

# **Globus Toolkit 6.0 Commandline Tools**

DRAFT

# Globus Toolkit 6.0 Commandline Tools

## Abstract

You can also download a [PDF version here](#)<sup>1</sup>.

DRAFT

---

<sup>1</sup> gtCommands.pdf

---

# Table of Contents

I. GSI Commands .....	1
globus-update-certificate-dir .....	2
grid-cert-diagnostics .....	3
grid-cert-info .....	5
grid-cert-request .....	7
grid-default-ca .....	11
grid-change-pass-phrase .....	13
grid-proxy-init .....	14
grid-proxy-destroy .....	17
grid-proxy-info .....	18
grid-mapfile-add-entry .....	20
grid-mapfile-check-consistency .....	22
grid-mapfile-delete-entry .....	24
II. GridFTP Commands .....	26
globus-url-copy .....	27
globus-gridftp-server .....	40
III. GRAM5 Commands .....	53
globus-fork-starter .....	54
globus-gatekeeper-admin .....	56
globus-gatekeeper .....	57
globus-gram-audit .....	60
globus-job-cancel .....	61
globus-job-clean .....	62
globus-job-get-output .....	63
globus-job-manager .....	65
globus-job-run .....	70
globus-job-status .....	73
globus-job-submit .....	75
globus-personal-gatekeeper .....	78
globus-rvf-check .....	80
globus-rvf-edit .....	81
globus-scheduler-event-generator-admin .....	82
globus-scheduler-event-generator .....	83
globusrun .....	84
IV. GSI-OpenSSH Commands .....	88
gsissh .....	89
gsiscp .....	90
gsisftp .....	91
V. Simple CA Commands .....	92
grid-ca-create .....	93
grid-ca-package .....	95
grid-ca-sign .....	97
Glossary .....	99

## List of Figures

1. Effect of Parallel Streams in GridFTP .....	38
--	----

DRAFT

# List of Tables

1. URL formats ..... 29

DRAFT

# GSI Commands

## Table of Contents

globus-update-certificate-dir .....	2
grid-cert-diagnostics .....	3
grid-cert-info .....	5
grid-cert-request .....	7
grid-default-ca .....	11
grid-change-pass-phrase .....	13
grid-proxy-init .....	14
grid-proxy-destroy .....	17
grid-proxy-info .....	18
grid-mapfile-add-entry .....	20
grid-mapfile-check-consistency .....	22
grid-mapfile-delete-entry .....	24

## Name

globus-update-certificate-dir — Update symlinks in the trusted CA directory

## Synopsis

```
globus-update-certificate-dir [-help] [-d DIRECTORY]
```

## Description

The **globus-update-certificate-dir** program creates symlinks between files (CA certificates, certificate revocation lists, signing policy, and certificate request configuration files) using the certificate hash the installed version of OpenSSL uses. OpenSSL 1.0.0 uses a different name hashing algorithm than previous versions, so CA distributions created with older versions of OpenSSL might not be able to locate trusted CAs and related files. Running **globus-update-certificate-dir** against a trusted CA directory will add symlinks to the files to the hash if needed.

The full set of command-line options to **globus-update-certificate-dir** consists of:

- help**                    Display a help message to standard output and exit
- d *DIRECTORY***        Create links in the trusted CA directory *DIRECTORY* instead of using the default search path.

## Environment

If the following variables affect the execution of **globus-update-certificate-dir**

- X509\_CERT\_DIR**        Default trusted certificate directory.
- HOME**                Path to the current user's home directory.
- GLOBUS\_LOCATION**    Path to the Globus installation.

## Name

grid-cert-diagnostics — Print diagnostic information about certificates and keys

## Synopsis

```
grid-cert-diagnostics [-h] | [-help] [-p] [-n] [-c CERTIFICATE]
```

## Description

The **grid-cert-diagnostics** program displays information about the current user's security environment, including information about security-related environment variables, security directory search path, personal key and certificates, and trusted certificates. It is intended to provide information to help diagnose problems using GSIC.

By default, **grid-cert-diagnostics** prints out information regarding the environment and trusted certificate directory. If the `-p` command-line option is used, then additional information about the current user's default certificate and key will be printed.

The full set of command-line options to **grid-cert-diagnostics** consists of:

<code>-h, -help</code>	Display a help message and exit.
<code>-p</code>	Display information about the personal certificate and key that is the current user's default credential.
<code>-n</code>	Check time synchronization with the <b>ntptime</b> command.
<code>-c <i>CERTIFICATE</i>, -c -</code>	Check the validity of the certificate in the file named by <i>CERTIFICATE</i> or standard input if the parameter to <code>-c</code> is <code>-</code> .

## Examples

In this example, we see the default mode of checking the default security environment for the system, without processing the user's key and certificate. Note the user receives a warning about a `cog.properties` and about an expired CA certificate.

```
% grid-cert-diagnostics
```

```
Checking Environment Variables
```

```
=====
```

```
Checking if X509_CERT_DIR is set... no
Checking if X509_USER_CERT is set... no
Checking if X509_USER_KEY is set... no
Checking if X509_USER_PROXY is set... no
```

```
Checking Security Directories
```

```
=====
```

```
Determining trusted cert path... /etc/grid-security/certificates
```

```
Checking for cog.properties... found
```

```
    WARNING: If the cog.properties file contains security properties,
              Java apps will ignore the security paths described in the GSI
              documentation
```

```
Checking trusted certificates...
```



```

=====
Getting trusted certificate list...
Checking CA file /etc/grid-security/certificates/1c4f4c48.0... ok
Verifying certificate chain for "/etc/grid-security/certificates/1c3f2ca8.0"... ok
Checking CA file /etc/grid-security/certificates/9d8788eb.0... ok
Verifying certificate chain for "/etc/grid-security/certificates/9d8753eb.0"... failed
    globus_credential: Error verifying credential: Failed to verify credential
    globus_gsi_callback_module: Could not verify credential
    globus_gsi_callback_module: The certificate has expired:
    Credential with subject: /DC=org/DC=example/OU=grid/CN=CA has expired.

