

REFINITIV EIKON

NETWORKING GUIDE

Eikon 4.0



Version history

Document version	Summary of Changes
1.0	▫ Initial version of the rebranded Refinitiv Eikon Networking Guide

Contents

About this document.....	4
Intended readership	4
In this guide.....	4
Eikon Desktop deployment profiles	5
Customer Managed	5
Elektron Managed Services	6
Refinitiv Hosted.....	7
Refinitiv Managed	8
Network configuration requirements	9
Configuration platform.....	9
IP subnet / TCP port	14
Firewall.....	15
Proxy.....	20
Internet property settings	23
Certificate management.....	24
Configuration for Eikon Desktop	30
Refinitiv Data Management Solutions	30
Configuration service	30
Elektron real-time proxy	32
Time series proxy.....	32
Appendix A: Eikon support tools.....	34
Dump Uploader.....	34
Appendix B: Eikon system and network test.....	35
Appendix C: United States Federal Information Processing Standard (FIPS)	36
Windows FIPS mode	36
Appendix D: Customer Managed over Internet.....	37
Defined host name	37
DNS	37
Appendix E: List of Acronyms.....	39

About this document

Intended readership

This document is intended for Eikon Support Group, Field Service Engineers, Client Implementation Specialist and Customer On-Boarding Specialists who is responsible for Eikon deployment at customer sites.

It is also be useful for Eikon customer's IT or Networking personnel to plan Eikon deployment.

In this guide

This guide provides an overview of network setup requirement for Eikon that deliver globally under Eikon platforms.

It contains TCP/IP standard ports, network routing, DNS and other relevant network information.

Product Change Notification 11803 – Refinitiv domains

For further information, refer to [PCN 11803](#).

Eikon Desktop deployment profiles

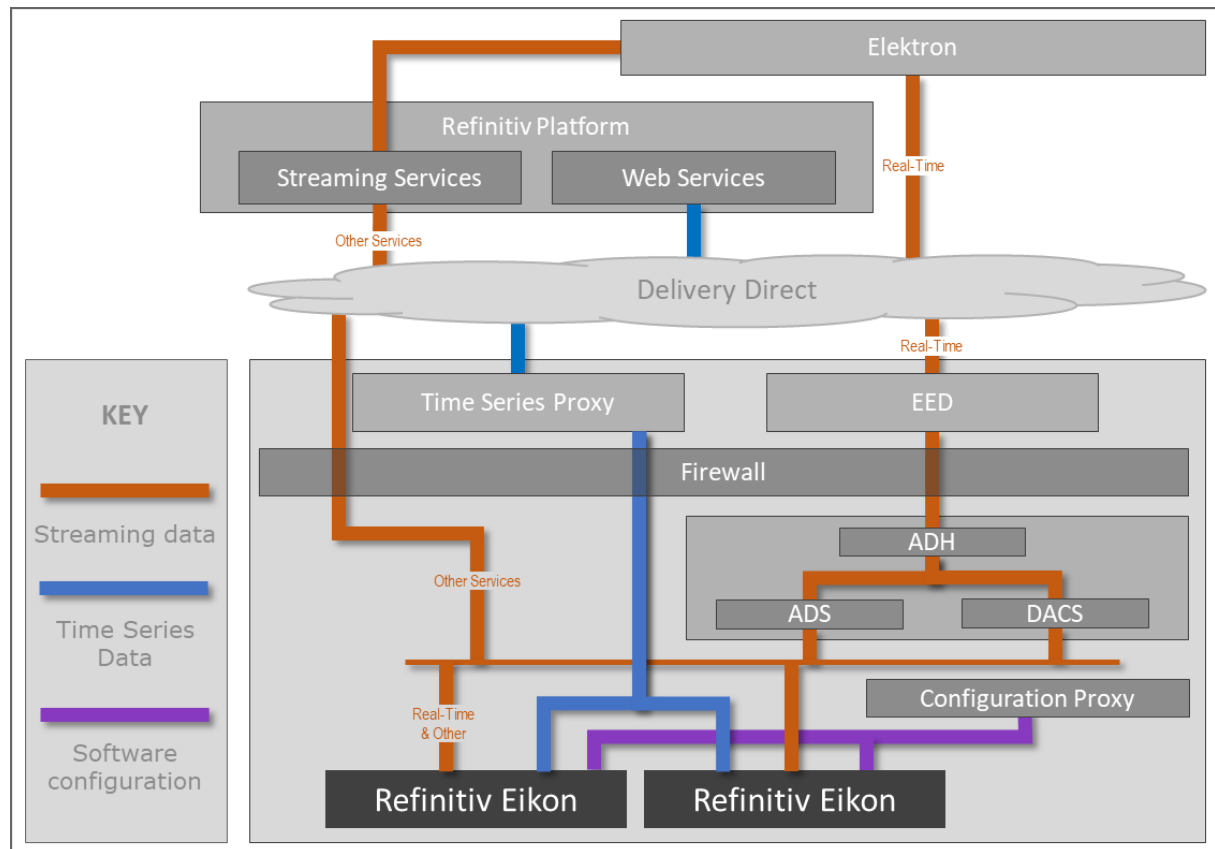
Customer Managed

Refinitiv Customer Managed connectivity is an option for customers who are co-located in a Refinitiv Network Point of Presence (N-PoP).

It enables customers to provide their own access circuit or cross-connect between the Refinitiv-managed Customer Premises Equipment (CPE) and the Refinitiv N-PoPs, which are in key financial centers globally.

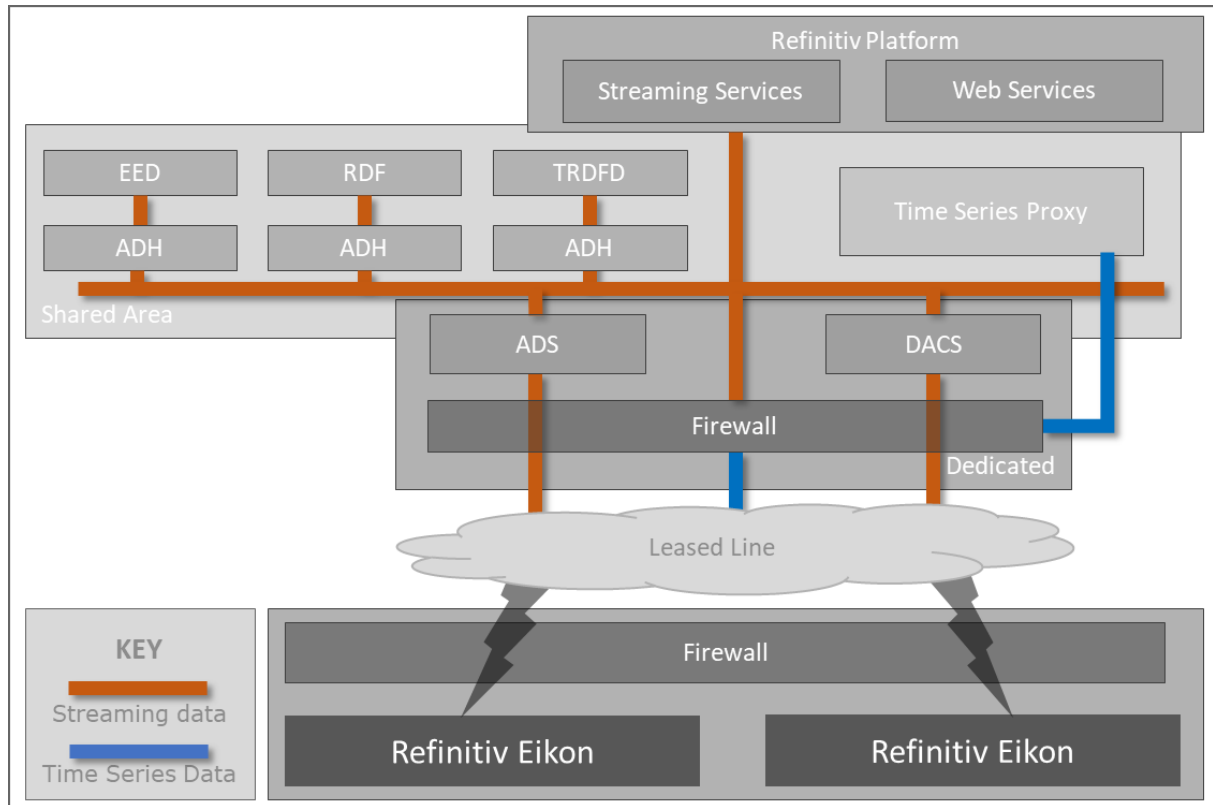
Customers use their own preferred supplier of network connectivity between their network and the Refinitiv aggregation router.

This is particularly useful for customers that co-locate or are in the same carrier hotel as a Delivery Direct N-PoP.



Elektron Managed Services

The Elektron Managed Services (EMS) solution offers market data, infrastructure, platform and connectivity, all as fully managed services hosted from one of our global data centers, delivered at the lowest total cost of ownership.



Refinitiv Hosted

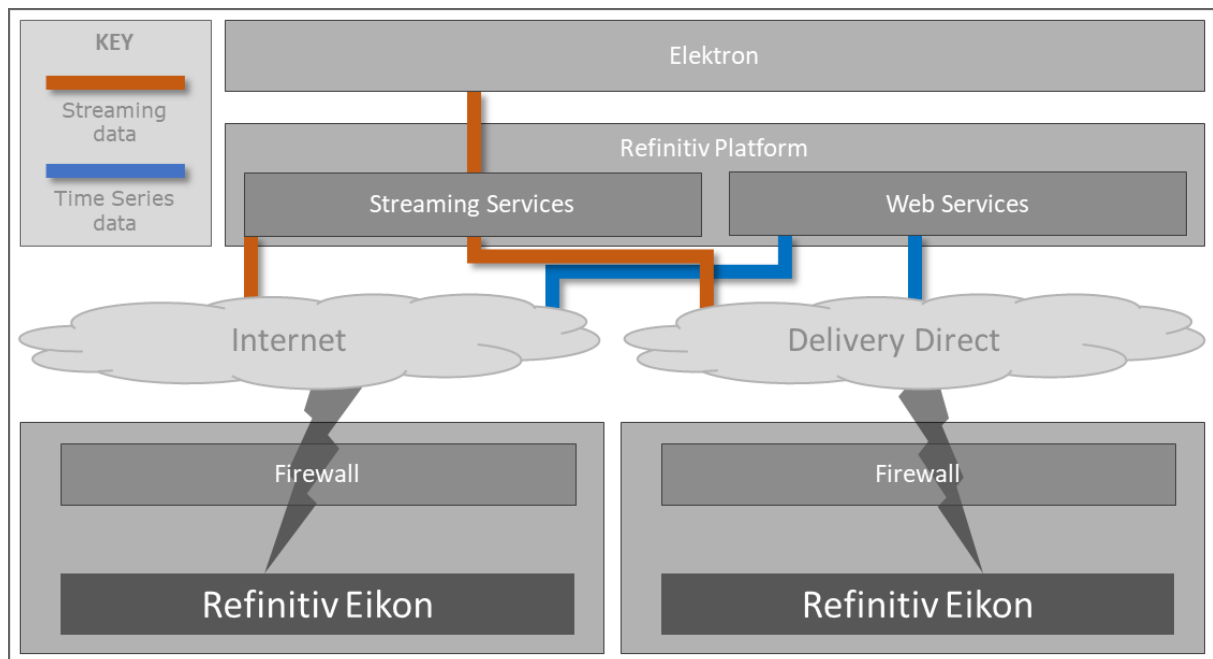
The Refinitiv Hosted solution is fully hosted by Refinitiv and no infrastructure is required on the customer site, apart from an Internet Service Provider (ISP). Eikon accesses streaming services and time series service over the Internet.

