TECHNICAL NOTES

ECaccess User Guide

User Support

Operations Department

Version 4.0

October 2011

European Centre for Medium-Range Weather Forecasts
Europäisches Zentrum für mittelfristige Wettervorhersage
Centre européen pour les prévisions météorologiques à moyen terme

European Centre for Medium-Range Weather Forecasts
Shinfield Park, Reading, RG2 9AX, United Kingdom

The information within this publication is given in good faith and considered to be true, but ECMWF accepts no liability for error, omission and for loss or damage arising from its use.

Contents

The ECaccess change history can be found at www.ecmwf.int/services/ecaccess/download/changelog.html

1 Introduction

The ECaccess software gives Member States [1] and other ECMWF users batch and interactive access to the ECMWF computing and archiving facilities. Access is available via the Internet as well as via RMDCN.

This user guide, which is intended for all users of the ECaccess software, describes the concepts and procedures for accessing data and running jobs at ECMWF. If you are to perform the administrative task of installing and/or maintaining the ECaccess software, you should study the *ECaccess Administrator's Guide* (see `http://www.ecmwf.int/services/ecaccess/download/`). For the gateway concepts and procedures see section 2.

This guide is structured as follows:

Getting started

- Section 2 describes the ECaccess global architecture, focusing on the FTP, Web, Telnet and X11 components.
- Section 3 gives an overview on interactive and shell script user authentication.

Running batch work at ECMWF

For automating data transfers and submitting batch jobs, refer to:

- Section 4 describes how initiate unattended transfers from ECMWF.
- Section 5 describes the ECaccess Shell commands.

ECaccess on-line

For access to on-line ECMWF computing facilities, refer to:

- Section 6 describes web-based management of jobs and file transfers to and from the ECHOME (for "ecgate" home directory), ECSCRATCH (for "ecgate" scratch directory) and ECFS directories.
- Section 7 describes web-based monitoring and trouble- shooting of batch jobs and file transfers.
- Section 8 describes logging in at ECMWF via the gateway's single-sign-on Telnet server component.
- Section 9 describes logging in at ECMWF via the gateway's single-sign-on SSH server component.
- Section 10 describes starting X11 applications on ECMWF servers using the single-sign-on X11 access component.

[1] In the following "Member States" (MS) includes "Co-operating States".

2 Ecaccess concepts

ECaccess is a framework for batch and interactive access to ECMWF services for Member States and other ECMWF users.

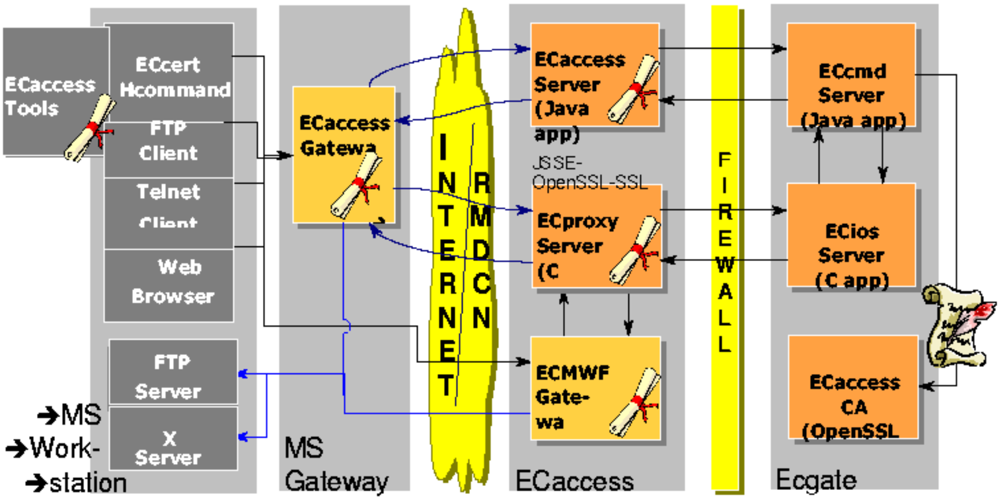


Figure 1: ECaccess design layout.

The components of ECaccess are:

- The ECaccess gateways: all Member State users can access the ECMWF computing and archiving facilities through a gateway. Full ECaccess functionality requires an ECaccess gateway to be installed at the Member State. Alternatively, reduced ECaccess functionality is available on the ECMWF ECaccess gateway.
- The ECaccess Server: all gateways are connected to this server. It provides technical and high level services to the gateway, allowing generic access to computing and archiving facilities at ECMWF (through "ecgate").
- The "ecgate" server: includes services such as the local LoadLeveler batch system, the (LoadLeveler) batch system on c1a (the High Performance Computing Facility) and access to the ECFS, HOME and SCRATCH storage areas.

To allow authentication and improve security, an ECaccess Certification Authority (ECCA) certifies all ECaccess components.

2.1 ECaccess gateway

The gateway software is provided for Member States' remote access to ECMWF computing and archiving facilities. Throughout the guide, the terms "gateway" and "ECaccess gateway" are used interchangeably. Gateways include a model for the management of "plugin" services. A plugin is a piece of code that handles requests/responses flowing through the gateway. Currently, there are plugins for incoming FTP, HTTP/S, X11, SSH and Telnet (MSgateways only) requests to ECMWF. Additional plugins are planned. On top of the SSH plugin the NX application can be used for interactive access to ECMWF. The ECMWF ECaccess gateway (hereafter referred to as "ECgateway") can be used on its own. Nevertheless, using a Member State ECaccess gateway (hereafter referred to "MSgateway") instead offers the following features and advantages over using the ECgateway on its own:

- Secure tunnel between ECMWF and MSgateway: all services are channelled through SSL (Secure Socket Layer) secure connections to ensure data integrity. For confidentiality, administrators can set up encryption.
- Security authentication: protocols such as FTP or Telnet use only basic security mechanisms during their login process. The MSgateway plugins invoke an SSL protocol component for user authentication.
- Low resource usage / fast response: opening and closing SSL connections takes a significant amount of CPU time, bandwidth and memory. MSgateways maintain a set of permanent SSL connections (to the ECaccess server) for their plugins.
- Web memory cache: pages collected by the MSgateway from ECMWF and passed to Member State browsers can be stored in a memory cache. If the same page is required again, it is retrieved from this cache. Since this cache is located on the MSgateway, this is quicker than access through the Internet.

2.2 Using an ECaccess gateway

If the basic features, available via the ECMWF ECaccess gateway interfaces, are sufficient, you can use "ecaccess.ecmwf.int" for the web and the FTP interface. The Shell commands (section 5) use "ecaccess.ecmwf.int" as the default gateway name. If you have access to RMDCN and want to use it for accessing ECMWF, you can use "msaccess.ecmwf.int" instead.

If you wish to use the advanced features, only available via a Member State ECaccess gateway, you will need to find out, on which host this gateway has been installed at your local site and which FTP and HTTPS ports are being used by that gateway. You may be able to obtain this information by running the `ecaccess-gateway-name` Shell command. If `ecaccess-gateway-name` is in your command path, it will provide information about the ECaccess gateway you are using.

If the command is not available, you will need to contact your local ECaccess administrator or Computing Representative. You can also email advisory@ecmwf.int.

2.3 Plugins

By default, the following plugins are automatically started on all the gateways:

- The FTP plugin: allows Member State users to submit jobs and to transfer files (between their own computer on one side and ECMWF file systems and ECFS on the other side). This extended FTP server can also be used for access to ECMWF computing and archiving facilities from within shell scripts.
- The HTTP/S plugin: for job and file transfer management/monitoring from a browser.
- The Telnet and the X11 plugins (available on MSgateways only): provide access to ECMWF servers with a single-sign-on login process. Communication and authentication are established through the gateway.

- SSH is increasingly used for external connections. ECaccess includes an SSH plugin which will allow you to access ECMWF and run X11. Note that only SSH protocol version 2 is supported.

3 Security authentication

The gateways uses two built-in security mechanisms to control access to ECMWF:

- Interactive authentication: users will be prompted for their ECMWF user identifier and the PASSCODE (obtained by entering their PIN number into the security token).
- Batch authentication: users need to create an ECaccess certificate before they access ECMWF facilities. This method allows Member State users to automate authentication within scripts. The HTTP/S, Telnet, X11 and SSH plugins support only the first method. The FTP plugin supports both.

The ECaccess certificate is a standard X509 digital certificate saved on the user's computer as a file. It identifies a user to the gateway. The ECaccess Certification Authority (ECCA) signs each certificate. Therefore, when a user provides his certificate to the gateway, its signature is checked using the ECCA public key for verification. A certificate can be created:

- Using the "ecaccess-certificate-create" command: this is described in section 5.1.
- Using the Web interface: login to the Web server (providing an ECMWF user identifier and token PASSCODE) and in the menu click the "Get Certificate" option to download the new Certificate, see section 6.

The ECaccess certificate is valid for 7 days for all services.

4 Unattended file transfer - ectrans

The ectrans command allows you to transfer files securely between ECMWF and remote sites. Like the UNIX “rcp” command, ectrans requires no password to be specified for the remote host: the ECaccess gateway performs the security checking. Unlike standard FTP, ectrans is suitable for unattended file transfers in scripts, cron jobs, etc., as it avoids the problems inherent in storing passwords in text files and sending passwords across networks.

Even if you don’t have a local gateway installed, you can benefit from the ectrans command by using the ECMWF ECaccess gateway. Please note that in this case the transfer is not as secured as when a Member State ECaccess gateway is used.

4.1 Target location

Users who wish to transfer files between ECMWF and Member State servers using ectrans need to declare one or more ectrans assiciations for the storage/retrieval of the remote file. This can be done either through the ECtools command ecaccess-association-put or through the ECaccess Web interface of the target gateway (see section 6.4). For every “msuser” declaration, the hostname and the login username and password need to be specified.

After the ECaccess gateway installation, the Member State ECaccess system administrator can customise the access methods for file transfers. These will be displayed through the ECaccess Web interface. Several schemes can be implemented, such as:

- The target directory for a particular destination is a sub-directory of a central directory configured by the administrator, with the sub-directory name matching the msuser name.
- The target directory for all file transfers to a given destination is a sub-directory of the msusers home directory. The administrator configures the sub-directory name.
- The target directory for a given destination is configurable by the user. The administrator determines whether or not the user is allowed to include “..” in the directory path.

Target directories can be located on:

- Member State servers running a standard FTP service accessible from the ECaccess gateway. This is known as a “genericFtp” destination and is the most convenient way of getting the files to the system you want, under the specified user ID.
- The server running the ECaccess gateway. This is known as a “genericFile” destination. All users will share in a common directory the files transferred using this destination.
- Member State servers running a proprietary application. The administrator provides ectrans with the implementation of the access protocol. The administrator can also use more complex rules to define special target locations for ECMWF users, Member State users or groups of Member State users. The command ??? described in the next section can be used to get the translated URL of a target location, giving a Member State user identifier and a destination name (passwords are displayed as ***).

4.2 ectrans command

With the ectrans command, Member State users who use their shell account at ECMWF can initiate secure file transfers between ECMWF (ecgate or HPCF systems) and Member State servers.

When ectrans is used to put a file (from ECMWF to a Member State), the ECaccess Server will spool the file in the user's "ectrans" transfer queue: if the connection between the ECMWF and Member State gateways is down or if any error occurs, the file will be kept in the spool area at ECMWF and you can resume the transfer either through the web interface or with the ECtools command ectret.

When ectrans is used to get a file (from a Member State to ECMWF) the transfer will fail by default, if the connection between the ECMWF and Member State gateway is down. A retry mechanism is available for all types of transfers. To show the ectrans usage:

```
$ ectrans -help
usage: ectrans [-gateway name] -remote msuser@[destination] \
          [-get|-put] -source [ec:|ectmp:]filename [args ...] (*)
        ectrans -check requestID (*)

 -gateway  {arg} - access gateway name (default (**): ecaccess.ecmwf.int)
 -remote   {arg} - access method (default (**): *none*)
 -source   {arg} - source file name
 -target   {arg} - target file name (default: same as -source)
 -mailto   {arg} - target email address (default: current user)
 -lifetime {arg} - lifetime of the file in the spool (default: 1w) (***) (****)
 -delay    {arg} - transmission delay (default: immediate transfer) (***) (****)
 -at       {arg} - transmission date (default: immediate transfer) (****)
 -format   {arg} - define the date format as used with -at (default: yyyyMMddHHmmss)
 -retryCnt {arg} - define the number of retries (default: async=144, sync=0)
 -retryFrq {arg} - define the frequency of retries (default: async=10m, sync=1m) (***)
 -maxTime  {arg} - define the maximum transfer duration (default: 12h) (***)
 -priority {arg} - transmission priority 0-99 (default: 99) (****)
 -put            - interactive/synchronous transfer (no spool)
 -get            - interactive/synchronous pull (rather than push) file
 -onsuccess      - mail sent on successful transfer
 -onfailure      - mail sent when transfer has failed
 -onretry        - mail sent when transfer is retried
 -keep           - keep the request in the spool till expiration (****) (*****)
 -remove         - always remove the request from the spool (****) (*****)
 -reject         - if existing target file (default)
 -append         - if existing target file
 -resume         - if existing target file
 -overwrite      - if existing target file
 -verbose        - verbose mode on
 -version        - print version number
 -help           - this message

    (*) If successful, a requestID is returned, which can be used in
          check requests. Exit code is 0 on success and >0 otherwise.
   (**) The default values depend on the GATEWAY or REMOTE environment
          variables.
  (***) Duration in weeks, days, hours, minutes or seconds (e.g. 1w|2d).
 (****) These options are only relevant when the spool is used. The spool
          is no used during interactive transfers (-get and -put options).
(*****) By default, successful requests are removed from the spool and
          failed requests are kept in the spool till expiration.
```

The "reject", "append", "resume" and "overwrite" options are mutually exclusive and determine what to do if there is an existing target file. The "mailto" option specifies an email address to be notified in case of a successful (option “onsuccess”) and/or a failed transfer (option “onfailure”). The “check” option prints the status of the specified request on the standard output.

The transfer status, which can be checked with the `ecaccess-ectrans-list` command or the Web interface, can takes values as listed in table 1.

Status	**Meaning**
INIT	Files are being transferred to the spool
COPY	Files are being transferred to the remote site
WAIT	Files are scheduled and waiting to be started
RETR	File transfer will be retried
STOP	Files have NOT been successfully transferred (error)
DONE	Files have been successfully transferred

Table 1: Transfer status.

4.2.1 Transfer to a Member State host via gateway

To transfer file “fff” from the current working directory on “ecgate” to the “genericFtp” destination of the use “myUser” on the ECaccess gateway “ecaccess.meteo.ms”:

```
$ ectrans -gateway ecaccess.meteo.ms \
          -remote myUser@genericFtp
          -source fff \
          -verbose
verbose: gateway=ecaccess.meteo.ms
verbose: echost=ecgate.ecmwf.int
verbose: ecport=644
verbose: action=spool
verbose: ecuser=xyz
verbose: source=fff
verbose: target=fff
verbose: keep=false
verbose: remove=false
verbose: option=reject
verbose: lifetime=1w
verbose: delay=(none)
verbose: at=(now)
verbose: format=yyyyMMddHHmmss
verbose: retryCnt=144
verbose: retryFrq=10m
File to upload (5140480 bytes)
9442903031
```

When a request has been spooled successfully, a requestID is returned immediately. `ectrans` will then return the exit code 0. The requestID can be used to reference the transfer, using the interface described in section 7 or with the command `ecaccess-ectrans-list`.

If the file is not successfully spooled, an error message is printed and the `ectrans` return code is -1.

4.2.2 Transfer from a Member State host via gateway

To transfer file “fff” at the “genericFtp” destination of the “myUser” msuser of the ECaccess gateway “ecaccess.meteo.ms” to the current directory at ECMWF:

```
$ ectrans gateway ecaccess.meteo.ms \
          -remote myUser@genericFtp \
          -get -source fff \
          -verbose
gateway: ecaccess.ecmwf.int
echost: ecgate.ecmwf.int
ecport: 644
action: get
ecuser: xyz
target: fff
source: fff
keep   : false
option: reject
File to download (0 bytes)
5140480 bytes to download
```

When the request has been carried out successfully, the result is returned immediately. Transfers from a Members State to ECMWF are not spooled; they are carried out synchronously. The `ectrans` return code is 0 if the file has been transferred successfully or -1 if the file has not been transferred successfully.

5 Shell commands

The ECaccess shell commands, also referred to as ECtools, are a set of scripts for the management of files, file transfers, jobs, ectrans associations and events at ECMWF. They can be run by any user and on any Member State host.

