Cargo Interactive User Guide

Version 2.0

11th June 2024

Contents

Cargo Interactive Overview

What is Cargo Interactive?

Cargo Interactive is the gateway to the Department of Home Affairs ('The Department') online cargo service facility, hosted by the Customs Connect Facility (CCF) platform. CCF accepts electronic transactions from both people (referred to as Users) and machines (referred to as Devices). Each User and Device transacting with The Department must first be registered to deal electronically with The Department.

Identity Manager is the application within Cargo Interactive used to register and maintain details of all Users and Devices that transact electronically with The Department for cargo reporting purposes.

For more information about Identity Manager, see the Identity Manager User Guide.

Who uses the Cargo Interactive application?

Only Users who have been registered to deal with Cargo Interactive can use this Application. Users identify themselves electronically with use PKI Digital Certificates to electronically identify themselves.

Users are registered either as Individuals who personally deal with The Department or as a representative of an Organisation. Devices are always registered as a representative of an Organisation.

Individuals

A User who deals with The Department as an Individual must first complete the Cargo Interactive Registration process. During this process they will digitally sign (with their PKI Digital Certificate) the User Agreement which outlines the terms and conditions of use of the CCF.

A registered User can use the Cargo Interactive application to:

- View their User details.
- Associate further PKI Digital Certificates with their account.

Organisations

An Organisation who deals with The Department must first have a suitably authorised representative complete the Cargo Interactive Registration process on behalf of the Organisation. During the process this representative will digitally sign (with their PKI Digital Certificate) the User Agreement which outlines the terms and conditions of use of the CCF. This representative is referred to as the Signing Authority.

Signing Authorities

A Signing Authority can use Identity Manager within Cargo Interactive to:

- View their User details.
- Register and maintain all Users associated with their Organisation.
- Register and maintain all Devices associated with their Organisation.
- Transfer their Signing Authority role to another Registered User of their Organisation.
- Grant (and remove) an administrative role to Registered Users of their Organisation.

If a registered User is granted an administrative role they are referred to as an Administrator. Administrators can use the Identity Manager to:

- View their User details.
- Register and maintain all Users associated with their Organisation.
- Register and maintain all Devices associated with their Organisation.

How this User Guide works

This User Guide has been divided into three chapters:

- Functions available to all Registered Users.
- Functions available to Users who have the Administrator role.
- Functions available to Users who are the Signing Authority for their Organisation.

The Signing Authority can perform all functions available to Users with the Administrative role.

How to Self-Register Your Organisation

Introduction

In order for a new organisation to communicate with The Department, it must first be registered in the Customs Connect Facility (CCF). The person who registers the organisation is the person that will sign the CCF User Agreement on behalf of the organisation thereby taking responsibility on behalf of the organisation for agreement to interact with The Department within defined terms and conditions.

This person will also be automatically assigned the Signing Authority role.

To Register for Cargo Interactive

Please refer to the “Cargo Interactive Identity Manager Self-Registration User Guide” document.

Functions Available to All Registered Users

To log into the Cargo Interactive application

Once a User has successfully logged into Cargo Interactive they will be presented with a menu of applications which they have rights to access. This includes ICS, TAPIN, and Identity Manager.

All registered Users have the rights to access the Identity Manager application.

STEP 1. Browse to the Cargo Interactive Homepage.

The Cargo Interactive page is available at https://www.ccf.customs.gov.au/.

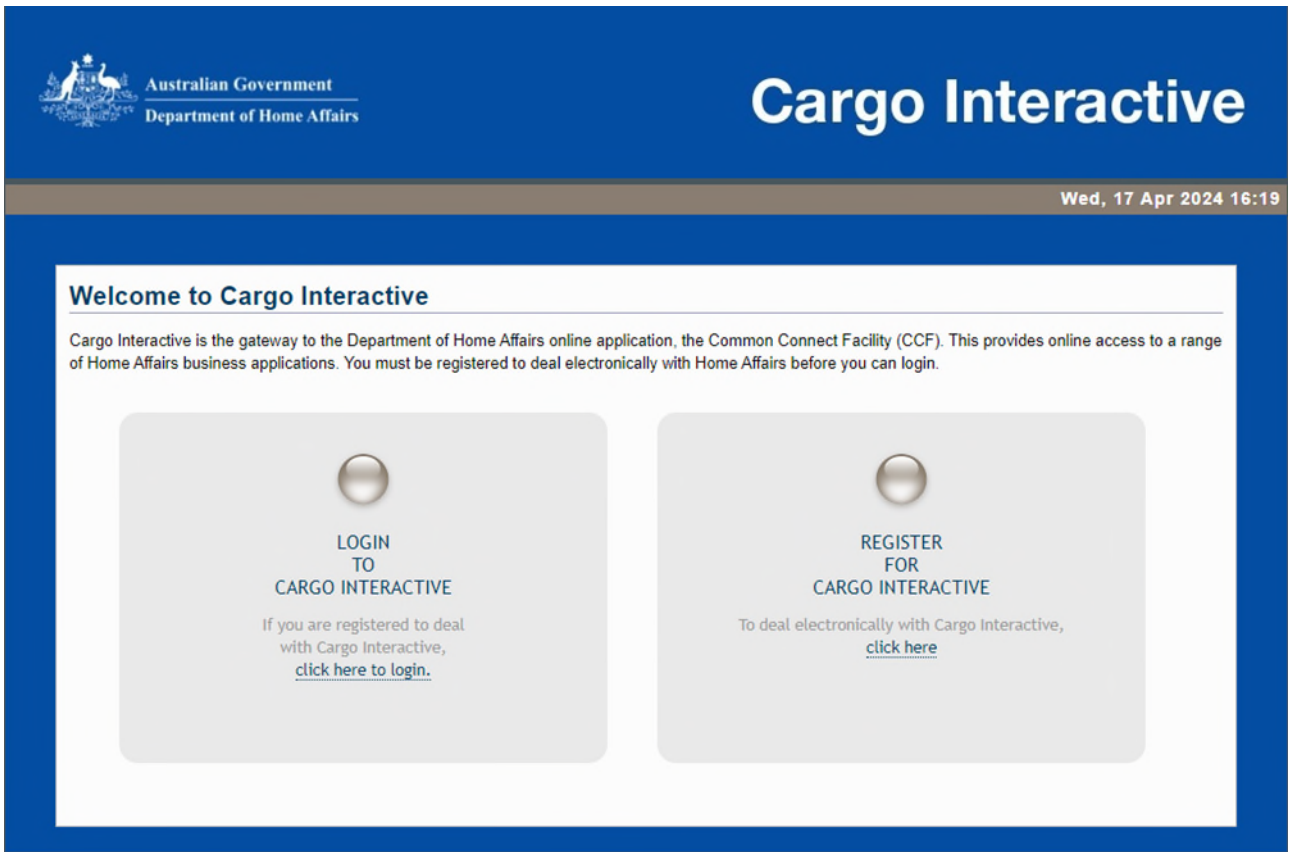

Figure 1: The Cargo Interactive Homepage.

STEP 2. Login to Cargo Interactive. The Terms and Conditions for use are displayed.

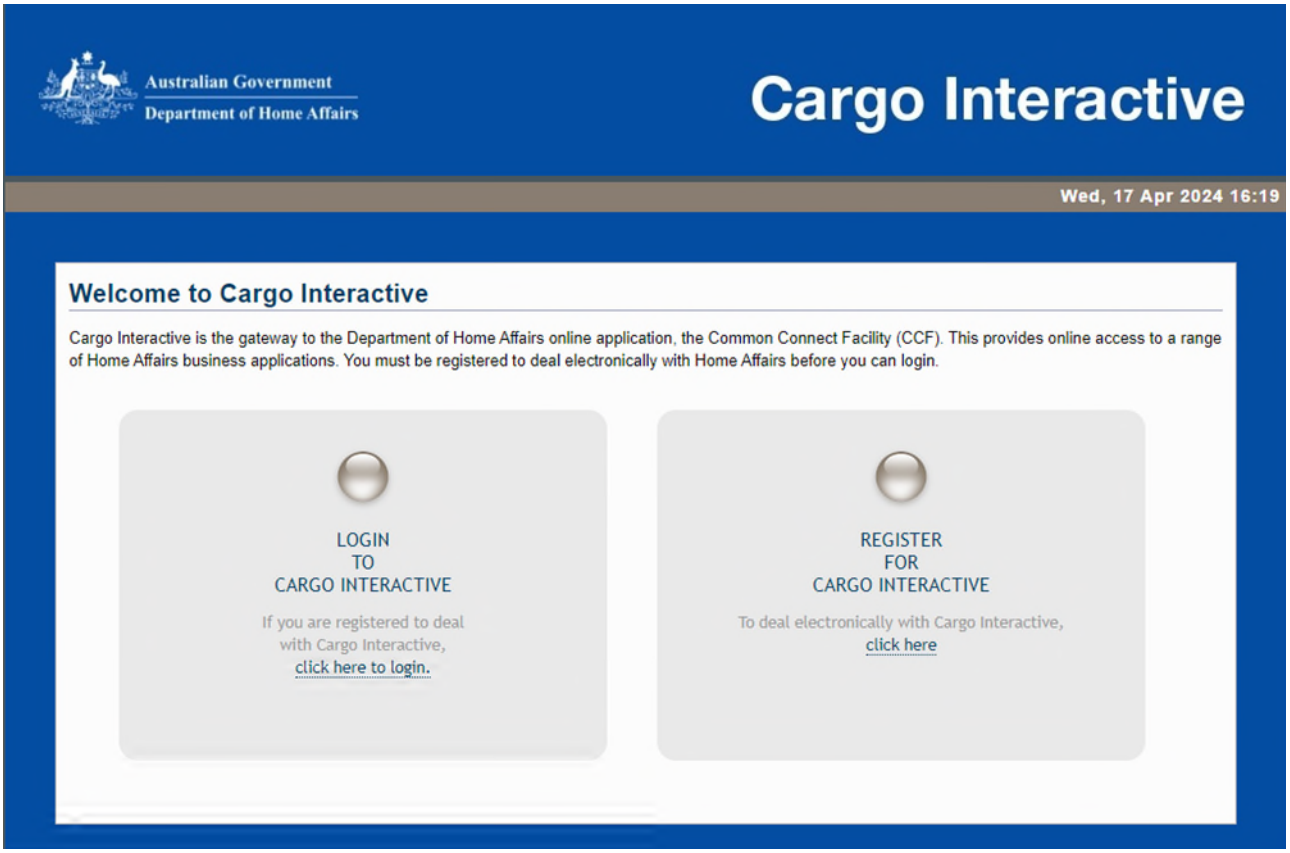

Figure 2: The Cargo Interactive Homepage with Login for Cargo Interactive highlighted.

NOTE

For institutions which are not registered with the Department, please consult the Cargo Interactive Identity Manager Self-Registration User Guide for more information on how to self-register.

STEP 3. Click on the Identity Manager link in the application menu.

If you agree to be bound by the terms of the CCF User Agreement, click “I agree”.

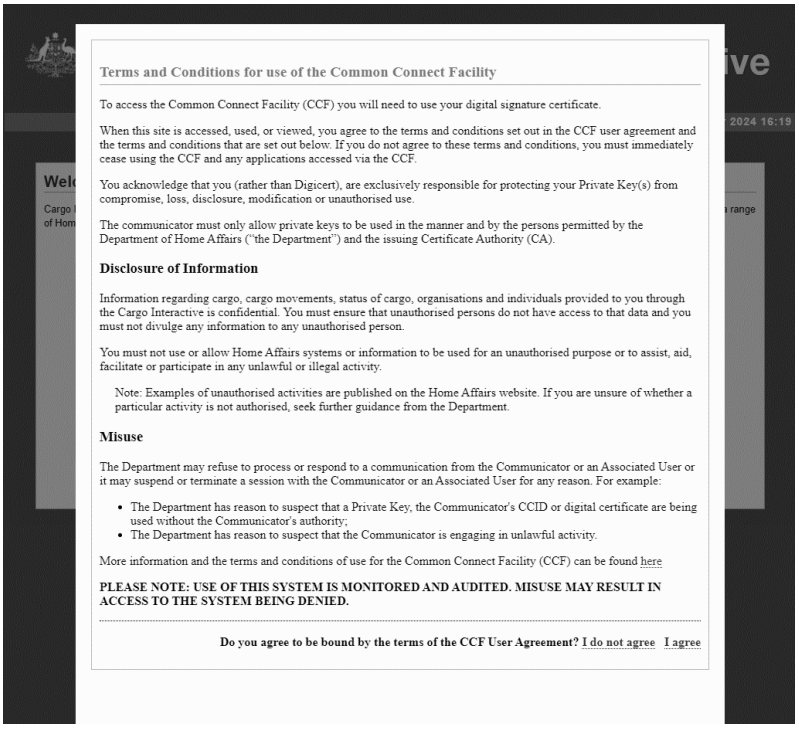

Figure 3: Click “I agree” to agree to be bound by the terms of the CCF User Agreement.

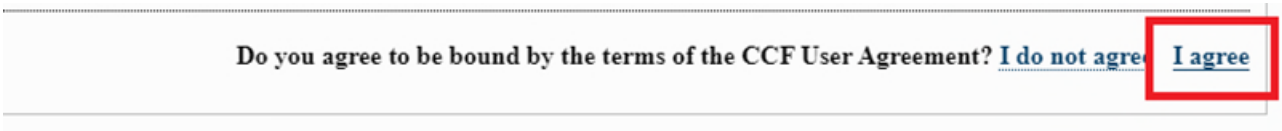

Figure 3a: Click “I agree” to agree to be bound by the terms of the CCF User Agreement (I agree highlighted).

STEP 4. Select Certificate for Authentication

NOTE

The appearance of the window to select a certificate for authentication, or to authorise access to your OS's certificate store, will vary depending on your particular certificate configuration and system specifications. These images are advisory in nature only.

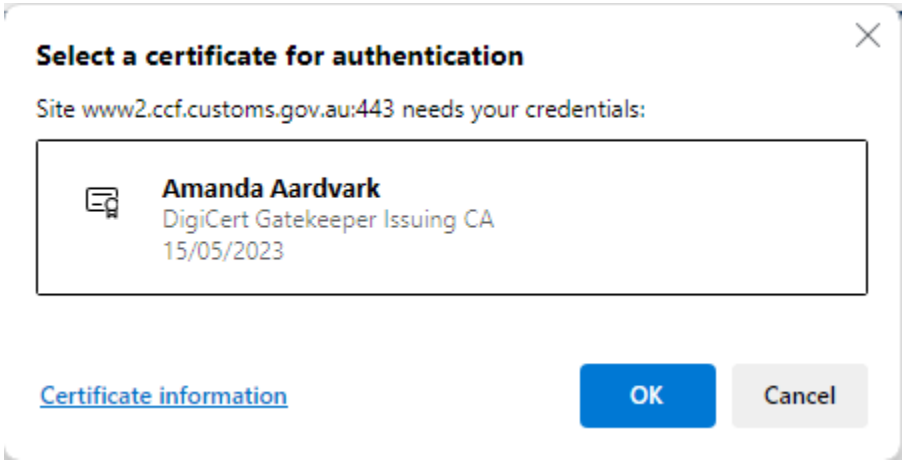

Figure 4: Certificate Selection Prompt

Figure 5: Credential Authorization Screen

To log into ICS

STEP 1. Log into Cargo Interactive.

See above.

STEP 2. Click on the ICS link in the application menu.

