator**.
- Change your directory prompt to the **Vitrear\_Resources\{media content}\Utilities\OS Configuration Scripts\GPOs** folder.
- Type ".\Vitrear\_ImportGPOScript.ps1" and press **Enter**.

```
PS C:\> cd "E:\Vitrear_Resources\Vitrear-7.x.x.x\Utilities\OS Configuration Scripts\GPOs"
PS E:\Vitrear_Resources\Vitrear-7.x.x.x\Utilities\OS Configuration Scripts\GPOs> .\Vitrear_GPOImportScript.ps1
```

- Type "R" (this selects ResetsGPO) and press **Enter**.

```
Type of installation
FOR THIS RELEASE, USE ONLY THE [R]Reset GPO OR [L]Local Server Role GPO OPTIONS WHEN MANUALLY EXECUTING THIS SCRIPT
[E] Extend [M] Management [A] Application [G] GovernmentDeployment [S] EnterpriseSingleServer [R] ResetGPO
[L] LocalServerRoleGPO[?] Help (default is "L"): R
```

The **Vitrear\_ImportGPOScript.ps1** script executes successfully resetting the server role policies and prompts user to restart

```
Confirm
Are you sure you want to perform this action?
Performing the operation "Enable the Local shutdown access rights and restart the computer." on target "localhost
(TEST--2019-MGT2)".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

- Type "Y" and press **Enter**.

The system restarts and you return to the OS login entry.

## Required User Rights Assignment Policies



### NOTE

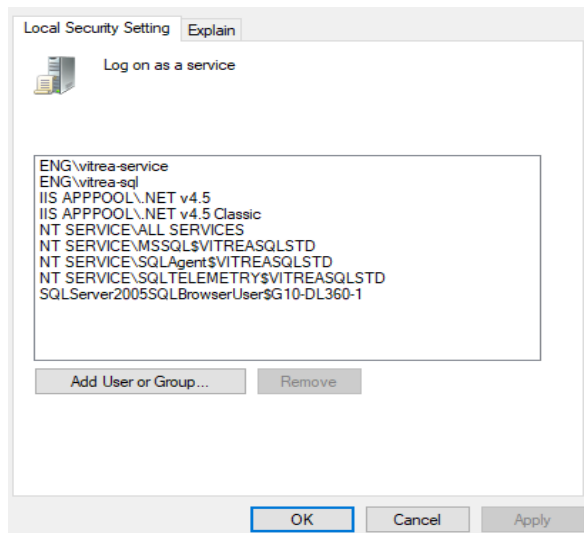
Do not remove the **Vitrea-Service** account from the policies listed below.

Listed below are local or domain group policies which must remain configured on your Vitrea Enterprise system.

### User Rights Assignments - Local Policies

The user rights assignment policies are automatically installed by the Vitrea installer.

1. To access the policies, right-click the **Start** button, select **Run** and type `gpedit.msc`.
2. Navigate to the **Local Computer Policy | Computer Configuration | Windows Settings | Security Settings | Local Policy | User Rights Assignment** directory.
3. Review the policies to ensure the **Vitrea-Service** account and the **IIS\_IUSRS** group are assigned to the "Log on as Batch" security policy.
4. Review the policies to ensure the **Vitrea-Service** account, the SQL service account (if installed locally), the **IIS APPPOOL** account(s), and other service accounts (such as those listed in the image below) are assigned to the "Log on as a Service" security policy. **NOTE:** In the image shown below, the **Vitrea-Service** account is not listed.



### NOTE

You will see other groups and/or users that are assigned to each security policy.

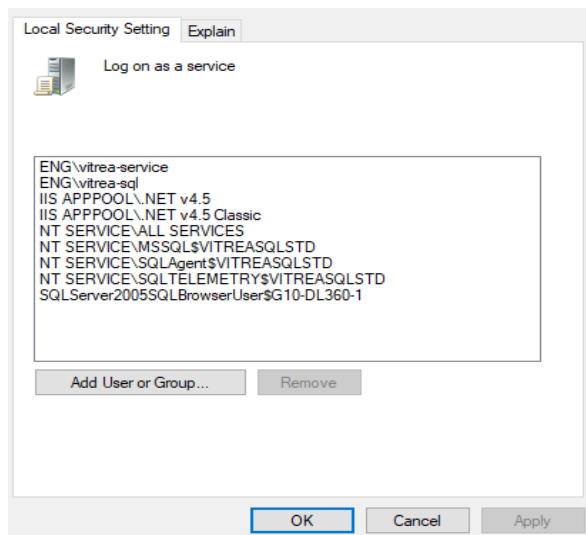
For troubleshooting purposes, access the "Debug Programs" security policy in the **Local Computer Policy | Computer Configuration | Windows Settings | Security Settings | Local Policy | User Rights Assignment** directory.

Some sites may wish to configure additional security policies such as "Deny log on as batch" security policy or "Deny log on as a service" security policy for their Enterprise Admins Group and Domain Admins Group. This is a supported configuration.

## User Rights Assignments - Domain Policies

The user rights assignment policies are automatically installed by the Vitrea installer.

1. To access the policies, select the **Start** button, select **Server Manager | Tools | Group Policy Management**.
2. Browse to your Group Policy Object and select **Edit**.
3. Navigate to the **Computer Configuration | Windows Settings | Security Settings | Local Policy | User Rights Assignment** directory.
4. Review the policies to ensure the **Vitrear-Service** account and the **IIS\_IUSRS** group are assigned to the "Log on as Batch" security policy.
5. Review the policies to ensure the **Vitrear-Service** account, the SQL service account (if installed locally), the **IIS APPPOOL** account(s), and other service accounts (such as those listed in the image below) are assigned to the "Log on as a Service" security policy. **NOTE:** In the image shown below, the **Vitrear-Service** account is not listed.



### NOTE

You will see other groups and/or users that are assigned to each security policy.

For troubleshooting purposes, access the "Debug Programs" security policy in the **Computer Configuration | Windows Settings | Security Settings | Local Policy | User Rights Assignment** directory.

Some sites may wish to configure additional security policies such as "Deny log on as batch" security policy or "Deny log on as a service" security policy for their Enterprise Admins Group and Domain Admins Group. This is a supported configuration.

## Configure Group Policy Settings for User Policies on Application Servers

### Configure Windows Settings

Complete this procedure to ensure the user profiles are created properly on each Application Server.

This procedure helps to force the internet zone settings every time the Application Server is used.

1. Right-click the **Start** button and enter `gpedit.msc` in the **Search programs and files** field.
2. Expand **User Configuration | Preferences | Windows Settings | Registry**.
3. Right-click **Registry** and select **New | Registry Item**.
4. On the New Registry Properties screen, verify the **Action** drop down menu, and select **Update**.
5. In the **Hive** field, enter `HKEY_CURRENT_USER`.
6. In the **Key Path** field, enter  
`Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap`.
7. In the **Value name** field, enter `IEHarden`
8. In the **Value type** field, enter `REG_DWORD`
9. In the **Value data** field, enter `0`
10. Select the **Decimal** radio button.
11. Access the **Administrative Tools** screen, right-click the **Application Server** subunit, and select **Link an Existing GPO**.

## Configure Group Policy Settings on Thin Client Computers

Group Policy Setting	Value	Rationale
<b>Computer Configuration   Administrative Templates   Windows Components   Remote Desktop Services   Remote Desktop Session Host   Device and Resource Redirection   Do not allow direct redirection</b>	<b>Enabled</b>	Allow the remotely logged on user to access local (client) drives on their own (client) computer, from within the remote session.

## Disable Thin Client Local Drive Access feature (Optional Procedure)

Group Policy Setting	Value	Rationale
Computer Configuration   Administrative Templates   Windows Components   Remote Desktop Services   Remote Desktop Session Host   Device and Resource Redirection   Do not allow drive redirection	Enabled	Specify whether to prevent the mapping of client drives in a Remote Desktop Services session.

