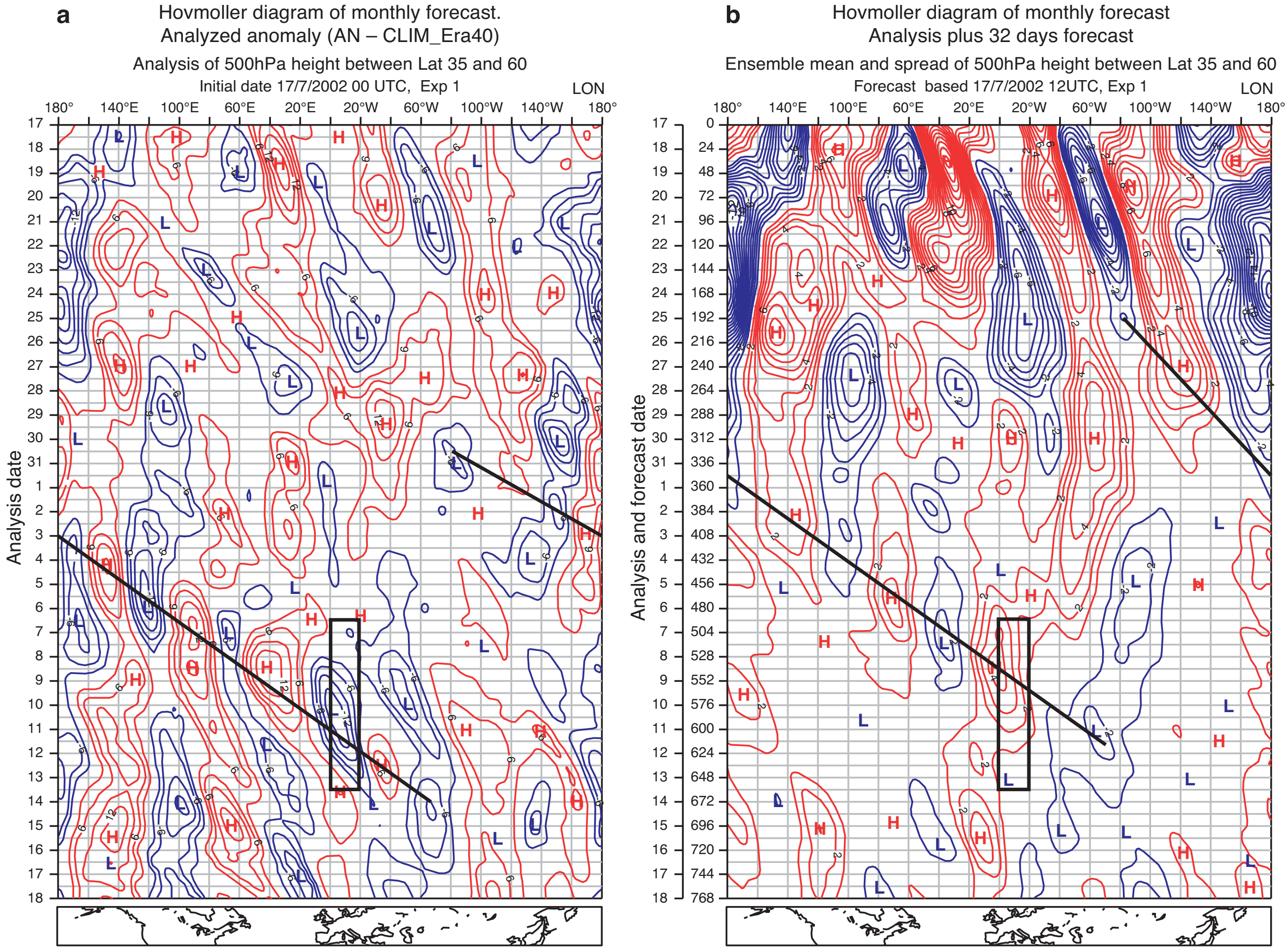


Figure 15 The Hovmöller diagram of 500 hPa geopotential anomaly of the analysis (left) and the monthly forecast (right) initialized at 00 UTC 17 July 2002. (a) The analysed geopotential anomaly with respect to ERA40 climate (1989-2001) (contour interval 3 dam, with red and blue representing positive and negative anomalies, respectively), and (b) the MF ensemble-mean anomaly with respect to the model climate (1989–2001) is shown (contouring interval 1 dam). The black rectangles in both plots highlight the space / time window in which the flood occurred. The solid black lines highlight the wave-train propagation.

References

Martyn, D.,1992: Climate of the World, Developments in Atmospheric Science, *Elsevier*

Vitart, F., 2002: Monthly forecasting at ECMWF. http://www.ecmwf.int/publications/member_states_meetings/seasonal_forecasters/2002/vitart_2002.pdf

Federico Grazzini and Gerald van der Grijn

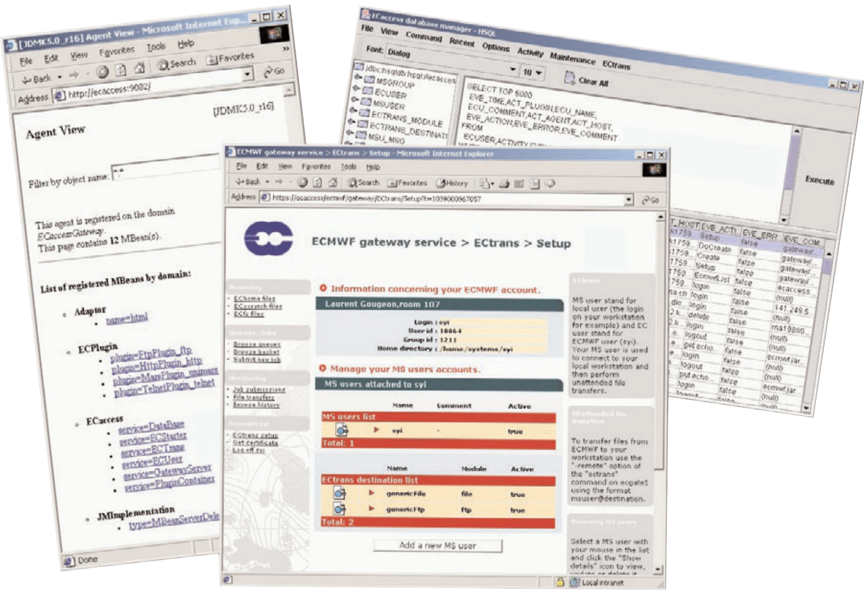
ECaccess: A portal to ECMWF

Soon after ECMWF became operational, access to the computing facilities for remote users became an important issue. Software was made available to all remote users to enable such access via the dedicated leased lines.

By the middle of the 1980s, the New Telecommunication System (NTS) software was running on the VAX servers, allowing remote users to submit and manage batch jobs from external sites to ECMWF and to transfer files between external sites and ECMWF.

In the early 1990s, UNIX and TCP/IP became the standards of choice and Telnet, FTP and X11 access for remote users became possible via the new UNIX-based servers. To secure that access, authentication became based on SecurID software. The equivalent of the NTS software was created in the UNIX-and-TCP/IP-based ECBATCH software package, consisting of the ECcopy and the ECcmd software and suitable for unattended access. ECmars software was created for direct access to part of the MARS system.

The Internet soon offered the possibility of access to all users, not only the Member State sites but also from anywhere in the world. A firewall with Telnet, FTP and X11 Gateways and extensions to the ECBATCH software package securely expanded the access range into the Internet.


