Relativity®

Pre-Installation Guide

May 10, 2024 | Version 12.3.805.2

For the most recent version of this document, visit our **documentation website**.

Table of Contents

1 Pre-installation

You must complete the pre-installation process to ensure that your environment is configured with the software, user accounts, directories, and other prerequisites required for an initial installation of Relativity. In addition, the Relativity Service Bus requires that you install and configure RabbitMQ.

As you set up your environment, use the Installation accounts and directories list to record information about your environment configuration that the installation process requires. You can download this document from Pre-Installation on the Relativity 2023 Documentation site.

For additional information, see the System Requirements and Environment Optimization guides.

Note: If you use a firewall, refer to the Ports Diagram in the Relativity Community to ensure that you configure your firewall correctly with Relativity.

Note: Relativity has deprecated support for Windows Service Bus beginning in Server 2023, and you must convert to RabbitMQ prior to upgrade.

2 Windows updates

Install the latest Microsoft Windows Server Service Pack on all Relativity servers.

However, compatibility for higher .NET versions is not guaranteed. We do not recommend installing higher .NET versions than what is listed as required by your Relativity version. Furthermore, install any smaller security patches, Windows updates, and anything else at your own discretion. We only test major service packs, not every Microsoft update. Deploy any patches to your test instance of Relativity first. Ensure that a rollback plan is in place if you discover any issues during deployment.

Ensure you disable the option to Install updates automatically on all Relativity servers. Apply any required updates during a planned maintenance window.

After installing Windows updates, reboot your machines before attempting to install Relativity. Complete this step to ensure that all Relativity components are properly installed. Incomplete Windows updates lock system files, which may cause silent failures and prevent the proper installation of Relativity components.

Note: You must enable Windows Network discovery on all machines.

3 Required certificates for Relativity

Relativity verifies that all HTTPS services running in your environment have a trusted certificate. The HTTPS services run on the following components of your Relativity installation, so they require that you install valid certificates:

- Analytics server
- Components that connect to the Services API
- Components that use HTTPS to connect to the REST API
- Viewer
- Agent servers
- Web servers
- Worker servers

For more information about required certificates and their corresponding Relativity servers, see All certificates used by Relativity servers on the Community site.

You need to add certificates to any server in your Relativity environment that is accessed by an HTTPS service. By adding these certificates, you will not see warning messages and insecure-connection icons displayed as you navigate to different components of your Relativity site. Use these guidelines for installing certificates in your Relativity environment:

- If your Relativity site is exposed to the internet, install a certificate on any server that users can access with HTTPS services.
- If Relativity users access your web server with different internal and external names, install a second certificate for the internal name.
- If you use different internal and external URLs bound to the same IP address on your servers, install a second certificate on the server for the internal IP address. You may want to consider using Server Name Indication (SNI), which is an extension to the Transport Layer Security (TLS). For more information, see IIS 8.0 Server Name Indication (SNI): SSL Scalability on the Microsoft website (http://www.iis.net/learn/get-started/whats-new-in-iis-8/iis-80-server-name-indication-sni-ssl-scalability).

  Note: If you do not want to use SNI in your environment, then configure separate IP addresses on your web servers for internal and external URLS. You might not be able to use SNI if your IIS or web browser versions do not support it.

For information about generating certificates for servers in your Windows domain, see Public Key Infrastructure Design Guidance on the Microsoft site, http://social.technet.microsoft.com/wiki/contents/articles/2901.public-key-infrastructure-design-guidance.aspx. We recommend that you use the Standalone offline root CA referenced in this article.

For information on setting up HTTPS for the Service Host Manager on web and agent servers, see Service Host Manager on the Relativity 2023 Documentation site.

For information on enabling HTTPS for Invariant Kepler Services, see the Worker Manager Server Installation Guide.

3.1 Microsoft Storage Sense

The Microsoft Storage Sense feature that is built in to Windows Server 2019 and later has the potential to cause instability in your Relativity Server instance by inadvertently clearing out Windows TEMP folders.

To mitigate this scenario, see the knowledge base article Temp folder inadvertent clean up by Windows on the Community.

You must have valid Community credentials to access this content.

3.2 Creating a self-signed certificate in PowerShell

To create a self-signed certificate with PowerShell 4.0, perform the following steps:

1. Open **PowerShell**.
2. Ensure you are running PowerShell in administrator mode. Otherwise, you will receive an error when attempting to create the certificate.
3. Import the PKI module into PowerShell via the following command:

```
Import-Module PKI
```

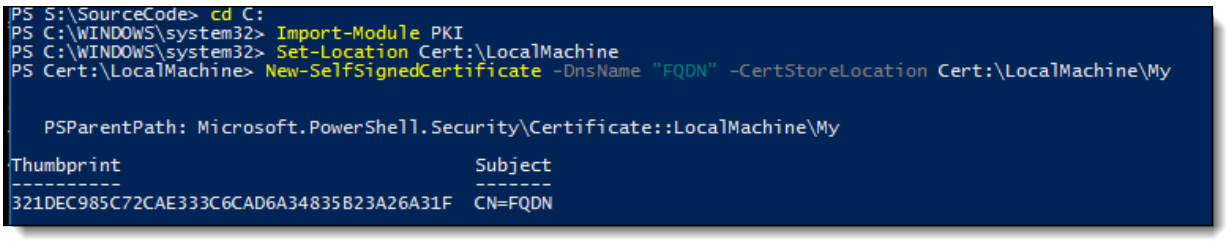
4. Create the certificate through the following commands, where "FQDN" is the fully-qualified domain name.

> **Note:** If you are performing these steps as part of enabling HTTPS for Invariant Kepler Services, the fully-qualified domain name will be for the Queue Manager. For details, see the Worker Manager Server Installation Guide.

```
Set-Location Cert:\LocalMachine
```

```
New-SelfSignedCertificate -DnsName "FQDN" -CertStoreLocation Cer-
t:\LocalMachine\My
```

5. Confirm that you have created a certificate in the personal store. Your PowerShell display should resemble the following image:



6. Create, or designate, a folder in your C drive to which you want to export the certificate, which you will do through the final Export-Certificate prompt included below. You will receive an error if that file path does not exist.
7. Export the certificate through the following commands:

```
Set-Location Cert:\LocalMachine\My
```

Doing this sets your location to the folder you just created the certificate in.

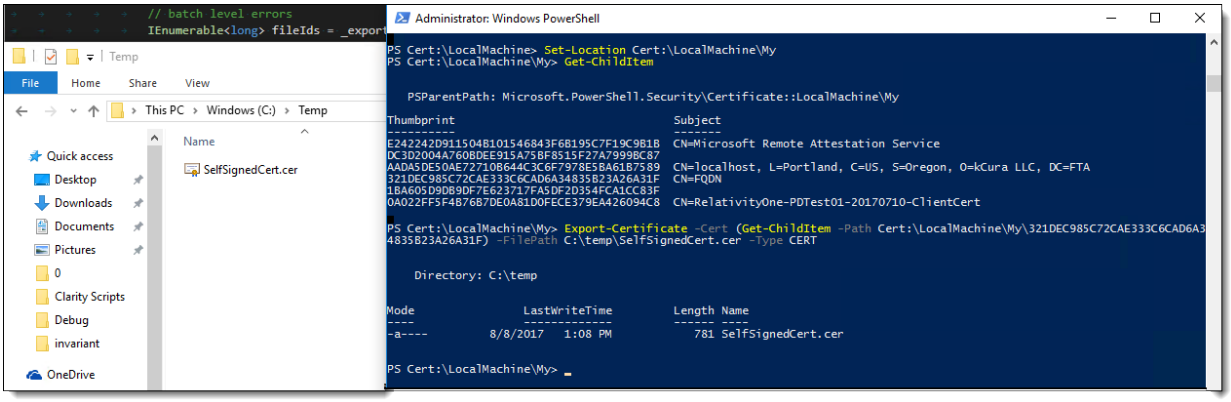
```
Get-ChildItem
```

This displays the thumbprint of all certificates in the folder you just created, including the one you just added. Make sure to copy the signature of the certificate you created and paste it into the following command.

```
Export-Certificate -Cert (Get-ChildItem -Path Cer-
t:\LocalMachine\My\CertificateSignature)  -FilePath C:\Tem-
p\SelfSignedCert.cer -Type CERT
```

Make sure you pasted the certificate signature you copied after running the Get-ChildItem command into this command, specifically in place of "CertificateSignature" above.

8. Confirm that you successfully exported the certificate you created. Your PowerShell display and corresponding folder should resemble the following image:



3.2.1 Certificate requirements for RabbitMQ

The Relativity Service Bus requires the installation of RabbitMQ as a prerequisite. To facilitate secure communication, RabbitMQ requires a certificate.

The certificate must include the following information:

- For any certificate, either the Subject Name, Subject Alternative Name, or both must be valid for the Fully Qualified Domain name that will be configured in Relativity.
- Private and public key.
- Valid start date, end date, and trust chain.
- Corresponding certificate for the authority that issued the certificate. A corresponding certificate is not required if using a self-signed certificate.
- Certificate itself, the private key, and the certificate for the authority must be in the PEM format. For more information, see Convert certificates to PEM format.

You can use one of the following options for obtaining a trusted certificate for RabbitMQ:

- **Using a certificate authority**—if using a certificate authority complete the following:
  - Request or generate a certificate with the required properties.
  - If you are using an internal certificate authority that is not capable of generating the key and certificate in PEM format directly, generate and convert the certificate, the certificate's private key, and the certificate authorities certificate to PEM format. For more information, see Convert certificates to PEM format.
  - **Self-signed certificate**—there are several ways to generate a self-signed certificate including:
    - Powershell
    - **OpenSSL**—use the following script to directly generate the files in the PEM format. You need to update the inputs for the following script for your environment.

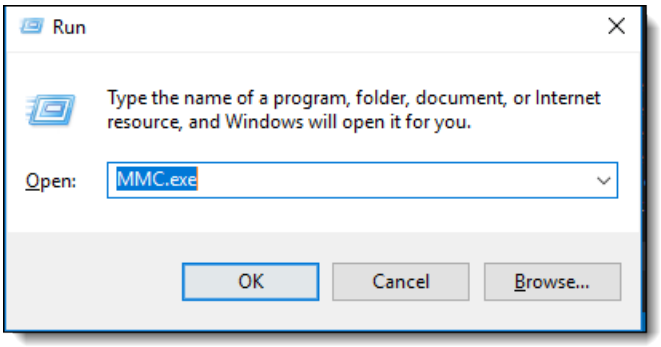
      Note: To run OpenSSL commands, you need to add the OpenSSL path to the environmental variable or run a command prompt as an admin at that directory.

```
@echo off

                                                                    REM IN YOU
makeCERT.bat
                                                                    REM AT CON
cert
                                                                    REM IT WIL
HOSTNAMEKey.pem, HOSTNAMECert.pem, HOSTNAMEpfx.pfx


                                                                    REM PLEASE
NEEDS.
                                                                    SET HOSTNA
                                                                    SET DOT=co
                                                                    SET COUNTR
                                                                    SET STATE=
                                                                    SET CITY=C
                                                                    SET ORGANI
                                                                    SET ORGANI
                                                                    SET EMAIL=

                                                                    (
                                                                    echo [req]
                                                                    echo defau
                                                                    echo promp
                                                                    echo defau
                                                                    echo x509_
                                                                    echo disti
                                                                    echo:
                                                                    echo [dn]
                                                                    echo C = %
                                                                    echo ST =
                                                                    echo L = %
                                                                    echo O = %
```

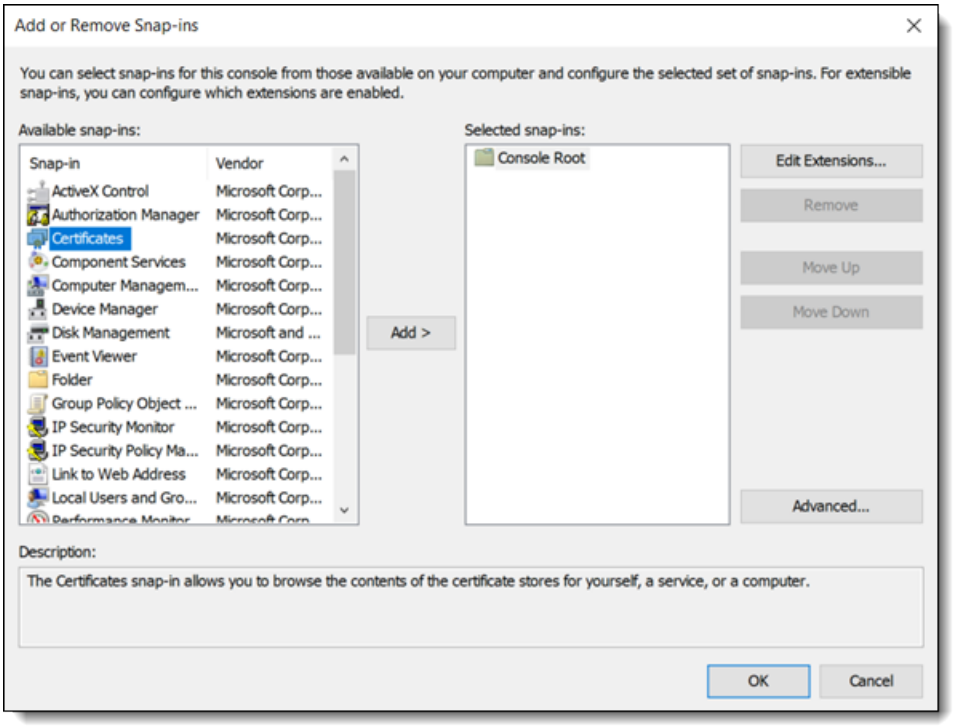
```
                                                                    echo OU =
                                                                    echo email
                                                                    echo CN =
                                                                    echo:
                                                                    echo [v3_r
                                                                    echo subje
                                                                    echo:
                                                                    echo [alt_
                                                                    echo DNS.1
                                                                    echo DNS.2
                                                                    )>%HOSTNAM

                                                                    openssl re
-keyout %HOSTNAME%Key.pem -days 3560 -out %HOSTNAME%Cert.pem -
config %HOSTNAME%.cnf
                        openssl pkcs12 -inkey %HOSTNAME%Key.pem -in %HOSTN
t.pem -export -out %HOSTNAME%pfx.pfx
```

Note: After updating the inputs at the beginning of the script for your environment, this script can be used to directly generate a self-signed certificate in the PEM format.

- **Existing Certificate from the Certificate Store**—RabbitMQ service does not use the Windows Certificate Store. Instead, certificates have to be configured in the RabbitMQ **advanced.config** file. You will need the certificate, private key, and CA certificate, or the same certificate for self-signed, all in the PEM format. In order to export the certificates from the Window Certificate Store perform the following steps:
  - Open **Run** on your desktop, and enter **MMC.exe**.



  - Click **OK**.
  - In the Console window, click **File** > **Add/Remove Snap-ins**.
  - Select **Certificates** under Available Snap-ins.



- Click **Add**.
- Select **Computer Account** and click **Next**.
- Select **Local Computer** and click **Finish.**
- Click **OK**.
- Right-click the certificate you want to export and click **All Tasks** > **Export**.
- On **Export Private Key** select **Yes, export the private Key**.
- On **Export File Format** select **Personal Information Exchange (.pfx)**.
- Select **Include all certificates in the certification path if possible**.
- Click **Next**.
- On **Security** select **Password**.
- Enter in a unique and secure password, you will need it for when converting the .pfx to a .pem.
- Save the file in a secure location.
- Using the Windows Certificate Manager store, export the .pfx certificate without the private key, making sure to choose the .der (.cer) option.

Convert certificates to PEM format

The certificates in RabbitMQ must be in PEM format. There are multiple ways to convert certificates to the PEM format. The following an example conversion done using OpenSSL:

1. If applicable, export the certificates from the Window Certificate Store. For more information. see Export existing certificates for conversion to PEM format.

2. Using OpenSSL, complete the following steps convert the certificate to PEM format:
    1. Save the private key as a PEM file:

        ```
        openssl pkcs12 -in <PathToPfx>.pfx -out <OutputPathForKey>.pem -
        nodes -nocerts
        ```

    2. Save the certificate as a PEM file:

        ```
        openssl pkcs12 -in <PathToPfx>.pfx -out <OutputPathForCert>.pem -
        nodes -nokeys
        ```

    3. Save the CA certificate as a PEM file, this step is not required for self-signed certificates:

        ```
        openssl x509 -inform der -in <PathToCACer>.cer -out <OutputPath>.pem
        ```

For more information on using OpenSSL to convert the certificate to PEM format, see How to convert a certificate into the appropriate format.

3.2.1.1 (Optional) Running the RabbitMQCertificate utility

When configuring the RabbitMQ TLS setting, you have the option of running the RabbitMQCertificate utility available on the Community, which contains a copy of OpenSSL. If you cannot use Powershell for any reason, then you need to use the manual setup instructions provided above.

To use the RabbitMQCertificate utility:

1. Download the **RabbitMQCertifcateUtility** from the Community.
2. Unzip the **RabbitMQCertificateUtility.zip** file and open the **RabbitMQCertificateUtility** folder.
3. Navigate to the **File** tab in your file explorer.
4. Select **Open Windows PowerShell** and then select **Open Windows PowerShell as administrator**.
5. Run the script by typing **.\RabbitMQCertificateTool.ps1** and clicking **Enter**.
6. Select one of the following options:
    - Option 1 to set up RabbitMQ with a self-signed certificate.
        - Provide a password, which will be used when creating the private key.
        - The password must not contain ! or &.
        - Restart the service when prompted.
        - Export the newly created certificate and install it on all web, agent, and Invariant servers.
    - Option 2 to use a PFX.
        - The PFX must be in the **C:\Users\{RSA}\AppData\Roaming\RabbitMQ** folder.
        - The PFX must be called **RabbitMQ.pfx**.
        - You must know the password for this PFX file, as you will be prompted for it when running this option.

