Relativity®

Workstation Configuration Guide

October 30, 2024 | Version 24.0.315.10

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

Table of Contents

1 Workstation configuration

Before using Relativity for document review, it's important to consider workstation configuration properties potentially required in your environment. This document outlines those workstation components that ensure Relativity's accessibility and functionality.

1.1 Considerations for all browsers

Relativity does not support the following:

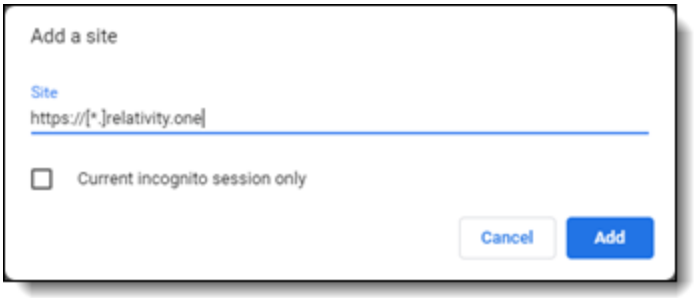
- Accessing the same Relativity instance with multiple tabs at the same time.
- Accessing the same Relativity instance with multiple browsers at the same time.

1.2 Google Chrome (Mac and PC) considerations

1.2.1 Disable pop-up blocker

Relativity opens new windows where you can perform specific actions. Your web browser's pop-up blocker may block new windows from opening by default. Refer to Manage pop-ups for instructions to disable the pop-up blocker in Google Chrome. For instructions to disable pop-up blocker using a wildcard in Chrome, open a Chrome web browser and follow the instructions below:

1. Click the three vertical dots in the upper right-hand corner in Chrome
2. Click Settings. Scroll down to the bottom
3. Click **Advanced**.
4. Click **Content Settings**.
5. Click **Pop-ups and redirects**.
6. Underneath Allow, click **Add**.
7. Enter in "https://[*.]relativity.one"



8. Click **Add**.
9. Close Settings in Chrome.

1.2.2 Additional settings

Refer to Browser specific considerations for information on additional settings for Chrome.

1.3 Safari (Mac only) considerations

1.3.1 Disable Pop-up blocker

Relativity opens new windows where you can perform specific actions. Your web browser's pop-up blocker may block new windows from opening by default. Make sure to disable the pop-up blocker when you're working in Safari.

1.3.2 Additional settings

Refer to Browser specific considerations for information on additional settings for Safari.

1.3.3 Disable Pop-up blocker

Relativity opens new windows where you can perform specific actions. Your web browser's pop-up blocker may block new windows from opening by default . Refer to your browser's privacy and security settings for instructions to disable the pop-up blocker.

1.3.4 Network considerations

- The viewer uses the RelativityWebAPI as well as the Relativity.Distributed components.

  Note: Inside the viewer, the Distributed piece is called from within the application, as indicated by the URL referenced in the bottom left corner of the viewer pane.

- The files retrieved in the viewer are HTTPS.

  Note: If a user does not have the latest Microsoft updates to add 3rd Party Certificate authorities as trusted certificates, an error message could occur, even if the user is using the correct website.

2 Browser-specific considerations

Refer to the following browser specific considerations when using Relativity.

2.1 End user browser and operating system requirements

Unless otherwise noted, this table lists the version of each browser that was available when Relativity performed testing for the annual Server release. Relativity does not incrementally test new browser versions for compatibility unless a version-specific issue is identified. If we discover any version-specific issues with browser compatibility, both this page and Known Issues will be updated.

Software	Latest Version Tested by Relativity
Chrome (Windows, Mac OSX)	130.0.6723.59
Edge (Windows, Mac OSX)	130.0.2849.52
Firefox (Windows, Mac OSX)	131.0.3
Safari (OSX 10.9)	TBD
Safari (OSX 10.10)	TBD

Note: Relativity does not currently support the Linux operating system for any browser.

2.2 Considerations for all browsers

Relativity does not support the following:

- Accessing the same Relativity instance with multiple tabs at the same time.
- Accessing the same Relativity instance with multiple browsers at the same time.

2.3 Changing the language settings in Chrome

Internet Explorer syncs the region and language settings with the operating system. Chrome does not have the same behavior.

You must manually change the language settings in Chrome to keep the language settings in sync with the operating system.