## Enable Configure Save to Media functionality (Optional Procedure)

Group Policy Setting	Value	Rationale
Computer Configuration   Administrative Templates   Windows Components   Remote Desktop Services   Remote Desktop Session Host   Device and Resource Redirection   Do not allow drive redirection	Disabled or Not configured	Enable the Save to Media functionality that allows you to save .STL files and other evidence to your client machine.

## Configure Group Policy Settings for Printing on the Application Servers

### Configure Deployed Printers

Complete this procedure to ensure printing services are available within the application on Application Servers.

1. Access the Vitrea Application Server GPO and add the Print and Document Services Role.
2. Access the Print Management screen, select **Print Servers** in the left pane and select **ServerName (local) | Printers**.
3. Right-click on the printer to deploy and select **Manage Sharing**.
4. On the Properties screen, select the **Share this printer** and the **List in the directory** check boxes and click **Apply**.
5. On the Print Management screen, right-click on the printer and select **Deploy with Group Policy**.
6. Locate the organizational unit on which to deploy the printer, click the **Create a New Group Policy Object** button, enter a policy name, and assign the policy to users, computers or both.

7. Access the Group Policy Management Console, locate the created policy, enable the **Printer Connection**, and verify the UNC path.

## Review Group Policy

It may be useful to use the following to review the applied policies from the command line:

- System-wide results: run **gpresult /H <HTML\_FILE\_NAME>**
- Check specific user: run **gpresult /USER <USERNAME> /H <HTML\_FILE\_NAME>**

# Appendix C: Graphics Card Drivers and Windows Updates



## NOTE

The content listed below is part of the **Enterprise Deployment Operating System Setup Guide**.

This appendix details how to install the latest video drivers and how to install the most current Windows updates on the Vitrea Enterprise deployment system at a customer site.

## Install Video Drivers - all video cards



## ROLE

This procedure is completed by the IT Administrator or Network Administrator.



## CAUTION

Do not mix video card drivers across multiple Application Servers in your Enterprise deployment. You must use the same video card driver on all Application Servers in your Enterprise deployment.



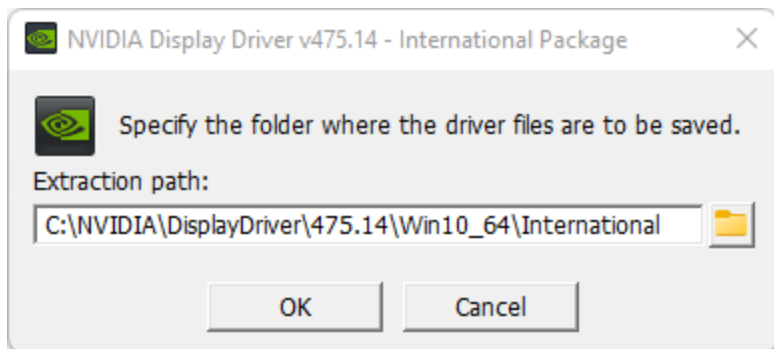
## NOTE

Complete this procedure only on Application Servers that use hardware-based visualization.

1. Navigate to the **Vitrea\_Resources\Utilities\Video Card Drivers** folder location.
2. Select the applicable driver based on operating system.
  - For Windows Server 2016, expand the **475.14** folder.
  - For Windows Server 2019/2022, expand the **553.62** folder.
3. For Windows Server 2016, expand the **475.14** folder and then expand the **Standard** folder. For Windows Server 2019/2022, expand the **553.62** folder.

### For Windows Server 2016

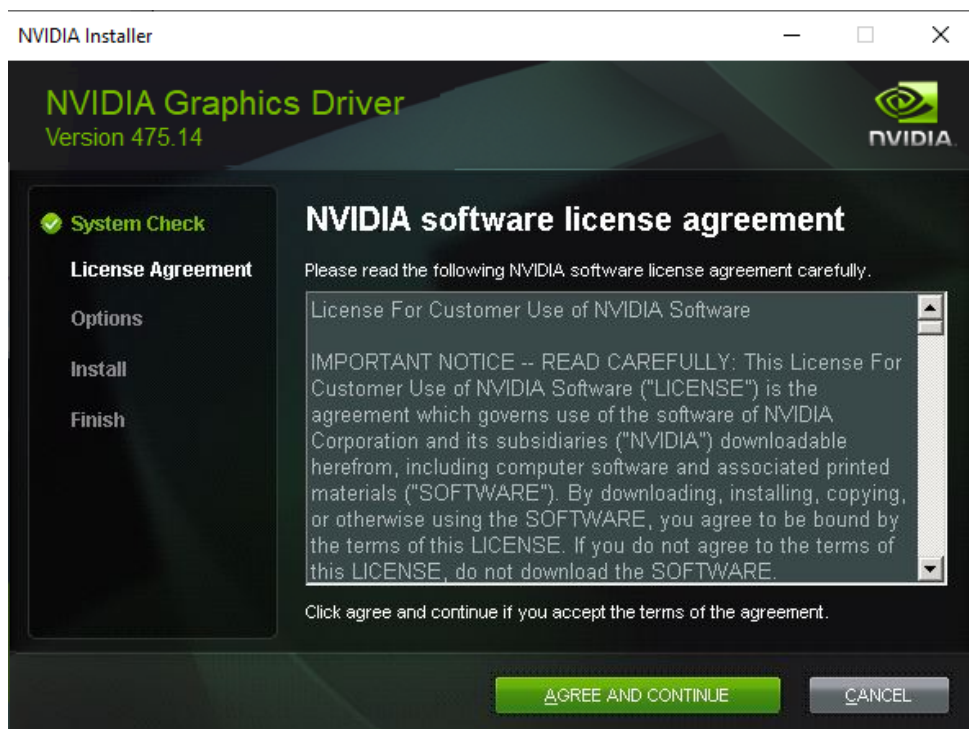
4. Double-click the desired driver file.



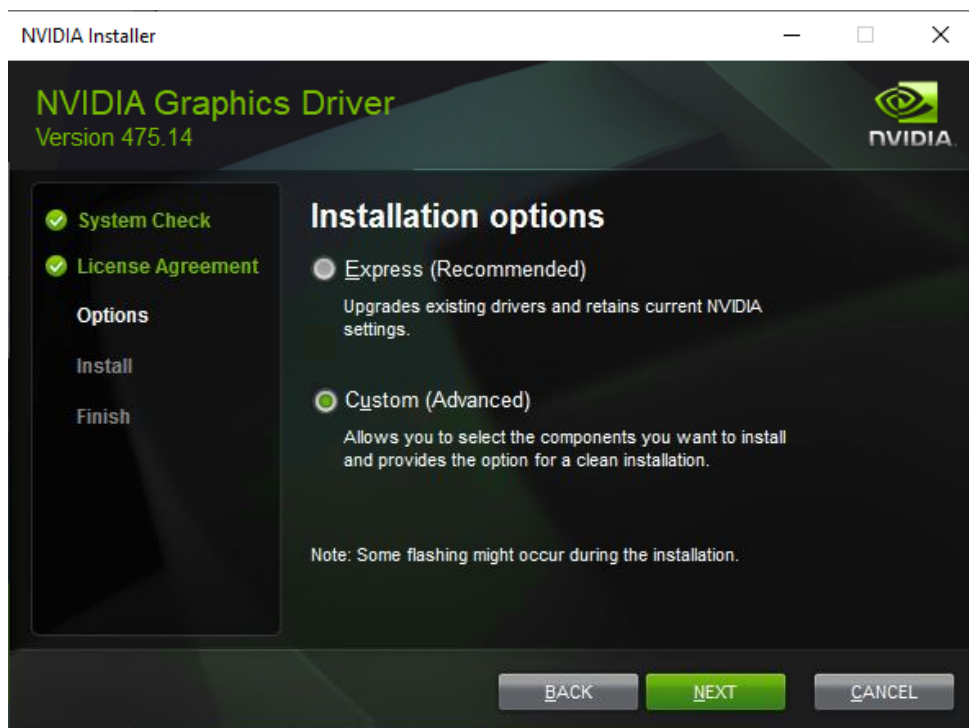
5. Click **OK**.



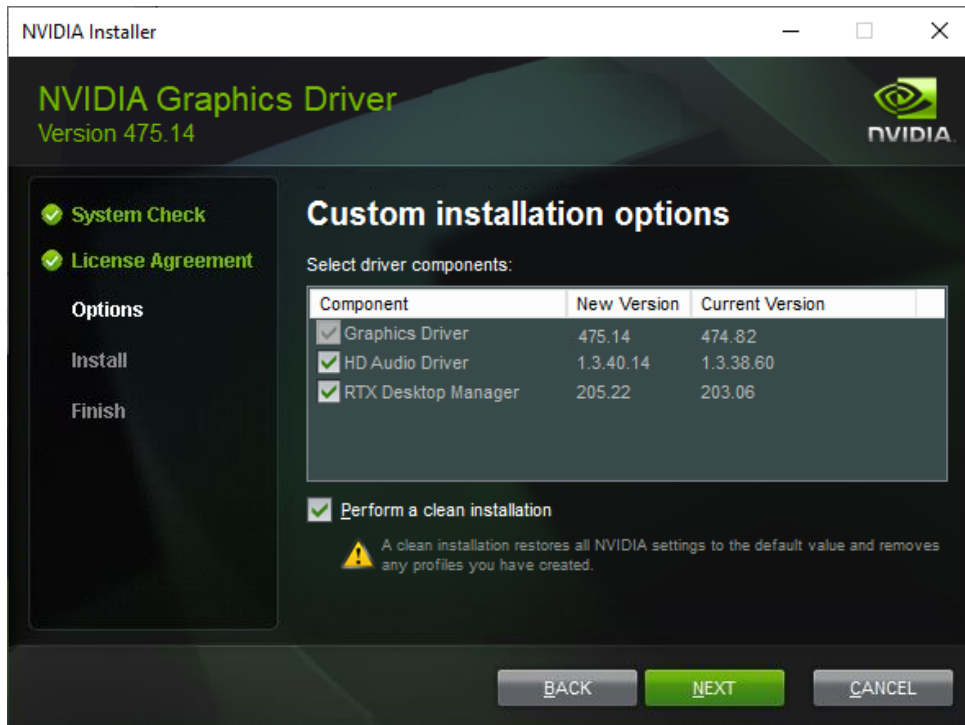




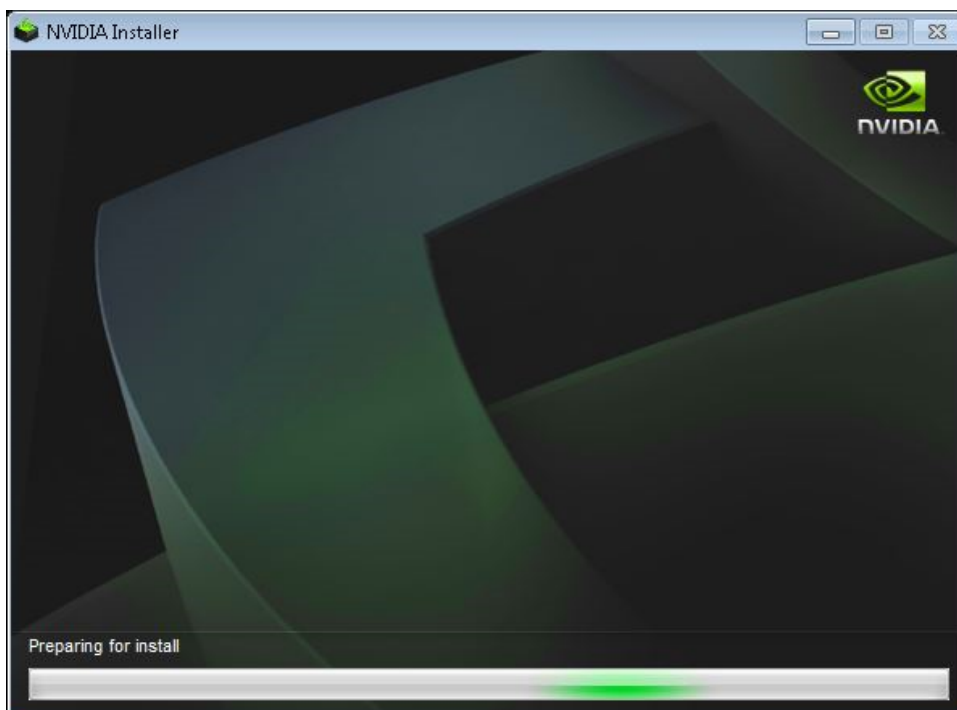
6. Click **Agree And Continue**.

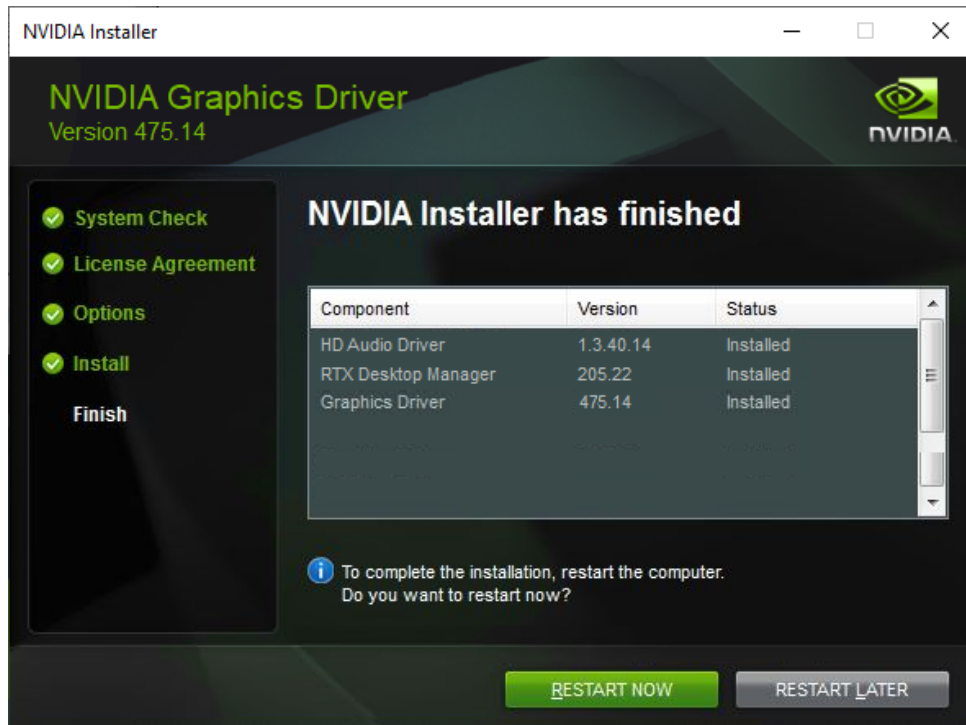


7. Select the **Custom (Advanced)** radio button and click **Next**.



8. In the **Select driver components** section, clear the **NVIDIA Ansel** checkbox.
9. Select the **Perform a clean installation** check box and click the **Next** button.

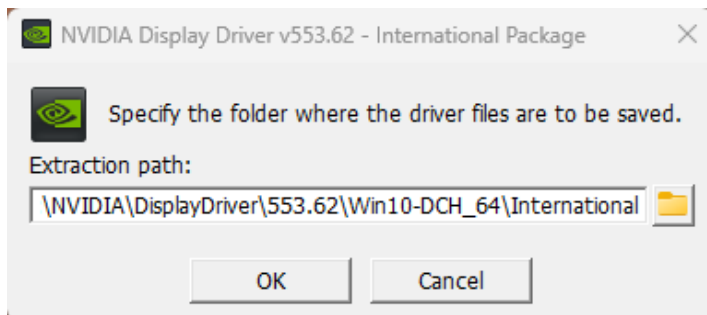




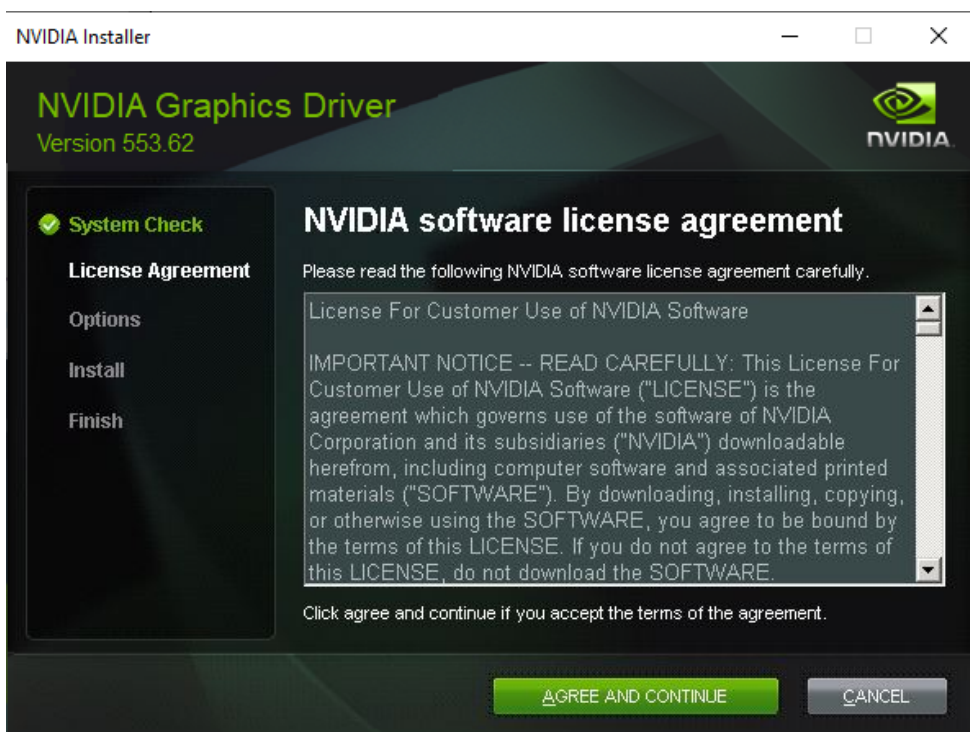
10. When the installation completes, click **Restart Now** to restart the machine.

For Windows Server 2019 or 2022

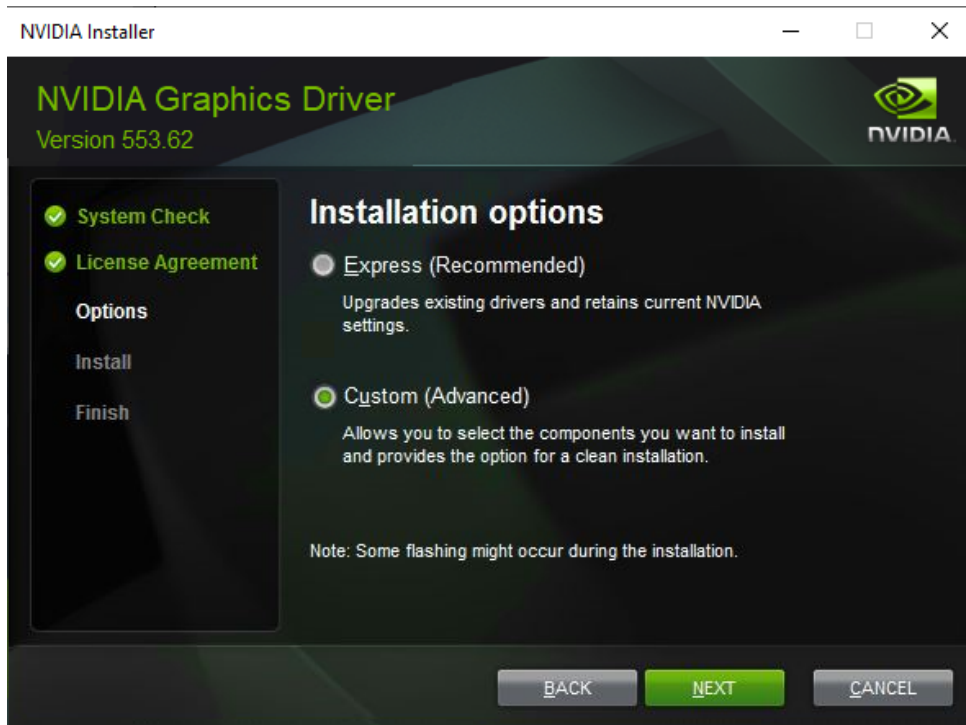
11. Double-click the desired driver file.



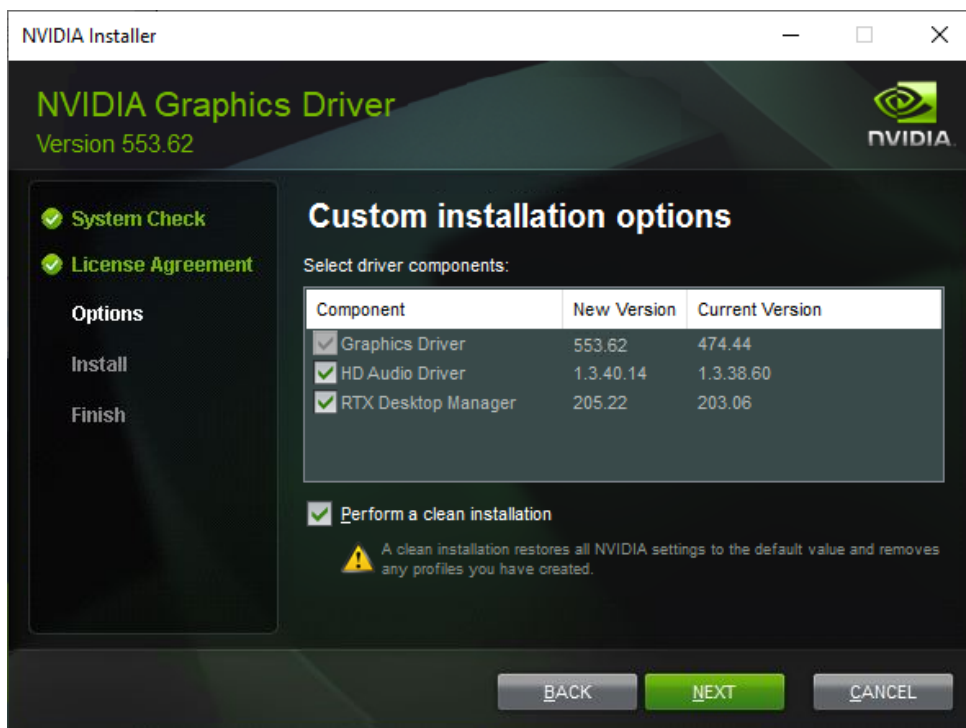
12. Click **OK**.



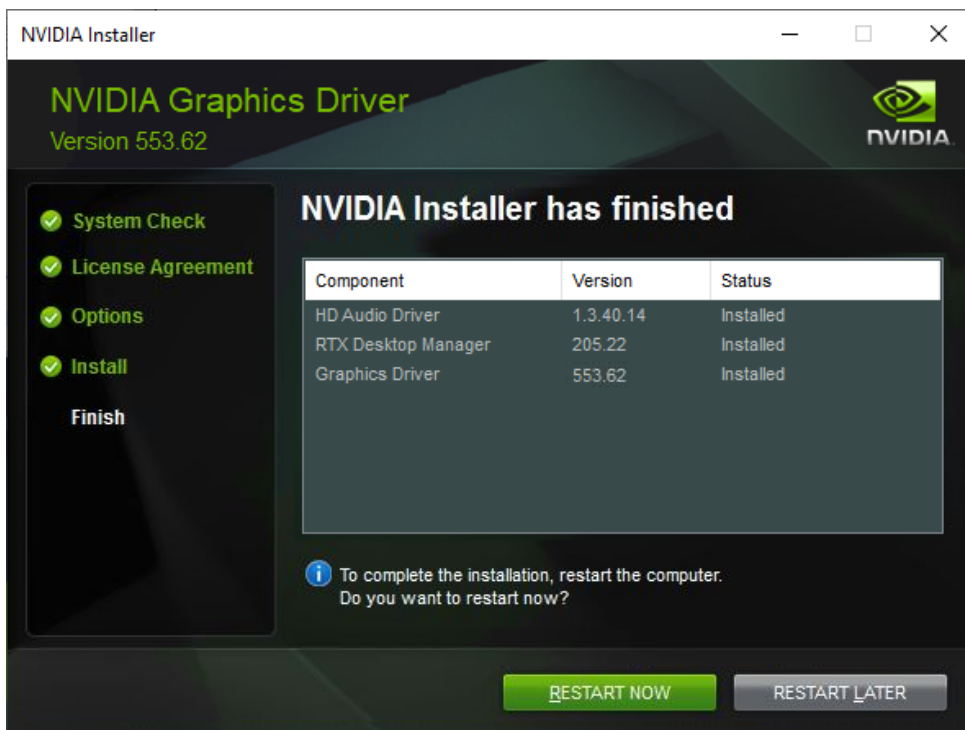
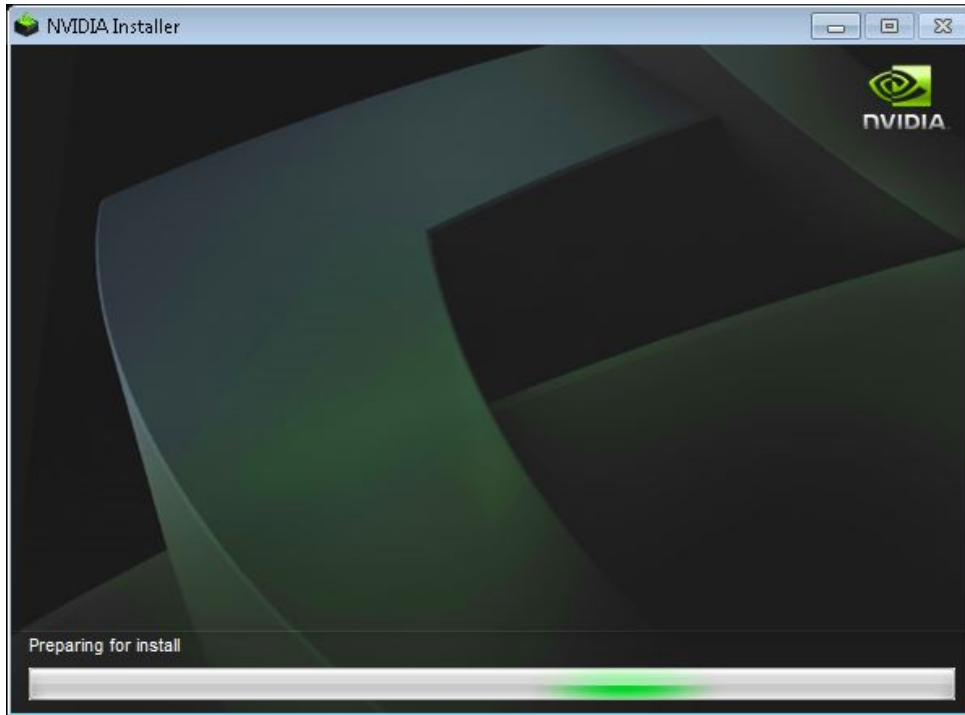
13. Click **Agree And Continue**.



14. Select the **Custom (Advanced)** radio button and click **Next**.



15. Select the **Perform a clean installation** check box and click the **Next** button.



16. When the installation completes, click **Restart Now** to restart the machine.



# Install Video Drivers for vGPU-driven Application Servers



## NOTE

vGPU video drivers should use version 11.4 or newer.

- To download the vGPU video drivers, navigate to the following location:  
<https://www.nvidia.com/Download/index.aspx?lang=en-us>

## Verify GPU Data Center Graphics Cards

If you are using Application Servers with GPU Data Center graphics cards, verify which type of video card access your servers will use: Direct Access (vDGA) or Shared (vGPU).

### Data Center GPUs for Visual Computing (vGPU)

vGPU memory settings for (512x512) vGPU profile

The table below lists how the vGPU memory settings will affect customer concurrency for a 512x512 vGPU profile.

The table describes the requirements for the vGPU profile which consists of the following criteria:

- 900 CUDA Cores per user
- a 4GB profile

Card	Memory	CUDA Cores	vGPU Profile	Slice Count - one/two/three users	PCI-E
P4 (2016)	8GB	2560	p4-4q	3413	PCI-e 3
P6 (2017)	8GB	2048	p6-4q	3413	PCI-e 3
T4 (2018)	16GB	2560	t4-4q	3413	PCI-e 3
V100 (2017)	32GB	5120	v100-4q	8731/19648	PCI-e 3
A2 (2021)	16GB	1280	A2-16q	19648	PCI-e 4
A10 (2021)	24GB	9216	A10-4q	8731/14184	PCI-e 4
A16 (2021)	4 x 16GB	4x1280	A16-4q	8731/19648	PCI-e 4
A40 (2020)	48GB	10752	A40-4q	8731/14184/19648	PCI-e 4
L4 (2023)	24GB	7424	l4-4q - 4 Users max	8731/14184	PCI-e 4
L40 (2022)	48GB	18176	l40-4q	8731/14184/19648	PCI-e 4

vGPU memory settings for (1024x1024) vGPU profile

The table below lists how the vGPU memory settings will affect customer concurrency for a 1024x1024 vGPU profile. The table describes the requirements for the vGPU profile which consists of the following criteria:

- 280 CUDA Cores per user
- an 8GB profile or greater

Card	Memory	CUDA Cores	vGPU Profile	Slice Count - one/two/three users	PCI-E
P4 (2016)	8GB	2560	p4-8q	2813	PCI-e 3
P6 (2017)	8GB	2048	p4-8q	2813	PCI-e 3
T4 (2018)	16GB	2560	t4-8q	2813	PCI-e 3
V100 (2017)	32GB	5120	v100-8q/v100-16q	2183/4912	PCI-e 3
A2 (2021)	16GB	1280	A2-16q	4912	PCI-e 4
A10 (2021)	24GB	9216	A10-8q/A10-12q	2183/3546	PCI-e 4
A16 (2021)	4 x 16GB	4x1280	A16-8q/A16-16q	2183/4912	PCI-e 4