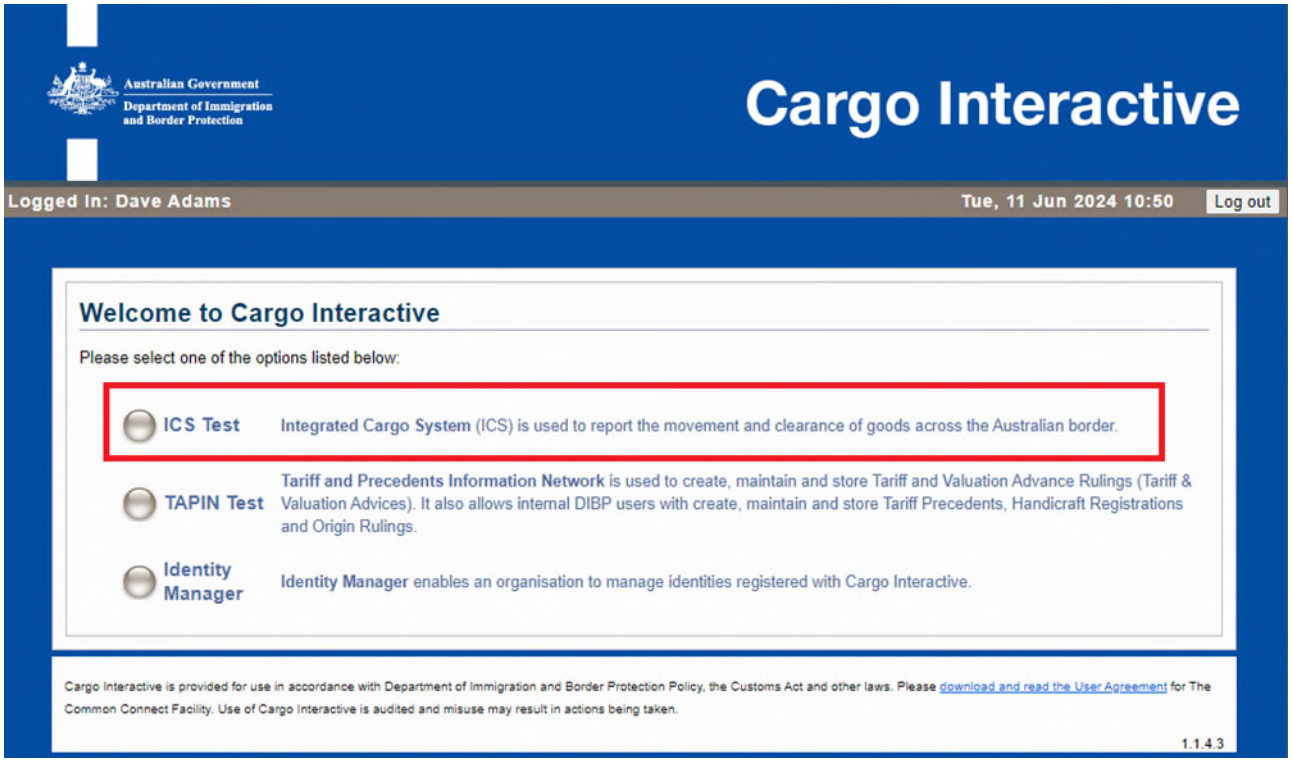

Figure 6a: Welcome to Cargo Interactive page with ICS highlighted

NOTE

These images were taken in the CCF Test environment. In the production environment, “ICS Test” and “TAPIN Test” will be labelled “ICS Prod” and “TAPIN Prod” respectively.

STEP 3. The ICS application opens.

The Integrated Cargo System Home Page will open.

To log into TAPIN

STEP 1. Log into Cargo Interactive.

See above.

STEP 2. Click on the TAPIN link in the application menu.

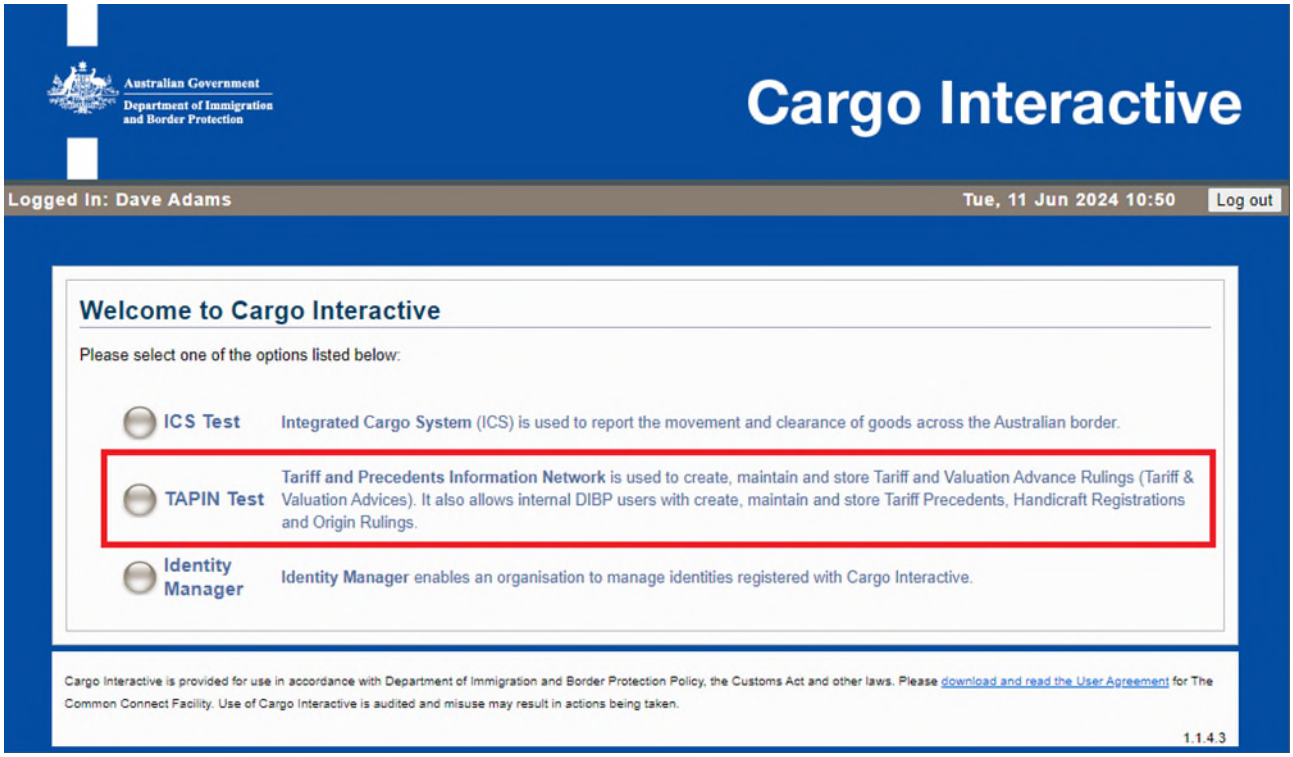

Figure 6b: Welcome to Cargo Interactive page with TAPIN highlighted

NOTE

These images were taken in the CCF Test environment. In the production environment, “ICS Test” and “TAPIN Test” will be labelled “ICS Prod” and “TAPIN Prod” respectively.

STEP 3. The TAPIN application opens.

The TAPIN Home Page will open.

To log into Identity Manager

STEP 1. Log into Cargo Interactive.

See above.

STEP 2. Click on the Identity Manager link in the application menu.

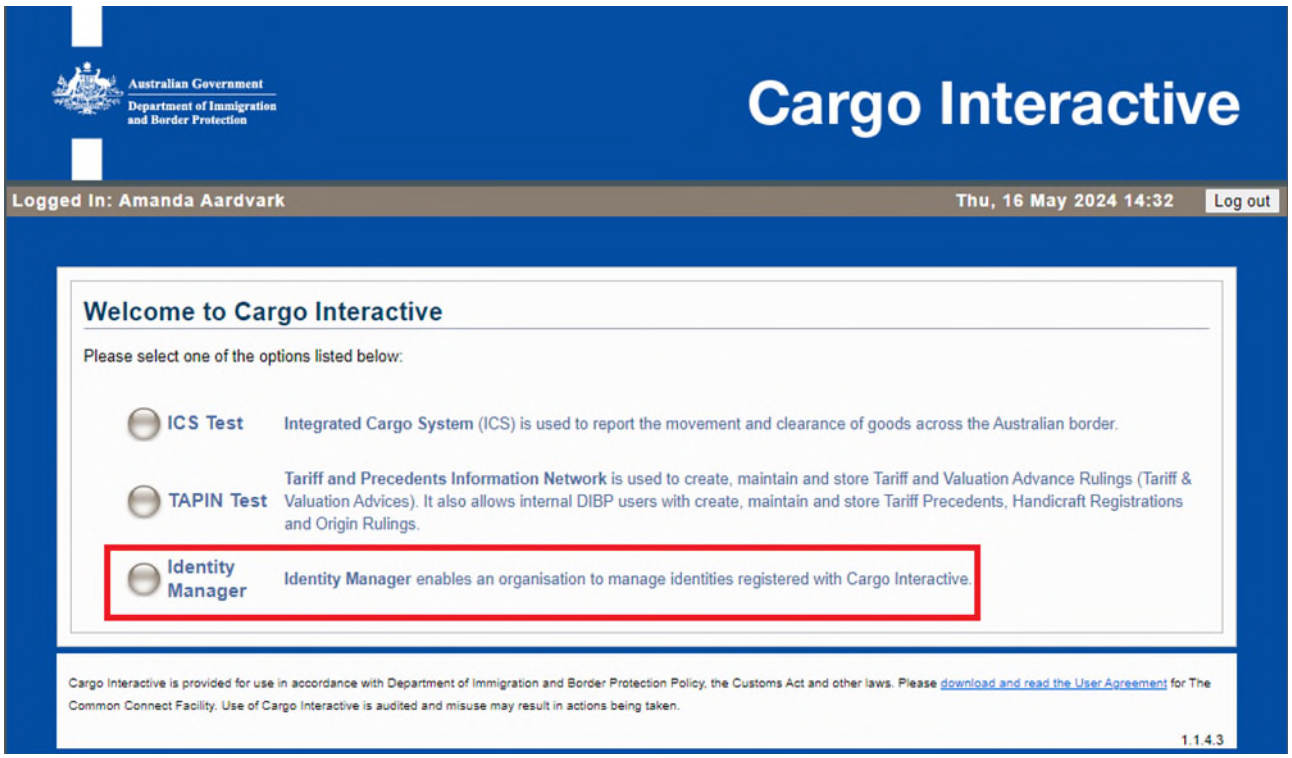

Figure 6c: Welcome to Cargo Interactive page with Identity Manager highlighted

STEP 3. The Identity Manager application opens.

If the user is an Administrator or Signing Authority, they will be taken to the **Organisation Detail Page**, otherwise they will be taken to their own **User Detail Page**.

To view your User details

You can view your User Details in the Identity Manager application within Cargo Interactive. This view will show you what Digital Certificates have been registered for your User and your current rights to access further applications in Cargo Interactive ("Rights to Applications)".

General Details

For Registered Users:

STEP 1. Login to Cargo Interactive.

STEP 2. Login to the Identity Manager application.

The Cargo Interactive Homepage is available at (https://www.ccf.customs.gov.au/).

See "Functions Available to All Registered Users" for more information.

STEP 3. Your User Details screen is displayed.

Figure 7: User Details (user)

For Administrators:

STEP 1. Login to the Identity Manager application.

The Cargo Interactive Homepage is available at (https://www.ccf.customs.gov.au/).

See "Functions Available to All Registered Users" for more information.

STEP 2. Your Organisation Detail screen is displayed.

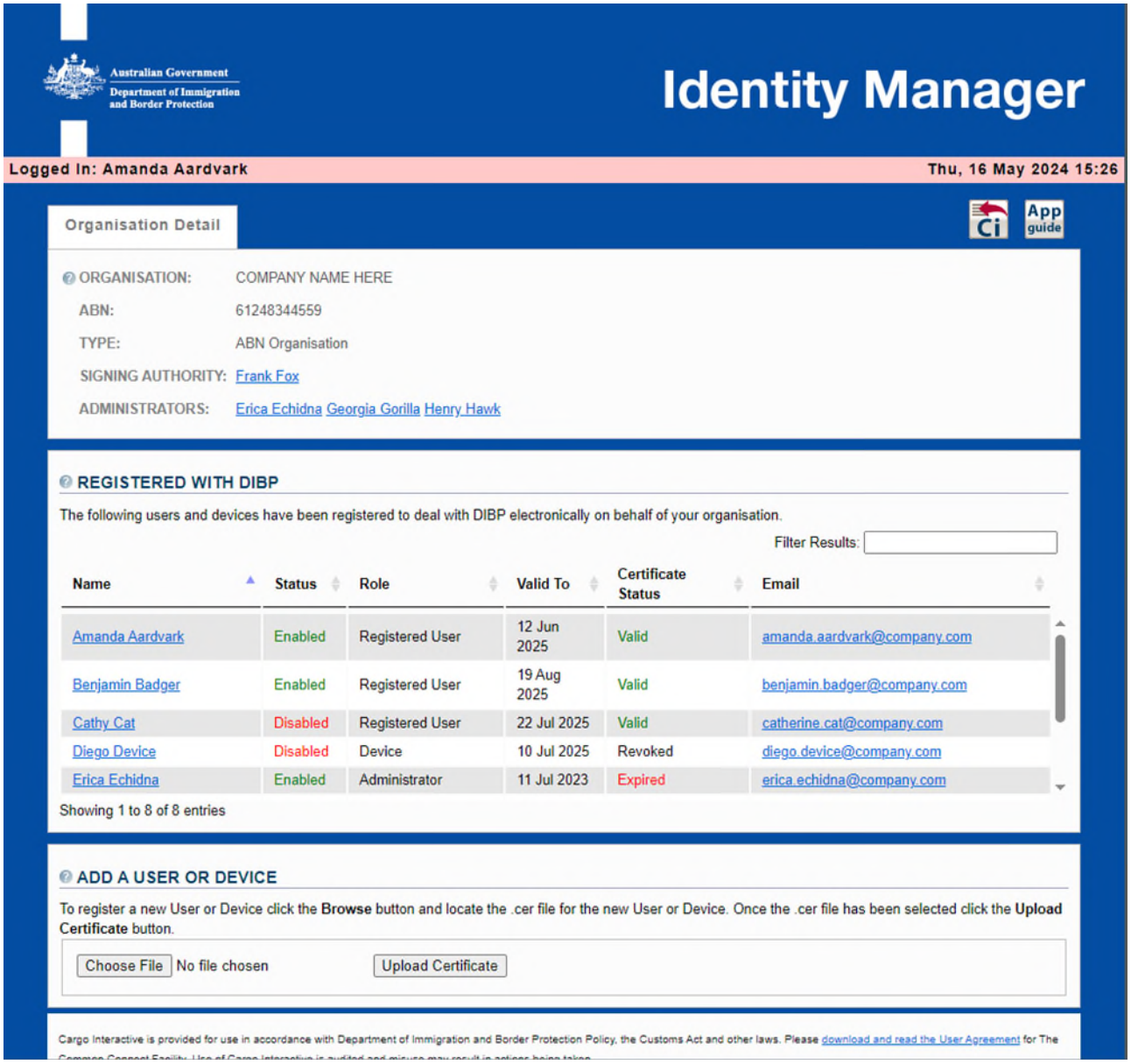

Figure 8: User Details (Administrator)

For Signing Authorities:

STEP 1. Login to the Identity Manager application.

The Cargo Interactive Homepage is available at (https://www.ccf.customs.gov.au/).

See “Functions Available to All Registered Users” for more information.

STEP 2. Your Organisation Detail screen is displayed.

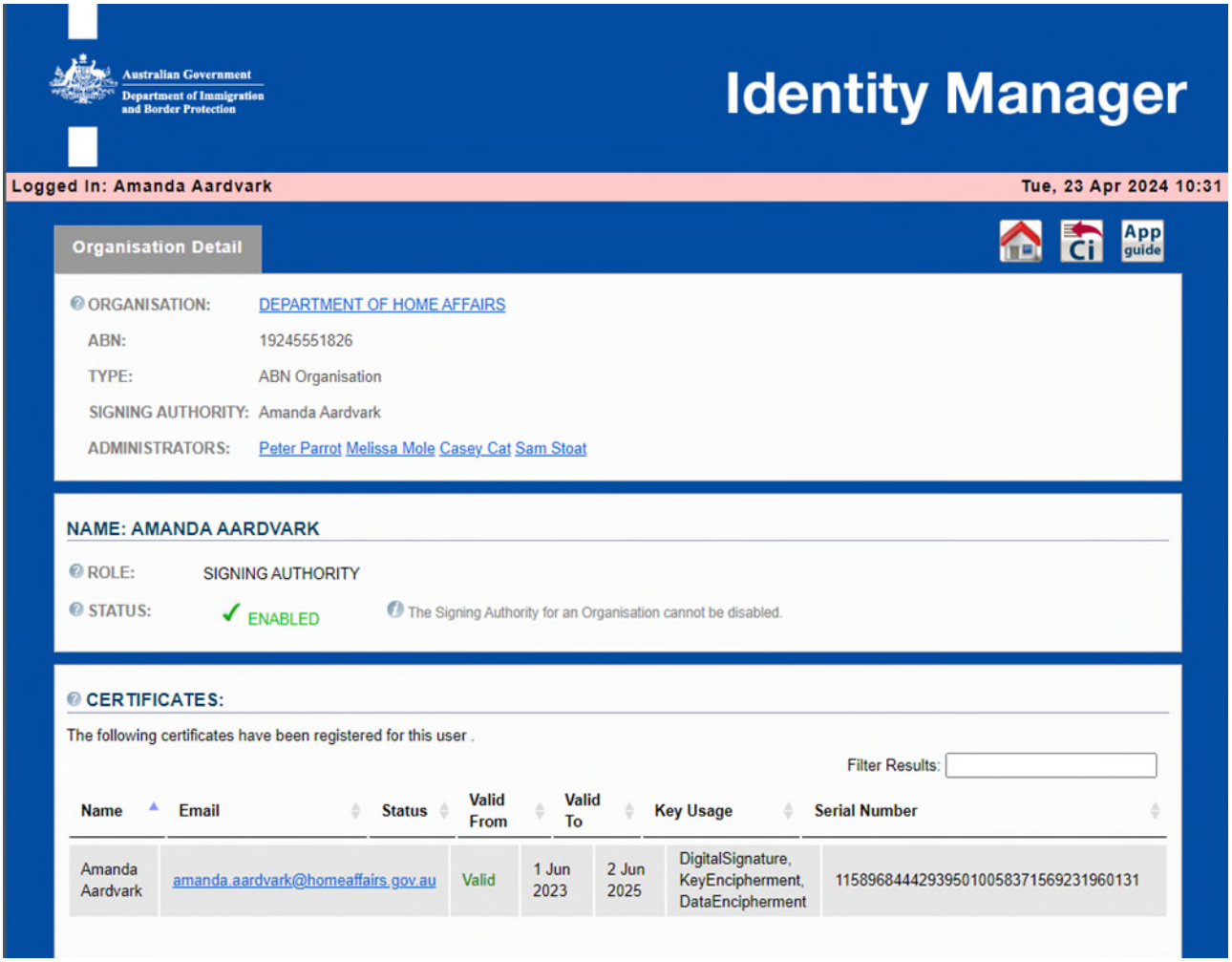

Figure 9: User Details (Signing Authority)

Certificate Details

An identity's Digital Certificate status can be Valid, Expired or Revoked.

