













# Iress Pro: Connect to Iress

The following topics will be updated or created:

## Contents

Help Table of Contents .....	2
Default Log In.....	3
Log in .....	3
Log in using multi-factor authentication .....	3
Activate Okta Log In .....	5
Prerequisites .....	5
Activate Okta log in.....	5
Multi-factor Authentication .....	7
Prerequisites .....	7
Set up multi-factor authentication .....	7
Change multi-factor authentication (Okta profile) .....	8
Network Configuration .....	10
Configure the Phoenix servers .....	10
Change the server manually.....	11
Change Your Password.....	12
Change your password .....	12
Change your password (Okta enabled) .....	12
Change Server Settings.....	13
Set the primary server connection .....	13
Set the secondary server connection .....	14
Force a connection .....	15
Synonym file .....	16
Directional .....	16
Microcontent.....	16

# Help Table of Contents

	IRESS Help
	IRESS Command List
	What's New In IRESS
	Core Help
	Connect to IRESS
	Default Log In
	Log In Queuing
	Network Configuration
	Change Your Password
	Activate Okta Log In
	Multi-factor Authentication
	IRESS Basics

<b>Topic info:</b>	
<b>Source</b>	Content/Connect_to_IRESS/Default_Log_In.htm
<b>ToC</b>	Iress Help > Core Help > Connect to IRESS > Default Log In
<b>Concept terms</b>	Login - Default IRESS; Login IRESS
<b>Keyword terms</b>	default;default:log in;authenticate;log in;log in:default log in;SMS;Google Authenticator;Okta;Okta:Okta Verify;multi-factor authentication:log in
<b>Concept links (see also)</b>	Login IRESS
<b>Alias ID (for new topics)</b>	

## Default Log In

The user code or username identifies a user in Iress and provides access to the functionality for which the user is authorized.

**Note:** From Iress Pro 21.1.17 onwards users are required to have access to [http://services.iress\\*](http://services.iress*) in order to access their user settings and use the application.

### [Iress service URLs and network configuration](#)

This topic explains how to log in to Iress using the direct login method and using multi-factor authentication (MFA).

## Log in

1. Launch Iress.
2. In the Login dialog box, type your user name and password.
3. Click Login.

## Log in using multi-factor authentication

To log in using multi-factor authentication you have to complete the prerequisite Okta steps and configure your multi-factor authentication method. [📘 Activate Okta Log In](#) [📘 Multi-factor Authentication](#)

1. Launch Iress.  
The Iress **Sign In** dialog box opens.
2. In the **Username** and **Password** boxes, type your login credentials.  
**Tip:** To autofill your login username, select the **Remember username** checkbox.
3. Click **Sign In**.
4. If you have multiple authentication methods configured, click the down arrow and select a method from the **Select an authenticator factor** list.
5. Complete authentication for your selected method:

### **Okta Verify - using push notification**

- i. Click **Send Push**.
- ii. On your mobile device, confirm that you are logging into Iress.

#### **Okta Verify - using code**

- i. Click **Or enter code**.
- ii. In the **Enter Code** box, type the code displayed in the Okta Verify app.
- iii. Click **Verify**.

#### **Google Authenticator**

- i. In the **Enter Code** box, type the code displayed in the Google Authenticator app.
- ii. Click **Verify**.

#### **SMS Authentication**

- i. Click **Send Code**.
- ii. In the **Enter Code** box, type the code received via SMS.
- iii. Click **Verify**.

<b>Topic info:</b>	
<b>Source</b>	Content/Connect_to_IRESS/Activate_Okta_Log_In.htm
<b>ToC</b>	Iress Help > Core Help > Connect to IRESS > Activate Okta Log In
<b>Concept terms</b>	Login - Default Iress;Login IRESS
<b>Keyword terms</b>	Okta;Okta:activate;log in:Okta;log in:activate;authenticate;Multi-factor authentication
<b>Concept links (see also)</b>	Login IRESS
<b>Alias ID (for new topics)</b>	-

## Activate Okta Log In

Iress uses Okta which supports multi-factor authentication (MFA) to provide you secure authentication when logging into Iress products. This topic explains the prerequisites required to use Okta, the initial steps you need to complete to activate your Okta login, and how to configure an authentication method. You only need to activate Okta login once for your account.