To change the language settings in Chrome, refer to the Chrome documentation.

Note: Make sure to place the selected language at the top of the Languages list, as Chrome uses the first language by default.

2.4 Using single sign-on (SSO) on a Mac in Chrome and Safari

In order for single sign-on (SSO) authentication to work on a Mac in Chrome and Safari, you must use SSO in conjunction with the Mac Keychain application.

- Safari considerations
  - Safari prompts for credentials the first time you access Relativity. If you select **Remember this password in my Keychain** you won't be prompted for credentials again
  - If you change your Active Directory password, you are prompted to update your Keychain at log in. This updates the Safari saved password and you are not prompted when accessing Relativity.
  - If you manually delete the entry in the Keychain, you are prompted for credentials when accessing Relativity.
- Chrome considerations
  - Chrome prompts you for credentials the first time you access Relativity. After you authenticate your machine, click **Yes** to remember the password and save the password in the Keychain.
  - Chrome pre-populates the prompt with credentials.

2.5 Pop-up blockers in Firefox

By default, Firefox blocks some pop-ups in Relativity. Normally, Firefox displays a message near the URL bar stating that a pop-up was blocked and asks whether to allow pop-ups for the website. For certain pop-ups, this message displays but then disappears immediately, before giving you a chance to allow pop-ups.

This error occurs in the Delete button in the action bar of any object's View page. To work around this issue, perform the following steps:

1. Navigate to the Firefox browser Options menu.
2. Click the **Content** tab, then under the Block pop-up windows section, click **Exceptions**.
3. Add the URL of Relativity (e.g.,, http://localhost/Relativity).

After performing these steps, Firefox doesn't block any Relativity pop-ups in the environment.

Alternatively, you can disable pop-up blocking for all websites by clearing the **Block pop-up windows** option in the Content tab.

2.6 Pop-up blockers in Safari

Similar to Firefox, Safari also blocks the Delete pop-up on any object's View page, but Safari never alerts the user. To work around this issue, open the Preferences menu, navigate to the **Security** tab, and clear the **Block pop-up windows** option. Safari no longer blocks pop-ups from any website.

2.7 Enable tabbing on a Mac in Safari or Firefox

When working in Relativity using Safari or Firefox on a Mac OS, you must configure the following settings to enable tabbing:

2.7.1 Safari

- Navigate to the Advanced tab from Safari Preferences, and then select **Press Tab to highlight each item on a webpage**.