The ECtools are using SOAP to access the ECaccess web server. “SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP Extension Framework.”

Running these commands requires a valid certificate. The command `ecaccess-certificate-create` will create a certificate in the user’s home directory (`$HOME/.eccert.crt`) from an ECMWF user identifier and a passcode (generated by a security token).

You need to ensure the following environment parameters are set with the correct values:

```
ECACCESS_HTTP=gateway.meteo.ms:9080
ECACCESS_HTTPS=gateway.meteo.ms:9443
```

(e.g. if your local ECaccess Gateway name is ”gateway.meteo.ms” and you are using the default ECaccess http/s ports 9080/9443)

The default values are pointing to the ecaccess.ecmwf.int server.

Your gateway administrator can provide other default values for these parameters. However, your environment variables take precedence over these default values.

If the directory containing the shell commands is not in your command path or you do not know the directory in which the shell commands are installed, try running the “ecaccess-gateway-name” command. If the command is not available, you will need to contact your Computing Representative, your local ECaccess administrator - if known - or User Support at ECMWF. Alternatively, you may wish to install the shell commands yourself (see `http://www.ecmwf.int/services/ecaccess/download/`).

The ECaccess Tools are organized in sets covering access to the whole computing and archiving facilities of ECMWF and are described in the following sections. Each command is documented with its own man page which provide explanation as well as examples on how to use it.

The following options are common to all the ECtools:

-help	Print a brief help message and exits.
-manual	Prints the manual page and exits.
-debug	Display the SOAP messages exchanged.
-version	Print the ECaccess version number.

5.1 Certificate management

The ECaccess certificate can be created using the command ecaccess-certificate-create. From an ECMWF user identifier and a PASSCODE (using a security token), it generates a certificate in `$HOME/.eccert.crt`.

Alternatively, a certificate can be created using the ECacess Web interface, see section 6.

The ECaccess Tools are also available at ECMWF. In contrast to using locally installed ECtools you will not need a certificate when using them at ECMWF as you have already been validated at login.

To display a help screen describing the `ecaccess-certificate-create` usage:

```
$ ecaccess-certificate-create -help
Usage:
    ecaccess-certificate-create [options] [user-id]

    Options: -help brief help message -manual full documentation -debug
    enable messages output

Options:
    -help   Print a brief help message and exits.

    -manual Prints the manual page and exits.

    -debug  Display the SOAP messages exchanged.
```

Certificates are PEM/Base64 encoded ASCII files.

OpenSSL can be used to decode and display certificate components.
To display the expiry of the various ECaccess services the command ecaccess-certificate-list can be used:

```
ecgate{/home/ectrain/trx}:1 --> ecaccess-certificate-list
submitJob            168h     Jan 18 11:56         job submission
getJobList           168h     Jan 18 11:56         job list
deleteJob            168h     Jan 18 11:56         delete a job
getJobResult         168h     Jan 18 11:56         job result
deleteFile           168h     Jan 18 11:56         delete file
getFileList          168h     Jan 18 11:56         get file list
mkdir                168h     Jan 18 11:56         make directory
getFileSize          168h     Jan 18 11:56         get file size
readFile             168h     Jan 18 11:56         read file
writeFile            168h     Jan 18 11:56         write file
moveFile             168h     Jan 18 11:56         move file
rmdir                168h     Jan 18 11:56         remove directory
chmod                168h     Jan 18 11:56         change file mode
getTempFile          168h     Jan 18 11:56         create temporary file
getTransferList      168h     Jan 18 11:56         get transfer list
```

As can be seen from the output, for a normal user-id the validity is 168 hours (7 days) for all services. The date/time shown refers to the expiration of the certificate.

5.2 General information

To display the computer operations system information (cosinfo), use the command ecaccess-cosinfo:

```
-> ecaccess-cosinfo
*******************************************************************************
*                                                                             *
*                                                                             *
*  Welcome to AIX Version 5.3!                                                *
*                                                                             *
*                                                                             *
*  Please see the README file in /usr/lpp/bos for information pertinent to    *
*  this release of the AIX Operating System.                                  *
*                                                                              *
*                                                                              *
********************************************************************************

ECMWF SYSTEM SESSIONS
--------------------

WEDNESDAY the 12th of JANUARY 2011:
----------------------------------

08:30-10:30 UTC Mars and ECFS System Session:
impact: Mars and ECFS will be unavailable

To reread the message please use: more /etc/motd or cat /etc/motd

===============================================================================
```

5.3 Gateway information

Commands named ecaccess-gateway-* (table 2) provide information about ECaccess gateways (see section 2.1).

Command	Purpose
ecaccess-gateway-list	List of ECaccess Gateways
ecaccess-gateway-name	Display the name of your default ECaccess Gateway

Table 2: Shell commands providing information on ECaccess gateways (ecaccess-gateway-).*

The command `ecaccess-gateway-name` is the only one which can be used without authentication/certificate.

5.4 File management

Files at ECMWF can be managed through the ECtools named ecaccess-file-*. The file location is specified with the following syntax

`[domain:][/user-id/]path`

where `domain:` can take the values as listed in table 3. The user-id refers to a an ECMWF computer user-id. Only if the domain is specified as an ECFS domain, then the user-id could also be a common pool, e.g. demeter.

Domain value	Purpose
home:	the ecgate `$HOME` file system
scratch:	the ecgate `$SCRATCH` file system
ec:	the ECFS domain ec:
ectmp:	the ECFS domain ectmp:
host-name:	any server at ECMWF, e.g. c1a

Table 3: Domain values.

If no domain is specified then an absolute path will translate to an absolute path on the ecgate server and a relative path will translate to a path in the HOME directory of the current user.

If no user-id is specified then the current user-id is selected by default. When you specify a host-name you are by default under the root directory; the user-id parameter can not be used with a host-name.

File location examples:

`bin/a.out`	file a.out in directory `$HOME/bin` of the current user
`home:bin/a.out`	file a.out in directory `$HOME/bin` of the current user
`/tmp/a.out`	file a.out in directory `/tmp` on ecgate
`home:/xzy/bin/a.out`	file a.out in directory `$HOME/bin` of user xzy
`ec:bin/a.out`	file a.out in directory bin in the current user's ECFS domain ec:
`ec:/xzy/bin/a.out`	file a.out in directory bin in user xzy's ECFS domain ec:
`c1a:/c1a/tmp/group/xzy/a.out`	file a.out in directory `/c1a/tmp/systems/xzy/` on c1a

Command	Purpose
ecaccess-file-chmod	Change ECaccess File Mode Bits
ecaccess-file-copy	Copy an ECaccess File
ecaccess-file-delete	Remove an ECaccess File
ecaccess-file-dir	List ECaccess Directory Contents
ecaccess-file-get	Download an ECaccess File
ecaccess-file-mget	Download Multiple ECaccess Files at once
ecaccess-file-mkdir	Make a Directory on the ECaccess File System
ecaccess-file-modtime	Show the Last Modification Time of an ECaccess File
ecaccess-file-move	Move or Rename ECaccess Files
ecaccess-file-mput	Upload Multiple Local Files on the ECaccess File System at once
ecaccess-file-put	Upload a File on the ECaccess File System
ecaccess-file-rmdir	Remove a Directory on the ECaccess File System
ecaccess-file-size	Show the Size of an ECaccess File

Table 4: Shell commands for file management (ecaccess-file-).*

5.5 Batch job management

Batch jobs at ECMWF can be managed through the ECtools named ecaccess-job/queue-*, see table 5. Possible values of the job status, which can be checked with the command ecaccess-job-list or via the Web interface, are listed in table 6.

A special service (see option -eventIds) allows to automatically submit jobs to be run when certain points in the daily ECMWF operational forecast suite have been reached. The main purpose is to ensure that certain data are available before e.g. submitting a MARS request. These events correspond to the different stages when the ECMWF operational activity has produced certain data or products. The list of events can be retrieved with the ”ecaccess-event-list” command.

5.6 Management of events

ECMWF maintains some notifications (events) which are linked to ECMWF's operational activity and offers the service for time-critical jobs (see also separate documentation at `http://www.ecmwf.int/services/computing/docs/tc_apps/index.html`). This service is also available to MS users who maintain their own notifications and can therefore create simple dependencies between different activities, at ECMWF and remote sites.

Command	Purpose
ecaccess-job-delete	Delete an ECaccess Job
ecaccess-job-get	Download a Job Output/Input/Error File
ecaccess-job-list	List all ECaccess Jobs
ecaccess-job-restart	Restart an ECaccess Job
ecaccess-job-submit	Submit a new ECaccess Job
ecaccess-queue-list	List available queues

Table 5: Shell commands for batch job management (ecaccess-job/queue-).*

Status	Meaning
DONE	Jobs have successfully completed
EXEC	Jobs are running
INIT	Jobs are being initialised
RETR	Jobs will be resubmitted
STDBY	Jobs are waiting for an event
STOP	Jobs have NOT completed (error)
WAIT	Jobs have been queued to the scheduler (e.g. LoadLeveler)

Table 6: Job status.

The shell commands to managed events are listed in table 7.

5.7 Management of ECtrans transfers

The commands for the management of ECMWF-initiated transfers (ectrans, see section 4.2) are listed in table 8. They can only be used for the management of transfers, which have used the ECaccess gateway as shown with the `ecaccess-gateway-name` command.

5.8 Management of ECtrans associations

Before making use of ectrans, users will need to declare an ectrans association, also referred to as 'remote Member State user (msuser)' for the storage/retrieval of the remote file. The management of these associations can be done through the ECtools named ecaccess-association-* listed in table 9.

Command	Purpose
ecaccess-event-clear	Clear an ECaccess Event
ecaccess-event-create	Create an ECaccess Event
ecaccess-event-delete	Delete an ECaccess Event
ecaccess-event-grant	Grant usage of an ECaccess Event
ecaccess-event-list	List available events
ecaccess-event-send	Trigger an ECaccess Event

Table 7: Shell commands for management of events at ECMWF (ecaccess-event-).*

Command	Purpose
ecaccess-ectrans-delete	Delete ECtrans
ecaccess-ectrans-list	List all ectrans transfers
ecaccess-ectrans-request	Request a new ECtrans transfer
ecaccess-ectrans-restart	Restart an existing ECtrans transfer

Table 8: Shell commands for management of ECMWF-initiated transfers (ecaccess-ectrans-).*

Command	Purpose
ecaccess-association-delete	Delete Association
ecaccess-association-get	Get the Association Descriptive File
ecaccess-association-list	List your ECtrans associations
ecaccess-association-protocol	List the supported ECtrans Protocol
ecaccess-association-put	Update/Create an Association

Table 9: Shell commands for management of ECtrans associations (ecaccess-association-).*

5.9 Execution return codes

The option '-debug' can be used with any ECtools command to display information concerning the SOAP messages exchanged. If an ECtool doesn't work correctly, please run it with the -debug option and send the output to ECMWF for further investigation.

Shell commands return 0 if successful, otherwise one of the error codes listed in table 10. Each time an error occurs, a message indicating the error is displayed to the user.

Code	Meaning	To do
0	successful command completion	:-)
1	...	...

Table 10: ECtools error codes.

6 The Web server

The ECaccess gateway HTTP/S interface allows Member States to manage their job submissions and file transfers from their Web browser, e.g. Firefox, Mozilla or Internet Explorer. This section gives an overview of what this interface provides and how it works. Please note that only interactive authentication as described in section 3 is supported.

The main purpose of the HTTP/S plugin is to provide easy access and monitoring for on-line users. For use from within shell scripts (batch), most of those features are also provided through the FTP plugin and are described in the previous sections.

6.1 Authentication

Assuming that the Member State ECaccess gateway (see section 2.2) runs on the server “ecaccess.meteo.ms”, users connect to the application by pointing their Web browser at “http://ecaccess.meteo.ms:9080/” and will be redirected to the login page. Note that the default HTTP port number used for ECaccess is 9080.

By giving an ECMWF user identifier and a passcode, the user is authenticated and routed to a personal page; a user context is maintained for the subsequent operations from his browser. Users have the ability to request everything available from their account, until the time allocation expires or the “logout” option from the “Account” menu is selected.

Users connecting for the first time to the login page of the Web server will receive a security alert from their browser. This is normal; users have to accept the HTTP/S plugin certificate as a trusted certificate to allow the encryption of communications.

The procedure to trust the certificate depends on the browser:

- If using Internet Explorer, you will receive a security alert. You will be given an option to view the certificate. Select it, and then select the “install certificate” option. Follow the instructions to install the certificate. Once you have returned to the security alert box, select the “Accept” option.
- If using Firefox or Mozilla, you will receive a security alert. Follow the instructions in the alert box to accept the certificate as certified. In the last dialogue box you will be given an option to accept this certificate for all your sessions. Select it.

Once this procedure is complete, your future connections to the HTTP/S plugin will not produce any security alerts.

6.2 Features

After successful authentication users are redirected from the login page to the main page, from which they will be provided with a menu including available operations described in this section.

Note that the ECaccess gateway administrator can set up the HTTP/S plugin to secure only the login process. Therefore, when redirected from the secured login page to the unsecured main page you may receive a security alert. This is a normal message; just select the “Accept” option to continue.

The main page provides the following options (organized through menu entries in the left margin):

Browsing menu

- Browse files: the user can browse through his ECHOME, ECSCRATCH or ECFS files and directories.
- Delete files: users can select files to be deleted from the different places listed above.
- Copy files: users can copy files between two domains (files can be copied from an ECSCRATCH directory to an ECFS directory, for example).
- Transfer files: users can use their browser facilities to transfer files between their computer and their ECHOME, ECSCRATCH or ECFS directories; files are transferred over an FTP connection.
- Add scripts to the job list: users can select one or several scripts and add them to their job list for later submission. Users may continue browsing files, adding more scripts to their basket.
- Select scripts for submission: users can select one or several scripts for immediate submission.
- Request secure file transfers: users can select files to be sent via their transfer spool (equivalent of the TSUB command of the FTP plugin or of the ectreq command of the Ectools or of the ectrans command on the systems at ECMWF).

Queues/Jobs menu

- Browse queues: users can browse through the “ecgate” queues to select a target queue for their next job request.
- Browse basket: users can select scripts from their basket for their next job request.
- Submit new jobs: users can specify complementary parameters related to the execution and confirmed action of their request. The application then submits the job request, which is sent to the job spool (equivalent of the JREQ command of the FTP plugin).

Monitoring menu

- Monitor job submissions: see section 7.1.
- Monitor secure file transfers: see section 7.2.
- Browse the events history: the history allows saving details (date, name and summary) concerning each event for later consultation by users themselves.

Account menu

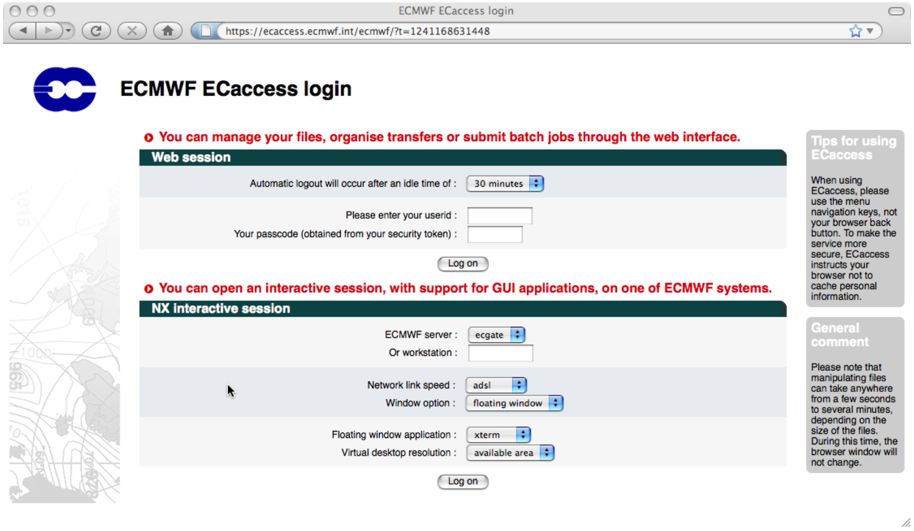
- Access the ECtrans configuration: the user can define the mapping between his ECMWF user identifier and his local user identifiers. He can also check his available destinations.
- Request a new ECaccess Certificate: the user can download a new ECaccess Certificate (description and purpose of these Certificates are discussed in section 3).
- Logout: the user context is deleted and the browser is sent back to the login page.

6.3 Users views

The following snapshots illustrate a typical interactive session a user could have using the web interface.

Different browsers on different operating systems may have different presentations of the same page.

First, under the heading “Web session”, login by providing your ECMWF user identifier and your passcode. You may modify the default value of 30 minutes to a greater value, if you plan to use the service with breaks of more than 30 minutes.