Valid – The User is registered in the Identity Manager and has a valid digital certificate registered with The Department.

Expired – The User is registered in the Identity Manager but the user's digital certificate registered with The Department has expired.

Revoked – The User is registered in the Identity Manager but their digital certificate registered with The Department has been revoked through Digicert.

To add a new certificate to your user details

You may wish to add additional Digital Certificates to your own User. This is usually done when your current Digital Certificate is about to expire and you have just purchased a new Digital Certificate.

Adding User Details is done within the Identity Manager application.

Digital Certificates are normally issued to Users as a pfx file that includes private key information. Only the public key should be uploaded as part of registration, so before proceeding ensure you have the public key as a .cer file.

STEP 1. View your User Details.

STEP 2. In the ADD CERTIFICATE form, select the Browse button.

STEP 3. The Choose File to Upload window displays.

STEP 4. Locate and select the .cer file for the Certificate you wish to add to your User.

STEP 5. Select the Open button.

The Choose File to Upload window closes and the file path of the certificate is displayed.

STEP 6. Select the Add Certificate button.

STEP 7. The User Details screen refreshes.

The new Certificate is displayed in the CERTIFICATES pane.

NOTE

Digital Certificates will only be accepted if they are:

- Currently valid,
- Issued by an accepted Certification Authority, and
- Appropriately bound to the Organisation.

Functions Available to All Users Who Have the Administrator Role

To view your organisation details

The Organisation Detail screen allows an Administrator or Signing Authority to view the details of their organisation, including all Users and Devices which have been registered to their Organisation.

STEP 1. Login to the Identity Manager application.

STEP 2. Your Organisation Detail screen is displayed.

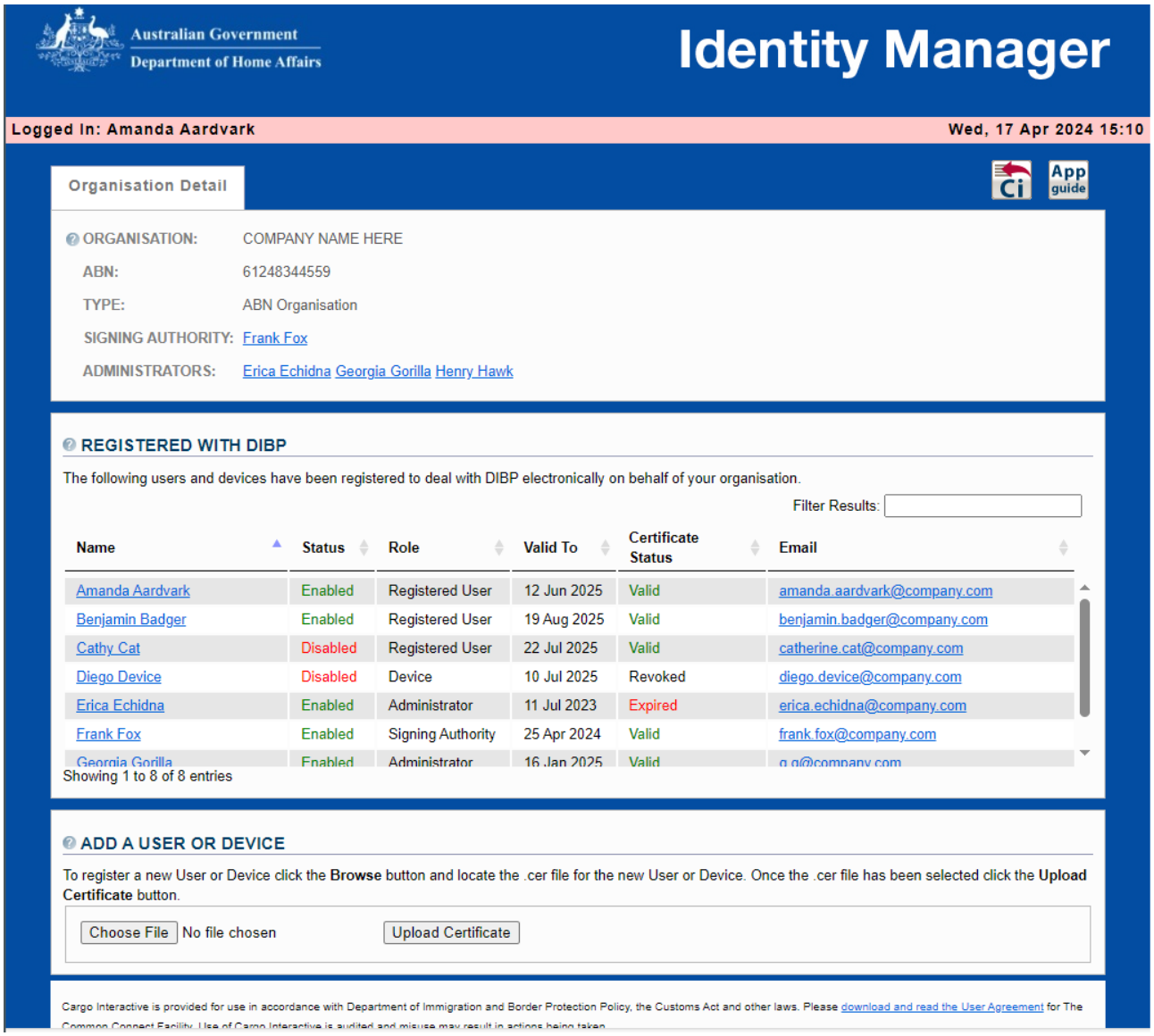

Figure 10: The Organisation Detail Screen

To search for a User or Device

The Organisation Detail screen allows an Administrator to Search all Users and Devices which have been registered to their Organisation.

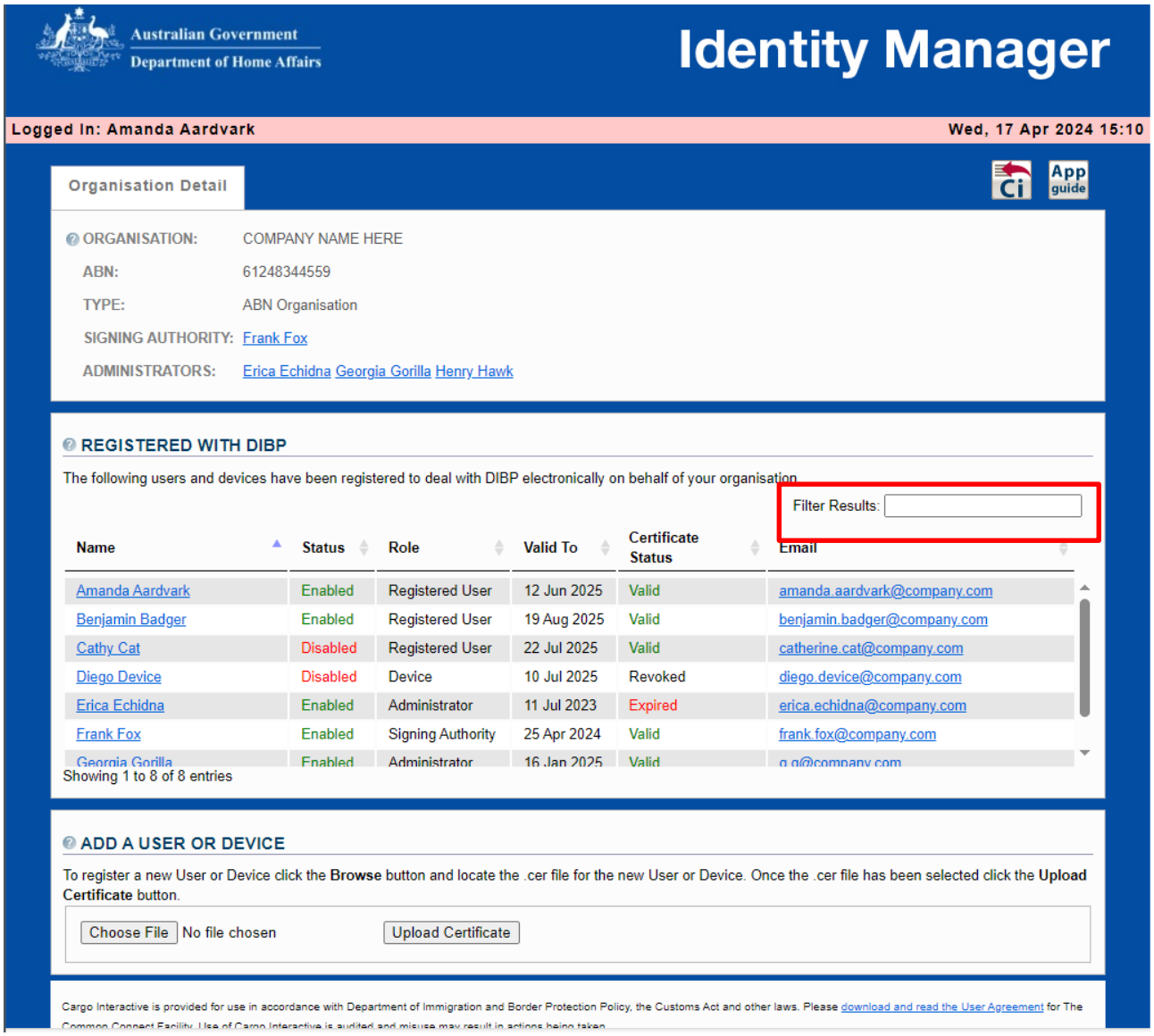

Figure 11: The Organisation Detail Screen (Filter Results highlighted)

STEP 1. View your Organisation Detail.

A list of all Users and Devices registered for the Organisation is displayed in the REGISTERED WITH DIBP pane.

STEP 2. Enter your search criteria in the Filter Results field.

The list of all Users and Devices will automatically filter the list of Users and Devices to show only those entries which match the filter criteria entered.

HINT

To quickly find a User or Device, enter the email address for the User or Device in the Filter Results field.

To add a new user or device

A new User or Device can be added to your Organisation by uploading the corresponding Digital Certificate. Ensure you upload a .cer file with the certificate's public key, not a .pfx file with the private key.

STEP 1. View your Organisation Detail.

STEP 2. In the ADD USER OR DEVICE pane, select the Choose File button.

(Note: some browsers may label this button as "Browse" or some other equivalent.)

The Choose File to Upload window displays.

STEP 3. Locate and select the .cer file for the Certificate for the User or Device you wish to add.

STEP 4. Select the Open button.

The Choose File to Upload window closes and the filepath of the certificate is displayed.

STEP 5. Select the Upload Certificate button.

STEP 6. The screen refreshes and the details of the new User or Device are displayed.

NOTE

Digital Certificates will only be accepted if they are:

- Currently valid,
- Issued by an accepted Certification Authority, and
- Appropriately bound to the Organisation.

To view details of a user

To view the detail of a User who has been registered to represent your Organisation, you will need to locate the User on the Organisation Detail page and select their name which has been linked to their User Details.

STEP 1. View your Organisation Detail.

STEP 2. In the REGISTERED WITH CCF pane, scroll until you see the User.

Use Filter Results if necessary.

The User appears in the list of Users and Devices.

STEP 3. Select the name of the User.

STEP 4. The User Details screen is displayed.

This should be for the User selected in STEP 3.

To view details of a device

To view the detail of a Device which has been registered to represent your Organisation, you will need to locate the Device on the Organisation Detail page and select its name which has been linked to the Device Details.

STEP 1. View your Organisation Detail.

STEP 2. In the REGISTERED WITH CCF pane, scroll until you see the Device.

Use Filter Results if necessary.

The Device appears in the list of Users and Devices.

STEP 3. Select the name of the Device.

STEP 4. The Device Details screen is displayed.

This should be for the Device selected in STEP 3.

To disable a user or device

When a new User or Device is added to Identity Manager they are automatically enabled. This means that they can deal electronically with The Department. In some circumstances, for example where an employee is on extended leave, an Organisation may wish to temporarily disable the identity for a User. This does not cancel the registration or revoke any Digital Certificates. While a User/Device is disabled they cannot deal with The Department electronically.

STEP 1. View the User/Device Details of the User/Device to be disabled.

STEP 2. In the User/Device Details pane, enter the reason for disabling this User/Device.

STEP 3. Select the DISABLE button.

STEP 4. The User/Device Details page will refresh.

The Status field will display the User/Device as DISABLED.

NOTE

If a User is disabled while they have an active session with Cargo Interactive, their session will not be terminated. The next time they attempt to authenticate to the Cargo Interactive their access will be denied.

WARNING

- A Signing Authority can NEVER be disabled.
- Only a Signing Authority can disable an Administrator.

To enable a user or device

An identity's login status can be enabled, pending, incomplete or disabled.

Enabled - An identity with an enabled login status has successfully registered with Customs using a current, valid certificate.

Disabled - While a User/Device is disabled they cannot deal with The Department electronically. A disabled User/Device can be re-enabled by an Administrator at any time using this function.

A disabled identity cannot:

- Auto rollover their certificate;
- Login to Cargo Interactive;
- Submit EDI transactions; or
- Be assigned the Signing Authority or Administrator roles for their organisation.

If a Registered User is disabled while they have an active session with the Gateway, their session will not be terminated within the Gateway. The next time they attempt to authenticate to the Gateway the session will be denied.

Pending - An identity with a pending login status has registered a valid certificate with Cargo Interactive, but an administrator for their organisation still needs to nominate which Cargo Interactive applications they can access on behalf of their organisation. Identities with a pending login status will remain in the Gateway directory for 7 days. They have NO access to applications until their login status changes to "enabled".

This status is assigned when an identity does not fully complete the process of registering with Cargo Interactive. In this instance the Signing Authority for the organisation may be able to assist by sending a new activation email to the identity so that they can complete the registration process.

NOTE

When a new User or Device is added to Identity Manager they are automatically enabled. This means that they can deal electronically with The Department. In some circumstances, for example where an employee is on extended leave, an Organisation may wish to temporarily disable the login for a User. This does not cancel the registration or revoke Digital Certificates.

To re-enable a User that had previously been disabled:

STEP 1. View the User/Device Details of the User/Device to be enabled.

STEP 2. In the User/Device Details pane, select the ENABLE button.

STEP 3. The User/Device Details page will refresh, the Status field will display the User/Device as ENABLED.

To add a new certificate to an existing user

Digital Certificates have a lifespan of 2 years and need to be replaced accordingly. When this happens the new Digital Certificates need to be registered against the User in the Identity Manager application. This function is used to add a new Digital Certificate to an existing User.

STEP 1. View the User Details for the User who has a new Digital Certificate.