A40 (2020)	48GB	10752	A40-8q/ A40-12q/A40-16q	2183/3546/4912	PCI-e 4
L4 (2023)	24GB	7424	l4-8q/l4-12q/l4-24q	2183/3546	PCI-e 4
L40 (2022)	48GB	18176	l40-8q/l40-12q/ l40-16q	2183/3546/4912	PCI-e 4

## Data Center GPUs for Visual Computing (vGPU)

- Data center GPU must be of the same generation/architecture as another Canon qualified/validated vGPU card.
- If the available GRID/data center GPU is not specifically listed as qualified by Canon at a minimum it must be of an equivalent generation/architecture
  - Tesla P Generation is the oldest supported generation of Data Center GPU that has been validated for use with Vitrea.
- Fixed Share or Equal Share scheduler must be set on vGPU Management.
- Data Center graphics card assigned to a VM must be a “Q” profile of at least 4GB framebuffer (xxx-4Q or larger).
- For performance reasons the quotient of the total number of CUDA cores available on the GRID/Data center GPU divided by the number of VMs assigned to that GPU must be greater than 900 (900 cores per user).
- Data center cards must be WDDM (Windows Display Drive Model) mode capable.
- For bare metal deployments please work with your Solutions Architect for correct system sizing.

Visit <https://dell.com/GPU> for current supported vGPU graphics cards for Dell hardware. NVIDIA Virtual GPU Software Documentation <https://docs.nvidia.com/grid/index.html>



## Data Center GPU License Requirements



### CAUTION

Canon Medical recommends that any customer dealing with critical healthcare, such as strokes or trauma centers, utilize Perpetual licenses to prevent performance degradation due to the possibility of expired licenses.

- NVIDIA Virtual GPU Software License Server software is required.
- An NVIDIA license system is required.
- Delegated License Service (DLS) is the recommended deployment of the NVIDIA license system to prevent loss of License server access verses with Cloud License Service (CLS) which can lose connectivity due to loss of internet access.
- NVIDIA RTX vWS licenses, license renewal, and software is the responsibility of the customer to purchase, configure and install as is ensuring all hardware is present on hardware compatibility lists, supported by OS and server vendors, etc.
  - Perpetual License(s) + SUMS are recommended to prevent licenses from expiring.
  - Virtual Dedicated Graphics Acceleration (vDGA) usage may require the use of vWS license with some data center GPU. Please review the NVIDIA Virtual GPU licensing guide for proper licensing.

Listed below is the expected performance degradation due to license expiration.

Elapsed Time	Performance Degradation
20 minutes	Frame rate is capped at 15 frames per second. The performance of Vitrea applications and processes that use CUDA is degraded.
24 hours	<ul style="list-style-type: none"> <li>• Frame rate is capped at 3 frames per second.</li> <li>• CUDA stops working and CUDA API function calls fail.</li> </ul> GPU resource allocations for a vGPU are limited, which will prevent Vitrea applications from rendering or running correctly or will cause them to report errors when started.

For more information about performance degradation, refer to the following NVIDIA article:  
<https://docs.nvidia.com/vgpu/16.0/grid-licensing-user-guide/index.html>.

NVIDIA Virtual GPU Licensing Guide: <https://www.nvidia.com/content/dam/en-zz/Solutions/design-visualization/solutions/resources/documents1/Virtual-GPU-Packaging-and-Licensing-Guide.pdf>

NVIDIA License System User Guide: <https://docs.nvidia.com/license-system/latest/nvidia-license-system-user-guide/index.html>

# Install Microsoft Windows Updates



## ROLE

This procedure is completed by the IT Administrator or VMware Administrator.

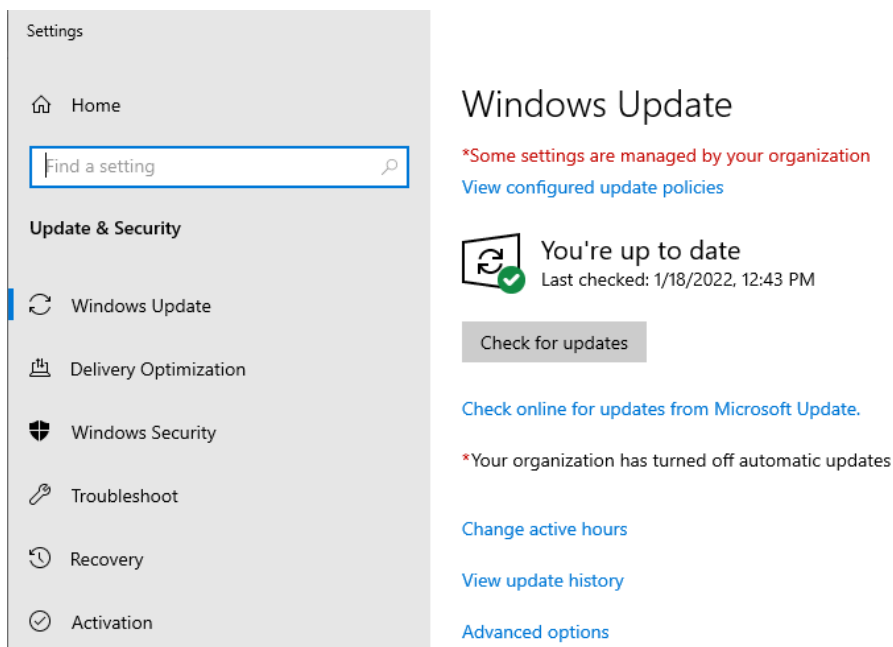


## NOTE

Canon Medical recommends that you install Microsoft Windows monthly updates. Follow your site's policy regarding software updates.

1. Right-click the **Start** button and select **Control Panel**.
2. Select the **System and Security** option.
3. Under the **Windows Update** heading, select the **Check for updates** option.

A screen similar to the one shown below displays.



4. Click the **Install** button.

Accept the cumulative updates and the version of .NET Framework that is listed.

5. Reboot if necessary.
6. Repeat Steps 1-4 until there are no important updates available.
7. Check/Apply updates until no monthly or important updates are available.
8. Complete this procedure on the servers in the enterprise deployment.

# Appendix D: Specific Antivirus exclusions



## NOTE

The content listed below is part of the **Enterprise Deployment Upgrade Guide**.

If your application does not support excluding folders and you need to exclude individual .exes, see this appendix for a complete list of .exes that can be excluded on the Management Server and Application Server.

## Management Servers Processes

C:\Program Files\Vital Images\AlgorithmExecutionContainer\_Release\_x64.exe  
C:\Program Files\Vital Images\Algorithms\_Plugins\_BoneRemoval\_Release\_x64.exe  
C:\Program Files\Vital Images\AngioReviewerStacker\_vc12\_ur64.exe  
C:\Program Files\Vital Images\Application\bin\VspAppTomcat.exe  
C:\Program Files\Vital Images\Application\jre\bin\java.exe  
C:\Program Files\Vital Images\AppShell\AppShell\_Release\_x64.exe  
C:\Program Files\Vital Images\AvCore\StudyTracker\StudyTracker.App.exe  
C:\Program Files\Vital Images\DatabaseDeploymentTool\jre\bin\java.exe  
C:\Program Files\Vital Images\DicomExportService\VI.ServiceExtension.DicomExport.Service.exe  
C:\Program Files\Vital Images\DicomPrintService\VI.ServiceExtension.DicomPrint.Service.exe  
C:\Program Files\Vital Images\Help\Node.exe  
C:\Program Files\Vital Images\Home\Node.exe  
C:\Program Files\Vital Images\inetinfo.exe  
C:\Program Files\Vital Images\Management\bin\VspMgmtTomcat.exe  
C:\Program Files\Vital Images\Management\jre\bin\java.exe  
C:\Program Files\Vital Images\MigrationService\VI.VIMS.Migration.Service.exe  
C:\Program Files\Vital Images\Part19ToPart10Converter\jre\bin\java.exe  
C:\Program Files\Vital Images\SessionHelper\Node.exe  
C:\Program Files\Vital Images\StackDefinitionBuilder\StackDefinitionBuilderTMDICOM\_Release\_x64.exe  
C:\Program Files\Vital Images\StudyList\Bonsai\_Shell\_Release.exe  
C:\Program Files\Vital Images\VIMS\ArchiveIntegrationAPI\Vitrear.AvCore.ArchiveIntegration.exe  
C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrear.AvDicom.CStoreSCP.exe  