ECMWF ECaccess login

https://ecaccess.ecmwf.int/ecmwf/?t=1241168631448

ECMWF ECaccess login

You can manage your files, organise transfers or submit batch jobs through the web interface.

Web session

Automatic logout will occur after an idle time of : 30 minutes

Please enter your userid :

Your passcode (obtained from your security token) :

Log on

You can open an interactive session, with support for GUI applications, on one of ECMWF systems.

NX interactive session

ECMWF server : ecgate

Or workstation :

Network link speed : adsl

Window option : floating window

Floating window application : xterm

Virtual desktop resolution : available area

Log on

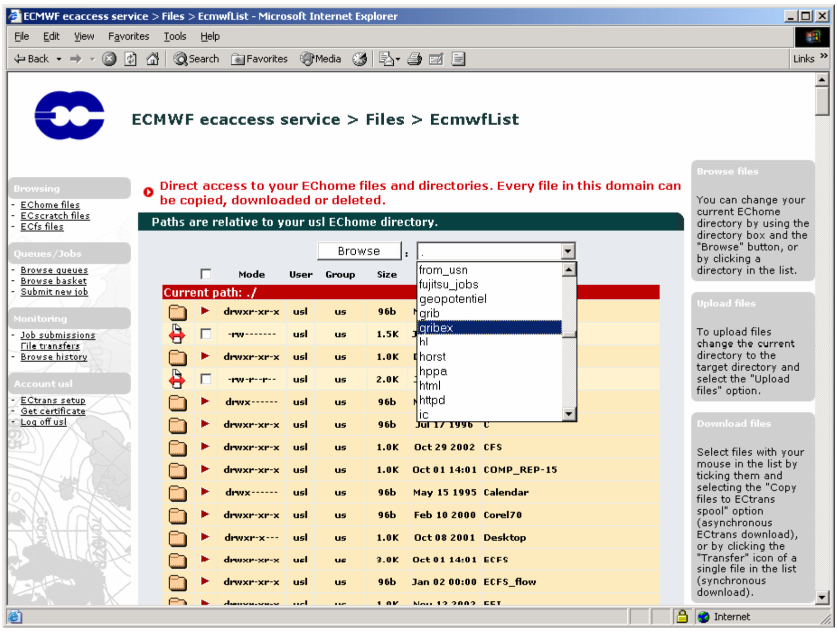
Tips for using ECaccess

When using ECaccess, please use the menu navigation keys, not your browser back button. To make the service more secure, ECaccess instructs your browser not to cache personal information.

General comment

Please note that manipulating files can take anywhere from a few seconds to several minutes, depending on the size of the files. During this time, the browser window will not change.

Once authenticated, your browser is redirected to the main page containing the menu described in the previous section (the default option is “Browsing > ECHOME files”). To browse other directories from your home directory, select a target directory and press the “Browse” button.



ECMWF ecaccess service > Files > EcmwfList - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Internet

ECMWF ecaccess service > Files > EcmwfList

Browsing
- EChome files
- ECscratch files
- ECfs files

Queues/Jobs
- Browse queues
- Browse basket
- Submit new job

Monitoring
- Job submissions
- File transfers
- Browse history

Account usl
- ECtrans setup
- Get certificate
- Log off usl

Direct access to your EChome files and directories. Every file in this domain can be copied, downloaded or deleted.

Paths are relative to your usl EChome directory.

Browse : .

from_usn
fujitsu_jobs
geopotentiel
grib
gribex
hl
horst
hppa
html
httpd
ic

Current path: ./

□	Mode	User	Group	Size		
	drwxr-xr-x	usl	us	96b		
□	-rw-------	usl	us	1.5K		
	drwxr-xr-x	usl	us	1.0K		
□	-rw-r--r--	usl	us	2.0K		
	drwx------	usl	us	96b		
	drwxr-xr-x	usl	us	96b	Jul 17 1996	C
	drwxr-xr-x	usl	us	1.0K	Oct 29 2002	CFS
	drwxr-xr-x	usl	us	1.0K	Oct 01 14:01	COMP_REP-15
	drwx------	usl	us	96b	May 15 1995	Calendar
	drwxr-xr-x	usl	us	96b	Feb 10 2000	Corel70
	drwxr-x---	usl	us	1.0K	Oct 08 2001	Desktop
	drwxr-xr-x	usl	us	3.0K	Oct 01 14:01	ECFS
	drwxr-xr-x	usl	us	96b	Jan 02 00:00	ECFS_flow

Browse files

You can change your current EChome directory by using the directory box and the "Browse" button, or by clicking a directory in the list.

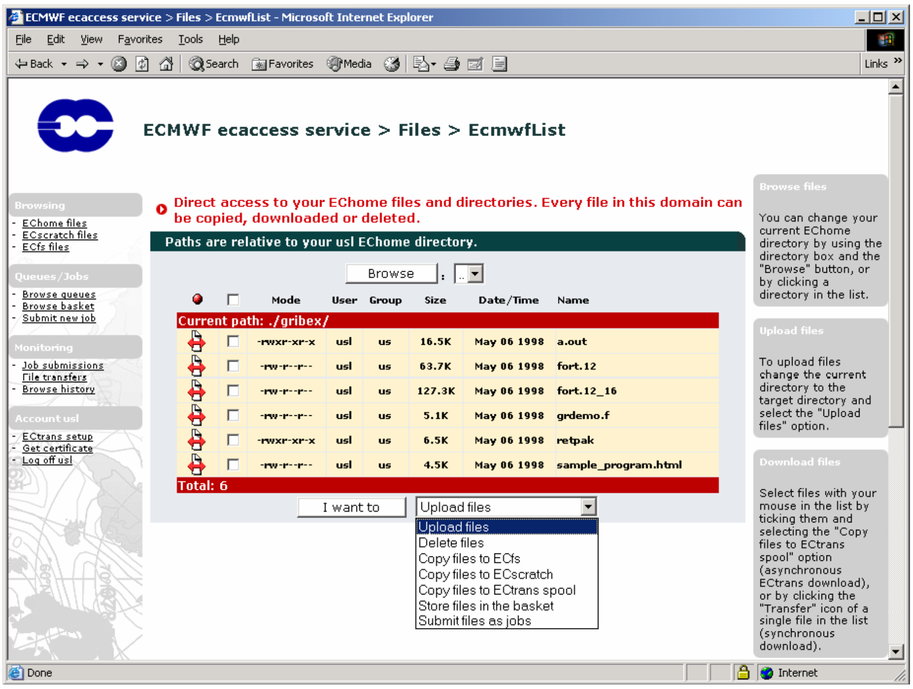
Upload files

To upload files change the current directory to the target directory and select the "Upload files" option.

Download files

Select files with your mouse in the list by ticking them and selecting the "Copy files to ECtrans spool" option (asynchronous ECtrans download), or by clicking the "Transfer" icon of a single file in the list (synchronous download).

To download a file from your current directory (./gribex in this case), click the transfer icon of the target file in the list. To upload a file into your current directory select the “Upload files” option and click the “I want to” button.



ECMWF ecaccess service > Files > EcmwfList

Direct access to your EChome files and directories. Every file in this domain can be copied, downloaded or deleted.

Paths are relative to your usl EChome directory.

Current path: ./gribex/

Mode	User	Group	Size	Date/Time	Name
-rwxr-xr-x	usl	us	16.5K	May 06 1998	a.out
-rw-r--r--	usl	us	63.7K	May 06 1998	fort.12
-rw-r--r--	usl	us	127.3K	May 06 1998	fort.12_16
-rw-r--r--	usl	us	5.1K	May 06 1998	grdemo.f
-rwxr-xr-x	usl	us	6.5K	May 06 1998	retpak
-rw-r--r--	usl	us	4.5K	May 06 1998	sample_program.html

Total: 6

Browse files

You can change your current EChome directory by using the directory box and the "Browse" button, or by clicking a directory in the list.

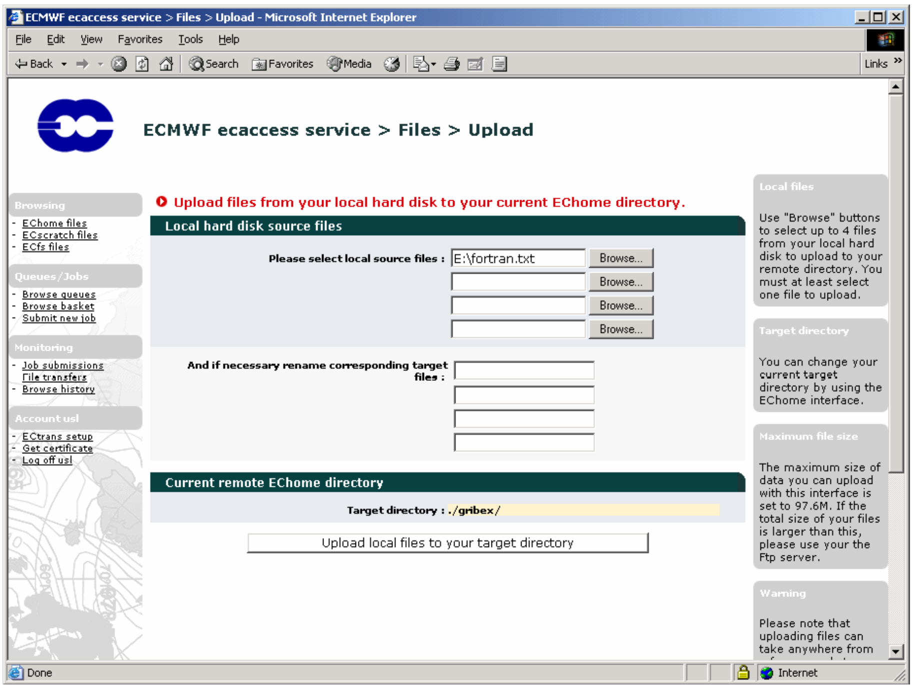
Upload files

To upload files change the current directory to the target directory and select the "Upload files" option.

Download files

Select files with your mouse in the list by ticking them and selecting the "Copy files to ECtrans spool" option (asynchronous ECtrans download), or by clicking the "Transfer" icon of a single file in the list (synchronous download).

Click the “Browse” button and select the file (`E:\fortran.txt`) you want to upload to your current directory (you may repeat the operation three times if you want to transfer more than one file). Then click the “Upload local files to your target directory”.



ECMWF ecaccess service > Files > Upload

Upload files from your local hard disk to your current EChome directory.

Local hard disk source files

Please select local source files : E:\fortran.txt

And if necessary rename corresponding target files :

Current remote EChome directory

Target directory : ./gribex/

Local files

Use "Browse" buttons to select up to 4 files from your local hard disk to upload to your remote directory. You must at least select one file to upload.

Target directory

You can change your current target directory by using the EChome interface.

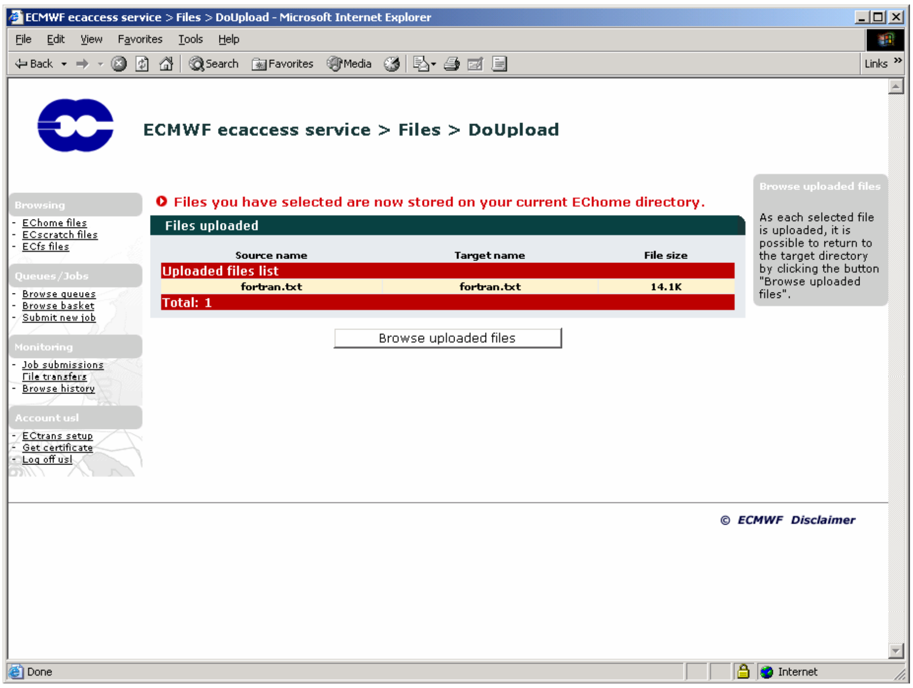
Maximum file size

The maximum size of data you can upload with this interface is set to 97.6M. If the total size of your files is larger than this, please use your the Ftp server.

Warning

Please note that uploading files can take anywhere from

Once uploaded, a summary is printed to inform you of the size of the files uploaded. You may click the “Browse uploaded files” to return to your current directory (where your files have been uploaded).



ECMWF ecaccess service > Files > DoUpload

Files you have selected are now stored on your current EChome directory.

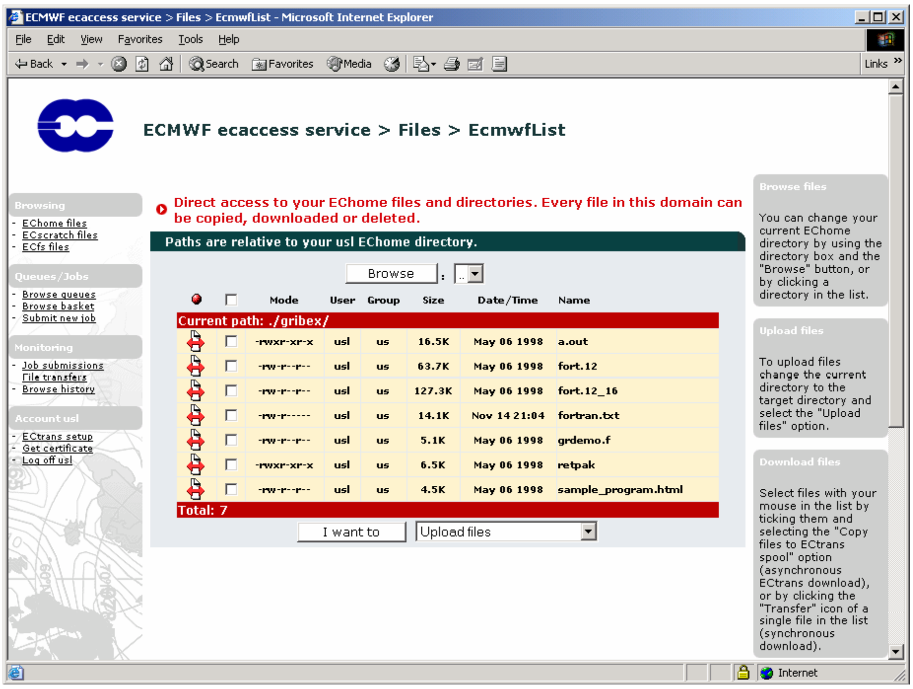
Files uploaded

Source name	Target name	File size
Uploaded files list		
fortran.txt	fortran.txt	14.1K
Total: 1		

Browse uploaded files

As each selected file is uploaded, it is possible to return to the target directory by clicking the button "Browse uploaded files".

You can see the “fortran.txt” file is now stored in your current directory. You can continue browsing directories and repeat the operation as many times as you need. To submit a job, you should first choose which system at ECMWF you want to use. To have a list of the systems at ECMWF supporting a batch service, click the “Browse queues” button.



ECMWF ecaccess service > Files > EcmwfList

Direct access to your EChome files and directories. Every file in this domain can be copied, downloaded or deleted.

Paths are relative to your usl EChome directory.

Browse : ..

