

DATASCOPE PRODUCT SUITE

ACCESSING DATASCOPE: OPTIONS & REQUIREMENTS

This document identifies the current connection options and requirements for accessing

- [DataScope Select](#)
- [Tick History](#)
- [DataScope Plus](#)
- [DataScope Equities & DataScope Fixed Income](#)

in both the Production and Disaster Recovery environments via the Internet and Private Network through Delivery Direct/Financial Community Network (FCN).

Clients are encouraged to access DataScope products via host-name-based URLs, not IP addresses. This is the recommended best practice as it requires no changes to client scripts or browser bookmarks in the event of a failover of the Production environment to the Disaster Recovery (DR) site. A failover automatically changes the Domain Name System (DNS) URL entries to point to the Disaster Recovery site for both the Internet and Private Network URLs. (Clients must ensure that their firewall configurations do not block DataScope Disaster Recovery IP addresses, which are listed later in this document.)

Actions that may trigger a failover to the Disaster Recovery site include, but are not limited to:

- Major hardware or network failure
- Power problems
- Acts of nature (tornado, hurricane, etc.)
- Malicious acts

Clients who access DataScope products via IP addresses will need to configure the Disaster Recovery IP addresses and repoint their access to the Disaster Recovery site if a failover is invoked. IP clients will also be responsible to repoint their access back to the primary Production environment site if notified by Refinitiv.

Clients who access DataScope via IP addresses should access the Disaster Recovery site only under one of these conditions:

- **Upon notification from Refinitiv of an actual failover.** Service alerts are provided to clients if a failover is invoked, and also when the Disaster Recovery site is ready for client access.
- **During a DataScope Disaster Recovery testing period.** Refinitiv schedules an annual client testing opportunity to support preparedness for Disaster Recovery site failover, notifying clients in advance via service alerts.

DataScope clients are encouraged to [subscribe](#) to service alerts. Please see the remaining sections of this document for connection options and requirements. This information is current as of the of document issue date identified below.

Contact one of our support contacts with questions:

- [Frontline Support](#)
- [OnlineSolutions](#)

Version 3.0 / Date of issue: May 2019

© Refinitiv 2019. All Rights Reserved. Reproduction or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. Refinitiv and the Refinitiv logo are trademarks of Refinitiv and its affiliated companies.

DataScope Select

Clients can connect to DataScope Select from four interfaces (GUI, FTP, SOAP API and REST API) accessed over the Internet or Private Network through Delivery Direct/FCN.

Internet

DataScope Select officially supports Internet Explorer 11, Mozilla Firefox and Google Chrome. Clients are encouraged to browse DataScope Select using modern versions of Internet Explorer to ensure optimal performance and reliability.

Host Name Access (recommended)

Interface	Production	Disaster Recovery
GUI	hosted.datascope.reuters.com	hosted.datascope.reuters.com
SOAP API	hosted.datascopeapi.reuters.com	hosted.datascopeapi.reuters.com
REST API	hosted.datascopeapi.reuters.com/RestApi/v1	hosted.datascopeapi.reuters.com/RestApi/v1
FTP	hosted.datascope.reuters.com	hosted.datascope.reuters.com

IP Access

Interface	Production	Disaster Recovery
GUI	192.165.219.225	159.220.29.23
SOAP API	192.165.219.152	159.220.29.21
REST API	192.165.219.152	159.220.29.21
FTP	192.165.219.225	159.220.29.23

Private Network - Delivery Direct/FCN

DataScope Select access is supported over Private Networks through Delivery Direct/FCN. These access methods also support an FTP Push option for extraction retrieval, as described in the next section.

Host Name Access (Recommended)

Interface	Production	Disaster Recovery
GUI	select.datascope.extranet.reuters.biz	select.datascope.extranet.reuters.biz

Interface	Production	Disaster Recovery
SOAP API	select.datascopeapi.extranet.reuters.biz	select.datascopeapi.extranet.reuters.biz
REST API	select.datascopeapi.extranet.reuters.biz/RestApi/v1	select.datascopeapi.extranet.reuters.biz/RestApi/v1
FTP	select.datascope.extranet.reuters.biz	select.datascope.extranet.reuters.biz

IP Access

Interface	Production	Disaster Recovery
GUI	159.43.0.1	159.43.7.36
SOAP API	159.43.0.2	159.43.7.35
REST API	159.43.0.2	159.43.7.35
FTP	159.43.0.1	159.43.7.36

FTP Push

This option enables Private Network clients to connect DataScope Select to their site via FTP using the following IP addresses and the instructions below. Additional configuration through the DataScope Select User Interface (**Preference** screen > **FTP Automated Delivery** tab) is required. Please see the *DataScope Select FTP User Guide* for details. This document is available on [MyRefinitiv](#).