[JDMK5.0_r16] Agent View - Microsoft Internet Exp...
File Edit View Favorites Tools Help
Back Search Favorites Go
Address http://ecaccess:9082/
Done
ECaccess database manager - HSQL
File View Command Recent Options Activity Maintenance ECtrans
Font: Dialog
Clear All
Execute
ECMWF gateway service > ECtrans > Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History Go
Address https://ecaccess/ecmwf/gateway/ECtrans/Setup?t=1039000967057
Local intranet

[JDMK5.0_r16]

Agent View

Filter by object name: *:*

This agent is registered on the domain *ECaccessGateway*.
This page contains **12** MBean(s).

List of registered MBeans by domain:

- **Adaptor**
  - name=html
- **ECPlugin**
  - plugin=FtpPlugin_ftp
  - plugin=HttpPlugin_http
  - plugin=MarsPlugin_unimars
  - plugin=TelnetPlugin_telnet
- **ECaccess**
  - service=DataBase
  - service=ECStarter
  - service=ECTrans
  - service=ECUser
  - service=GatewayServer
  - service=PluginContainer
- **JMImplementation**
  - type=MBeanServerDele

jdbc:hsqldb:hsql://ecacces
MSGROUP
ECUSER
MSUSER
ECTRANS_MODULE
ECTRANS_DESTINATI
MSU_MSG

```
SELECT TOP 5000
 EVE_TIME,ACT_PLUGIN,ECU_NAME,
 ECU_COMMENT,ACT_AGENT,ACT_HOST,
 EVE_ACTION,EVE_ERROR,EVE_COMMENT
FROM
 ECUSER,ACTIVITY
```

ECMWF gateway service > ECtrans > Setup

- ECHome files
- ECscratch files
- ECfs files

- Browse queues
- Browse basket
- Submit new job

- Job submissions
- File transfers
- Browse history

- ECtrans setup
- Get certificate
- Log off syi

Information concerning your ECMWF account.

Laurent Gougeon,room 107

Login : syi
User id : 10864
Group id : 1211
Home directory : /home/systems/syi

Manage your MS users accounts.

MS users attached to syi

	Name	Comment	Active
MS users list			
	syi	-	true
Total: 1			

	Name	Module	Active
ECtrans destination list			
	genericFile	file	true
	genericFtp	ftp	true
Total: 2			

Add a new MS user

MS user stand for local user (the login on your workstation for example) and EC user stand for ECMWF user (syi). Your MS user is used to connect to your local workstation and then perform unattended file transfers.

To transfer files from ECMWF to your workstation use the "-remote" option of the "ectrans" command on ecgate1 using the format msuser@destination.

Select a MS user with your mouse in the list and click the "Show details" icon to view,

Nevertheless, over time, the limitations of these methods became apparent: users need to be very knowledgeable; the user interfaces are disparate and not always easy to use; there are many different transport mechanisms involved, so problems with access are sometimes difficult to resolve. It also became necessary to offer facilities to interact with ECFS and to simplify the access method for users to avoid the double authentication process. In conclusion, to amalgamate all the different access methods to ECMWF services in a single package, ECaccess was created.

What does ECaccess do?

The new ECaccess software package provides a portal for registered users to access the ECMWF computing and archiving facilities with single step authentication from anywhere on the Internet. Authentication is performed in a uniform way, using SecurID cards and standard X509 certificates.

ECaccess allows registered users to connect to Ecgate1 and open X11 windows, to transfer files, archive and retrieve data in ECFS and submit jobs from any Unix workstation or Microsoft Windows PC. Jobs can currently be submitted to Ecgate1 and the VPPs. Submission to the IBM HPC will be offered early in 2003. Users can monitor and control submitted jobs through a Web interface. Job output data can be transferred to user workstations or PCs via the 'ectrans' command.

ECaccess replaces the current Ecbatch/Eccopy service and the Telnet, FTP and X11 specific Gateways (tn-gw.ecmwf.int, ftp-gw.ecmwf.int, x-gw.ecmwf.int).

ECaccess architecture

The ECaccess Gateway is the interface between the client and the ECaccess server. The Gateway can be located within the protected Local Area Network (LAN) or in a DeMilitarised Zone (DMZ). If located outside the protected area, the firewall must be configured to permit legitimate traffic between the clients and the Gateway and between the Gateway and the ECaccess server.

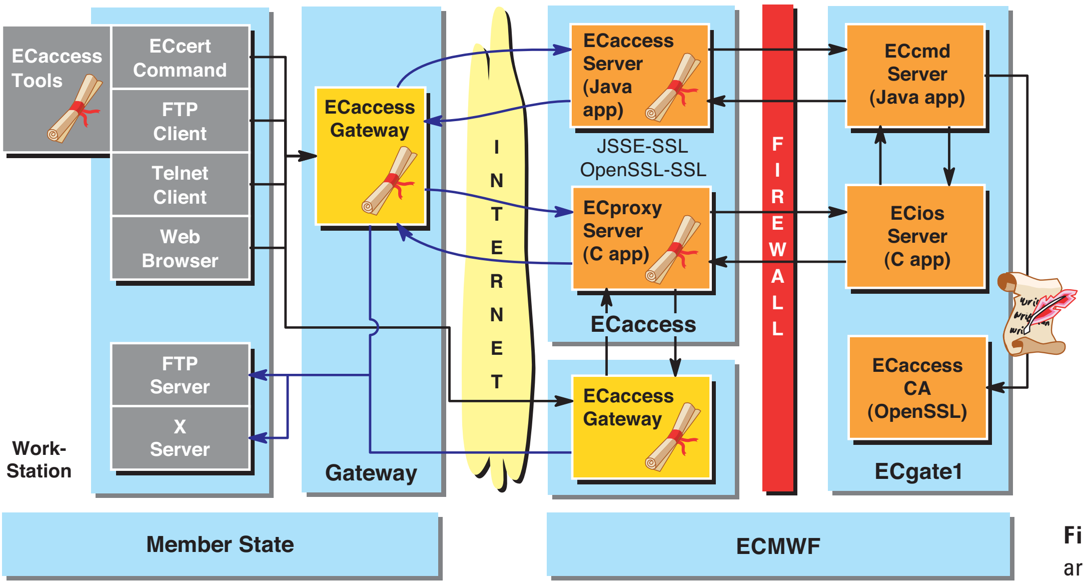


Figure 1 The ECaccess architecture.

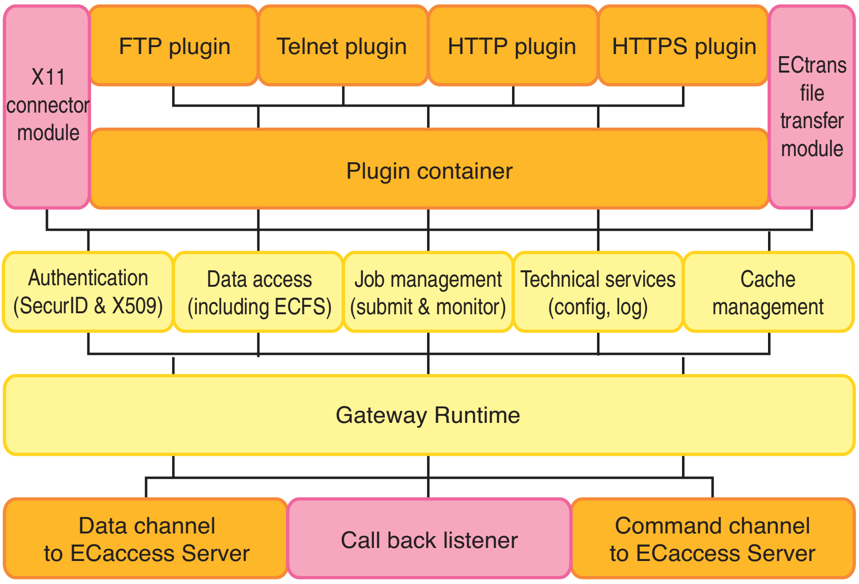

X11 connector module
FTP plugin
Telnet plugin
HTTP plugin
HTTPS plugin
ECtrans file transfer module
Plugin container
Authentication (SecurID & X509)
Data access (including ECFS)
Job management (submit & monitor)
Technical services (config, log)
Cache management
Gateway Runtime
Data channel to ECaccess Server
Call back listener
Command channel to ECaccess Server

Figure 2 The ECaccess Gateway internal architecture.