Note: The use of MFA is not required during Okta activation. Once Okta is activated, the use of MFA during Iress login is optional.

### Prerequisites

- Iress Pro version 21.1.17 or above
- Okta enabled at a user, group or company level by an administrator
- Firewall access to [Iress Services](#) and Okta
  - \*okta.com
  - \*oktacdn.com

### Activate Okta log in

1. Once all prerequisites are met, open and login to Iress with the process and credentials you previously used.
2. Close Iress completely by doing one of the following:
  - Click the **X** at the top-right corner of the Iress window.
  - Select **File > Exit**.
3. Open Iress again.  
The Iress **Sign In** dialog box opens.
4. In the **Username** and **Password** boxes, type your login credentials.
5. Click **Sign In**.
6. In the **Email address** box, type your email address.
7. Click **Submit**.  
An activation code is sent to your email account.
8. In the **Email validation number** box, type the activation code.

9. Click **Submit**.

Okta is activated and you are logged in to Iress.

Your Okta login is now activated. The Iress **Sign In** dialog box will display when you open Iress. If required, at your next login you can configure a multi-factor authentication method. [📘 Multi-factor Authentication](#)

<b>Topic info:</b>	
<b>Source</b>	Content/Connect_to_IRESS/Multifactor_Authentication.htm
<b>ToC</b>	Iress Help > Core Help > Connect to IRESS > Multi-factor Authentication
<b>Concept terms</b>	Login IRESS;Login - Default Iress
<b>Keyword terms</b>	Okta;authenticate;multi-factor authenticationmulti-factor authentication:set up;multi-factor authentication:change;multi-factor authentication:remove;SMS;Okta:Okta Verify;Google Authenticator
<b>Concept links (see also)</b>	Login IRESS
<b>Alias ID (for new topics)</b>	-

## Multi-factor Authentication

Iress uses Okta which supports multi-factor authentication (MFA) to provide you secure authentication when logging into Iress products. Once Okta is activated and MFA is enabled for your account you can configure an authentication method. This topic explains how to configure or change authentication methods.

### Prerequisites

- MFA enabled at a user, group or company level by an administrator
- A mobile authenticator application
  - Okta Verify
  - Google Authenticator

### Set up multi-factor authentication

After you have activated your Okta login, at your next login you are prompted to set up a MFA method. You can configure up to 3 MFA methods.

**Tip:** Configure SMS Authentication and one of either Okta Verify or Google Authenticator, so you have access to a backup authentication method in the event of a change or loss of mobile device, or loss of data connection or Wi-Fi. Alternatively, you can remove and set up methods in your [Okta profile](#).

1. On your iPhone or Android mobile device, download and install either **Okta Verify** or **Google Authenticator**.
2. Open Iress.  
The Iress **Sign In** dialog box opens.
3. In the **Username** and **Password** boxes, type your login credentials.  
**Tip:** To autofill your login username, select the **Remember username** checkbox.
4. Click **Sign In**.  
The **Set up multifactor authentication** screen displays.
5. For your chosen authenticator application, click **Setup** and complete the required steps for the selected method as detailed below.
6. If you are not configuring all authentication options, click **Finish**.

If you have configured multiple authentication methods, the next time you log in to Iress you can choose which authentication method to use for that login. ⓘ [Log in using multi-factor authentication](#)

## Okta Verify

- i. Select your mobile device type, then click **Next**.  
A QR code displays.
- ii. On your mobile device, launch the **Okta Verify** application.
- iii. In the app, select the **+**, then select **Organization**.
- iv. Select **Yes, Ready to Scan**.
- v. Scan the on-screen QR code with your mobile device.