●	□	Mode	User	Group	Size	Date/Time	Name
Current path: ./gribex/							
	□	-rwxr-xr-x	usl	us	16.5K	May 06 1998	a.out
	□	-rw-r--r--	usl	us	63.7K	May 06 1998	fort.12
	□	-rw-r--r--	usl	us	127.3K	May 06 1998	fort.12_16
	□	-rw-r-----	usl	us	14.1K	Nov 14 21:04	fortran.txt
	□	-rw-r--r--	usl	us	5.1K	May 06 1998	grdemo.f
	□	-rwxr-xr-x	usl	us	6.5K	May 06 1998	retpak
	□	-rw-r--r--	usl	us	4.5K	May 06 1998	sample_program.html
Total: 7							

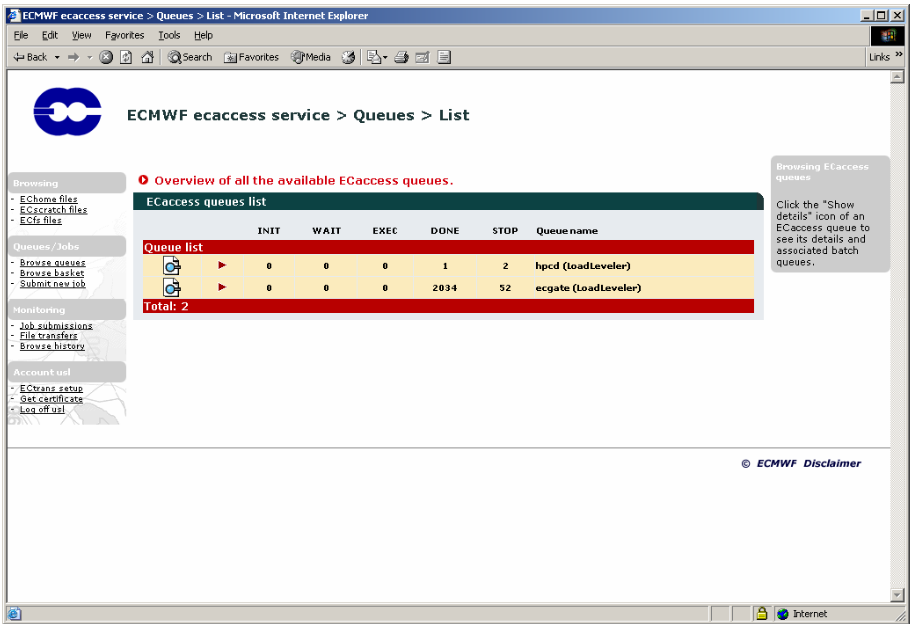
I want to: Upload files

You can change your current EChome directory by using the directory box and the "Browse" button, or by clicking a directory in the list.

To upload files change the current directory to the target directory and select the "Upload files" option.

Select files with your mouse in the list by ticking them and selecting the "Copy files to ECtrans spool" option (asynchronous ECtrans download), or by clicking the "Transfer" icon of a single file in the list (synchronous download).

The queues shown are known as ECaccess queues. For each of these ECaccess queues, you can click on the “show details” icon to see its associated batch queues on the system at ECMWF, e.g. below for the ECaccess queue hpcd:


ECMWF ecaccess service > Queues > List - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
Internet

ECMWF ecaccess service > Queues > List

Browsing
- EChome files
- ECscratch files
- ECfs files

Queues/Jobs
- Browse queues
- Browse basket
- Submit new job

Monitoring
- Job submissions
- File transfers
- Browse history

Account usl
- ECtrans setup
- Get certificate
- Log off usl

Overview of all the available ECaccess queues.

ECaccess queues list

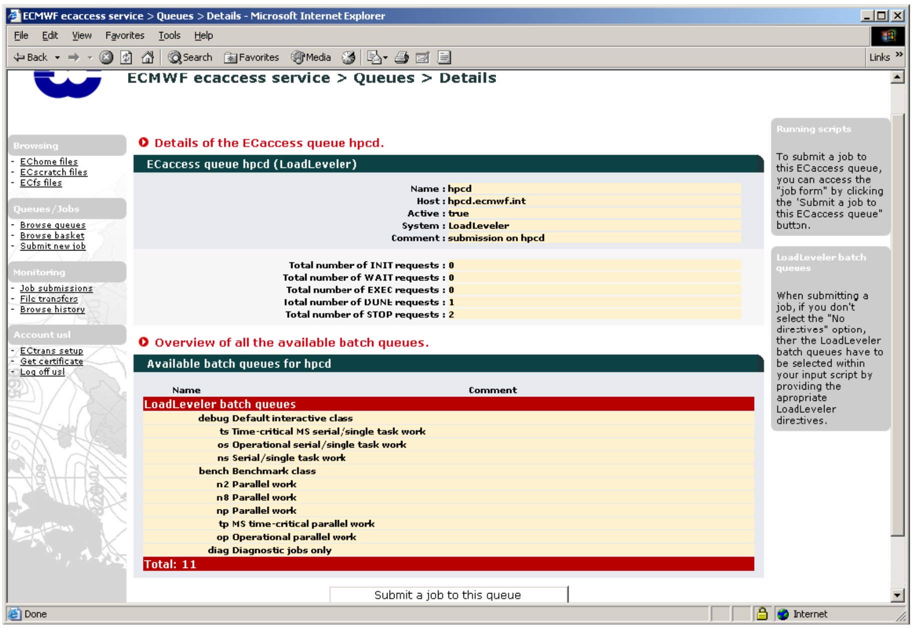
		INIT	WAIT	EXEC	DONE	STOP	Queue name
Queue list							
	▶	0	0	0	1	2	hpcd (LoadLeveler)
	▶	0	0	0	2034	52	ecgate (LoadLeveler)
Total: 2							

Browsing ECaccess queues

Click the "Show details" icon of an ECaccess queue to see its details and associated batch queues.

© ECMWF Disclaimer

To submit a new job, select the "Submit new job" option in the "Queues/Jobs" menu.


ECMWF ecaccess service > Queues > Details - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links
Done
Internet

ECMWF ecaccess service > Queues > Details

Browsing
- EChome files
- ECscratch files
- ECfs files

Queues/Jobs
- Browse queues
- Browse basket
- Submit new job

Monitoring
- Job submissions
- File transfers
- Browse history

Account usl
- ECtrans setup
- Get certificate
- Log off usl

Details of the ECaccess queue hpcd.

ECaccess queue hpcd (LoadLeveler)

Name : hpcd
Host : hpcd.ecmwf.int
Active : true
System : LoadLeveler
Comment : submission on hpcd

Total number of INIT requests : 0
Total number of WAIT requests : 0
Total number of EXEC requests : 0
Total number of DONE requests : 1
Total number of STOP requests : 2

Overview of all the available batch queues.

Available batch queues for hpcd

Name	Comment
LoadLeveler batch queues	
debug	Default interactive class
ts	Time-critical MS serial/single task work
os	Operational serial/single task work
ns	Serial/single task work
bench	Benchmark class
n2	Parallel work
n8	Parallel work
np	Parallel work
tp	MS time-critical parallel work
op	Operational parallel work
diag	Diagnostic jobs only
Total: 11	

Submit a job to this queue

Running scripts

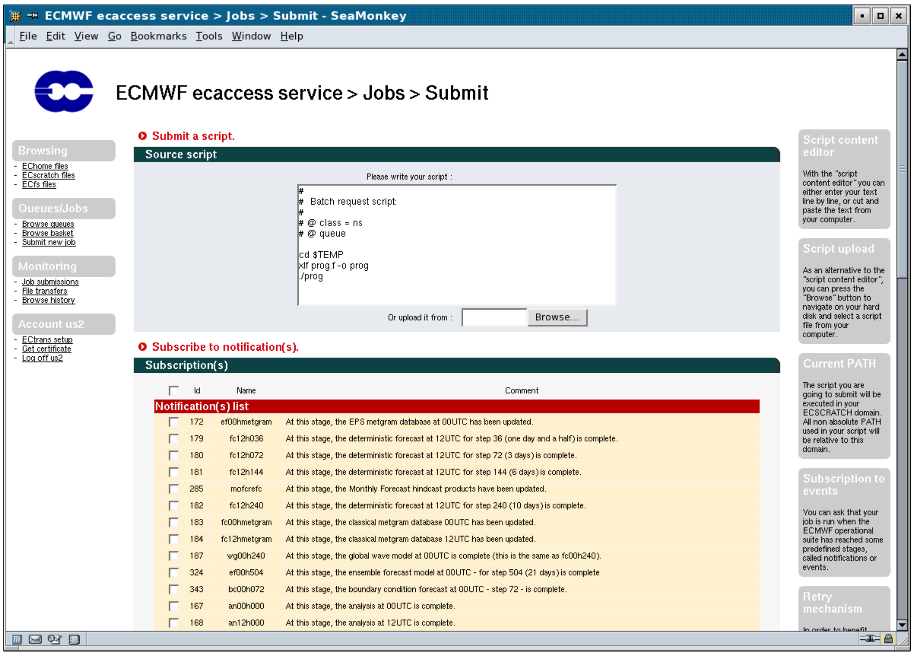
To submit a job to this ECaccess queue, you can access the "job form" by clicking the 'Submit a job to this ECaccess queue" button.

LoadLeveler batch queues

When submitting a job, if you don't select the "No directives" option, ther the LoadLeveler batch queues have to be selected within your input script by providing the apropriate LoadLeveler directives.

You may enter your script in the text area provided or select a script from your computer. Select the target queue ("hpcd" in this case). Note that the batch queue (or class) and other batch directives have to be included in your script. Alternatively, you can inform ECaccess that your script does not contain batch directives. In this case, default values will be used and ECaccess will fully manage your submission. Once your script is read, click the "Submit job" button to send your request to the server.

The list of notifications allows you to attach your job to one event in the ECMWF operational suite. Please refer to www.ecmwf.int/services/computing/docs/ms_items/tc_for_MS.html. for further details.


ECMWF ecaccess service > Jobs > Submit - SeaMonkey
File Edit View Go Bookmarks Tools Window Help
Browse...

ECMWF ecaccess service > Jobs > Submit

Browsing
- EChome files
- ECscratch files
- ECfs files

Queues/Jobs
- Browse queues
- Browse basket
- Submit new job

Monitoring
- Job submissions
- File transfers
- Browse history

Account us2
- ECtrans setup
- Get certificate
- Log off us2

Submit a script.

Source script

Please write your script :

```
#
#  Batch request script:
#
# @ class = ns
# @ queue

cd $TEMP
xlf prog.f -o prog
./prog
```

Or upload it from :

Subscribe to notification(s).

Subscription(s)

☐	Id	Name	Comment
Notification(s) list			
☐	172	ef00hmetgram	At this stage, the EPS metgram database at 00UTC has been updated.
☐	179	fc12h036	At this stage, the deterministic forecast at 12UTC for step 36 (one day and a half) is complete.
☐	180	fc12h072	At this stage, the deterministic forecast at 12UTC for step 72 (3 days) is complete.
☐	181	fc12h144	At this stage, the deterministic forecast at 12UTC for step 144 (6 days) is complete.
☐	285	mofcrefc	At this stage, the Monthly Forecast hindcast products have been updated.
☐	182	fc12h240	At this stage, the deterministic forecast at 12UTC for step 240 (10 days) is complete.
☐	183	fc00hmetgram	At this stage, the classical metgram database 00UTC has been updated.
☐	184	fc12hmetgram	At this stage, the classical metgram database 12UTC has been updated.
☐	187	wg00h240	At this stage, the global wave model at 00UTC is complete (this is the same as fc00h240).
☐	324	ef00h504	At this stage, the ensemble forecast model at 00UTC - for step 504 (21 days) is complete
☐	343	bc00h072	At this stage, the boundary condition forecast at 00UTC - step 72 - is complete.
☐	167	an00h000	At this stage, the analysis at 00UTC is complete.
☐	168	an12h000	At this stage, the analysis at 12UTC is complete.

Script content editor

With the "script content editor" you can either enter your text line by line, or cut and paste the text from your computer.

Script upload

As an alternative to the "script content editor", you can press the "Browse" button to navigate on your hard disk and select a script file from your computer.

Current PATH

The script you are going to submit will be executed in your ECSCRATCH domain. All non absolute PATH used in your script will be relative to this domain.

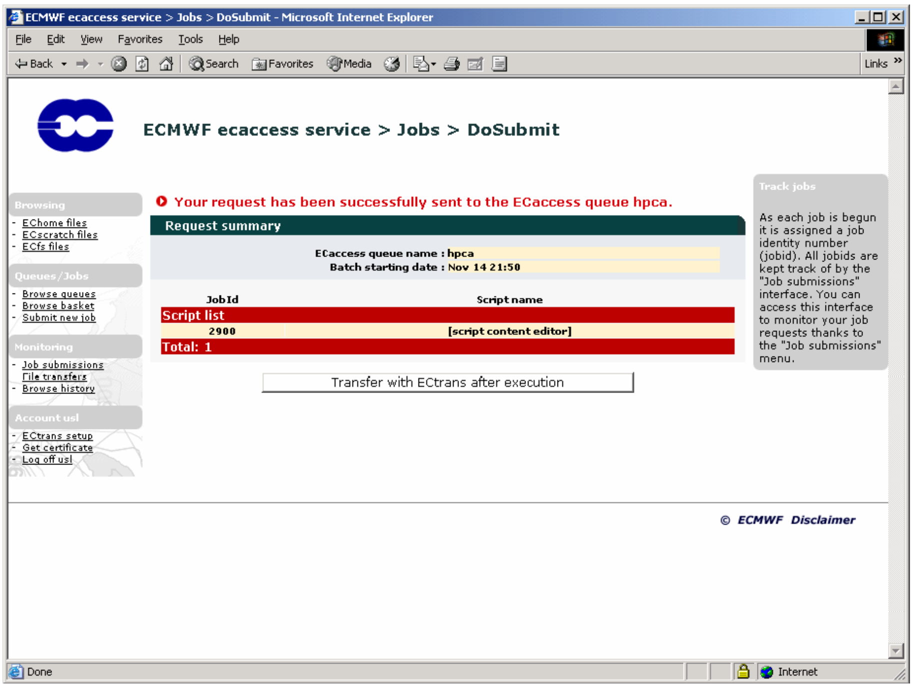
Subscription to events

You can ask that your job is run when the ECMWF operational suite has reached some predefined stages, called notifications or events.

Retry mechanism

In order to benefit

Once the job is submitted, a summary screen gives you the job identifier number of your new job request. It can be used to reference the submitted job using the monitoring interface (described in the next section). If you want to arrange a secure file transfer of the result, click the “Transfer with Ectrans after execution” button.


ECMWF ecaccess service > Jobs > DoSubmit - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Done
Internet
Transfer with ECtrans after execution

ECMWF ecaccess service > Jobs > DoSubmit

Browsing
- EChome files
- ECscratch files
- ECfs files

Queues/Jobs
- Browse queues
- Browse basket
- Submit new job

Monitoring
- Job submissions
- File transfers
- Browse history

Account usl
- ECtrans setup
- Get certificate
- Log off usl

Your request has been successfully sent to the ECaccess queue hpca.

Request summary

ECaccess queue name : hpca
Batch starting date : Nov 14 21:50

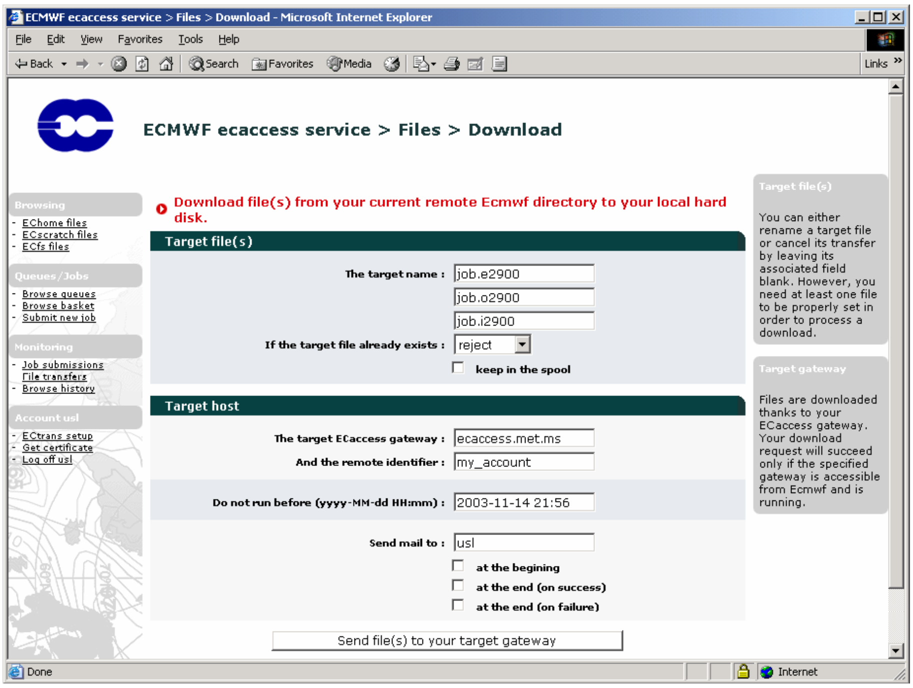
JobId	Script name
Script list	
2900	[script content editor]
Total: 1	

Track jobs

As each job is begun it is assigned a job identity number (jobid). All jobids are kept track of by the "Job submissions" interface. You can access this interface to monitor your job requests thanks to the "Job submissions" menu.