The ECaccess Gateway has been developed using Java[tm] object oriented programming technology, and can be run on almost any platform. This is done to avoid the usual porting issues existing with other languages such as C/C++.

The ECaccess tools, installed on the remote user's workstation or PC, offer high-level commands allowing users to manage their files and jobs from within batch scripts. The ECaccess tools are provided for several target operating systems and C sources are included to allow easy porting to most popular programming environments.

Finally, the ECaccess Server provides technical and high-level services to the Gateways, allowing generic access to computing and archiving facilities at ECMWF through Ecgate1. Two types of connections are maintained between the ECaccess Server and the ECaccess Gateways, one dedicated to data transfer and one dedicated to job and file management. The ECproxy Server carries out data transfer. It is a pure C, multithreaded application allowing fast transfer rates. The ECaccess Server, based on Enterprise Java Bean (EJB) technology, part of the Java2 Enterprise Edition (J2EE) framework, carries out the jobs and files management. Figure 1 gives a general overview of the ECaccess architecture:

Full ECaccess functionality requires a Gateway to be installed on the remote site. A Gateway is available at ECMWF for individual users, but secure file transfers from ECMWF to remote sites can be performed only if a Gateway is installed on the remote site.

Security

ECaccess addresses security at two levels: user authentication is performed using SecurID cards; batch requests (job submissions, file transfers, etc.) and Gateways are authenticated with X509 certificates.

A public-key infrastructure has been set-up by ECMWF to deliver:

- X509 certificates (valid for seven days) to authenticate users batch requests: users can request a certificate through a SecurID login process.
- X509 certificates (valid for two years) to authenticate ECaccess Gateways: administrators can register and get a certificate for their Gateway on the ECMWF Web site at http://www.ecmwf.int/services/ecaccess.

SSL is used to guarantee the integrity of the application data and the confidentiality of the transferred jobs and the monitoring information.

ECaccess Gateway

Figure 2 represents the internal organisation of the ECaccess Gateway.

The Gateway includes built-in mechanisms to maintain a secure connection with the ECaccess Server, to authenticate users and manage their requests, to transfer data and submit jobs.

The Gateway includes a model for the management of 'plug-in' services. A plug-in is a piece of code that handles requests/responses flowing through the Gateway. Currently, there are plug-ins for incoming FTP, HTTP/S, X and Telnet requests to ECMWF. Other plug-ins will be added in the future.

Plug-ins

- The FTP plug-in lets users submit jobs and transfer files between their own workstation or PC and the ECMWF file systems. This extended FTP server can be used for access to ECMWF computing and archiving facilities in interactive mode with a standard FTP client (or an FTP browser) or in batch mode from within shell scripts.
- The HTTP and HTTPS plug-ins let users manage and monitor their jobs and transfer files. They offer the same functionalities as the FTP plug-in from an HTTP browser.
- The Telnet plug-in provides access to Ecgate1 with a single-sign-on login process. Communication and authentication is established through the Gateway. The login process is secure and overcome the limitation of the current Telnet specific Gateway.

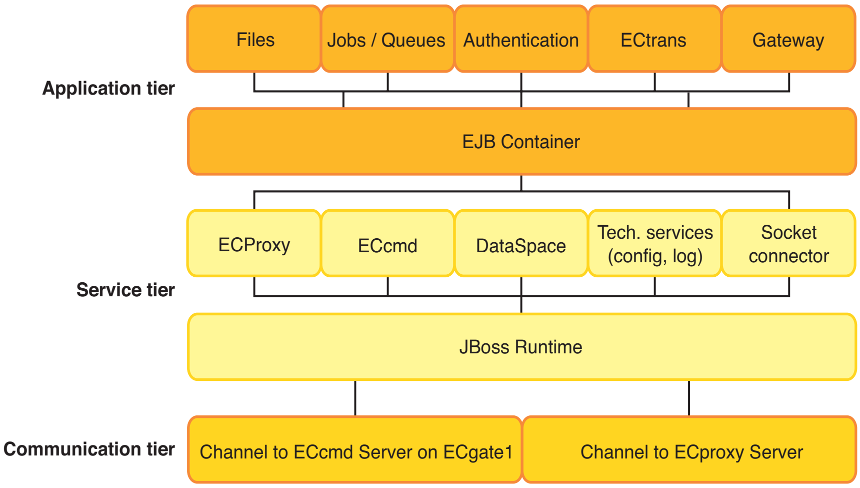


Figure 3 The ECaccess Server internal architecture.

Call back

The Call back listener receives notifications from the ECaccess Server and activates either the ECtrans file transfer module to transfer data to a remote user's workstation, or the X11 connector module to open connections to a remote user's X11 server.

ECaccess Server

The ECaccess Server runs on the ECMWF side. Figure 3 represents the internal architecture of the ECaccess Server.

The ECaccess Server includes built-in mechanisms, such as the Java Authentication and Authorization Service (JAAS) and the SSL protocol, to authenticate the Gateways and provide a secure framework for remote access to ECMWF services.

The application tier provides public services to the Gateways. The Enterprise Java Bean (EJB) container relies on the services tier, which provides internal services to the EJB components (Files, etc.). The communication tier manages communications between the Gateways and the ECproxy Server, for the data transfers, and between the ECaccess Server and the ECcmd daemon.

Why do I need ECaccess?

With ECaccess, scientists from institutions anywhere in Europe can access the complex computer environment at ECMWF via the Internet using any standard FTP, Telnet or HTTP client. Jobs can be prepared and submitted remotely. Data produced by the jobs or MARS retrievals can be transferred back to the remote user's workstation or PC. Debugging or monitoring a suite of jobs can be done interactively starting the X11 applications via a Telnet connection.

ECaccess offers remote users uniform access to ECMWF services in both interactive and batch mode. In particular, ECaccess enables remote users to:

- Connect directly to Ecgate1 via Telnet.
- Open X11 windows on Ecgate1, the VPPs and the HPCs.
- Transfer and manage HOME, SCRATCH, ECFS or MARS files.
- Submit and monitor jobs from any desktop.
- Automate file transfers from ECMWF to any workstation or PC using ECtrans.

How do I use ECaccess?

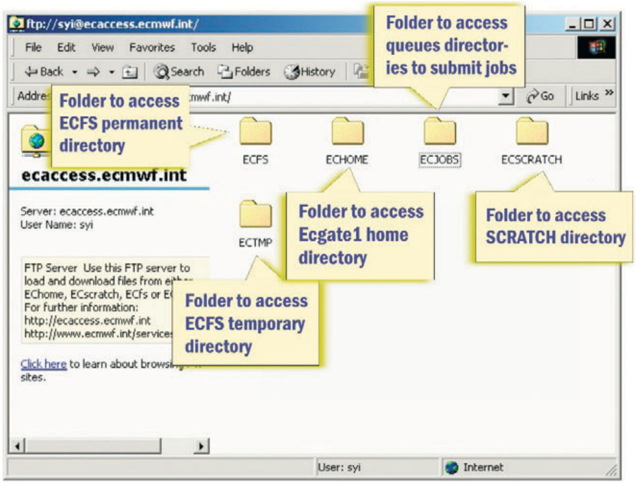
In order to use ECaccess, an account at ECMWF is required. Authentication is performed using SecurID cards to use the ECaccess services in interactive mode, or by creating a seven-day X509 certificate for batch access. Users connect to an ECaccess Gateway and go through an authentication procedure. The Gateway authenticates external users and contacts the ECaccess server, which in turn manages access to ECMWF services. Connections to the ECaccess Gateway can be made interactively via standard Telnet, FTP and HTTP clients or in batch mode via the ECaccess tools (a set of UNIX commands which can be called from batch scripts).