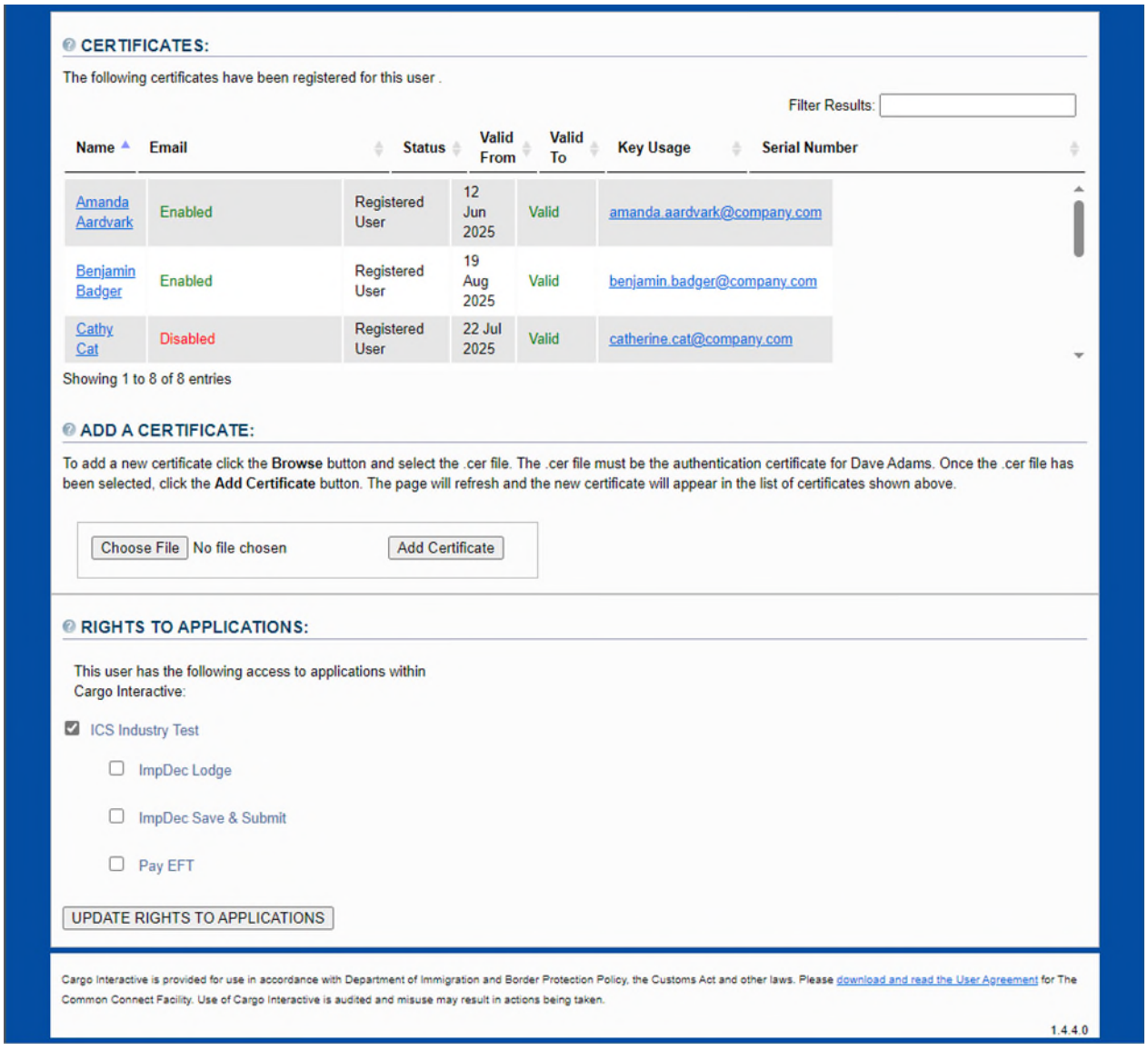

Figure 12: User Details Screen

STEP 2. In the ADD CERTIFICATE form, select the Choose File button.

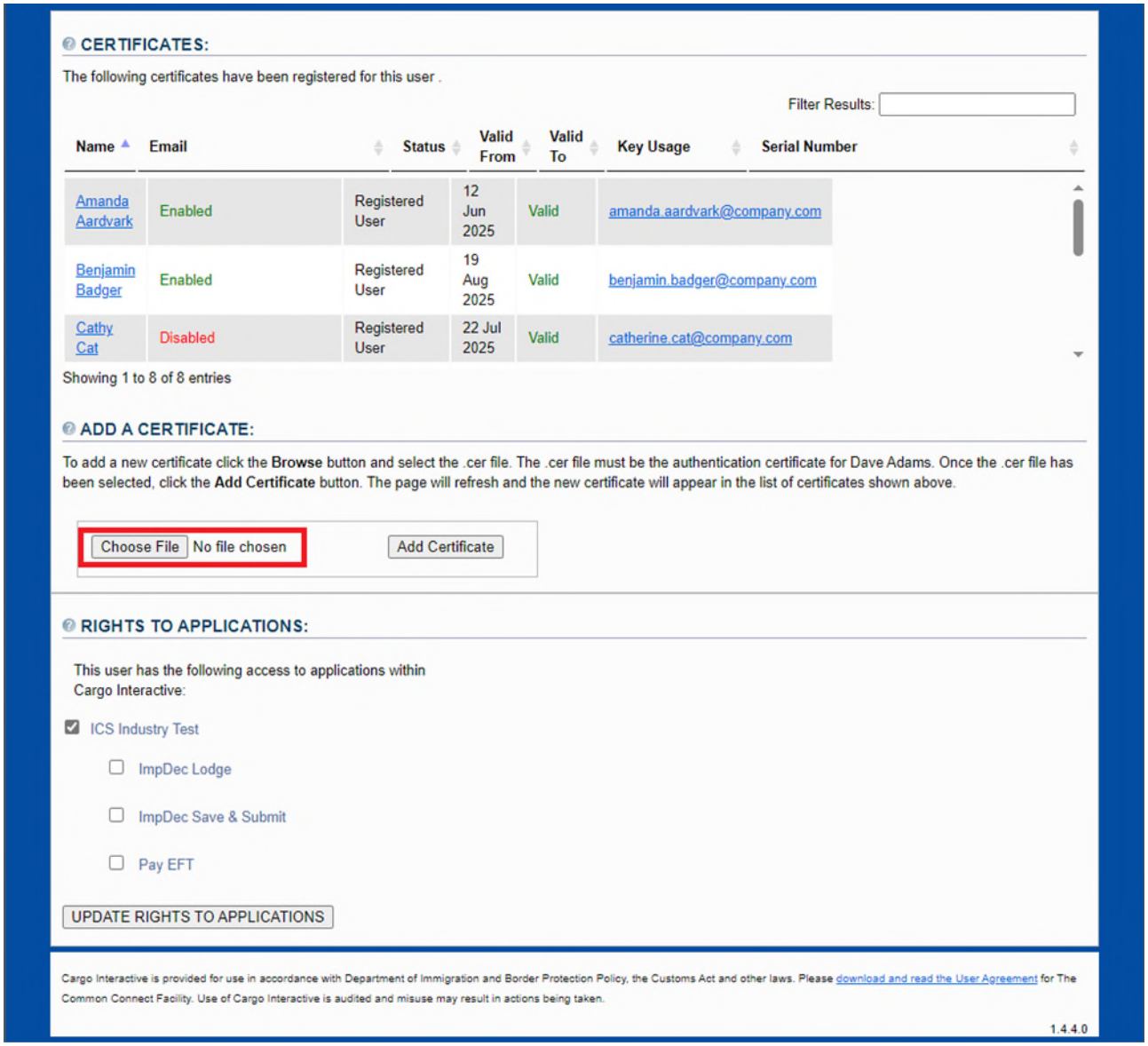

Figure 13: User Details Screen (Choose File button highlighted)

STEP 3. The Choose File to Upload window displays.

STEP 4. Locate and select the .cer file for the Signing Certificate you wish to add to your User.

STEP 5. Select the Open button.

The Choose File to Upload window closes and the filepath appears in the Add Certificate form.

STEP 6. Select the Add Certificate button.

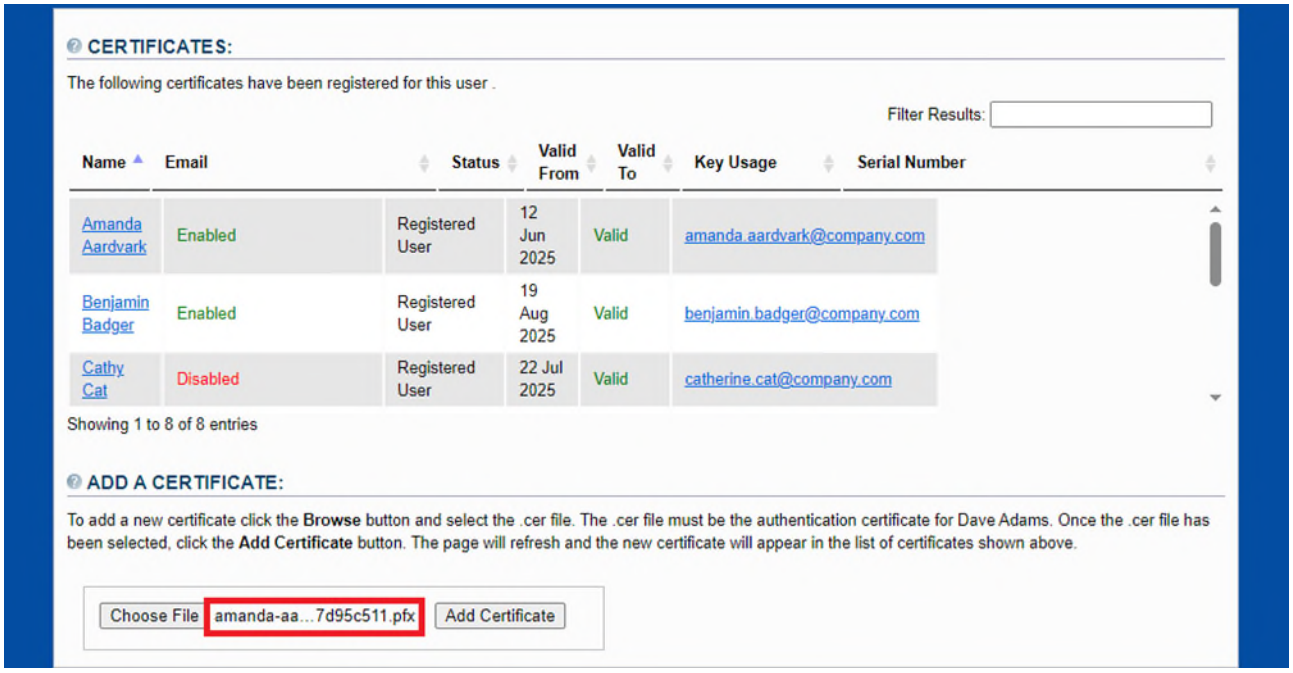

Figure 14: User Details Screen (Certificate Filename highlighted)

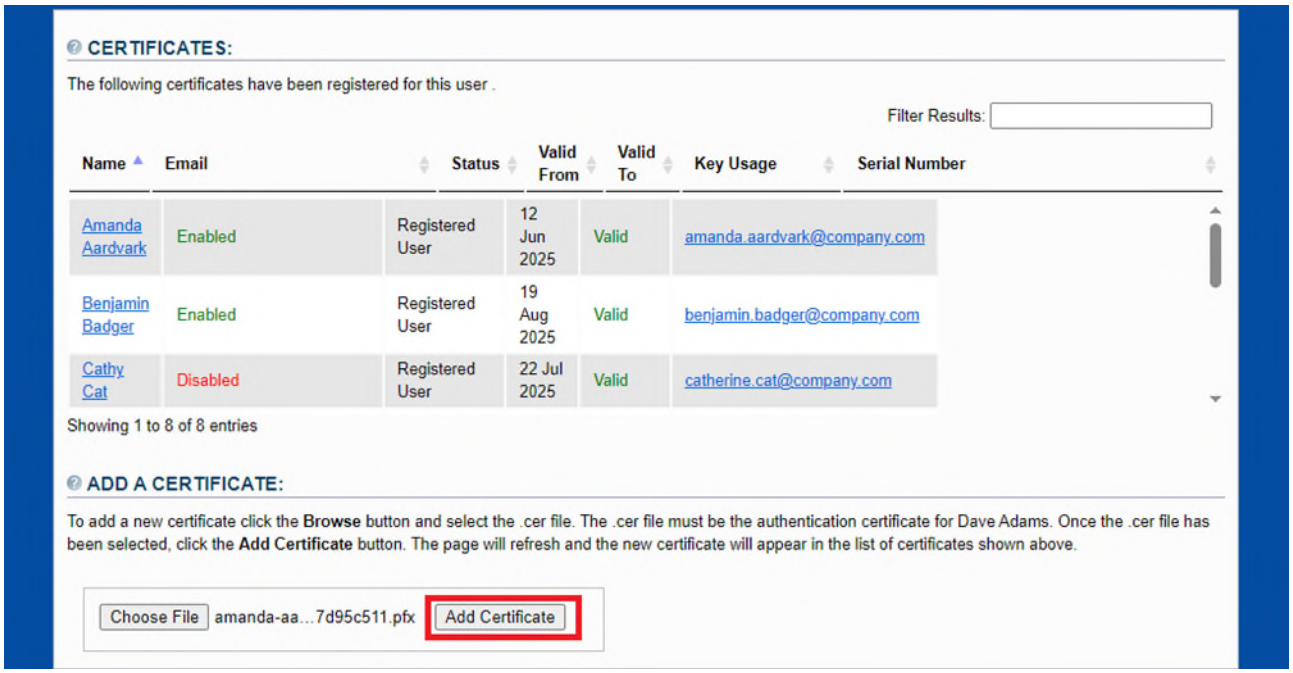

Figure 15: User Details Screen (Choose File button highlighted)

STEP 7. The User Details screen refreshes.

The new Signing Certificate is displayed in the CERTIFICATES pane.

NOTE

Digital Certificates will only be accepted if they are:

- Currently valid,
- Issued by an accepted Certification Authority, and
- Appropriately bound to the Organisation.

To add a new certificate to an existing device

Digital Certificates have a lifespan of 2 years and need to be replaced accordingly. When this happens the new Digital Certificates need to be registered against the Device in the Identity Manager application. This function is used to add a new Digital Certificate to an existing Device.

STEP 1. View the Device Details for the Device which has a new Digital Certificate.

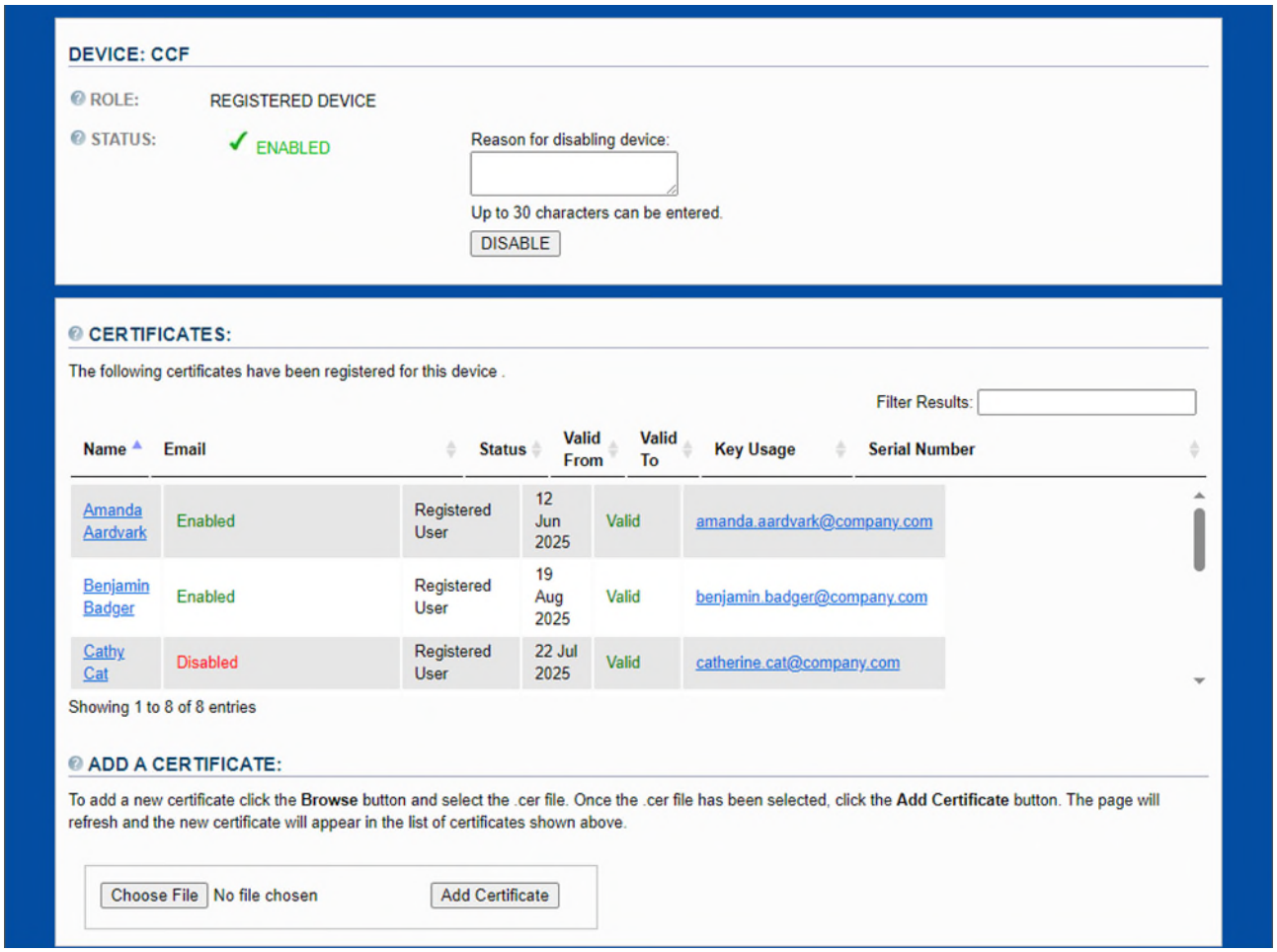

Figure 16: The Add Certificate to Device Form

STEP 2. In the ADD CERTIFICATE form, select the Choose File button.