Internet

The Internet is enabling an increasing number of customers to connect with the global financial community worldwide. Internet connectivity is enabling cost effective, high-performance, resilient and flexible access in more places globally. It enables customers to make their own choice of service provider and take advantage of increased business agility.

Private network

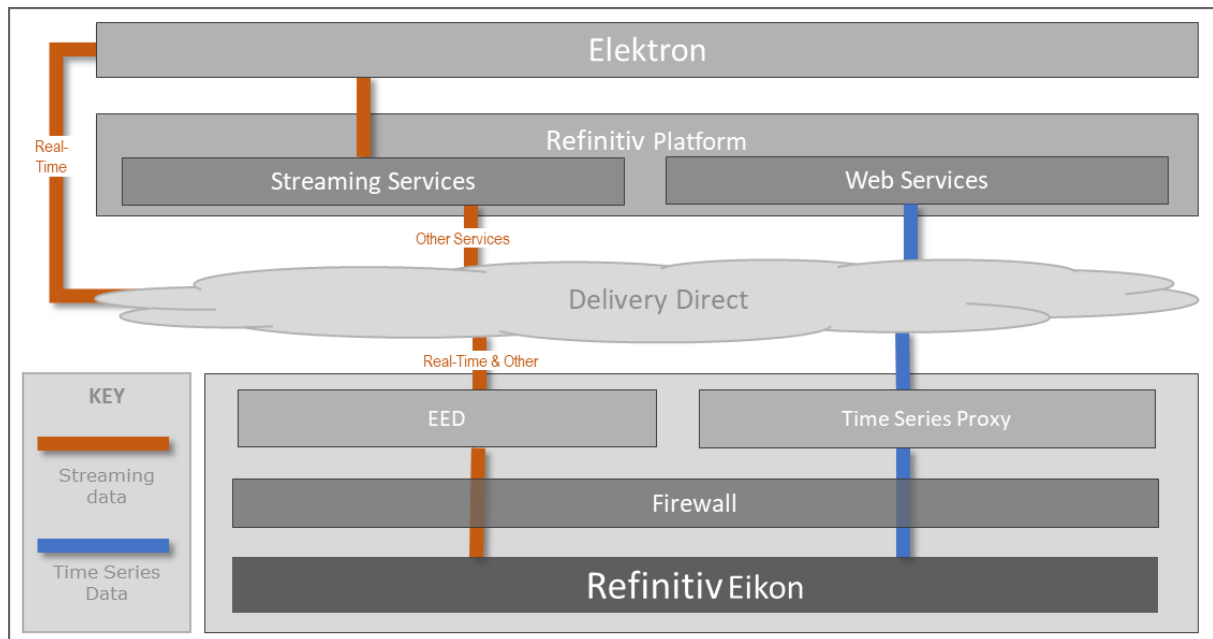
The customer connects to Refinitiv services through the special circuit which is managed by Refinitiv. This connection is provided by a third-party telco, such as Telefonica, Verizon, Telstra, and so on, but Refinitiv manages the installation and maintenance of the circuit.



Refinitiv Managed

The Refinitiv Managed solution provides a fully managed communications service to customer sites.

The service architecture has been designed to enable the delivery of Refinitiv products and services through high-quality, low-latency networks that leverage the latest advances in metro Ethernet (MAN) technology.



Network configuration requirements

Configuration platform

This section provides an overview and diagram of each customer connectivity for Eikon.

It also includes a fast track and step-by-step configuration guideline on how to configure network and additional products for Eikon in a flowchart format.

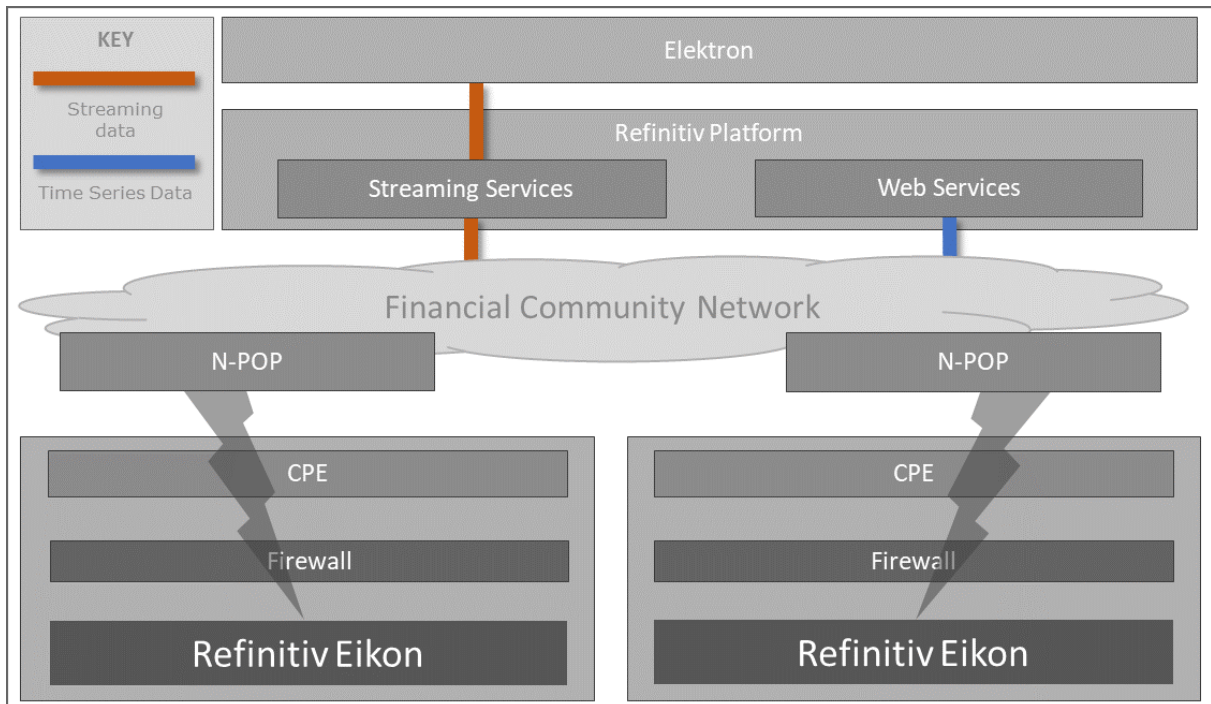
Financial Community Network and Delivery Direct

Financial Community Network (FCN)

The Financial Community Network is a private network customer connectivity solution, which the customer procures directly from the Financial Community Network provider.

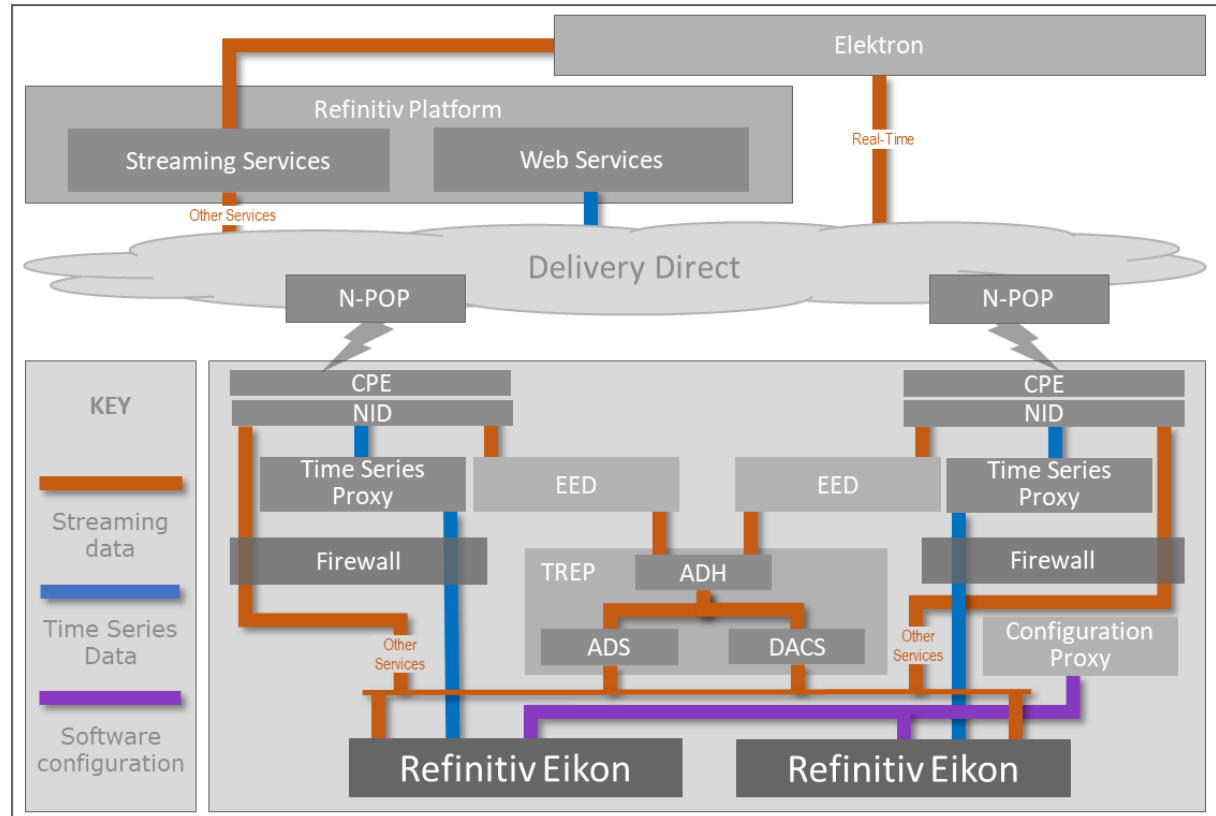
It provides the lowest cost private network option for the customer. As data demands grow, we are evolving our connectivity solutions to allow lower unit costs for a given capacity. The Financial Community Network enables Refinitiv to offer the lowest cost private network access option to the customer.

The Financial Community Network delivers cost effective and resilient private network access, supporting a subset of Refinitiv strategic products.



