Explorer Online Gateway Edition User Guide

Overview

This article will cover the basic functionality of Medical-Objects Explorer Online when running in Gateway Edition mode. If you have any questions or require any further information, please contact the Helpdesk on (07) 5456 6000.

Requirements

Explorer Online was designed to run on desktops, laptops and modern tablets running Windows, MacOS or Linux. Mobile phones are not currently supported.
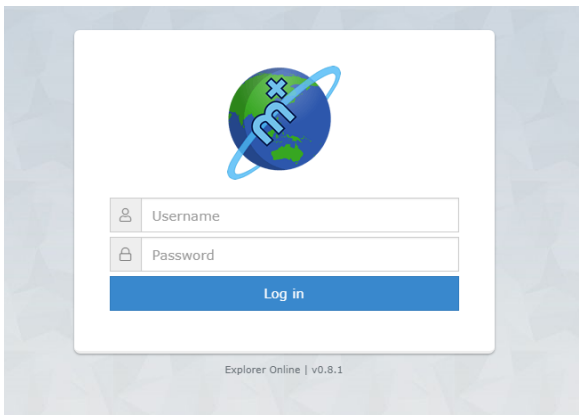
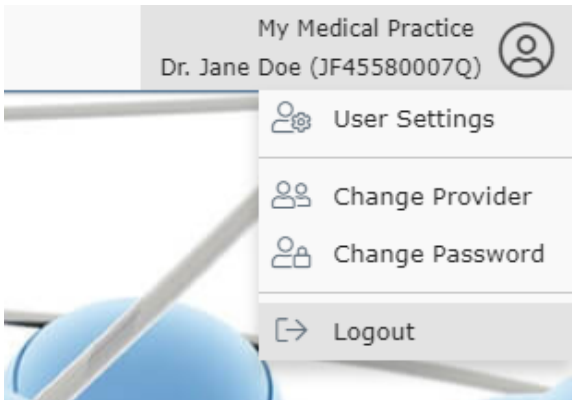Please take note of the browser requirements below.

Supported Browsers

- Microsoft Internet Explorer 11
- Microsoft Edge
- Chrome
- FireFox
- Opera
- Safari 8+

Logging in and out

When first loading Explorer Online you will be presented with a login screen. Simply enter in your username and password and click login to proceed.

Once logged in you can **Logout** again or **Change Provider** by simply clicking on the **User Menu** in the top right hand corner of the screen.

Tip!

You will be automatically logged out after 10 minutes of inactivity. You can change this via the **User Settings** option in the **User Menu**.

Setting up Two-Factor Authentication

Two-factor authentication is a security feature that helps protect your account in addition to your password. With two-factor authentication, a special login code together with your username and password will need to be entered each time someone tries to access your account from a computer or device that isn't recognised.

In order to generate the special login codes, you will need to install a free app which supports the Time-based One-time Password Algorithm (TOTP) such as Google Authenticator, Authy and Microsoft Authenticator. There are many others, and some of these apps also support generating codes from desktop computers.

To enable two-factor authentication can be enabled through the following steps.

1. Once you have logged in, Two-Factor Authentication can be enabled by clicking 'Enable Two-factor Authentication' on the '**Security**' section in the **Dashboard.**
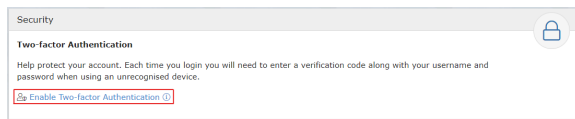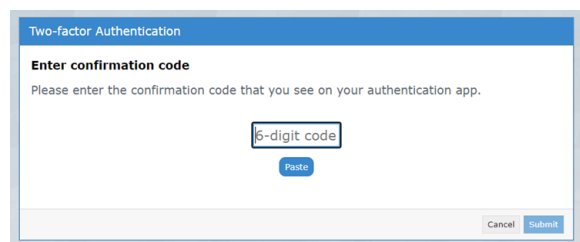