Interface	Production IP Address Connecting to Client	DR IP Address Connecting to Client
FTP	159.43.0.6	159.43.7.46

Clients must also configure their firewalls as follows to allow for the FTP/SFTP connections to be initiated from the DataScope Select FTP Hosts:

1. Launch the DataScope Select console and change the global static NAT IP address that the Refinitiv hosts will target. (Provided by the Delivery Direct carrier).
2. Open the following firewall ports: 80, 443, 20, 21 and 22/TCP. (Source: 159.43.0.0/29; Destination: DataScope Select servers).
3. Selectively forward *.datascope.extranet.reuters.biz on the client DNS.

Tick History

Tick History v2 is hosted on the DataScope Select platform, and you can access it via the GUI and REST API interfaces using the same connection options as those for DataScope Select. (Note that Tick History does not support the SOAP API and FTP interfaces.) Tick History also has the additional connection requirement described in this section.

If your company's firewall requires sites to be whitelisted, and your company downloads Tick History output directly from Amazon Web Services (AWS) as described below, then you should whitelist several locations.

This applies to downloading output directly from AWS via:

- The REST API, by specifying the **x-direct-connect** HTTP header.
- The graphical user interface (GUI), by selecting **Enable Direct Download From S3** in the Tick History File Delivery section of the Preferences screen.

It applies to directly downloading Venue by Day packages, and custom reports, from AWS.

If your firewall allows the use of wildcard characters, whitelist the following locations:

- `https://*.amazonaws.com/tickhistory*/*`
- `https://tickhistory*.amazonaws.com/*`

If your firewall does *not* allow wildcards, whitelist the following locations:

- `https://tickhistory.query.production.pln-results.s3.amazonaws.com/`
- `https://tickhistory.query.production.hdc-results.s3.amazonaws.com/`
- `https://tickhistory.query.production.pln-results.s3-us-west-1.amazonaws.com/`
- `https://tickhistory.query.production.pln-results.s3.us-west-1.amazonaws.com/`
- `https://tickhistory.query.production.hdc-results.s3.us-east-1.amazonaws.com/`
- `https://s3-us-west-1.amazonaws.com/tickhistory.query.production.pln-results/`
- `https://s3.us-west-1.amazonaws.com/tickhistory.query.production.pln-results/`
- `https://s3.us-east-1.amazonaws.com/tickhistory.query.production.hdc-results/`
- `https://s3.amazonaws.com/tickhistory.query.production.pln-results/`
- `https://s3.amazonaws.com/tickhistory.query.production.hdc-results/`
- `https://s3.amazonaws.com/tickhistory.query.production.hdc-ebd` (Venue By Day only)
- `https://s3.amazonaws.com/tickhistory.query.production.pln-ebd` (Venue By Day only)

However, if either of the following applies to you, we recommend that you download Tick History output from Refinitiv, in the standard way, not directly from AWS:

- If your firewall requires whitelisting, but you cannot whitelist domain-based URLs, only IP addresses, then do not download directly from AWS.
- If you access Tick History not via the Internet, but via a private network such as Delivery Direct (DD) or Financial Community Network (FCN), then do not download directly from AWS.

DataScope Plus

Clients can connect to the DataScope Plus interface over the Internet, Private Network through Delivery Direct/FCN, or via a standard FTP connection. File retrieval is available via FTP Pull only. FTP Push is not supported.

Internet

Host Name Access (recommended)

Interface	Production	Disaster Recovery
GUI	hosted.datascope.reuters.com	hosted.datascope.reuters.com
FTP	prodcddis.thomsonreuters.com	prodcddis.thomsonreuters.com

IP Access

Interface	Production	Disaster Recovery
GUI	192.165.219.225	159.220.29.23
FTP	159.220.50.21	164.57.208.61

Private Network - Delivery Direct/FCN

Host Name Access (recommended)

Interface	Production	Disaster Recovery
GUI	select.datascope.extranet.reuters.biz	select.datascope.extranet.reuters.biz
FTP	prodcddis.extranet.thomsonreuters.biz	prodcddis.extranet.thomsonreuters.biz

IP Access

Interface	Production	Disaster Recovery
GUI	159.43.0.1	159.43.7.36
FTP	159.43.5.13	159.43.12.130

DataScope Equities & DataScope Fixed Income

Clients can access DataScope Equities and DataScope Fixed Income files over a standard FTP connection via the Internet or Private Network through Delivery Direct or FCN. File retrieval is available via FTP Pull only. FTP Push is not supported.

Production

Connection Type	HTTP/HTTPS	FTP	IP Address
Internet	www.rds.reuters.com	ds1.rds.reuters.com	159.220.29.24
Delivery Direct/FCN	www.rds.rservices.com	ds1.rds.rservices.com	159.43.7.49

Disaster Recovery

Connection Type	HTTP/HTTPS	FTP	IP Address
Internet	www.rds.reuters.com	ds1.rds.reuters.com	159.220.34.140
Delivery Direct/FCN	www.rds.rservices.com	ds1.rds.rservices.com	159.43.0.25