4 User and group accounts

Configure the following user and group accounts in your environment.

4.1 Relativity service account

Make sure that the Relativity services account has local administrator privileges on each of the servers where you want to install Relativity. You must log in under this account when installing this software. You can find additional requirements for this account under the sections describing how to configure specific servers. For additional information about this account, see Relativity service account information on page 64.

The Windows Service Component and the Relativity COM Plus Component run under the Relativity Service Account. Verify that this account is configured as follows:

- Create account in Active Directory.
- Add account to the Administrators group on all machines running Relativity components.
- If using a workgroup, verify that the account has identical credentials on all Relativity servers.

5 Database server setup

Set up the database server by completing the steps in this section.

Note: The SQL sa account must exist with the name **sa**, and be enabled during installs.

5.1 Required software

The following software must be installed on the database server:

- Windows Server 2022, Windows Server 2019, Windows Server 2016
- SQL Server 2022, SQL Server 2019, or SQL Server 2017

  Note: SQL Server 2019 requires Windows Server 2016 or 2019.

Relativity supports in-place upgrades to SQL 2016 to any higher supported version. For details on SQL Server upgrade, follow the EDDS migration Guide. To determine if you should upgrade your current SQL Server version to SQL Server 2019, note the following considerations. Contact Relativity Support with any further questions.

- The base operating system of your SQL Server must be at a minimum Windows Server 2016. Any Windows Server version below 2016 will require an EDDS migration to be performed to a server with a proper operating system version and SQL version. Relativity does not support in-place operating system upgrades.
- SQL Server version lower than SQL 2016 will require an EDDS migration since upgrading to SQL Server 2019 or higher from versions lower than SQL Server 2016 has not been tested by Relativity.
- .NET 4.7.2, 4.8, or 4.8.1
- .NET 3.5

Additional considerations:

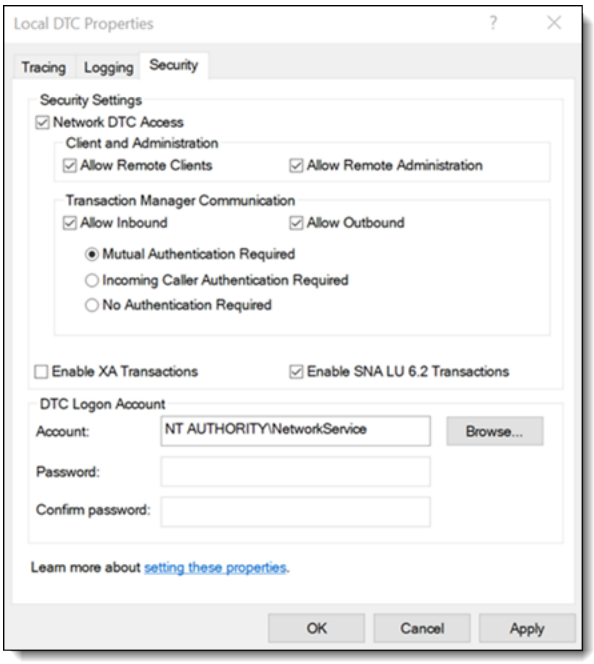
- Each environment is different, research settings that your specific environment may utilize before performing any upgrades.
- Ensure that you have tested backups before performing any upgrades.
- Although an in-place SQL upgrade is supported by Relativity. Performing an EDDS migration is the cleanest way to perform a SQL upgrade.

Note: Relativity requires Full Text Search from the Database Engine Services feature as part of the SQL Server installation.

5.2 Enable Microsoft DTC

Microsoft DTC must be enabled on the SQL Server along with the following configuration changes:

1. Add the **Application Server** role and select **Distributed Transactions**. Select **Incoming Remote Transactions** and **Outgoing Remote Transactions**.
2. Type **dcomcnfg** on your Start menu and press **Enter** to open Component Services.
3. Expand **Component Services** > **Computers** > **My Computer** > **Distributed Transaction Coordinator**.
4. Right-click **Local DTC** and click **Properties**.
5. Click the **Security** tab.
6. Select the following check boxes. For additional details on DTC enablement, see the Deployment workbook on the Relativity Community.



   - **Allow Remote Clients**
   - **Allow Inbound**
   - **Allow Outbound**
7. Click **Apply**.
8. Click **Yes** to restart the MSDTC service.
9. Click **OK**.

5.3 Assign admin permissions to the Relativity service account

You must configure permissions for the Relativity service account on the SQL Server as part of the database setup process. Make sure that the Relativity service account has local administrator and system admin permissions on the SQL Server.

5.4 Create SQL Server login

The following login must be added to the SQL Server environment. Set this account to **Never Expire** and **Not Enforce Password policy**.

Note: The Relativity installer creates this SQL Server account if it does not already exist.

The EDDSDBO account is the login used by the owner of all objects in the EDDS system databases. Follow these guidelines for configuring this account:

- Authenticate this user with SQL Server Authentication.
- Give this account only the following server roles:
  - bulkadmin
  - dbcreator
  - public
- If you have multiple SQL Servers, create this account on each server with the same name, permissions, and credentials.
- Make sure that password for EDDSDBO account doesn't contain an equals sign (=), carats (< or >), double quotes ("), parenthesis, curly braces ({ or }), or semicolons (;).

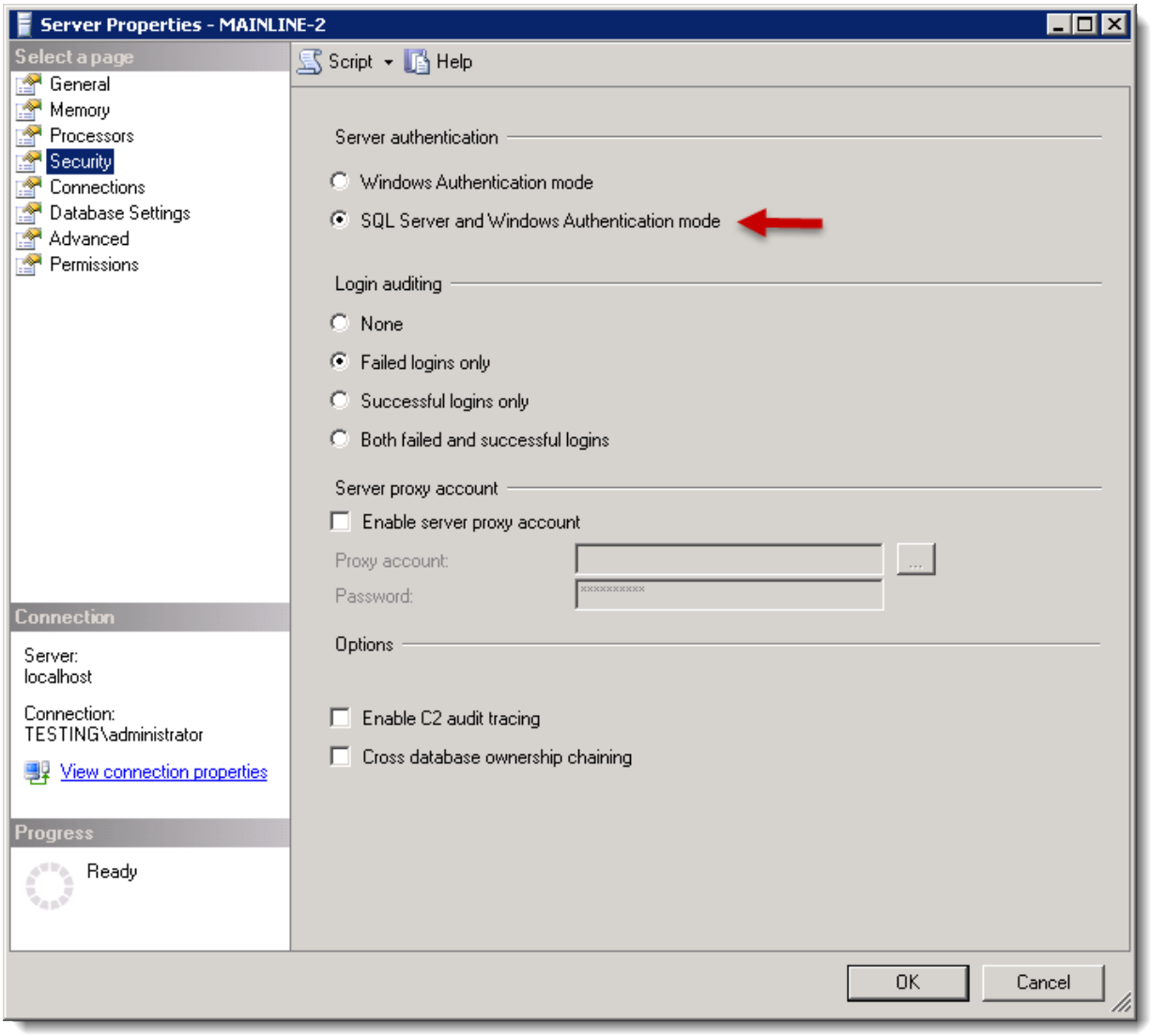
5.5 Set authentication mode

After creating a SQL Server login, you must set the Windows authentication mode property on the server.

Complete the following steps to set the authentication mode:

1. Log in to Microsoft SQL Server Management Studio.
2. Right-click on your server in the Object Explorer, and then click **Properties** in the menu.

3. On the Server Properties dialog box, click the **Security** page.



4. Under Server authentication, click **SQL Server and Windows Authentication mode**.
5. Click **OK**.

5.6 Create BCP share

Create a directory on the SQL Server in a location where the Relativity Service Account can read and write. In addition, give SQL services permissions to read from this directory. For more information about transferring data with BCPPath, see RDC transfer modes in the Desktop Client Guide or the Data Transfer Guide. Follow these guidelines for setting up this directory:

- Make sure that this directory is an actual folder, not merely a drive letter.
- Confirm that the account running SQL has access to this directory. If it does not have access to this folder, it cannot create new cases. This directory is used for temporary files during imports, exports, case creations, and dtSearch queries.

- Place this share on the drive housing the backup files for optimal performance. This share should be named BCPPath in every instance.
- If you have multiple SQL Servers, create this share on each server and use the BCPPath as the share name on all servers.
- Make sure the account running the SQL services has rights to the BCPPath. Bulk import fails when this account does not have these rights.

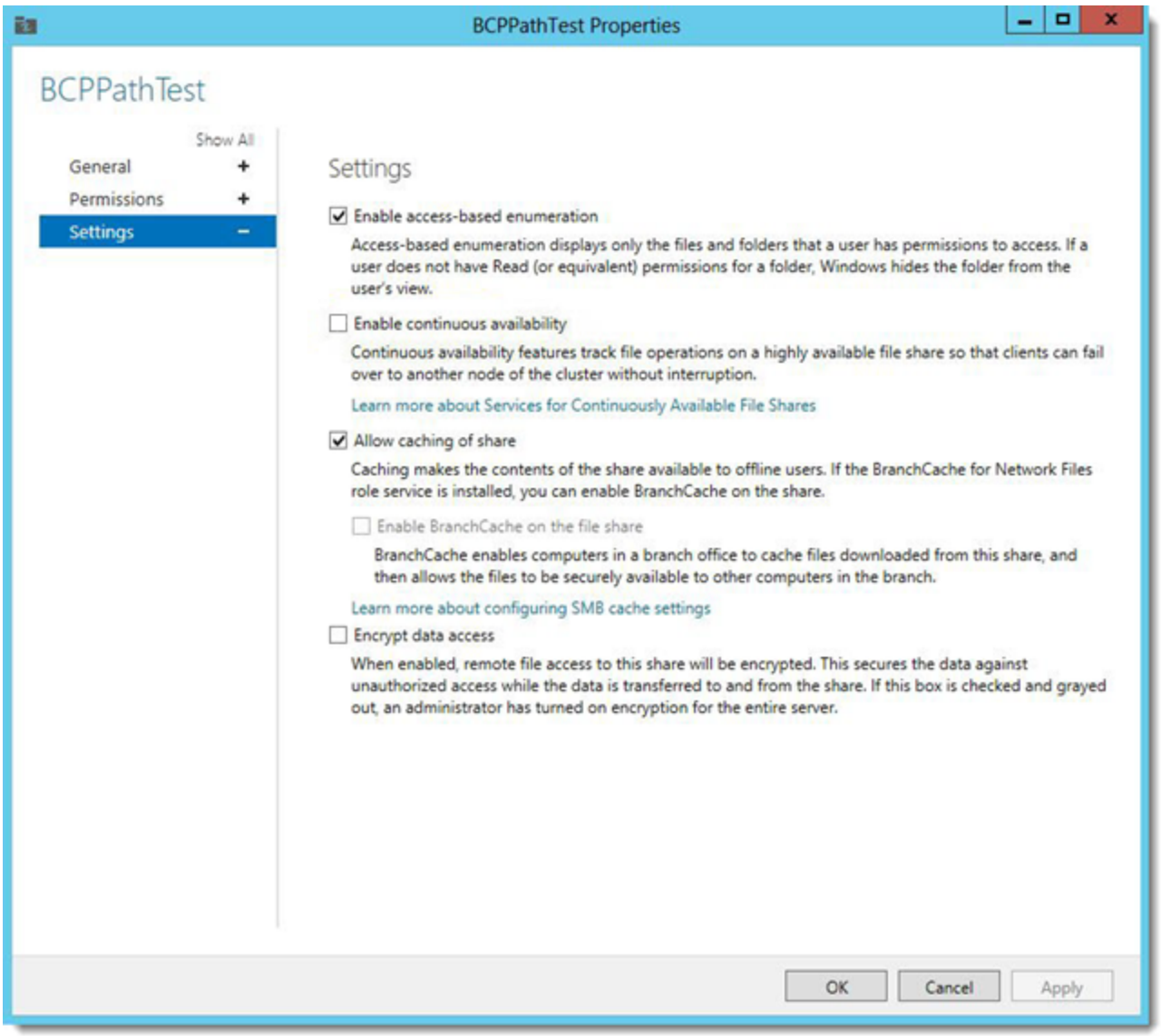
Note: Consider setting up an SQL Service Account that is a domain account with local admin rights. You should review the security requirements of your organization before setting up this account. To create a SQL Server Service account available from Microsoft, see Configure Windows Service Accounts and Permissions, http://msdn.microsoft.com/en-us/library/ms143504.aspx.

Complete the following steps to share the folder:

1. Right-click the folder and go to **Properties**.
2. Open the Sharing tab and click **Share**.
3. Enter the Relativity Service Account name, domain\account, and click **Add**.
4. Select the service account on the share list and set the Permission Level to a minimum of **Read/Write**.
5. Click **Share**.
6. When the share completes, click **Done**.
7. On the Document Properties dialog box, select the **Security** tab.
8. Verify that the Relativity Service Account has Full Control security permissions to the folder itself.

5.6.1 Update the permissions on the BCPPath file share

In the **Failover Cluster Manager**, you must update the permission settings for the BCPPath file share to ensure the case creation occurs properly on the failover cluster. When you create the BCPPath on a clustered disk, verify that **Enable continuous availability** option is not selected under **Settings** on the BCPPath Properties page. See the sample settings on the following screen shot:



Note: You must configure this setting only for SQL Server 2012, 2014, and 2016.

5.7 Optionally configure an authentication token-signing certificate

When you run the Relativity installer, it automatically adds an authentication token-signing certificate, named RelativityIdentityCertificate, to the certificate store on your primary database server. However, you also have the option to use your own certificate rather than the one created by the Relativity installer.

Note: You only need to install an authentication token-signing certificate if you do not want to use the default certificate called provided by the Relativity installer.

Before you begin installing Relativity, you may want to configure the token-signing certificate in the store on your primary database server. The other servers in your Relativity installation automatically retrieve this

certificate information from the EDDS database server, so you do not need to configure their certificates individually.

Note: For a clustered environment, you need to export a copy of your RelativityIdentityCertificate from the primary database server, and install the certificate to each database server hosting the EDDS.

5.7.1 Pre-installation steps for a token-signing certificate

You may want to install your custom token-signing certificate on the database server before you install Relativity in your environment. However, you can also complete these steps after installation.

Use this procedure to configure your certificate:

1. Obtain a signed certificate and install it on the certificate store on your primary database server.
2. Copy the thumbprint of the certificate for later use. You need this value to update the instance setting after you install Relativity. See Post-installation steps for a token-signing certificate on page 64.
3. Install Relativity on the database and other servers. For more information, see Relativity installation or Upgrading your primary SQL Server on the Relativity 2023 Documentation site.

After you install Relativity complete the steps in Post-installation steps for a token-signing certificate on page 64.

5.8 (Optional) Restrict account permissions for third party applications

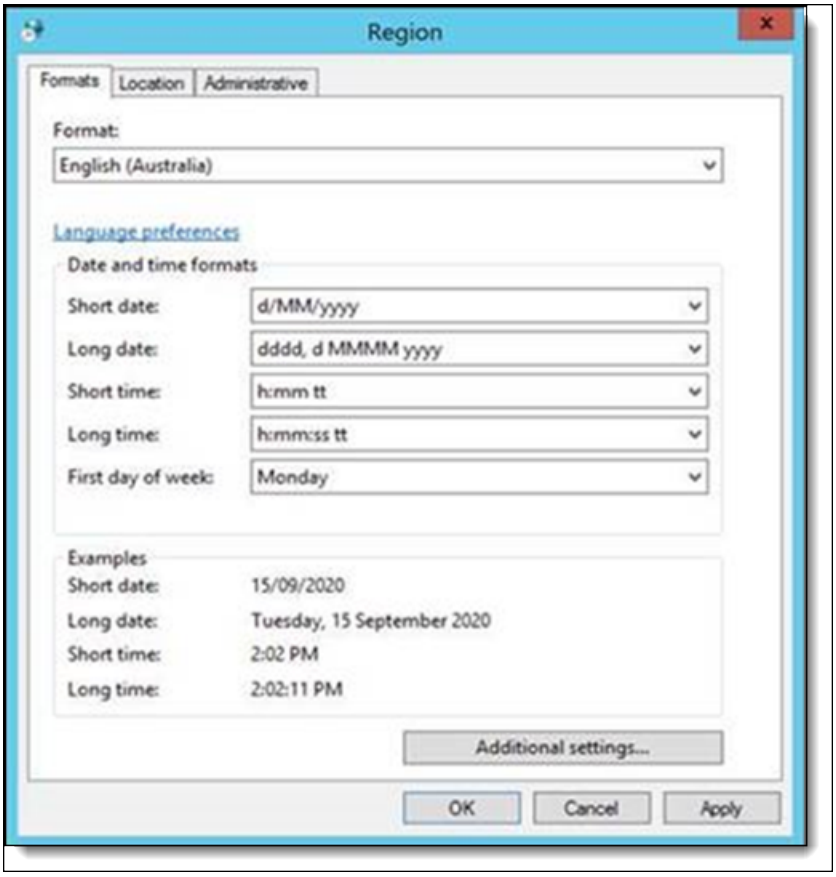
This section describes how to allow a user to execute worker operations in a user account that is independent of the default account used in Processing. This user account can be configured without admin level permissions in order to make the file conversions execute un-managed code in a highly secure fashion.

