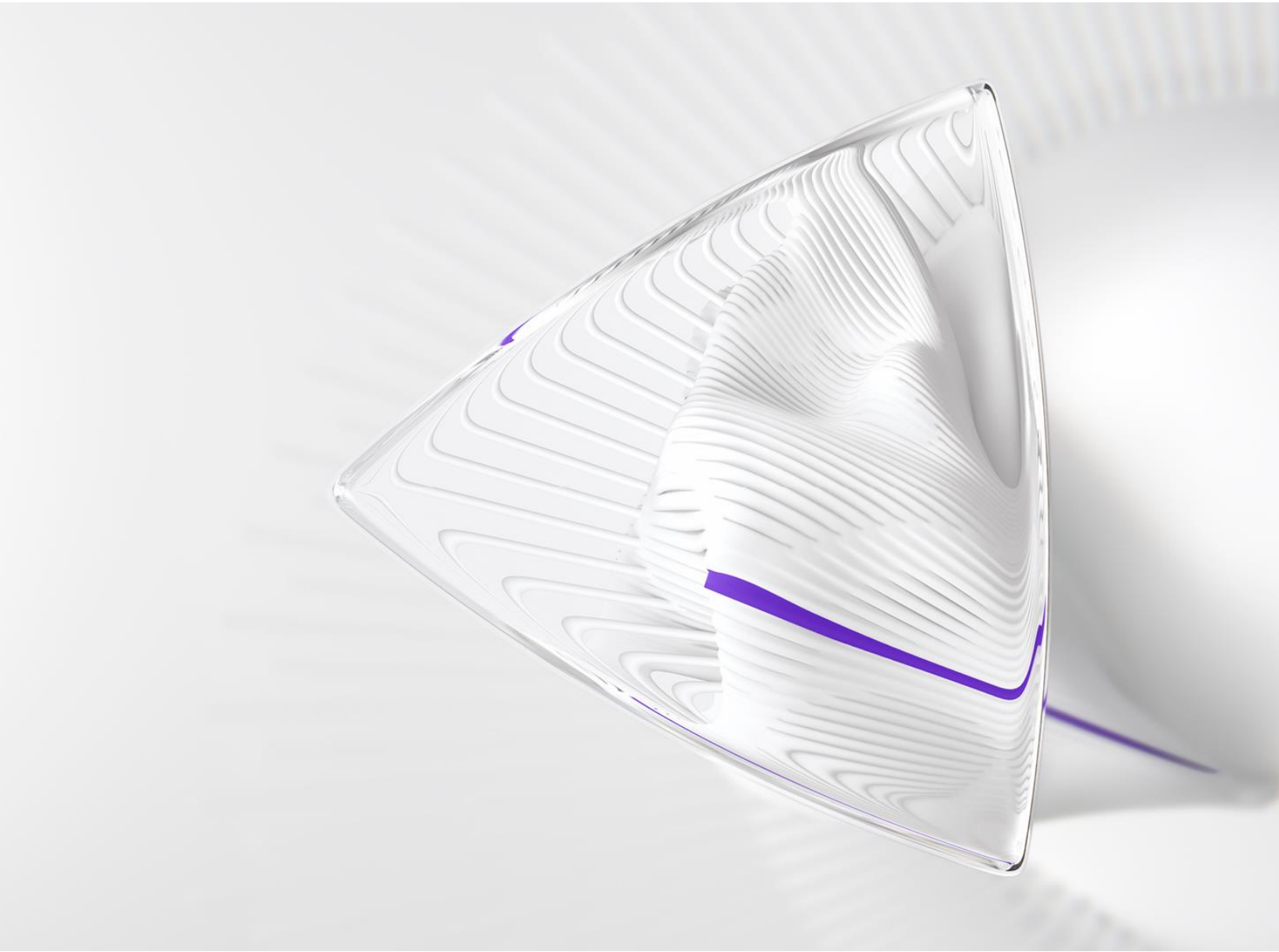
Clarivate™

EndNote Security Overview

Including EndNote Desktop and Online



In line with commercial industry standards, the Clarivate employs a dedicated Information Security team to protect its infrastructure from attacks or attempts to compromise the security and proper functioning of its IT and communications systems. These measures include deploying multiple firewalls and implementing proactive security scans and updates to prevent attacks on these systems in order to keep all EndNote user data secure.