## Google Authenticator

- i. Select your mobile device type, then click **Next**.  
A QR code displays.
- ii. On your mobile device, launch the **Google Authenticator** application.
- iii. In the app, select the **+**, then select **Scan a QR code**.
- iv. Scan the on-screen QR code with your mobile device.  
A verification code displays on your mobile device.
- v. Click **Next**.
- vi. On the **Setup Google Authenticator** screen, in the **Enter Code** box, type the verification code.
- vii. Click **Verify**.

## SMS Authentication

- i. On the **Receive a code via SMS to authenticate** screen, select your country from the dropdown list.
- ii. In the **Phone number** box, type your phone number.
- iii. Click **Send code**.  
A code is sent via SMS to your mobile device.
- iv. In the **Enter Code** box, type the received code.
- v. Click **Verify**.

## Change multi-factor authentication (Okta profile)

You can access your Okta profile to remove and add multi-factor authentication methods.

1. In a web browser, go to <https://cdn.iress.com/pe/iress-id/tmd/login.html>.
2. Click your Iress region.  
The Iress **Sign In** dialog box opens.
3. In the **Username** and **Password** boxes, type your login credentials.
4. Click **Sign In**.
5. If configured, [log in using multi-factor authentication](#).  
The Iress Okta dashboard displays.



6. In the top right corner, click the down arrow next to your profile name, and select **Settings**. Your **Account** settings screen displays.
7. Click **Edit Profile**.
8. If configured, [log in using multi-factor authentication](#).
9. In the **Extra Authentication** section, select the required action next to a method.

## Set up a MFA method

- i. Next to a method, click **Set Up**.  
The **Set up multifactor authentication** window displays.
- ii. Click **Setup** and complete the required steps for the selected method as detailed above. ⓘ [Set up multi-factor authentication](#)

## Remove a MFA method

- i. Next to a method, click **Remove**.  
A confirmation dialog box opens.
- ii. Click **Yes**.

If you remove all MFA methods from your profile, the next time you log in to Iress you will be prompted to add an authentication method. ⓘ [Set up multi-factor authentication](#)

<b>Topic info:</b>	
<b>Source</b>	Content/Connect_to_IRESS/Network_Configuration.htm
<b>ToC</b>	Iress Help > Core Help > Connect to IRESS > Network Configuration
<b>Concept terms</b>	Network Config IRESS; Login IRESS; Settings - Behaviour IRESS
<b>Keyword terms</b>	Options menu;connecting to IRESS;network configuration;settings:network configuration;settings:service URLs;service urls
<b>Concept links (see also)</b>	Settings - Behaviour IRESS
<b>Alias ID (for new topics)</b>	

## Network Configuration

Iress can be configured to connect to one or two Phoenix servers. Server configuration is recorded in the **Iress Settings** dialog box. Several URLs also need to be allow listed to allow Iress to connect to our services, such as user settings.

The URLs for these services, by region, are:

Region	Services URL
<b>All regions</b>	For identity and access management: <ul style="list-style-type: none"> <li>*.okta.com</li> <li>*.oktacdn.com</li> </ul> Third-party authorities used to validate Iress web certificates: <ul style="list-style-type: none"> <li>http://ocsp.sca1b.amazontrust.com</li> <li>http://ocsp.digicert.com</li> </ul>
<b>AU/NZ</b>	pro.iress.com.au pro.iress.com
<b>SG</b>	pro.iress.com.au pro.iress.com pro.iress.com.sg
<b>UK</b>	pro.iress.co.uk pro.iress.com
<b>CA</b>	pro.iress.co.ca pro.iress.com
<b>ZA</b>	pro.iress.co.za pro.iress.com

## Configure the Phoenix servers

- Open the **Iress Settings** dialog box by doing one of the following:
  - Choose **Options > Settings**.
  - In the status bar in the bottom right corner of the Iress window, double-click the client name.
- Select the **Network Configuration** tab.
- In the **Primary Connection** section, enter details for the primary server by doing the following:
  - In the **Connection Type** list, select **WEBSOCKETS**.