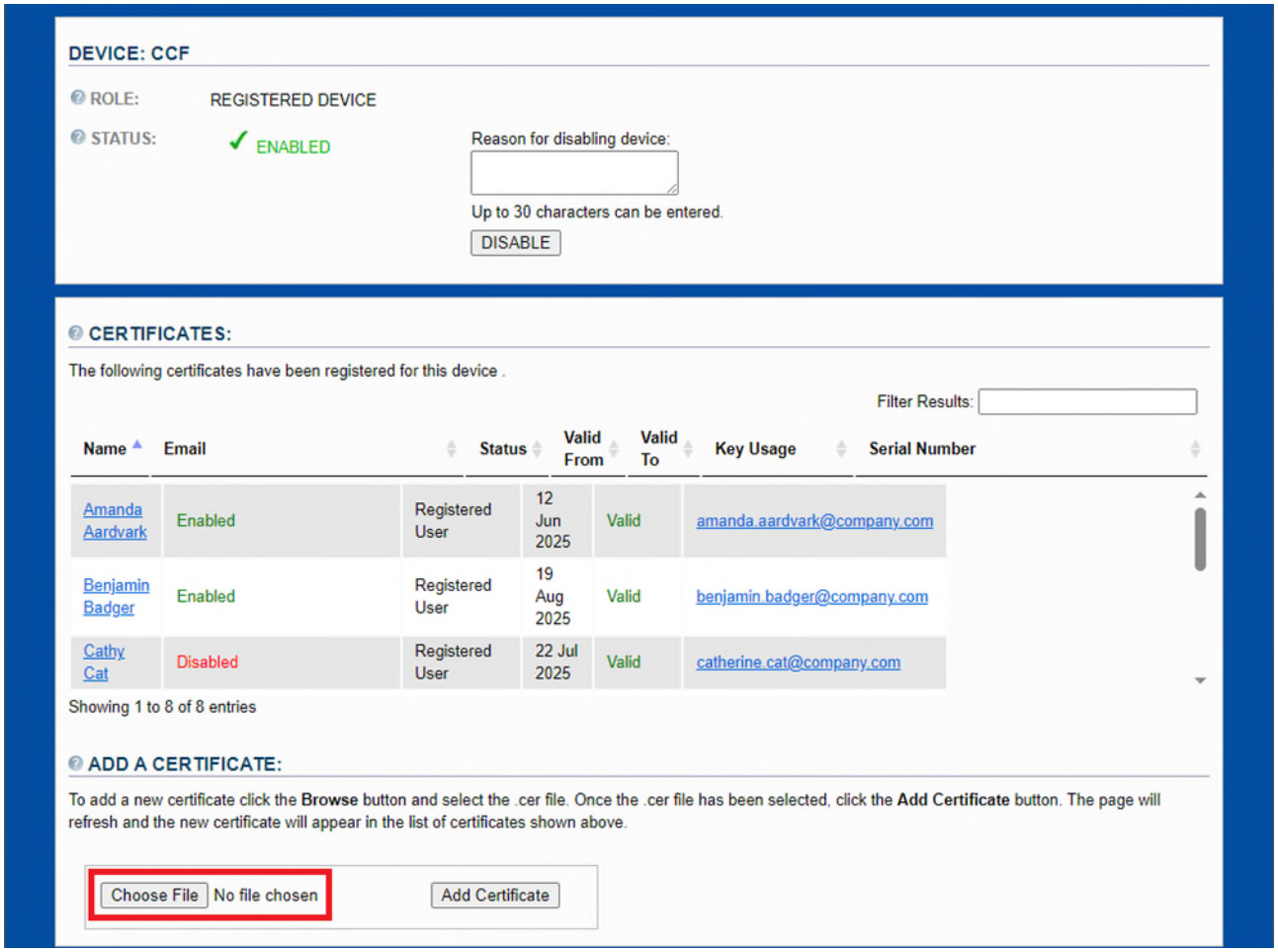

Figure 17: The Add Certificate to Device Form (Choose File highlighted)

STEP 3. The Choose File to Upload window displays.

STEP 4. Locate and select the .cer file for the Certificate you wish to add to your Device.

STEP 5. Select the Open button.

The Choose File to Upload window closes and the filepath of the selected certificate appears in the Add Certificate form.

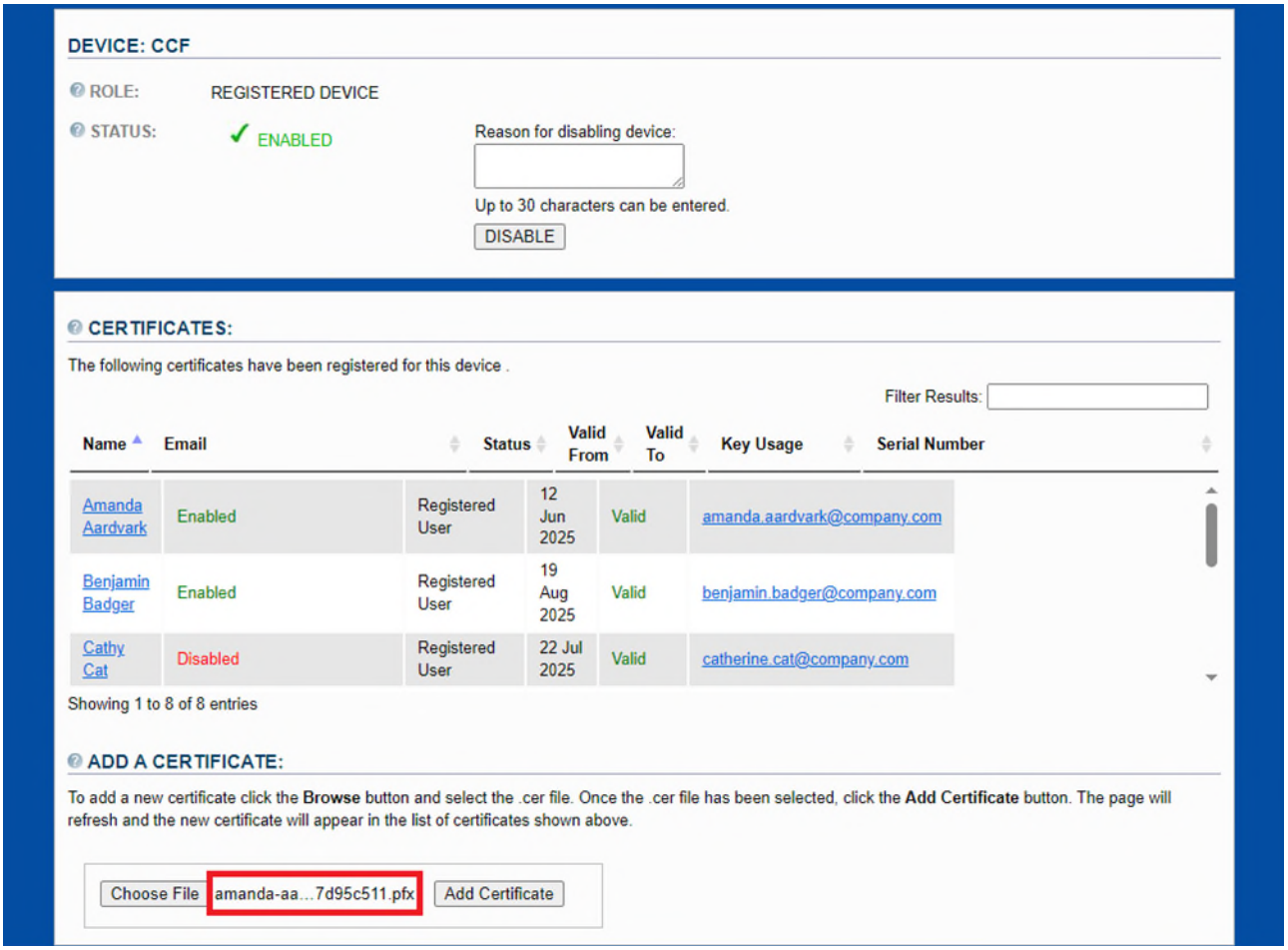

Figure 18: The Add Certificate to Device Form (Filename highlighted)

STEP 6. Select the Add Certificate button.

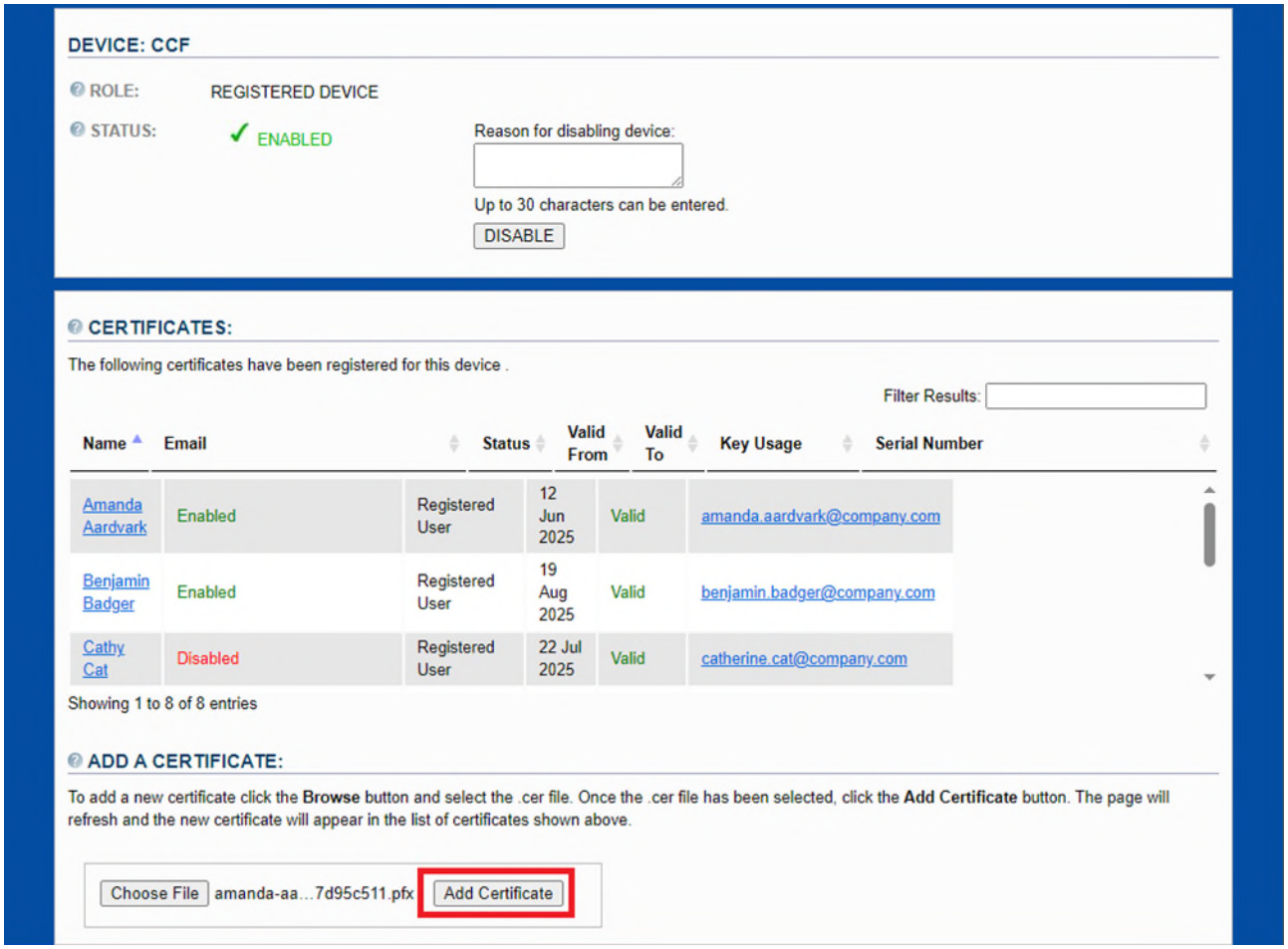

Figure 19: The Add Certificate to Device Form (Add Certificate Button highlighted)

STEP 7. The Device Details screen refreshes.

The new Certificate is displayed in the CERTIFICATES pane.

To grant a user rights to access applications

The Department grants Organisations the rights to access certain Cargo Interactive applications (for example the Integrated Cargo System (ICS)). When a User is created however, they are only granted the base Rights to Access these applications. Administrators can then grant (or remove) certain elevated Rights to Applications.

For example, multiple Users within an Organisation may require access to ICS, but only one or two Users would need the specific elevated right to Amend the EDI site information for the Organisation. The Administrator would therefore only grant that AMEND EDI SITE right to those specific Users.

STEP 1. View the User Details for the User whose Rights to Access Applications are to be modified.

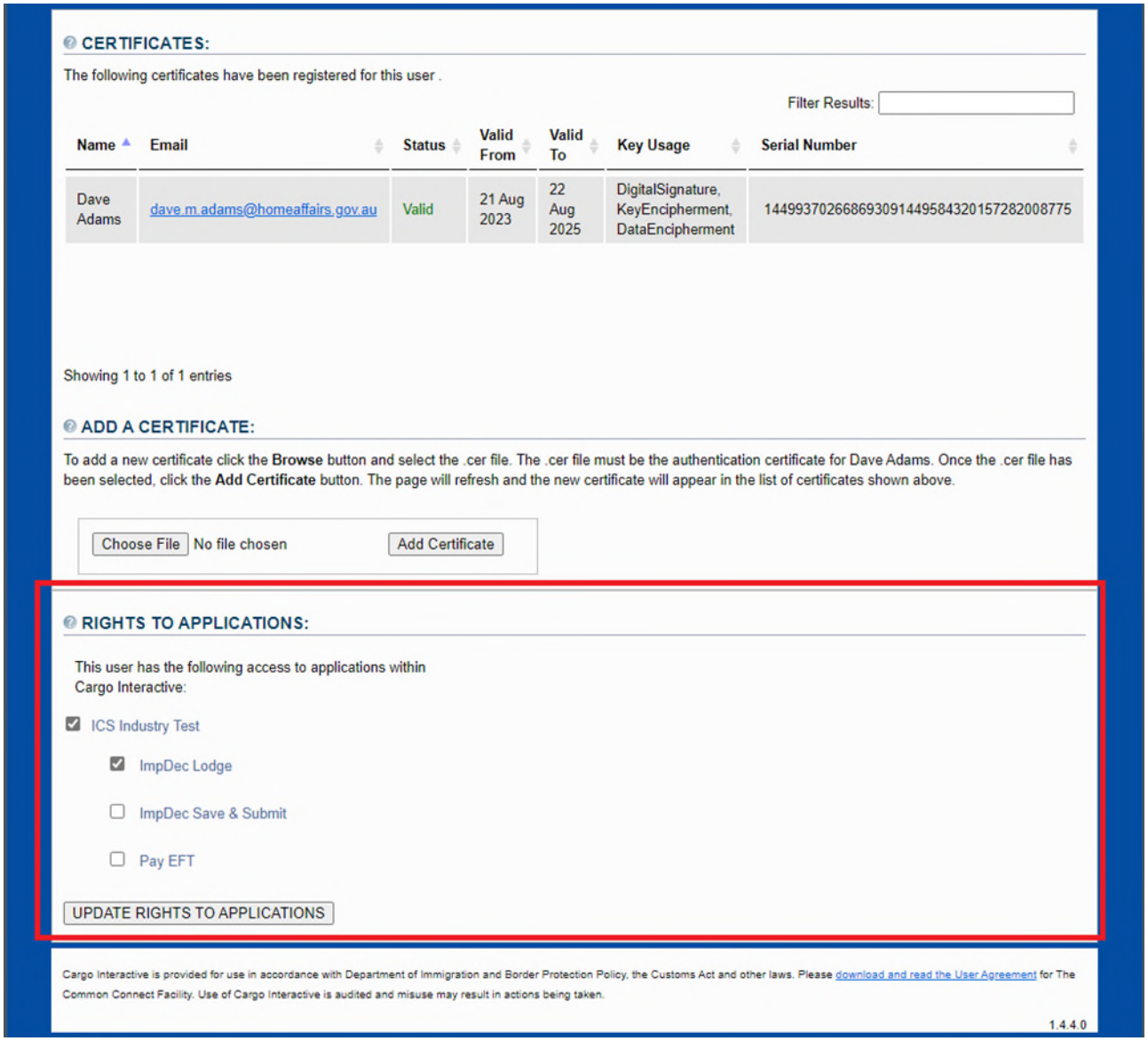

Figure 20: The Rights to Access Applications screen (Rights To Applications pane highlighted)

STEP 2. In the RIGHTS TO APPLICATIONS pane, toggle the check boxes to reflect the Rights to Access Applications for the User.