C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrear.AvDicom.FileCopier.exe  
C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrear.AvDicom.FileCleanup.exe

C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrea.AvDicom.Processor.exe  
 C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrea.AvDatabase.Maintenance.exe  
 C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrea.AvCore.AutoDelete.exe  
 C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrea.AvDicom.PrintSCU.exe  
 C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrea.AvDicom.QRSCP.exe  
 C:\Program Files\Vital Images\VIMS\Vims\bin\Vitrea.AvDicom.CStoreSCU.exe  
 C:\Program Files\Vital Images\VitreaConduitService\Vitrea.Conduit.Service.exe.config  
 C:\Program Files\Vital Images\VitreaCourierService\Vitrea.Courier.Service.exe  
 C:\Program Files\Vital Images\VitreaLicenseStewardService\Vitrea.LicenseSteward\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaRemoteDesktopServices\RemoteDesktopInfo.Service.exe  
 C:\Program Files\Vital Images\VitreaSharedImagePoolService\bin\Vitrea.SharedImagePool\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaSharedImagePoolService\bin\Vitrea.SharedImagePoolWorker\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaSPAInfoServices\Vitrea.SPA\SPATool\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaSPAInfoServices\Vitrea.SPA\Vitrea.SystemProvisionAllocator\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaSPAInfoServices\Vitrea.SystemInfo\SystemInfo.Service.exe  
 C:\Program Files\Vital Images\VitreaSystemHealthService\SystemHealth.Service.exe  
 %appdata%\local\oleamedical\

## Application Server Processes

C:\Program Files\Vital Images\AngioReviewerStacker\_vc12\_ur64.exe  
 C:\Program Files\Vital Images\Application\bin\VspAppTomcat.exe  
 C:\Program Files\Vital Images\Application\jre\bin\java.exe  
 C:\Program Files\Vital Images\AppShell\AppShell\_Release\_x64.exe  
 C:\Program Files\Vital Images\ColonCAD\ColonCADJIT\_Release\_x64.exe  
 C:\Program Files\Vital Images\ColonCAD\Algorithms\_Plugins\_ColonCADPlugin\_Release\_x64.exe  
 C:\Program Files\Vital Images\ColonCAD\Algorithms\_Plugins\_iCADPlugin\_Release\_x64.exe  
 C:\Program Files\Vital Images\CTBoneRemovalJIT\BoneRemovalJIT\_Release\_x64.exe  
 C:\Program Files\Vital Images\CTBoneRemovalJIT\Algorithms\_Plugins\_BoneRemoval\_Release\_x64.exe  
 C:\Program Files\Vital Images\DatabaseDeploymentTool\jre\bin\java.exe  
 C:\Program Files\Vital Images\Help\Node.exe  
 C:\Program Files\Vital Images\Home\Node.exe  
 C:\Program Files\Vital Images\inetinfo.exe  
 C:\Program Files\Vital Images\LungTextureAnalysisJIT\LungTextureAnalysisJIT\_Release\_x64.exe  
 C:\Program Files\Vital Images\LungTextureAnalysisJIT\Algorithms\_Plugins\_Denoising\_Release\_x64.exe

C:\Program Files\Vital Images\OleaSphere\jre\bin\java.exe  
 C:\Program Files\Vital Images\OleaSphere\Sphere\native\OleaSphereHost.exe  
 C:\Program Files\Vital Images\Part19ToPart10Converter\jre\bin\java.exe  
 C:\Program Files\Vital  
 Images\Plugins\VAF\AbdominalMotionCorrectionPlugin\1.0.1\AbdominalMotionCorrectionPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\BodyDomainLocationPlugin\1.1.1\BodyDomainLocationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\BodyDomainLocationPlugin\1.2.0\BodyDomainLocationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\BodyRegistrationPlugin\2.1.0\BodyRegistrationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\BoneSegmentationPlugin\1.4.0\BoneSegmentationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\BoneSubtractionPlugin\1.3.0\BoneSubtractionPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\BrainGyrusMappingPlugin\2.2.0\BrainGyrusMappingPlugin.exe  
 C:\Program Files\Vital  
 Images\Plugins\VAF\CoronaryTrackingLabellingPlugin\1.1.1\CoronaryTrackingLabellingPlugin.exe  
 C:\Program Files\Vital  
 Images\Plugins\VAF\CoronaryVesselSegmentationPlugin\1.2.3\CoronaryVesselSegmentationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\DEImageGenerationPlugin\3.0.0\DEImageGenerationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\DEImageGenerationPlugin\3.2.0\DEImageGenerationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\DEImageGenerationPlugin\3.3.0\DEImageGenerationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\DiffusionFilterPlugin\1.0.1\DiffusionFilterPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\DomainTrimPlugin\1.1.0\DomainTrimPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\FatMeasurementPlugin\1.0.2\FatMeasurementPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\FatMeasurementPlugin\1.0.2\client.exe  
 C:\Program Files\Vital Images\Plugins\VAF\FollowUpRegistrationPlugin\1.3.1\FollowUpRegistrationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\HeadNeckSubtractionPlugin\2.2.0\HeadNeckSubtractionPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\HeartSegmentationPlugin\1.0.1\HeartSegmentationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\ImageReformattingPlugin\1.3.1512\ImageReformattingPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\ImageReformattingPlugin2\1.5.674\ImageReformattingPlugin2.exe  
 C:\Program Files\Vital  
 Images\Plugins\VAF\LandmarkBasedRigidRegistrationPlugin\3.1.0\LandmarkBasedRigidRegistrationPlugin.exe  
 C:\Program Files\Vital  
 Images\Plugins\VAF\LandmarkBasedRigidRegistrationPlugin\3.2.1\LandmarkBasedRigidRegistrationPlugin.exe  
 C:\Program Files\Vital  
 Images\Plugins\VAF\LungSegmentationIntensityBasedPlugin\1.3.0\LungSegmentationIntensityBasedPlugin.exe  
 C:\Program Files\Vital  
 Images\Plugins\VAF\LungSegmentationIntensityBasedPlugin\1.4.1\LungSegmentationIntensityBasedPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\LungTextureAnalysisPlugin\1.0.7\LungTextureAnalysisPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\MRCoronaryAnalysisPlugin\1.0.1\MRCoronaryAnalysisPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\OrthoThumbnailPlugin\1.2.0\OrthoThumbnailPlugin.exe

C:\Program Files\Vital Images\Plugins\VAF\RegionEditingPlugin\1.3.985\RegionEditingPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\SimilarityFilterPlugin\1.0.23\SimilarityFilterPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\SnapshotReaderPlugin\7.15.9631\SnapshotInspector\_Release\_x64.exe  