```

In this example, we show a user with a mismatched private key and certificate:

```
% grid-cert-diagnostics -p
```

```

Checking Environment Variables
=====
Checking if X509_CERT_DIR is set... no
Checking if X509_USER_CERT is set... no
Checking if X509_USER_KEY is set... no
Checking if X509_USER_PROXY is set... no

Checking Security Directories
=====
Determining trusted cert path... /etc/grid-security/certificates
Checking for cog.properties... not found

Checking Default Credentials
=====
Determining certificate and key file names... ok
Certificate Path: "/home/juser/.globus/usercert.pem"
Key Path: "/home/juser/.globus/userkey.pem"
Reading certificate... ok
Reading private key...
ok
Checking Certificate Subject...
"/O=Grid/OU=Example/OU=User/CN=Joe User"
Checking cert... ok
Checking key... ok
Checking that certificate contains an RSA key... ok
Checking that private key is an RSA key... ok
Checking that public and private keys have the same modulus... failed
Private key modulus: D294849E37F048C3B5ACEEF2CCDF97D88B679C361E29D5CB5
219C3E948F3E530CFC609489759E1D751F0ACFF0515A614276A0F4C11A57D92D7165B8
FA64E3140155DE448D45C182F4657DA13EDA288423F5B9D169DFF3822EFD81EB2E6403
CE3CB4CCF96B65284D92592BB1673A18354DA241B9AFD7F494E54F63A93E15DCAE2
Public key modulus : C002C7B329B13BFA87BAF214EACE3DC3D490165ACEB791790
600708C544175D9193C9BAC5AED03B7CB49BB6AE6D29B7E635FAC751E9A6D1CEA98022
6F1B63002902D6623A319E4682E7BFB0968DCE962CF218AAD95FAAD6A0BA5C42AA9AAF
7FDD32B37C6E2B2FF0E311310AA55FFB9EAFDF5B995C7D9EEAD8D5D81F3531E0AE5
Certificate and and private key don't match

```

## Name

grid-cert-info — Display information about a certificate

## Synopsis

```
grid-cert-info [-help] [-usage] [-version] [-versions]
```

```
grid-cert-info [-file CERTIFICATE-FILE] [-rfc2253] [-all]
```

```
[-subject] | [-s]
```

```
[-issuer] | [-i]
```

```
[-issuerhash] | [-ih]
```

```
[-startdate] | [-sd]
```

```
[-enddate] | [-ed]
```

## Description

The **grid-cert-info** program displays information contained within a certificate file. By default it shows a text representation of the entire certificate. Specific facts about the certificate can be shown instead by using command-line options. If any of those options are used, then the default display is suppressed. This can be added to the output by using the **-all** command-line option.

If multiple display options are included on the command-line, the facts related to those will be displayed on separate lines in the order that they occur. If an option is specified multiple time, that fact will be displayed multiple times.

The full set of command-line options to **grid-cert-info** are:

<b>-help</b> , <b>-usage</b>	Display the command-line options to <b>grid-cert-info</b> and exit.
<b>-version</b> , <b>-versions</b>	Display the version number of the <b>grid-cert-info</b> command. The second form includes more details.
<b>-file</b> <i>CERTIFICATE-FILE</i>	Display information about the first certificate contained in the file named by <i>CERTIFICATE-FILE</i> instead of the default user certificate.
<b>-rfc2253</b>	Display X.509 distinguished names using the string representation defined in RFC 2253 instead of the default OpenSSL oneline format.
<b>-all</b>	Display the text representation of the entire certificate in addition to any other facts requested by command-line options. This is the default if no fact-specific command-line options are used.
<b>-subject</b> , <b>-s</b>	Display the subject name of the X.509 certificate.
<b>-issuer</b> , <b>-i</b>	Display the issuer name of the X.509 certificate.
<b>-issuerhash</b> , <b>-ih</b>	Display the default hash of the issuer name of the X.509 certificate. This can be used to locate which CA certificate in the trusted certificate directory issued the certificate being inspected.
<b>-startdate</b> , <b>-sd</b>	Display a string representation of the date and time when the certificate is valid from. This is displayed in the format used by the OpenSSL <b>x509</b> command.
<b>-enddate</b> , <b>-ed</b>	Display a string representation of the date and time when the certificate is valid until. This is displayed in the format used by the OpenSSL <b>x509</b> command.

## Examples

Display the validity times for the default certificate

```
% grid-cert-info -sd -ed
Aug 31 12:33:47 2009 GMT
Aug 31 12:33:47 2010 GMT
```

Display the same information about a different certificate specified on the command-line

```
% grid-cert-info -sd -ed -f /etc/grid-security/hostcert.pem
Jan 21 12:24:48 2003 GMT
Jul 15 11:30:57 2020 GMT
```

Display the subject of a certificate in both the default and the RFC 2253 forms.

```
% grid-cert-info -subject
/DC=org/DC=example/DC=grid/CN=Joe User
% grid-cert-info -subject -rfc2253
CN=Joe User,DC=grid,DC=example,DC=org
```

## Environment Variables

The following environment variables affect the execution of **grid-cert-info**:

**X509\_USER\_CERT** Path to the default certificate file to inspect.

## Name

grid-cert-request — Generate a X.509 certificate request and corresponding private key

## Synopsis

```
grid-cert-request [-help] [-h] [-?] [-usage]
[-version] [-versions]
```

```
grid-cert-request [ -cn NAME | -commonname NAME ]
[-dir DIRECTORY] [-prefix PREFIX]
[ -nopw | -nodes | -nopassphrase ]
[ -nopw | -nodes | -nopassphrase ]
[-ca [HASH]] [-verbose] [ -interactive | -int ] [-force]
```

```
grid-cert-request -host FQDN [-service SERVICE] [-dns FQDN...] [-ip IP-ADDRESS...]
[-dir DIRECTORY] [-prefix PREFIX]
[-ca [HASH]] [-verbose] [ -interactive | -int ] [-force]
```

## Description

The **grid-cert-request** program generates an X.509 Certificate Request and corresponding private key for the specified name, host, or service. It is intended to be used with a CA implemented using the `globus_simple_ca` package.

The default behavior of **grid-cert-request** is to generate a certificate request and private key for the user running the command. The subject name is derived from the `gecos` information in the local system's password database, unless the `-commonname`, `-cn`, or `-host` command-line options are used.