2. It will prompt you for your password
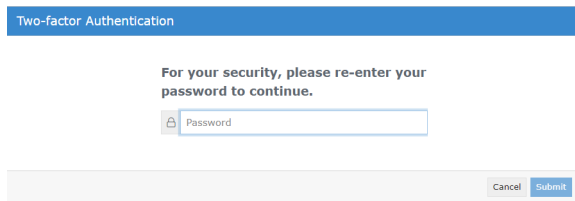
3. Decide whether you would like to set your device as a trusted device (this will allow you to skip these Two-Factor steps for 30 days on the selected device). Simply use the toggle button below "Trust this device" to select your choice, then select "Proceed".
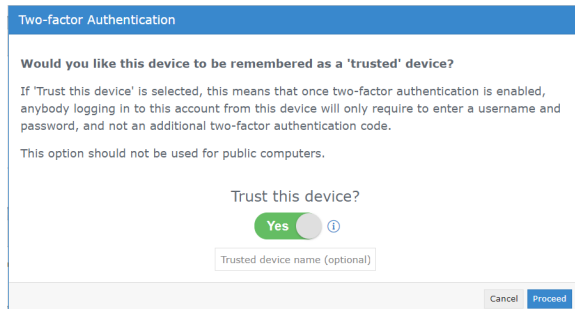
4. Open your Two-Factor Authentication app and scan the QR code provided (or enter the optional code), then click "Continue".
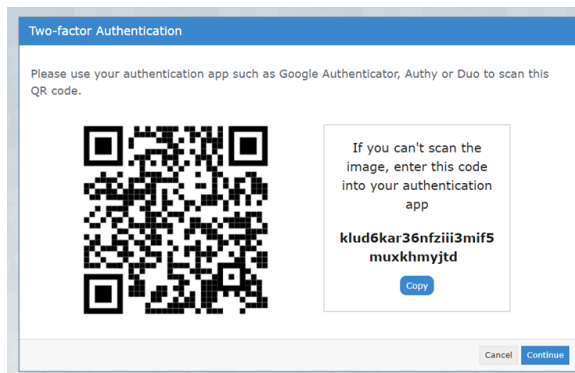
5. Enter the code your app provided you, then select "Submit".
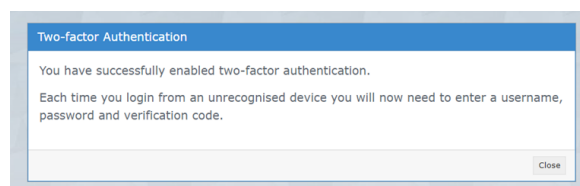

6. Your Two-Factor Authentication is now setup – Click "Close".
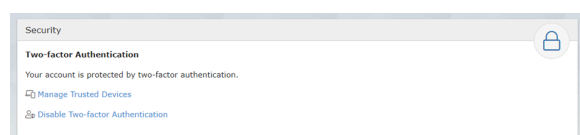
Managing Trusted Devices

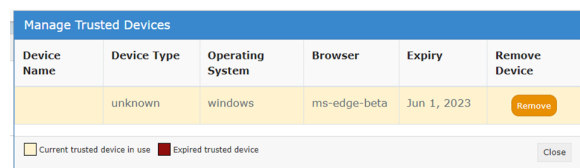1. Locate the "Security" section on your Medical Objects dashboard, and select "Manage Trusted Devices".

2. A list of trusted devices should display. Simply click "Remove" to delete a trusted device.

Please note: Trusted devices will allow you to skip the Two-Factor steps for 30 days - once the 30 days expires they will show as a "Expired Trusted Device". This means the next time you log into the portal on this device you will be prompted to enter the code you receive from your Two-Factor Authentication app.

2FA F.A.Q

What is two-factor authentication?

Two-factor authentication is a security feature that helps protect your account in addition to your password. With two-factor authentication, a special login code together with your username and password will need to be entered each time someone tries to access your account from a computer or device we don't recognise.

What do I need to be able to use it?