- ii. In the **Socket Address** box, type the first service URL for your region from the list above.
- iii. In the **Port** box, select 443.
4. In the **Secondary Connection** section, enter details for the secondary server by doing the following:
  - i. Tick the **Fail Over after** checkbox. The data entry fields become enabled.
  - ii. In the **Fail Over after** box, type the time in seconds that Iress will wait before attempting to reconnect to the secondary server if it fails.
  - iii. In the **Connection Type** list, select **WEBSOCKETS**.
  - iv. In the **Socket Address** box, type the second URL for your region from the list above.
  - v. In the **Port** box, select 443.

Do not change the value in the **Connecting To** list. This displays the connection in current use.

5. Click **OK**.

## Change the server manually

To change the server manually, both a primary and a secondary server must be configured.

1. Open the **Iress Settings** dialog box by doing one of the following:
  - Choose **Options > Settings**.
  - Double-click the client name on the status bar in the bottom right corner of the Iress window.
2. Select the **Network Configuration** tab.
3. In the **Connecting To** list, select the server to which the connection will be made, i.e. **Primary** or **Secondary**.
4. Click **Apply**. Iress connects to the selected server.
5. Click **OK**.

<b>Topic info:</b>	
<b>Source</b>	Content/Connect_to_IRESS/Change_Your_Password.htm
<b>ToC</b>	Iress Help > Core Help > Connect to IRESS > Change Your Password
<b>Concept terms</b>	Password IRESS; Login IRESS; Login - Default Iress
<b>Keyword terms</b>	password;changing\; see modifying:password;log in:changing your password;logins:changing;Okta;Okta:password;resetting:passwords
<b>Concept links (see also)</b>	Login IRESS
<b>Alias ID (for new topics)</b>	

## Change Your Password

You can change your password at any time.

### Change your password

1. Choose **File > Change Password**. The **Change Password** dialog box opens.
2. In the **Old password** box, type your current password.
3. In the **New password** box, type your new password.  
**Note:** We recommend that you create passwords at least 14 characters long, with a mix of upper and lowercase and alphanumeric characters and symbols.
4. In the **Verify new password** box, type your new password again.
5. Click **Change password**.

### Change your password (Okta enabled)

1. On the Iress **Sign In** dialog box, click **Forgot password?**
2. In the Username box, type your Iress username.
3. Click **Reset**.  
An email is sent to your email address with a link to reset your password.  
**Note:** The reset link is active for 2 hours, after which you will need to restart the password reset process.
4. In the email, click **Reset password**.  
The **Set your password** screen opens in your web browser.
5. In the **New password** box, type a new password that meets the password requirements.
6. In the **Repeat password** box, type the new password again.
7. Click **Set Password**.  
The **Password Reset Complete** screen displays.
8. Click **Open Iress Pro**.
9. In the **Password** box, type your new password.
10. Click **Sign In**.

<b>Topic info:</b>	
<b>Source</b>	Content/IRESS_Administration/User_Manager/Change_Server_Settings.htm
<b>ToC</b>	Iress Help > IRESS Administration > User Manager > Change Server Settings
<b>Concept terms</b>	User Man - Manage IRESS
<b>Keyword terms</b>	forcing a server connection;modifying - IRESS:server connections;connecting to IRESS;secondary connection;settings;settings:server
<b>Concept links (see also)</b>	User Man IRESS;User Man - Manage IRESS;Network Config IRESS
<b>Alias ID (for new topics)</b>	

## Change Server Settings

*The User Manager command is only available to authorized users.*

**Note:** This command displays static information. To update the information displayed, click **Refresh**.

Authorized users can set the primary and secondary connections for one or more users and change the users current connection to either their primary or secondary setup.