By default, **grid-cert-request** writes user certificate requests and keys to the `$HOME/.globus` directory, and host and service certificate requests and keys to `/etc/grid-security`. This can be overridden by using the `-dir` command-line option.

The full set of command-line options to **grid-cert-request** are:

<code>-help</code> , <code>-h</code> , <code>-?</code> , <code>-usage</code>	Display the command-line options to <b>grid-cert-request</b> and exit.
<code>-version</code> , <code>-versions</code>	Display the version number of the <b>grid-cert-request</b> command. The second form includes more details.
<code>-cn NAME</code> , <code>-commonname NAME</code>	Create a certificate request with the common name component of the subject set to <i>NAME</i> . This is used to create user identity certificates.
<code>-dir DIRECTORY</code>	Write the certificate request and key to files in the directory specified by <i>DIRECTORY</i> .
<code>-prefix PREFIX</code>	Use the string <i>PREFIX</i> as the base name of the certificate, <code>certificate_request</code> , and key files instead of the default. For a user certificate request, this would mean creating files <code>\$HOME/.globus/PREFIXcert_request.pem</code> , <code>\$HOME/.globus/PREFIXcert.pem</code> , and <code>\$HOME/.globus/PREFIXkey.pem</code> .
<code>-ca CA-HASH</code>	Use the certificate request configuration for the CA with the name hash <i>CA-HASH</i> instead of the default CA chosen by running <b>grid-default-ca</b> .
<code>-verbose</code>	Keep the output from the OpenSSL certificate request command visible after it completes, instead of clearing the screen..

<code>-interactive, -int</code>	Prompt for each component of the subject name of the request, instead of generating the common name from other command-line options. Note that CAs may not sign certificates for subject names that don't match their signing policies.
<code>-force</code>	Overwrite any existing certificate request and private key with a new one.
<code>-nopw, -nodes, -nopassphrase</code>	Create an unencrypted private key for the certificate instead of prompting for a passphrase. This is the default behavior for host or service certificates, but not recommended for user certificates.
<code>-host FQDN</code>	Create a certificate request for use on a particular host. This option also causes the private key associated with the certificate request to be unencrypted. The <i>FQDN</i> argument to this option should be the fully qualified domain name of the host that will use this certificate. The subject name of the certificate will be derived from the <i>FQDN</i> and the service option if specified by the <code>-service</code> command-line option. If the host for the certificate has multiple names, then use either the <code>-dns</code> or <code>-ip</code> command-line options to add alternate names or addresses to the certificates.
<code>-service SERVICE</code>	Create a certificate request for a particular service on a host. The subject name of the certificate will be derived from the <i>FQDN</i> passed as the argument to the <code>-host</code> command-line option and the <i>SERVICE</i> string.
<code>-dns FQDN,...</code>	Create a certificate request containing a <code>subjectAltName</code> extension containing one or more host names. This is used when a certificate may be used by multiple virtual servers or if a host has different names when contacted within or outside a private network. Multiple DNS names can be included in the extension by separating them with a comma.
<code>-ip IP-ADDRESS,...</code>	Create a certificate request containing a <code>subjectAltName</code> extension containing the IP addresses named by the <i>IP-ADDRESS</i> strings. This is used when a certificate may be used by services listening on multiple networks. Multiple IP addresses can be included in the extension by separating them with a comma.

## Examples

Create a user certificate request:

```
% grid-cert-request
```

A certificate request and private key is being created.

You will be asked to enter a PEM pass phrase.

This pass phrase is akin to your account password, and is used to protect your key file.

If you forget your pass phrase, you will need to obtain a new certificate.

A private key and a certificate request has been generated with the subject:

```
/O=org/OU=example/OU=grid/CN=Joe User
```

If the CN=Joe User is not appropriate, rerun this script with the `-force -cn "Common Name"` options.

Your private key is stored in `/home/juser/.globus/userkey.pem`

Your request is stored in `/home/juser/.globus/usercert_request.pem`

Please e-mail the request to the Example CA `ca@grid.example.org`  
You may use a command similar to the following:

```
cat /home/juser/.globus/usercert_request.pem | mail ca@grid.example.org
```

Only use the above if this machine can send AND receive e-mail. if not, please mail using some other method.

Your certificate will be mailed to you within two working days.  
If you receive no response, contact Example CA at `ca@grid.example.org`

Create a host certificate for a host with two names.

```
% grid-cert-request -host grid.example.org -dns grid.example.org,grid-internal.example.org
```

A private host key and a certificate request has been generated  
with the subject:

```
/O=org/OU=example/OU=grid/CN=host/grid.example.org
```

-----  
The private key is stored in `/etc/grid-security/hostkey.pem`  
The request is stored in `/etc/grid-security/hostcert_request.pem`

Please e-mail the request to the Example CA `ca@grid.example.org`  
You may use a command similar to the following:

```
cat /etc/grid-security/hostcert_request.pem | mail ca@grid.example.org
```

Only use the above if this machine can send AND receive e-mail. if not, please mail using some other method.

Your certificate will be mailed to you within two working days.  
If you receive no response, contact Example CA at  
`ca@grid.example.org`

## Environment Variables

The following environment variables affect the execution of **grid-cert-request**:

<code>X509_CERT_DIR</code>	Path to the directory containing SSL configuration files for generating certificate requests.
<code>GRID_SECURITY_DIR</code>	Path to the directory containing SSL configuration files for generating certificate requests. This value is used if <code>X509_CERT_DIR</code> is not set.
<code>GLOBUS_LOCATION</code>	Path to the directory containing the Globus Toolkit. This is searched if neither the <code>X509_CERT_DIR</code> nor the <code>GRID_SECURITY_DIR</code> environment variables are set.

## Files

<code>\$HOME/.globus/ usercert_request.pem</code>	Default path to write a user certificate request.
---	---

<code>\$HOME/.globus/ usercert.pem</code>	Default path to write a user certificate.
<code>\$HOME/.globus/ userkey.pem</code>	Default path to write a user private key.
<code>/etc/grid-security/ hostcert_request.pem</code>	Default path to write a host certificate request.
<code>/etc/grid-security/ hostcert.pem</code>	Default path to write a host certificate.
<code>/etc/grid-security/ hostkey.pem</code>	Default path to write a host private key.
<code>TRUSTED-CERT-DIR/globus- user-ssl.conf, TRUSTED- CERT-DIR/globus-user- ssl.conf.CA-HASH</code>	SSL configuration file for requesting a user certificate. The first form is the default location, the second form is used when the <code>-ca</code> command-line option is specified.
<code>TRUSTED-CERT-DIR/globus- host-ssl.conf, TRUSTED- CERT-DIR/globus-host- ssl.conf.CA-HASH</code>	SSL configuration file for requesting a host or service certificate. The first form is the default location, the second form is used when the <code>-ca</code> command-line option is specified.