100

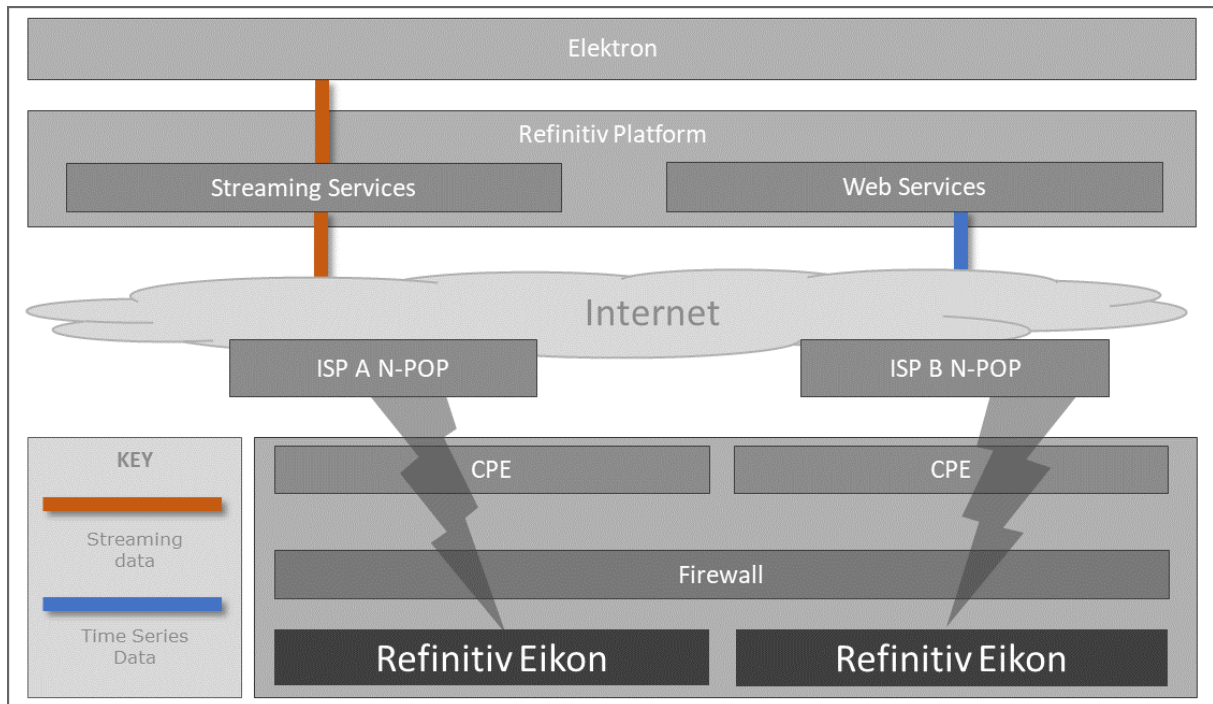
As data demands grow, we are evolving our connectivity solutions to allow lower unit costs for a given capacity. Delivery Direct is extending cost effective access to deep market content at low latency. Today, we have coverage in Japan, Hong Kong, Singapore, Australia, US and Western Europe, and this footprint is being extended to address all the locations our customers do business.



Internet

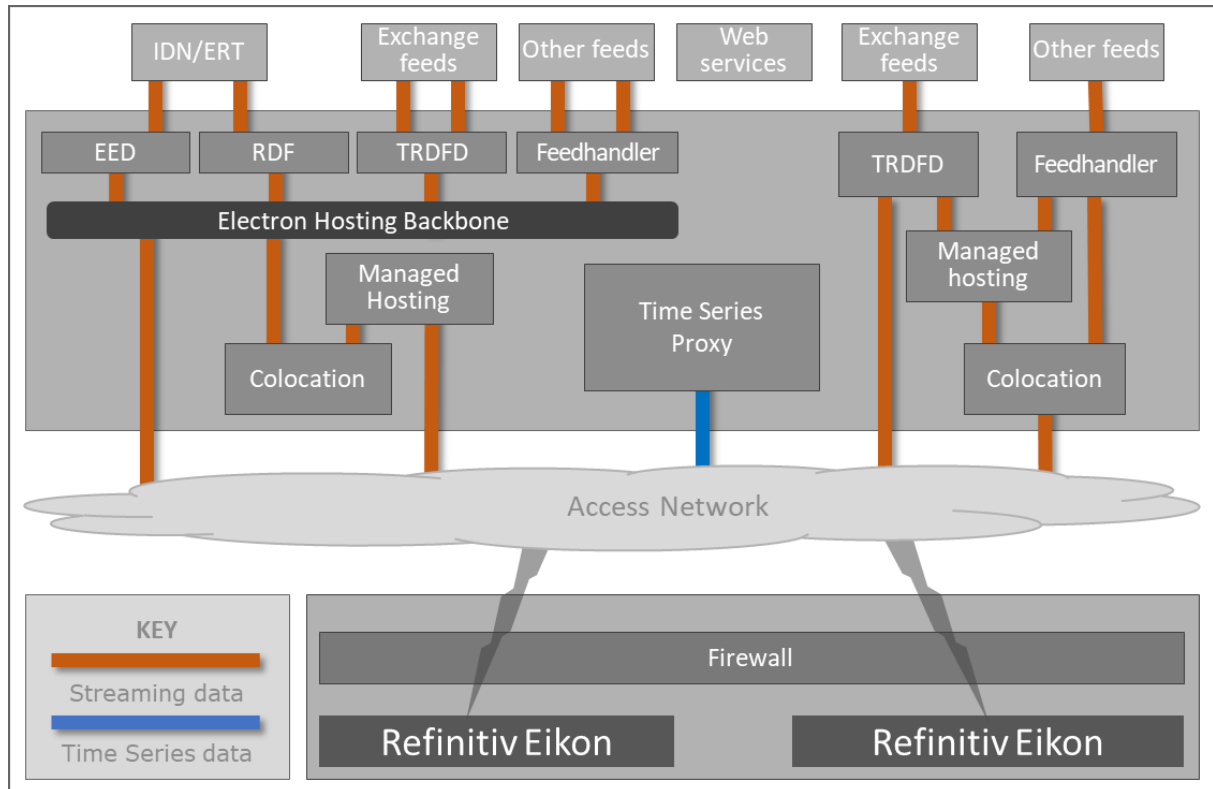
The Internet is enabling an increasing number of customers to connect with the global financial community worldwide.

Refinitiv Internet connectivity is enabling cost effective, high-performance, resilient and flexible access in more places globally, thus enabling your business to take advantage of a greater level of business agility.



Elektron Managed Services

The Elektron Managed Services solution offers market data, infrastructure, platforms, and connectivity. All as fully managed services from one of our global data centers and delivered at a lower total cost of ownership.



Hybrid environment

The Hybrid environment is a mixed site that deploys Eikon, Refinitiv Managed, and Customer Managed solutions on a single global network.

Other Refinitiv products

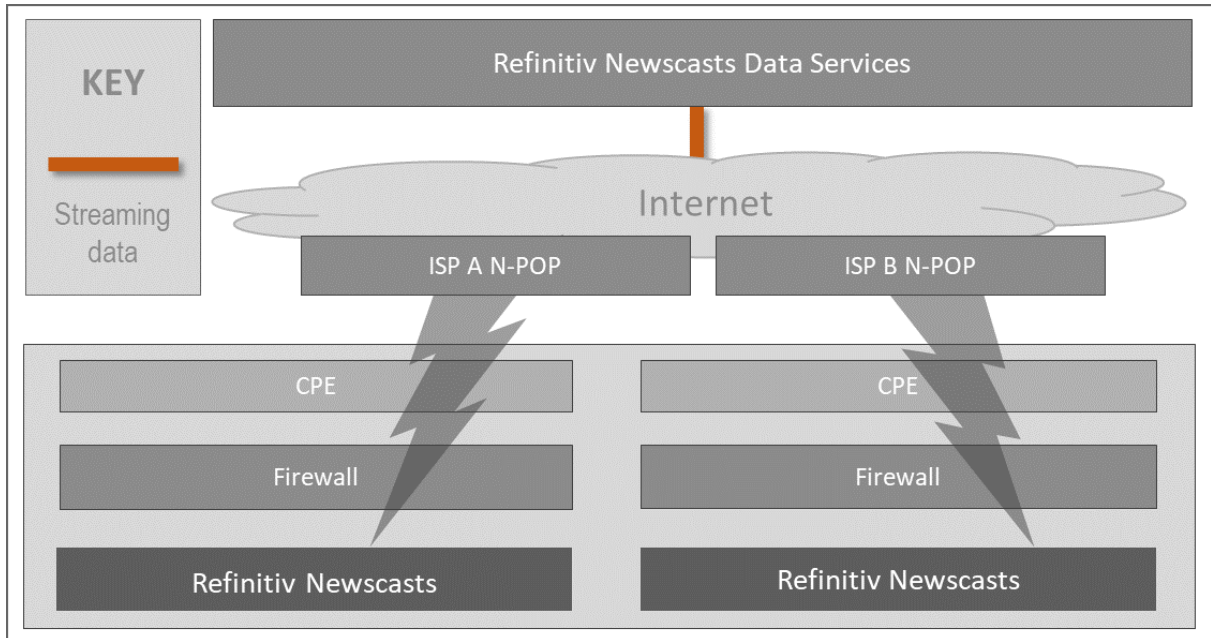
Refinitiv Newscasts

Important: Reuters Insider is being rebranded to Refinitiv Newscasts. This is currently planned for the fourth quarter of 2020.

Refinitiv Newscasts is a multimedia platform that delivers the following forms of media to each desktop or mobile device, from a global Content Delivery Network (CDN):

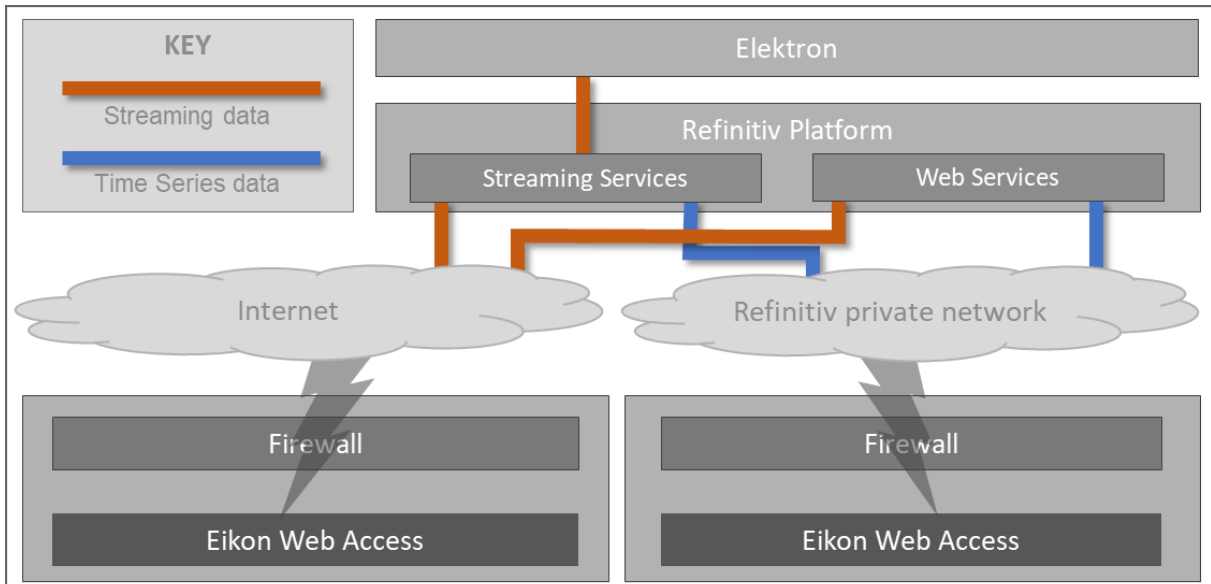
- Live video
- Video on-demand
- Audio content

Refinitiv Newscasts is powered by best-in-breed technology through a 3rd party agreement and is accessible to devices which have internet access.