© ECMWF Disclaimer

If required, modify the default values (gateway name, user identifier) and specify the erase option of the secure file transfer (erase option is discussed in section 4.2). Then click the “Send file(s) to your target host” to proceed.



ECMWF ecaccess service > Files > Download

Download file(s) from your current remote Ecmwf directory to your local hard disk.

Target file(s)

The target name : job.e2900
job.o2900
job.i2900

If the target file already exists : reject

□ keep in the spool

Target host

The target ECaccess gateway : ecaccess.met.ms

And the remote identifier : my_account

Do not run before (yyyy-MM-dd HH:mm) : 2003-11-14 21:56

Send mail to : usl

□ at the begining

□ at the end (on success)

□ at the end (on failure)

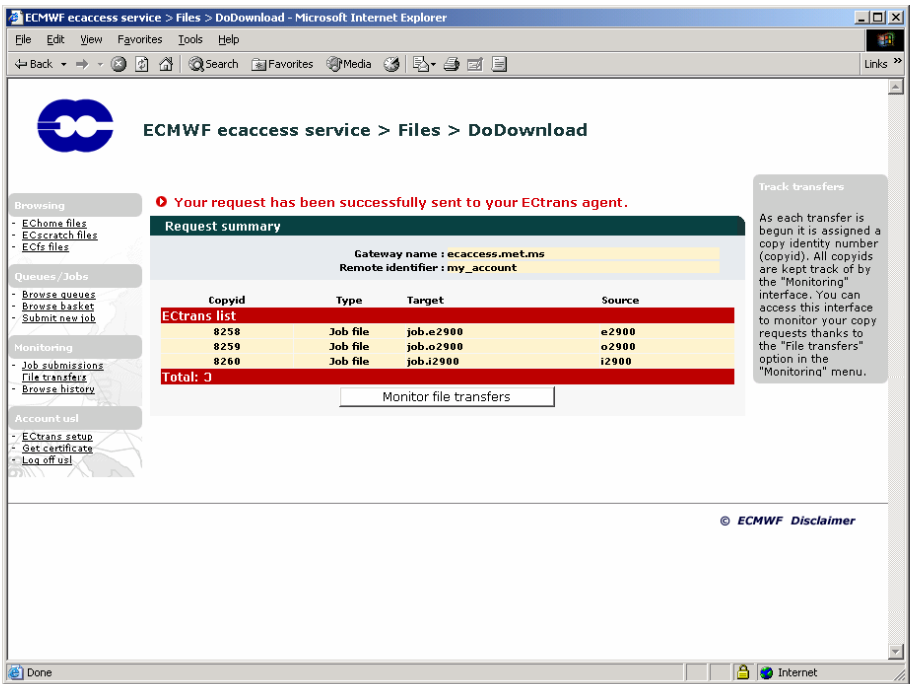
Target file(s)

You can either rename a target file or cancel its transfer by leaving its associated field blank. However, you need at least one file to be properly set in order to process a download.

Target gateway

Files are downloaded thanks to your ECaccess gateway. Your download request will succeed only if the specified gateway is accessible from Ecmwf and is running.

Once it is spooled, a summary screen gives you the copy identifier number of your new transfer request. It can be used to reference the secure file transfer using the monitoring interface (described in the next section.



ECMWF ecaccess service > Files > DoDownload

Your request has been successfully sent to your ECtrans agent.

Request summary

Gateway name : ecaccess.met.ms
Remote identifier : my_account

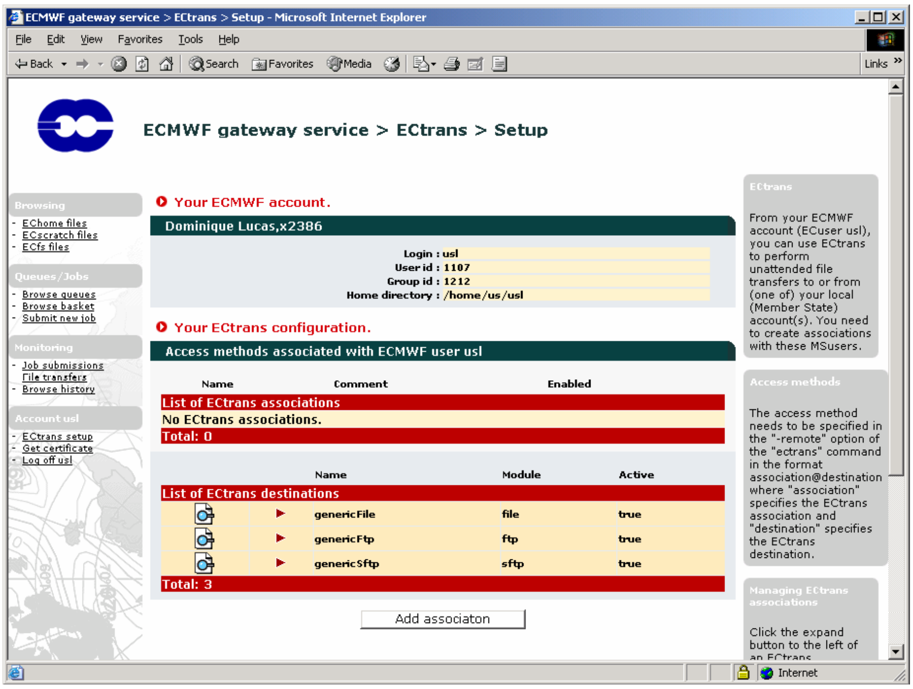
Copyid	Type	Target	Source
ECtrans list			
8258	Job file	job.e2900	e2900
8259	Job file	job.o2900	o2900
8260	Job file	job.i2900	i2900
Total: 3			

Track transfers

As each transfer is begun it is assigned a copy identity number (copyid). All copyids are kept track of by the "Monitoring" interface. You can access this interface to monitor your copy requests thanks to the "File transfers" option in the "Monitoring" menu.

6.4 Ectrans setup

Before being able to launch unattended transfers from ECMWF (section 4) back to your site, using the command ectrans, you will have to configure ectrans association between your ECMWF User ID and the destination system and User. This is done through the web interface, by clicking “ECtrans setup” from the lower left panel.



ECMWF gateway service > ECtrans > Setup

Your ECMWF account.

Dominique Lucas,x2386

Login : usl
User id : 1107
Group id : 1212
Home directory : /home/us/usl

Your ECtrans configuration.

Access methods associated with ECMWF user usl

Name	Comment	Enabled
List of ECtrans associations		
No ECtrans associations.		
Total: 0		

		Name	Module	Active
List of ECtrans destinations				
		genericFile	file	true
		genericFtp	ftp	true
		genericSftp	sftp	true
Total: 3				

ECtrans

From your ECMWF account (ECuser usl), you can use ECtrans to perform unattended file transfers to or from (one of) your local (Member State) account(s). You need to create associations with these MSusers.

Access methods

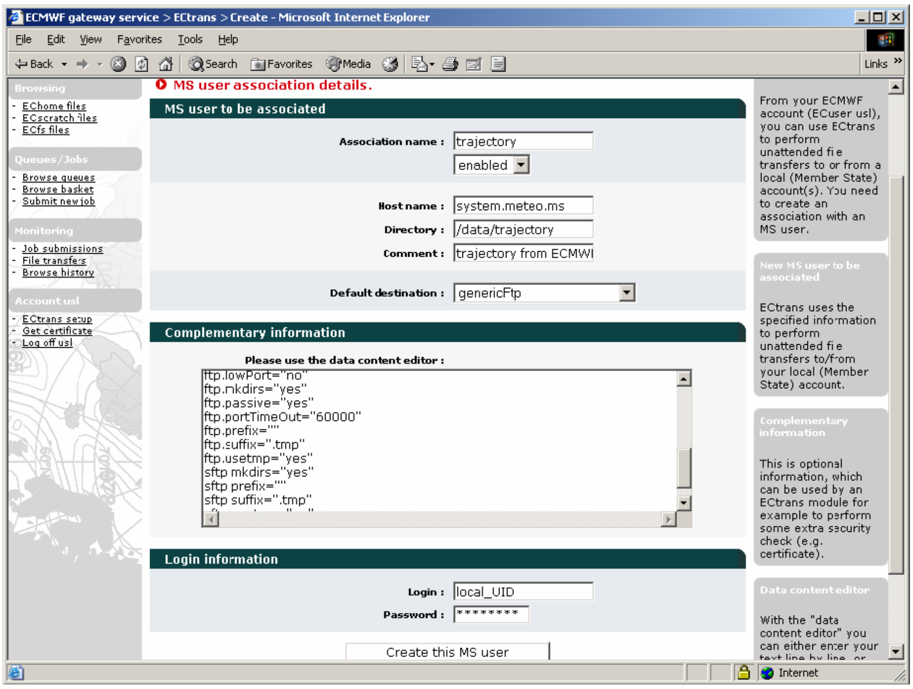
The access method needs to be specified in the "-remote" option of the "ectrans" command in the format association@destination where "association" specifies the ECtrans association and "destination" specifies the ECtrans destination.

Managing ECtrans associations

Click the expand button to the left of an ECtrans

To create a new association, click the “Add association” button. Choose an Association name, “trajectory” in the example below. This is the name that will be used as “msuser” with the ectrans command. Fill in the remaining info, giving the required information on your local system.

In the example below, we create an association named trajectory that will be used to transfer files using ftp by default to a local system named “system.meteo.ms” as a user `local_UID`. The data transferred will be written into the directory /data/trajectory. The local files will have a temporary suffix “.tmp” added to their names during the transfer. Note that you can change the configuration of the ectrans association by modifying the options given in the window titled “Complementary information”:



MS user association details.

MS user to be associated

Association name : trajectory

enabled

Host name : system.meteo.ms

Directory : /data/trajectory

Comment : trajectory from ECMWI

Default destination : genericFtp

Complementary information

Please use the data content editor :

```
ftp.lowPort="no"
ftp.mkdirs="yes"
ftp.passive="yes"
ftp.portTimeOut="60000"
ftp.prefix=""
ftp.suffix=".tmp"
ftp.usetmp="yes"
sftp mkdirs="yes"
sftp prefix=""
sftp suffix=".tmp"
```

Login information

Login : local_UID

Password : ********

From your ECMWF account (ECuser usl), you can use ECtrans to perform unattended file transfers to or from a local (Member State) account(s). You need to create an association with an MS user.

New MS user to be associated

ECtrans uses the specified information to perform unattended file transfers to/from your local (Member State) account.

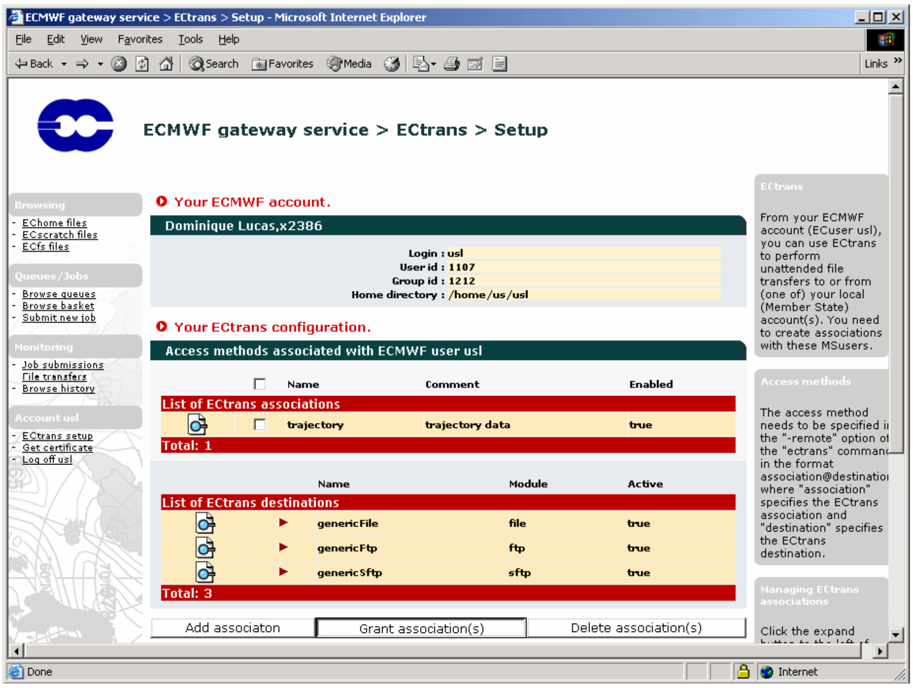
Complementary information

This is optional information, which can be used by an ECtrans module for example to perform some extra security check (e.g. certificate).

Data content editor

With the "data content editor" you can either enter your

When you have entered all the information for your association, click the button “Create this MS user”. A new association has been defined for you. Please note that (between all users) an association name can be defined only once per gateway. You can define more associations, e.g. to transfer files from ECMWF to different systems or other local UIDs. You can also allow other users at ECMWF to transfer files with ectrans to your association. To do this, click the “Grant Association(s)” button:



ECMWF gateway service > ECtrans > Setup

Your ECMWF account.

Dominique Lucas,x2386

Login : usl
User id : 1107
Group id : 1212
Home directory : /home/us/usl

Your ECtrans configuration.

Access methods associated with ECMWF user usl

	☐	Name	Comment	Enabled
List of ECtrans associations				
	☐	trajectory	trajectory data	true
Total: 1				

		Name	Module	Active
List of ECtrans destinations				
	▶	genericFile	file	true
	▶	genericFtp	ftp	true
	▶	genericSftp	sftp	true
Total: 3				

ECtrans

From your ECMWF account (ECuser usl), you can use ECtrans to perform unattended file transfers to or from (one of) your local (Member State) account(s). You need to create associations with these MSusers.

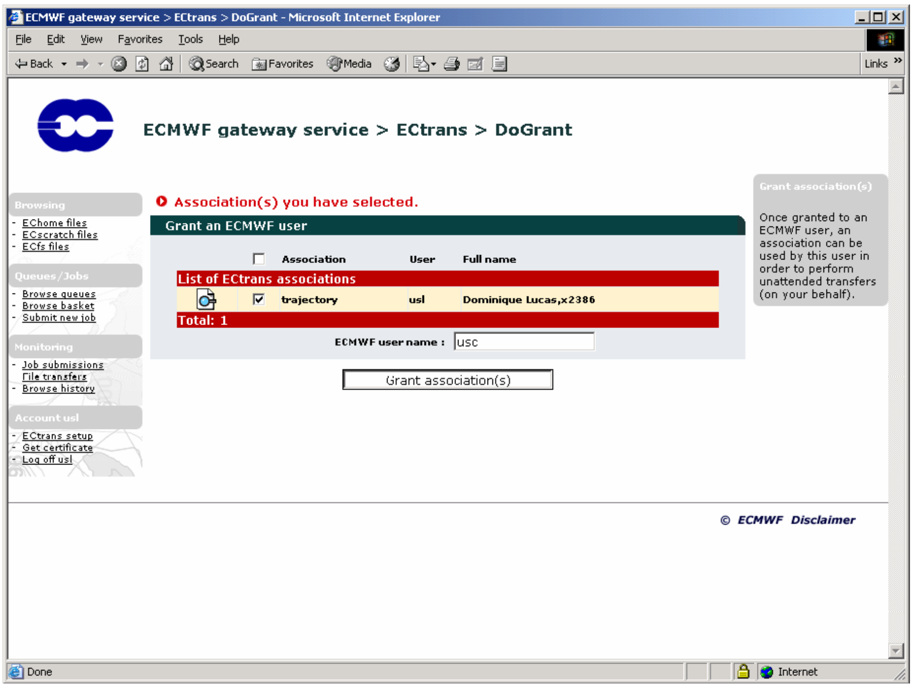
Access methods

The access method needs to be specified i the "-remote" option o the "ectrans" comman in the format association@destinatio where "association" specifies the ECtrans association and "destination" specifies the ECtrans destination.

Managing ECtrans associations

Click the expand

Select the association to which you want to give access to another user. Enter the ECMWF user name. Then grant the association.



ECMWF gateway service > ECtrans > DoGrant

Association(s) you have selected.