Managing files

Files can be managed interactively via FTP and HTTP or in batch mode via the ECaccess tools.

The root directory of the FTP server (Figure 4) contains the ECaccess domains: ECFS and ECTMP (the user's ECFS permanent and temporary directories); ECHOME (the user's home directory on Ecgate1); ECSCRATCH (the scratch directory) and ECJOBS (the queue directory).

Simply use drag and drop to transfer files between a local folder and any of the target ECaccess domains.



Folder to access queues directories to submit jobs

Folder to access ECFS permanent directory

Folder to access Ecgate1 home directory

Folder to access SCRATCH directory

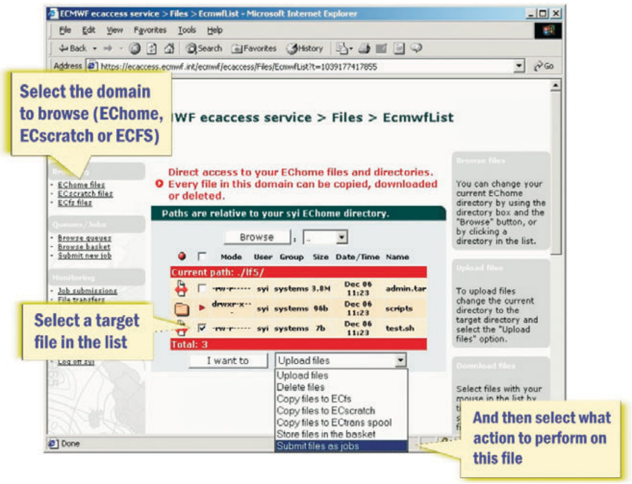
Folder to access ECFS temporary directory

Server: ecaccess.ecmwf.int
User Name: syi

FTP Server Use this FTP server to load and download files from ei
EChome, ECscratch, ECfs or E
For further information:
http://ecaccess.ecmwf.int
http://www.ecmwf.int/service

Click here to learn about browsi
sites.

Figure 4 The root directory of the ECaccess FTP server.



ECMWF ecaccess service > Files > EcmwfList - Microsoft Internet Explorer

Address: https://ecaccess.ecmwf.int/ecmwf/ecaccess/Files/EcmwfList?t=1039177417855

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 syi EChome directory.

Mode	User	Group	Size	Date/Time	Name
Current path: ./lf5/					
-rw-r-----	syi	systems	3.8M	Dec 06 11:23	admin.tar
drwxr-x---	syi	systems	96b	Dec 06 11:23	scripts
-rw-r-----	syi	systems	7b	Dec 06 11:23	test.sh
Total: 3					

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.

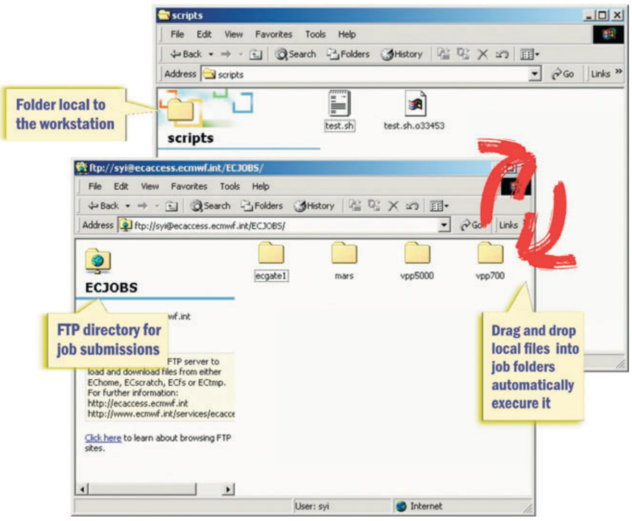
To upload files change the current directory to the target directory and select the "Upload files" option.

Select the domain to browse (EChome, ECscratch or ECFS)

Select a target file in the list

And then select what action to perform on this file

Figure 5 Access to the ECaccess domains.



scripts

Address: scripts

ftp://syi@ecaccess.ecmwf.int/ECJOBS/

Address: ftp://syi@ecaccess.ecmwf.int/ECJOBS/

FTP server to load and download files from either EChome, ECscratch, ECfs or ECtmp. For further information: http://ecaccess.ecmwf.int http://www.ecmwf.int/services/ecacce

Click here to learn about browsing FTP sites.

Folder local to the workstation

FTP directory for job submissions

Drag and drop local files into job folders automatically execure it

Figure 6 Jobs submissions using an FTP browser.

With an HTTP browser, the ECaccess domains can be selected using the 'Browsing' menu of the ECaccess Web interface (Figure 5). Within the selected domain, users can transfer or delete files, submit jobs and browse directories:

With the ECaccess tools, remote users can select a target domain by setting the environment variable ECDOMAIN, and then manage or transfer files to and from this domain.

For example, to manage ECFS files, a remote user will set ECDOMAIN to ECFS and use the following commands:

- 'ecls' or 'ecdir': to print the list of ECFS files.
- 'ecget' or 'ecreget': to retrieve an ECFS file.
- 'ecput': to store a local file in ECFS.
- 'ecmkdir' or 'ecrmdir': to create or remove ECFS directories.
- 'ecdelete' or 'ecchmod': to delete or change permissions of an ECFS file.

Managing jobs

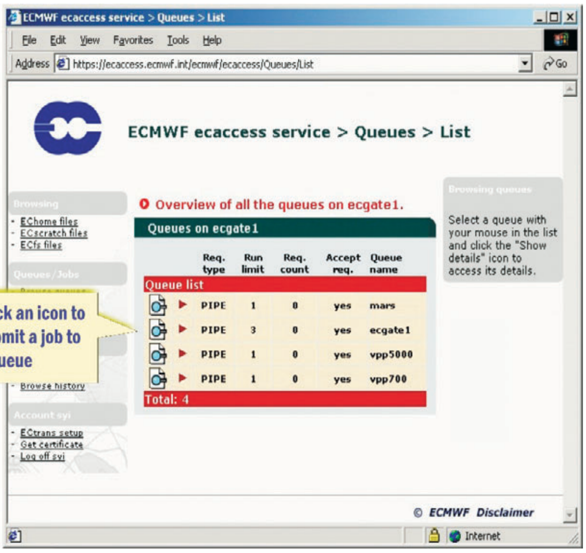
Jobs can be managed interactively via FTP and HTTP or in batch mode via the ECaccess tools.

The ECaccess FTP server can also be used to submit jobs. To submit a job from an FTP browser, click on the ECJOBS folder of the ECaccess root directory. Each ECJOBS subfolder is a target queue for job submissions (Figure 6).

A script dragged and dropped into an ECJOBS subfolder is automatically submitted as a new job. Once executed, the job input file is renamed to include the job identifier and the job output file is created. All the files associated with the job can later be inspected or dragged and dropped into a directory local to the user's workstation or PC.

A user can also use an HTTP browser to submit jobs step-by-step using the 'Browse queues' menu of the ECaccess WEB interface (Figure 7).

The list of available queues is displayed in a table with an icon for each queue. A target queue can be selected by clicking the appropriate icon. After having checked the details of the selected queue, click the 'Submit a job to this queue' button to include the job into the specified queue (Figure 8).