Eikon Web Access

The Eikon Web Access solution is an additional access point, providing a selection of the most important features and information, without having to install the Eikon desktop or mobile application.



IP subnet / TCP port

Generic protocol and ports

Important: Reuters Insider is being rebranded to Refinitiv Newscasts. This is currently planned for the fourth quarter of 2020.

Protocol	Port Number	Refinitiv Services	Required For
TCP	1024+ ⇒ 80 1024+ ⇐ 80 1024+ ⇒ 443 1024+ ⇐ 443	Refinitiv Platform	<ul style="list-style-type: none"> Administration services View service Search & navigation service Time series service Messaging service Trading service Update service Refinitiv Remote Support (TRRS) Datastream service Refinitiv Newscasts (Internet Only) - see Important note above FXall
TCP	1024+ ⇒ 14002 1024+ ⇐ 14002 1024+ ⇒ 80 1024+ ⇐ 80	Real Time Data	<ul style="list-style-type: none"> Elektron Edge Customer Managed Advanced Distribution Server (ADS)
TCP/UDP	1024+ ⇒ 53 1024+ ⇐ 53	DNS Server	Domain Name Resolution from Domain Name Server
TCP	1024+ ⇒ 80 1024+ ⇐ 80 1024+ ⇒ 443 1024+ ⇐ 443 1024+ ⇒ 8443 1024+ ⇐ 8443 1024+ ⇒ 16000-16020	FIT Trading	TRFIT
TCP	1024+ ⇒ 10240 1024+ ⇐ 10240	Contribution	<ul style="list-style-type: none"> Insertlink Eikon Excel

Financial Community Network and Delivery Direct

Customer connectivity DNS Migration repository: <https://my.refinitiv.com/content/mytr/en/policies/private-network-overview.html>

Internet

Refinitiv does not divulge IP address information under any circumstances. This would prevent us from changing IP addresses, when needed and without notification. Additionally, these IP addresses may not always be under our direct control.

Firewall

HTTP 1.1 compliant proxy

Eikon requires HTTP/1.1, as shown in the [Internet Properties settings](#) section. If a proxy server does not support HTTP/1.1 or disables HTTP/1.1, the proxy sends HTTP/1.0 to the server. Therefore, Eikon key station gets a response from HTTP/1.0 Eikon platform, instead of HTTP/1.1.

Important: It is vital to enable an HTTP/1.1 compliant proxy to avoid the disconnect problem between Eikon key station and Eikon platform at the head end. The streaming service requires a persistent connection, which is supported in the HTTP/1.1 specification.

For further information, see <http://www8.org/w8-papers/5c-protocols/key/key.html>.

The cache mechanism of HTTP/1.0 is different from HTTP/1.1. In HTTP/1.0, a cache revalidates an entry using the *If-Modified-Since* header, which uses absolute timestamps with one-second resolution. This could lead to caching errors, either because of clock synchronization errors or lack of resolution. HTTP/1.1 introduced the concept of an opaque cache validate string, known as an *entity tag*. If two responses for the same resource have the same entity tag, then they must be identical.

Content filtering domain

If content filtering policy is implemented on the Internet proxy or firewall, the following DNS suffixes must be set to ALLOW for Eikon.

Important: Reuters Insider is being rebranded to Refinitiv Newscasts. This is currently planned for the fourth quarter of 2020.

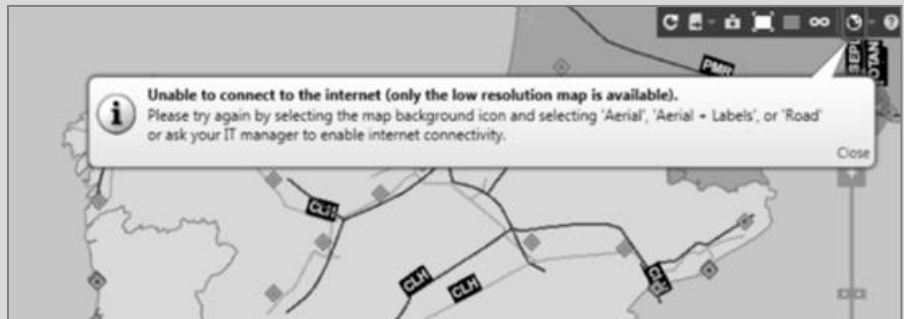
DNS	Refinitiv Service
*.session.rservices.com	Contribution address
api.widget.cx	Refinitiv Newscasts (Box Embed Widget) - see Important note above
autex.com	Autex
autexnow.com	Autex
bing.com	Search engine
bit.ly	Bit.ly Integration Information
blogs.reuters.com	News URL link
breakingviews.com	News URL link
cdn.mathjax.org	MathJax JavaScript display engine
chrome.google.com	Refinitiv Add-in for Office 365 (RAIFO) Chrome Extension
collab.platform.refinitiv.com	Eikon Messenger
comodo.com	Certificate Management
complinet.com	Refinitiv Accelus*
ctldl.windowsupdate.com	Microsoft Disallowed Certificate Trust List
cxvid-livecapture.s3.amazonaws.com	Refinitiv Newscasts (Recording Video and Images) - see Important note above
depth.finance	Ironfly Market Depth App (Add-on)
dev.virtualearth.net	Interactive Map
dkro418ulhd2a.cloudfront.netic	Refinitiv Newscasts - see Important note above

DNS	Refinitiv Service
ec2-54-214-9-26.us-west-2.compute.amazonaws.com	Interactive Map
edgefcs.net	Street Event contents
embed.widget.cx	Refinitiv Newscasts (Box Embed Widget) - see Important note above
fxall.com	Trading Service
globalrelay.com	Refinitiv Messaging Compliance*
googleapis.com	Google
kaltura.com	Refinitiv Newscasts - see Important note above
lipperweb.com	Lipper Market Insight
loanconnector.com	Loan Connector
loanpricing.com	Load Pricing
m3u8service.hosted.cx	Refinitiv Newscasts - see Important note above
media-server.com	Street Event content
pictures.reuters.com	News URL link
r.reuters.com	News URL link
refinitiv.com	Refinitiv Webservices
refinitiv.net	Refinitiv Webservices
reut.rs	Bit.ly Integration Information
reuters.com	News URL link
reutersinsider.com	Refinitiv Newscasts - see Important note above
Note: Refinitiv will be migrating to hosted.newscasts.refinitiv.com	
reutersmedia.net	News URL link
salesforce.com	Eikon Migration Tools
salesforceliveagent.com	Eikon Messenger
sdn.reuters.com	Securitized Derivatives Network
Note: Refinitiv will be migrating to sdn.refinitiv.com	
sectigo.com	Certificate Management
secure.force.com	Eikon Messenger
streetsight.thomson.com	Street Sight
symantec.com	Certificate Management
thomson.112.2o7.net	Refinitiv Newscasts (used for analytic and report of user interactions) - see Important note above
thomsonreuters.com	Refinitiv Webservices
thomsonreuters.net	Refinitiv Webservices
thomsonreuters.wdtinc.com	Interactive Map
tiles.virtualearth.net	Interactive Map
tmsnrt.rs	Bit.ly Integration Information
today.reuters.com	News URL link
topnews.reuters.com	News URL link

DNS	Refinitiv Service
tradeweb.com	Tradeweb
trainingportal.us	Refinitiv E-Learning
trmcs-documents.s3.amazonaws.com	Central Bank Polls [CBP]
uk.reuters.com	News URL link
webtrendslive.com	Eikon Migration Tools

Notes:

- Customers can use thomsonreuters.com, reuters.com, and refinitiv.com instead of adding multiple entries from the table.
- Third Party apps in Eikon might require access to specific domain on the internet which isn't covered within this guide. It is advisable to contact the Developer of the app directly to enquire if any additional access to the domain on the Internet is required.
- The Interactive Map ► (opposite) works in Low Resolution mode only on a private network (Delivery Direct) where there is no internet connection.



HTTPS tunneling

Eikon uses HTTPS tunneling to connect the Eikon platform to the streaming service. In some proxy servers, HTTP/HTTPS tunneling is disabled by default, for example, Websense. However, other proxy servers can be set to enable or disable tunneling, for example, Blue Coat ProxySG.

HTTPS tunneling must be enabled for the following URLs:

Network	URL Allowance
Internet	*.cp.thomsonreuters.com *.refinitiv.com *.thomsonreuters.net *.refinitiv.net
Private Network	*.cp.extranet.thomsonreuters.biz *.refinitiv.biz *.thomsonreuters.net *.refinitiv.net

Exe files (Core package)

The following processes are based in the Eikon Install and Eikon Cache folders.

Firewall	Process Name	Services
X	Eikon.exe (.eik file extension)	Eikon 4.0 Desktop (Main Eikon process)
X	EikonBox.exe	Eikon 4.0 (Eikon viewer process)
	EikonBoxNet.exe	Eikon 4.0 (Eikon viewer .Net process)

Firewall	Process Name	Services
	EikonDM.exe ⁴	Eikon Configuration Manager
	TRDiagnostic.exe	Eikon Office Diagnostics tool
	TRUserServiceHostv4.exe	Refinitiv Common Office User Service Daemon (for Microsoft Office)
	InsertLink.exe ²	InsertLink Client Application
	InsertLinkConfigMgr.exe ²	InsertLink Configuration Manager
	MSWin.exe ¹	MetaStock Professional for Eikon
	ConnectionManagement.exe	Eikon 4.0 Connection Management
	DSChartingUtil.exe ³	Invoked from Add-ins for navigating to the Charting website
	ReportManager.exe ³	Invoked from Add-ins for Chart Report Generation
	EikonSupportTool.exe	Collects and sends dump and log files to the Eikon platform to facilitate investigation
	CPDisplayMessage.exe	Displays messages within the Eikon UI for various components
	EikonUtilityToolbox.exe	Allows end-users to clear the application cache, log files, select automatic sign-in, and choose connections
	IEBrg.exe	Handles RACE URLs (reuters:// protocol and a few others) and passes them to Eikon
	KMAPI.exe	Supports screenshot sharing from any Eikon app, through MS Outlook
	KMAPIx64.exe	Supports screenshot sharing from any Eikon app, through MS Outlook (64-bit version)
	KobraConfigDump.exe	Writes Eikon configuration files in the logs folder
	PLMigrationTool.exe	Eikon Office migration tool
	PLReportViewer.exe	Eikon Office migration tool - Report viewer

Where:

¹ This process is required for Refinitiv MetaStock Pro add-ons.