To restrict account permissions:

1. Create the desired user account on the worker machines that will be doing work for Processing.
   - The user account is not required to have permissions to access a file share or network.
   - The user account does need to be able to read and write local temporary files.
   - A single account name and password will be used for all workers in use by Invariant. This can be a local user account created on each worker.
2. Store the user account name and password in Secret Store so that Processing can access them. This information can be configured in Secret Store either through the InvariantResponse.txt file used during installation or using the Secret Store client utility.

   Note: The date format settings for this user account should be set up the same way as the Relativity service account. For example, if a service account is set up with the date format of DD/MM/YYYY, then the restricted user account must follow this format. Otherwise, applications executed under the restricted user account can be affected by mismatched date formatting. To verify your date format settings, see the regional format date and time configuration under the

workers Windows settings.



6 Web server setup

This section describes how to prepare your web server for installing Relativity. Install the following software on the web server:

- Windows Server 2022, Windows Server 2019, Windows Server 2016
- .NET 4.7.2, 4.8, or 4.8.1
- .NET 3.5

6.1 Setting IIS options

Make these updates on all web servers in your Relativity installation:

1. Install the required versions of the .NET Framework Full Profile on all web servers.
2. Configure the Legacy Unhandled Exception Policy on all web servers:
    a. Browse to the following directory on your web server: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
    b. Open the **Aspnet.config file** in a text editor.
    c. Locate the tag **<legacyUnhandledExceptionPolicy>**.
    d. Set the **enabled** attribute to **true**. This sample code illustrates the attribute that you need to update:

```
<legacyUnhandledExceptionPolicy enabled="true" />
```

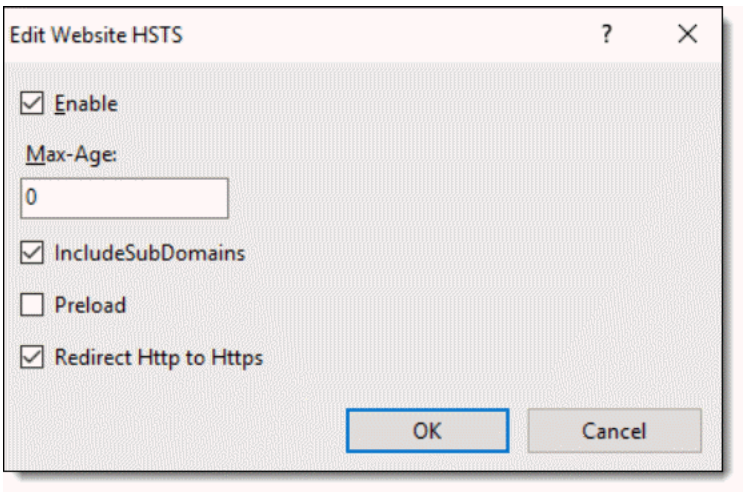
    e. Save the changes to the file.

6.1.1 Trusted Site

Make sure the certificate that the web server is using for HTTPS has been installed to the trusted root on all Relativity Servers.

6.1.2 HTTP Strict Transport Security

IIS 10.0 provides native support for HTTP Strict Transport Security (HSTS). If you enable this and check **Redirect HTTP to HTTPS** you must also configure Service Host Manager for HTTPS connections across the entire environment.



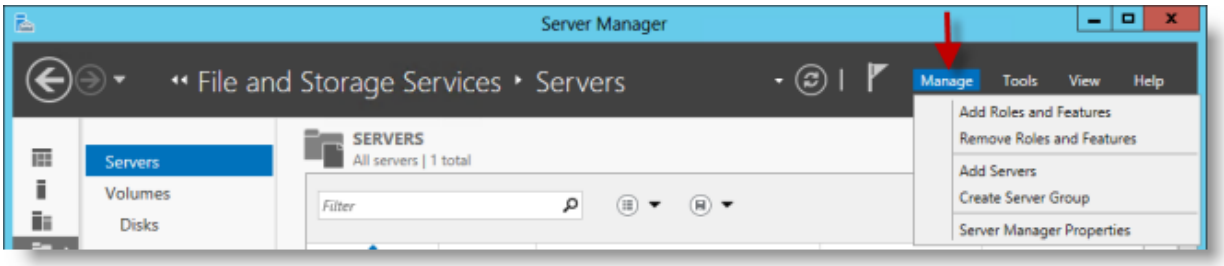
6.2 IIS role service configuration

Relativity requires that you configure several role services in the IIS. You also have the option of using a full installation of the Web Server (IIS) role.

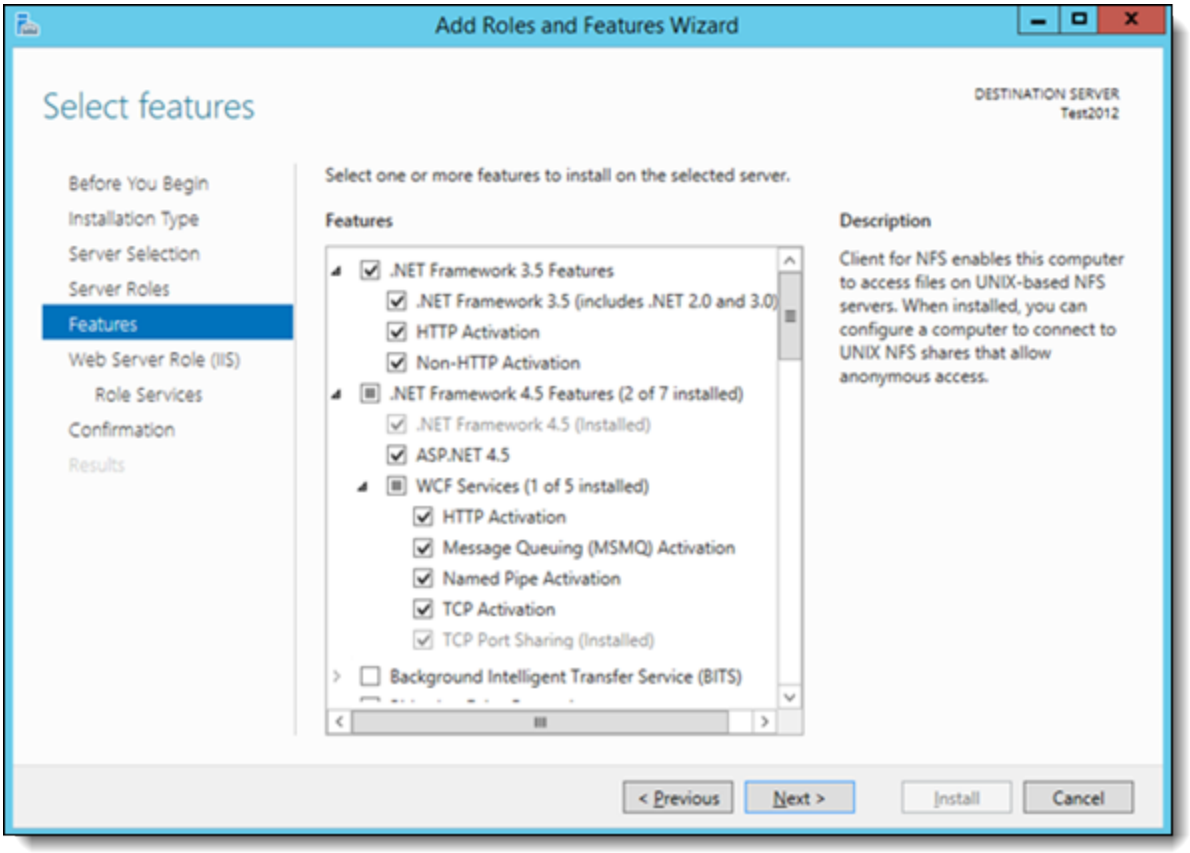
6.2.1 IIS roles on Windows Server 2022

For the IIS on Windows Server 2022, use this procedure to view the minimum role service requirements for Relativity:

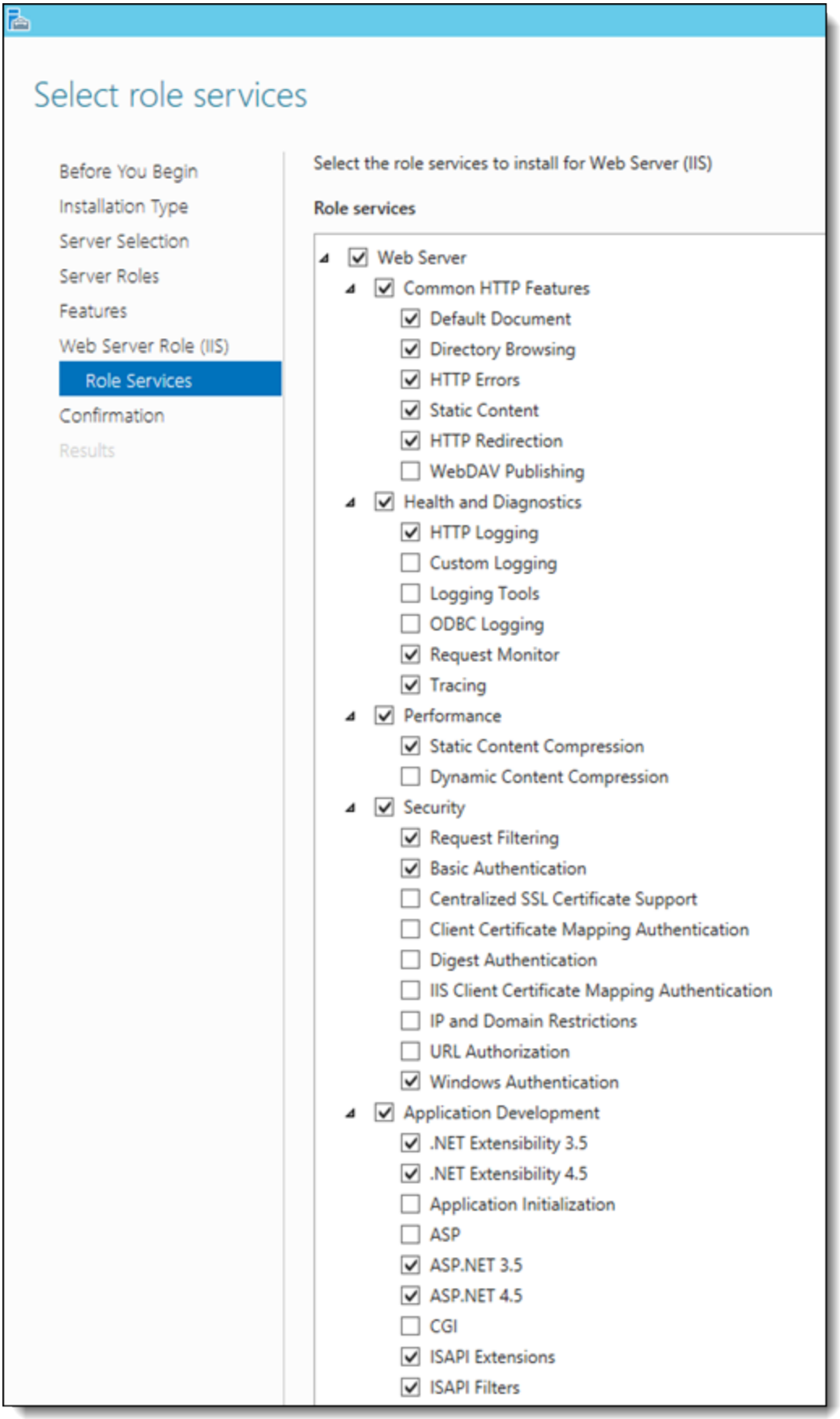
1. Open the **Server Manager** on Windows Server 2022.
2. Click **Manage** to display a drop-down menu.
3. Click **Add Roles and Features**. The Add Roles and Features wizard appears.



4. Click **Next** on the Before you begin dialog box.
5. Click **Next** on the Select installation type dialog box.
6. On the Select destination server dialog box, select **Server Roles**.
7. Select Web Server (IIS), and then click **Install**.
8. On the pop-up window, ensure that **Include management tools (if applicable)** is checked, and then click **Add Features**.
9. Click **Next** to go to the Features page.
10. Review the following illustration for Features configuration settings:



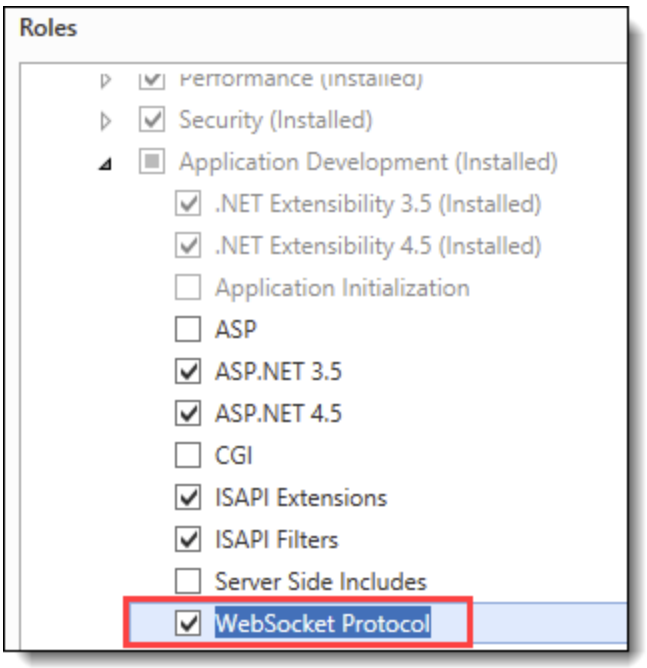
11. Click **Next** to confirm the applicable Features.
12. Click **Next** on the Web Server Role (IIS) page.
13. On the Role Service page, review the following illustration for minimum role service requirements for Relativity:


Select role services
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Request Filtering
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 4.5
Application Initialization
ASP
ASP.NET 3.5
ASP.NET 4.5
CGI
ISAPI Extensions
ISAPI Filters

14. Click **Next** to confirm the Role Services.
15. Click **Install**.

6.3 Enabling the WebSocket protocol

You might need to have the WebSocket protocol enabled on the IIS to support documentation conversion and imaging. Confirm that you have this protocol enabled on your web server. If you do not currently have it enabled on the IIS, see the WebSocket <webSocket> page on the Microsoft web site for instructions about setting it up. It is available at this URL: https://www.iis.net/configreference/system.webserver/websocket.



6.4 Configuring log file options

If you enabled logging on the IIS, you can avoid performance and other issues by limiting the size of log files, as well as the number of trace files stored on the IIS. This section describes how to configure these features in your environment for optimum performance.

6.4.1 Windows log file options

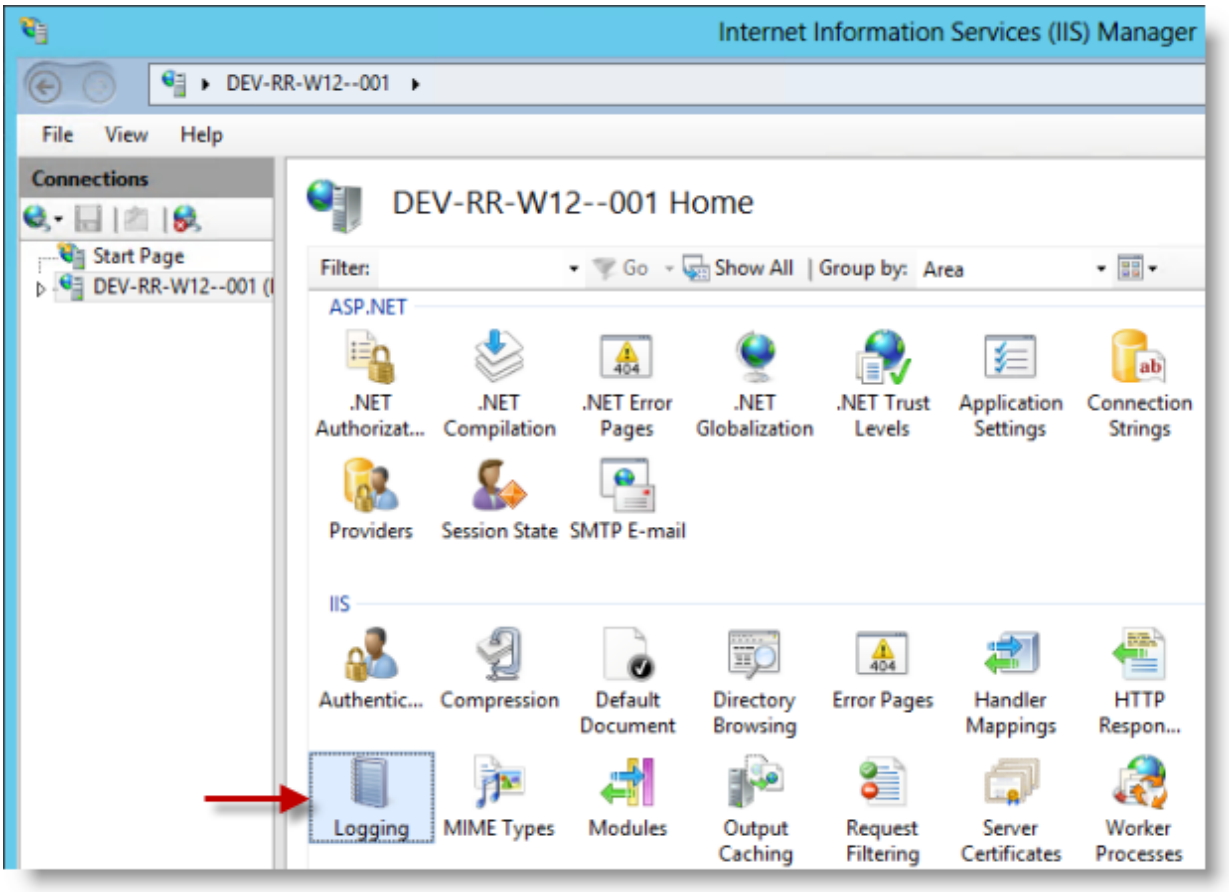
Use the instructions in this section to configure logging settings for Windows.