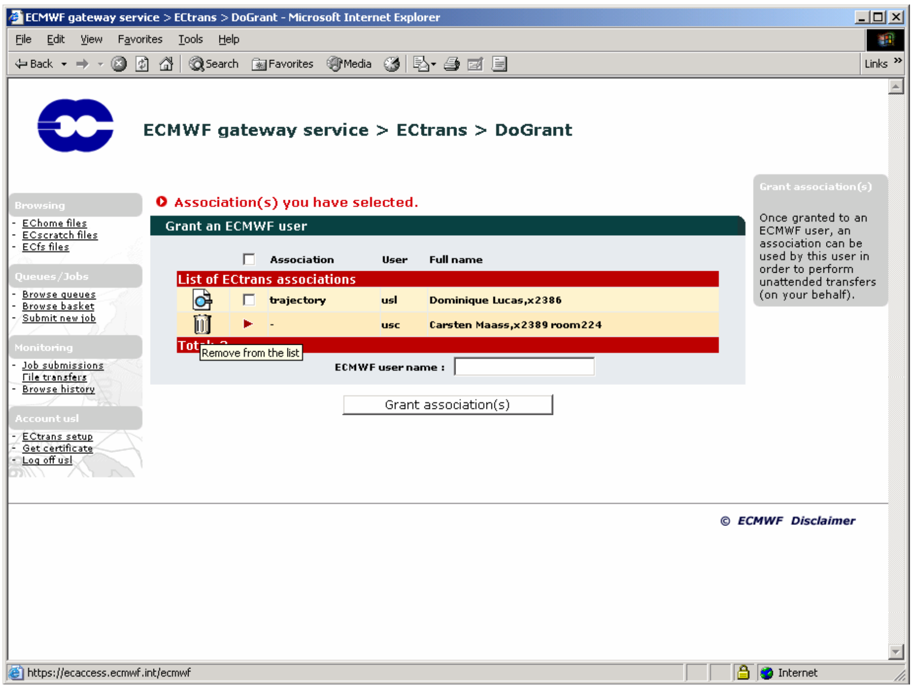
Grant an ECMWF user

	□ Association	User	Full name
List of ECtrans associations			
	☑ trajectory	usl	Dominique Lucas,x2386
Total: 1			

ECMWF user name : usc

Once granted to an ECMWF user, an association can be used by this user in order to perform unattended transfers (on your behalf).

The UID and name of the person you have given access to the destination is now added to the list. To remove an entry from the list, click the “Remove from the list” icon on the left:



ECMWF gateway service > ECtrans > DoGrant

Association(s) you have selected.

Grant an ECMWF user

	□ Association	User	Full name
List of ECtrans associations			
	□ trajectory	usl	Dominique Lucas,x2386
	► -	usc	Carsten Maass,x2389 room224
Total: 2			

ECMWF user name :

Once granted to an ECMWF user, an association can be used by this user in order to perform unattended transfers (on your behalf).

6.5 NX service

A service using the NX technology allows users to run at ECMWF X Window based applications like Metview, XCdp, or a simple xterm.

The easiest way to use this service is via a web browser, see section 6.5.1.

It is also possible to connect using a standalone NX client application completely independent of any web browser, see section 6.5.2. A similar service is available through the ECaccess gateway “msaccess.ecmwf.int” and through your local gateway provided that you have installed the ECaccess gateway v3.3.0 at least.

NX allows you to run remote X Window sessions even across slow or low-bandwidth network connections, making it possible to start sessions from clients running on Windows, Linux, Mac OS X and Solaris platforms.

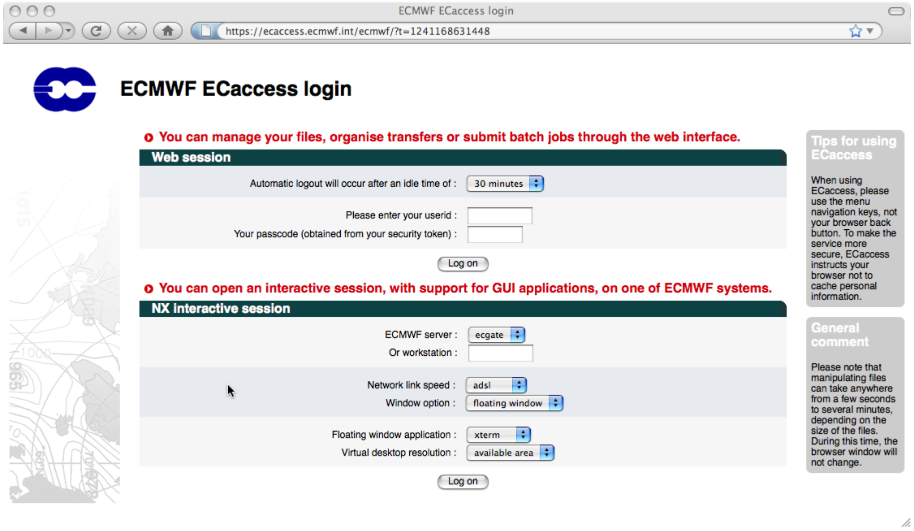
Thanks to exclusive X protocol compression techniques and an integrated set of proxy agents, NX improves the power of the X Window System to transparently run graphical desktops and applications through the network. Even on slow or low-bandwidth network connections, you can get a fast response thanks to the NX lazy encoding algorithm and NX capability to automatically tune itself to network bandwidth and latency parameters.

In addition NX allows having both standalone X terminal and “virtual desktops” independent of the web browser session used to start them. The windows can be minimised and the web browser can even be terminated.

For more information on NX, please see www.nomachine.com/documents.php.

6.5.1 How to connect using a web browser

The easiest way to connect to ECMWF using the NX service is simply to go to: `http://ecaccess.ecmwf.int/`. You will get to a page like:



ECMWF ECaccess login

https://ecaccess.ecmwf.int/ecmwf/?t=1241168631448

ECMWF ECaccess login

You can manage your files, organise transfers or submit batch jobs through the web interface.

Web session

Automatic logout will occur after an idle time of : 30 minutes

Please enter your userid :

Your passcode (obtained from your security token) :

Log on

You can open an interactive session, with support for GUI applications, on one of ECMWF systems.

NX interactive session

ECMWF server : ecgate

Or workstation :

Network link speed : adsl

Window option : floating window

Floating window application : xterm

Virtual desktop resolution : available area

Log on

Tips for using ECaccess

When using ECaccess, please use the menu navigation keys, not your browser back button. To make the service more secure, ECaccess instructs your browser not to cache personal information.

General comment

Please note that manipulating files can take anywhere from a few seconds to several minutes, depending on the size of the files. During this time, the browser window will not change.

Using various drop down menus in the *bottom part of the page* you will be able to select the type of NX session you want to establish. Please note that your web browser needs to be Java enabled.

You can connect to both ecgate and the supercomputer using the drop down menu “ECMWF server”.

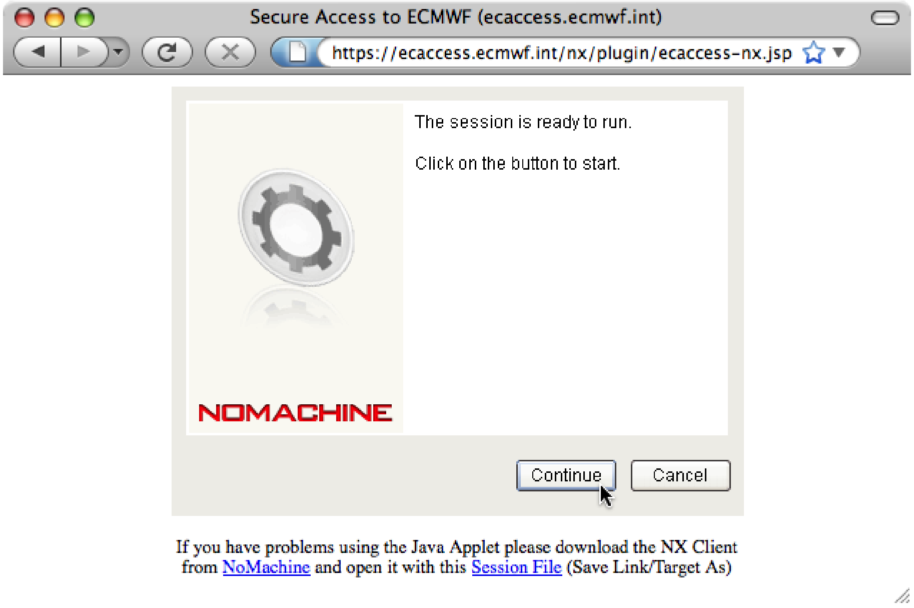
You can select the type of network link you are using with the menu “Network link speed”. This will select a number of options which should by optimal for your configuration.

You can select the type of window you want to have using the “Window option” menu: if you select “floating window” you will get a single X Window application like xterm or Metview (you can choose the application using the next menu). If, instead, you select “virtual desktop” you will get a fully working desktop using the WindowMaker window manager. In this case you can select the “Virtual desktop resolution” to be either “available area” or “full screen”.

6.5.2 *Example of session starting a standalone xterm on the supercomputer*

In this case you need to select “c1a” as “ECMWF server”, specify your type of network link (you can leave this to the default “adsl”), then select “floating window” as “Window option, leave the default “Floating window application” to “xterm” and press “Log on”.

This, after some windows warning about certificates and ssh key which you need to accept, will display the following page:

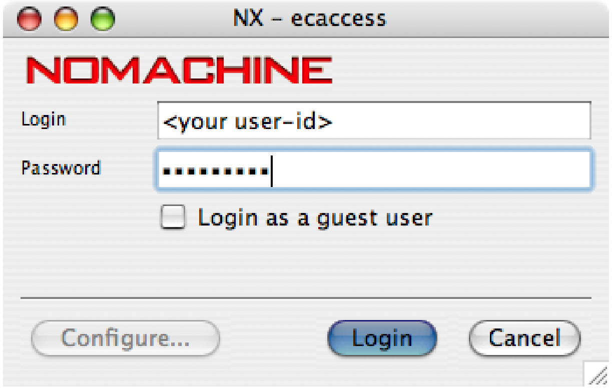

Secure Access to ECMWF (ecaccess.ecmwf.int)
https://ecaccess.ecmwf.int/nx/plugin/ecaccess-nx.jsp
NOMACHINE
Continue
Cancel

The session is ready to run.

Click on the button to start.

If you have problems using the Java Applet please download the NX Client from NoMachine and open it with this Session File (Save Link/Target As)

You will need to click on the “Continue” button to start the NX connection. The following window will appear:

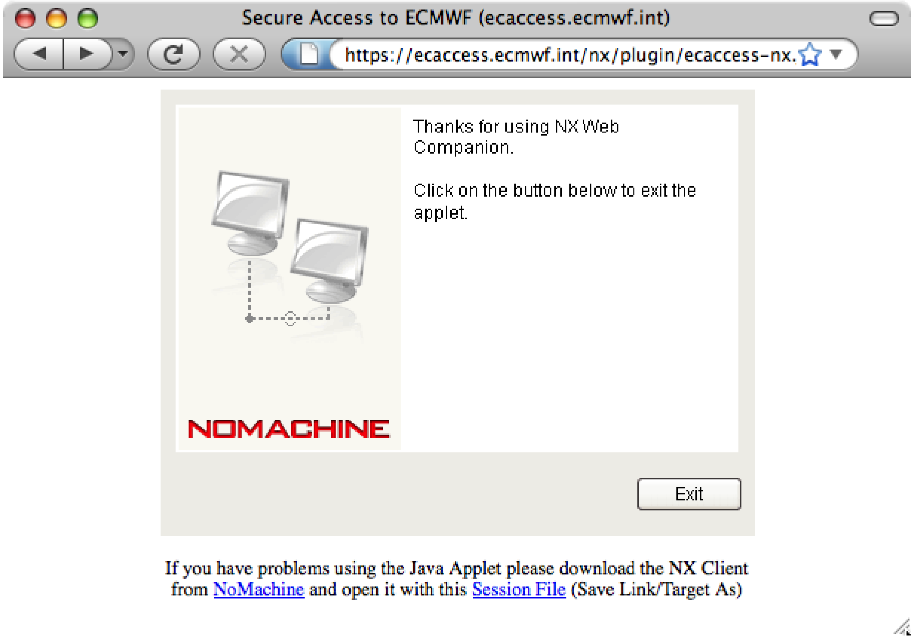


Login <your user-id>

Password ••••••••••

□ Login as a guest user

This window allows you to enter your userid and corresponding *passcode generated by your security token*. After entering the appropriate information click on “Login” to proceed. The Java applet in the web browser will display various messages detailing the progress of the connection to ECMWF (depending on your firewall setup you may get various warning messages: you will need to authorise all sessions from anything related to NX - nxclient, nxauth, nxssh, etc) until this will be displayed in your browser:



Secure Access to ECMWF (ecaccess.ecmwf.int)

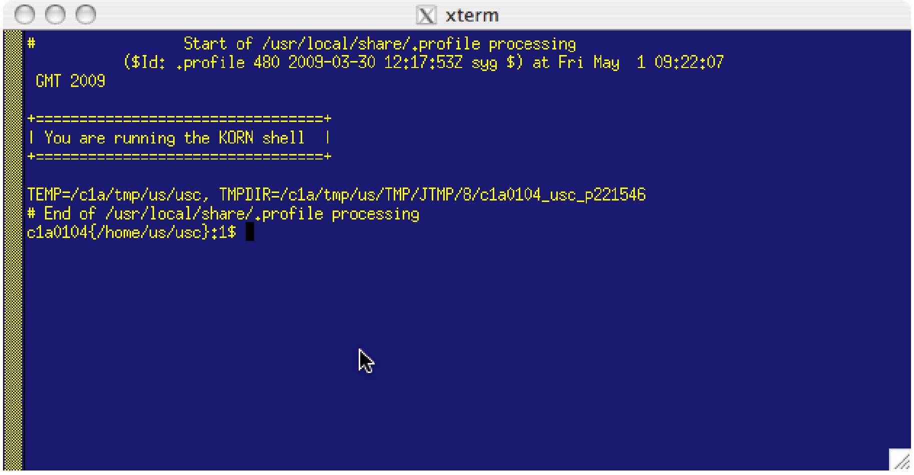
https://ecaccess.ecmwf.int/nx/plugin/ecaccess-nx.

Thanks for using NX Web Companion.

Click on the button below to exit the applet.

If you have problems using the Java Applet please download the NX Client from NoMachine and open it with this Session File (Save Link/Target As)

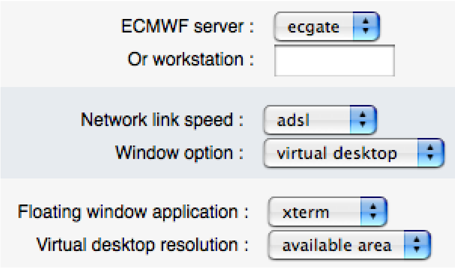
The application you have requested to start, in this case an “xterm”, should also start as a separate X based window. You can now minimise (or even close) your web browser and start using your xterm.



```
#                  Start of /usr/local/share/.profile processing
           ($Id: .profile 480 2009-03-30 12:17:53Z syg $) at Fri May  1 09:22:07
 GMT 2009

+================================+
| You are running the KORN shell  |
+================================+

TEMP=/c1a/tmp/us/usc, TMPDIR=/c1a/tmp/us/TMP/JTMP/8/c1a0104_usc_p221546
# End of /usr/local/share/.profile processing
c1a0104{/home/us/usc}:1$
```

6.5.3 *Example of session starting a virtual desktop on ecgate*

In this case select the following (for the link speed you can leave the default “adsl”):

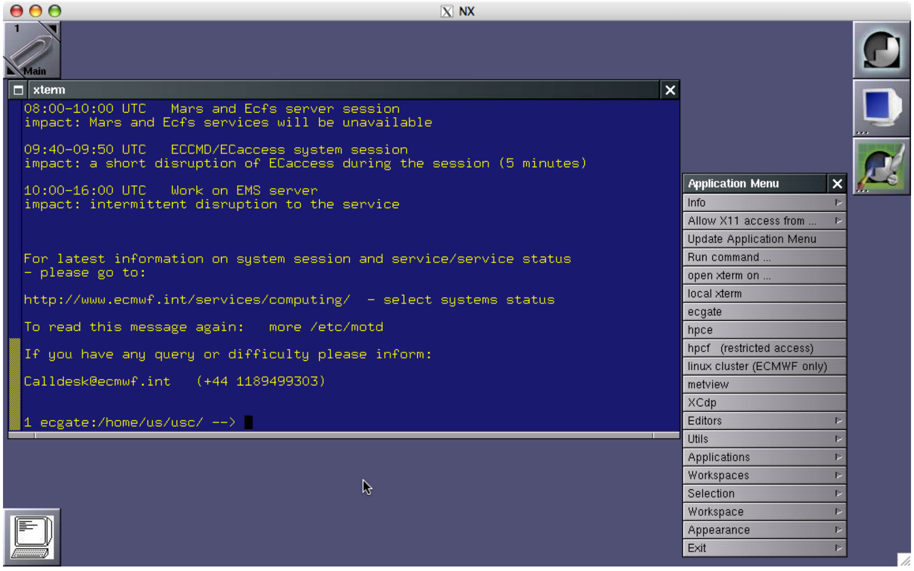


ECMWF server : ecgate
Or workstation :

Network link speed : adsl
Window option : virtual desktop

Floating window application : xterm
Virtual desktop resolution : available area

and press “Log on”. The login process will be the same as the one described in the previous example but at the end the following window will appear:



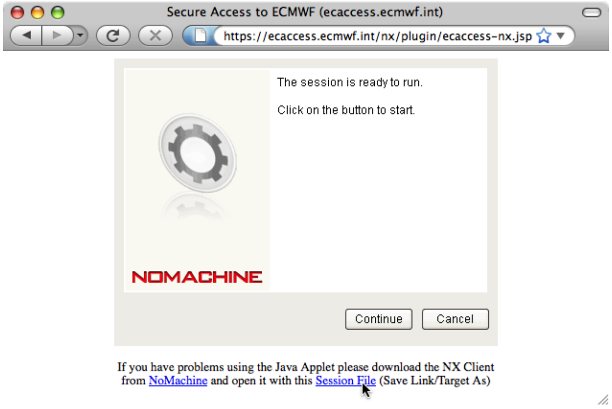
```
08:00-10:00 UTC   Mars and Ecfs server session
impact: Mars and Ecfs services will be unavailable

09:40-09:50 UTC   ECCMD/ECaccess system session
impact: a short disruption of ECaccess during the session (5 minutes)

10:00-16:00 UTC   Work on EMS server
impact: intermittent disruption to the service



For latest information on system session and service/service status
- please go to:

http://www.ecmwf.int/services/computing/  - select systems status

To read this message again:   more /etc/motd

If you have any query or difficulty please inform:

Calldesk@ecmwf.int   (+44 1189499303)


1 ecgate:/home/us/usc/ -->
```

Figure 2: Virtual desktop on ecgate started using NX.