² This process is required for Refinitiv InsertLink add-on.

³ This process is required for DataStream for Microsoft Office. (DFO).

⁴ The EikonDM.exe process is also running in %TEMP% location.

Exe files in apps

App folder name	Name of exe file
THOMSONREUTERS.EIKON.BATCHENGINE	TR.Batch.Printer.exe
THOMSONREUTERS.EIKON.BUSSPY	EikonBusSpyApp.exe
THOMSONREUTERS.EIKON.BUSSPY	protogen.exe
THOMSONREUTERS.EIKON.LIBRARYADMIN	ThomsonReuters.UpdateSystem.Admin.Introspector.exe
THOMSONREUTERS.EIKON.LOGVIEWER	LogViewerHost.exe
THOMSONREUTERS.EIKON_OFFICE.PDFLINK	DocumentManager.exe
THOMSONREUTERS.EIKON.PERFVIEWER	PerfViewerHost.exe
THOMSONREUTERS.EIKON.REMOTESUPPORTTOOL	embedhook-x86.exe
THOMSONREUTERS.EIKON.REMOTESUPPORTTOOL	spinner.exe
THOMSONREUTERS.EIKON.SUBMITABUG	EikonBugsJiraHeartbeat.exe
THOMSONREUTERS.EIKON.SUBMITABUG	EikonBugsJiraUploader.exe

App folder name	Name of exe file
THOMSONREUTERS.EIKON.SUBMITABUG	EikonBugsLauncher.exe
THOMSONREUTERS.INTERNAL.ITRACKER	iTracker.exe
THOMSONREUTERS.SDK.UI.CONTROLSGALLERY	ThomsonReuters.Desktop.SDK.UI.ControlsGallery.exe
TR.DATASTREAMCHARTING	DSChartingUtil.exe
TR.DATASTREAMCHARTING	FontSetup.exe
TR.DATASTREAMCHARTING	ICAddinMetaFlyWrapper.exe
TR.DATASTREAMCHARTING	Thomson.Reuters.Datastream.Charting.DSChartingCustomUriExport.exe
TR.DATASTREAMCHARTING	Thomson.Reuters.Datastream.Charting.ICAddinSchedulerConversionTool.exe
TR.DATASTREAMCHARTING	ThomsonReuters.ReportManager.exe
TR.PRESENTATIONTOOLS	ThomsonReuters.ProgressReportingService.exe
TR.OFFICE.CORE / TR.OFFICE.CORE64	TRDiagnostics.exe
TR.OFFICE.CORE / TR.OFFICE.CORE64	TRUserServiceHostV4.exe

Note: All the above files are in the user profile: `...\Eikon User\Cache\LibraryCache\Apps\`

HTTP user agent

When you visit a webpage, an Internet browser sends the user-agent string to the server hosting the site that the user is visiting. This string indicates which browser the user is visiting, its version number, and detail about your system, such as operating system and version. The web server can use this information to provide content that is tailored for user specific browser.

Understand User-Agent String on MSDN: [http://msdn.microsoft.com/en-us/library/ms537503\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms537503(v=vs.85).aspx)

To set a rule to block unknown web browsers, you need to allow the signatures for Eikon to be accessible.

From Eikon 4.0.36 and above, the following are the new user agent string: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.2454.0.50 EikonViewer/45.2454.0.50 Safari/537.36.

The following is an example user-agents list running on Windows 7, IE 9, .Net 3.5, and .Net 4.0 running Eikon 4.0.

Process	User-Agent	Signature
Eikon.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0;	MSIE
Excel.exe	SLCC2;.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.3)	
	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2;.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.3; Refinitiv File Download 6.0)	MSIE
	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; NET CLR 1.1.4322;.NET CLR 2.0.50727; .NET CLR 3.0.04506.30; InfoPath.1) AAA-AS/RDP	MSIE
	Mozilla/5.0 (Windows NT 6.1; AppleWebKit/537.36 (KHTML, Like Gecko) Chrome/45.2454.0.50 Safari/537.36. Eikon-Renderer/17.1.7.4867 Eikon/7.1.270	Eikon
	Refinitiv Desktop Agent/2.9.0.18 Bootstrap/2.9.0.10 Implementation/2.9.0.12	Refinitiv Desktop Agent

Process	User-Agent	Signature
	Mozilla/5.0 (compatible; MSIE 9.0; Win 32; Trident/5.0)	MSIE
	RFA	RFA
	Microsoft-CryptoAPI/6.1	Microsoft-CryptoAPI
TRUserServiceHostV4.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2;.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.3; Refinitiv File Download 6.0)	MSIE
InsertLink.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2;.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.3; Refinitiv File Download 6.0)	MSIE
	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322;.NET CLR 2.0.50727; .NET CLR 3.0.04506.30; InfoPath.1) AAA-AS/RDP	MSIE
	RFA	RFA
EikonDM.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2;.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; Refinitiv File Download 6.0)	MSIE
EikonBox.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2;.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.3)	MSIE

To support HTML5, since version 2.0 SR1, Eikon integrates Chromium objects as an HTML5 rendering. If you have rules to filter or allow Microsoft Internet Explorer only, the following rules need to be added:

	Action
Allow Internet Explorer only / Block unknown Web Browser	Create rule to allow all the signatures on user-agent, as shown in the above table
Block Google Chrome	Create a rule to allow Eikon and Chrome Create rule to deny Chrome without Eikon

Proxy

Proxy terminology

Basic authentication

The *Basic* authentication scheme is based on the model that the client must authenticate itself with a user ID and a password for each realm. The realm value should be considered an opaque string, which can only be compared for equality with other realms on that server. The server services the request, only if it can validate the user ID and password for the protection space of the Request-URI. There are no optional authentication parameters.

For Basic, the framework described above is utilized as follows:

```
challenge    = "Basic" realm
credentials = "Basic" basic-credentials
```

Upon receipt of an unauthorized request for a URI within the protection space, the origin server may respond with a challenge. For example:

```
WWW-Authenticate: Basic realm="WallyWorld"
```

where "WallyWorld" is the string assigned by the server to identify the protection space of the Request-URI. A proxy may respond with the same challenge using the Proxy-Authenticate header field.

To receive authorization, the client sends the user ID and password, separated by a single colon (:) character, within a base64 [7] encoded string in the credentials.

```
basic-credentials = base64-user-pass
base64-user-pass = <base64 [4] encoding of user-pass>
user-pass = userid ":" password
userid = *<TEXT excluding ":">
password = *TEXT
```

Windows NT LAN Manager (NTLM) authentication

Windows Challenge/Response (NTLM) is the authentication protocol used on networks that include systems running the Windows operating system and on standalone systems.

Note: The Microsoft Kerberos security package adds greater security than NTLM to systems on a network. Although Microsoft Kerberos is the protocol of choice, NTLM is still supported. NTLM must also be used for logon authentication on stand-alone systems.

For more information about Kerberos, see Kerberos authentication on page 21.

NTLM credentials, based on data obtained during the interactive logon process, consist of:

- Domain name
- Username, and
- One-way hash of the user's password

NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication performs a calculation that proves it has access to the secured NTLM credentials.

Interactive NTLM authentication over a network typically involves two systems:

- Client system, where the user is requesting authentication, and
- Domain controller, where information related to the user's password is kept

Noninteractive authentication, which may be required to allow a user that has logged-on already to access a resource, such as a server application, typically involves three systems:

- Client
- Server, and
- Domain controller, which does the authentication calculations on behalf of the server

Kerberos authentication

The Kerberos protocol defines how clients interact with a network authentication service. Clients obtain tickets from the Kerberos Key Distribution Center (KDC), and they present these tickets to servers when connections are established. Kerberos tickets represent the client's network credentials.

The Kerberos authentication protocol provides a mechanism for mutual authentication between entities before a secure network connection is established. The Kerberos protocol assumes that transactions between clients and servers take place on an open network where most clients and many servers are not physically secure, and packets traveling along the network can be monitored and modified at will. The assumed environment is like today's Internet, where an attacker can easily pose as either a client or a server and can readily eavesdrop on or tamper with communications between legitimate clients and servers.

Qualified proxy

Eikon is qualified to use the following proxies for authentication:

Proxy	Authentication Method
Apache or Squid	Basic
Microsoft ISA or Microsoft Fore Front	Integrated (NTLM/Kerberos)

Notes:

- Microsoft ISA is partial HTTP 1.1 compliant. See more detail in <http://technet.microsoft.com/en-us/library/cc302548.aspx>. It is strongly recommended to upgrade to an HTTP 1.1 proxy compliant.
- Squid 3.1 and 3.2 claims HTTP 1.1 support. Earlier versions do not support HTTP 1.1 because it cannot fully handle Expect: 100-continue 1xx responses, and/or chunked messages. It is strongly recommended to use version 3.1, 3.2. See more detail in <http://wiki.squid-cache.org/Features/HTTP11>.

Other related proxy configuration

Web Proxy Auto-Discovery (WPAD) protocol

Disable the **Automatically detect settings** configuration in Internet Explorer to avoid any potential latency and connection issues with Eikon 4.0.29 or below.

Eikon version 4.0.30 onwards manages this configuration. So, it is no longer mandatory to disable the setting.

Download policy

Eikon installation packages use executable (*.exe) and 7zip format (*.eik) files to guarantee the best compression rates for the downloaded packages.

These files are checked and signed by Refinitiv before they are published through the update service. Subsequent updates are also packaged as executable files.

The site or workstation firewall must be configured to allow downloading of these packages through the HTTP protocol (port 80):

Domain	Rebranded Domain ¹	Download
customers.thomsonreuters.com		For installation bootstrap, system Test standalone over Internet
*.download.cp.thomsonreuters.net ²	cdn.refinitiv.net ²	For Eikon packages on Update Service and Eikon Apps
*.download.cp.thomsonreuters.com ²	cdn.refinitiv.com ²	
*.download.cp.extranet.thomsonreuters.biz ²	cdn.extranet.refinitiv.biz ²	For Eikon packages on Update Service and Eikon Apps

Eikon desktop proxy process

Desktop Proxy is a recent Eikon component aimed at handling seamless failover of Eikon web requests into Refinitiv data centers. If Desktop Proxy is activated, web proxies that enforce user authentication through the Kerberos or Digest protocols, without possible fallback to other schemes such as NTLM or Basic, may disrupt Eikon connectivity.

¹ For further information regarding domain rebranding, see [Product Change Notification 11803 – Refinitiv domains](#).

² These domains use Amazon CloudFront as the source of Eikon package and its components as a storage.