6.4.1.1 Setting file size for IIS requests log

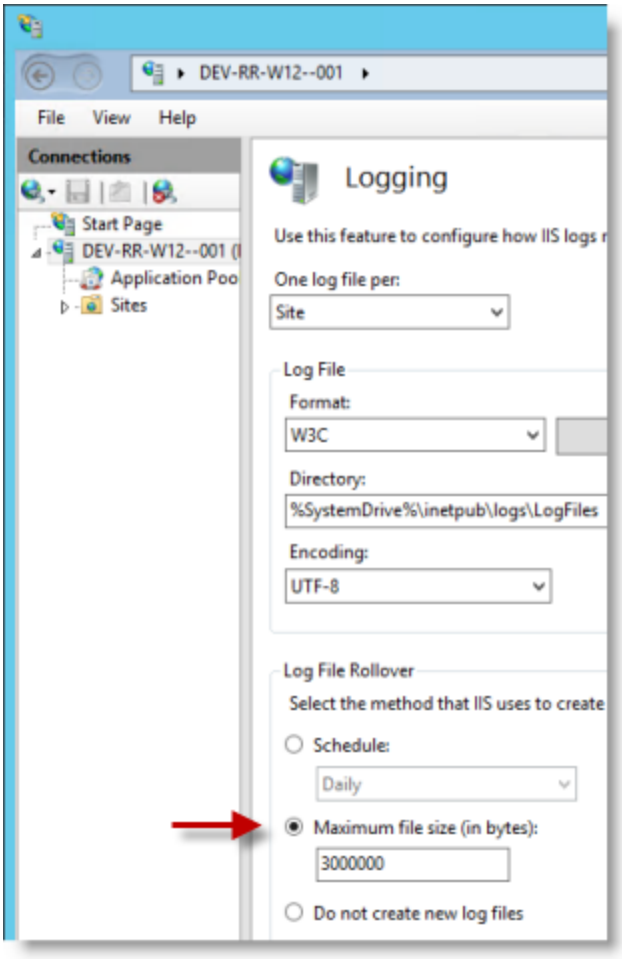
Logging is a default role installed on the IIS and enabled in most environments. Use the following instructions to set the maximum size for the log files:

1. Open the **Server Manager**.
2. On the **Tools** menu, select **Internet Information Services (IIS) Manager**.
3. Expand the server node to display the Features View.

4. Double-click the **Logging** icon to display the Logging page.



5. Update the maximum file size for your environment if necessary. The following illustration shows the maximum file size used to restrict the log files from growing larger than 3 MB.

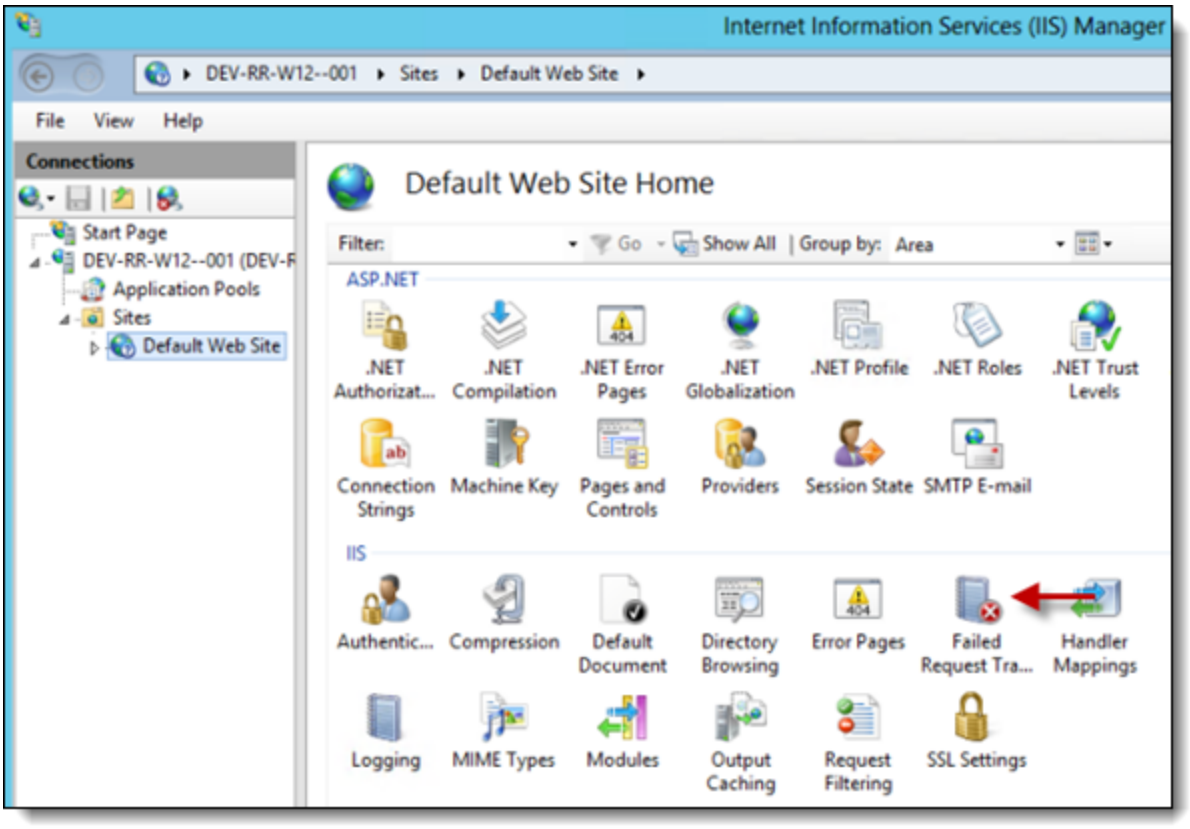


6.4.1.2 Setting the file size for failed trace logging

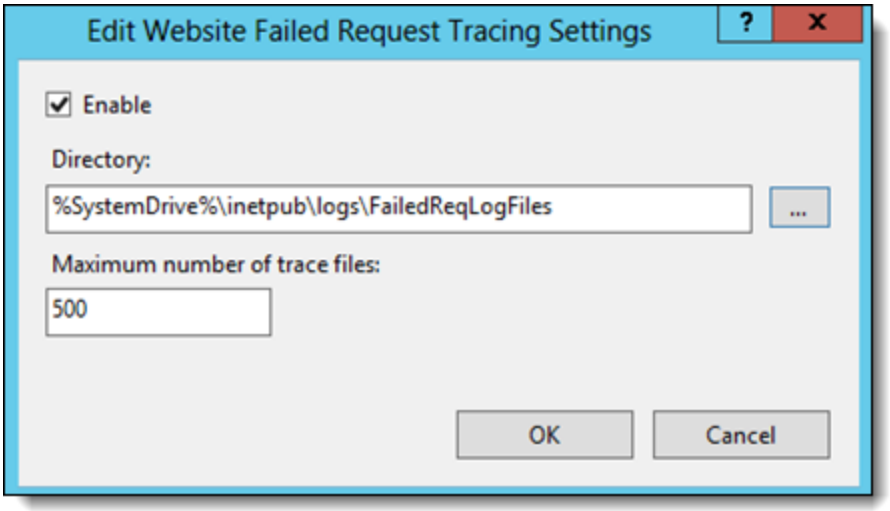
If you manually installed the failed trace logging through the Role Services on your IIS, complete the following steps to set the maximum number trace files stored.

1. Open the **Server Manager**.
2. On the **Tools** menu, select **Internet Information Services (IIS) Manager**.
3. Expand the server node to display the Features View.
4. Highlight the **Default Web Site**.

5. Double-click the **Failed Request Tracing** icon to display the Failed Request Tracing Rules page.



6. Right-click on the rules to display a pop-up menu, and then click **Edit Site Tracing**.



7. Update the value in the **Maximum number of trace files** box. This value should be set no higher than 500.

6.5 Configuring SSL on a web server

Before installing Relativity, we recommend that you set up SSL on the IIS for your Relativity instance. This configuration provides added security for the communication between the web server and the browser on a client computer. Your browser uses this secure connection to verify that it is communicating with the Relativity server. It also provides additional protection against the theft of cookies used to maintain a session between the browser and the server.

Note: You are not required to configure SSL on the web server hosting Relativity. If you decided not to use HTTPS in your environment, you must set the CookieSecure instance setting to **False** before logging in to Relativity, or you receive an error message. You can also complete this setup after installation but before logging in to Relativity. For more information, see Instance setting table on the Relativity 2023 Documentation site.

The process for configuring SSL on your web server includes these steps:

- Obtaining a certificate for your web server below
- Installing a certificate on your web server below
- Configuring HTTPS site bindings below
- Updating the SSL setting on the IIS on the next page
- Setting up HTTPS for Service Host Manager on page 33

6.5.1 Obtaining a certificate for your web server

To set up SSL on your web server, you must obtain a certificate, which is digital identification document used by the browser to authenticate the server. A server certificate contains detailed identification information, such as the name of the organization affiliated with the server content, the name of the organization that issued the certificate, and a public key used to establish an encrypted connection. It provides a way for the browser to confirm the authenticity of web server content and the integrity of the SSL-secured connection before transmitting information.

You can obtain a certificate from Microsoft Certificate Services or from a mutually trusted CA. A CA confirms your identity to ensure the validity of the information contained in your certificate. In general, you must provide your name, address, organization, and other information.

Note: If you do not issue your server certificate through Microsoft Certificate Services, a third-party certification authority must approve your request and issue your server certificate.

6.5.2 Installing a certificate on your web server

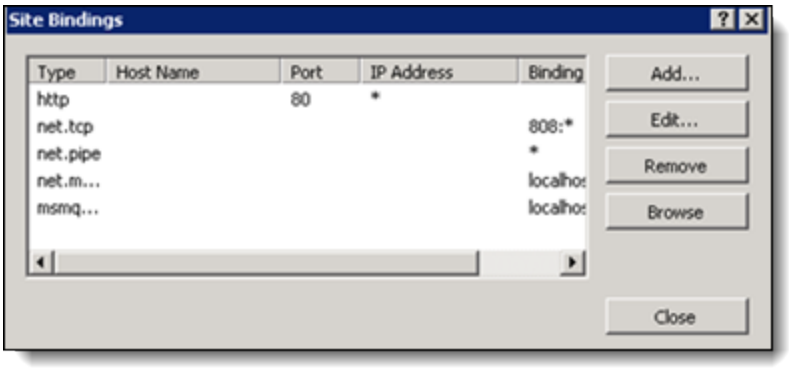
After obtaining an SSL certificate, install it in the certificate store on your web server. For more information, see Import or export certificates and private keys on the Microsoft Windows website.

6.5.3 Configuring HTTPS site bindings

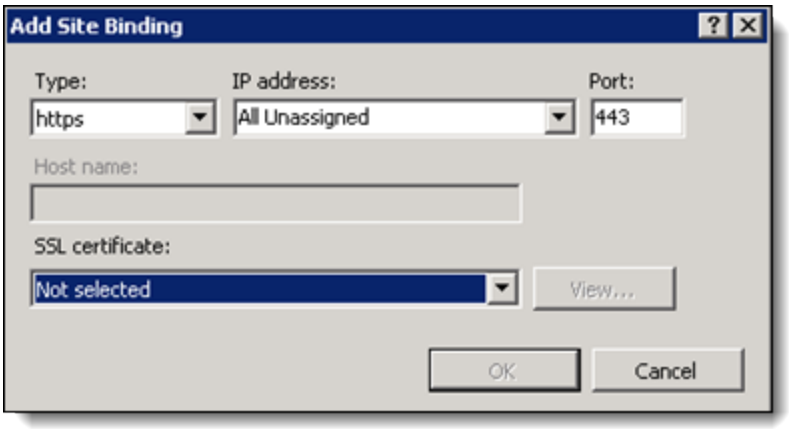
The IIS resets after you configure the HTTPS site bindings and update the SSL setting as described in the following section.

Use these steps to configure HTTPS site bindings:

1. Open the IIS Manager.
2. In the IIS Manager Connections pane, expand **Sites**.
3. Right -click on the **Default Web Site**, and then click **Edit Bindings** on the menu.



4. Click **Add** to display the Add Site Binding dialog box.



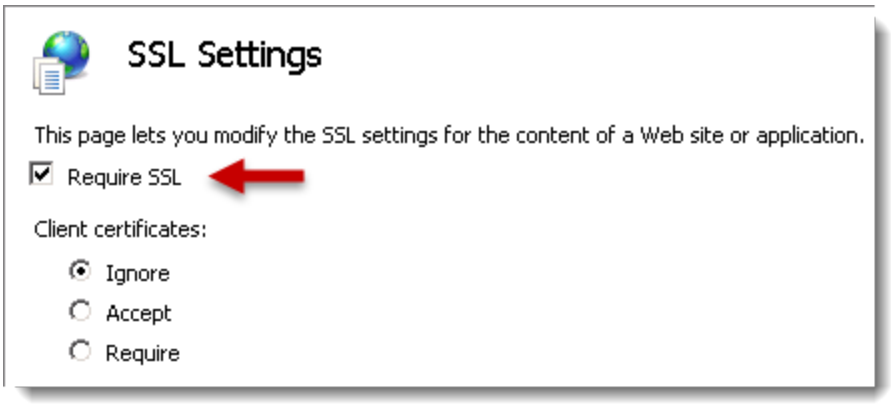
5. In the **Type** drop-down menu, select **https**.
6. In the **SSL certificate** drop-down menu, select your certificate.
7. Click **OK**. You now see **https** listed in the Type column.
8. Click **Close**.

6.5.4 Updating the SSL setting on the IIS

Use the following steps to configure SSL settings on the IIS:

1. Open IIS Manager.
2. Navigate to the Relativity virtual directory, and then select **Relativity**.
3. Double-click **SSL Settings**.

4. Select **Require SSL**.



5. Click **Apply** in the Actions pane.

6.5.5 Setting up HTTPS for Service Host Manager

You also need to enable HTTPS for the Service Host Manager service, which must run on all web and agent machines that use Relativity. For a detailed overview of this service and configuration steps, see Service Host Manager on the Documentation 2023 site.

7 Agent server setup

An agent server performs background processing. It requires the following software:

- Windows Server 2022, Windows Server 2019, Windows Server 2016
- .NET 4.7.2, 4.8, or 4.8.1
- .NET 3.5

In most environments, the Relativity installer automatically enables Microsoft DTC and HTTP activation. You may require the following instructions if you need to troubleshoot your installation or if its configuration requires you manually complete these steps.

7.1 Enabling Microsoft DTC

You must enable Microsoft DTC on the Agent server along with the following configuration changes:

1. Add the **Application Server** role and select **Distributed Transactions**. Select **Incoming Remote Transactions** and **Outgoing Remote Transactions**.

   Note: As of Windows Server 2016 the Application Server role has been deprecated. Use the Distributed Transaction Coordinator, if it is not present on your machine download the Microsoft Distributed Transaction Coordinator (MSDTC) 2016 Management Pack for Microsoft System Center located here, download.

2. Type **dcomcnfg** on your Start menu , and then press **Enter** to open Component Services.
3. Expand **Component Services** > **Computers** > **My Computer** > **Distributed Transaction Coordinator**.
4. Right-click **Local DTC**, and then click **Properties**.
5. Click the **Security** tab.
6. Select the following check boxes:
   - Allow Remote Clients
   - Allow Inbound
   - Allow Outbound
7. Click **Apply**.
8. Click **Yes** to restart the MSDTC service.
9. Click **OK**.

7.2 Enabling HTTP activation

You must enable HTTP activation on your agent server as follows for Microsoft Windows Server 2012 R:

1. Click **Start** > **Administrative Tools** > **Server Manager**.
2. In the Server Manager Dashboard, click **Manage** > **Add Roles and Features**.