## Name

grid-default-ca — Select default CA for certificate requests

## Synopsis

```
grid-default-ca [-help] [-h] [-usage] [-u] [-version] [-versions]
```

```
grid-default-ca -list [-dir CA-DIRECTORY]
```

```
grid-default-ca [-ca CA-HASH] [-dir CA-DIRECTORY]
```

## Description

The **grid-default-ca** program sets the default certificate authority to use when the **grid-cert-request** script is run. The CA's certificate, configuration, and signing policy must be installed in the trusted certificate directory to be able to request certificates from that CA. Note that some CAs have different policies and use other tools to handle certificate requests. Please consult your CA's support staff if you are unsure. The **grid-default-ca** is designed to work with CAs implemented using the `globus_simple_ca` package.

By default, the **grid-default-ca** program displays a list of installed CA certificates and prompts the user for which one to set as the default. If invoked with the `-list` command-line option, **grid-default-ca** will print the list and not prompt nor set the default CA. If invoked with the `-ca` option, it will not list or prompt, but set the default CA to the one with the hash that matches the `CA-HASH` argument to that option. If **grid-default-ca** is used to set the default CA, the caller of this program must have write permissions to the trusted certificate directory.

The **grid-default-ca** program sets the CA in the one of the grid security directories. It looks in the directory named by the `GRID_SECURITY_DIR` environment, the `X509_CERT_DIR`, `/etc/grid-security`, and `$GLOBUS_LOCATION/share/certificates`.

The full set of command-line options to **grid-default-ca** are:

<code>-help, -h, -usage, -u</code>	Display the command-line options to <b>grid-default-ca</b> and exit.
<code>-version, -versions</code>	Display the version number of the <b>grid-default-ca</b> command. The second form includes more details.
<code>-dir CA-DIRECTORY</code>	Use the trusted certificate directory named by <code>CA-DIRECTORY</code> instead of the default.
<code>-list</code>	Instead of changing the default CA, print out a list of all available CA certificates in the trusted certificate directory
<code>-ca CA-HASH</code>	Set the default CA without displaying the list of choices or prompting. The CA file named by <code>CA-HASH</code> must exist.

## Examples

List the contents of the trusted certificate directory that contain the string Example:

```
% grid-default-ca | grep Example
15) cd1186ff - /DC=org/DC=Example/DC=Grid/CN=Example CA
```

Choose that CA as the default:

```
% grid-default-ca -ca cd1186ff
```



setting the default CA to: /DC=org/DC=Example/DC=Grid/CN=Example CA

linking /etc/grid-security/certificates/grid-security.conf.cd1186ff to  
/etc/grid-security/certificates/grid-security.conf

linking /etc/grid-security/certificates/grid-host-ssl.conf.cd1186ff to  
/etc/grid-security/certificates/grid-host-ssl.conf

linking /etc/grid-security/certificates/grid-user-ssl.conf.cd1186ff to  
/etc/grid-security/certificates/grid-user-ssl.conf

...done.

## Environment Variables

The following environment variables affect the execution of **grid-default-ca**:

GRID_SECURITY_DIRECTORY	Path to the default trusted certificate directory.
X509_CERT_DIR	Path to the default trusted certificate directory.
GLOBUS_LOCATION	Path to the Globus Toolkit installation directory.

## Bugs

The **grid-default-ca** program displays CAs from all of the directories in its search list; however, **grid-cert-request** only uses the first which contains a grid security configuration.

The **grid-default-ca** program may display the same CA multiple times if it is located in multiple directories in its search path. However, it does not provide any information about which one would actually be used by the **grid-cert-request** command.

## See Also

grid-cert-request(1)

## Name

grid-change-pass-phrase — Change the passphrase of a private key

## Synopsis

```
grid-change-pass-phrase [-help] [-usage] [-version] [-versions]
```

```
grid-change-pass-phrase [-file PRIVATE-KEY]
```

## Description

The **grid-change-pass-phrase** program changes the passphrase protecting a private key or PKCS12 bundle containing a private key and certificate. By default, **grid-change-pass-phrase** uses the `X509_USER_KEY` environment variable to locate the private key. If that is not set, then it looks for `$HOME/.globus/userkey.pem` and `$HOME/.globus/usercred.p12` in succession. The path to a key can be specified by using the `-file` command-line option.

The full set of command-line options to **grid-change-pass-phrase** are:

<code>-help, -usage</code>	Display the command-line options to <b>grid-change-pass-phrase</b> and exit.
<code>-version, -versions</code>	Display the version number of the <b>grid-change-pass-phrase</b> command. The second form includes more details.
<code>-file <i>PRIVATE-KEY</i></code>	Change the passphrase of the private key named by <i>PRIVATE-KEY</i> instead of the default.

## Examples

Change the passphrase of the default private key:

```
% grid-change-pass-phrase
```

```
Enter pass phrase for /home/juser/.globus/userkey.pem:  
writing RSA key  
Enter PEM pass phrase:  
Verifying - Enter PEM pass phrase:
```

## Environment Variables

The following environment variables affect the execution of **grid-change-pass-phrase**:

`X509_USER_KEY` Path to the default private key file.

## Name

grid-proxy-init — Generate a new proxy certificate

## Synopsis

```
grid-proxy-init [-help] [-usage] [-version]
```

```
grid-proxy-init [-debug] [-q] [-verify]
[[-valid HOURS:MINUTES] | [-hours HOURS]] [-cert CERTFILE] [-key KEYFILE] [-certdir CERTDIR] [-out
PROXYPATH] [-bits BITS]
[-policy POLICYFILE]
[[-pl POLICY-OID] | [-policy-language POLICY-OID]] [-path-length MAXIMUM] [-pwstdin] [-limited] [-
independent] [[-draft] | [-old] | [-rfc]]
```

## Description

The **grid-proxy-init** program generates X.509 proxy certificates derived from the currently available certificate files. By default, this command generates a [RFC 3820](http://www.ietf.org/rfc/rfc3820.txt)<sup>1</sup> Proxy Certificate with a 512 bit key valid for 12 hours in a file named `/tmp/x509up_uUID`. Command-line options and variables can modify the format, strength, lifetime, and location of the generated proxy certificate.