 C:\Program Files\Vital Images\Plugins\VAF\TACEFeederRankingPlugin\1.0.0\TACEFeederRankingPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\TACEVessel2PointsTrackingPlugin\2.1.0\TACEVessel2PointsTrackingPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\TACEVesselAnalysisPlugin\3.0.2\TACEVesselAnalysisPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\TumorSelectPlugin\1.1.1794\TumorSelectPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\TwoPassBoneSegmentationPlugin\1.3.1\TwoPassBoneSegmentationPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\VisiblePickPlugin\1.1.0\VisiblePickPlugin.exe  
 C:\Program Files\Vital Images\Plugins\VAF\VisiblePickPlugin\1.2.1\VisiblePickPlugin.exe  
 C:\Program Files\Vital Images\SessionHelper\Node.exe  
 C:\Program Files\Vital Images\StudyList\Bonsai\_Shell\_Release.exe  
 C:\Program Files\Vital Images\Vitrea Remote Kiosk\VitreaKioskShell\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaClassic\bin\_x64\Vitrea\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaCourierService\Vitrea.Courier.Service.exe  
 C:\Program Files\Vital Images\VitreaLicenseStewardService\Vitrea.LicenseSteward\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaSPAInfoServices\Vitrea.SPA\SPATool\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaSPAInfoServices\Vitrea.SPA\Vitrea.SystemProvisionAllocator\_Release\_x64.exe  
 C:\Program Files\Vital Images\VitreaSPAInfoServices\Vitrea.SystemInfo\SystemInfo.Service.exe  
 C:\Program Files\Vital Images\ColonCAD\veralook\veralook\_ccad10.exe  
 C:\Program Files\Vital Images\ColonCAD\veralook\veralook\_ccad11.exe  
 C:\CMSC US\CMSC\CMSCWSClinicalApp\_US\bin\TWSLauncher.exe  
 %appdata%\local\oleamedical\

## Invia 4DM Antivirus Exceptions

Users must have read/write/modify privileges for the following directories within 4DM for full functionality:

- C:\Program Files\INVIA\Corridor4DM
- C:\Users\Public\Documents\INVIA\Corridor4DM
- C:\ProgramData\INVIA\Corridor4DM\tmpdata

### Exceptions for the following executables

- Corridor4DM.exe – runs the 4DM program

- INVIA.exe – Runs licensing on the license manager server
- RLM.exe – Runs licensing on the license manager server
- LicensingManagerApp.exe – Runs the license interface from the clients and server
- C4DM\_Validate.exe – Runs validation confirming that 4DM is installed without any issues
- AuditLoggerService – Runs audit logging for 4DM
- dpiCheck – Runs dpi check

Exceptions for the following ports for license communication between the clients and 4DM license manager server

- 5053
- 5054
- 5055

Additional 4DM services that may require exceptions:

- 4DM Audit Log Service
- INVIA Software Licensing (on the workstation or the server where License Manager resides)

## Anti malware Exclusions

Anti malware software may require additional exclusions than are listed below.



### NOTE

Work with your customer site's IT department to add the appropriate exclusions. You may need to enable **Debug/Learning** mode in the Anti malware software to find all of the required exclusions as each anti malware software is unique.

## Exclusions

C:\inetpub  
C:\ProgramData\Vital Images  
C:\Program files\Vital images  
C:\Program Files\Mirada Medical

## CiscoAMP Policy

Canon Medical recommends that customers create a specific policy to be assigned to systems running the Vitrea product(s). Anti malware software will require specific exclusions into the policy profile.



## CAUTION

This is not an exhaustive list, due to the constant changing security landscape your deployment may require additional settings. Refer to the CiscoAMP for Endpoints documentation for explanation of how to use Debug Logging for your environment.

### Modes and Engines

#### Conviction modes

Title:	Setting:
Files	Quarantine
Network	Audit, may be required to be set to Disabled
Malicious Activity Protection	Audit, may be required to be set to Disabled
System Process Protection	Protect
Detection Engines	Check TETRA and Exploit Prevention

### Advanced Settings

#### Network

Title:	Setting:
Detection Action	Audit
Blacklist Data Source	Custom and Cisco

#### Questionable directories that may need exceptions:

C:\CMSC US\CMSC\CMSCWSClinicalApp\_US\bin

## SentinelOne policy

The exception listed below was recommended by Sentinel one to resolve an issue where it would lock files being handled by the VitreaCourierService and robocopy after batch evidence creation which would cause delays in opening the report page.

Complete the steps below.

1. Launch the SentinelOne interface.
2. In the **Exclusion Types** column, select the **Path** option.
3. In the main window, select the **Exclusions** tab.
4. Click the **Exclusion Type** dropdown menu and select **Path**.
5. Click the **OS** dropdown menu and select the desired operating system.
6. In the **Path** field, enter `\Device\HarddiskVolume*\Program Files\OEM\AMS\Service\ams.exe`.
7. In the **Exclusions Mode** section, select the **Performance Focus - extended** radio button.
8. Select the **Save** button.



# Appendix E: Run the System Hardening Script



## NOTE

The content listed below is part of the **Enterprise Deployment Upgrade Guide**.

## Run the System Hardening Script on the Management Server



## NOTE

Only complete this procedure if you opted out of running the system hardening script as part of the Management Server upgrade process.

This appendix describes how to execute a Microsoft PowerShell script to harden the Windows server operating system after the installation of Vitrea software on a Management Server or on an Application Server. Canon Medical recommends you run this script to enable system hardening settings.

## To run the System Hardening Script on the Management Server

1. Navigate to **E:\Vitrear<sub>Resources</sub>\<media contents>\Utilities\OS Configuration Scripts\Windows Server\Post** location and copy the folder location from the Address bar.
2. Click the **Start** button and type `PowerShell`.
3. Right-click **Windows PowerShell** and select **Run as administrator**.
4. Type `"cd"` and press **Spacebar**.
5. Right-click and select **Paste**.
6. Add quotation marks to the folder path string only, as shown below.
7. Press **Enter**.



## NOTE

The screen examples shown below are based on a Windows server operating system.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd\
PS C:\> cd "E:\Vitrea_Resources\Vitrea-7.x.x\Utilities\OS Configuration Scripts\Windows Server\Post"
PS E:\Vitrea_Resources\Vitrea-7.x.x\Utilities\OS Configuration Scripts\Windows Server\Post> .\RunScript.bat
```