2.7.2 Firefox

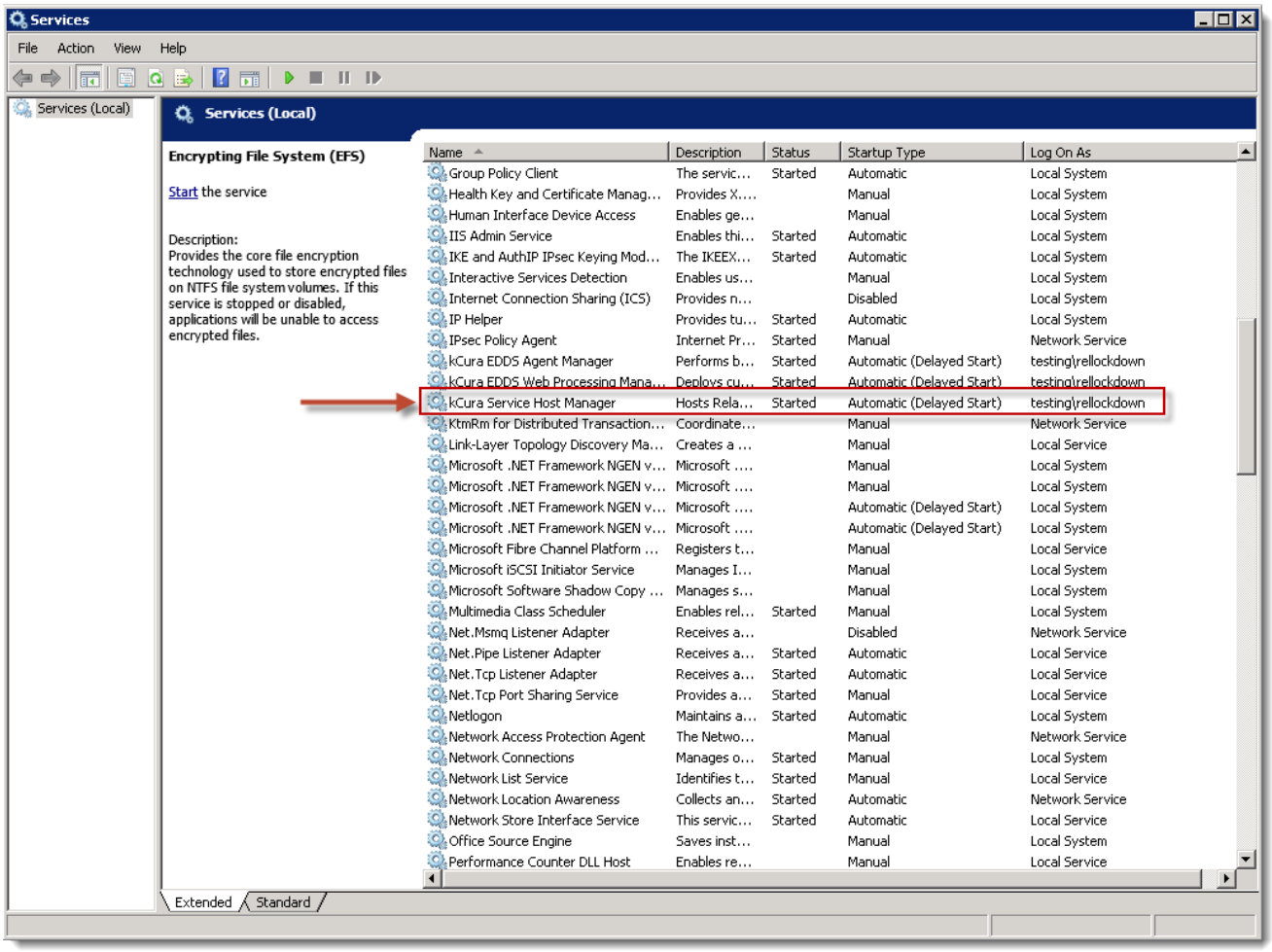
1. Click **Keyboard** from System Preferences, and then navigate to the Shortcuts tab.
2. Select **All Controls** near the bottom of the window in the Full Keyboard access section.

Enabling the All Controls setting can cause a cursor to appear to the right of any items you've highlighted using the Tab key. To stop this cursor from appearing, perform the following steps:

1. Navigate to the Advanced tab from System Preferences.
2. Click the **General** subtab if necessary, and then select **Always use the cursor keys to navigate within pages**.