X.509 proxy certificates are short-lived certificates, signed usually by a user's identity certificate or another proxy certificate. The key associated with a proxy certificate is unencrypted, so applications can authenticate using a proxy identity without providing a passphrase.

Proxy certificates provide a convenient alternative to constantly entering passwords, but are also less secure than the user's normal security credential. Therefore, they should always be user-readable only (this is enforced by the GSI libraries), and should be deleted after they are no longer needed.

This version of **grid-proxy-init** supports three different proxy formats: the old proxy format used in early releases of the Globus Toolkit up to version 2.4.x, an IETF draft version of X.509 Proxy Certificate profile used in Globus Toolkit 3.0.x and 3.2.x, and the RFC 3820 profile used in Globus Toolkit Version 4.0.x and 4.2.x. By default, this version of **grid-proxy-init** creates an RFC 3820 compliant proxy. To create a proxy compatible with older versions of the Globus Toolkit, use the `-old` or `-draft` command-line options.

The full set of command-line options to **grid-proxy-init** are:

<code>-help, -usage</code>	Display the command-line options to <b>grid-proxy-init</b> .
<code>-version</code>	Display the version number of the <b>grid-proxy-init</b> command
<code>-debug</code>	Display information about the path to the certificate and key used to generate the proxy certificate, the path to the trusted certificate directory, and verbose error messages
<code>-q</code>	Suppress all output from <b>grid-proxy-init</b> except for passphrase prompts.
<code>-verify</code>	Perform certificate chain validity checks on the generated proxy.
<code>-valid <i>HOURS:MINUTES</i>, -hours <i>HOURS</i></code>	Create a certificate that is valid for <i>HOURS</i> hours and <i>MINUTES</i> minutes. If not specified, the default of twelve hours and no minutes is used.
<code>-cert <i>CERTFILE</i>, -key <i>KEYFILE</i></code>	Create a proxy certificate signed by the certificate located in <i>CERTFILE</i> using the key located in <i>KEYFILE</i> . If not specified the default certificate and

<sup>1</sup> <http://www.ietf.org/rfc/rfc3820.txt>

	key will be used. This overrides the values of environment variables described below.
<code>-certdir CERTDIR</code>	Search <i>CERTDIR</i> for trusted certificates if verifying the proxy certificate. If not specified, the default trusted certificate search path is used. This overrides the value of the <code>X509_CERT_DIR</code> environment variable
<code>-out PROXYPATH</code>	Write the generated proxy certificate file to <i>PROXYPATH</i> instead of the default path of <code>/tmp/x509up_uUID</code> .
<code>-bits BITS</code>	When creating the proxy certificate, use a <i>BITS</i> bit key instead of the default 512 bit keys.
<code>-policy POLICYFILE</code>	Add the certificate policy data described in <i>POLICYFILE</i> as the ProxyCertInfo X.509 extension to the generated proxy certificate.
<code>-pl POLICY-OID, -policy-language POLICY-OID</code>	Set the policy language identifier of the policy data specified by the <code>-policy</code> command-line option to the oid specified by the <i>POLICY-OID</i> string.
<code>-path-length MAXIMUM</code>	Set the maximum length of the chain of proxies that can be created by the generated proxy to <i>MAXIMUM</i> . If not set, the default of an unlimited proxy chain length is used.
<code>-pwstdin</code>	Read the private key's passphrase from stdin instead of reading input from the controlling tty. This is useful when scripting <b>grid-proxy-init</b> .
<code>-limited</code>	Create a limited proxy. Limited proxies are generally refused by process-creating services, but may be used to authorize with other services.
<code>-independent</code>	Create an independent proxy. An independent proxy is not treated as an impersonation proxy but as a separate identity for authorization purposes.
<code>-draft</code>	Create a IETF draft proxy instead of the default RFC 3280-compliant proxy. This type of proxy uses a non-standard proxy policy identifier. This might be useful for authenticating with older versions of the Globus Toolkit.
<code>-old</code>	Create a legacy proxy instead of the default RFC 3280-compliant proxy. This type of proxy uses a non-standard method of indicating that the certificate is a proxy and whether it is limited. This might be useful for authenticating with older versions of the Globus Toolkit.
<code>-rfc</code>	Create an RFC 3820-compliant proxy certificate. This is the default for this version of <b>grid-proxy-init</b> .

## Examples

To create a proxy with the default lifetime and format, run the **grid-proxy-init** program with no arguments. For example:

```
% grid-proxy-init
Your identity: /DC=org/DC=example/CN=Joe User
Enter GRID pass phrase for this identity:
Creating proxy ..... Done
Your proxy is valid until: Thu Mar 18 03:48:05 2010
```

To create a stronger proxy that lasts for only 8 hours, use the `-hours` and `-bits` command-line options to **grid-proxy-init**. For example:

```
% grid-proxy-init -hours 8 -bits 1024
Your identity: /DC=org/DC=example/CN=Joe User
Enter GRID pass phrase for this identity:
Creating proxy ..... Done
Your proxy is valid until: Thu Mar 17 23:48:05 2010
```

## Environment Variables

The following environment variables affect the execution of **grid-proxy-init**:

<code>X509_USER_CERT</code>	Path to the certificate to use as issuer of the new proxy.
<code>X509_USER_KEY</code>	Path to the key to use to sign the new proxy.
<code>X509_CERT_DIR</code>	Path to the directory containing trusted certificate certificates and signing policies.

## Files

The following files affect the execution of **grid-proxy-init**:

<code>\$HOME/.globus/usercert.pem</code>	Default path to the certificate to use as issuer of the new proxy.
<code>\$HOME/.globus/userkey.pem</code>	Default path to the key to use to sign the new proxy.

## Compatibility

For more information about proxy certificate types and their compatibility in GT, see <http://dev.globus.org/wiki/Security/ProxyCertTypes>.

