BIONOVA® cloud

Understanding Security Features of the new Bionova® Cloud environment

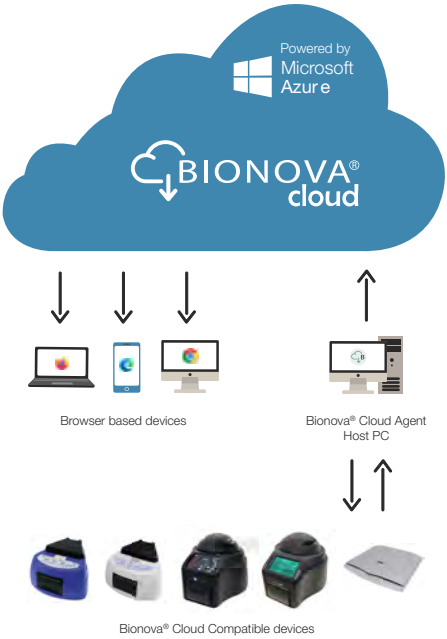
Rev. 1 | April 2022

Terragene®

Index

How does Bionova® Cloud works?

The new Bionova® Cloud environment is a Cloud based solution that integrates the information generated by Terragene® electronic devices with an easy-to-use Web App for the traceability of sterilization and disinfection control applications.
The Bionova® Cloud environment is composed by two main components: the **Bionova® Cloud Traceability Software** which is a Web Based application, and the **Bionova® Cloud Agent** which is a Microsoft™ Windows App that acts as an interface between the Terragene® compatible devices and the web based application.



The Bionova® Cloud Agent handles all communications with Terragene® compatible electronic devices and the Host PC where the Agent App runs.
Bionova® Cloud Agent then acts as an interface between the Terragene® compatible devices and the Bionova® Cloud Traceability software and sends the information generated from the devices to the Microsoft™ Azure powered Cloud server where the Traceability Software Web App runs and stores the information.
The user can then access to the Cloud saved information through any device with a compatible web browser.

Comunications fundamentals

Communication is at the very core of Bionova® Cloud Environment's DNA.
For the Bionova® Cloud Environment to be able to carry out its intended use, internet connectivity is needed for:
- Communication between a Web browser and Bionova® Cloud's Microsoft™ Azure servers (for the user to be able to access the Cloud stored data).
- Communication between the Bionova® Cloud Agent Windows APP and the Bionova® Cloud's Microsoft™ Azure servers (for readout results from Terragene® electronic devices to be synchronized to the Cloud Servers).

In both cases, all internet communication is carried out using standardized HTTPS-TLS protocols. No additional protocols or special ports are required to use the Bionova® Cloud Environment or any of its modules.

Keep in mind that, as a rule of thumb, if you can access Google or Gmail from your PC Web browser, then you can use Bionova® Cloud and Bionova® Cloud Agent on your PC without any additional configuration.
Please refer to the Bionova® Cloud User Manual for more information on Bionova® Cloud Environment system requirements (Bandwith, used endpoints, etc).

Nature of the information generated, handled and stored by Bionova® Cloud

The information handled and stored by the Bionova® Cloud Environment is comprised of information related to the readout result of Terragene® sterilization, disinfection and hygiene indicators by Terragene® electronic devices, and accessory information entered by the User to the Web application to add context about the infection control process in which the indicator is used.

No Protected Health Information (PHI) is stored or handled by the Bionova® Cloud Traceability Software, Bionova® Cloud Agent, nor any of its components.

Information handled by Bionova® Cloud Agent

Information of Bionova® Auto-reader Incubators

The Information handled is related to the incubation and readout process of the indicator used: either a SCBI or a

↲ Nature of the information generated, handled and stored by Bionova® Cloud

Pro1Micro Hygiene Monitoring Indicator. This information includes the readout result, readout time, incubation temperature and such. The information comprises the same information available on the incubation result ticket.

For the Trazanto® reader

The Information handled is related to the readout of chemical, and washing indicators. This information includes the readout result, and information related to the indicator such as indicator type, batch number, reference values and such.

Bionova® Cloud Agent does not retrieve any type of information from the Host PC where it runs, nor any other user device connected to the Host PC, outside the information that is sent by Compatible Terragene® Devices to the Bionova® Cloud Agent.

Information stored by Bionova® Cloud Traceability Software

The information handled and stored by the Traceability Software Web Application consists of the information sent by the Bionova® Cloud Agent *(see previous section)*, information imputed by the User to add context about the infection control process in which the read out result is created, and login details and preferences for the users of the Web App.
Bionova® Cloud Traceability software does not retrieve any information from the host PC, outside the information that is sent by the Bionova® Cloud Agent to the Traceability software.