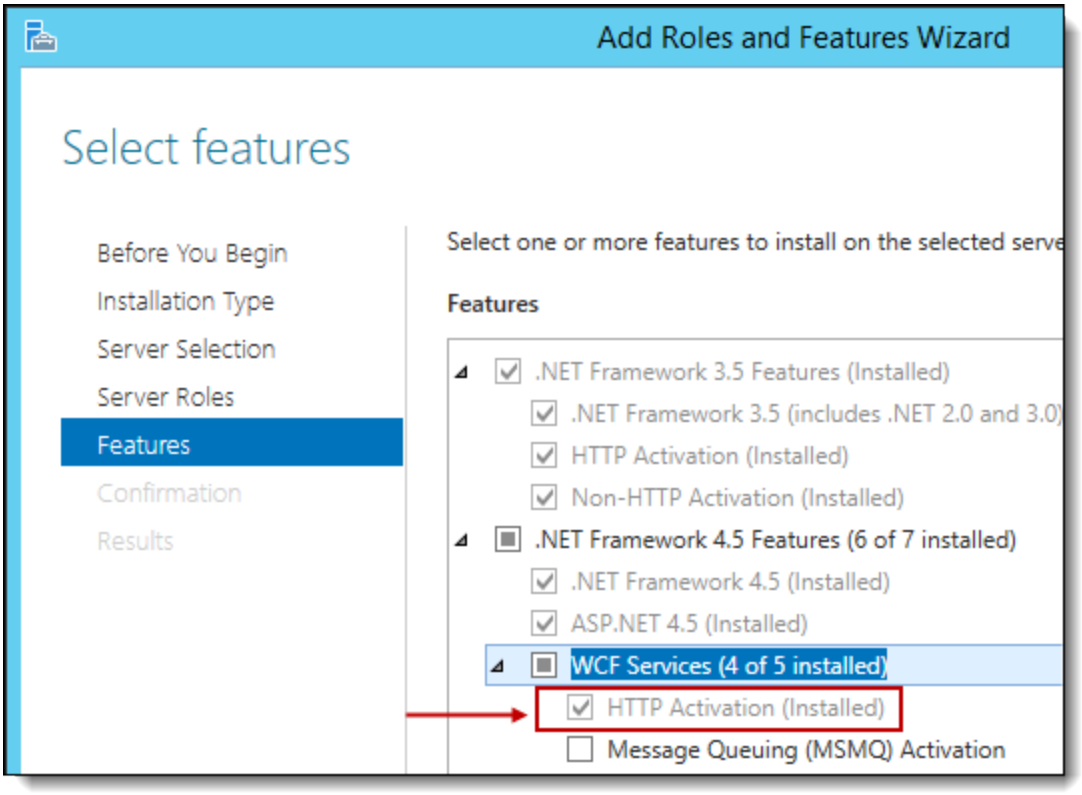
3. In the Add Roles and Features, choose **Server Selection**.
4. Select the server running the agents is selected in the **Server Pool** box, and then click **Next**.
5. Click **Features** in the sidebar of the wizard.
6. Select the following check boxes in the **Feature** box:
   - .NET Framework 3.5 Features

     Note: Ensure all check boxes below .NET Framework 3.5 Features are checked.

   - .NET Framework 4.5 Features

     Note: Ensure all check boxes below .NET Framework 4.5 Features are checked.

   Make sure that **HTTP Activation** is installed and selected when you expand each of these sections.
7. Install any missing features are necessary.
8. When the installation is complete, expand **.NET Framework 3.5 Features** and **.NET Framework 4.5 Features** to verify that **HTTP Activation** is installed.



7.3 Message broker options

Relativity requires that you install and configure RabbitMQ before you install or upgrade Relativity.

RabbitMQ is the most widely deployed open source message broker with more than 35,000 production deployments. Additionally, RabbitMQ is fully supported on the latest Windows operating systems, features

full support for TLS 1.2, and includes superior monitoring, administration, and performance capabilities. For more information, see the RabbitMQ website. The process for installing and configuring RabbitMQ includes these steps:

Use the following guidelines to optimize the RabbitMQ installation:

- **RabbitMQ installation**—for a typical installation, install RabbitMQ on a server or VM that is accessible throughout your Relativity instance. Must be accessible by all Web and Agent servers. Minimum of 2 GB of RAM, 2 CPU cores, and 10 GB of free disk space. Recommend 4-8 GB of RAM, 4 CPU cores, 40 GB of free disk space. Additionally, in environments where large batch jobs may be sent to RabbitMQ, such as mass conversions with greater than 25,000 documents, disk IO may become a factor in performance. Relativity recommends RabbitMQ's mnesia database be located on a drive with less than 15 ms latency and at least 30 mb/sec read/write speeds. For information about configuring RabbtitMQ's directories, see the RabbitMQ website.
- **Clustering and High Availability**—a typical Relativity installation requires only a single RabbitMQ server. However, high availability can be achieved by deploying multiple RabbitMQ servers in a cluster. For more information, see Setting up RabbitMQ for high availability.

Before installing RabbitMQ, complete the following prerequisites:

- If you wish to have RabbitMQ and Relativity communicate over TLS, see Certificate requirements for RabbitMQ.
- Ensure that you have the prerequisites for RabbitMQ. You need to meet these requirements to set up your cluster correctly.
- For a typical installation, identify the server or VM where you want to install RabbitMQ. To install RabbitMQ on multiple hosts, identify the servers or VMs for this purpose. The cluster can have any number of servers, but three servers is recommended. For more information, see Best practices for RabbitMQ.
- Relativity agent and web servers must be able to communicate with the cluster over the following ports:
  - TCP: 5672 (non TLS configurations) and/or 5671 (TLS configurations)
  - HTTP(S): 15672 (non TLS configurations) and / or 15671 (TLS configurations)
- Install Erlang and RabbitMQ
- Configure RabbitMQ

Installing Erlang and RabbitMQ

Note: The RabbitMQ 3.10 series became unsupported by the vendor on 12/31/2023. We cannot guarantee compatibility of RabbitMQ 3.10.x with Server 2022 or Server 2023 after 12/31/2023 and recommend upgrading to a supported version of RabbitMQ. For details on RabbitMQ's version policies, see RabbitMQ versions. If you are upgrading to 3.12.x, review the RabbitMQ upgrade overview beforehand to avoid issues during the upgrade process.

Note: You must use RabbitMQ version 3.11.x, or 3.12.x and a compatible version of Erlang; however, you cannot currently run version 3.12.x with any supported version of Erlang above v25.x. Ensure that you're using the 64-bit version of Erlang, or else the system will be constrained to 2GB of memory.

Complete the following steps to install Erlang and RabbitMQ:

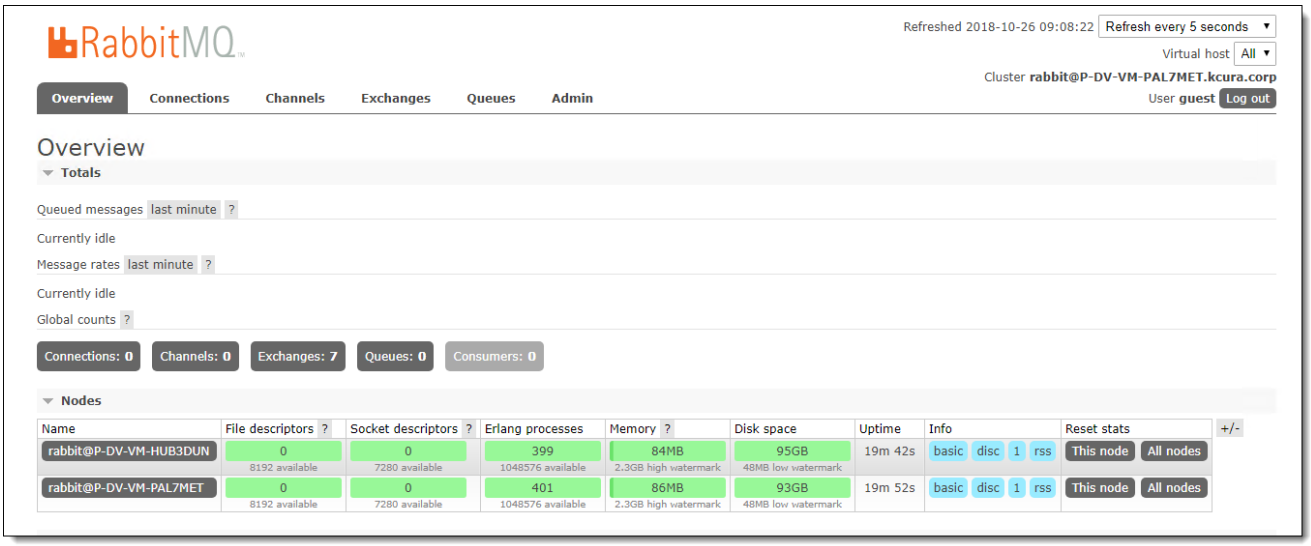
1. Download and install the latest version of Erlang that is compatible with RabbitMQ 3.11.x or 3.12.x. With how frequently both RabbitMQ and Erlang upgrade their products, we recommend you review the RabbitMQ-Erlang version requirements here. Be sure to run the installer in Administrator mode.
2. Complete the steps in the Installation Configuration Wizard.
3. When the installation process completes, click **Close**. You have now installed Erlang.
4. Download and install RabbitMQ 3.11.x or above here. Be sure to run the installer in Administrator mode.
5. Complete the steps in the Installation Configuration Wizard.
6. When the installation process completes, click **Finish**. You have now installed RabbitMQ.
7. Search **RabbitMQ Command Prompt (sbin dir)** on your machine. Open the RabbitMQ command prompt.
8. In the RabbitMQ command prompt, run the following command:

   ```
   rabbitmq-plugins enable rabbitmq_management
   ```

   This command enables the management plugin, management UI, and management API. Relativity's RabbitMQ provider requires the management API to perform certain operations.
9. Restart the RabbitMQ Windows Service.
10. Open a browser and navigate to **http://localhost:15672/**
11. Log in with the following credentials:
    - **Username**—guest
    - **Password**—guest

Note: The default user guest can only log in from local host.

You should see an overview and your server displaying various green statistics.



Configuring RabbitMQ

Note: RabbitMQ requires .NET 3.5

After installing Erlang and RabbitMQ, you need to complete the following steps to configure RabbitMQ:

- Create a new virtual host to be used by Relativity
- Create a new user to be used by Relativity

Create a new virtual host to be used by Relativity
Complete the following steps to create a new virtual host to be used by Relativity:

Note: Virtual hosts in RabbitMQ are analogous to Namespaces in Azure Service Bus.

1. Open a browser and navigate to **http://localhost:15672/**
2. Log in using the following credentials:
   - **username**—guest
   - **password**—guest

   Note: The default user guest can only log in from local host.
3. Click **Admin** > **Virtual Hosts**.
4. Expand **Add a new virtual host**.
5. Enter a name for a virtual host to be used in the Name field. For example, Relativity.
6. Click **Add virtual host**.

Create a new user to be used by Relativity
Complete the following steps to create a new user to be used by Relativity:

1. Open a browser and navigate to **http://localhost:15672/**
2. Log in using the following credentials:
   - **username**—guest
   - **password**—guest

   Note: The default user guest can only log in from local host.
3. Click **Admin** > **Users**.
4. Expand **Add users**.
5. Enter a user name and password in the Username and Password fields.
6. Select **Admin**, under the Tags field.
7. Click **Add user**.
8. Expand **All users**.
9. Click on the user you just created.

10. Expand **Permissions**.
11. Select the virtual host you created in the previous steps in the Virtual Host drop-down menu.
12. In the Configure regexp, Write regexp, and Read regexp fields ensure the value is set to **.*** .
13. Click **Set permission**, the permissions now display under current permissions.

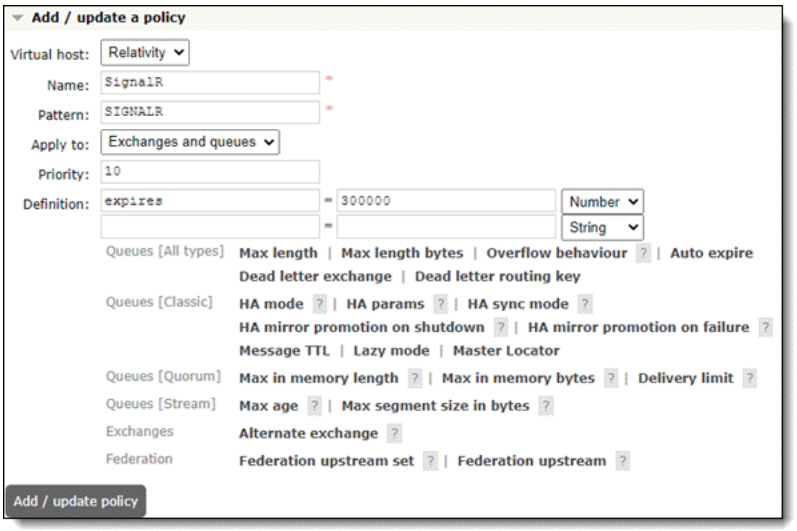
Note: For advanced deployment and configuration options, see the RabbitMQ website.

Adding a new RabbitMQ policy for SignalR

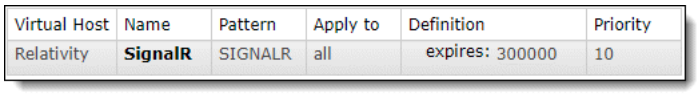
A SignalR policy ensures all SignalR queues are deleted after five minutes without a consumer, rather than the default setting of one hour. In addition, high availability policies are not applied to SignalR queues, limiting the performance impact of many queues.

To add a SignalR policy:

1. Open your browser and navigate to **http://localhost:15672/**.
2. Log in using the following credentials. The default user guest can only log in from local host.
   - **username**: guest
   - **password**: guest
3. Click **Admin > Policies**.
4. Expand the **Add / update a policy** section.
5. Select a virtual host to be used, specifically **Relativity**.
   - **Name**—SignalR
   - **Pattern**—SIGNALR
   - **Priority**—10
   - **Definition**—expires = 300000 | Number



6. Click **Add / update policy** to save the policy. Confirm the policy has been saved in the following format:



Virtual Host	Name	Pattern	Apply to	Definition	Priority
Relativity	**SignalR**	SIGNALR	all	expires: 300000	10

Configure RabbitMQ For TLS

Note: TLS is optional and controlled by the TLSENABLED response file input and EnableTLSForServiceBus instance setting.

In order to setup RabbitMQ to use TLS for secure communication you must update the server side configuration of RabbitMQ. To enable SSL communication with the RabbitMQ server in Relativity, you must also update the instance setting. The following section documents the minimum requirements for using RabbitMQ over TLS with Relativity. For complete documentation of RabbitMQ with TLS, see the RabbitMQ website.

Note: Relativity only supports TLS 1.0, 1.1, and 1.2. SSL3 is NOT supported. When TLS is enabled for Relativity the ports 5671 and 15671 must be open and available for use by RabbitMQ.

1. Before you begin, you need a certificate. For more information, see Certificate requirements for RabbitMQ.
2. Navigate to your RabbitMQ directory. On Windows, this defaults to **C:\Users\<user>\AppData\Roaming\RabbitMQ**, <user> is the user account used to install the service.
3. Depending on the version of RabbitMQ, download the **advanced.config** file. The slashes in the advanced.config file must be forward slashes (/); entering backward slashes will result in an error.

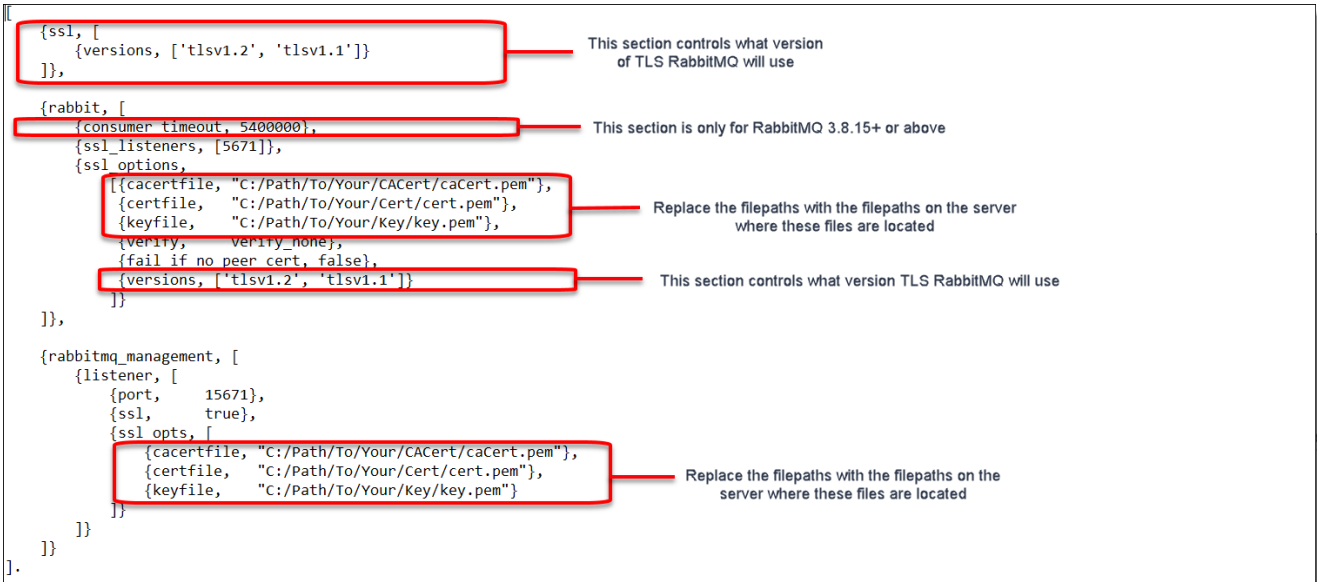
Below RabbitMQ 3.8.15+	**RabbitMQ 3.8.15+ or above**
advanced.config	advanced.config

```
[
    {ssl, [
        {versions, ['tlsv1.2', 'tlsv1.1']}
    ]},

    {rabbit, [
        {consumer_timeout, 5400000},
        {ssl_listeners, [5671]},
        {ssl_options,
            [{cacertfile, "C:/Path/To/Your/CACert/caCert.pem"},
             {certfile,   "C:/Path/To/Your/Cert/cert.pem"},
             {keyfile,    "C:/Path/To/Your/Key/key.pem"},
             {verify,     verify_none},
             {fail_if_no_peer_cert, false},
             {versions, ['tlsv1.2', 'tlsv1.1']}
            ]}
    ]},

    {rabbitmq_management, [
        {listener, [
```

```
            {port,     15671},
            {ssl,      true},
            {ssl_opts, [
                {cacertfile, "C:/Path/To/Your/CACert/caCert.pem"},
                {certfile,   "C:/Path/To/Your/Cert/cert.pem"},
                {keyfile,    "C:/Path/To/Your/Key/key.pem"}
            ]}
        ]}
    ]}
].
```

Note: Before editing the **advanced.config** file, ensure the certificate files are converted into the .PEM format. For more information, see Convert certificates to PEM Format.