General Security

Clarivate Information Security (*InfoSec*) team is responsible for ensuring that all Clarivate applications, platforms, and infrastructures are fully protected, and that our customer data is safeguarded at all times. The InfoSec team conducts on-going and regular security audits, as well as security reviews against all Clarivate applications, platforms, and infrastructures are conducted regularly. InfoSec team members ensure that security posture of both infrastructure and application is improved by delivering security architecture designs, standards, and integrations across the entire Clarivate global landscape. The InfoSec security compliance team performs audit reviews, and other regulatory reviews where required to ensure that Clarivate meets industry regulation requirements.

Clarivate conducts both application and infrastructure vulnerability assessments regularly to ensure that the entire platform and application vulnerabilities are identified, reviewed, and mitigated. The Clarivate Information Security policy is approved and sponsored by the Executive Committee. All Information Security Policies are reviewed and updated at a minimum of biennially. Clarivate asset management program is based on Information Technology Infrastructure Library (ITIL) disciplines and is subject to our pending ISO 27001 certification.

All access traffic is recorded, documented, and monitored across our Cloud Environment. Other security controls are implemented across Clarivate to ensure full virtual security protection of the Cloud Environment and their assets. Access to our Cloud Environment is controlled through IAM provisioning and security groups.

All employees are required to complete awareness training on the Company's Code of Business Conduct and Ethics that includes Information Security training. Further specialized training is completed based on job role, such as Application Developers and Customer Facing staff.

Network and Host Security

A number of standard security devices and solutions are in place to protect and safeguard both applications and data, and together make up the holistic enterprise security architecture and Cloud Environment security strategy. The holistic prevention and protection strategies in place include firewalls, load balancers, log management, detection sensors, and vulnerability scanners. Also included are complete enterprise end-point solution tools like Anti-Virus, Anti-Spyware, Anti-Malware, and next generation intelligent security tools.

Clarivate Security Operation Center (SOC) team provides ongoing security infrastructure and application monitoring. The SOC team utilizes advanced and next generation security tools and services to provide holistic security monitoring and protection to Clarivate assets around the globe. Detection and sensors, vulnerability scanners, and application white-listing tools are deployed across our Cloud Environment to monitor and / or block malicious activities including spoofing, hijacking, and DOS. Other security tools, including protection tools, are in place to protect Clarivate on-demand and internal applications and platforms. Clarivate has Intrusion Detection Systems (IDS) and other proactive security monitoring tools in place to ensure that our Cloud Environment is monitored around the clock. Further, a dedicated team of security analysts provide continuous monitoring and analysis of the latest security threats, to ensure malicious activities are identified and defeated immediately.

Clarivate Information Security team provides security risk assessments, application and infrastructure vulnerability assessment through the Enterprise Security Services (ESS) group, who in turn conduct regular threat and vulnerability assessments against Clarivate platforms and applications. The InfoSec team also provides Application Security Assessments (ASAs) against Clarivate applications to ensure security controls are integrated and implemented. Any critical code flaws are identified and fixed by the development community of Clarivate. Further, the ESS group also works with industry leading security groups to conduct 3rd party security reviews against Clarivate applications and platforms where required.

As part of Clarivate Multi-Layer Security (MLS) architecture, enterprise version firewalls by multiple world-class industry vendors are implemented across different zones to secure and protect applications. All firewall systems follow the Clarivate SLA to receive the latest vendor updates and patches. SOC will utilize network logs and other logs to assess and identify cyber threats. Additional network security tools are in place to monitor security activities across the entire infrastructure.

Online Security

EndNote online offers Secure Sockets Layer (SSL) connections for subscribers. The SSL security protocol provides an https secured connection that supports SHA-256 with RSA Encryption for communications with the EndNote online site. This is the same technology that most e-commerce websites use to encrypt credit card information and is the industry standard security protocol for protecting sensitive data while in transit.

EndNote online offers browser and Word plugins. The Cite While You Write plugin for Word is optional, but is required in order for users to be able to insert and automatically format citations and references within their Word format manuscript. All plugins use SSL for user authentication requests.