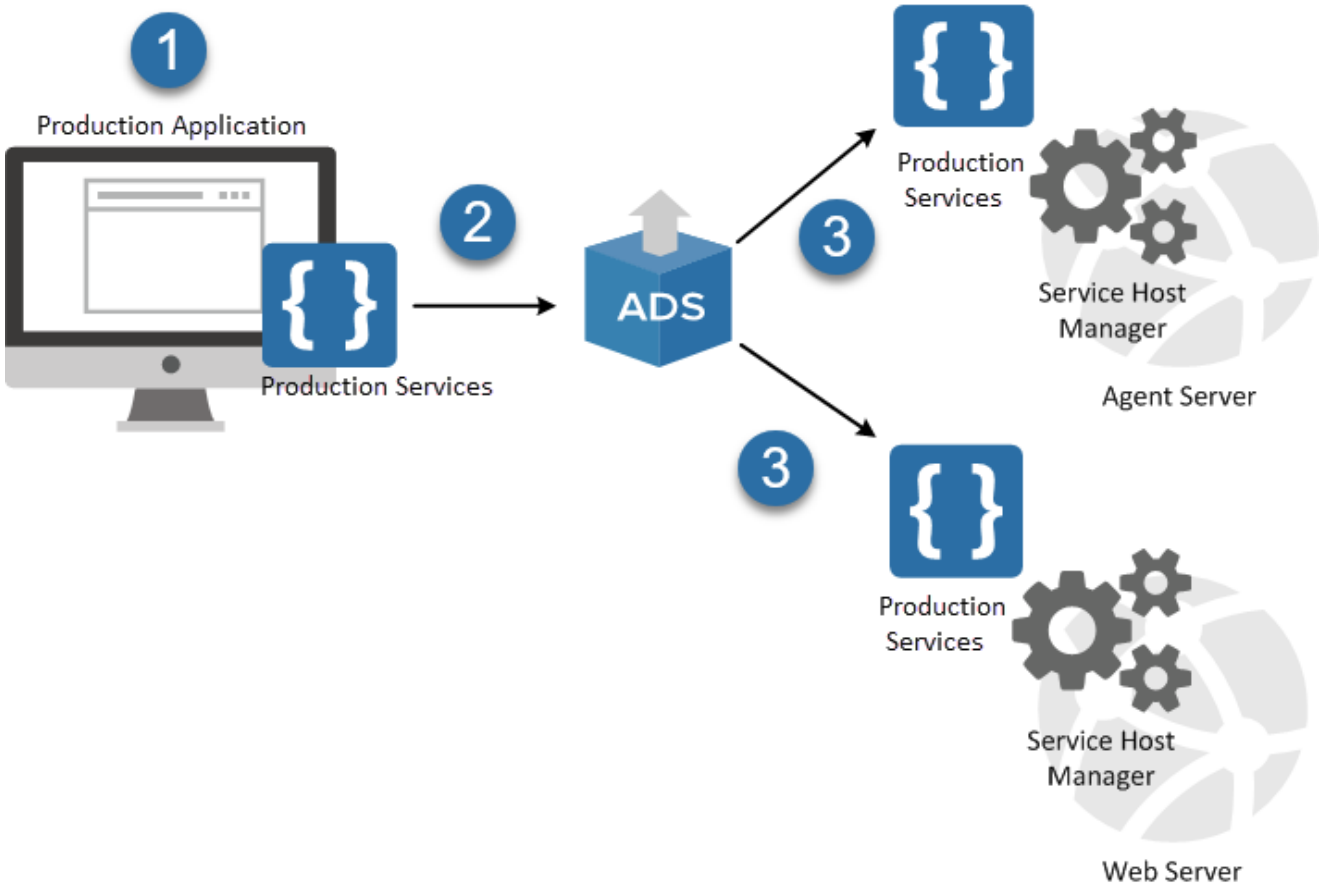
3 Service Host Manager

Relativity services defined within the Relativity.Services application and other applications, such as Production, run inside of the kCura Service Host Manager service on all web and agent servers in a Relativity environment. kCura Service Host Manager must be running on all web and agent machines to use Relativity.



3.1 Productions example

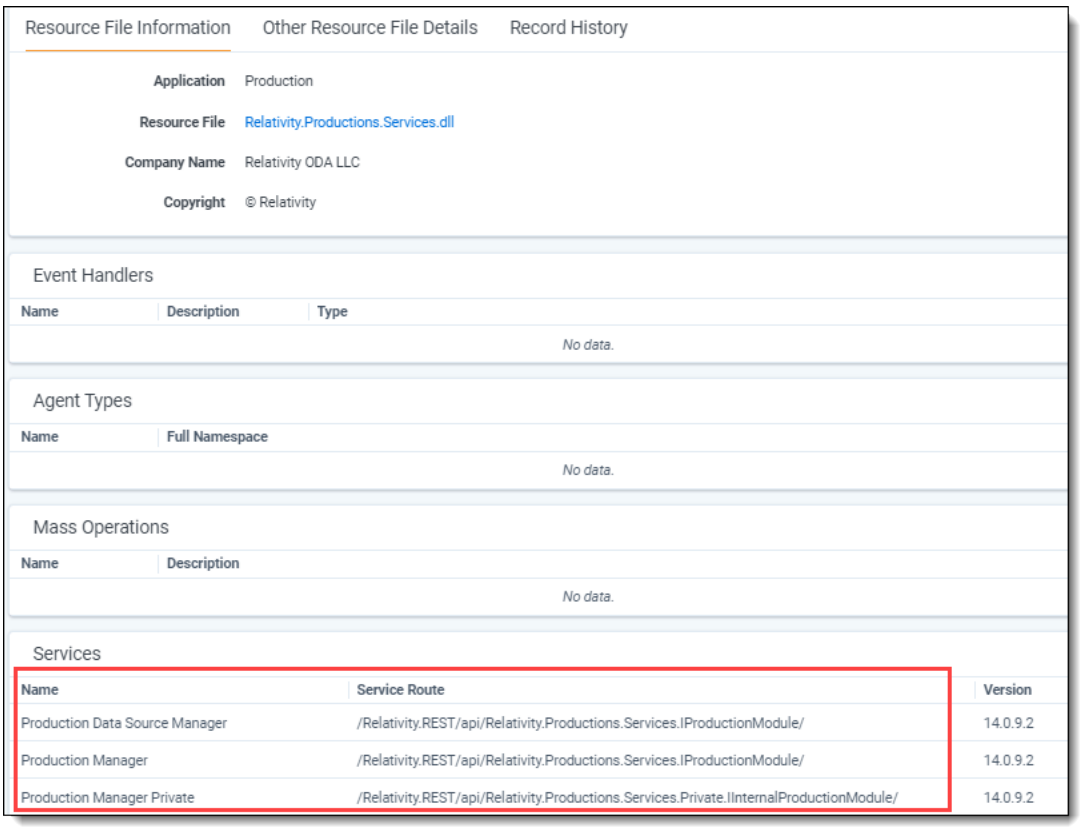
The following diagram illustrates how the Service Host Manager is used by Relativity productions:



1. Production is a Relativity application installed by default.
2. When you install Relativity, the Production application is deployed using the Application Deployment System (ADS).
3. As part of the application installation, the ADS deploys the services included in the Production application to all web and agent servers in your environment. These services are run by the Service Host Manager.

When you use Relativity productions, the browser user interface calls the services, for example, to create, update, or run productions. If the Service Host Manager is down, you can't interact with productions.

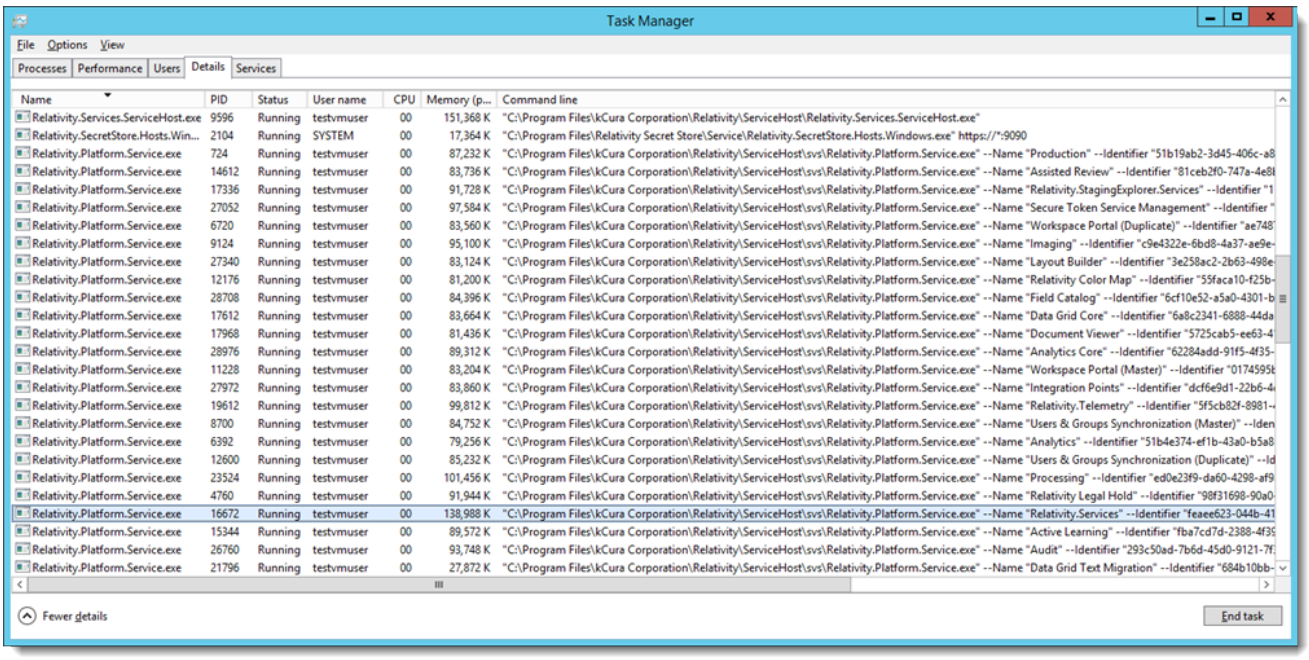
You can view the services associated with a Relativity application using the Resource Files tab. The following example displays the services in the **Relativity.Productions.Services.dll**.