ECMWF ecaccess service > Queues > List

Address: https://ecaccess.ecmwf.int/ecmwf/ecaccess/Queues/List

ECMWF ecaccess service > Queues > List

Overview of all the queues on ecgate1.

Queues on ecgate1

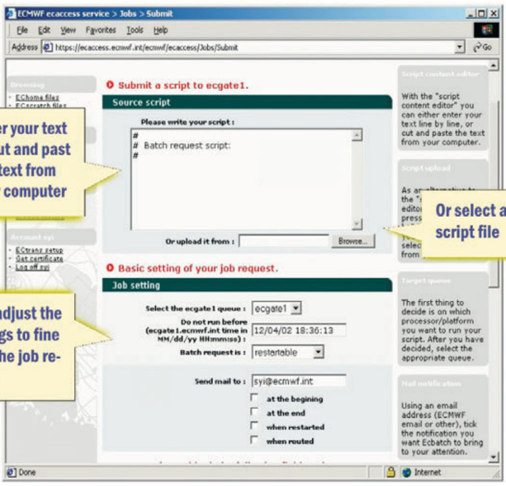
Req. type	Run limit	Req. count	Accept req.	Queue name
Queue list				
PIPE	1	0	yes	mars
PIPE	3	0	yes	ecgate1
PIPE	1	0	yes	vpp5000
PIPE	1	0	yes	vpp700
Total: 4				

Select a queue with your mouse in the list and click the "Show details" icon to access its details.

© ECMWF Disclaimer

Click an icon to submit a job to a queue

Figure 7 Selection of a target queue for a job submission.



ECMWF ecaccess service > Jobs > Submit

Address: https://ecaccess.ecmwf.int/ecmwf/ecaccess/Jobs/Submit

Submit a script to ecgate1.

Source script

Please write your script :

```
#
#  Batch request script:
#
```

Or upload it from :

Basic setting of your job request.

Job setting

Select the ecgate1 queue : ecgate1

Do not run before (ecgate1.ecmwf.int time in MM/dd/yy HH:mm:ss) : 12/04/02 18:36:13

Batch request is : restartable

Send mail to : syi@ecmwf.int

□ at the begining
□ at the end
□ when restarted
□ when routed

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

The first thing to decide is on which processor/platform you want to run your script. After you have decided, select the appropriate queue.

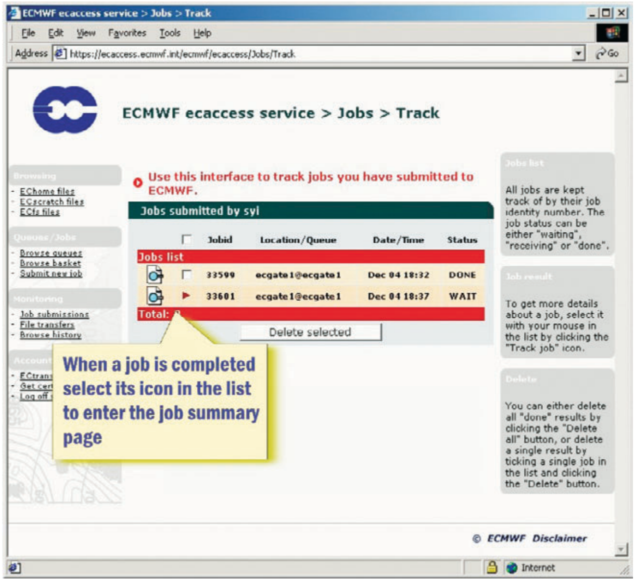
Using an email address (ECMWF email or other), tick the notification you want Ecbatch to bring to your attention.

Enter your text or cut and past the text from your computer

Or select a local script file

Then adjust the settings to fine tune the job request

Figure 8 Batch request settings.



ECMWF ecaccess service > Jobs > Track

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

Jobs submitted by syl

	□	Jobid	Location/Queue	Date/Time	Status
Jobs list					
	□	33599	ecgate1@ecgate1	Dec 04 18:32	DONE
	▶	33601	ecgate1@ecgate1	Dec 04 18:37	WAIT
Total: 2					

All jobs are kept track of by their job identity number. The job status can be either "waiting", "receiving" or "done".

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

You can either delete all "done" results by clicking the "Delete all" button, or delete a single result by ticking a single job in the list and clicking the "Delete" button.

When a job is completed select its icon in the list to enter the job summary page

Figure 9 Batch request monitoring.

Once the source script is provided (either from a local file or from a text entered in the job input text area) and the settings have been checked, click the 'Submit job' button.

Once submitted, jobs can be monitored using the job track interface. The monitoring interface provides remote users with information on the job requests referenced by the job identifier number. To access it, click the 'Job submissions' link in the 'Monitoring' menu (Figure 9).

Jobs submitted via the Web interface or via the ECtools commands will appear in the list of jobs.

Once the job has completed (status is DONE), its outputs can be managed (Figure 10).

The output, input and error files associated to the selected job can be transferred to an ECaccess domain or directly edited using the job editor of the Web interface.

With the ECaccess tools, remote users can prepare batch scripts, transfer them to ECMWF, submit them and retrieve the results. The status of submitted jobs can be interactively monitored.

To submit a job, a user will execute the 'ecjput' command, specifying the name of the queue where the job is to start, and the name of the file located on the remote user's workstation or PC ('ecjreq' can be used if the file is located at ECMWF). Optionally, an email address to receive a notification when the job is started or completed can be provided. Then the following commands are available to monitor and manage the job requests:

- 'ecjget': to get the job output files.
- 'ecjdel': to delete and cancel a job request.
- 'ecjls': to list the submitted job requests.

Unattended file transfers

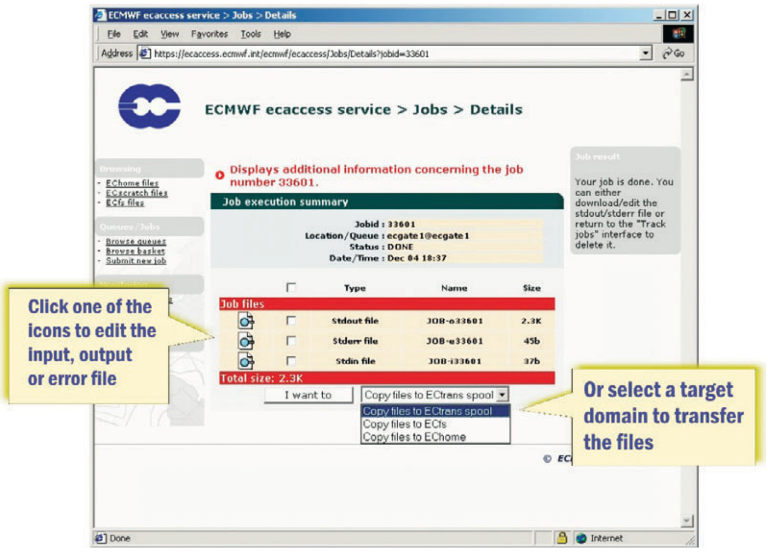
The ECtrans command is provided for batch script running at ECMWF, on ECMWF user accounts. Its purpose is to automate files transfers from the VPPs, Ecgate1 or the HPCs using the secure file transfer feature of the ECaccess Server (Figure 11).

Managing users and hosts

An external user makes a file transfer request from ECMWF, providing a remote user identifier and a remote destination. The destination is either a target file on the ECaccess Gateway host, or an FTP destination on a remote server or remote user's workstation or PC. The connecting parameters to these remote destinations (remote user identifier and passwords) are held in the ECaccess Gateway database.

Via his HTTP browser a user can define the mapping between his ECMWF user identifier and his local user identifiers. He can also check his available destinations by clicking the 'ECtrans setup' link in the 'Account' menu (Figure 12).