Proxy script

Eikon can process proxy script, but the following Microsoft principles must be followed:

- The Content-Type response header must be application/x-ns-proxy-autoconfig
- Or the URL file extension must be .pac, .js, or .dat
- And the proxy script address cannot be defined as file://<URL>

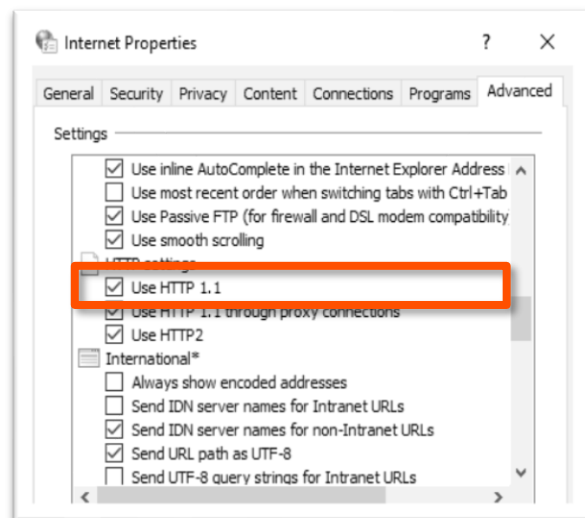
Internet property settings

Eikon supports HTTP 1.1, TLS1.0, 1.1 and 1.2 terminologies. Ensure that these options are enabled in **Internet Properties**, under the **Advanced** tab.

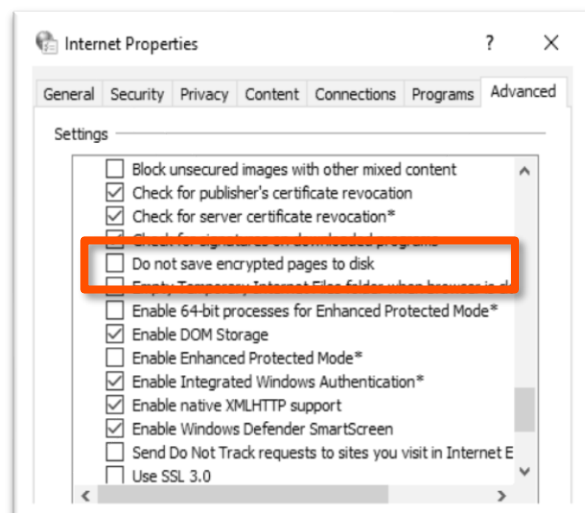
Note: SSL 3.0 is discontinued and discouraged from support due to a Poodle vulnerability.

To do this:

1. Enable HTTP 1.1

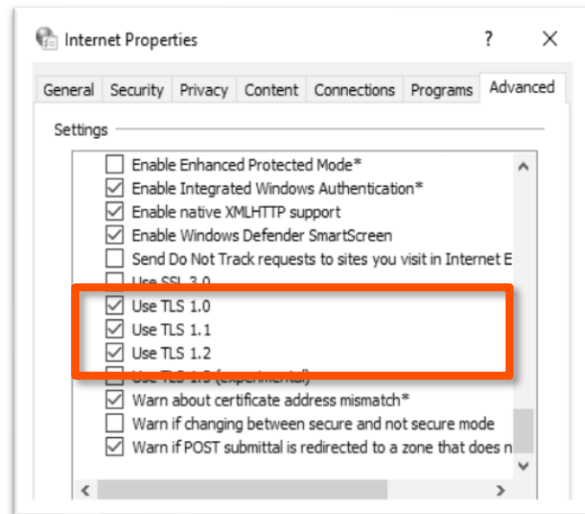


2. Disable Do not save encrypted pages to disk



3. Enable TLS 1.0, 1.1 and 1.2

Note: Information about SSL 3.0 end of support could be found on PCN: 7929 and 7994.



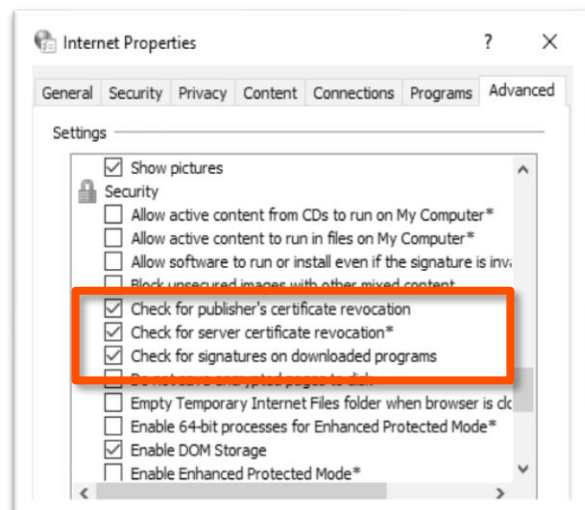
4. (Recommended) For host with no internet access, Disable the following **Certificate revocation** options:

- Check for publisher's certificate revocation
- Check for server certificate revocation
- Check for signatures on downloaded programs

Note: If an Internet connection is available, these options should be left enabled.

Impact (if not implemented):

Eikon displays a popup message, requesting the updating of certificates at startup, during operation, and when exiting Eikon.



Certificate management

For security purposes, the Eikon and Eikon Excel for Wealth Management packages require up-to-date certificates during installation, start-up and update. To ensure continuous access to Eikon, it is crucial that the approach taken for certificate management validation must be appropriate for the user's network.

The SSL certificate is used when validating the status of the certificates during Eikon authentication, signing, or encryption operations. Failures to validate the certificates prevent the product from working properly. The validation can be either CRL- or OCSP-based on the user's operating system. For further information, see Certificate revocation below.

The certificates must be validated through the Internet or Internal Certificate Infrastructure, Microsoft Online Responder, OCSP Proxy and so on, unless delegated to an internal certificate management system.

Certificate authorities

Eikon uses the following root certificates:

	Trusted Root Certificate Authorities		Intermediate Certificate Authorities		
	CN	O	Issued by	CN	O
Symantec Corporation	Symantec Class 3 Public Primary Certification Authority – G4	Symantec Trust Network	Symantec Class 3 Secure Server CA – G4	VeriSign Class 3 Public Primary Certification Authority – G5	VeriSign Trust Network
Comodo	COMODO RSA Certification Authority	COMODO CA Limited	COMODO RSA Organization Validation Secure Server CA	COMODO RSA Organization Certification Authority	Comodo CA Limited

Notes:

- We strongly recommend that certificates marked as Intermediate are also installed on machines for proper Eikon usage.
- The Trusted root certificates that are required by Microsoft Windows are listed in the following knowledge base article <https://support.microsoft.com/en-us/help/293781/trusted-root-certificates-that-are-required-by-windows-server-2008-r2>. It is necessary that all of them are available on the machine.

Certificate revocation

Public key infrastructure (PKI) consists of multiple components, including certificates, certificate revocation lists (CRL), and certification authorities (CA). In most cases, applications that depend on X.509 certificates, such as Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), and smart cards, are required to validate the status of the certificates used when performing authentication, signing, or encryption operations. Certificate status and revocation checking is the process by which the validity of certificates is verified, based on two main categories: time and revocation status.

- Time certificates are issued for a fixed period of time and considered valid as long as the expiration date of the certificate is not reached, unless revoked before that date.
- Revocation status certificates can be revoked before their expiration date because of multiple reasons, such as key compromise or suspension. Before performing any operation, applications often validate that the certificate was not revoked.

Supported certificate status determination methods

Windows operating systems from Vista onwards support both CRL and OCSP as a method of determining certificate status. The OCSP support includes both the client component as well as the Online Responder, which is the server component.

Certificate revocation checking

When an application performs a certificate evaluation, the validation is performed on all certificates in that certificate's chain. This includes every certificate from the end-entity certificate presented to the application to the root certificate.

When the first certificate in the chain is validated, the following process takes place:

1. The certificate chaining engine attempts to build the chain for the certificate inspected, by:
 - querying the local certificate store, or
 - downloading from one of the URLs available in the inspected certificate's authority information access extensions.

For all certificate chains that end in a trusted root, all certificates in the chain are validated. To do this, verify that:

- the server name matches the certificate common name
- each certificate's signature is valid
- the current date and time fall within each certificate's validity period
- each certificate is not corrupt or malformed

Note: Once the certificates have been installed then it will no longer verify with the certificate owner.

2. Each certificate in the certificate chain is checked for revocation status. Revocation checking is performed either by using a CRL or OCSP, based on the certificate configuration.
3. After the validation check is completed, the certificate chaining engine returns the results of the validation check to the application that originated the validation request. The results indicate whether:
 - all certificates in the chain are valid
 - the chain terminates at a non-trusted root CA
 - any certificates in the chain are not valid, or
 - the revocation status for any of the certificates in the chain cannot be determined

For more information, see Certificate Revocation and Status Checking at:

<http://go.microsoft.com/fwlink/?LinkID=27081>

Certificate Revocation List (CRL)

A CRL is a file, created and signed by a CA, that contains serial numbers of certificates that have been issued by that CA and are revoked. In addition to the serial number for the revoked certificates, the CRL also contains the revocation reason for each certificate and the time the certificate was revoked.

CRL types

Currently, two types of CRL exist:

- Base: A complete list of revoked certificates
- Delta: Only those certificates that have been revoked since the last publication of a base CRL

Drawbacks

The major drawback of CRL is their potentially large size, which limits the scalability of the CRL approach. The large size adds significant bandwidth and storage burdens to the CA and relying party, and therefore limits the ability of the system to distribute the CRL. Bandwidth, storage space, and CA processing capacity can also be negatively affected if the publishing frequency gets too high. Numerous attempts have been made to solve the CRL size issue through the introduction of partitioned CRL, delta CRL, and indirect CRL.

Another drawback of CRL is latency; because the CRL publishing period is predefined, information in the CRL might be out of date until a new CRL or delta CRL is published.

All these approaches have added complexity and cost to the system, without providing an ideal solution to the underlying problem.

Online Certificate Status Protocol (OCSP)

OCSP is a Hypertext Transfer Protocol (HTTP) that allows a relying party to submit a certificate status request to an OCSP responder. This returns a definitive, digitally signed response indicating the certificate status. The amount of data retrieved per request is constant regardless of the number of revoked certificates in the CA. Most OCSP responders get their data from published CRL and are therefore reliant on the publishing frequency of the CA. Some OCSP responders can, however, receive data directly from the CA's certificate status database and consequently provide near real-time status.

Drawbacks

Scalability is the major drawback of the OCSP approach. Since it is an online process and is designed to respond to single certificate status requests, it results in more server hits, requiring multiple and sometimes geographically dispersed servers to balance the load.

The response signing and signature verification processes also take time, which can adversely affect the overall response time at the relying party. Since the integrity of the signed response depends on the integrity of the OCSP responder's signing key, the validity of this key must also be verified after a response is validated by the client.

Troubleshooting

Eikon uses the Microsoft Crypto API to check and download the CRL from a CRL distribution point. The Crypto API internally uses the WinHTTP API to download the HTTP-based URL for the CRL distribution point.

If the proxy is not reachable or is incorrect, WinHTTP is not able to download the CRL and the certificate revocation check fails. Therefore, Eikon cannot create a secure connection to the platform, causing the program to shut down or display an error message.