## See Also

`grid-proxy-destroy(1)`, `grid-proxy-info(1)`

## Name

grid-proxy-destroy — Destroy the default proxy certificate

## Synopsis

```
grid-proxy-destroy [-help] [-usage] [-version]
```

```
grid-proxy-destroy [-debug] [-dryrun] [-default] [-all] [--] [FILENAME...]
```

## Description

The **grid-proxy-destroy** program removes X.509 proxy files from the local filesystem. It overwrites the data in the files and removes the files from the filesystem. By default, it removes the current user's default proxy (either `/tmp/x509up_uUID` where `UID` is the current POSIX user id, or the file pointed to by the `X509_USER_PROXY` environment variable) unless a list of proxy file paths are included as part of the command line.

Use the `--` command-line option to separate a list of proxy paths from command line options if the proxy file begins with the `-` character.

The full list of command-line options to **grid-proxy-destroy** are:

- `-help, -usage` Display the command-line options to **grid-proxy-destroy**.
- `-version` Display the version number of the **grid-proxy-destroy** command
- `-debug` Display verbose error messages.
- `-dryrun` Do not remove the proxy, but display the path of the files that would have been removed, or the directory where they would have been removed from if the `-all` command-line option is used.
- `-default` Remove the default proxy in addition to the files included on the command-line. Only needed if other paths are included on the command-line.
- `-all` Remove the default proxy and all delegated proxies in the temporary file directory.

## Environment Variables

The following environment variables affect the execution of **grid-proxy-destroy**:

`X509_USER_PROXY` Path to the default user proxy.

## See Also

`grid-proxy-init(1)`, `grid-proxy-info(1)`

## Name

grid-proxy-info — Display information about a proxy certificate

## Synopsis

```
grid-proxy-info [-help] [-usage] [-version]
```

```
grid-proxy-info [[-subject] | [-s]]
[[-issuer] | [-i]]
[-identity] [-type] [-timeleft] [-strength] [-all] [-text] [-path] [-rfc2253]
[{ -exists | -e }
[[-valid HOURS:MINUTES] | [-v HOURS:MINUTES]]
[[-hours HOURS] | [-h HOURS]]
[[-bits BITS] | [-b BITS]]]
```

## Description

The **grid-proxy-info** program extracts information from an X.509 proxy certificates, and optionally displays or returns an exit code based on that information.

The default mode of operation is to print the following facts about the current user's default proxy: subject, issuer, identity, type, strength, path, and time left. If the command-line option `-exists` or `-e` is included in the command-line, nothing is printed unless one of the print options is specified. Instead, **grid-proxy-info** determines if a valid proxy exists and, if so, exits with the exit code 0; if a proxy does not exist or is not valid, **grid-proxy-info** exits with the exit code 1. Additional validity criteria can be added by using the `-valid`, `-v`, `-hours`, `-h`, `-bits`, or `-b` command-line options. If used, these options must occur *after* the `-e` or `-exists` command-line options. Those options are only valid if one of the `-e` or `-exists` command-line options is used.

The complete set of command-line options to **grid-proxy-info** are:

<code>-help</code> , <code>-usage</code>	Display the command-line options to <b>grid-proxy-info</b> .
<code>-version</code>	Display the version number of the <b>grid-proxy-info</b> command
<code>-debug</code>	Display verbose error messages.
<code>-file PROXYFILE</code> , <code>-f PROXYFILE</code>	Read the proxy located in the file <i>PROXYFILE</i> instead of using the default proxy.
<code>-subject</code> , <code>-s</code>	Display the proxy certificate's subject distinguished name.
<code>-issuer</code> , <code>-i</code>	Display the proxy certificate issuer's distinguished name.
<code>-identity</code>	Display the proxy certificate's identity. For non-independent proxies, the identity is the subject of the certificate which issued the first proxy in the proxy chain.
<code>-type</code>	Display the type of proxy certificate. The type string includes the format ("legacy", "draft", or RFC 3280 compliant), identity type ("impersonation" or "independent"), and policy ("limited" or "full"). See <code>grid-proxy-init(1)</code> for information about how to create different types of proxies.
<code>-timeleft</code>	Display the number of seconds remaining until the proxy certificate expires.
<code>-strength</code>	Display the strength (in bits) of the key associated with the proxy certificate.

<code>-all</code>	Display the default information for the proxy when also using the <code>-e</code> or <code>-exists</code> command-line option.
<code>-text</code>	Display the proxy certificate contents to standard output, including policy information, issuer, public key, and modulus.
<code>-path</code>	Display the path to the file containing the default proxy certificate.
<code>-rfc2253</code>	Display distinguished names for the subject, issuer, and identity using the string representation described in RFC 2253, instead of the legacy format.
<code>-exists, -e</code>	Perform an existence and validity check for the proxy. If a valid proxy exists and matches the criteria described by other command-line options (if any), exit with 0; otherwise, exit with 1. This option must be before other validity check predicate in the command-line options. If this option is specified, the output of the default facts about the proxy is disabled. Use the <code>-all</code> option to have the information displayed as well as the exit code set.
<code>-valid HOURS:MINUTES, -v HOURS:MINUTES, -hours HOURS, -h HOURS</code>	Check that the proxy certificate is valid for at least <i>HOURS</i> hours and <i>MINUTES</i> minutes. If it is not, <b>grid-proxy-info</b> will exit with exit code 1.
<code>-bits BITS, -b BITS</code>	Check that the proxy certificate key strength is at least <i>BITS</i> bits.

## Environment Variables

The following environment variables affect the execution of **grid-proxy-info**:

`X509_USER_PROXY` Path to the default user proxy.

## See Also

`grid-proxy-init(1)`, `grid-proxy-destroy(1)`



## Name

grid-mapfile-add-entry — Add an entry to a gridmap file

## Synopsis

```
grid-mapfile-add-entry [-help] [-usage] [-version] [-versions]
```

```
grid-mapfile-add-entry {-dn DISTINGUISHED-NAME} {-ln LOCAL-NAME... }
[[-d] | [-dryrun]]
[[-mapfile MAPFILE] | [-f MAPFILE]]
```

## Description

The **grid-mapfile-add-entry** program adds a new mapping from an X.509 distinguished name to a local POSIX user name to a gridmap file. Gridmap files are used as a simple authorization method for services such as GRAM5 or GridFTP.