The window manager available on this desktop is called WindowMaker. By right clicking on the mouse you will get an Application Menu which allows you to start an xterm or other X based applications. The main desktop window is a standalone X Window and can be minimised. If you prefer, you can start a virtual desktop in full screen mode by choosing the “Virtual desktop resolution” option “full screen”. Section 6.5.5 below describes the usage of WindowMaker in more detail.

6.5.4 How to connect using a standalone NX client

In addition to using the web browser based access to ECMWF via NX described previously, you can also download a standalone NX client. To do this, go to www.nomachine.com/download.php and select the NX client for your platform. The installation is quite straightforward and is described in more detail at www.nomachine.com/documents/client/install.php. You can then use the “Download session file” option available through the web interface:



Secure Access to ECMWF (ecaccess.ecmwf.int)

https://ecaccess.ecmwf.int/nx/plugin/ecaccess-nx.jsp

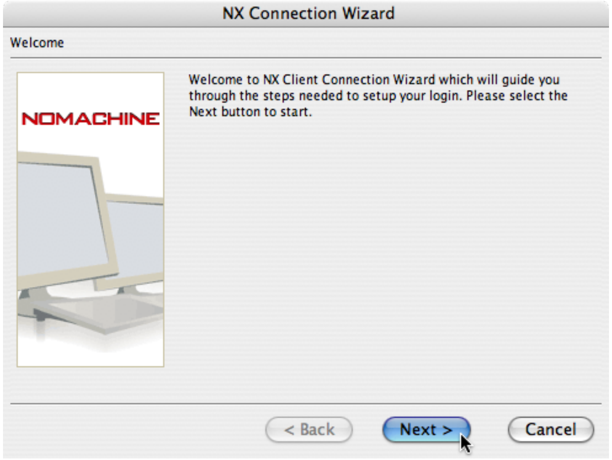
The session is ready to run.

Click on the button to start.

If you have problems using the Java Applet please download the NX Client from NoMachine and open it with this Session File (Save Link/Target As)

This URL allows you to download a complete configuration file which can be used with your standalone NX client. You can have multiple configuration files, say one for a standalone xterm on ecgate and another one for a full virtual desktop still on ecgate, and then select the appropriate one from your NX client.

Alternatively, you can use the NX client “Wizard” to setup your own configuration as described in the NX client documentation available at www.nomachine.com/documents/configuration/client-guide.php We recommend using this option for advanced users only. We also recommend that you first look at one of the configuration files which you can obtain by downloading the “session file”. The first time you start the NX client the following window will appear:

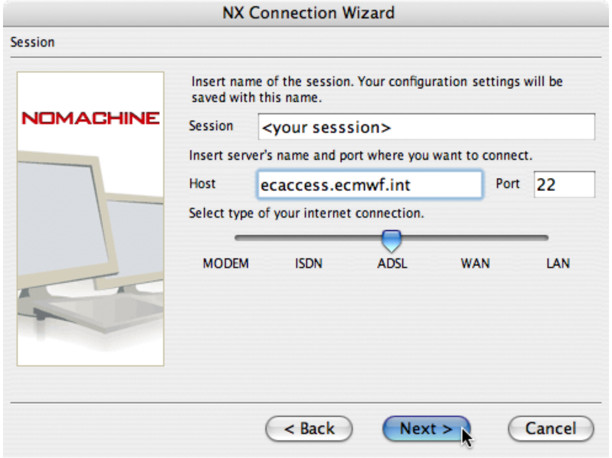


NX Connection Wizard

Welcome

Welcome to NX Client Connection Wizard which will guide you through the steps needed to setup your login. Please select the Next button to start.

You will have to click “Next” where you will be asked to enter the name of your NX session (in the example `<your session>`) and the host to connect to. You will have to enter the ECaccess host name “ecaccess.ecmwf.int” as host:



Insert name of the session. Your configuration settings will be saved with this name.

Session: <your sesssion>

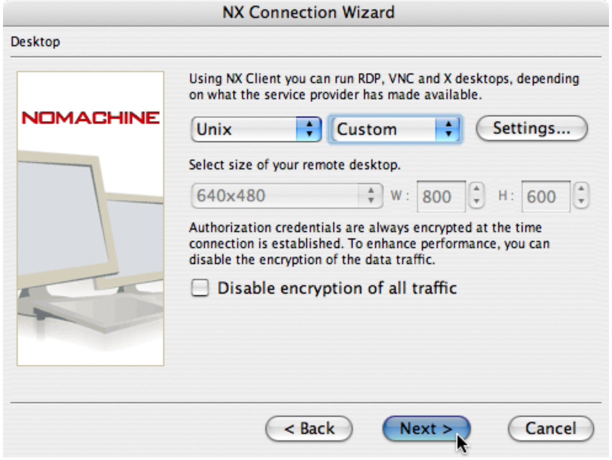
Insert server's name and port where you want to connect.

Host: ecaccess.ecmwf.int Port: 22

Select type of your internet connection.

MODEM ISDN ADSL WAN LAN

You will then get the following window where you can choose you type of desktop. You will need to choose “Unix” and “Custom”:



Using NX Client you can run RDP, VNC and X desktops, depending on what the service provider has made available.

Unix | Custom

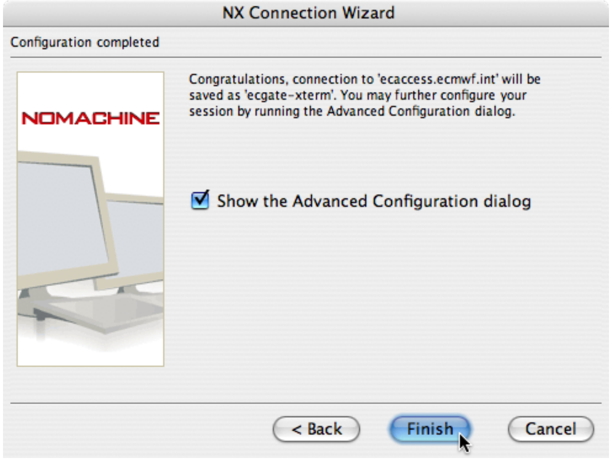
Select size of your remote desktop.

640x480 W: 800 H: 600

Authorization credentials are always encrypted at the time connection is established. To enhance performance, you can disable the encryption of the data traffic.

□ Disable encryption of all traffic

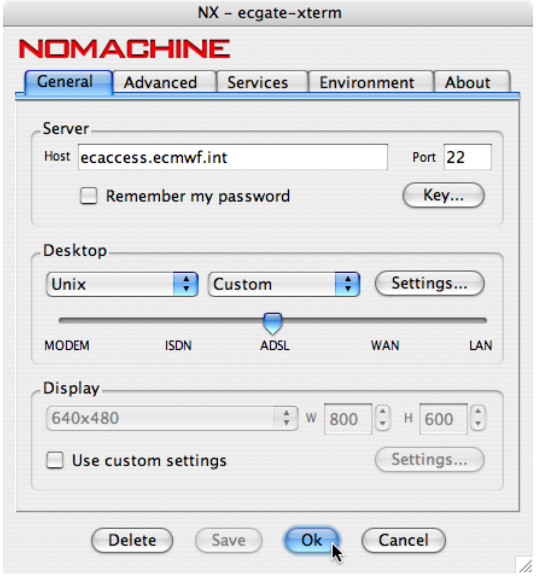
Click on “Next” to get the following window:



Congratulations, connection to 'ecaccess.ecmwf.int' will be saved as 'ecgate-xterm'. You may further configure your session by running the Advanced Configuration dialog.

☑ Show the Advanced Configuration dialog

Check the “Show the Advanced Configuration dialog” box and click the Finish button. You will get the following window:



NX – ecgate-xterm

NOMACHINE

Server

Host ecaccess.ecmwf.int Port 22

□ Remember my password

Desktop

Unix Custom

Display

640x480 W 800 H 600

□ Use custom settings

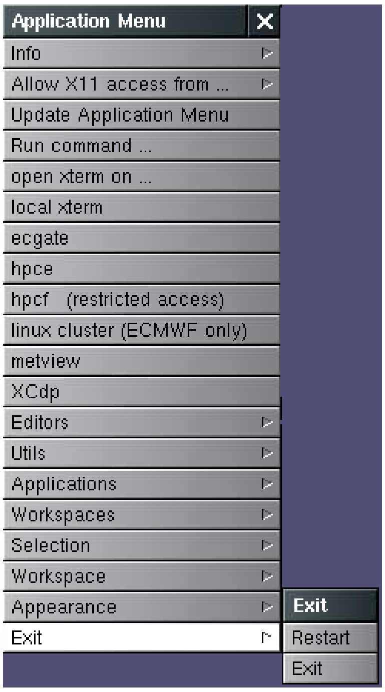
If you then click “Ok” you will be able to start your session. In this case you will get a standalone xterm on ecgate. Depending on your firewall setup you may get various warning messages. You will need to authorise all sessions from anything related to NX (nxclient, nxauth, nxssh, etc).

6.5.5 WindowMaker overview

WindowMaker is a popular window manager for the X Window System, allowing graphical applications to be run on Unix-like operating-systems. It is designed to emulate NeXT’s GUI as an OpenStep-compatible environment and has been described as “one of the most useful and universal window managers available.” WindowMaker has a reputation for being fast, efficient and highly stable and is very popular among open source solutions for use on both newer and older machines. More information on WindowMaker can be found at http://en.wikipedia.org/wiki/Window_Maker and www.windowmaker.info.

WindowMaker is the window manager which is used when you connect with NX to either ecgate or the supercomputer and select the “virtual desktop” option. For example, when you connect to ecgate using the virtual desktop you will get a desktop as shown in figure 2.

The main customisation which has been implemented is a specific “Application Menu” which you can obtain when right-click (opposite mouse button for left-handed mouse) on the desktop. The menus on ecgate and the supercomputer are designed to be very similar with the one on ecgate offering more choices regarding the available applications. The usage of the menus should be quite straightforward. To terminate a WindowMaker session you need to select the “Exit” option from the menu:


Application Menu
Info
Allow X11 access from ...
Update Application Menu
Run command ...
open xterm on ...
local xterm
ecgate
hpce
hpcf (restricted access)
linux cluster (ECMWF only)
metview
XCdp
Editors
Utils
Applications
Workspaces
Selection
Workspace
Appearance
Exit
Exit
Restart
Exit

7 Monitoring tools

The purpose of the monitoring interface is to provide Member States users with information concerning:

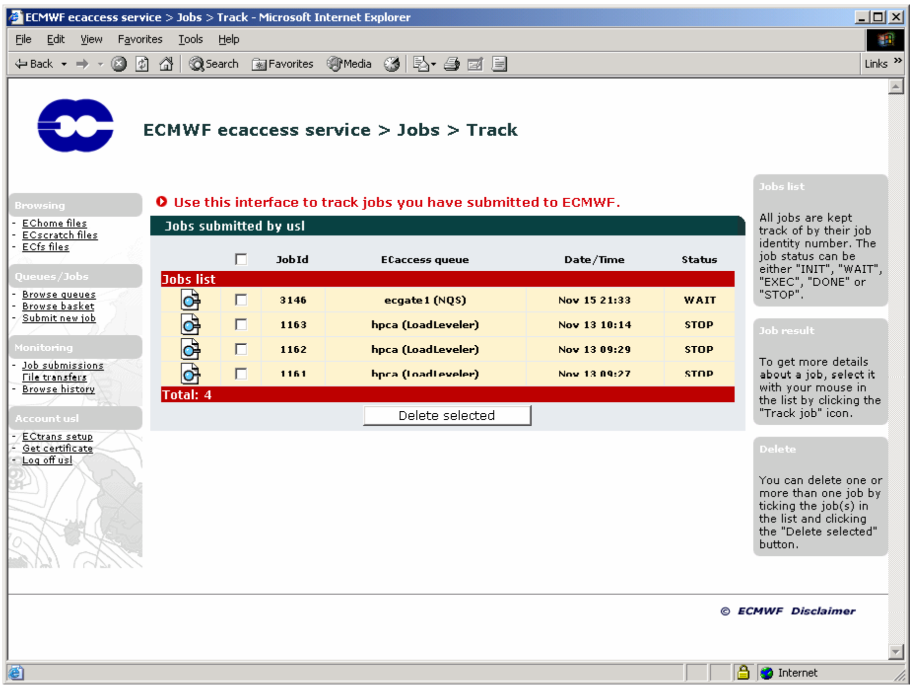
- Job requests referenced by the job identifier number, which is returned by the `ecaccess-job-submit` command (see section 5).
- Secure file transfer requests referenced by the copy identifier number, which is returned by the `ecaccess-ectrans-` command (see section 5) or the `ectrans` command (see section 4.2).

The monitoring interface is accessible through the ECaccess HTTP/S plugin, which supports the interactive method of authentication described in section 3.

Procedures to login and use this plugin are discussed in the previous section. The following discussion assumes that you are connected.

7.1 Monitoring batch job submissions

To access this interface, select the option “Job submissions” in the “Monitoring” menu.



ECMWF ecaccess service > Jobs > Track

Use this interface to track jobs you have submitted to ECMWF.

Jobs submitted by usl

	□	JobId	ECaccess queue	Date/Time	Status
Jobs list					
	□	3146	ecgate1 (NQS)	Nov 15 21:33	WAIT
	□	1163	hpca (LoadLeveler)	Nov 13 10:14	STOP
	□	1162	hpca (LoadLeveler)	Nov 13 09:29	STOP
	□	1161	hpca (LoadLeveler)	Nov 13 09:27	STOP
Total: 4					

Delete selected

Jobs list

All jobs are kept track of by their job identity number. The job status can be either "INIT", "WAIT", "EXEC", "DONE" or "STOP".

Job result

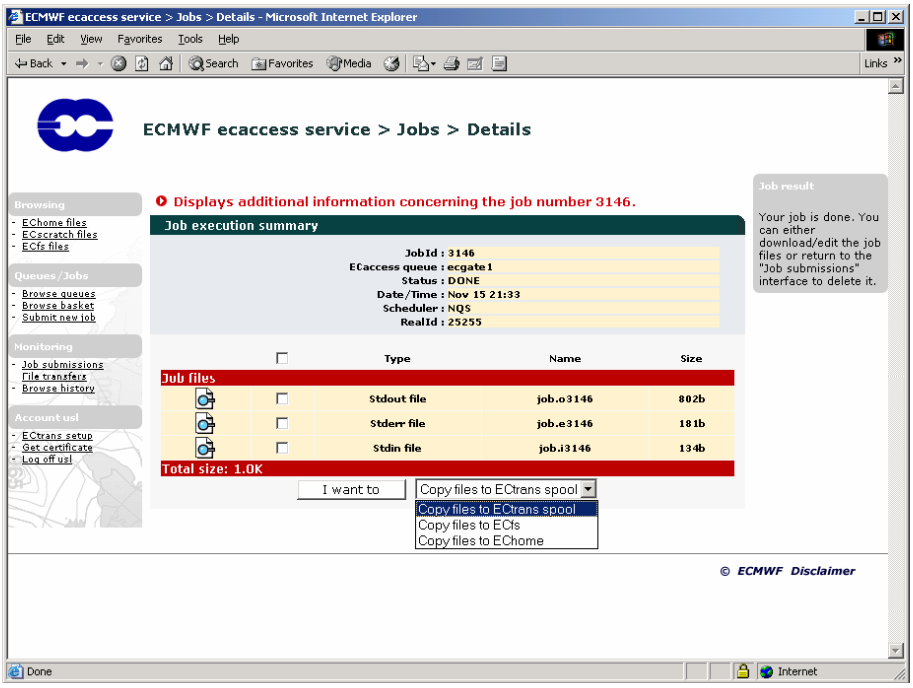
To get more details about a job, select it with your mouse in the list by clicking the "Track job" icon.