Local users (MS users) can be created, updated or deleted. The parameters attached to a local user are a hostname (e.g. the remote workstation or PC for FTP access), a user identifier and a password (e.g. the login parameters of the FTP account). Details on local users and destinations can be viewed by clicking on the appropriate icon.


ECMWF ecaccess service > Jobs > Details
File Edit View Favorites Tools Help
Address https://ecaccess.ecmwf.int/ecmwf/ecaccess/Jobs/Details?jobid=33601
Go
ECHome files
ECscratch files
ECfs files
Browse queues
Browse basket
Submit new job
I want to
Copy files to ECtrans spool
Copy files to ECtrans spool
Copy files to ECfs
Copy files to EChome
Done
Internet

ECMWF ecaccess service > Jobs > Details

Displays additional information concerning the job number 33601.

Job execution summary

Jobid : 33601
Location/Queue : ecgate1@ecgate1
Status : DONE
Date/Time : Dec 04 18:37

	□	Type	Name	Size
Job files				
	□	Stdout file	JOB-o33601	2.3K
	□	Stderr file	JOB-e33601	45b
	□	Stdin file	JOB-i33601	37b
Total size: 2.3K				

Your job is done. You can either download/edit the stdout/stderr file or return to the "Track jobs" interface to delete it.

Click one of the icons to edit the input, output or error file

Or select a target domain to transfer the files

Figure 10 Outputs of a batch request.

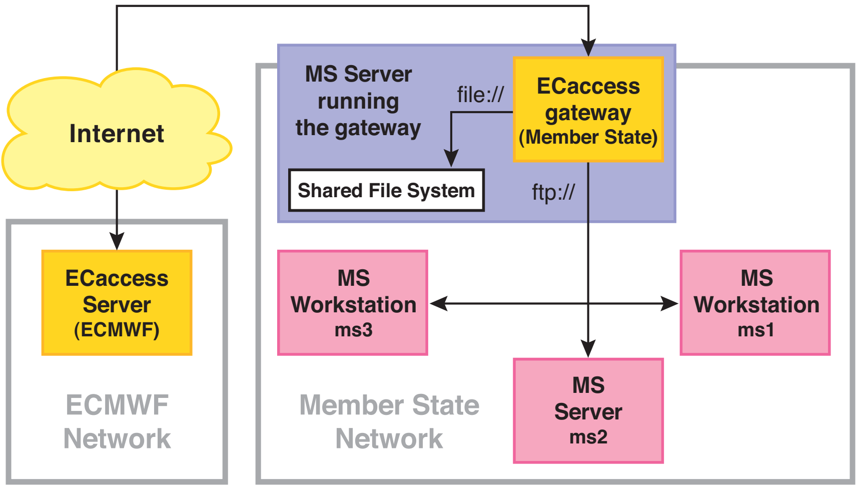
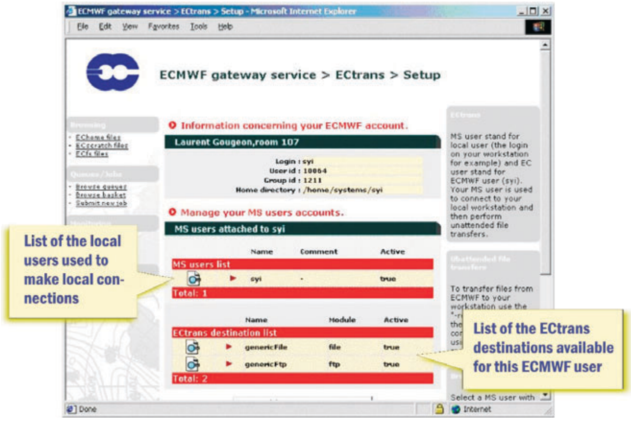


Figure 11 ECtrans mechanism.



ECMWF gateway service > ECtrans > Setup - Microsoft Internet Explorer

ECMWF gateway service > ECtrans > Setup

Information concerning your ECMWF account.

Laurent Gougeon,room 107

Login : syi
User id : 10064
Group id : 1211
Home directory : /home/systems/syi

Manage your MS users accounts.

MS users attached to syi

	Name	Comment	Active
MS users list			
	syi	-	true
Total: 1			

	Name	Module	Active
ECtrans destination list			
	genericFile	file	true
	genericFtp	ftp	true
Total: 2			

MS user stand for local user (the login on your workstation for example) and EC user stand for ECMWF user (syi). Your MS user is used to connect to your local workstation and then perform unattended file transfers.

To transfer files from ECMWF to your workstation use the

Select a MS user with

List of the local users used to make local connections

List of the ECtrans destinations available for this ECMWF user

Figure 12 ECtrans setup.

Sending files

Figure 13 shows the usage of the ECtrans command.

Flags can be used to specify the action to perform in case of an existing target file, to request notification in case of a successful and/or a failed transfer and to specify whether the transfer is from ECMWF to a remote site or the other way. When transfers are performed from ECMWF to a remote site, files are transferred to the ECtrans spool. A transfer identifier is returned for each spooled request. This identifier can later be used to monitor the transfer.

With an HTTP browser, a user can monitor the ECtrans spool, by clicking the 'File transfers' link in the 'Monitoring' menu. The list of the spooled requests is then displayed. To get details for a specific request, click the appropriate icon in the list (Figure 14).

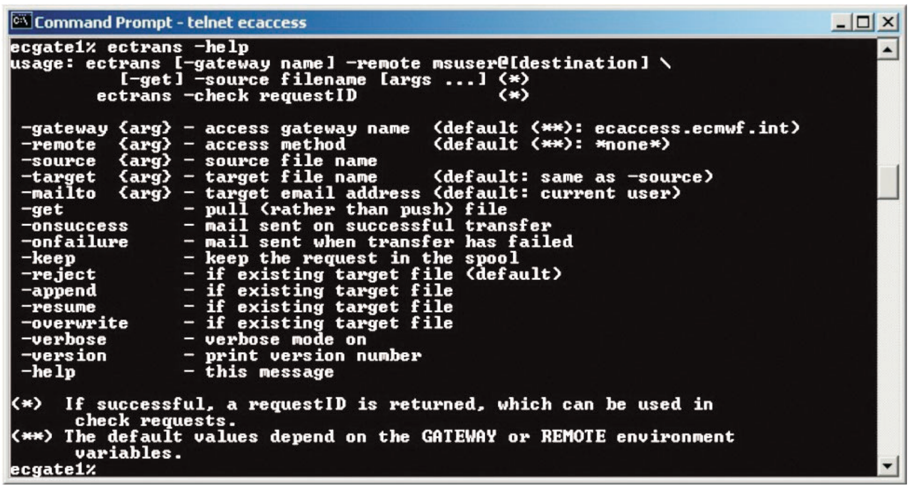
The transfer status is either INIT (spooling of the source file is still in progress), COPY (the transfer of the spooled file to the target destination is still in progress), DONE (the transfer was successful) or STOP (the transfer has failed). When the transfer is completed (successful or not) the user can restart it if necessary, providing new transfer parameters.

Similar transfer management can be performed using the ECaccess tools. For example, to initiate a file transfer from the ECaccess domain ECSCRATCH, the user will set ECDOMAIN to ECSCRATCH and use the 'ectreq' command. The following commands are also available:

- 'ectls': to list the transfers carried out by ECTrans.
- 'ectret': to retry a failed transfer.
- 'ectdel': to cancel a transfer and remove its file from the spool.
- 'ectinfo': to display the target destination of a transfer request.