The **grid-mapfile-add-entry** program verifies that the *LOCAL-NAME* is a valid user name on the system on which it was run, and that the mapping between *DISTINGUISHED-NAME* and *LOCAL-NAME* does not already exist in the gridmap file.

By default, **grid-mapfile-add-entry** will modify the gridmap file named by the GRIDMAP environment variable if present, or the file `/etc/grid-security/grid-mapfile` if not. This can be changed by the use of the `-mapfile` or `-f` command-line options.

If the gridmap file does not exist, **grid-mapfile-add-entry** will create it. If it already exists, **grid-mapfile-add-entry** will save the current contents of the file to a new file with the string `.old` appended to the file name.

The full set of command-line options to **grid-mapfile-add-entry** are:

<code>-help, -usage</code>	Display the command-line options to <b>grid-mapfile-add-entry</b> .
<code>-version, -versions</code>	Display the version number of the <b>grid-mapfile-add-entry</b> command. The second form includes more details.
<code>-dn <i>DISTINGUISHED-NAME</i></code>	The X.509 distinguished name to add a mapping for. The name should be in OpenSSL's oneline format.
<code>-ln <i>LOCAL-NAME...</i></code>	The POSIX user name to map the distinguished name to. This name must be a valid username. Add multiple <i>LOCAL-NAME</i> strings after the <code>-ln</code> command-line option. If any of the local names are invalid, no changes will be made to the gridmap file. Note that if multiple occurrences of the <code>-ln</code> command-line option are present, only the the last one will be added.
<code>-d, -dryrun</code>	Verify local names and display diagnostics about what would be added to the gridmap file, but don't actually modify the file.
<code>-mapfile <i>MAPFILE</i>, -f <i>MAPFILE</i></code>	Modify the gridmap file named by <i>MAPFILE</i> instead of the default.

## Examples

Add a mapping between the current user's certificate to the current user id to a gridmap file in `$HOME/.gridmap`:

```
% grid-mapfile-add-entry -f $HOME/.gridmap -dn "`grid-cert-info -subject`" -ln "`id -un`"
```

```
Modifying /home/juser/.gridmap ...  
/home/juser/.gridmap does not exist... Attempting to create /home/juser/.gridmap  
New entry:  
"/DC=org/DC=example/DC=grid/CN=Joe User" juser  
(1) entry added
```

Add a mapping between the a distinguished name and multiple local names:

```
% grid-mapfile-add-entry -dn "/DC=org/DC=example/DC=grid/CN=Joe User" juser" local1 local2  
Modifying /home/juser/.gridmap ...  
/home/juser/.gridmap does not exist... Attempting to create /home/juser/.gridmap  
New entry:  
"/DC=org/DC=example/DC=grid/CN=Joe User" local1,local2  
(1) entry added
```

## Environment Variables

The following environment variables affect the execution of **grid-mapfile-add-entry**:

**GRIDMAP** Path to the default gridmap to modify.

## Files

The following files affect the execution of **grid-mapfile-add-entry**:

/etc/grid-security/grid-mapfile	Path to the default gridmap to modify if <b>GRIDMAP</b> environment variable is not set.
---------------------------------	--

## See Also

grid-mapfile-check-consistency(8), grid-mapfile-delete-entry(8)

## Name

grid-mapfile-check-consistency — Add an entry to a grid map file

## Synopsis

```
grid-mapfile-check-consistency [-h] [-help] [-usage] [-version]
```

```
grid-mapfile-check-consistency [-mapfile MAPFILE] | [-f MAPFILE]
```

## Description

The **grid-mapfile-check-consistency** program performs basic checks for validity of a gridmap file. These checks include checks for existence, duplication of entries, and valid local user names. If the gridmap file is valid, **grid-mapfile-check-consistency** exits with a zero exit code, otherwise it exits with a non-zero exit code. In either case, it displays information about its progress as it parses and validates the gridmap file.

By default, **grid-mapfile-check-consistency** will check the gridmap file named by the GRIDMAP environment variable if present. If that variable is not set, it will check the file `$HOME/.gridmap` for non-root users if present. If that doesn't exist or **grid-mapfile-check-consistency** is run as root, it will then check `/etc/grid-security/grid-mapfile`. This can be changed by the use of the `-mapfile` or `-f` command-line options.

The full set of command-line options to **grid-mapfile-check-consistency** are:

<code>-help, -h, -usage</code>	Display the command-line options to <b>grid-mapfile-check-consistency</b> .
<code>-version</code>	Display the version number of the <b>grid-mapfile-check-consistency</b> command.
<code>-mapfile <i>MAPFILE</i>, -f <i>MAPFILE</i></code>	Check the gridmap file named by <i>MAPFILE</i> instead of the default.

## Examples

Check that the gridmap file in `/etc/grid-security` is valid:

```
% grid-mapfile-check-consistency -f /etc/grid-security/grid-mapfile
Checking /etc/grid-security/grid-mapfile
Verifying grid mapfile existence...OK
Checking for duplicate entries...OK
Checking for valid user names...OK
```

Check a gridmap file that has an invalid local user name:

```
% grid-mapfile-check-consistency -f /etc/grid-security/grid-mapfile
Checking /etc/grid-security/grid-mapfile
Verifying grid mapfile existence...OK
Checking for duplicate entries...OK
ERROR: baduser is not a valid local username
ERROR: Found 1 invalid username(s)
```

## Environment Variables

The following environment variables affect the execution of **grid-mapfile-check-consistency**:

**GRIDMAP** Path to the default gridmap to check.

## Files

The following files affect the execution of **grid-mapfile-check-consistency**:

<code>\$HOME/.gridmap</code>	Path to the default gridmap to check if the GRIDMAP environment variable is not set for non-root users.
<code>/etc/grid-security/grid-mapfile</code>	Path to the default gridmap to check if GRIDMAP environment variable is not set and the above file does not exist.