The below image is an example of the **advanced.confg** file setup for TLS utilizing a self-signed certificate:



Notes:

- In the advanced.confg file, ports 5671 and 15671 are specified in the file and are required for Relativity.
- The settings *verify* and *fail_if_no_peer_cert* are used for Client Certificates. Relativity does not support Client Certificates with RabbitMQ at this time, and requires username password authentication. As a result, **verify** must be set to *verify_none*, and **fail_if_no_peer_cert** must be set to *false*.
- For more information on how to configure RabbitMQ for TLS, see TLS Support and Configuring Cipher Suites.

Setting up RabbitMQ for high availability.
In order to deploy RabbitMQ in a high availability configuration, create a cluster of servers, nodes, hosting RabbitMQ. Once configured, Relativity can continue to function in the event that any individual RabbitMQ node goes down. While this section provides the basic steps necessary set up a RabbitMQ cluster, clustering in RabbitMQ supports many different configurations and network topologies. For more information, see clustering on the RabbitMQ website.

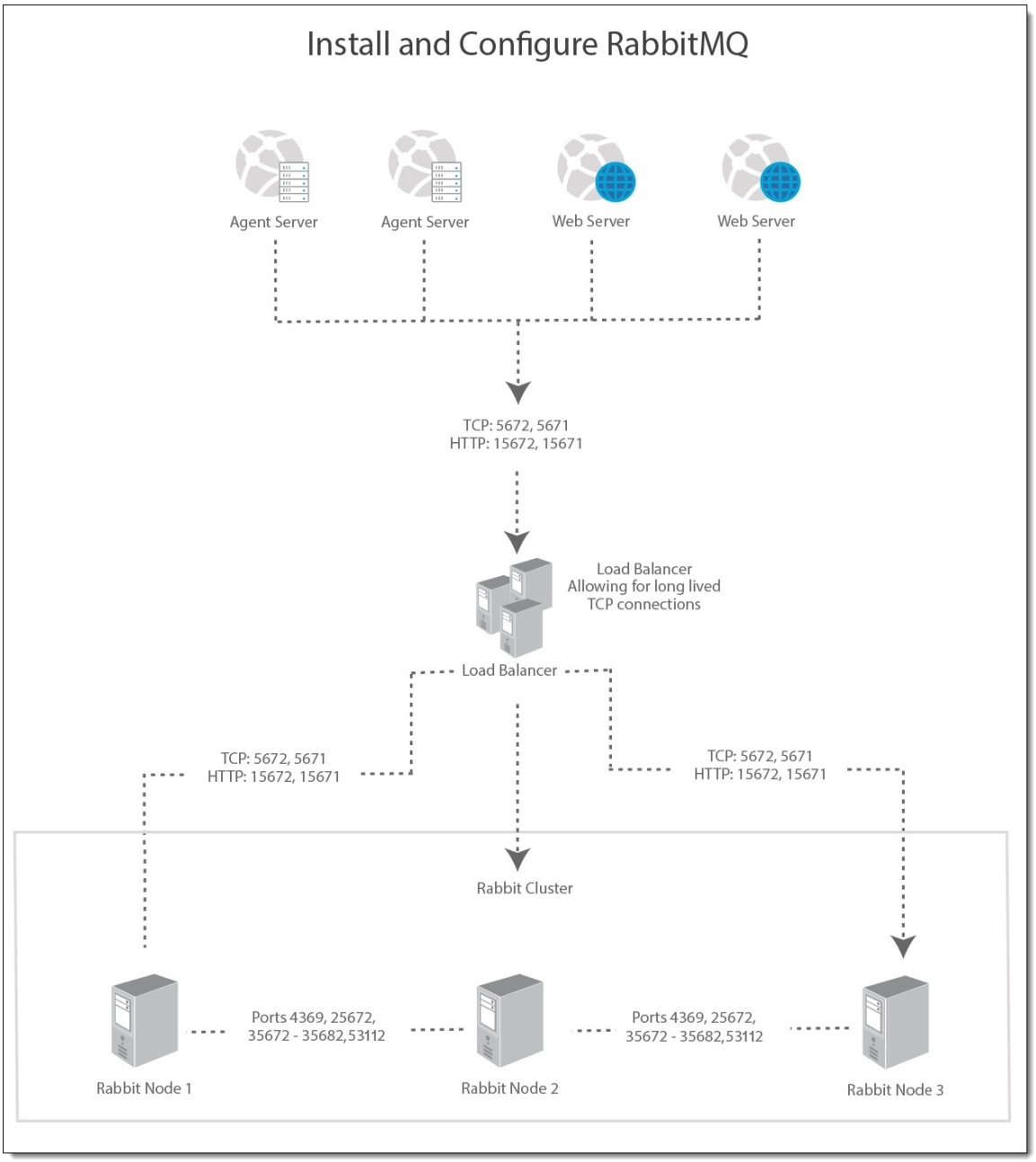
Optional configuration topics not included in this section include:

- Alternative cluster formation techniques
- TLS for inter-node (clustering) traffic

Planning the cluster

To achieve high availability, your cluster must include at least two nodes, servers, hosting RabbitMQ. We recommend having at least three nodes. It is highly recommended that all nodes communicate over a reliable LAN. A reliable network connection between nodes is important for avoiding partitions. For more information, see partitions on the RabbitMQ website.

- Review the port requirements, see ports on the RabbitMQ website.
- Relativity agent and web servers must be able to communicate with the cluster over the following ports:
  - TCP: 5672 (non TLS configurations) and / or 5671 (TLS configurations)
  - HTTP(S): 15672 (non TLS configurations) and / or 15671 (TLS configurations)
- Options for handling node failures:
  - Manual Fail Over
    - No special network configuration required.
    - Manual updates to relativity configuration and service restarts needed in the event of node failure.
  - Load Balancer/Proxy
    - Configure Relativity's service bus instance settings to connect to a load balancer for the cluster.
    - HTTP and TCP traffic should be load balanced across at least two nodes in the cluster.
    - The load balancer must allow for long lived TCP connections to avoid a degradation in performance.
    - In the event of a node failure, Relativity processes connected to the node will attempt to reconnect until successful allowing the load balancer to the direct the connection to a healthy node.
    - Round Robin or other more advanced routing techniques can be used.
  - Dynamic DNS
    - Configure Relativity to connect to a domain name which is dynamically routed to the RabbitMQ nodes with a very short time to live.
    - Effectively a Round Robin Load Balancer.



Creating the cluster

Note: The following steps assume a windows server based RabbitMQ deployment.

1. Before forming a cluster, install Erlang and RabbitMQ on each server you which to include in the cluster. For more information, see Installing Erlang and RabbitMQ.
2. Obtain an Erlang cookie to be used by the cluster. This cookie is used for inter-node authentication and is randomly generated on start-up if not present. For a cluster, the values much match on every host. For more information, see the RabbitMQ website.

1. Log into the host server.
2. Navigate to **C:\WINDOWS\system32\config\systemprofile**.
3. Copy the **.erlang.cookie** file to a central location. This will serve as the shared cookie for the cluster.

3. For each host server:
    1. Run **rabbitmqctl stop_app** in the RabbitMQ command prompt.

    Note: If you run into issues while running RabbitMQ commands, trying restarting the RabbitMQ windows service. If you still see issues, try rebooting the server.

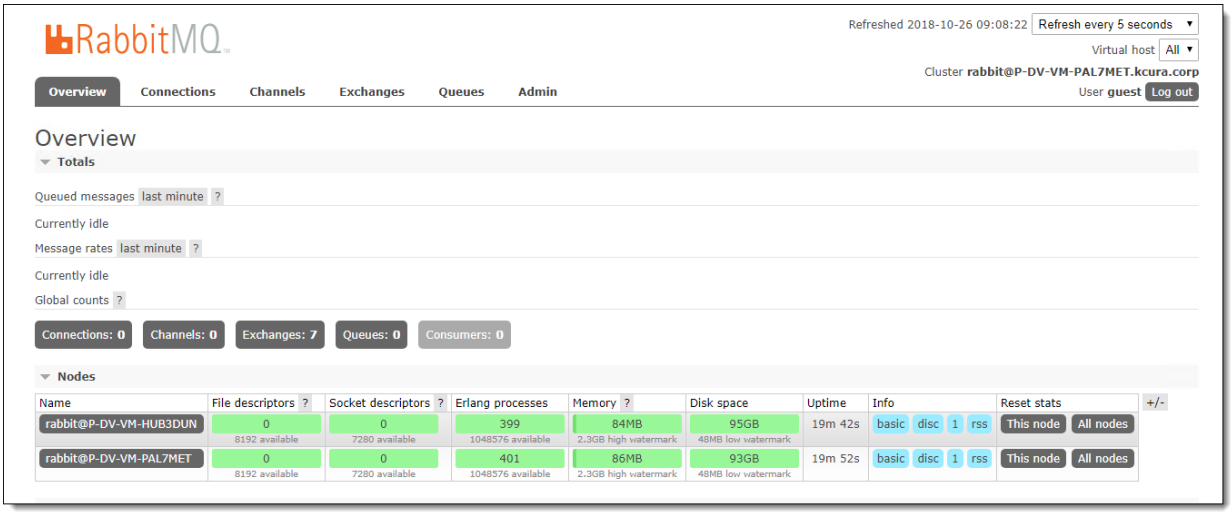
    2. Run **rabbitmqctl reset**.
    3. Replace the **.erlang.cookie** file at **C:\WINDOWS\system32\config\systemprofile** with the one you copied to a central location.
    4. Run **rabbitmqctl join_cluster rabbit@%ComputerNameOfHostThatCookieWasCopiedFrom%**.

    Note: Do not use the FQDN of the server or the command will error without the RABBITMQ_USE_LONGNAME setting in RabbitMQ set. Also, the host name is case sensitive.

    5. Replace the .erlang.cookie file at **C:\Users\%USERNAME_THAT_INSTALLED_RABBITMQ%\.erlang.cookie** with the one you copied to a central location.
    6. Open RabbitMQ command prompt.
4. Run **rabbitmqctl cluster_status** on any host in the RabbitMQ command prompt and confirm the output for nodes and running nodes contains all hosts.

    Note: Ensure the management plugin is enabled on each node. For more information, see Installing Erlang and RabbitMQ.

5. Verify the status of the cluster on the RabbitMQ management page.



Notes:

- If any of the nodes are missing, log into that node and complete the steps found under Creating a cluster.
- If any of the nodes are yellow, this likely means the management plugin has not been enabled. Log in to that host and run **rabbitmq-plugins enable rabbitmq_management** in the RabbitMQ command prompt. For more information, see Installing Erlang and RabbitMQ.

Configuring the cluster

By default, each queue and exchange only exists on a single node in the cluster. This means that those queues and exchanges are no longer be available if those nodes go down. For high availability, it is also necessary to ensure the individual queues and exchanges on the cluster are mirrored across multiple nodes. For more information, see the RabbitMQ website.

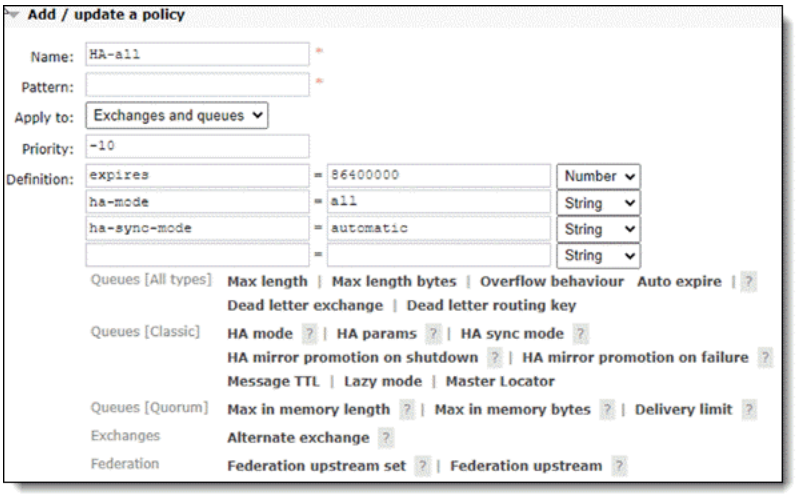
Note: If your cluster has more than three nodes, it may be beneficial to configure your queues and exchanges to be mirrored across an exact number of nodes in order to limit internode communication.

The following steps can be used to configure all queue and exchanges to be mirrored across all nodes.

1. Open a browser and navigate to **http://localhost:15672/**
2. Log in using the following credentials:
   - **username**—guest
   - **password**—guest

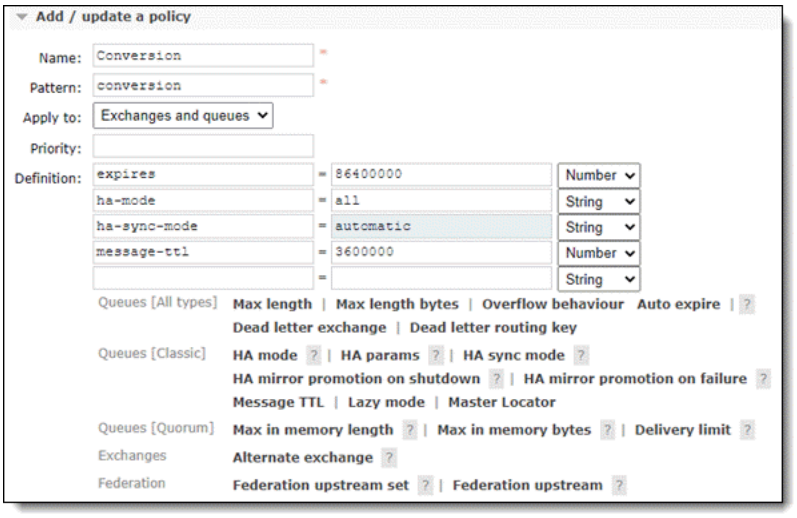
   Note: The default user guest can only log in from local host.
3. Click **Admin** > **Policies**.
4. Expand **Add / update a policy**.
5. Select a virtual host to be used. For example, Relativity.

6. Enter the following information:
    - **Name**—Ha-all
        - This will apply to all queues that are not SignalR or Conversion. In addition to the normal HA values, it also places a default expiration on all queues of 24 hours. The addition of the expiration value should help to clean up miscellaneous orphaned queues, such as ResourcePoolStatus queues for agents that no longer exist.
        - The 24-hour expiration only starts after the policy has been applied. This means the orphaned queues will not be cleaned up immediately, but will be cleaned up 24 hours after creating the policy.
    - **Pattern**—leave blank, means the policy will apply to everything.
    - **Priority**— -10
    - **Definition**
        - expires = 86400000 | Number
        - ha-mode = all | String
        - ha-sync-mode = automatic | String

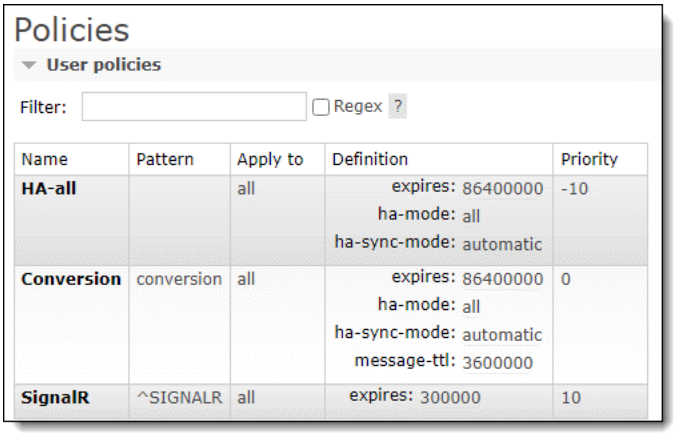


7. Click **Add policy**. The policy now appears under **User policies**.
8. Add another policy for Relativity Document Conversions by first selecting **Relativity** again as the virtual host to be used.
9. Enter the following information:
    - **Name**—Conversion
        - This policy applies to all conversion queues. This includes all values from the new HA-All policy as well as lowering the message time to live to 1 hour, down from 24 hours. The reduced message time to live will help discard conversion requests for especially large documents that are taking a very long time to convert.
        - The messages will not be discarded if they are currently in an unacked/in progress state, and restarting or deleting and recreating conversion agents may still be required.

- **Pattern**—Conversion
- **Priority**—0
- **Definition**
  - expires = 86400000 | Number
  - ha-mode = all
  - ha-sync-mode = automatic
  - message-ttl = 3600000 | Number



10. Confirm that all policies are properly logged. From the queues page, all SignalR queues should display SignalR under features. All conversion queues should display Conversion under features. All other queues should display HA-All under features.



8 File (document) share or server

You can use a file share or server as a repository for documents stored in Relativity. You must create a directory that is used as the root of the directories and documents created through the Relativity system. This file share must be a folder rather than a drive letter. For example, C:\Fileshare instead of just the C drive.