Telnet

The ECaccess Telnet server allows remote users to log into their shell account at ECMWF and execute commands on



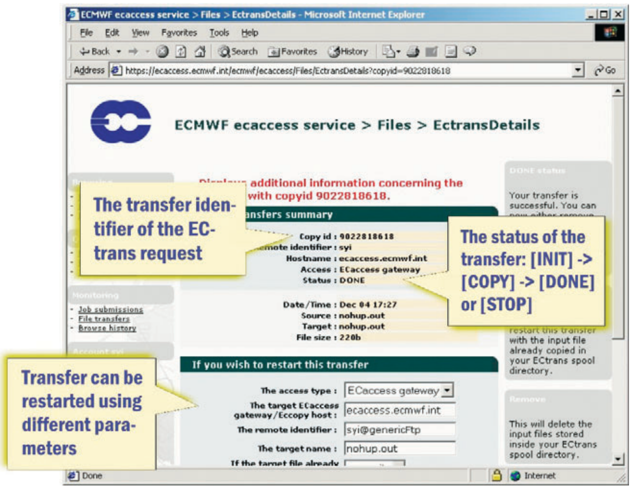
Command Prompt - telnet ecaccess

```
ecgate1% ectrans -help
usage: ectrans [-gateway name] -remote msuser@[destination] \
          [-get] -source 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)
 -get           - pull (rather than push) file
 -onsuccess     - mail sent on successful transfer
 -onfailure     - mail sent when transfer has failed
 -keep          - keep the request in 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.
(**) The default values depend on the GATEWAY or REMOTE environment
     variables.
ecgate1%
```

Figure 13 Usage of the 'ectrans' command.


ECMWF ecaccess service > Files > EctransDetails - Microsoft Internet Explorer

Address: https://ecaccess.ecmwf.int/ecmwf/ecaccess/Files/EctransDetails?copyid=9022818618

ECMWF ecaccess service > Files > EctransDetails

Displays additional information concerning the ... with copyid 9022818618.

...ansfers summary

Copy id : 9022818618
Remote identifier : syi
Hostname : ecaccess.ecmwf.int
Access : ECaccess gateway
Status : DONE

Date/Time : Dec 04 17:27
Source : nohup.out
Target : nohup.out
File size : 220b

If you wish to restart this transfer

The access type : ECaccess gateway
The target ECaccess gateway/Eccopy host : ecaccess.ecmwf.int
The remote identifier : syi@genericFtp
The target name : nohup.out
If the target file already ...

Your transfer is successful. You can ...

... restart this transfer with the input file already copied in your ECtrans spool directory.

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

The transfer identifier of the ECtrans request

The status of the transfer: [INIT] -> [COPY] -> [DONE] or [STOP]

Transfer can be restarted using different parameters

Figure 14 ECtrans monitoring.

Ecgate1. The ECaccess Telnet server comes with a dedicated UNIX command, available on Ecgate1, called 'ecxterm'. Started from an ECaccess Telnet session, this command allows the opening of X applications from any host at ECMWF to any target remote user's workstation or PC.

X11

The ECaccess X11 plug-in allows remote users who have an X server running on their workstation or PC to log into their shell account at ECMWF and start X applications on any ECMWF host.

On ECgate1, a user can open xterm windows with the 'ecxterm' command. To open xterm windows on a different ECMWF system, the 'hostname' option of 'ecxterm' can be used.

The 'ecxterm' command is also part of the ECaccess tools. Remote users can start an 'xterm' on Ecgate1 running the 'ecxterm' command from their local desktop.

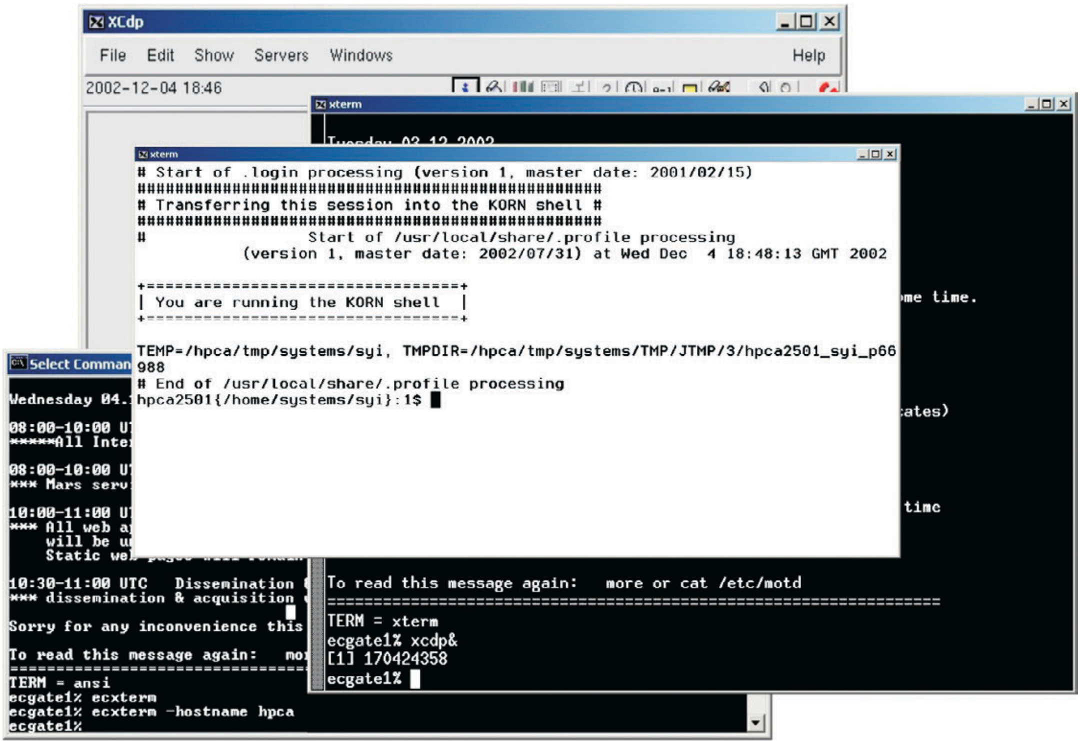
ECaccess administration

The ECaccess administration package provides tools to manage and monitor the ECaccess Gateway. The package includes a database and a log manager. Through graphic interfaces, administrators can interrogate the ECaccess database and monitor the log created by the Gateway activity. Using an HTTP browser, administrators can manage and monitor the services of the Gateway (e.g. start and stop the FTP, HTTP, Telnet or ECtrans service).

Next steps

There currently is only a single ECMWF ECaccess Gateway, for access via the Internet. In the near future, a second ECMWF ECaccess Gateway will be made available for access via RMDCN. Also, ECaccess will continue to be enhanced and adapted to facilitate the life of remote users and allow access to the new ECMWF resources.

If you wish to use ECaccess or make it available to your users, further information regarding ECaccess installation, administration and usage can be found at the ECMWF Web site: http://www.ecmwf.int/services/ecaccess. Also, you may wish to contact ecaccess@ecmwf.int.