3.2 Identifying a process running a specific service

The services running in the Service Host Manager are hosted as individual processes. Each of these services execute as a separate instance of Relativity.Platform.Service.exe, resulting in improved stability, and greater ease in identifying services that have failed. To minimize downtime experienced by Relativity users, the Service Host Manager now attempts to restart a failed service up to three times, rather than require a full restart of the service host.

To determine the application service running in a process, open the **Task Manager**, then select the **Details** tab, and view the **Command line** column. You may need to right-click on the column headings and then select the Command line column to display it.



You can prevent services from starting by listing them in the ServiceHostExclusionList instance setting. If you add a GUID for a service to this list while the Service Host is running, the service shuts down dynamically. Similarly, if you remove a GUID, the service starts dynamically. Do not suspend required services unless Customer Success or Relativity engineers advise you to do so.

3.3 Port configuration

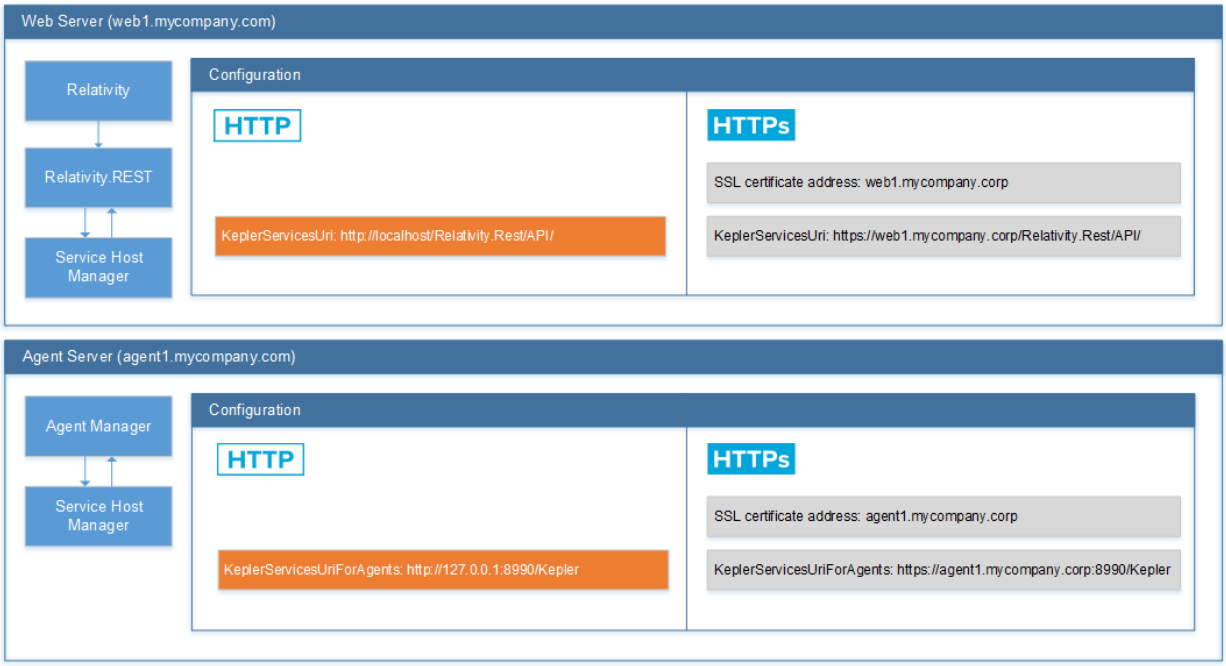
In certain network environments, it may be necessary to customize port settings for the Service Host Manager:

- Service Host Manager by default runs on port 8995 (http://localhost:8995). If the port is not available on your system, add the **ServiceHostServiceLocation** instance setting with a different port value to explicitly specify the port to use.
  - **Name** – ServiceHostServiceLocation
  - **Section** - kCura.Service.ServiceHost
  - **Value** - specify the port number to use
- Individual service endpoints deployed with the Service Host are assigned port numbers from the default range of 10000–20000. To specify a different port number range, add the **ServiceHostPortRange** instance setting.
  - **Name** – ServiceHostPortRange
  - **Section** - kCura.Service.ServiceHost
  - **Value** - specify the port ranges to use
    - The range value must be pipe-delimited (20000|30000). You can look up the port number assigned to a specific service in the EDDS.ApplicationServiceLocation table. This table is only populated while the service is running.

