
blud_direct
SM
An Immucor Technical Support Solution

# blud_direct℠

In order to maintain a high level of service to our customers in their use of our automated instruments*, Immucor offers an industry exclusive remote support solution using high speed internet connectivity. This solution, known as blud_direct™, raises the bar on the level of support available to blood bank instrument customers. Powered by NTR Global's NTR support application, remote support has never been faster or easier.

With blud_direct, Immucor Technical Support Representatives (TSRs) are able to remotely access Immucor instrumentation over a high speed internet connection. This connection uses Secure Socket Layer (SSL) technology, which is initiated from the instrument. Through blud_direct, access to the instrument is always in the hands of the customer.

As Information Security is a top priority, blud_direct takes into account three aspects of security—authentication, authorization, and encryption. Furthermore, blud_direct records transcripts of the support session to an audit log. This log can then be emailed to the customer as a record of access.

## Authentication

Immucor access to administer a blud_direct session and all its utilities are secured with logins and passwords. Passwords are stored encrypted and do not travel across the Internet during the login process. This ensures that only Immucor personnel are working with the customer in accessing an Immucor instrument computer.

## Authorization

Once authenticated to blud_direct, the TSR will generate a unique key (session code) to pass to the customer over the phone that will open the secure session. The session code is unique per session. Before the TSR can use the remote control features of blud_direct, the customer must approve the TSR access to the Immucor instrument computer. This places authorization to the instrument computer in the hands of the customer.

## Encryption

blud_direct ensures that data is concealed from unauthorized access. All sessions are encrypted with 256-bit AES encryption and strict security measures that refuse unauthorized personnel access. If there is a need for data transfer, blud_direct uses strict security algorithms and additional security levels, as needed, to encrypt data before transfer, ensuring total security.

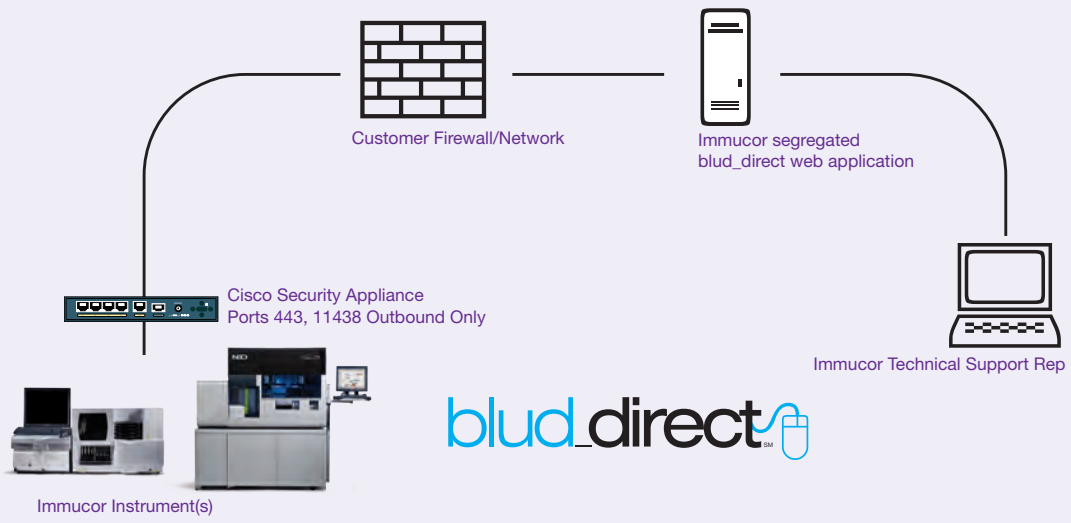
* NEO® and Echo®

## Technical Overview

blud_direct is a web based SSL application initiated from the instrument computer (customer initiated) via the world wide web. It can be accessed as long as an Internet connection is made available to the Immucor Instrument computer. To begin a session, the customer is directed to the Help menu of the instrument software. From there a link is provided to visit the main page of the blud_direct website (https://support.immucor.com/blud_direct), where the customer is prompted to enter a session code. The session code is generated by the Technical Support Representative (TSR) and provided to the customer over the phone. Upon entering the unique session code, a blud_direct session is established, similar in form to an instant message chat. The session is completely private and safe. The full conversation is transmitted in encrypted form, recorded and routed to the receiver. If remote access is deemed necessary, the TSR will send a request for remote control through the chat conversation to the instrument user. In order to give the TSR access to the instrument computer, the customer must accept the request (grant permission) from their conversation window. Once the customer clicks on the Accept button, the remote control module is activated, initiating a connection back to Immucor, providing access as if the TSR was in front of the instrument computer. Once the session is ended, remote control is terminated. A new session is then necessary for an Immucor TSR to be able to access the Instrument computer again.