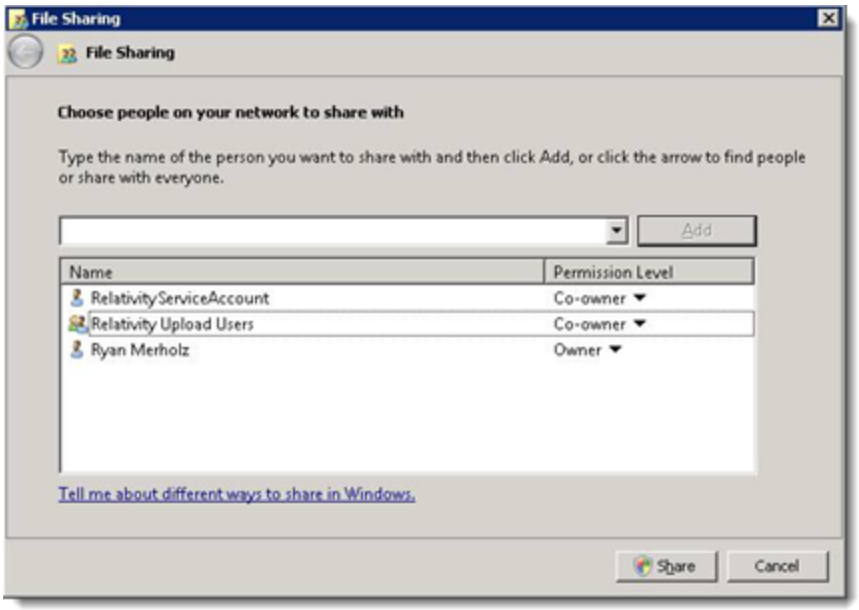
In addition, confirm that the Full Text, .ldf files, .mdf files, and Backups are all specified to the folder level. Do not specify them to only a drive.

Note: For information about setting up processing servers, see Database and worker server for processing or native imaging on page 59 and Pre-installation on page 5.

8.1 Create share

The document root directory is exposed to the Relativity application through a shared drive. Use these steps to share the folder:

1. Right-click the folder, and go to **Properties**.
2. Open the Sharing tab, and click **Share**.
3. Enter the Relativity Service Account name, domain\account, and then click **Add**.
4. Select the service account on the share list, and then change **Permission Level** to **Co-owner**.
5. Enter the **Relativity Upload Users** group, and then click **Add**.
6. Select the group on the share list, and then set the **Permission Level** to **Co-owner**.



7. Click **Share**.
8. When the share completes, click **Done**.
9. On the Document Properties dialog box, select the **Security** tab.

10. Verify that the users and groups you added to the share also have **Full Control** security permissions to the folder itself.

9 Cache location server

The cache location server requires the same permissions as the file share. For more information, see Pre-installation on page 5.

Note: During installation or upgrade, Relativity automatically creates a cache location server based on the location of your file repository. You can also manually add cache location servers. For more information, see Cache location servers on the Relativity 2023 Documentation site.

10 Analytics server setup

Before completing the steps for upgrading to Analytics 2023, make sure you have completed the steps contained in this section.

10.0.1 Required software

The following software must be installed on the analytics server:

- Windows Server 2019, Windows Server 2016
- .NET Version 4.8.1

10.1 CAAT 4.5.0 and above

The following table breaks down which versions of Microsoft Visual C++ are required for which versions of CAAT.

	Required Microsoft Visual C++ version (Redistributable x86 and x64)			
CAAT version	**2010**	**2012**	**2013**	**2015**
CAAT 4.2.5 and above	✓	✓	✓	✓

	Required Microsoft Visual C++ version (Redistributable x86 and x64)			
CAAT version	**2010**	**2012**	**2013**	**2015**
CAAT 4.2.5 and above	✓	✓	✓	✓

10.1.1 Create installation index directory

1. Create a folder called CAAT on the root of the C: drive.
2. The Analytics index directory must also be created before installing Analytics. We recommend that you not keep the index directory on the C: drive due to the size requirements. We recommend you use locally-attached storage referenced by a drive letter, such as E:\AnalyticsData, rather than a UNC path. For more information, see Index directory requirements in the Analytics Guide. Do not create a local drive map to a UNC. For example, do not open \\servername\CAAT1 and map it to drive Z. This is because drive mappings are specific to each Windows user and may not be available to the Relativity Service Account.

10.1.2 Assign permissions to the analytics directories

You must configure permissions for the necessary directories on the analytics server. Follow these steps to assign the proper permissions:

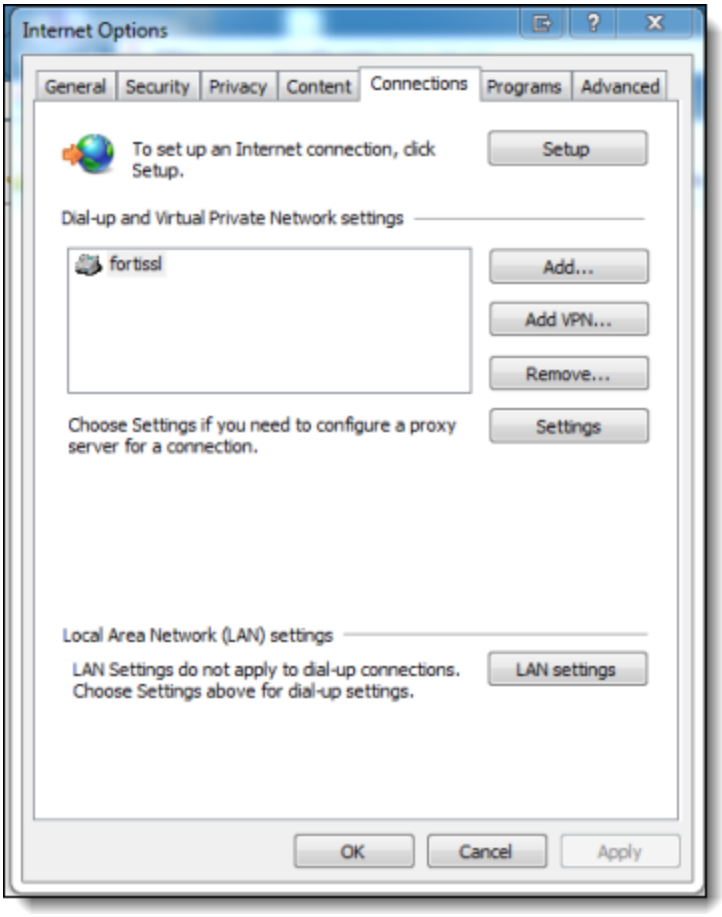
1. Add the Relativity Service Account user to both the Administrators and the Users group.
2. Navigate to C:\CAAT\ and add Full Control permissions to both the Administrators and the Users group.

- Right-click on **C:\CAAT**.
- Navigate to the **Security** tab.
- Edit the Users group permissions and add **Full Control**.
- Edit the Administrators group permissions and add **Full Control**.
- Click **Apply**.

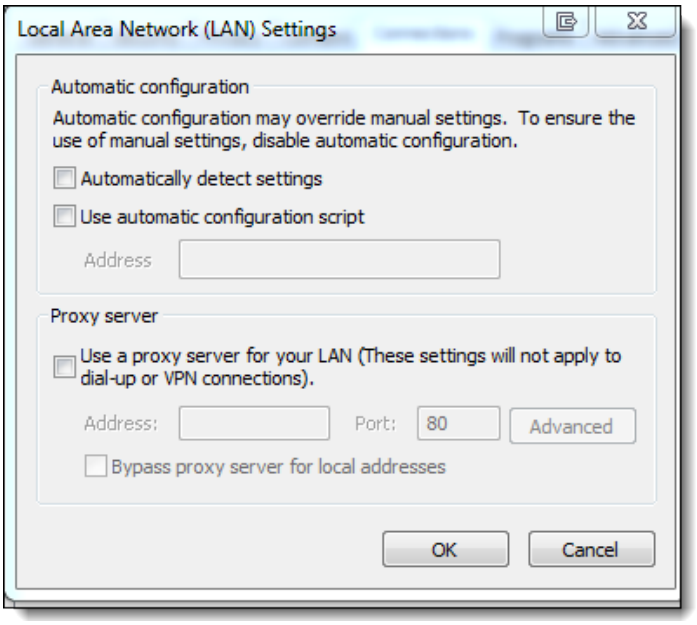
3. Navigate to the index directory and add Full Control permissions to both the Administrators and the Users group.
   - Right-click on the index directory folder.
   - Navigate to the **Security** tab.
   - Edit the Users group permissions and add **Full Control**.
   - Edit the Administrators group permissions and add **Full Control**.
   - Click **Apply**.
4. Reboot the server after all user or permission changes.

10.1.3 Required setup

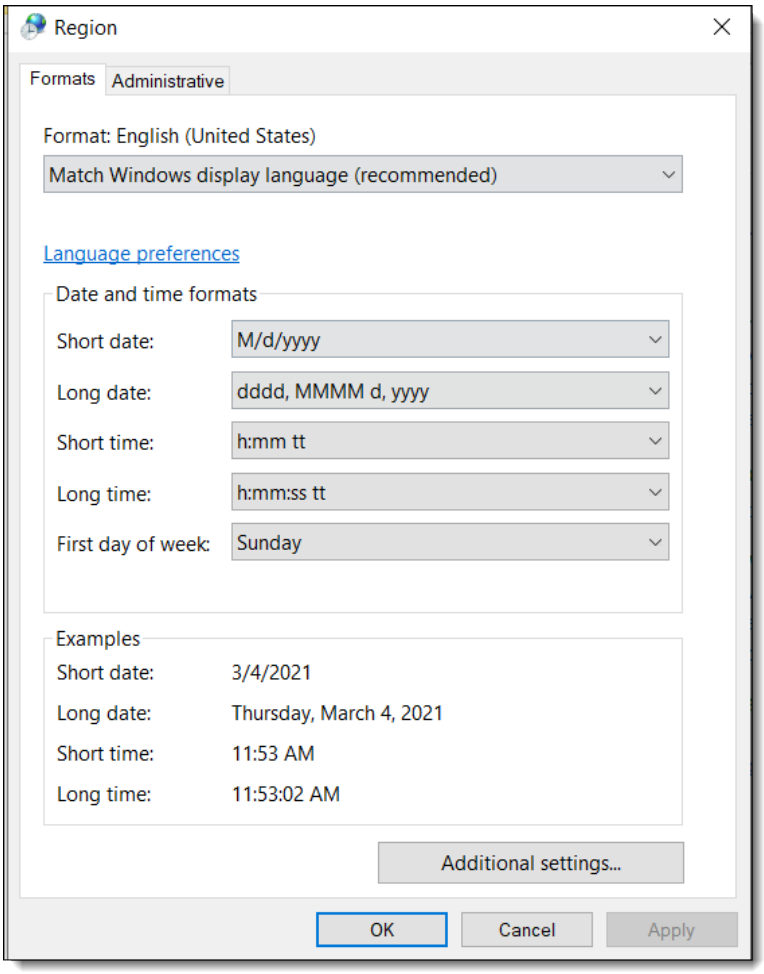
1. The web server needs to be able to communicate with the analytics server via TCP ports 445, 8080, and 8443. .
2. Disable anti-virus programs. At minimum it needs to be set to ignore the C:\CAAT installation folder as well as the index directory.
3. Ensure that proxy settings are disabled on the analytics server by performing the following steps:
   - Go to **Internet Options** using the Control Panel.
   - Select the **Connections** tab.



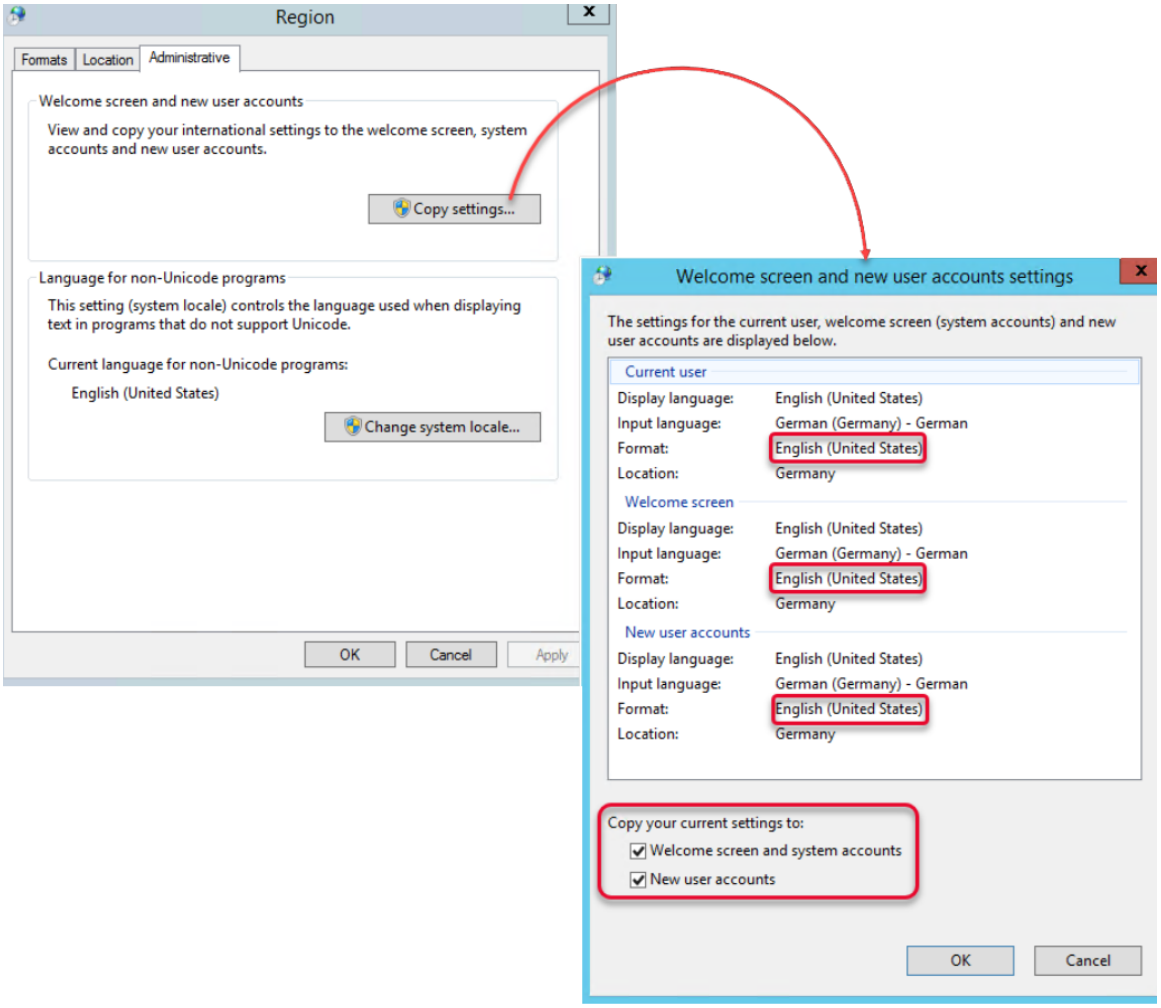
- Select **LAN Settings** and ensure the Proxy server section is cleared:



4. Click **OK** to save your changes.
5. Ensure that the required display language is set on the analytics server by performing the following steps:
    - On the Analytics server, click the **Start** button.
    - Click **Control Panel**.
    - Click **Change date, time, or number formats**.



    - Click the **Administrate** tab.
    - Select **Copy settings** and ensure the correct language is set:



- Click **OK** to save your changes.

10.2 Elasticsearch server setup

10.2.1 Required software

The following software must be installed on the Elasticsearch server:

- Windows Server 2016 or Windows Server 2019

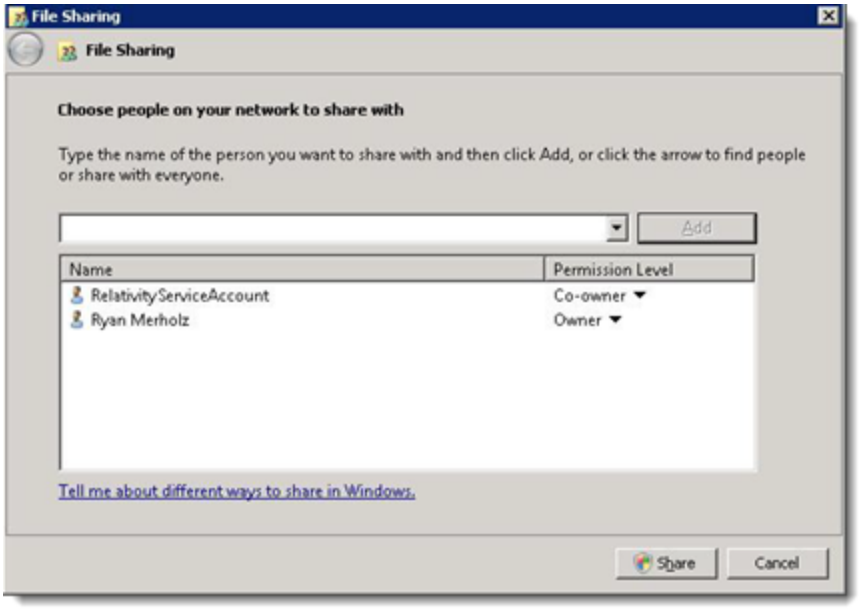
11 Index share - dtSearch repository

Create a root directory for the directories created by dtSearch index builds within the system.

11.1 Create share

The dtSearch index directory is exposed to the Relativity application through a shared drive. Use these steps to share the folder:

1. Right-click on the folder, and then go to **Properties**.
2. Open the Sharing tab, and then click **Share**.
3. Enter the Relativity Service Account name, domain/account, and then click **Add**.
4. Select the service account on the share list, and then set the Permission Level to **Co-owner**.



5. Click **Share**.
6. When the share completes, click **Done**.
7. On the Document Properties dialog box, select the **Security** tab.
8. Verify that the Relativity Service Account also has **Full Control** security permissions to the folder itself.

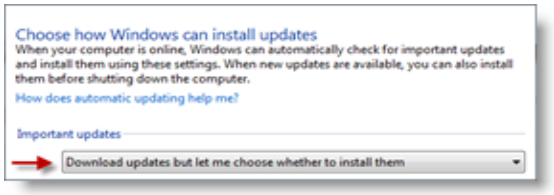
12 SMTP server setup

Relativity requires access to an SMTP server to handle the delivery of error messages, job notifications, and billing statistics to both internal contacts and to us at Relativity. We provide an easy to use SMTP connectivity tool, which Customer Support runs against your system to verify the servers can properly communicate with your specified SMTP server.