8. Type `.\runscript.bat` and press **Enter**.

```
Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run E:\Vitrea_Resources\Vitrea-7.x.x\Utilities\OS Configuration Scripts\Windows
Workstation\Post\VitreaWorkstationPostScript.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"):
```

9. If you are prompted with a security warning as shown above, type **R** and press **Enter**.

```
Administration: Windows PowerShell
Type of installation
What type of deployment is this (some roles/features differ)?
[E] Extend [M] Management [A] Application [S] EnterpriseSingleServer [G] GovernmentDeployment [?] Help
(default is "E"):
```

10. On the PowerShell screen, select the **[M] Management** script profile (selections available are server-based deployments only).
11. Press **Enter**.

The script executes and finalizes system configuration. It provides a computer reboot prompt when the script is finished.

```
Administration: Windows PowerShell
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Vital Images\Installer
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Vital Images
PSChildName : Installer
PSDrive : HKLM
PSProvider : Microsoft.PowerShell.Core\Registry

A computer restart is required to apply settings. Restart computer now?
Confirm
Are you sure you want to perform this action?
Performing the operation "Enable the Local shutdown access rights and restart the computer." on target "localhost
(VML-2016MT-BM)".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

12. To reboot the system, type **A** on the PowerShell screen and press **Enter**.

# Run the System Hardening Script on the Application Server



## NOTE

Only complete this procedure if you opted out of running the system hardening script as part of the Application Server upgrade process.

## To run the System Hardening Script on the Application Server

1. Navigate to **E:\Vitrea\_Resources\<media contents>Utilities\OS Configuration Scripts\Windows Server\Post** location and copy the folder location from the Address bar.
2. Click the **Start** button and type **PowerShell**.
3. Right-click **Windows PowerShell** and select **Run as administrator**.
4. Type “cd” and press **Spacebar**.
5. Right-click and select **Paste**.
6. Add quotation marks to the folder path string only, as shown below.
7. Press **Enter**.



## NOTE

The screen examples shown below are based on a Windows server operating system.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd\
PS C:\> cd "E:\Vitrea_Resources\Vitrea-7.x.x\Utilities\OS Configuration Scripts\Windows Server\Post"
PS E:\Vitrea_Resources\Vitrea-7.x.x\Utilities\OS Configuration Scripts\Windows Server\Post> .\RunScript.bat
```

