Login failed, access denied

If you have entered the wrong Username and/or Passcode, one of the following messages will appear:

- **"HPDIA0201W The client supplied invalid authentication information."** (internet access)
- **"Access denied. Credentials rejected. Try again"** (CHMI access)

Before trying to login again, do the following:

- Only when using Internet access: delete the cookies and temporary Internet files via the Internet options of your web browser. Close the web browser and open it again.
- Check the UTC time of your PC.
- Enter the correct UserID in the "Username" field.
- Wait until the software token has generated a new token code.
- Generate a new Passcode and try to login again.
- If you tried several times to login, but still fail to connect to the Network Operations Access Service, contact the CSO Technical Helpdesk to guide you through the login procedure.

Check the UTC time of your PC

The RSA SecurID Software token is based on UTC time. Your authentication to NM Protected Applications will only be successful if the UTC time of your PC is set correctly. To check the UTC time of your PC, go to the following webpage:
http://www.cfmu.eurocontrol.int/utc.html

This page does not show the real UTC time, it calculates to what time the UTC time is set on your local PC, based on your PC's settings. If the date or time shown do not correspond to real UTC time, change your PC clock or time zone by double-clicking the time display on the Windows taskbar.

I am always referred back to the login page or sitemap without any error message

(Internet access only)

You might be referring to an old URL. To correct the URL, go to the EUROCONTROL public homepage and select the section relevant to the Network Operations system access.
www.eurocontrol.int/network-operations

At the right-hand side you see the different NM Protected Applications. Choose the correct link according to the application you want to use. If the URL is correct, delete the cookies and temporary internet files via the Internet options of your web browser and try to login again.

Why do I need to re-login when polling?

(CHMI access only)
When using the polling option in the CHMI application, you need to re-login after 10 times of polling. The duration between the different logins depends on your polling-settings. By default, the polling is done every 10 minutes and the application polls for 10 times, so after 10 x 10 (100) minutes the login screen is shown. You can change the time settings of the polling and create a larger time window between the re-logins. To do so, click on 'File' in the menu bar of the CHMI application. There, you choose the option 'Preferences'. A new window will popup, here you have to choose CHMI/ATFCM Application/ General/Dates and Times. At the right side you should see 'Basic poll time interval'. This value can be adapted to, for example, 15 minutes instead of 10. After you have done this, you confirm by clicking on the 'Done' button. Now the polling will occur every 15 minutes for 10 times, which results in a time window of 150 minutes between the different login screens.

Online help

You can also find the FAQ about Login problems on EUROCONTROL Network Management public website under Network Operations.
Click on "FAQ" at the left-hand side of the page.

User Technical Documentation

For more details, consult the Network Manager Connection Guide in the Network Operations library of the Network Management website.

Contact the CSO Technical Helpdesk

Tel.: 00 32 2 745 1997
Fax: 00 32 2 729 90 23
e-mail: nm.cso.help-desk@eurocontrol.int

EUROCONTROL

www.eurocontrol.int

Quick Connection Guide to Operational Collaboration

Network Manager Protected Applications

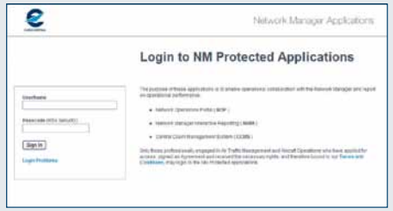
Operational Collaboration Applications

1) Internet Applications
(NOP Portal, NMIR & CCMS-Web):
Open your web browser and surf to
http://www.eurocontrol.int/network-operations

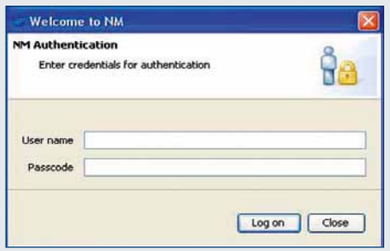
At the right-hand side, choose one of the "**Protected Applications**"

- Select NOP to access the Network Operations Portal.
- Select NMIR to access the Network Manager Interactive Reporting.
- Select CCMS to access the Claim Management System.

The following login screen will appear:



2) CHMI Applications
(CIFLO, CIREN, CIAO, CITO): Click on Start/Programs/Applications/ATFCM to start the application. The **following login screen will appear:**



How to login?

- In the "Username" field, enter the UserID that has been assigned to you by the Network Manager (for example: p0xxx1).
- In the "Passcode" field, enter the Passcode that is generated by the RSA SecurID Software Token after entering your PIN code. (See section "How to generate your Passcode?")
- Press the Login button (Sign In/Log on). Pay attention: press the login button only once, otherwise our system will see it as a security violation and will reject the passcode you entered.

First login with a new token

A new token which has been installed on your system is disabled for security reasons by default. You have to contact the CSO Technical Helpdesk to enable your token.

What is the Username or UserID?

Your "Username" or "UserID" is a login name which has been assigned to you by the Network Manager (for example: p0xxx1). The "UserName" is not case sensitive.

What is the PIN code?

The PIN code is your personal code, chosen by yourself the first time your token was activated. This is a number between 4 and 8 digits long. If you do not remember your PIN code, you can contact the CSO Technical Helpdesk to have it reset.

It your token is used by multiple users on a shared working position, do not forget to communicate this new PIN code to your colleagues, as the PIN code is related to the UserID.

What is the token code?

The token code is a random number generated by the RSA SecurID Software Token. Every minute a new token code is generated, making the previous one invalid.

What is the Passcode?

The passcode is the combination of your personal PIN code and the token code. It is generated by the RSA SecurID Software Token after entering your PIN code. This is the only valid code to connect to the NM Protected Applications.

RSA SecurID Software Token

Start the RSA SecurID Software Token by clicking on Start/Programs/RSA SecurID Software Token/RSA SecurID Software Token.

NM supports 2 versions of the RSA SecurID Software: version 3.0.7 (Windows XP compatible) and version 4.1.1 (Windows XP, Vista and Windows 7 compatible). The 2 versions have a different appearance and work in a slightly different way (as explained below).

Version 3.0.7

If you have a different view from the one above, click on "View" in the menu bar of the Software Token and select "Token View". We recommend using the 'Token View' mode.

Version 4.1.1

How to generate your Passcode?

- Start up the RSA SecurID Software Token.
- Only for version 3.0.7: wait until the Software Token generates a new token code to be sure you have sufficient time to login. The token code is only valid for one minute. The validity time is indicated by the small dashes at the left-hand side of the numeric display. Each dash corresponds to 10 seconds. When no dashes are visible, the token code has expired and you will no be longer able to login with this code. A new token code will be generated automatically within 10 seconds.
- Enter your PIN code on the Software Token by clicking the numbered boxes on the Software Token (version 3.0.7) or via the number keys on your keyboard.
- Press the ENTER button or click on the little arrow (version 4.1.1).
- Click on "Copy!" in the menu bar of the Software Token (version 3.0.7) or on the "Copy" button (version 4.1.1).
- Return to the Login screen and paste the passcode into the "Passcode" field. (click your right mouse button and select "Paste" from the drop-down menu or press CTRL + V simultaneously).