These changes affect the **Network Configuration** tab in the **Iress Settings** dialog box. [i Network Configuration](#)

### Set the primary server connection

**Note:** If the user is connected to the primary server, completing this procedure forces the user to connect to the new primary server.

1. [Open](#) the User Manager command.
2. [Display](#) user information in the right pane.
3. Select the user/s you want to modify by doing one of the following:

#### Select one user

- Right-click the name of the user and select **Set / Change Connection**.

#### Select multiple users

- i. Hold down the **Ctrl** key and click each user.
- ii. Right-click any of the selected lines and select **Set / Change Connection**.

The **Connection** dialog box opens.

4. Select the **Set Primary Connection** option.
5. Click **Next**.

6. In the **Connection Type** list, select the connection type.
7. Enter the connection details by doing one of the following:

#### The connection type is Websockets

- i. In the **Socket Address** box, type the server name or IP address.
- ii. In the **Port** box, type 443.

#### The connection type is Named Pipes

- In the **Pipe Name** box, type the name of the pipe; for example, \\servername\pipe\pnx.srv.
8. Click **Next**. A summary of your choices displays.
  9. Click **Finish**.

## Set the secondary server connection

**Note:** If the user is connected to the secondary server, completing this procedure forces the user to connect to the new secondary server.

1. [Open](#) the User Manager command.
2. [Display](#) user information in the right pane.
3. Select the user/s you want to modify by doing one of the following:

#### Select one user

- Right-click the name of the user and select **Set / Change Connection**.

#### Select multiple users

- i. Hold down the **Ctrl** key and click each user.
- ii. Right-click any of the selected lines and select **Set / Change Connection**.

The **Connection** dialog box opens.

4. Select the **Set Secondary Connection** option.
5. Click **Next**.
6. To enable the secondary connection, tick the **Fail Over after** checkbox.

**Note:** If you want to disable the secondary connection, untick the **Fail Over after** checkbox and proceed to step 9.

7. In the **Connection Type** list, select the connection type.
8. Enter the connection details:

### The connection type is Websockets

- i. In the **Socket Address** box, type the server name or IP address.
- ii. In the **Port** box, type 443.

### The connection type is Named Pipes

- In the **Pipe Name** box, type the name of the pipe, e.g. \\servername\pipe\pnx.srv.
9. Click **Next**. A summary of your choices displays.
  10. Click **Finish**.

## Force a connection

1. [Open](#) the User Manager command.
2. [Display](#) user information in the right pane.
3. Select the users you want to modify by doing one of the following:

#### Select one user

- Right-click the name of the user and select **Set / Change Connection**.

#### Select multiple users

- i. Hold down the **Ctrl** key and click each user.
- ii. Right-click any of the selected lines and select **Set / Change Connection**.

The **Connection** dialog box opens.

4. Select the **Force Connection to PRIMARY/SECONDARY** option.
5. Click **Next**.
6. In the **Force Connection** list, select the connection you want to use. Select **Primary** to use the primary server, or **Secondary** to use the secondary server.
7. Click **Next**. A summary of your choices displays.
8. Click **Finish**.

## Synonym file

File info:	
Source	Project/Advanced/Synonym_Iress

Based on current results in Central Analytics

### Directional

Synonym	Word
password	reset locked forgot Passwrod password Forgotten Frget Forgt pass
System information	sysinfo
system	sysinfo
login	Log in Logging in
2FA	MFA

### Microcontent

File info:	
Source	Content/Resources/MicroContent/ConnectToIress.filmco

Phrase	Link
Change password Password Password change	Content/Connect_to_IRESS/Change_Your_Password.htm#Change_Password
Reset password Forgot Forgotten Password reset	Content/Connect_to_IRESS/Change_Your_Password.htm#Reset_Password
Login Log in Log on logon	Connect/Connect_to_IRESS/Default_Log_In