EndNote online log files are recorded on production in line with the requirements for incident investigation and event monitoring. Access to production systems is restricted to authorized users and production systems are housed in industry standard infrastructure with controlled entry. Web Services are used to access internal content from the Web of Science.

If you are using the EndNote desktop client with EndNote online -- meaning you are syncing and/or sharing your library or groups from your library, or having a library shared to you by another EndNote user -- all communication between the desktop and online is encrypted (i.e., travels over SSL) when synchronizing EndNote libraries and groups.

Disaster Recovery

Our business continuity strategy for the EndNote online application and services includes redundant servers across multiple availability zones, network components, and storage systems for High Availability (HA) capability on products and components.

There is no routinely scheduled downtime for EndNote online, but in the case that it needs to be taken offline for maintenance and fixes, information will be posted as a notice upon login ahead of downtime.

EndNote reference data is redundant across 3 availability zones and regular backups are in place. EndNote file attachments are stored across multiple availability zones with 99.999999999% (11 9's) of durability over a given year.

Use in Virtual Environments

Does EndNote work with Citrix Application Hosting?

We do not officially support use in virtual environments such as Citrix Application Hosting.

Does Endnote support use over Virtual Private Network (VPN)?

We do not officially support use in this environment. Libraries can be opened while on local storage or a fast LAN connection (e.g., same building). There are known performance issues trying to open a library from off-site locations that can lead to library damage. Due to this potential risk, we do not recommend this particular use.

Customization

What customizations are available?

EndNote allows the end user to customize:

- Bibliographic Styles
- Import Filters
- Connection Files
- Central location of styles, filters and connections for network environment
- Definition of reference types and fields
- OpenURL Links and Proxy URLs for Find Full Text
- Duplicate field control
- Spellcheck terms and language
- Term Lists for synonym control with Journal titles
- Display fonts and fields

These customizations are also available to the administrator for mass installation using the MSI.

Common Ports Used for Online Search

210 is the base port used for most sites and thereby the most commonly used by Horizon and Innopac servers. 2100 is also commonly used by Innopac systems, 2200 is the default for Unicorn systems, and 7090 is common to the Voyager system, including the Library of Congress.

210, 2020, 2100, 2101, 2121, 2200, 3950, 5666, 7090, 7190, 7290, 7390, 7490, 7690, 7890, 9909, 9991, 9999, 20011, 20012, 21210

Less Common Ports Used for Online Search

211, 212, 220, 221, 223, 1111, 1616, 1921, 2010, 2102, 2103, 2104, 2108, 2111, 2112, 2113, 2116, 2132, 2203, 2205, 2210, 2211, 2222, 2227, 2300, 2400, 2500, 2600, 2800, 3200, 3333, 4151, 4201, 4210, 5009, 5200, 5205, 5210, 5302, 5305, 5405, 5500, 5505, 5605, 5705, 5805, 6005, 6105, 6205, 6305, 6333, 6405, 6433, 6505, 6605, 6705, 6805, 6905, 7005, 7019, 7025, 7091, 7099, 7105, 7205, 7280, 7305, 7405, 7505, 7590, 7605, 7705, 7788, 7790, 7805, 7819, 7990, 8010, 8019, 8090, 8105, 8110, 8190, 8205, 8305, 8888, 9190, 9290, 9390, 9490, 9535, 9590, 9690, 9825, 9830, 9840, 9850, 9855, 9860, 9865, 9870, 9875, 9880, 9885, 9895, 9929, 9949, 9992, 9993, 9996, 9997, 9998, 10090,

10190, 10290, 10390, 10490, 10646, 10790, 10890, 10990, 11090, 11390, 11490, 11590, 12090, 12490, 12590, 12690, 12890, 12990, 13090, 13190, 13290, 13390, 13490, 13590, 17590, 18290, 20010, 24210, 55200, 57090

Support

Our support policy covers EndNote desktop versions 20, X9 (19), and X8 (18) and the currently live version of EndNote online. This does not include compatibility support for new operating systems and word processors introduced after a release that are not covered by that version's system requirements.

For more information about Clarivate's Information Security, please visit **https://clarivate.com/information-security/**