To discover a proxy server:

1. Check the static proxy settings

Windows	Command
Windows 7, 8, and 10	Netsh.exe winhttp show proxy

2. If there is no static proxy setting, the API tries to retrieve the Internet Explorer settings in the following order. The following registry locations are queried, based on the executing identity:

Windows	Command
Current User	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Network Service	HKEY_USERS\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Local System	HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Local Service	HKEY_USERS\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Any Other user	HKEY_USERS\<<SID of that user>> \Software\Microsoft\Windows\CurrentVersion\ Internet Settings

3. If the Internet Explorer proxy settings are not present for the executing user or if the Internet Explorer settings for the process identity indicate **Automatically detect settings** or **Use automatic configuration script**, then the Crypto API will try to automatically discover a proxy for the CRL in question.

For more information, see Microsoft KB 2623724: <http://support.microsoft.com/kb/2623724>

WinHTTP proxy configuration

For Windows Vista onwards, use `Netsh.exe winhttp`.

Note: `Netsh.exe` requires administrative rights to modify machine configuration.

Usage

The following examples show the syntax use for various commands for Windows Vista onwards:

Command Line	Description
<code>Netsh winhttp show proxy</code>	Display the current WinHTTP proxy settings
<code>Netsh winhttp reset proxy</code>	Set direct access
<code>Netsh winhttp import proxy source=ie</code>	Import proxy setting from current user's Internet Explorer manual settings
<code>Netsh winhttp set proxy proxy-server bypass-list="optional-by-pass-list"</code>	Specify one proxy server and optional list of hosts that should be accessed directly.
<code>Netsh winhttp set proxy proxy-server="proxy-server-list " bypass-list="optional-by-pass-list"</code>	Specify one or more proxy server and optional list of hosts that should be accessed directly.

Where:

Proxy-server-list
Proxies are listed in a specific protocol as Windows Vista onwards, where protocol is either http or https, and proxy_name is the name of the proxy server.
For Windows 10, protocol=proxyname:port;

Optional-bypass-list
The list contains host names or an IP address that is known locally. This list can contain wildcards (*) that cause the application to bypass the proxy server for addresses that fit the specified pattern. For example, both *.microsoft.com and *.org are acceptable wildcard patterns.

Note: The wildcard character must be the left-most character in the list. So, for example, myserver.* is not supported.

To list multiple addresses and host names, separate them with blank spaces or semicolons in the proxy bypass string. If the "<local>" macro is specified, the function bypasses any host name that does not contain a period.

Windows 7 example

- Import the current Internet Proxy setting to WinHTTP (for manual setting on Internet Explorer):

```
C:\> netsh winhttp import proxy source=ie
Current WinHTTP proxy settings under:
Proxy Server(s) : 10.42.72.142:8080
Bypass List: <local>
```

- Set up proxy1.test.com as a proxy for WinHTTP and bypass proxy for the local domain, *.extranet.thomsonreuters.biz and *.thomsonreuters.net:

```
c:\>netsh winhttp set proxy proxy1.test.com bypass-list ="<local>;
*.extranet.thomsonreuters.biz;*.thomsonreuters.net"
Current WinHTTP proxy settings under:
Proxy Server(s) : proxy1.test.com
Bypass List : <local>;*.extranet.thomsonreutes.biz;*.thomsonreutes.net
```

- Set up Proxy1.test.com for an http protocol on port 80 and Proxy2.test.com for https protocol on port 3128, and direct access to the local domain, *.extranet.thomsonreuters.biz and *.thomsonreuters.net:

```
C:\>netsh winhttp set proxy proxy-server="http=proxy1.test.com:8080;  
https=proxy2.test.com:3128" bypass-  
list="<local>;*.extranet.thomsonreuters.biz;*.thomsonreuters.net"  
Current WinHTTP proxy settings under:  
Proxy Server(s) : http=proxy1.test.com:8080; https=proxy2.test.com:3128  
Bypass List : <local>;*.extranet.thomsonreuters.biz;*.thomsonreuters.net
```

- Clear the WinHTTP configuration

```
C:\> netsh winhttp reset proxy  
Current WinHTTP proxy settings:  
Direct access (no proxy server).
```

Configuration for Eikon Desktop

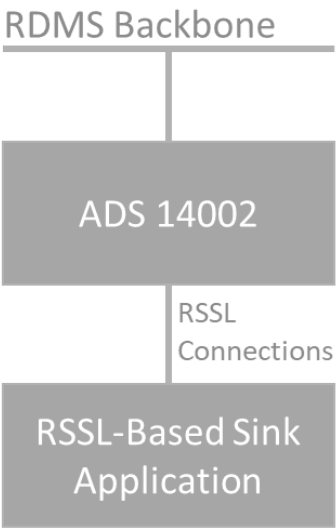
Refinitiv Data Management Solutions

To provide real-time data, the Refinitiv Data Management Solution (RDMS) components (Advanced Distribution Server - ADS) requires the network service to be made available through TCP/IP. ADS can be configured to listen for RSSL-based inbound connections on port rmds rssl sink (14002).

To allow Eikon to receive real-time services from ADS, on the client machine, define these services in the file %systemroot%\System32\drivers\etc\services.

The following table describes the TCP/IP standard ports for the Refinitiv Enterprise Platform:

Protocol	Port Number	Refinitiv Services	Required For
TCP	1024 + ⇒ 14002	ADS	Realtime Data Service (RSSL)
	1024 + ⇐ 14002		



Configuration service

Eikon reads its base configuration from the hosted configuration services. This contains most of the configuration parameters.

Basic configuration

This is used by Refinitiv Hosted and Refinitiv Managed users.

On startup of Eikon, the user's configuration parameters are read from the Document and Preference Store (DAPS) and Common Platform Admin Portal (CPAC) Server. All other configuration settings are downloaded from the Refinitiv platform.

Notes:

Refinitiv Hosted: There are no configuration settings stored locally apart from the logging levels. These can be set in Configuration Manager but nothing else can be configured locally.

Refinitiv Managed: Same as above. However, in this case, the following hostnames need to be resolved by the desktop:

- tr-streaming-proxy (streaming proxy or Elektron Edge IP Address)
- tr-timeseries-proxy (Time Series Proxy IP Address)

Other configuration

There are three deployment mode levels that provide control over the configuration for Refinitiv Customer Managed site:

- Customer Managed (Local Configuration Files)
- Customer Managed (Using Configuration Proxy)
- Customer Managed (Hosted Configuration)

Local configuration files

As the Eikon Desktop is mainly registry free, the configuration is file-based. The main configuration files are:

- OverrideConfiguration.xml (Customer Managed users only)
- RFA.rfa-configuration-file (Customer Managed users only)
- MachineConfiguration.xml (all deployments)

When Eikon is installed by a user with administrative rights, these files are in the following directory by default:

```
<installation_path>\Eikon\<X,Y,Z>\Config
```

When the Configuration Manager is started, its settings are imported from the MachineConfiguration.xml file.

On Eikon startup, the user's configuration parameters are read from CPAC Servers and combined with settings from the local configuration files, OverrideConfiguration.xml and RFA.rfa-configuration-file. These two configuration files are then merged with the common platform configuration parameters, which were loaded during Eikon startup, to produce the desktop configuration.

When Eikon shuts down, it rewrites its preference values to the DAPS Server.

Configuration Proxy

Configuration Proxy is a user-owned web server that allows users to centrally manage the Eikon desktop configuration. It consists of an XML-based configuration data structure that the user hosts on an Internet web server. It removes the dependency on the Configuration Manager and the need to deploy configuration files to each workstation.

To set up Eikon to obtain its configuration files from the Configuration Proxy:

1. Configure Eikon as Customer Managed (using Configuration Proxy) in Configuration Manager.
2. After confirming that the install is functioning correctly, copy the following files to the web server folder on your Configuration Proxy:
 - OverrideConfiguration.xml
 - RFA.rfa-configuration-file
3. Configure Eikon to access the configuration files on the Configuration Proxy.

Hosted Configuration

The Hosted Configuration process is a method of uploading a user's local configuration details to the Refinitiv Platform configuration service. This allows users to download the site configuration, whilst signing into Eikon.

The following files would need to be uploaded to the common platform:

- OverrideConfiguration.xml
- RFA.rfa-configuration-file

Elektron Managed Services

Users must add a host record entry for Refinitiv Data Platform services into local DNS servers with a local server IP address. The entry should use the same DNS suffixes that were used when setting up on the Advanced TCP/IP settings on the workstation.

Deployed Services	DNS entry
ADS server	tr-elektronhosting-ads
Time series proxy	tr-elektronhosting-timeseries-proxy
Update proxy	tr-elektronhosting-update-proxy

For the ADS server entry, users can choose to use multiple ADS names. So, if one is not available, the server asks their local DNS for the next name.

DACS server

DACS allows users to control who can access and use various sets of data in their financial information management system.

Protocol	Port Number	Refinitiv Services	Required For
TCP	1024+ ⇒ 8250	DACS Server	Permission Service DACS Daemon
	1024+ ⇐ 8250		
	1024+ ⇒ 8261	ADS	Permission Proxy
	1024+ ⇐ 8261		
	1024+ ⇒ 8302	DACS Server	Permission Service DACS Daemon
	1024+ ⇐ 8302		

Elektron Managed Services Protocol & Port

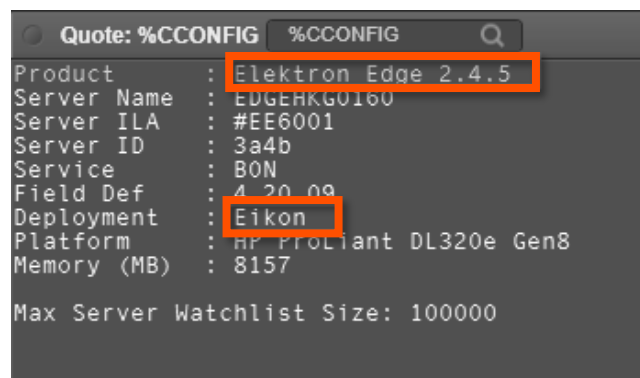
Protocol	Port Number	Refinitiv Services	Required For
TCP	1024+ ⇒ 8261 1024+ ⇐ 8261	Permission Proxy	Elektron Managed service

Elektron real-time proxy

Elektron Edge version 2.4.5, which has been developed exclusively for Refinitiv Managed Eikon customers. It is a direct replacement for the streaming proxy device that is currently in use and facilitates the obsolescence of both BT Delivery and IDN, upon which the streaming proxy is dependent.

For further information, see the sections Refinitiv Managed and Network configuration requirements.

Users can simply verify the deployment mode from Eikon Desktop by entering %CCONFIG RIC into the **Quote** box. Results should be like those shown in the example opposite, where the **Product** field indicates the Elektron version and the **Deployment** field indicates the client type, **Eikon**.



Time series proxy

The time series service is a centrally managed service that provides time series data to Eikon, in place of the older DBU. Eikon retrieves the historical data from the time series service and combines this with streaming data from streaming service or local Refinitiv Data Management Solutions (formerly TREP), providing time series updates to the desktop.

Refinitiv Hosted	In this deployment, Eikon time series desktop components, such as Metastock Object and Time and Sales, connect to the time series service, using the time series API to chart and display timeseries data.
Refinitiv Managed Customer Managed	In these deployments, Eikon time series desktop components connect to the time series proxy, using the time series API to chart and display timeseries data.