3.4 HTTPS configuration

Follow these steps to enable HTTPS for the Service Host Manager:

1. Change the values of the KeplerServicesUri and KeplerServicesUriForAgents instance settings to HTTPS URIs for each server.



Note: The values of KeplerServicesUri and KeplerServicesUriForAgents for HTTPS URIs must match the SSL certificate address, so they cannot use *localhost* or *127.0.0.1*.

2. Set up the certificate on each server:
   - Install the certificate to the Personal certificate store for the Computer Account on all web and agent servers.

     Note: If the certificate is self-signed, you must add it to both the Personal and the Trusted Root Certification Authorities certificate stores for the Computer Account on all web and agent servers.

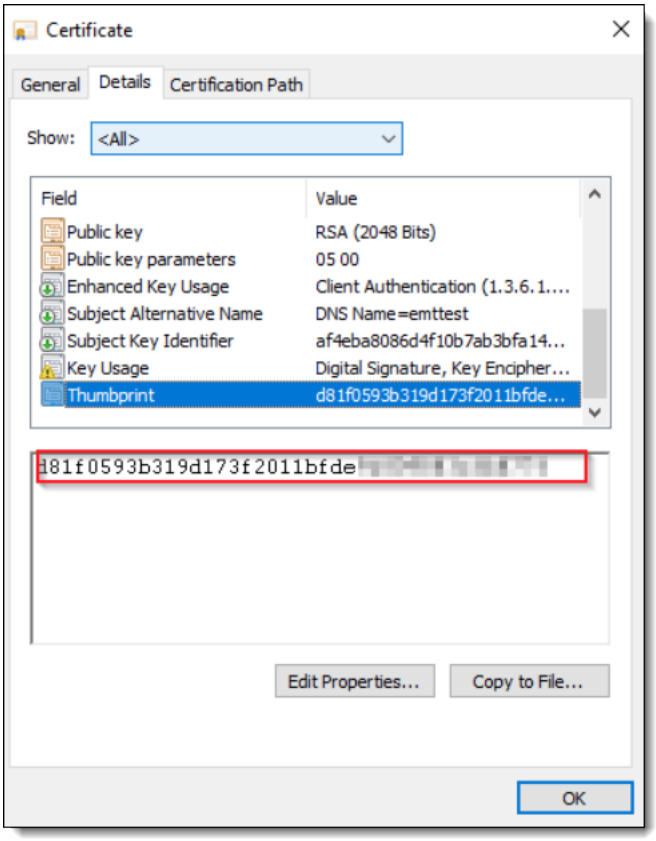
     The certificate is bound to IP 0.0.0.0 on the machine hosting Service Host Manager (specified in the **KeplerServicesUri** instance setting), and the URI of the agents server (**KeplerServicesUriForAgents** instance setting). The port that the certificate is bound to is as follows:

     - **Service Host Manager** – the port that the certificate is bound to is determined when the service is started by iterating through the ports specified in the **ServiceHostPortRange** instance setting (default is 10000 – 20000, as described above). For example, for productions services the certificate may be bound to port 10001 and processing services to port 10002.

- **Agents URI** – the certificate is bound to the port specified in the URI in the **KeplerServicesUriForAgents** instance setting. For example, *https://agent1.mycompany.corp:8990* binds the certificate to port 8990.

  Note: The host name specified in the KeplerServicesUri and KeplerServicesUriForAgents instance settings for each web and agent server must match the certificate's Issued To or Subject Alternative Name value. Domain wildcard values are supported. For example, if the agent server's host name is *https://rel-agent-server1*, the KeplerServicesUriForAgents instance setting must be *https://rel-agent-server1:8990/Kepler* and the certificate must have *rel-agent-server1* in the Issued To or Subject Alternative Name field.