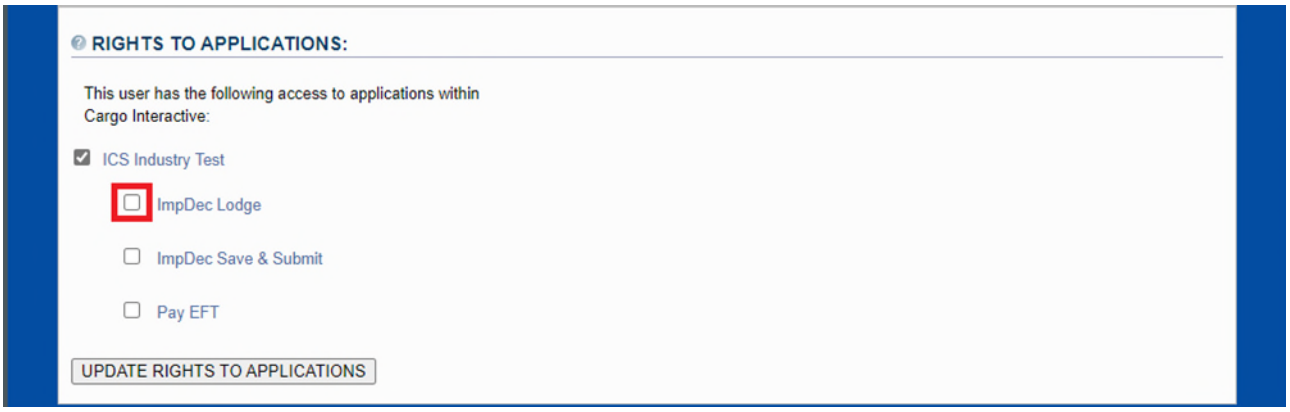

Figure 21: The Rights to Applications pane (Sample checkbox highlighted)

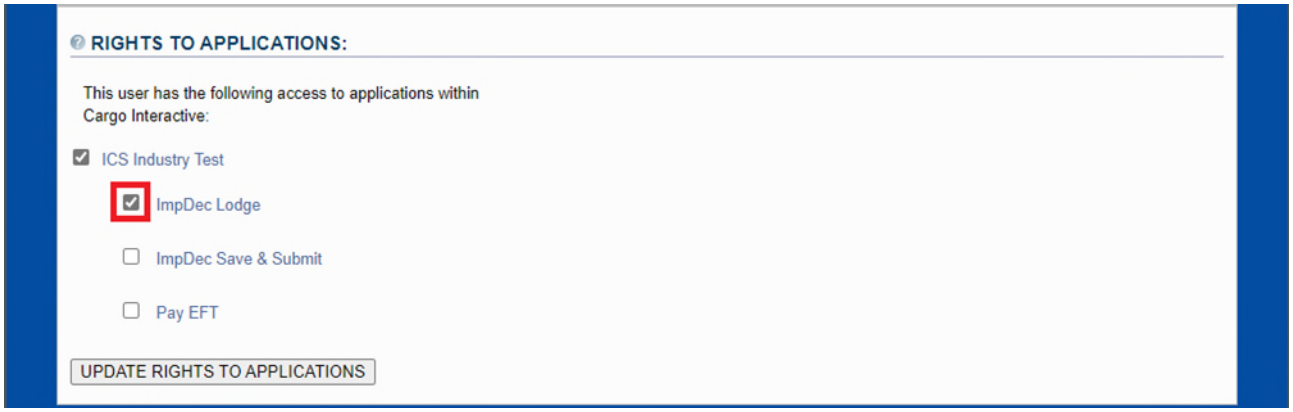

Figure 22: The Rights to Applications pane (Checked checkbox highlighted)

STEP 3. Select the UPDATE RIGHTS TO APPLICATIONS button.

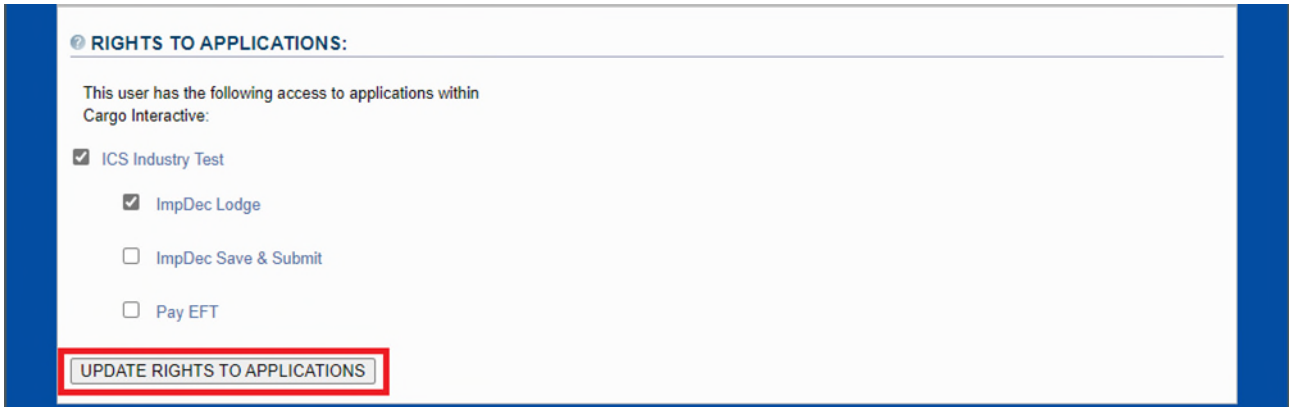

Figure 23: The Rights to Applications pane (Update Rights to Applications Button highlighted)

STEP 4. The User Details screen is refreshed displaying the updated Rights to Applications.

To enable a user who is pending registration

When an unregistered User belonging to an Organisation attempts to login to Cargo Interactive, an application for registration is automatically created on their behalf.

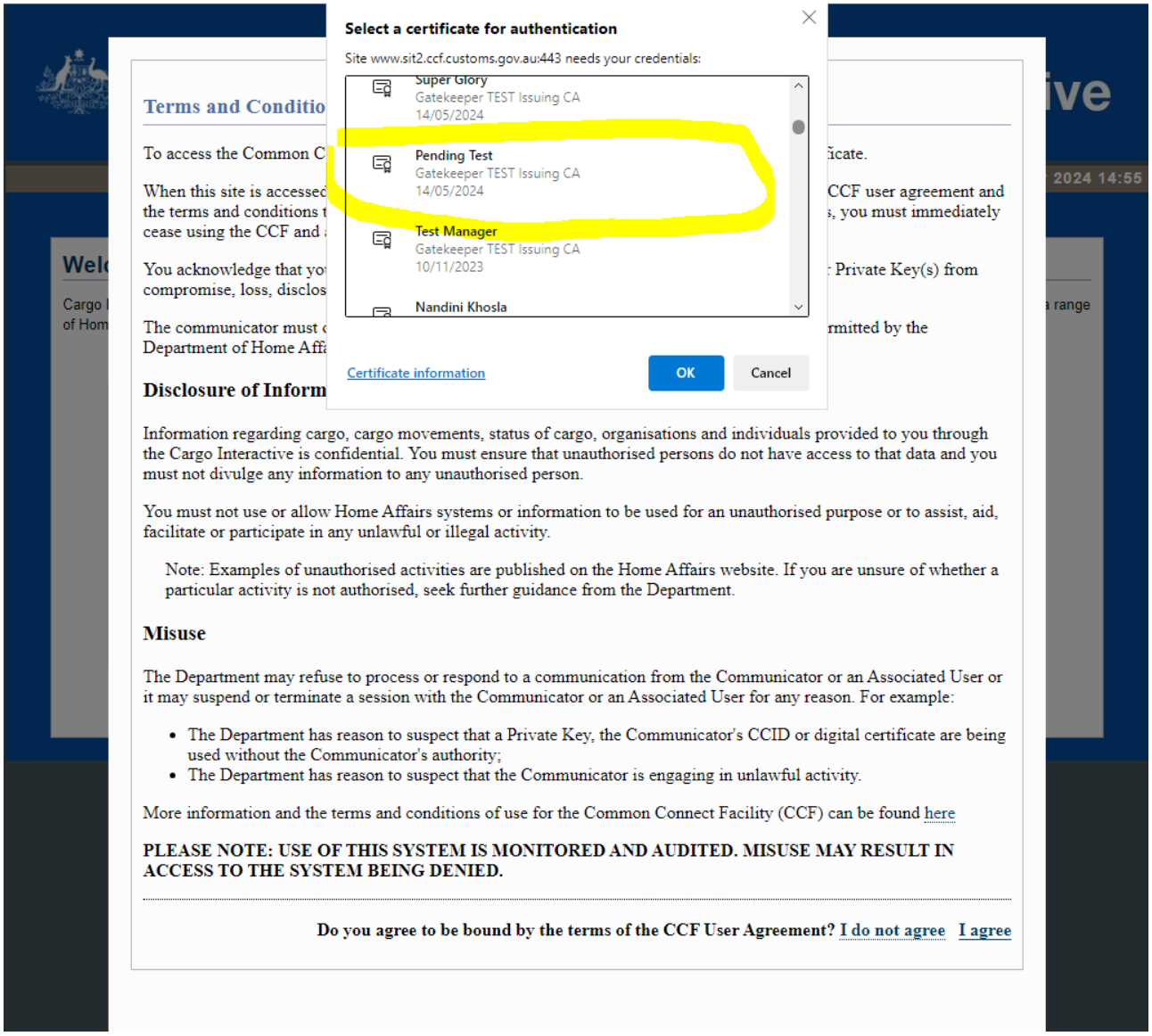

Figure 24: Selecting A Certificate Pending Registration

They are not enabled and cannot deal with Customs electronically. The unregistered User must first be enabled by an Administrator.

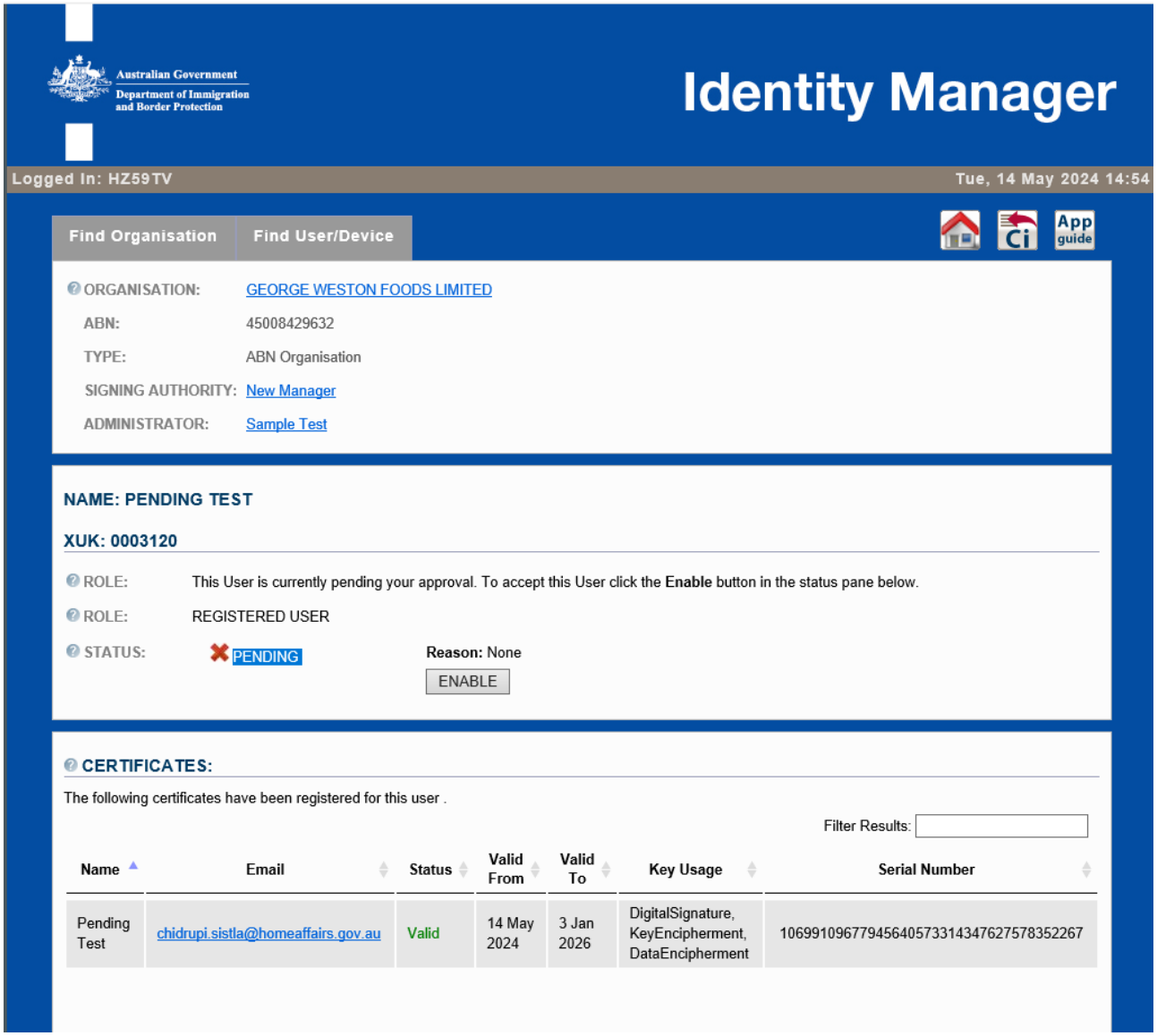

Figure 25: User Information For User Who Is Pending Registration

Note that attempting to log in with such a user will result in a Permission Denied.

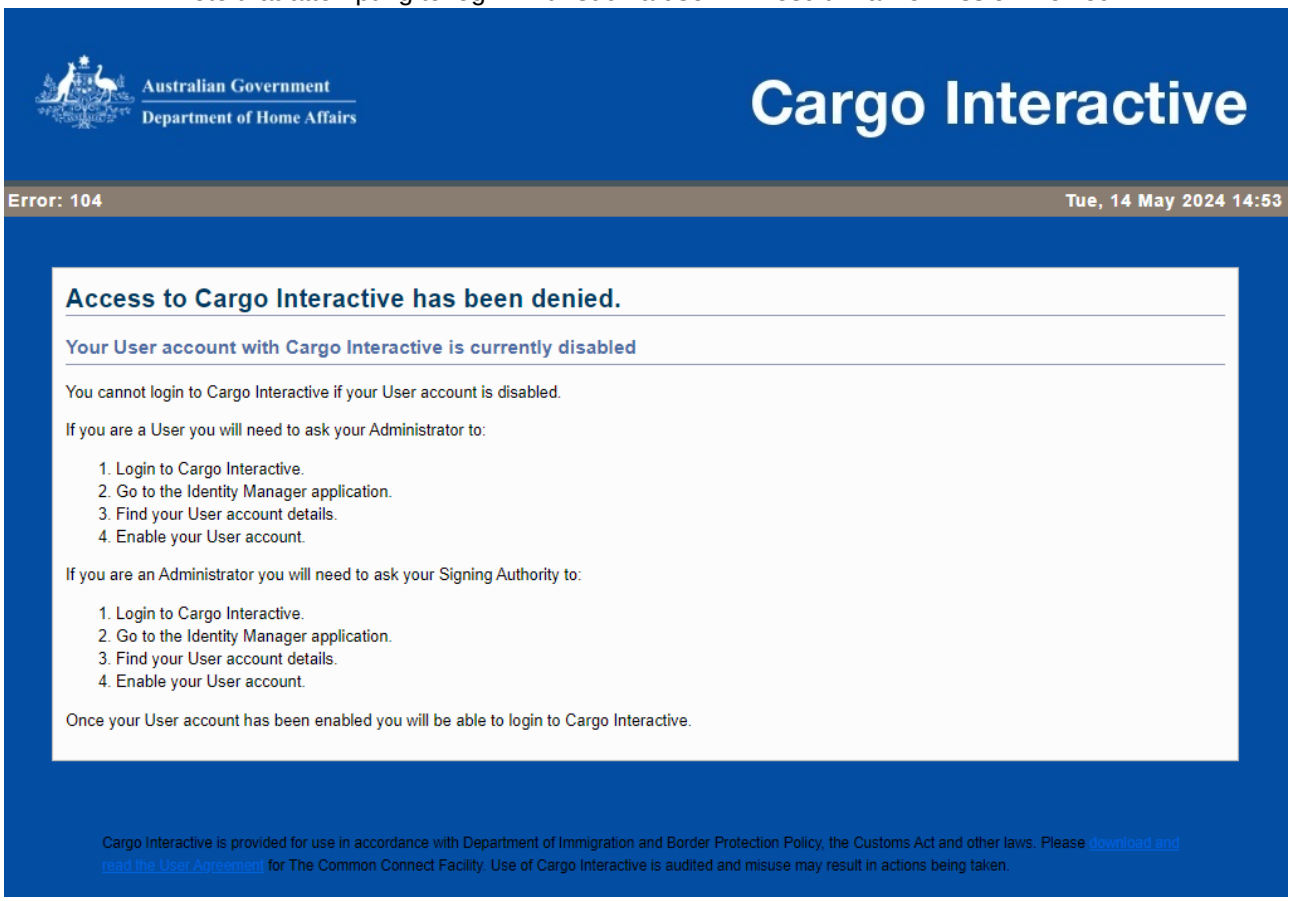

Figure 26: Access Denied When User Account Is Disabled

For Administrators and Signing Authorities, the unregistered User is displayed in the list of Registered with The Department for the Organisation with a status of “Pending”.