Security features of communication, access and Cloud data storage of Bionova® Cloud

Terragene® supports a continuously improving security program that reduces risk, responds to threats and protects our company's intellectual property and the privacy of data while driving compliance with regulatory requirements and industry best practices. Committed to scientific advancement, we employ the latest security tools and offer solutions that enable our customers to push the boundaries of innovation.

These are some of the security features implemented to keep our customer data private and secure:

Bionova® Cloud Agent
Communication

- Encripted communication with web service via Transport Layer Security Protocol (TLS).
- Password protected access to web service.
- Encryption certificates provided by Trusted Certificate Authority (Microsoft™ Azure).

Data Safety

Bionova® Cloud data is stored in Microsoft™ Azure Storage and encrypted by Microsoft™ Azure Cloud servers by 256-bit Advanced Encryption Standard (AES-256).

Access Control

- Administrative access requires multifactor authentication (MFA).
- Encryption certificates validation.
- Tampering protection provided by Microsoft™ Azure against malware, distributed denial-of-service.

Communication

- Encripted communication with web service by 256-bit encryption and HTTPS.
- Password protected access to web service.
- Encryption certificates provided by Trusted Certificate Authority (Microsoft™ Azure).

Bionova® Cloud's Microsoft™ Azure based Cloud infrastructure

The Bionova® Cloud Traceability Software Web application and all its stored data is powered by Microsoft™ Azure state of the art Cloud infrastructure.

Servers location

Microsoft™ Azure is a well recognized Cloud service provider with servers all over the world. The Microsoft™ Azure servers in which Bionova® Cloud Traceability Software currently runs are located on Microsoft™ Data centers located on the West Coast of the United States of America.

Microsoft™ Azure data security

The security strategy implemented by Microsoft™ Azure for securing the data tier of Bionova® Cloud follows the layered defense-in-depth approach as shown in the picture below, and moves from the outside in:

At a very broad level, we can say that Microsoft™ Azure protects customer data by implementing 4 different layers of security.

Network security Layer: Firewalls prevent network access to the server until access is explicitly granted based on IP address or Microsoft™ Azure Virtual network traffic origin.

Acces management layer: Authentication and authorization implementing a secure login process through encryption.

Threat protection: SQL Database and SQL Managed Instance secure customer data by providing auditing and threat detection capabilities.

Information protection and encryption: All Cloud user stored information is encrypted. This includes Encryption-in-transit, Encryption-at-rest, Encryption-in-use, Dynamic data masking and Key management with Microsoft™ Azure Key Vault.

For more information about Microsoft™ Azure security features please visit the following article: An overview of Azure SQL Database and SQL Managed Instance security capabilities.

FAQs

How are my passwords managed?
Once you create your administrator account for your company, a two steps validation process will be carried out for validation for the Administrator e-mail address.

After e-mail address validation, the Administrator can add users to the company using the Bionova® Cloud web interface. Whenever a new user is added to the company, a validation e-mail will be sent to the user e-mail address.

In case of losing your login details, Administrators and Users alike can follow the steps on the Bionova® Cloud login page for resetting their password. The process will send a password reset request e-mail to the user previously validated e-mail address.

Is the information saved on Bionova® Cloud private?
Yes, only the personnel within your organization can access your company's stored information.

To what kind of information Terragene® has access to?
Terragene® can not access to your login details information nor to your account details. All information gathered by Terragene® from Bionova® Cloud is anonymous and it's only used to provide metrics for the performance of the Bionova® Cloud environment. For more details, please check the *Bionova® Cloud EULA*.

Will my information be available to any third party at any moment?
No, your information is kept private only for the users of your company that use the Bionova® Cloud environment. No information will be shared with third parties at any moment.

Can I connect other Traceability Softwares to Bionova® Cloud maintaining encryption?
Yes, Bionova® Cloud Traceability Software can export the Cloud stored data to other traceability softwares using an HL7 protocol implementation. The connection between the software is encrypted by secure authentication and SSl encryption.

↲ FAQs

Do I need any special communication protocols or to open ports on my PC or LAN to run Bionova® Cloud Agent or Bionova® Cloud Traceability software?

No special ports or protocols are needed to use Bionova® Cloud Environment or any of its modules because communication with the Microsoft™ Azure Servers where Bionova® Cloud runs is carried out using standard protocols and ports (HTTPS-TLS).