Note: Make sure that the newly created agent and web servers used in your Relativity environment are configured to permit the relay of messages to external recipients. If you do not provide this permission, job notifications and other messages are blocked.

13 Environment modification for processing or native imaging

Before running the Invariant, worker manager server, installer, you must perform the following steps to modify your environment.

Component	Environment Configuration Settings
Database	■ Disable User Access Control (UAC). ■ Enable your firewall according to the Ports Diagram and Relativity Server Security document on the Relativity Community portal under the Security Resources folder.
Queue Manager	None
Workers	■ Enable the Desktop Experience Windows Feature. ■ Disable User Access Control (UAC). Disabling UAC on the worker server suppress pop-ups from the application in which the processing engine opens files. ■ Enable your firewall according to the Ports Diagram and Relativity Server Security document on the Relativity Community portal under the Security Resources folder. ■ Set Windows Updates to download, but allow you to choose whether to install. You can set this option through the Control Panel under System and Security. 

For more information, see the Worker manager server Installation guide.

14 Database and worker server for processing or native imaging

The following sections provide basic information about setting up the database server for processing or native imaging. For more information, see the Worker manager server Installation guide.

Note: If you are only installing Collect or Legal Hold, you do not need this pre-requisite.

14.1 Required software

Install the following software on the database server:

- Windows Server 2022, Windows Server 2019, Windows Server 2016
- SQL Server 2022, SQL Server 2019, or SQL Server 2017

  Note: SQL Server 2019 requires Windows Server 2016 or 2019.

Relativity supports in-place upgrades to SQL 2016 to any higher supported version. For details on SQL Server upgrade, follow the EDDS migration Guide. To determine if you should upgrade your current SQL Server version to SQL Server 2019, note the following considerations. Contact Relativity Support with any further questions.

- The base operating system of your SQL Server must be at a minimum Windows Server 2016. Any Windows Server version below 2016 will require an EDDS migration to be performed to a server with a proper operating system version and SQL version. Relativity does not support in-place operating system upgrades.
- SQL Server version lower than SQL 2016 will require an EDDS migration since upgrading to SQL Server 2019 or higher from versions lower than SQL Server 2016 has not been tested by Relativity.
- .NET 4.7.2, 4.8, or 4.8.1
- .NET 3.5

Additional considerations:

- Each environment is different, research settings that your specific environment may utilize before performing any upgrades.
- Ensure that you have tested backups before performing any upgrades.
- Although an in-place SQL upgrade is supported by Relativity. Performing an EDDS migration is the cleanest way to perform a SQL upgrade.

The following table provides a breakdown of the required software:

Note:

- You must install a version of Microsoft Office no earlier than 16.0.4783.1000, the December 2018 update for Office.
- We recommend that you upgrade Invariant prior to upgrading Microsoft Office. If you upgrade Microsoft Office first, your workers will fail to validate, and Invariant will not run until you upgrade it.
- We recommend that you uninstall Microsoft Office 2013 before installing Office 2016.
- OneNote 2016 cannot export files containing more than 300 pages to PDF. Processing extracted text will fail in this case, as well.
- With the introduction of Office 2016 support, the font used to image text files is now Google's Noto Sans; previously, this was Microsoft's Arial Unicode.

14.2 Relativity Service Account

The Relativity Service Account must be the owner of all objects in the processing databases and have permissions for logging in to the SQL Server environment. It must be set up as follows:

- Configure the account with Windows Authentication.
- Ensure that the account has local administrator rights to perform the installation of the native imaging database and queue manager.
- Ensure that this account has SQL administrator rights.
- Do not include special characters in the Relativity service account active directory account name.

14.3 Create Invariant worker network file path share

Create a directory on the SQL Server in a location where the Relativity Service Account can read and write. Make sure that SQL services can also read from this directory. This directory must be an actual folder, not a drive letter. It stores the installation files for worker servers.

14.4 Required Microsoft Visual C++ redistributables

14.5 Relativity Service Account

The following table breaks down which versions of Microsoft Visual C++ are required for which versions of Relativity/Invariant. Note that you are required to install each version of Microsoft Visual C++ only if you are upgrading to the Relativity/Invariant version listed and not if you are installing it for the first time.

	Required Microsoft Visual C++ version (Redistributable x86 and x64)				
Relativity/Invariant version	**2010**	**2012**	**2013**	**2015**	
10.3.287.3/5.3.282.2	✓	✓	✓	✓	

Relativity/Invariant version	Required Microsoft Visual C++ version (Redistributable x86 and x64)			
	2010	2012	2013	2015
Server 2021/ 6.1.1798	✓	✓	✓	✓
Server 2022/7.1.431.1	✓	✓	✓	✓
12.3.805.2/7.3.804.12	✓	✓	✓	✓

The Relativity Service Account must be given local administrator rights to each worker server. The installation process uses this account. It must remain logged in to each server to run local processes during native imaging.

15 Obtaining applications for native imaging and processing

On the Relativity Native Imaging/Processing worker, you must install additional software to support imaging and processing.

Note: If you are only installing Collect or Legal Hold, you do not need this pre-requisite.

For convenience, this section includes links to download pages for specific software, which may require licensing or may be downloaded for free:

- Lotus Notes v8.5.2 with Fix Pack 4 or Lotus Notes v8.5.3 with Fix Pack 6

  Note: When you visit the IBM site to download Lotus Notes, you have the option of buying the software online or downloading a free trial of it. If you select the free trial, you are required to sign in with an IBM user ID, which you must create if you don't already have one.

- SolidWorks eDrawings 2015 (64-bit), with the option to view 3D XML and PRO/E files
- JungUm Global Viewer v9.1 or higher available at https://www.jungum.-com/ReNew/En/Download/EtcDownload.html

16 Default log file location

The default file location for Relativity logs is set by the **%RELATIVITY_LOGS%** environment variable. Define the variable on all machines in your Relativity environment, web servers, agent servers, except SQL Servers.

17 Post-installation considerations

After you install Relativity, review the post-installation considerations listed in this section.

17.1 User group for uploading documents

You can improve performance when documents are uploaded with the Win Relativity component by creating a group of users with Full Control permissions on the file share used as a document repository. This group can import and export documents in *Direct* mode, which is significantly faster than *Web* mode.

17.2 Relativity service account information

The Relativity installer automatically creates the Relativity service account. It assigns this account an email address, as the user name, and a default password. We highly recommend that you change the default Forms password through the Relativity UI after the software is deployed. However, you should not disable this account or modify any other authentication information assigned to it.

The Active Directory (AD) domain also includes a Relativity services account, which has the same user name. The Relativity services account on this domain must log in to Relativity to perform various tasks. Tasks like running agents and authenticating against the Relativity Services API. The audit history for Relativity often lists the Relativity services account as the user who performed a task. To avoid destabilizing your environment, we recommend that you do not change the user settings in Relativity for this account or the AD domain for this account. Since Relativity uses AD authentication for the Relativity services account only for performing agent tasks, you can change the Forms authentication password through the Relativity UI without encountering any environment issues.

As previously mentioned, the Relativity service account is sometimes used to identify the user who performed certain tasks in the software. For example, you might set up a dtSearch index job that includes a private search created by one of your users. The Relativity service account needs access to this private search in order to build the index automatically. It is the only account that can provide this functionality within Relativity.

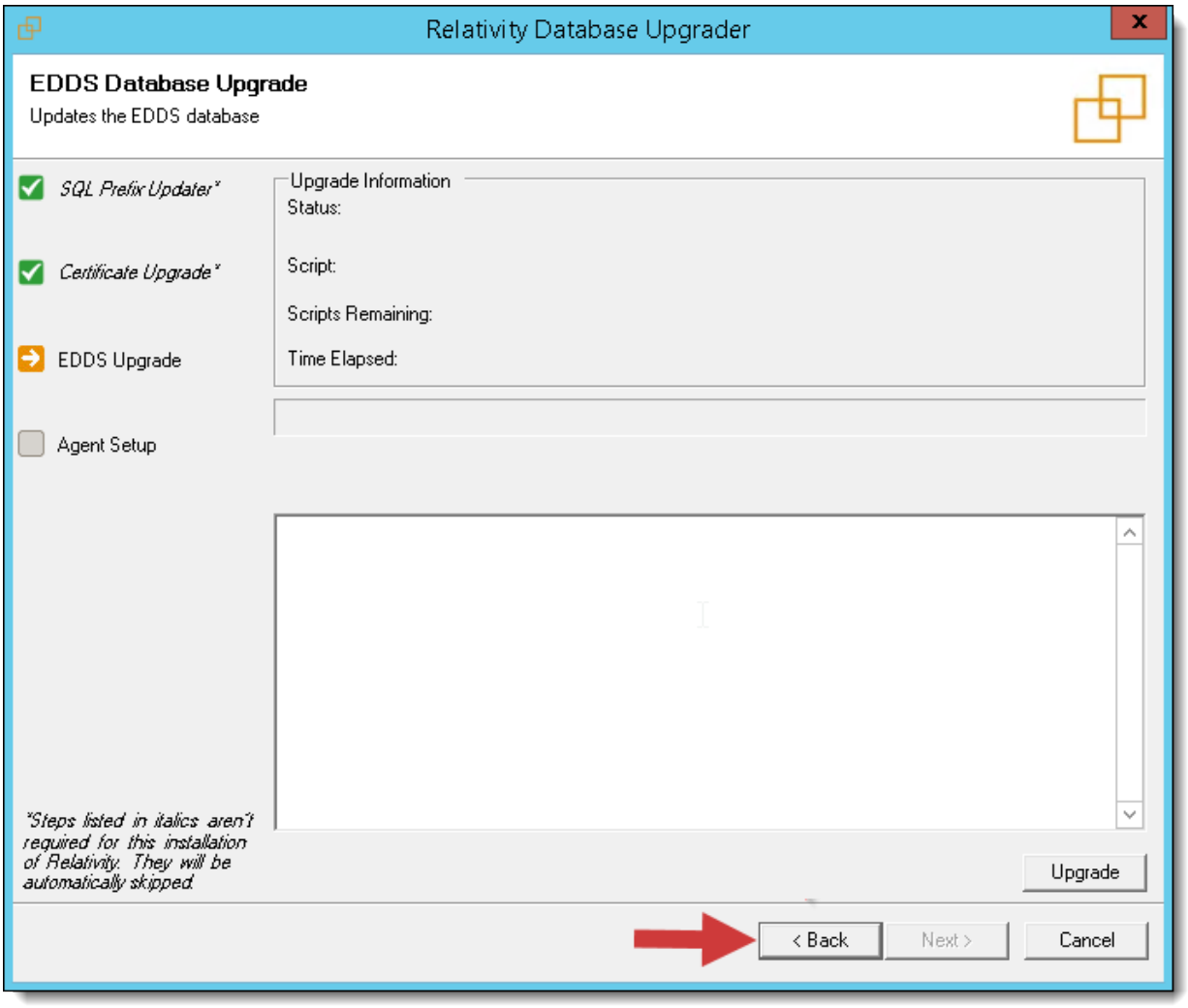
17.3 Post-installation steps for a token-signing certificate

Note: To minimize any interruption to your Relativity workflows, we recommend that you complete the following process during off-hours.

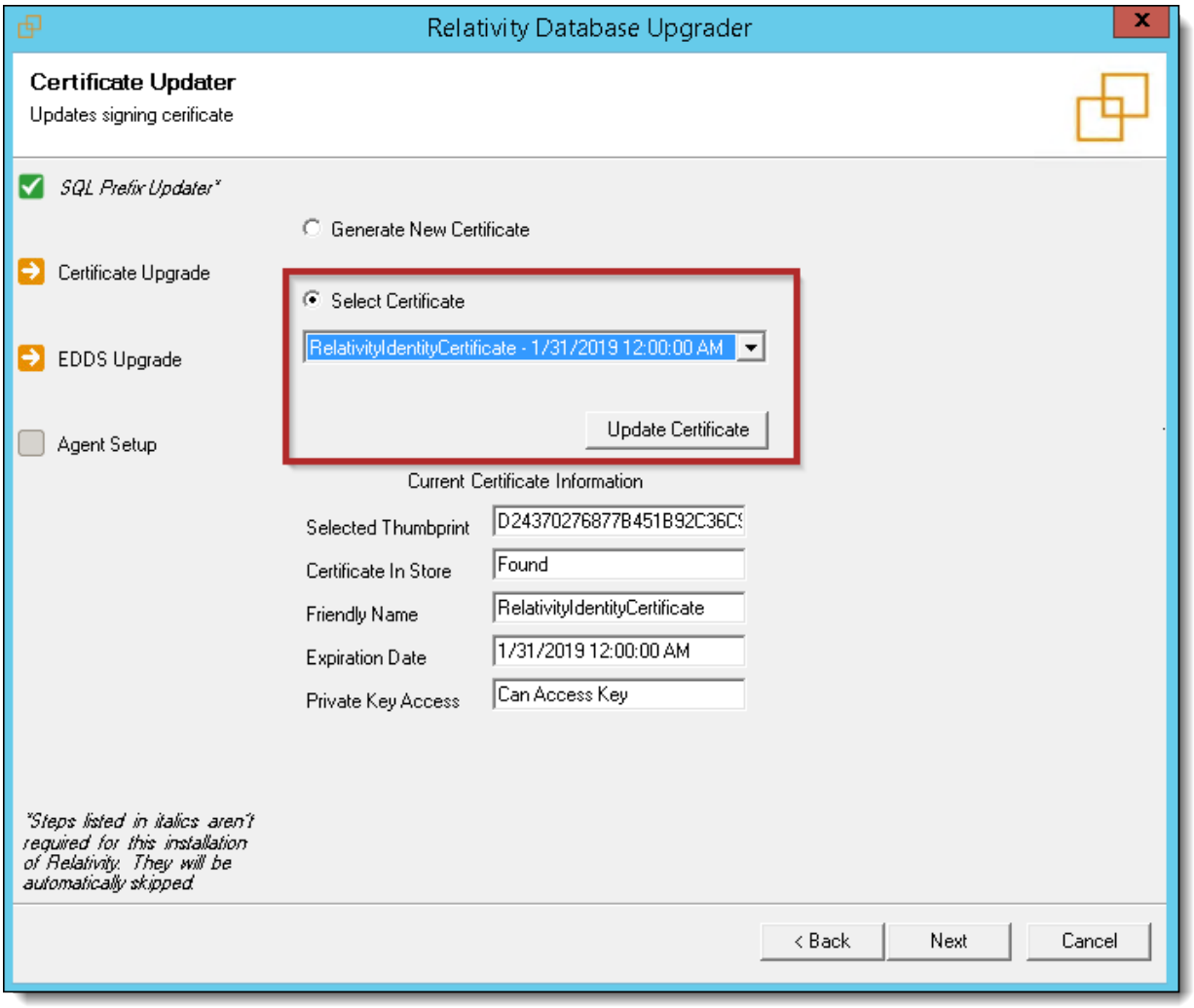
After installation, perform the following steps for a token-signing certificate:

1. On the primary SQL server, navigate to the Relativity install directory and then navigate to the Procuro folder. Typically C:\Program Files\kCura Corporation\Relativity\Procuro.
2. Run the kCura.EDDS.Procuro.exe application as an administrator.

3. On the EDDS Database Upgrade window, click **Back**.



4. Select the certificate that you wish to use as the signing certificate. The certificate must already be in the Personal store on the machine for it to appear in the drop-down menu.



5. Click **Update Certificate**.
6. Restart all of the Relativity services in the environment and IIS.

17.4 Logo customization

Customize your Relativity web interface with your company's logo. To accommodate variable space requirements, provide two logos with different sizes. The height may be 50 pixels and the width is discretionary. You can hide the logo using a setting in the Instance setting table. The name of the logo file is also set in the Instance setting table. Add the logos to the images folder at the root of the EDDS directory.

17.5 Resource groups

A workspace does not contain resource servers after you install Relativity. After the agents start up, the servers self-register. They are not automatically associated with a resource group. To associate these

servers to a resource group, you must manually add them through the Resource Group tab available only from Home. For more information, see Servers in the Admin guide.

17.6 License keys

After you install Relativity, you need to either activate new licenses or renew your current ones by requesting and applying activation keys for the applications you intend to use in your Relativity instance, including Processing. Relativity licensing includes flexible options that you can tailor to the size, type, and other requirements of your organization as part of your contractual agreement with us. For more information, see the Relativity Licensing Guide.

17.7 Relativity instance name

During a first-time installation, you must provide a name for your Relativity instance. This value is displayed on License details page available through the License tab. It is stored as the instance setting in the Relativity.LicenseManager section of the Instance setting table on the EDDS database.

Note: Modifying the instance name by updating this setting in the Instance setting table immediately invalidates your Relativity and Processing licenses.

When you request a Relativity license, this instance name is included in the request key. Contact the Customer Support team on the Community site for additional information.

In the RelativityResponse.txt file, the RELATIVITYINSTANCENAME value records the Relativity Instance Name option when you perform a first-time installation. For more information see, Relativity installation on the Relativity 2023 Documentation site.

Proprietary Rights

This documentation ("**Documentation**") and the software to which it relates ("**Software**") belongs to Relativity ODA LLC and/or Relativity's third party software vendors. Relativity grants written license agreements which contain restrictions. All parties accessing the Documentation or Software must: respect proprietary rights of Relativity and third parties; comply with your organization's license agreement, including but not limited to license restrictions on use, copying, modifications, reverse engineering, and derivative products; and refrain from any misuse or misappropriation of this Documentation or Software in whole or in part. The Software and Documentation is protected by the **Copyright Act of 1976**, as amended, and the Software code is protected by the **Illinois Trade Secrets Act**. Violations can involve substantial civil liabilities, exemplary damages, and criminal penalties, including fines and possible imprisonment.