If the user is not displayed because the list is too long, use the Filter Results option to find them. To do this you can enter any of the following details:

- Registered Users first name
- Registered Users Surname
- Device name
- Status
- Identity Type
- Email address

Once the correct user has been identified, proceed.

STEP 1. View the User Details of the PENDING User.

STEP 2. Click on the ENABLE button to enable the PENDING User.

STEP 3. The User Details screen is refreshed displaying the User as a REGISTERED USER with an ENABLED Status.

Functions Available to Users Who Are the Signing Authority For Their Organisation

To grant a user administrative privileges

A Signing Authority can grant a Registered User Administrator privileges which allows them to perform all functions outlined in the section of this User Guide entitled, “Functions Available to All Users Who Have the Administrator Role”.

STEP 1. View the User Details of the User to be granted Administrative privileges.

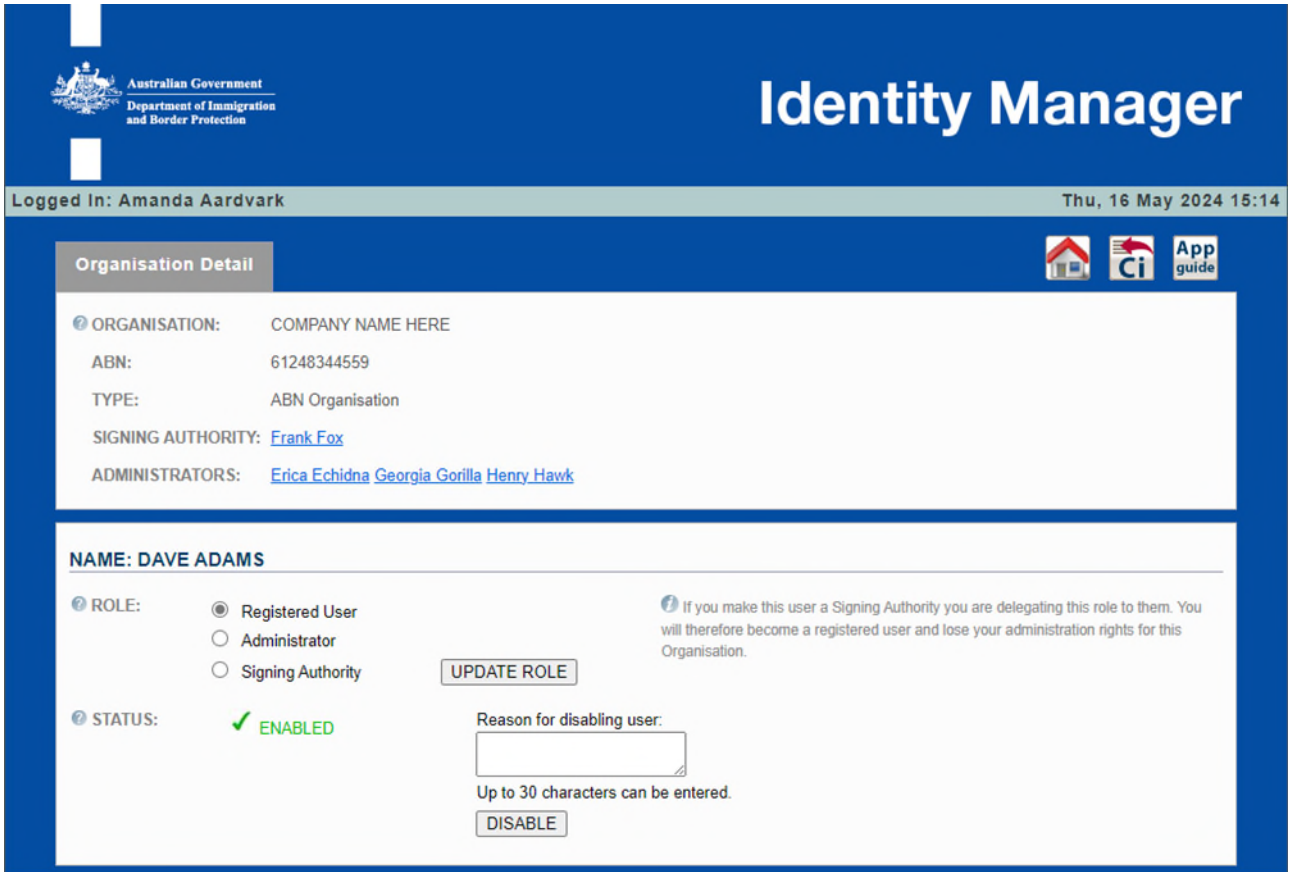

Figure 27: User Details of User To Be Granted Administrative Privileges

STEP 2. In the Role field, select the ADMINISTRATOR radio button.

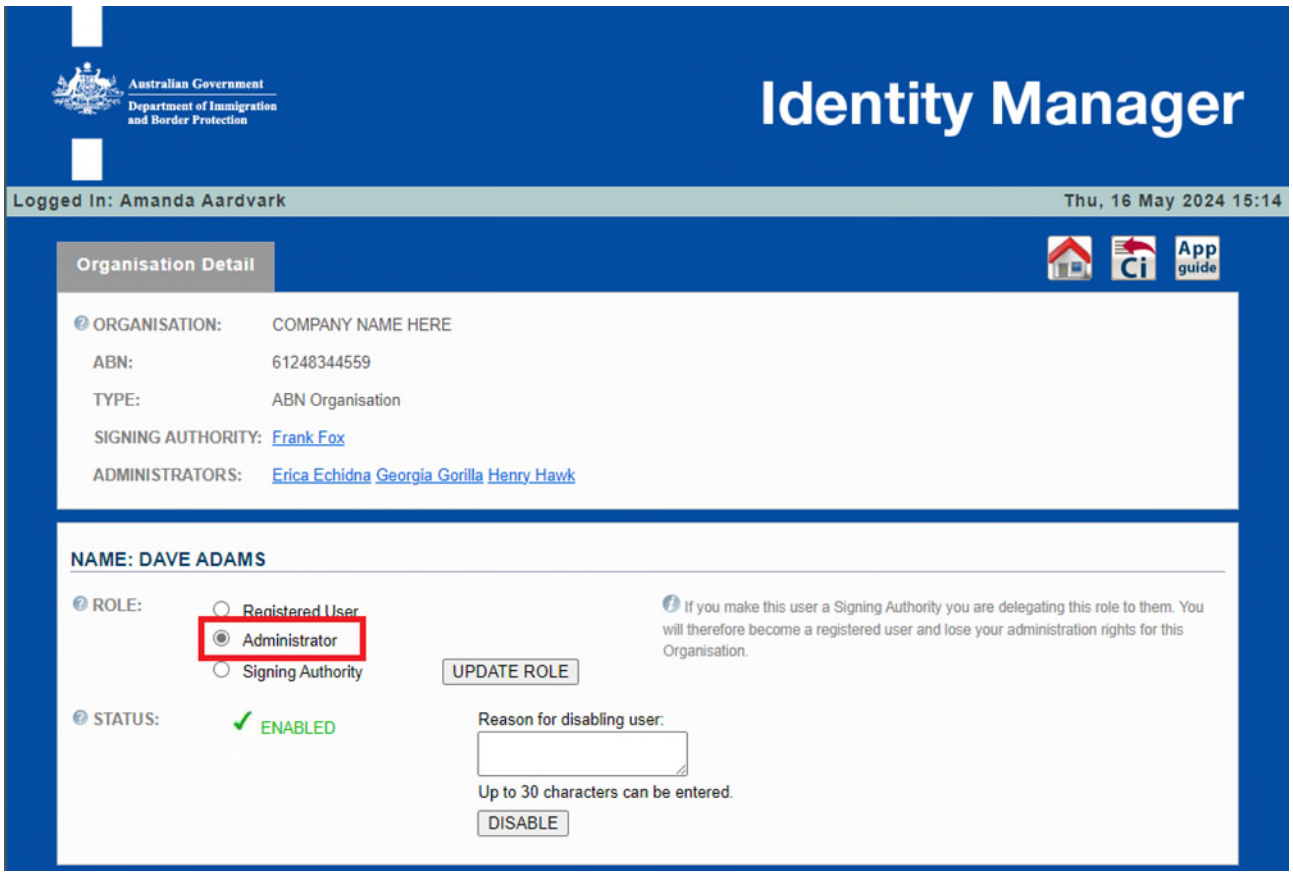

Figure 28: User Details of User To Be Granted Administrative Privileges (Administrator highlighted)

STEP 3. Select the UPDATE ROLE button.

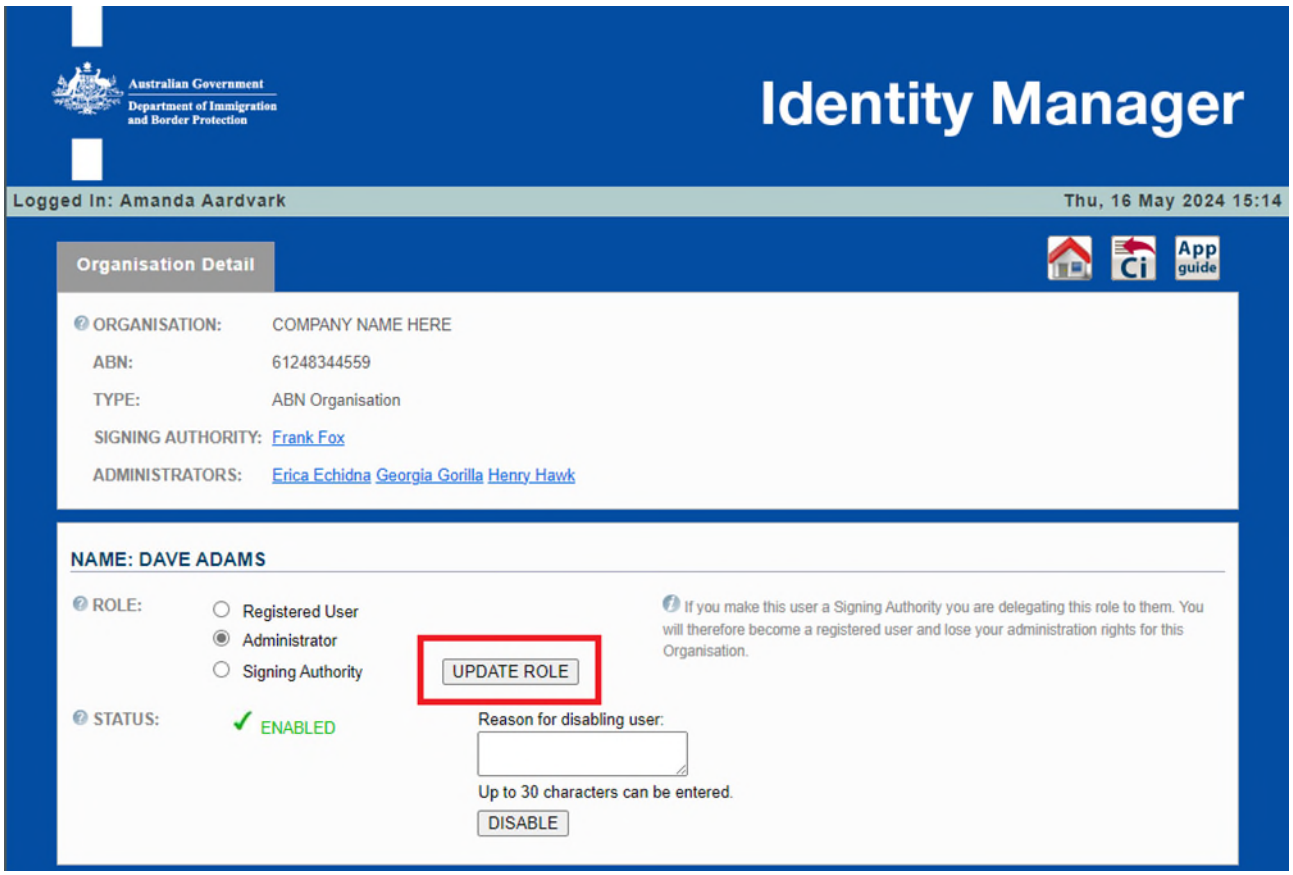

Figure 29: User Details of User To Be Granted Administrative Privileges (Update Role Button highlighted)

STEP 4. The User Details page will refresh, the Role field will display the User as an ADMINISTRATOR.

WARNING

Only Users who currently have a **STATUS** of **ENABLED** can be granted Administrative privileges.

To remove administrative privileges from a user

A Signing Authority can remove Administrator privileges from a Registered User at any time.

> **NOTE**
>
> A Signing Authority can assign their responsibility as a Signing Authority to another Registered User for the Organisation. Once done, the current Signing Authority will LOSE ALL SPECIAL PRIVILEGES and only be recognised by Cargo Interactive as a REGISTERED USER for their Organisation. The new Signing Authority will gain access to all functions.
>
> The Signing Authority can also remove a user from Administrator privileges at any time.

STEP 1. View the User Details of the User that will have Administrative privileges removed.

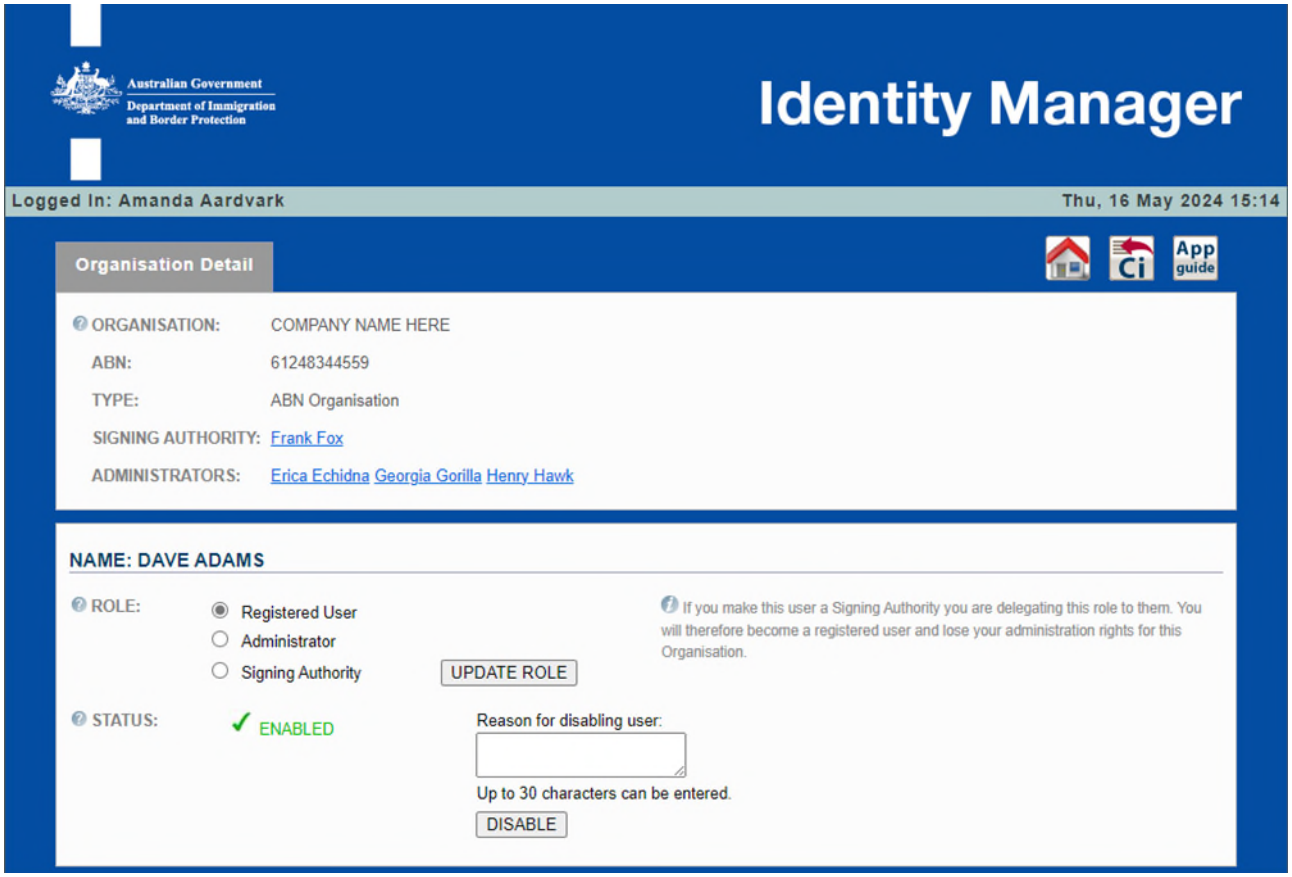

Figure 30: User Details of User To Have Administrative Privileges Removed

STEP 2. In the Role field, select the REGISTERED USER radio button.