In order to generate the special login codes, you will need to install an app which supports the Time-based One-time Password Algorithm (TOTP) such as Google Authenticator, Authy, Microsoft Authenticator or Duo. There are many others, and some of these apps also support generating codes from desktop computers.

Do I always need to enter a code when logging in?

During login, you can choose not to use two-factor authentication again on that specific device by setting it as a 'trusted device'. If you select this option, that device will only ask for your username and password when logging in for the next 30 days. You will still be protected, because when you or anyone else tries to sign in to your account from an unrecognised device, two-factor authentication will be required.

Browser third party cookies need to be enabled for Explorer Online and two-factor authentication to operate correctly. They are usually enabled by default.

You should not choose to trust a public device.

How do I enable two-factor authentication?

To enable two-factor authentication, you will need to use your app to scan a QR code generated by Explorer Online (or type in the code if you cannot scan it). Your app will then generate a confirmation code which you need to enter when prompted by Explorer Online.

Your account will now be two-factor authentication enabled, and you will need to generate a code with your app whenever prompted by Explorer Online during login.

Can this be made mandatory for everyone at the organisation?

Two-factor authentication can be made mandatory for all users. This will force each account on login to enable two-factor authentication (if it is not already enabled). Please contact our helpdesk (helpdesk@medicalobjects.com) if you would like this enabled.

How to reset two-factor authentication?

If you have lost your device or app which was used to enable two-factor authentication, email helpdesk@medicalobjects.com for assistance.

Dashboard Navigation

The Dashboard is the default page that will appear once you have logged into Explorer Online. The Dashboard is split into two sections: the navigation menu and the main content area.
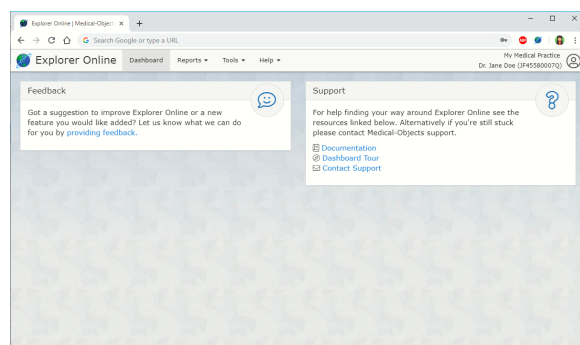

Navigation Menu
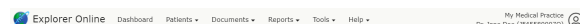
This is the main navigation menu. The menu is dynamically built up based on what features your server has enabled and what permissions your user account has. If a menu item is missing you may need to call the Helpdesk to correct your user permissions or enable a server feature.
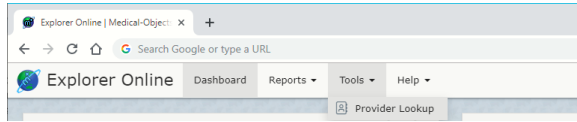
Changing Your Password

Click on the **User Menu**, then click **Change Password**.
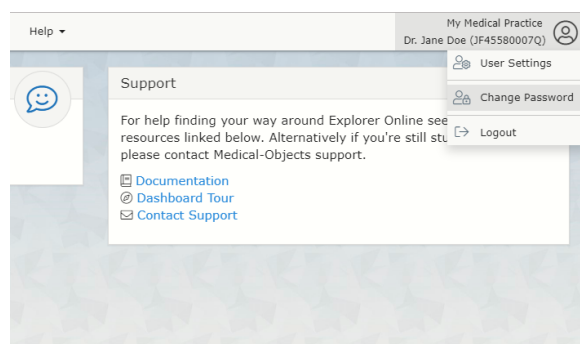
Provider Lookup

The **Provider Lookup** feature allows you to easily search details and check if a provider is routable (setup to receive sent results).

