Increasing Incisive inCLOUD security

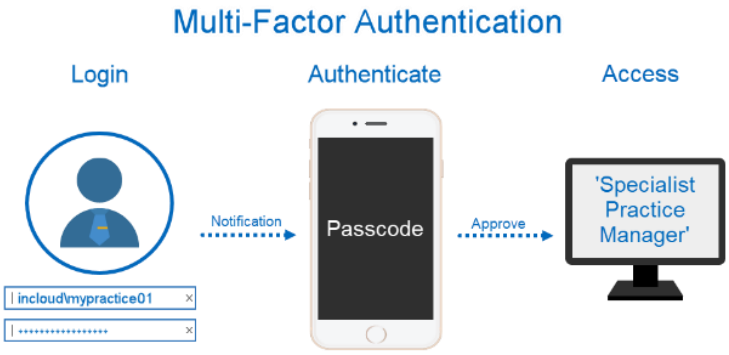
Incisive inCLOUD is including another layer of security, to protect your information even further.

New servers have been added to the computing farm, which are configured to require 'Multi-factor Authentication' (MFA or 2FA) to allow a remote connection to be established. This does mean there is an additional step in the process to log on, but it is a very effective barrier to unwanted cyber-intruders.

All new users of Incisive inCLOUD are using the MFA system and we are also requiring all existing customers to also upgrade the method they use to connect.

The authentication levels used to secure the Incisive inCLOUD system are:

1. inCLOUD network connection using your usual login e.g. incloud\mypractice01
2. Passcode input, generated from the Authpoint app or hardware token (new step)
3. Incisive application login



In addition, only connections from New Zealand based IP addresses (your router's internet address) are permitted, without needing to use a separate VPN connection.

The passcode is generated either from an app on your phone or a special hardware generator. These create a one-time passcode which you input during the connection process. This method of Multi-Factor Authentication is now used in all public hospitals, after the malware attack on the Waikato DHB last year.

There are several key reasons we have chosen to include MFA:

- CertNZ recommends MFA/2FA protection as an important security step;
- the Privacy Act requires health agencies to take 'reasonable security safeguards' to protect health information;
- the National Cyber Security Centre's advisory for the increased threat of targeted cyber intrusion because of military actions between Ukraine and Russia.

Frequently asked questions.

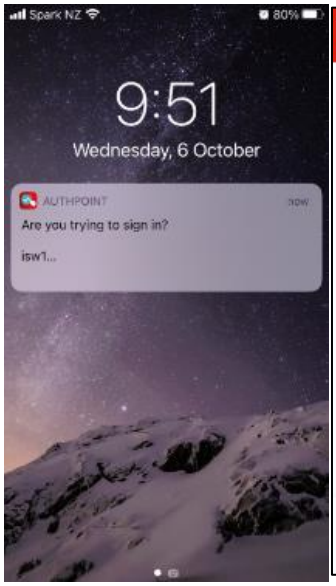
What will change for us?

1. The icon that you use to connect to the Incisive inCLOUD will need to be modified so it points to the new system (secure.incloud.clinic instead of incisive.incloud.clinic)
2. You will need the Authpoint app installed on a mobile phone or a hardware passcode generator, so that you can use either, each time you connect to the Incisive inCLOUD.

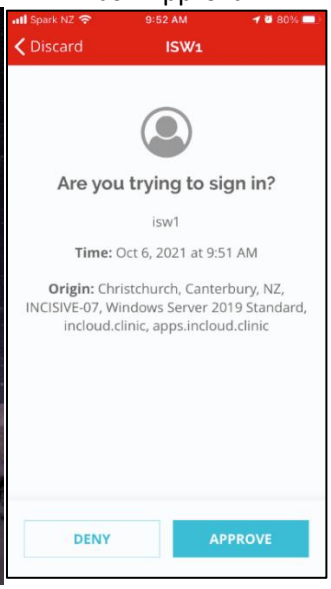
How does the MFA work?

During the process to connect to Incisive inCLOUD, a screen will appear prompting whether you want to use the 'Push' or 'One-Time-Passcode' option. If the Push option is used a notification will appear, which can be 'Approved', or if the Passcode option is used, the number can be entered from either the Authpoint app or Hardware token generator. The Incisive application will then continue to start. See the Multi Factor Authentication (MFA) training videos.