8. Type **.\runscript.bat** and press **Enter**.

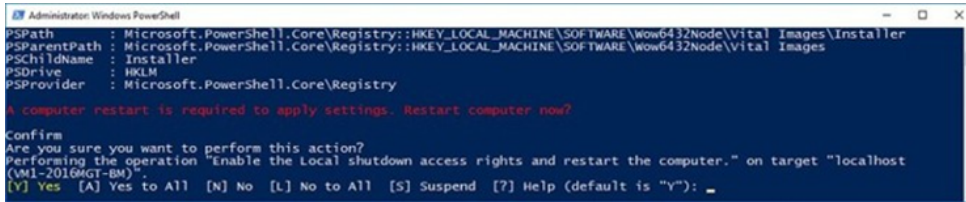
```
Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run E:\Vitrea_Resources\Vitrea-7.x.x\Utilities\OS Configuration Scripts\Windows
Workstation\Post\VitreaWorkstationPostScript.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): |
```

9. If you are prompted with a security warning as shown above, type **R** and press **Enter**.

```
Administrator: Windows PowerShell
Type of installation
What type of deployment is this (some roles/features differ)?
[E] Extend [M] Management [A] Application [S] EnterpriseSingleServer [G] GovernmentDeployment [?] Help
(default is "E"):
```

10. On the PowerShell screen, select the **[A] Application** script profile (selections available are server-based deployments only).
11. Press **Enter**.

The script executes and finalizes system configuration. It provides a computer reboot prompt when the script is finished.



12. To reboot the system, type **A** on the PowerShell screen and press **Enter**.

## System Hardening Script Settings

Listed below are the settings that are configured when the system hardening script is executed.

### Windows 2016/2019/2022 System Hardening Script settings

Setting	Description
Explicitly add and block Chargen and QOTD services UDP and TCP	Security Enhancement
Explicitly add and block TimeStamp Exposure ICMP service ICMP4	Security Enhancement
Add "Auditors" user group	
Disable SMBv1 protocol in Windows Features	Security Enhancement
Remove Powershell2.0 Engine	Security Enhancement
Install Windows BitLocker feature	
Disable WDigest Authentication	Security Enhancement
Mitigation for Microsoft Browser Information Disclosure Vulnerability CVE-2017-8529	Security Enhancement
Add key and set Remote Assistance to Disabled	Security Enhancement
Add key and set fAllowUnsolicited to Disabled	Security Enhancement
V-21954 Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites	Security Enhancement
V-81495 Disable TLS RC4 cipher in .Net -Post Install	Security Enhancement
Enable FIPS Crypto filter	Security Enhancement

Enable UAC Run all users in Admin approval mode and proper Consent Prompt - REQUIRES RESTART	Security Enhancement
Local Policies\Security Options\Network security: LAN Manager authentication level	Security Enhancement
Add key to ensure Default Passwords for Automatic Logons are disabled	Security Enhancement
Spectre/Meltdown/Foreshadow adding reg keys	Security Enhancement
Add key and set Allow Fallback to SSL 3.0 to Disabled	Security Enhancement
Set Windows Firewall to Protect all network connections >  Enabled	Security Enhancement
The Windows SMB client must be configured to always perform SMB packet signing	Security Enhancement
The Windows SMB client must be enabled to perform SMB packet signing when possible	Security Enhancement
Unencrypted passwords must not be sent to third-party SMB Servers	Security Enhancement
The Windows SMB server must be configured to always perform SMB packet signing	Security Enhancement
The Windows SMB server must perform SMB packet signing when possible	Security Enhancement
Change Access to IIS log files to restricted	Security Enhancement
Setting restricted access to IIS web administration tools. Set for InetMgr.exe	Security Enhancement
Explicitly add and block SQL Browser service TCP and UDP	Security Enhancement
Add the "SQLService" group for auditing	Security Auditing
Set ACLs for Patients directory(PHI)	Security Enhancement
Set ACLs for Database File and Log repository(PHI)	Security Enhancement
Set ACLs for DBBackup(PHI)	Security Enhancement
Create Audit Trace directory and assign access control at E:\SQLTraceAuditing	Security Auditing
Set Audit Trace access control at C:\Program Files\Microsoft SQL Server\MSSQL12.VITALS\SQL EXPRESS\MSSQL\Log - ACLS	Security Auditing
FSRM config for max audit repository limit/warning	Security Auditing
Set Max Connections for SQL Instance	Security Enhancement
Initializes SQL Trace setup per the DISA requirements	Security Enhancement
Set up auditing for success and failure for the SQL Program 64-bit directories and subs	Security Auditing
Set up auditing for success and failure for the 32-bit SQL Program directories and subs	Security Auditing
Initialize on DISA Trace Triggers	Security Enhancement
Disable Named Pipes and in SQL Config Manager	Security Enhancement
Disable Shared Memory in SQL Config Manager	Security Enhancement
Remove write access for standard users for most Vitrea AV folders in ProgramData	Security Enhancement
Reset Patients directory ownership to "SYSTEM"	Security Enhancement