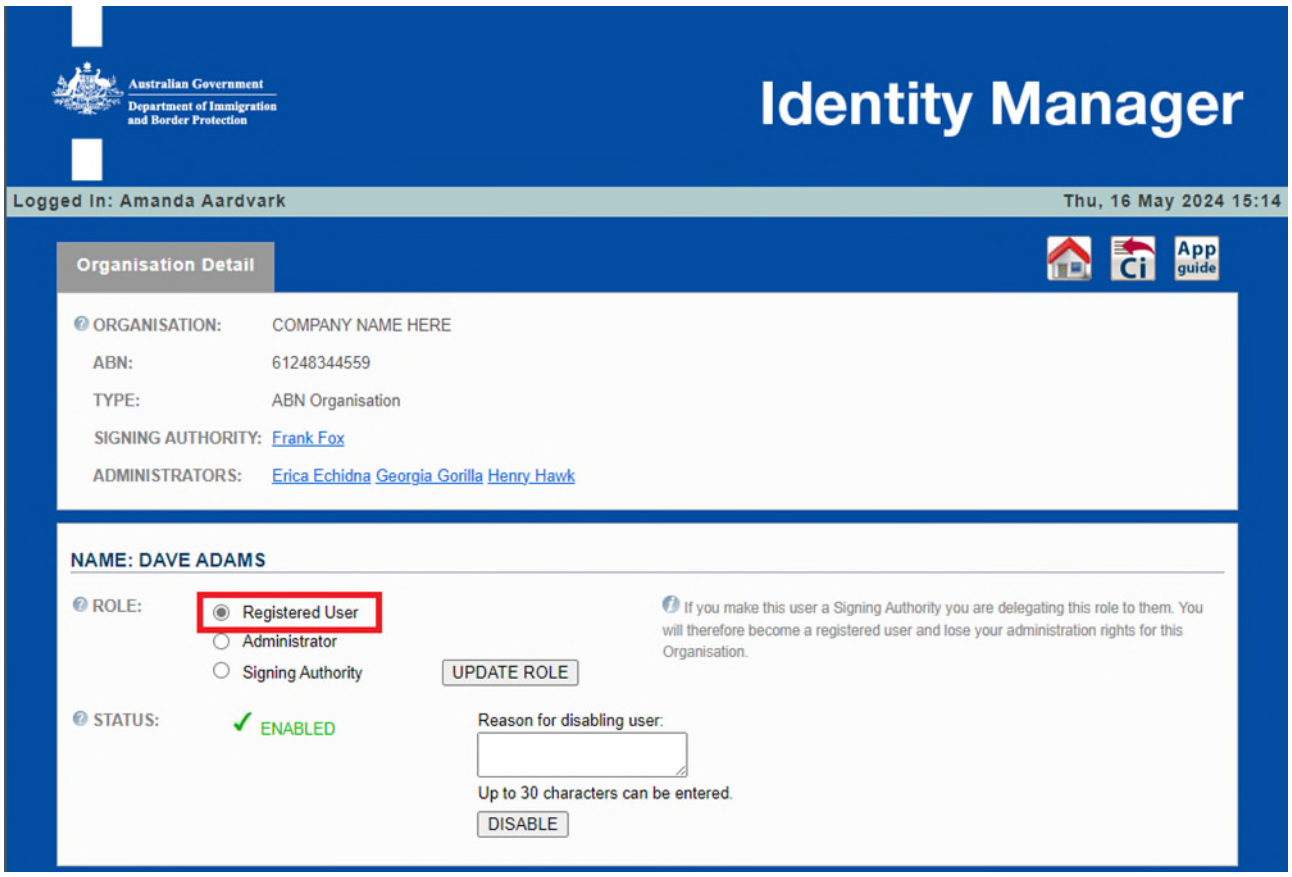

Figure 31: User Details of User To Have Administrative Privileges Removed (Registered User highlighted)

STEP 3. Select the UPDATE ROLE button.

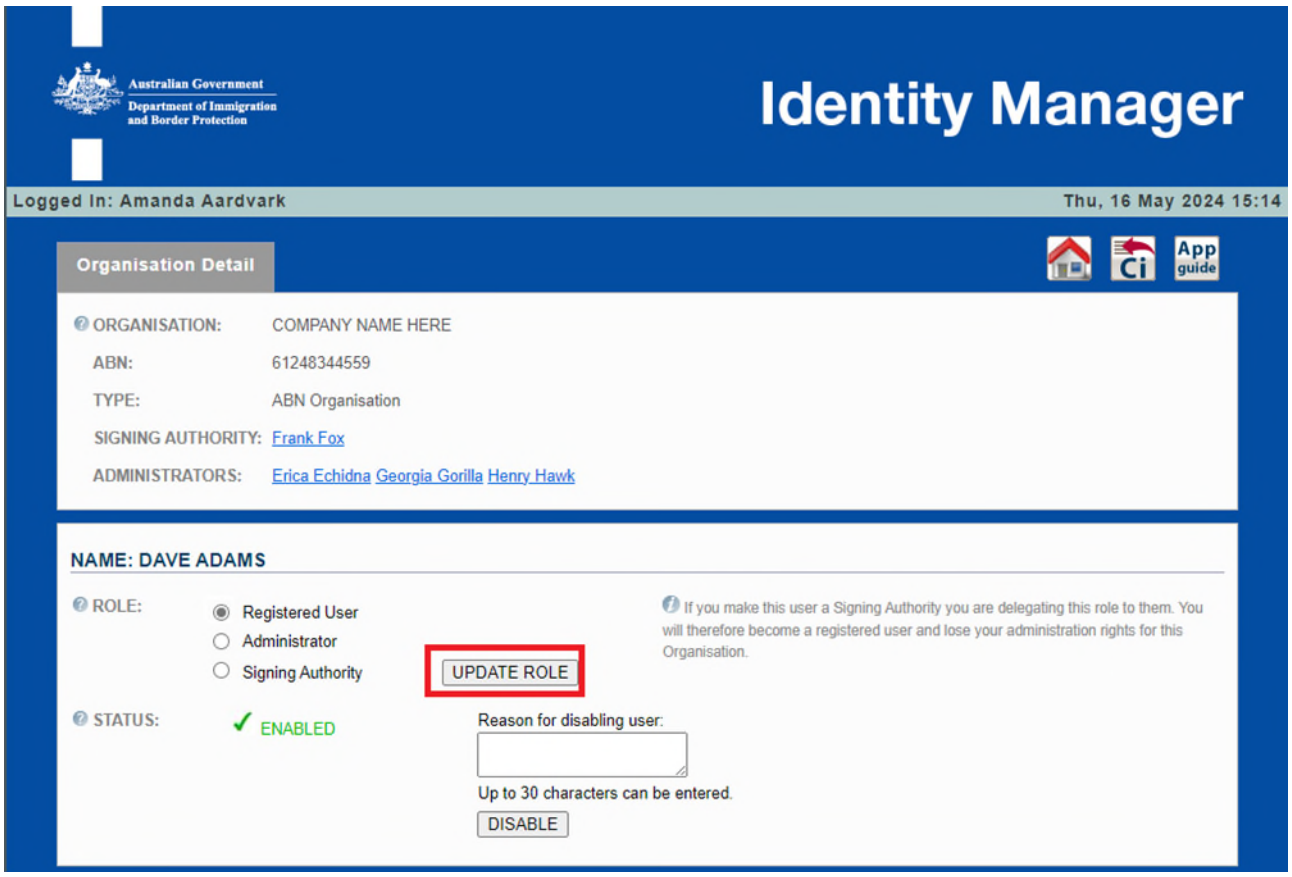

Figure 32: User Details of User To Have Administrative Privileges Removed (Update Role Button highlighted)

STEP 4. The User Details page will refresh, the Role field will display the User as REGISTERED USER.

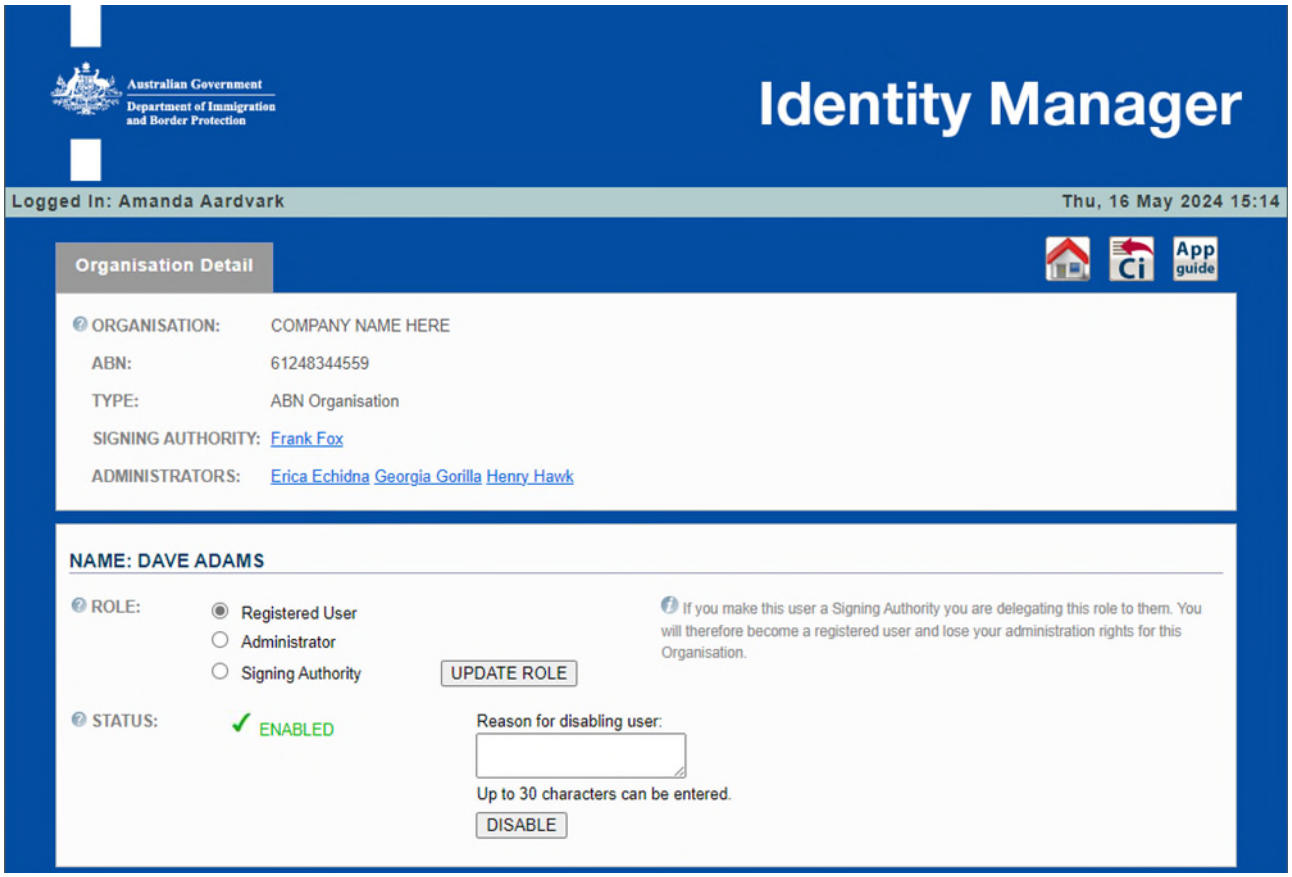

Figure 33: User Details of User To Have Administrative Privileges Removed

To assign signing authority rights to another user

A Signing Authority can assign their responsibility as a Signing Authority to another Registered User for the Organisation. Once done, the current Signing Authority will LOSE ALL SIGNING AUTHORITY PRIVILEGES and only be recognised by The Department as a REGISTERED USER for their Organisation.

WARNING

There can only be **ONE SIGNING AUTHORITY** at any time for each Organisation. When a Signing Authority grants this role to another user they **IMMEDIATELY LOSE** all associated privileges.

STEP 1. View the User Details of the User to be granted the Signing Authority role for the Organisation.

If the user is not displayed because the list is to long use the Filter Results option to find them. To do this you can enter any of the following details and the results will be filtered as you type:

- Registered Users first name
- Registered Users Surname
- Device name
- Status
- Identity Type
- Email address

STEP 2. In the Role field, select the SIGNING AUTHORITY radio button.

STEP 3. Select the UPDATE ROLE button.

STEP 4. The User Details page will refresh.

The current User will be made into a REGISTERED USER and the User Details page displayed will be for the current User.

WARNING

Only Users who currently have a **STATUS** of **ENABLED** can be granted the Signing Authority role.

NOTE

If Registered User is currently logged on they will not see the benefits of the new privileges until they re-authenticate (log off and on again).

Terminology

Key Terms

The meaning of key terms used within this User Guide are defined below.

Term	Meaning
Administrator	A User who has been registered to deal electronically with The Department on behalf of an Organisation, and has the additional responsibility of being able to register and maintain other Users and Devices for that Organisation.
Cargo Interactive	Cargo Interactive is the gateway to the Department of Home Affairs ("The Department") online services facility commonly called the Customs Connect Facility (CCF). This facility provides online access to a range of The Department's cargo-related business applications. Before you can login you must be registered to deal electronically with The Department.
Digital Certificate	A Gatekeeper compliant PKI digital certificate issued by Digicert is required to deal with The Department electronically.
Device	See Registered Device.
Enabled	A status attributed to a User or Device when they are currently authorised by an Organisation to deal electronically with The Department.
Disabled	A status attributed to a User or Device when they are NOT currently authorised to deal electronically with The Department.
Identity Manager	Identity Manager is an application that is used to register and maintain details of all Users and Devices that transact electronically with The Department for cargo-related purpose.
Pending	A status attributed to a User when they have applied to become a registered User for an Organisation but an Administrator is yet to confirm their authority to represent the Organisation by ENABLING them.
Registered Device	An Organisation's Machine which has a Digital Certificate which has been successfully registered through the Identity Manager application.
Registered User	A Person who has purchased a Digital Certificate which has been successfully registered through the Cargo Interactive Registration process or through the Identity Manager application.
Role	The role of the User defines what authorities or actions they can perform on behalf of themselves and their organisation. The roles are Registered User, Administrator, and Signing Authority. There is no limit to the number of Users or Administrators which can be registered for an Organisation. There can only be one Signing Authority for an Organisation at a time.

Term	Meaning
Signing Authority	A User who digitally signed the Cargo Interactive User Agreement (or who has been assigned this role). This User has the ultimate responsibility for managing Users and Devices that deal with The Department for their Organisation.
Status	A User/Device status can have a status of **ENABLED**, **DISABLED** or **PENDING**. A User/Device with an **ENABLED** status can currently deal electronically with The Department (provided they have a current and registered Digital Certificate). A User/Device with a **DISABLED** status CANNOT currently deal electronically with The Department. A User with a **PENDING** status has a valid certificate which is associated with a known Organisation, but have not yet been authorised to represent the Organisation by an Administrator or Signing Authority for the Organisation. Pending Users remain in Identity Manager for 7 days. They have NO access to applications until their login status changes to ENABLED.
User	See Registered User.