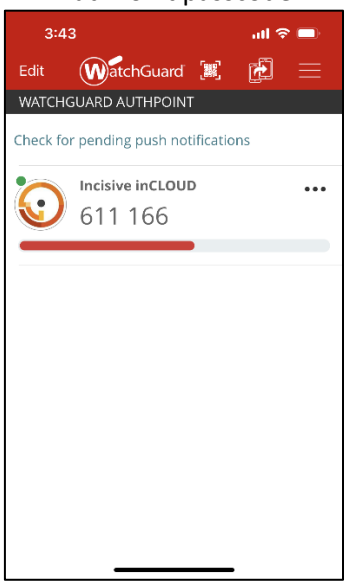
Push Notification



Push Approval



AuthPoint passcode



Hardware passcode

What happens if I don't have my phone?

We recommend that you have access to both the Watchguard passcode generator and also the Authpoint app, so there are alternative methods of generating the passcode. If neither are available, there is a 'Forgot Token' option where we need to be involved to allow access for a limited time.

The Incisive inTOUCH mobile app can also be used to access your clinic or operating lists and view the patient's records.

We are a large practice/hospital and different staff frequently use the same computer.

There is no change with how you currently use Incisive inCLOUD except that the first person who logs on will need to enter a Passcode from either the Authpoint app or the Watchguard passcode generator.

Is each staff member going to need the Authpoint app on their phone?

The Passcode that is generated is linked to an individual Incisive inCLOUD login. This means that for each login there will need to be either a specific hardware passcode generator or an Authpoint app token. It is possible (but not very practical) to have the Authpoint app on a single a 'Practice' based phone, which has the ability to remotely 'Approve' a connection or issue a One-Time Passcode (OTP) for multiple logins.

If the user is accessing Incisive inCLOUD from different locations (such as the specialist) then they should always use the Authpoint app on their own phone.

Are there charges?

The MFA technology is provided through an internationally respected company which does charge for its products and services. There will be changes to our fees to cover their costs and the hardware

token generator can be purchased separately. Given the severe disruption that can occur from cyber-attacks, security costs are now regarded as an expected overhead of doing business.

Everyone using Incisive inCLOUD will need to upgrade to the same level of high security.

I use an Apple Mac. Do I need to use MFA?
Yes.

Is the change going to disrupt the running of our practice/hospital?
All the preparation can be completed in the background while you continue to use the existing connection method. When you are ready to start using MFA, you just start using a different shortcut icon. Everything will continue to function as it is now. The connection process will take slightly longer.

When is the change going to occur and what do we need to do?
The process to migrate existing Incisive inCLOUD users to use secure.incisive.incloud, has already started. We will shortly be inviting you to be involved as we expect that everyone will be migrated before the end of the year. We will work with you to ensure the timing works well for you.

You will need to:

- decide how many Watchguard hardware tokens you want;
- download and install the Watchguard Authpoint app, for the mobile users; and
- provide an email address for each connection.

What are the options if I don't want to use MFA?
Because the database that you use for your records, is the same for any Windows operating system, we can remove your records from the Incisive inCLOUD system so you can have them on your own on-site server.

Are any other security changes going to occur?
The Windows tsclient link to your computer's drives will eventually be disabled and is replaced with the 'Incisive Files' drive that has been provided to assist with easy upload and download of files/photos to and from the Incisive inCLOUD system. This allows us to virus-scan the files being uploaded and close another possible intrusion point from your computer.

The operating system for the servers is being upgraded to Windows Server 2022, which has significant improvements in the detection and protection against malware attempts.

Is MFA going to make my information completely secure?
As I'm sure you have experienced, the cyber-security requirements are in a state of constant change. Protection is almost always a patching exercise to cover the holes that have previously been exposed by those wanting to get to your information or use you as a spring-board into someone else's system.

100% protection would mean that the Incisive inCLOUD system would have to be so locked down that remote access from your own computers or devices, would be virtually impossible to use and very expensive to implement. To provide a system that is workable for you, there is always a degree of compromise between accessibility and protection. Which is why we have backups and fail-over functions.