Reset DBBackup directory ownership to "SYSTEM"	Security Enhancement
Reset Database file directory ownership to "SYSTEM"	Security Enhancement
Reset SQLTraceAuditing directory ownership to "SYSTEM"	Security Auditing
Reset Standard SQL Trace directory ownership to "SYSTEM"	Security Enhancement
Explicitely add and block SQL Browser service TCP and UDP	Security Enhancement
Add the "SQLService" group for auditing	Security Auditing
Set ACLs for Patients directory(PHI)	Security Enhancement
Set ACLs for Database File and Log repository(PHI)	Security Enhancement
Set ACLs for DBBackup(PHI)	Security Enhancement
Create Audit Trace directory and assign access control at E:\SQLTraceAuditing	Security Auditing
Set Audit Trace access control at C:\Program Files\Microsoft SQL Server\MSSQL12.VITALSQLEXPRESS\MSSQL\Log - ACLS	Security Enhancement
FSRM config for max audit repository limit/warning	Security Auditing
Set Max Connections for SQL Instance	Security Enhancement
Initializes SQL Trace setup per the DISA requirements	Security Enhancement
Set up auditing for success and failure for the SQL Program 64-bit directories and subs	Security Auditing
Set up auditing for success and failure for the 32-bit SQL Program directories and subs	Security Auditing
Initialize on DISA Trace Triggers	Security Auditing
Disable Named Pipes and in SQL Config Manager	Security Enhancement
Disable Shared Memory in SQL Config Manager	Security Enhancement
Reset Patients directory ownership to "SYSTEM"	Security Enhancement
Reset DBBackup directory ownership to "SYSTEM"	Security Enhancement
Reset Database file directory ownership to "SYSTEM"	Security Enhancement
Reset SQLTraceAuditing directory ownership to "SYSTEM"	Security Enhancement
Reset Standard SQL Trace directory ownership to "SYSTEM"	Security Enhancement
Explicitely add and block SQL Browser service TCP and UDP	Security Enhancement
Add the "SQLService" group for auditing	Security Auditing
Add the "Auditor" to "Users" group and adding the user "Auditor" to the "Auditors" group	Security Auditing
Add key to ensure Automatic Logons are disabled	Security Enhancement
Set ACLs for Patients directory(PHI)	Security Enhancement
Set ACLs for Database File and Log repository(PHI)	Security Enhancement
Set ACLs for DBBackup(PHI)	Security Enhancement

Create Audit Trace directory and assign access control at E:\SQLTraceAuditing	Security Auditing
Set Audit Trace access control at C:\Program Files\Microsoft SQL Server\MSSQL12.VITALSQLEXPRESS\MSSQL\Log - ACLS	Security Auditing
FSRM config for max audit repository limit/warning	Security Auditing
Set Max Connections for SQL Instance	Security Enhancement
Initializes SQL Trace setup per the DISA requirements	Security Enhancement
Set up auditing for success and failure for the SQL Program 64-bit directories and subs	Security Auditing
Set up auditing for success and failure for the 32-bit SQL Program directories and subs	Security Auditing
Initialize on DISA Trace Triggers	Security Auditing
Disable Named Pipes and in SQL Config Manager	Security Enhancement
Disable Shared Memory in SQL Config Manager	Security Enhancement
Unzip LGPO.zip	Security Enhancement
Import DoD GPO for hardening Windows Server 2016/2019/2022-Computer configurations	Security Enhancement
Import DoD GPO for hardening Windows Server 2016/2019/2022-User configurations	Security Enhancement
Import DoD GPO for hardening Internet Explorer 11-Computer configurations	Security Enhancement
Import DoD GPO for hardening Internet Explorer 11-User configurations	Security Enhancement
Import DoD GPO for hardening Windows Defender for 2016/2019/2022-Machine configurations	Security Enhancement
BOOKMARK Import DoD GPO for hardening Windows Firewall configuration	Security Enhancement
V-205807 Windows Server 2019 must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs	Security Enhancement
V-3338 Named pipes that can be accessed anonymously must be configured to contain no values	Security Enhancement
Add key and set Use of the Tabular Data Control (TDC) ActiveX control to Disabled for the Internet Zone	Security Enhancement
Add key and set Use of the Tabular Data Control (TDC) ActiveX control to Disabled for the Restricted Sites Zone	Security Enhancement
Set Windows Update policy - Windows Update "Do not connect to any Windows Update Internet locations" to Enabled	Security Enhancement
Add Legal Notice Caption key and text	Security Enhancement
HTTP API Server version must be removed from the HTTP Response Header information	Security Enhancement
Reset Patients directory ownership to "SYSTEM"	Security Enhancement
Reset DBBackup directory ownership to "SYSTEM"	Security Enhancement
Reset Database file directory ownership to "SYSTEM"	Security Enhancement
Reset SQLTraceAuditing directory ownership to "SYSTEM"	Security Auditing

Reset Standard SQL Trace directory ownership to "SYSTEM"	Security Enhancement
Set Machine IIS Machine Key Validation to "HMACSHA256"	Security Enhancement
IIS MIME Extension removal	Security Enhancement
IIS 10.0 MaxConnection setting configured to Limit Max Simultaneous Connections to 1024	Security Enhancement
IIS Event Logging set to "Both..."	Security Enhancement



#### NOTE

The SQL Browser Service has been disabled and is no longer required.

## Windows 2022 OS Configuration Settings

Setting	Description
Explicitly adds Microsoft's OpenMP Patch registry key – Critical for Vitrea Windows Server 2022 support	OS Configuration

## Printer Security Configuration

To access the Local Security Policy, navigate to the following path: **Local Computer Policy | User Configurations | Administrative Templates | Control Panel | Printers**

Setting	Description
Disable Browse the network to find printer. Set to Disabled.	Security Enhancement
Prevent Addition of printers. Set to Enabled.	Security Enhancement
Prevent Deletion of Printers. Set to Enabled.	Security Enhancement

## Vitrea System Checker Script and Reporting

The **VitreaSystemChecker.ps1** script produces a report that confirms the status of security and best practice configurations set by the system hardening script.

By default, the **VitreaSystemChecker.ps1** script runs automatically following reboot of the operating system at the end of the Vitrea installation process. The results file for this script execution is located at **C:\ProgramData\Vitrea\SystemChecker**.

To confirm configurations are set properly by the system hardening script, open the **SysChkrReport {machinename,date,time}.html** file in any Internet browser.

The status of a given configuration is reported as "OK" displaying in green, or "Not OK" displaying in red, based upon its intended configuration.





## NOTE

If you opted out of running the system hardening script as part of the Vitrea installation process, the **VitrearSystemChecker.ps1** script does not execute automatically.

To run the **VitrearSystemChecker.ps1** script manually, navigate to **E:\Vitrear\_Resources\<media contents>\Utilities\Scripts\SystemChecker**, open the ReadMe file and follow the Script Execution instructions.

# Appendix F: VMware Procedures



## NOTE

The content listed below is part of the **Enterprise Deployment Operating System Setup Guide**.

This appendix describes how to verify Enhanced vMotion Compatibility (EVC) is enabled and how to reconfigure the vCPU cores on the Vitrea Enterprise deployment system at a customer site.

## Verify EVC is enabled

Enhanced vMotion Compatibility (EVC) is a cluster feature that ensures CPU compatibility between hosts in a cluster so that you can seamlessly migrate virtual machines within the EVC cluster.

Complete this procedure to verify Enhanced vMotion Compatibility (EVC) is Enabled on the customer site system.



## NOTE

The procedure differs by which version of the Vitrea software is installed on the system.

### For systems with Vitrea 7.15.6 and older installed

The EVC level for the vmWare host must be L4/Sandy Bridge generation or higher. AVX2 Instruction Set is necessary for the application.

1. Navigate to a virtual machine in the vCenter Server inventory.
2. On the **Configure** tab, select **VMware EVC**.
3. Click the **Edit** button.  
The Change EVC Mode dialog box displays.
4. Select the **Enable EVC with Intel hosts** radio button.
5. From the drop down menu, select **Intel "Sandy Bridge" Generation**.
6. Click **OK**.

### For systems with Vitrea 7.15.7 and newer installed

The EVC level for the vmWare host is L6/Haswell generation or higher. The vm must be able to access SSE4.2.

1. Navigate to a virtual machine in the vCenter Server inventory.
2. On the **Configure** tab, select **VMware EVC**.
3. Click the **Edit** button.  
The Change EVC Mode dialog box displays.
4. Select the **Enable EVC with Intel hosts** radio button.

5. From the drop down menu, select **Intel "Haswell" Generation**.
6. Click **OK**.

## Configure the vCPU cores on the system

When implementing the enterprise deployment solution in a VMware environment, all MAC addresses must be static.



### NOTE

When deploying virtual Application Servers, be sure to set a maximum of 1 or 2 sockets for each guest. The default is the same number of sockets as vCPUs.

**Example:** 8 sockets and 8 cores would be the default. Change this to 1 socket and 8 cores.

The Vitrea software will run inefficiently if the default is not changed. A warning also displays in System Health if too many sockets are found.

To configure the VMware socket value, complete the steps below.

### Using VMware VSphere 7.x/ESXi



For VMware VSphere 7.x/ ESXi, navigate to the **CPU** section in the Edit Settings window to set your Cores per socket value.

For more information, refer to the <https://docs.vmware.com/en/VMware-vSphere/index.html> article.

### Using VMware VSphere 8.x/ESXi

Edit Settings |

×

> Boot Options

Expand for boot options

> Power management

Expand for power management settings

> Advanced

Expand for advanced settings

> Fibre Channel NPIV

Expand for Fibre Channel NPIV settings

✓ CPU Topology

CPU

8

Cores per Socket

8

ⓘ

Sockets: 1

⚠

The manual configuration for cores per socket might result in reduced performance.

×

CPU Hot Plug

☐ Enable CPU Hot Add

NUMA Nodes

Assigned at power on

ⓘ

Device Assignment

Manually assign devices to NUMA nodes.

Device Name	NUMA Node
SCSI controller 0	Unassigned

CANCEL

OK

For VMwareVSpheer 8.x/ ESXi, navigate to the **CPU Topology** section in the Edit Settings window to set your Cores per socket value.

For more information, refer to the <https://docs.vmware.com/en/VMware-vSphere/index.html> article.