- Upon initialization, Service Host and the Agent Manager attempt to automatically configure HTTPS and select the certificate (because KeplerServicesUri and KeplerServicesUriForAgents instance settings include the HTTPS prefix). Certificate selection logic is as follows:
  - Open the Personal store for the Computer Account and look for an exact host name match. The host name comes from the KeplerServicesUri and KeplerServicesUriForAgents instance settings.
  - If there is no exact host name match, query the store for all valid certificates and use the one with the largest encryption key.
  - If there are no valid certificates, look for a wildcard certificate that would work.
  - If there are no valid wildcard certificates and the scheme is set to HTTPS, an exception is logged.
- To override the default automatic certificate selection behavior, add the SslCertificateThumbprint instance setting for the server to explicitly specify the certificate to use:
  - **Name** – SslCertificateThumbprint.
  - **Section** – kCura.Service.ServiceHost.
  - **Value** – the thumbprint of the certificate for SSL bindings. For instructions on retrieving the thumbprint, see Retrieve the Thumbprint of a Certificate.



Note: Ensure there are no leading, trailing, or intervening spaces in the thumbprint value. You may need to specify a different thumbprint for each Agent or Web server. If you do, create multiple instance settings with different Machine Name values for each server.

3. Set the value of the EnforceHttps instance setting as necessary:
   - EnforceHttps ensures that your KeplerServicesUri and KeplerServicesUriForAgents instance settings are set to HTTPS. If you have EnforceHttps set to On and your Kepler Uris are not set accordingly, Service Host will fail to host your services.
   - EnforceHttps can ensure that all incoming Service Host Manager traffic uses HTTPS. If any request comes in as HTTP and EnforceHttps is set to On, Service Host will not accept the request. Setting EnforceHttps to Off does not force traffic to use HTTPS and allows HTTP. Setting EnforceHttps to Warn will still allow your services to be stood up as HTTP, but will log a warning.

3.4.1 Removing certificate bindings

Relativity unbinds certificates from ports as part of the services normal shutdown cycle. Because abnormal shutdowns can also occur, and Service Host Manager uses a range of ports, it is possible that over time all ports in the range may be bound to certificates. Removing bindings for server maintenance one-by-one can be time-consuming, so the recommended way of clearing them is by using command line. You must shut down Service Host Manager before running this command:

```
Relativity.Services.ServiceHost.exe --unbindports
```

3.5 HTTPS setup for dtSearch service

The dtSearch service is a self-hosted webservice that runs on any agent server on which the dtSearch Search Manager agent is enabled. Like Service Host, this service is not TLS-encrypted out of the box, but you now have the ability to enable this feature beginning in Server 2022.

To enable HTTPS on the dtSearch service, perform the following steps:

1. Fully configure Service Host for HTTPS, per the HTTPS configuration on page 12 steps above.
2. Set the EnforceHttps instance setting to On. This instance setting can only be set to On if the Service Host has been fully configured for HTTPS.
3. Install a valid SSL Certificate. We recommend re-using the same certificate used to secure ServiceHost on each agent machine. This is possible because, like Service Host, the agent hostname is used in the URI for all calls to the search service. To confirm this, you can review the KeplerServicesUriForAgents instance setting. If for any reason you are not using agent hostnames, this topic contains best practices for configuring a certificate for each agent by hostname.
4. Register the SSL certificate to the search service's port. The default port for the dtSearch Search Service is 6870, but this can be overridden via the SearchAgentServicePort instance setting. Unlike Service Host, the search service will not auto-register your certificate on startup. This must be carried out by a server administrator or via automation of your own.
5. Enable HTTPS for the search service via the toggle kCura.EDDS.Agents.Toggles.EnableHttpsDTSearchToggle. This Relativity toggle, once enabled, will cause the search service to automatically switch to the HTTPS protocol. No manual restart is required.

3.6 Troubleshooting hosted services

If an application error indicates that a service did not deploy successfully, start by reviewing the information on the Errors tab. If you are unable to identify the cause on the Errors tab, review the Relativity log.

In most cases, Service Host Manager errors are resolved when the service restarts. Once the Service Host Manager restarts, a new end point is generated and service is redeployed.

If the problems persist, review the Service Host Manager port and HTTPS settings described above.

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.