XCdp

2002-12-04 18:46

xterm

```
# Start of .login processing (version 1, master date: 2001/02/15)
#####################################################
# Transferring this session into the KORN shell #
#####################################################
#                    Start of /usr/local/share/.profile processing
             (version 1, master date: 2002/07/31) at Wed Dec  4 18:48:13 GMT 2002

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

TEMP=/hpca/tmp/systems/syi, TMPDIR=/hpca/tmp/systems/TMP/JTMP/3/hpca2501_syi_p66
988
# End of /usr/local/share/.profile processing
hpca2501{/home/systems/syi}:1$
```

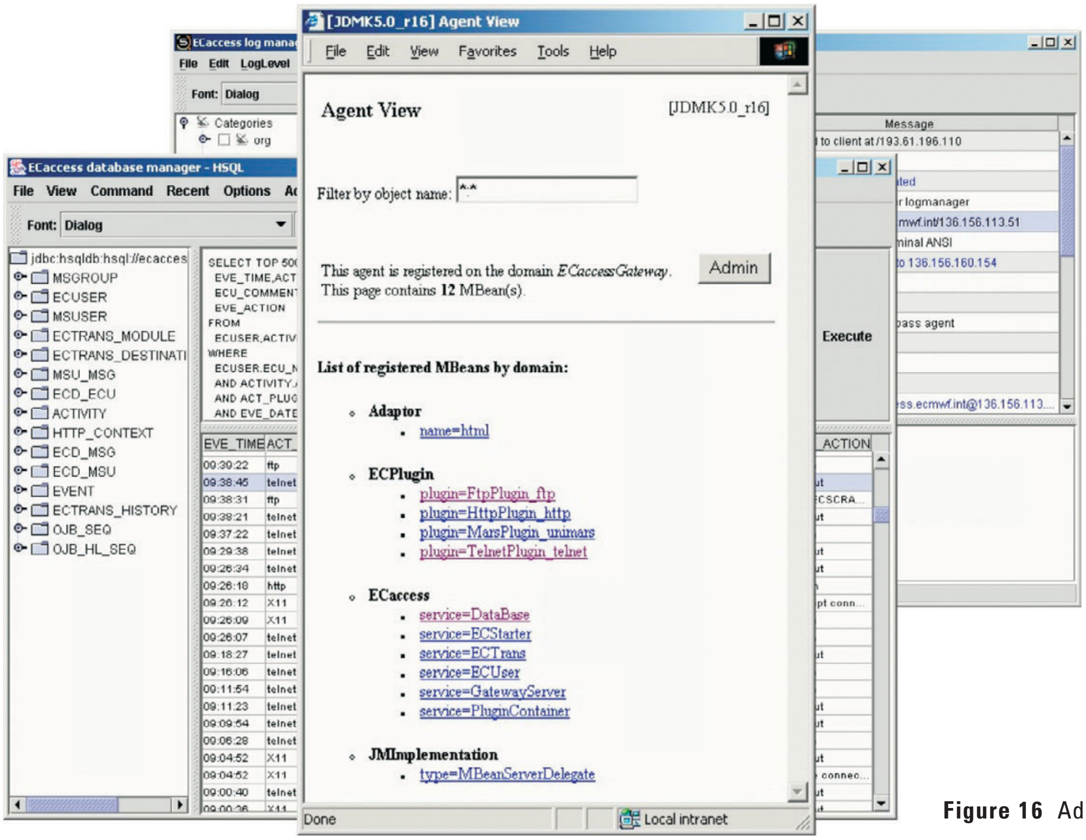
xterm

```
Tuesday 03.12.2002
...me time.
...ates)
...time
To read this message again:   more or cat /etc/motd
==================================================================
TERM = xterm
ecgate1% xcdp&
[1] 170424358
ecgate1%
```

Select Command...

```
Wednesday 04.1...
08:00-10:00 U...
*****All Inte...
08:00-10:00 U...
*** Mars serv...
10:00-11:00 U...
*** All web a...
    will be u...
    Static we...
10:30-11:00 UTC   Dissemination ...
*** dissemination & acquisition ...
Sorry for any inconvenience this
To read this message again:   mo...
=====================================
TERM = ansi
ecgate1% ecxterm
ecgate1% ecxterm -hostname hpca
ecgate1%
```

Figure 15 In the following example, once logged on Ecgate1 with a Telnet client, the user has opened an 'xterm' window and used this window to start an 'xcdp' session. An 'xterm' window has also been opened on the HPCA using the command 'ecxterm -hostname hpca'.



jdbc:hsqldb:hsql://ecacces
MSGROUP
ECUSER
MSUSER
ECTRANS_MODULE
ECTRANS_DESTINATI
MSU_MSG
ECD_ECU
ACTIVITY
HTTP_CONTEXT
ECD_MSG
ECD_MSU
EVENT
ECTRANS_HISTORY
OJB_SEQ
OJB_HL_SEQ

```
SELECT TOP 50(
  EVE_TIME,ACT
  ECU_COMMENT
  EVE_ACTION
FROM
  ECUSER,ACTIV
WHERE
  ECUSER.ECU_N
  AND ACTIVITY.
  AND ACT_PLUG
  AND EVE_DATE
```

EVE_TIME	ACT_
09:39:22	ftp
09:38:45	telnet
09:38:31	ftp
09:38:21	telnet
09:37:22	telnet
09:29:38	telnet
09:26:34	telnet
09:26:18	http
09:26:12	X11
09:26:09	X11
09:26:07	telnet
09:18:27	telnet
09:16:06	telnet
09:11:54	telnet
09:11:23	telnet
09:09:54	telnet
09:06:28	telnet
09:04:52	X11
09:04:52	X11
09:00:40	telnet
09:00:36	X11

Agent View [JDMK5.0_r16]

Filter by object name: *:*

This agent is registered on the domain *ECaccessGateway*.
This page contains **12** MBean(s).

List of registered MBeans by domain:

- **Adaptor**
  - name=html
- **ECPlugin**
  - plugin=FtpPlugin_ftp
  - plugin=HttpPlugin_http
  - plugin=MarsPlugin_unimars
  - plugin=TelnetPlugin_telnet
- **ECaccess**
  - service=DataBase
  - service=ECStarter
  - service=ECTrans
  - service=ECUser
  - service=GatewayServer
  - service=PluginContainer
- **JMImplementation**
  - type=MBeanServerDelegate

```
 to client at /193.61.196.110
ted
r logmanager
mwf.int/136.156.113.51
inal ANSI
o 136.156.160.154
pass agent
ss.ecmwf.int@136.156.113...
```

```
t
CSCRA...
t
t
t
pt conn...
t
t
t
t
 connec...
t
```

Figure 16 Administration tools

Matteo Dell'Acqua, Laurent Gougeon and Dieter Niebel

ECMWF programme of activities 2003 to 2006

The Director presented the Centre's programme of activities for the years 2003 to 2006 to Council in December 2002. The Committees had examined the scientific, technical, administrative and policy aspects of the programme in detail during the autumn, and the Committee Chairmen reported to Council on the generally supportive views of their Committees.

Council delegates expressed support and enthusiasm for the programme during a detailed and lengthy discussion; it was clear that the Member States' and Co-operating States' National Meteorological Services all have a great interest in the Centre and its progress.

During the four-year period, the Centre's Computer Hall will be substantially enlarged, and new office accommodation will be constructed.

Introduction and executive summary

Our mission is to deliver operational forecasts of increasingly high quality and scope from a few days to a few seasons ahead. Our targets for this four-year programme (2003–2006) are to:

- continue extension of the skill of medium-range forecasts, both deterministic and probabilistic, (from three days to ten days ahead) at the rate of one day per decade
- prepare by 2003/4 an assessment of seasonal forecast skill over the last 40 years;
- continually improve the timeliness and reliability of product dissemination, and availability of the computer facilities to the Member States [1];
- extend the range of reliable forecasts of severe weather over land and sea towards day 4 and day 5.

The research and operational activities necessary to achieve these targets flow naturally from our responsibilities, capabilities and opportunities, and entail:

- Development of a suitably comprehensive earth-system data assimilation capability to make best use of all available data (especially satellite data) to provide analyses, together with estimates of the uncertainty of the analyses;
- Development of a suitably comprehensive and integrated high-resolution earth-system model, using efficient and economical numerical methods with a comprehensive and extensively-validated physical parametrization packages together with estimates of uncertainty in these packages;
- Development of the methodology of ensemble forecasting for medium-range, extended-range and seasonal forecasting, with an emphasis on forecasting severe weather;
- Operational delivery of an enhanced range of meteorological and associated products;

[1] Throughout this document, where appropriate, the term 'Member State' is taken to include Co-operating State.