Delete

You can delete one or more than one job by ticking the job(s) in the list and clicking the "Delete selected" button.

© ECMWF Disclaimer

Your submitted jobs are listed. You are informed of the status of the jobs (meanings of the different values are provided in the help tips). You can use the “show details” icon to get more information about a job. For example, if a job submission failed, you can get the reason for this failure by looking at the job details. Once a job is marked as “DONE” you can select it with your mouse to see its output.



ECMWF ecaccess service > Jobs > Details

Displays additional information concerning the job number 3146.

Job execution summary

JobId : 3146
ECaccess queue : ecgate1
Status : DONE
Date/Time : Nov 15 21:33
Scheduler : NQS
RealId : 25255

Job result

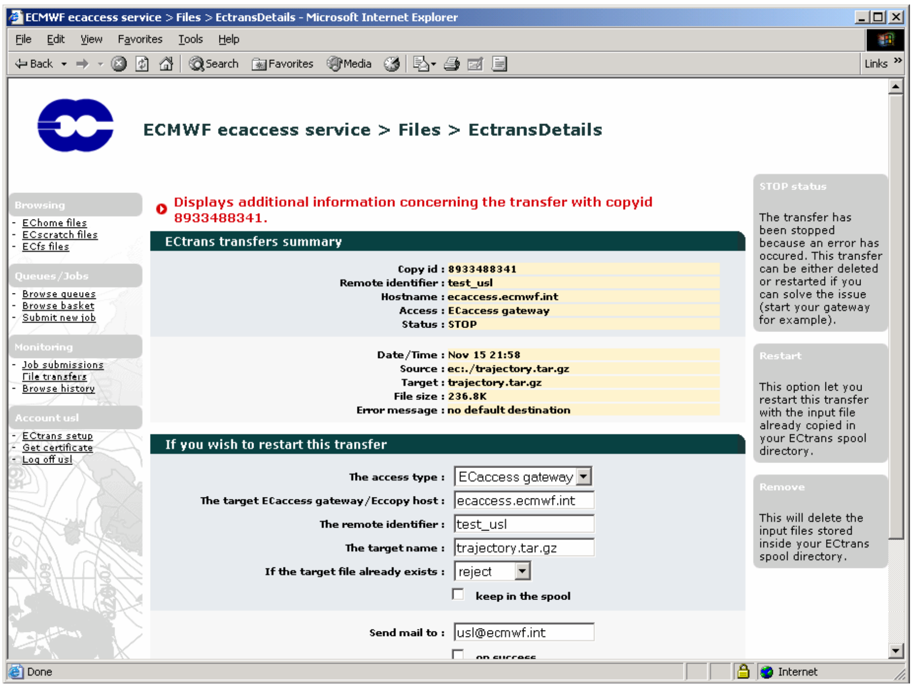
Your job is done. You can either download/edit the job files or return to the "Job submissions" interface to delete it.

	□	Type	Name	Size
Job files				
	□	Stdout file	job.o3146	802b
	□	Stderr file	job.e3146	181b
	□	Stdin file	job.i3146	134b
Total size: 1.0K				

I want to — Copy files to ECtrans spool
Copy files to ECtrans spool
Copy files to ECfs
Copy files to EChome

© ECMWF Disclaimer

You can view the content of the output, error or input files associated with the job. You can also choose not to consult these files on-line but copy them to one of your directories or get them using the secure file transfer feature. Use the “I want to” button for this purpose. To edit one of them, just click the edit icon on the corresponding line.



ECMWF ecaccess service > Files > EctransDetails

Displays additional information concerning the transfer with copyid 8933488341.

ECtrans transfers summary

Copy id : 8933488341
Remote identifier : test_usl
Hostname : ecaccess.ecmwf.int
Access : ECaccess gateway
Status : STOP

Date/Time : Nov 15 21:58
Source : ec:./trajectory.tar.gz
Target : trajectory.tar.gz
File size : 236.8K
Error message : no default destination

If you wish to restart this transfer

The access type : ECaccess gateway
The target ECaccess gateway/Eccopy host : ecaccess.ecmwf.int
The remote identifier : test_usl
The target name : trajectory.tar.gz
If the target file already exists : reject
□ keep in the spool

Send mail to : usl@ecmwf.int
□ on success

STOP status

The transfer has been stopped because an error has occured. This transfer can be either deleted or restarted if you can solve the issue (start your gateway for example).

Restart

This option let you restart this transfer with the input file already copied in your ECtrans spool directory.

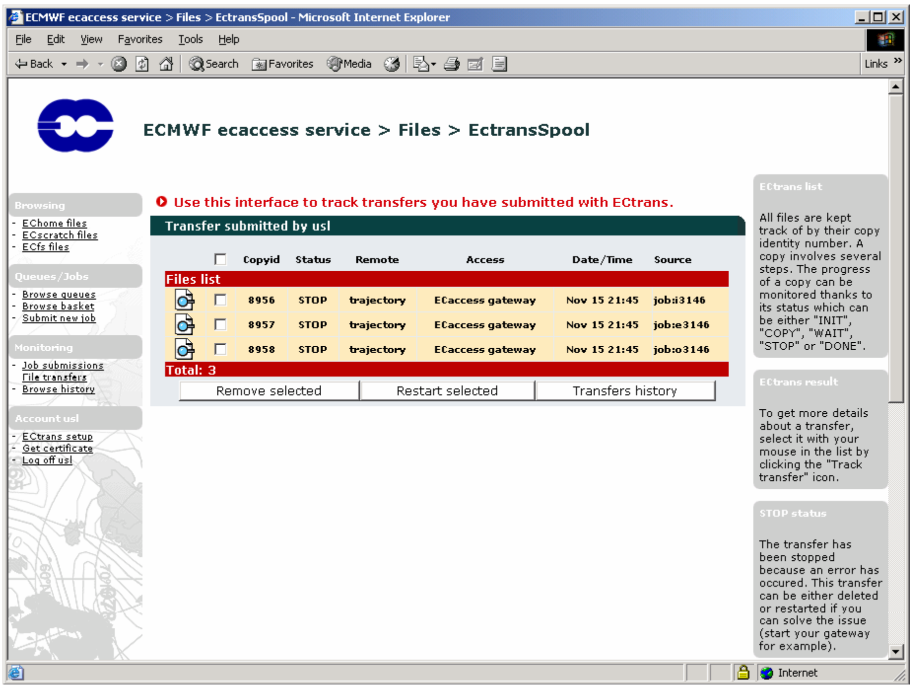
Remove

This will delete the input files stored inside your ECtrans spool directory.

You may use the cut and paste function of the operating system to get the complete file, or just read it on-line.

7.2 Monitoring ectrans file transfers

To access this interface, select the option “File transfers” in the “Monitoring” menu.



ECMWF ecaccess service > Files > EctransSpool - Microsoft Internet Explorer

ECMWF ecaccess service > Files > EctransSpool

Use this interface to track transfers you have submitted with ECtrans.

Transfer submitted by usl

Files list

	□	Copyid	Status	Remote	Access	Date/Time	Source
	□	8956	STOP	trajectory	ECaccess gateway	Nov 15 21:45	job:i3146
	□	8957	STOP	trajectory	ECaccess gateway	Nov 15 21:45	job:e3146
	□	8958	STOP	trajectory	ECaccess gateway	Nov 15 21:45	job:o3146

Total: 3

ECtrans list

All files are kept track of by their copy identity number. A copy involves several steps. The progress of a copy can be monitored thanks to its status which can be either "INIT", "COPY", "WAIT", "STOP" or "DONE".

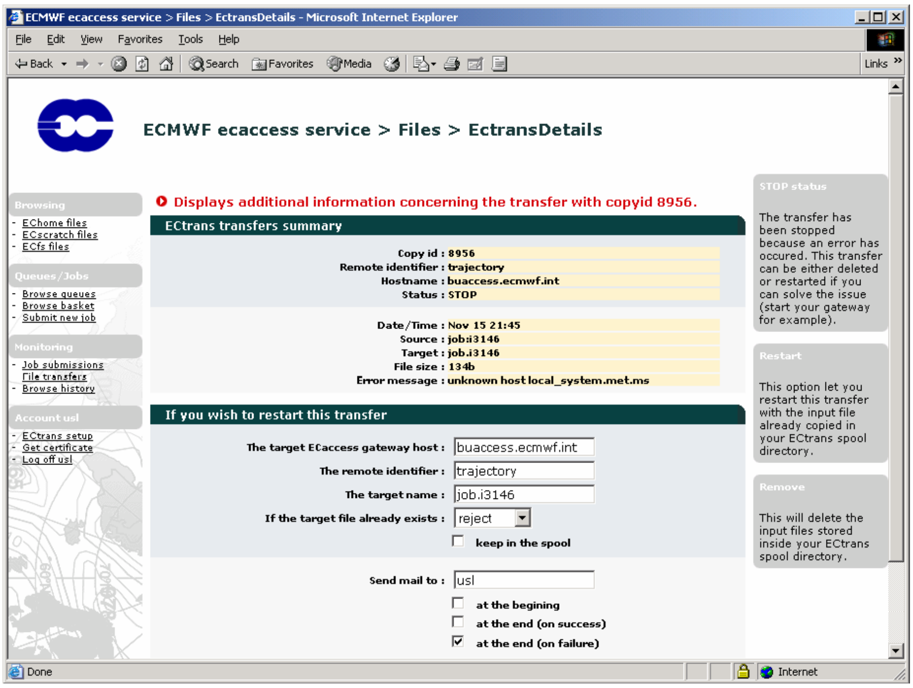
ECtrans result

To get more details about a transfer, select it with your mouse in the list by clicking the "Track transfer" icon.

STOP status

The transfer has been stopped because an error has occured. This transfer can be either deleted or restarted if you can solve the issue (start your gateway for example).

A list displays your transfer requests. You are informed of the status of the transfers (meanings of the different values are provided in the help tips). Once a transfer is marked as “DONE” or “STOP” you can select it with your mouse and obtain the following screen:



ECMWF ecaccess service > Files > EctransDetails - Microsoft Internet Explorer

ECMWF ecaccess service > Files > EctransDetails

Displays additional information concerning the transfer with copyid 8956.

ECtrans transfers summary

Copy id : 8956
Remote identifier : trajectory
Hostname : buaccess.ecmwf.int
Status : STOP

Date/Time : Nov 15 21:45
Source : job:i3146
Target : job.i3146
File size : 134b
Error message : unknown host local_system.met.ms

If you wish to restart this transfer

The target ECaccess gateway host : buaccess.ecmwf.int
The remote identifier : trajectory
The target name : job.i3146
If the target file already exists : reject
□ keep in the spool

Send mail to : usl
□ at the begining
□ at the end (on success)
☑ at the end (on failure)

STOP status

The transfer has been stopped because an error has occured. This transfer can be either deleted or restarted if you can solve the issue (start your gateway for example).

Restart

This option let you restart this transfer with the input file already copied in your ECtrans spool directory.

Remove

This will delete the input files stored inside your ECtrans spool directory.

8 The Telnet server

The Telnet plugin **(available only on MSgateways)** allows Member State users to log into their shell account at ECMWF and execute commands directly on an ECMWF machine. When contacting the ECaccess service with telnet, you will see something like:

```
Connected to ecaccess.
Escape character is ’ˆ]’.
Authorized access only.

***********************************************
   For further information, read the ECaccess
   documentation at:
   -> http://www.ecmwf.int/services/ecaccess/

   You can also use ECaccess to load/download
   files from your EChome, ECscratch  or ECfs
   directories using the ECaccess FTP server:
   -> ftp://uid@ecaccess.ecmwf.int/

   Use your UID and the SecurID code to login!
***********************************************

TelnetPlugin v3.0.0_2005010701
login: xyz
Passcode:******
```

The prompt is for your login name (which is your ECMWF user identifier). You will then be prompted for your passcode (obtained by entering your PIN number into your security token), and then you will get a UNIX prompt, typically ’$’ or ’%’. A login with telnet puts you automatically in your home directory.

Note that a different message may be displayed during your login procedure, as this message is customisable by the gateway administrator. This option gives the opportunity to broadcast important notes to Member State users (availability of a new product, disruptions planned for maintenance purposes, etc.).

The Telnet plugin supports only the interactive method of authentication described in section 3.

Note that the gateway at ECMWF will close telnet sessions idle for 6 hours. If you use a Member State ECaccess gateway, note that the default port number used by ecaccess is 9023. You’ll therefore have to run:

```
-> telnet ecaccess.meteo.ms 9023
```

Your Ecaccess administrator may have changed this. If the ECaccess shell commands are available to you, you can check the port number to use with ???.

9 The SSH server

The SSH plugin (part of the gateway) allows Member State users to log into their shell account at ECMWF and execute commands directly on “ecgate”. The first time you use SSH to ECaccess, you will see something like:

```
-> ssh xyz@ecaccess.ecmwf.int
The authenticity of host 'ecaccess.ecmwf.int (193.61.196.110)' can't be
established.
DSA key fingerprint is 9e:e3:f0:12:f5:08:61:d8:55:89:1a:40:e6:18:b8:42.
Are you sure you want to continue connecting (yes/no)? yes
***********************************************
   For further information, read the ECaccess
   documentation at:
   -> http://www.ecmwf.int/services/ecaccess/

   You can also use ECaccess to load/download
   files from your EChome, ECscratch  or ECfs
   directories using the ECaccess FTP server:
   -> ftp://uid@ecaccess.ecmwf.int/

   Use your UID and the SecurID code to login!
***********************************************

Password authentication
xyz's password ******
```

You will then be prompted for your passcode (obtained by entering your PIN number into your security token), and then will get a UNIX prompt, typically ’$’ or ’%’. A login with SSH puts you automatically in your home directory on ecgate.

Note that a different message may be displayed during your login procedure, as this message is customisable by the gateway administrator. This option gives the opportunity to broadcast important notes to Member State users (availability of a new product, disruptions planned for maintenance purposes, etc.).

The SSH plugin supports only the interactive method of authentication described in section 3.

Note that the gateway at ECMWF will close SSH sessions idle for 6 hours.

Note also that if you use a Member State ECaccess gateway, there is no need to use ssh, as the connection between the MS gateway and ECMWF is already secure. Using telnet will do. If you decide to use your MS gateway (and your gateway administrator has opened this service), you may need to contact port number 9022, like in:

```
-> ssh -p 9022 -l xyz ecaccess.meteo.ms
```

10 X11 connections

The X11 plugin (part of the gateway) allows Member State users who have an X11 server running on their workstation to log into their shell account and start X11 applications directly on ECMWF systems.

First, users must check that their DISPLAY environment variable is properly set up on their workstation:

```
-> echo $DISPLAY
hostname:0.0
```

The content of this variable is the name of the display to which X11 applications will connect (usually the name of the user workstation).

If users have a server access control program for X, they must add the gateway hostname to their host list allowed to make connections to their X11 server, e.g., assuming that the Member State ECaccess gateway (see section 2.2) runs on the server “ecaccess.meteo.ms”, with the “xhost” command

```
-> xhost +ecaccess.meteo.ms
ecaccess.meteo.ms being added to access control list
```

The MS gateway is then authorized to open connections to their X11 server. Note that the “xhost” command is only required for telnet, not for ssh.

After these preliminary settings you should be able to request an X11 proxy via your telnet or SSH connection. Each subsequent X11 application started from this xterm window (including new xterm) will make connections to your X11 server.

10.1 Starting xterm within a SSH session

By connecting to “ecaccess.ecmwf.int” with the SSH plugin described in section 9, after having been validated with your security token, you will first have to select the system at ECMWF to access.

Note that you may have to use “ssh -X” to open the X11 tunnel.