Eikon and time series proxy connectivity

The option to use a time series proxy is configured in Administration services for the customer.

The parameter `TIMESERIES.TSI.WEB_CLIENT_WRAPPER.WEB_CLIENT.LOCAL_CACHE_DEPLOYED` determines whether the user is configured to use a time series proxy:

TRUE The user retrieves timeseries data from a local time series proxy.

FALSE The user retrieve timeseries data directly from time series service

Note: The parameter should be set to **TRUE** for Refinitiv Managed and Refinitiv Customer Managed deployments that have a deployed time series proxy.

The parameter `TIMESERIES.TSI.WEB_CLIENT_WRAPPER.WEB_CLIENT.PROXY_HOSTNAME` is used to define the time series proxy hostname. By default, this is set to `tr-timeseries-proxy`.

Time series proxy DNS setup

Eikon attempts to connect to a local time series proxy using the naming convention of `tr-timeseries-proxy`. This host needs to be resolved by the local DNS.

If users have...	Then...
More than one time series proxy on-site	each individual IP address should be associated with the same hostname, <code>tr-timeseries-proxy</code> .
Multiple time series proxies installed across different sites and have a global DNS	User must not use the default name. The hostname should be changed in the following format <code>tr-timeseries-proxy-SITE_LOCATIONID</code> . These names must be added in customer's DNS and be updated in the customer's profile in AAA.

Time series proxy protocol and port

Services	Protocol	Port
Eikon	HTTP	
Time series service	HTTP, SOAP	80
Web service routing	SOAP	
Management console	HTTPS, SSH	8082, 22
Monitoring	SNMP	161

Note: Since 1st November 2018, the installation policy for the deployed time series proxy for any Eikon installation has changed and there is no requirement for it. The only exception is for sites that have 100 or more Eikon installations and are in one of the following countries or regions:

- South America
- South Africa
- Australasia
- Japan
- China

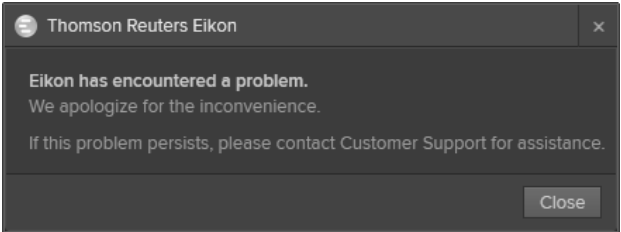
Appendix A: Eikon support tools

Dump Uploader

Dump upload workflow

If a crash occurs, Eikon DumpUploader submits jobs to the Background Intelligent Transfer Service (BITS) Admin on the PC for uploading the generated dump file. BITSAdmin schedules the upload of dump files, without using all available bandwidth.

If this fails, DumpUploader falls back to call Webservice to upload the dump file immediately.

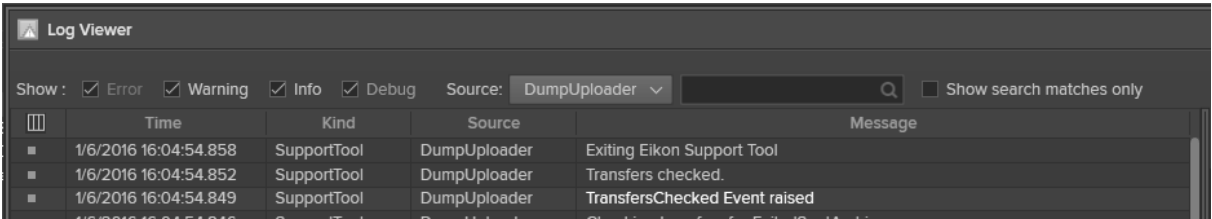


Client machine address

We use a CPURL to retrieve the server address where the dump is to be sent: `cpurl://streaming.apps.cp./`

Dump files upload log


The DumpUploader generates log files, named `SupportTool.<date>.<time>.p<process id>.log`, in the Eikon log folder. They can be seen using the Log Viewer, by filtering the Source with **DumpUploader**.



Appendix B: Eikon system and network test

To ensure your computer and network meet the requirements to install and run Eikon, use the testing tool that is available on the Eikon download site: eikon.tr.com.

Note: Refinitiv is migrating to eikon.refinitiv.com, for Internet users, and eikon.extranet.refinitiv.biz, for private network users.

REFINITIV 

Contact us

Private Network Users >

REFINITIV
EIKON™

Welcome to the ultimate set of financial tools.
New to Refinitiv Eikon? Find out more here.

Sign in & Download >

Refinitiv Eikon - Web Access

Sign in >

PC Requirements
View the recommended PC requirements for Refinitiv Eikon.
PC Requirements ↓

System and Network Test
Ensure your computer and network meet the requirements to install and run Refinitiv Eikon.
Run the Test ↓

Web Access
Compare features with the desktop application and check system requirements.
Features & Requirements ↓

Appendix C: United States Federal Information Processing Standard (FIPS)

The United States Federal Information Processing Standard (FIPS) 140 defines cryptographic algorithms, which are approved for use by US Federal government computer systems for the protection of sensitive data by computers that are subject to US government regulations. An implementation of an approved cryptographic algorithm is considered FIPS 140-compliant, only if it has been submitted for and has passed National Institute of Standards and Technology (NIST) validation.

Windows FIPS mode

Eikon is not supported in a Federal Information Processing Standards (FIPS) 140 series environment.

As such, enabling the FIPS feature may prevent Eikon from starting, due to a failure to download its components from the Refinitiv platform. This would result in the error message shown opposite.

Therefore, Refinitiv advises that FIPS mode is disabled.

For more information, see the links below:

- <https://support.microsoft.com/en-ph/help/811833/-system-cryptography-use-fips-compliant-algorithms-for-encryption,-hashing,-and-signing-security-setting-effects-in-windows-xp-and-in-later-versions-of-windows>
- <https://blogs.technet.microsoft.com/secguide/2014/04/07/why-were-not-recommending-fips-mode-anymore/>



Appendix D: Customer Managed over Internet

Customer Managed over Internet mode is a sub deployment, where Eikon connects the real time data on a user's own local Refinitiv Data Management Solutions (formerly TREP) infrastructure, while other content, such as Views, Search, Time Series, and so on, are sourced from the Eikon platform, through the Internet.

This mode addresses certain connectivity issues, for instance:

- Remote sites that do not have the same bandwidth as that of a Private Network line
- Mixed environment sites that have both Eikon for Wealth Management Internet and Eikon desktop users

Note: The direct Contribution to IDN does not work in this mode.

Defined host name

To enable this mode, a client has to define the following host on DNS or host file:

Host name	IP address
tr-customer-managed-internet	127.0.0.1

During the startup process, Eikon checks the host name and IP address of `tr-customer-managed-internet`. If they match, the application activates Customer Managed over Internet.

If the DNS entry is not found or there is an IP address mismatch, the application runs in normal Customer Managed mode.

DNS

Scenario 1: All users use Customer Managed over Internet

DNS	Authoritative DNS Server	Refinitiv Service
refinitiv.com	Internet	Refinitiv Web services
thomsonreuters.com	Internet	Refinitiv Web services
cp.thomsonreuters.net	Internet	Eikon
refinitiv.net	Internet	Eikon
customers.reuters.com ³	Internet	Customer Zone
trading.refinitiv.net	Internet	Trading Service

Scenario 2: Primary is Customer Managed over Internet, keep Private Network as a backup when Internet connection is down:

DNS	Authoritative DNS Server	Refinitiv Service
thomsonreuters.com	Internet	Refinitiv Web services
refinitiv.com	Internet	Refinitiv Web services
extranet.thomsonreuters.biz	Extranet DNS	Eikon, Customer Zone, Collaboration
*.refinitiv.biz	Extranet DNS	Eikon, Customer Zone, Collaboration
heartbeat.ciam.refinitiv.net	Internet/Extranet	Eikon Heartbeat

³ The customers.reuters.com DNS will be decommissioned.

DNS	Authoritative DNS Server	Refinitiv Service
login.cp.thomsonreuters.net	Internet/Extranet	Login Services
identity.ciam.refinitiv.net	Internet/Extranet	Login Services
download.cp.thomsonreuters.net	Internet/Extranet	Download Services
cp.thomsonreuters.net	Extranet DNS/ Internet	Eikon
refinitiv.net	Internet/Extranet	Eikon
customers.reuters.com ⁴	Internet/ Extranet DNS	Customer Zone
trading.refinitiv.net	Internet/ Extranet DNS	Trading Service

Notes:

- If heartbeat URL is running on Extranet network, the client runs Eikon Customer Managed, not Customer Managed over Internet.
- Login.cp.thomsonreuters.net can authorize Eikon login to either Extranet or Internet.
- When the Internet is down, Eikon runs on Local Mode.

⁴ The customers.reuters.com DNS will be decommissioned.

Appendix E: List of Acronyms

Terms	Definition
AAA	Authentication, Authorization, Administration
ADS	Advanced Distribution Server
AMERS	Americas
APAC	Asia Pacific
BDN	Bridge Data Network
CA	Certification Authority
CFI	Contribution Frontend IP
COIN	Community of Interest Network
CP	Common Platform
CPE	Customer Premise Equipment
DACS	Data Access Control System
DD	Delivery Direct
DFC	Data Feed Collector
DFH	Data Feed Hub
DFR	Data Feed Receiver
DNS	Domain Name Service
eBGP	External Border Gateway Protocol
eDNS	Refinitiv Extranet DNS
EMEA	Europe, Middle East and Africa
EMS	Elektron Managed Service
FCE	Financial Community Extranet
FCN	Financial Community Network
FQDN	Fully Qualified Domain Name
GPIC	Global Product Integration & Connectivity
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDN	Integrated Data Network
IE	Internet Explorer
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MIME	Multipurpose Internet Mail Extensions
MPLS	Multi-Protocol Label Switching
NGTx	Next Generation Transactions
NTLM	NT LAN Manager (Microsoft Windows)
PKI	Public Key Infrastructure
POP	Point of Presence

Terms	Definition
QoS	Quality of Service
RFA	Robust Foundation API
RSSL	Reuters Source Sink Library
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Source Sink Library / Secure Sockets Layer
TAM	Technical Account Manager
TCP	Transmission Control Protocol
TSP	Time series proxy
UDP	User Datagram Protocol
URL	Universal Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

Legal Information

© Refinitiv 2020. All rights reserved.

Refinitiv does not guarantee that any information contained in this document is and will remain accurate or that use of the information will ensure correct and faultless operation of the relevant service or equipment. Refinitiv, its agents and employees, accepts no liability for any loss or damage resulting from reliance on the information contained in this document.

This document contains information proprietary to Refinitiv and may not be reproduced, disclosed, or used in whole or part without the express written permission of Refinitiv.

Any software, including but not limited to, the code, screen, structure, sequence, and organization thereof, and documentation are protected by national copyright laws and international treaty provisions. This document is subject to U.S. and other national export regulations.

Nothing in this document is intended, nor does it, alter the legal obligations, responsibilities or relationship between yourself and Refinitiv as set out in the contract existing between us.