1. To access the **Provider Lookup** feature, click on the **Tools** tab, then click **Provider Lookup**.

2. Enter the details of the provider in the search box, enter the surname first if you are searching by the **Name** search type. Press the **Search** button or hit the enter key to load results.
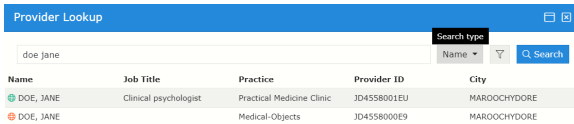
3. You can check to see if the provider number is routable by looking for the green globe in the **Name** column.
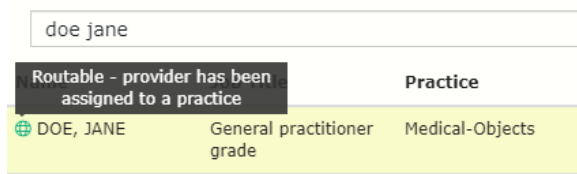
Having issues finding a doctor? Try the following:

⚠️

- Change the search type to **Organisation**, and search for the practice name.

- Try a partial name search if you're unsure of the full name. "Bob Johnson" can be found by searching for "John B" or "Jo Bob".

- If the doctor has a space in their surname, try leaving out the space. For example, "Bob Von Doctor" can by found by searching "VonDoctor" as the surname.

Activity Report

The Activity Report allows you to view the transaction history of both incoming and outgoing documents. You can access the Activity Report via the **Reports** top menu option.
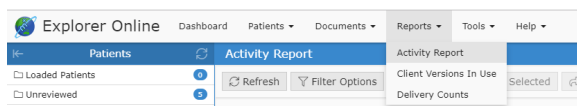
When selecting the Activity Report menu option you will be presented with a window listing the report filtering options available. These will help you narrow the report down to only the documents you're interested in. By default, the filter options will show the current daily activity. You can leave it at that or you can click on the drop down button next to the end date to select a pre-defined range.

Filter Options

Report Date:

| From | 03/10/2018 | 📅 | | To | 04/10/2018 | 📅 | ▾ |

| | |
Patient:	Today
	Last 7 days
Recipient Provider Number:	Last 14 days
	Last 30 days
Author Provider Number:	
	All this month
Delivered:	All last month

| Clear Filters | | Cancel | **Apply Filters** |

Tips
ⓘ

- You can hide or show columns via the grid menu (☰) which can be accessed by clicking the far button on the grid.
- You can drag to re-order columns. The position of columns will be remembered.
- You can reset the grid layout by choosing **Reset View** from the grid menu.

Understanding the report

Date	The date the document was created.
Patient	Patient name. SURNAME, First name (Date of Birth)
Recipient	The provider the document was addressed to.
Report Title	The document title.
Author	The provider that authored the document.
To Practice	The server name of the practice that the document was sent to. This is generally the practice name.
Status	The status of the document. The most common are; • Final result - document stored and verified. Can only be changed with a corrected result. • Not yet verified - document stored but not yet verified. • Correction - correction to the document.
Delivery Type	The software of the recipient that received the document.
Delivered	This is a timestamp for when the document was delivered. It does not necessarily mean that the document has been viewed or reviewed - only that it has been delivered. If this field is blank then the document has not been delivered.
Reviewed	The document has been marked as reviewed at the receiver's end. This column will only be populated if the receiver's **Delivery Type** is *EQUATORDXTRAY*. If not then it's best to look at the **ACK** column for an indication if the document has been acknowledged.
ACK	This column allows you to know whether or not the document has been acknowledged. To see what each icon in this column means; refer to the **ACK Legend** that can be found in the top right. Hover your mouse over each icon for a description. ACK Legend: ⊘ ✓ ✗
View	Clicking the icon in this column will display the document.

Viewing documents in the report

You can view a single document by clicking on the view document icon ( ) in the **View** column of the grid. This will open the document in the document viewer window.

From this window you can perform various actions on the single document such as print, forward or loading the patient file via the **All Documents** button. You can also navigate to other documents via the back and forward buttons in the top right.

Bulk Actions

You can select multiple documents in the grid and then perform an action on the selection. Currently the bulk actions available are;

- Printing
- Forwarding
- Exporting to CSV (this exports the transaction details and not the document itself, useful for auditing purposes)