## Architecture

As the connectivity is established by the customer (instrument user) from the instrument to blud_direct, the instrument computer requires Outbound Internet access to the blud_direct secure website (HTTPS). Instrument access to the Internet will first go through a Cisco security appliance to the facility infrastructure. The intended purpose of the security appliance is to provide protection for the Immucor, FDA cleared instrumentation being operated on a network. The Instrument computer connects to the security appliance, which in turn will connect to the network. The Cisco security appliance will operate as any other computer device (node) on the network. To properly configure the connection settings, Immucor personnel will need to identify the IP address, Subnet Mask, and Gateway assigned from the customer IT department. In preparation to deploy blud_direct with your Immucor instrument, a network drop for the Internet connection must be located/activated.




To allow connectivity for blud_direct, ports 443 (https) and 11438 are allowed on the Cisco security appliance to initiate Outbound traffic. Once a connection is established on one of these ports, two-way communication is then permitted. The trigger for remote control (port 11438 connection) is the customer action of clicking to accept the request for access. It is important to note that because connectivity is initiated by and must be further approved by the customer, Immucor does not have anytime access. It will not be necessary to open any Inbound ports.

## Benefits

- Using the high-speed Internet connection, support is at a fast connection speed.
- Faster support reduces instrument downtime.
- Issues resolved via remote access to the instrument computer reduce the number of service visits.
- All information is communicated in a safe, highly secured manner with complete patient confidentiality maintained at all times

## FAQs

### Is patient information being moved from our Immucor instrument?

Diagnostic archives and event logs are commonly the type of information being accessed. Exposure to patient information is purely accidental. If it becomes necessary to access result files containing patient information, authorization from the customer is requested. This information is used only to the extent necessary for conducting an effective investigation.

### Are communications secure?

Yes, blud_direct utilizes the Secure Socket Layer (SSL) protocol, commonly used for secure transactions over the web. Additionally, the application uses 256-bit AES encryption to further secure the communication.

### Is there software loaded on our instrument computer?

No. There is no software to load on the computer. Only when remote control is requested and approved, a small plug-in is downloaded and activated on the instrument computer. When the support session is ended, the plug-in is deleted from the instrument computer leaving no footprint.

### Can anyone simply access our instrument from outside our network?

No. blud_direct is initiated from the instrument side and a support session can only be established by means of the session code supplied by an Immucor Technical Support Representative. Immucor does not have anytime access to the Instrument computer.

### Is the Cisco Security Appliance absolutely necessary?

Yes. The Cisco Security Appliance is necessary to protect the instrument computer from network threats. The Cisco Security Appliance configuration is designed to allow only the necessary connection for blud_direct and, if applicable, the Instrument interface connection to a Laboratory Information System. All other communication is blocked. It is important to note that Immucor does not have anytime access to the security appliance.

### What ports are being used for blud_direct?

The Cisco Security Appliance will be configured to allow outbound traffic from the instrument computer to blud_direct on ports 443 (https) and 11438. Port 443 is used for the initial communication to the blud_direct website and for the chat session. Port 11438 is used for the remote control feature.

### Will any changes be required to our network?

blud_direct will require Internet access, therefore, a connection allowing traffic on the ports specified in this document will need to be made accessible. No other changes are required to your network infrastructure. If desired, Access Control Lists can be used to specify the connectivity between the source IP address (customer network) and the destination address (blud_direct). Please contact Immucor for the blud_direct destination address.

### Can a VPN connection be used?

The use of a VPN connection is not mandatory for blud_direct to function. All communication with blud_direct is encrypted. While a VPN connection is not required, Immucor personnel can work with you to establish a site to site VPN tunnel. In using a site to site VPN, communication will still be initiated outbound from the customer side, the difference being that the communication to blud_direct will occur over the VPN tunnel instead of the Internet. Please note that the use of a site to site VPN connection does not negate the need for the Cisco Security Appliance.

To learn more or to set up a consultation with one of our Blood Bank Business Managers, **call 855.IMMUCOR** (855.466.8267) or **visit www.immucor.com**.

**In Canada:**

1.800.565.0653
DBLCustomerService@immucor.com

IMMUCOR