## See Also

`grid-mapfile-add-entry(8)`, `grid-mapfile-delete-entry(8)`

DRAFT

## Name

grid-mapfile-delete-entry — Remove entries from a gridmap file

## Synopsis

```
grid-mapfile-delete-entry [-help] [-usage] [-version] [-versions]
```

```
grid-mapfile-delete-entry {-dn DISTINGUISHED-NAME} {-ln LOCAL-NAME...}  
[[-d] | [-dryrun]]  
[[-mapfile MAPFILE] | [-f MAPFILE]]
```

## Description

The **grid-mapfile-delete-entry** program deletes mappings from a gridmap file. If both the *-dn* and *-ln*> options are specified, **grid-mapfile-delete-entry** removes entries which meet both criteria (remove entries mapping *DISTINGUISHED-NAME* to *LOCAL-NAME* for each *LOCAL-NAME* specified). If only *-dn* or *-ln* is specified *all* entries for that *DISTINGUISHED-NAME* or *LOCAL-NAME* are removed.

By default, **grid-mapfile-delete-entry** will modify the gridmap file named by the GRIDMAP environment variable if present, or the file `/etc/grid-security/grid-mapfile` if not. This can be changed by the use of the *-mapfile* or *-f* command-line options.

Prior to modifying a gridmap file, **grid-mapfile-delete-entry** saves its current contents to a file with the string `.old` appended to the original file name.

The full set of command-line options to **grid-mapfile-delete-entry** are:

<i>-help</i> , <i>-usage</i>	Display the command-line options to <b>grid-mapfile-delete-entry</b> .
<i>-version</i> , <i>-versions</i>	Display the version number of the <b>grid-mapfile-delete-entry</b> command. The second form includes more details.
<i>-dn</i> <i>DISTINGUISHED-NAME</i>	The X.509 distinguished name to remove from the gridmap file. If the <i>-ln</i> option is not specified, remove all entries for this name; otherwise, remove entries that match both this name and the local name. The name should be in OpenSSL's oneline format.
<i>-ln</i> <i>LOCAL-NAME...</i>	The POSIX user name to remove from the gridmap file. Include multiple <i>LOCAL-NAME</i> strings after the <i>-ln</i> command-line option to remove multiple names from the gridmap. If the <i>-dn</i> option is not specified, remove all entries for these names; otherwise, remove entries that match the <i>DISTINGUISHED-NAME</i> and any of the <i>LOCAL-NAME</i> values.
<i>-d</i> , <i>-dryrun</i>	Display diagnostics about what would be removed from the gridmap file, but don't actually modify the file.
<i>-mapfile</i> <i>MAPFILE</i> , <i>-f</i> <i>MAPFILE</i>	Modify the gridmap file named by <i>MAPFILE</i> instead of the default.

## Examples

Remove all mappings for a distinguished name:

```
% grid-mapfile-delete-entry "/DC=org/DC=example/DC=grid/CN=Joe User"
```

```
Modifying /etc/grid-security/grid-mapfile ...
Deleting entry: "/DC=org/DC=example/DC=grid/CN=Joe User" juser,juser2
(1) entry deleted
```

Remove the mapping between a distinguished name and a single local username:

```
% grid-mapfile-delete-entry "/DC=org/DC=example/DC=grid/CN=Joe User" -ln juser2
Modifying /etc/grid-security/grid-mapfile ...
Current entry: "/DC=org/DC=example/DC=grid/CN=Joe User" juser
(1) mapping removed: (juser2), (0) not present and ignored
(0) entries deleted
```

## Environment Variables

The following environment variables affect the execution of **grid-mapfile-delete-entry**:

**GRIDMAP** Path to the default gridmap to modify.

## Files

The following files affect the execution of **grid-mapfile-delete-entry**:

/etc/grid-security/grid-mapfile	Path to the default gridmap to modify if <b>GRIDMAP</b> environment variable is not set.
---------------------------------	--

## See Also

grid-mapfile-add-entry(8), grid-mapfile-check-consistency(8)

# GridFTP Commands

## Table of Contents

globus-url-copy .....	27
globus-gridftp-server .....	40

DRAFT

## Name

globus-url-copy — Multi-protocol data movement

## Synopsis

globus-url-copy

## Tool description

**globus-url-copy** is a scriptable command line tool that can do multi-protocol data movement. It supports gsiftp:// (GridFTP), ftp://, http://, https://, and file:/// protocol specifiers in the URL. For GridFTP, globus-url-copy supports all implemented functionality. Versions from GT 3.2 and later support file globbing and directory moves.

- [Before you begin](#)
- [Command syntax](#)
- [Command line options](#)
  - [Informational options](#)
  - [Utility options](#)
  - [Reliability options](#)
  - [Performance options](#)
  - [Security-related options](#)
- [Default usage](#)
- [MODES in GridFTP](#)
- [If you run a GridFTP server by hand](#)
- [How do I choose a value for the TCP buffer size \(-tcp-bs\) option?](#)
- [How do I choose a value for the parallelism \(-p\) option?](#)
- [Limitations](#)
- [Interactive clients for GridFTP](#)

## Before you begin

### Important

To use gsiftp:// and https:// protocols in globus-url-copy, you must have a [certificate](#). However, you may use ftp://, http:// or sshftp:// protocols without a certificate.

1. First, as with all things Grid, you *must* have a valid proxy certificate to run globus-url-copy in certain protocols (gsiftp:// and https://, as noted above). If you are using ftp://, http:// or sshftp:// protocols, you may skip ahead to [Command syntax](#)



If you do not have a certificate, you must obtain one.

If you are doing this for testing in your own environment, the SimpleCA provided with the Globus Toolkit should suffice.

If not, you must contact the Virtual Organization (VO) with which you are associated to find out whom to ask for a certificate.

One common source is the DOE Science Grid CA<sup>1</sup>, although you must confirm whether or not the resources you wish to access will accept their certificates.

Instructions for proper installation of the certificate should be provided from the source of the certificate.

Please note when your certificates expire; they will need to be renewed or you may lose access to your resources.

2. Now that you have a certificate, you must generate a temporary proxy. Do this by running:

```
grid-proxy-init
```

Further documentation for **grid-proxy-init** can be found here.

3. You are now ready to use **globus-url-copy**! See the following sections for syntax and command line options and other considerations.

## Command syntax

The basic syntax for **globus-url-copy** is:

```
globus-url-copy [optional command line switches] Source_URL Destination_URL
```

where:

[optional command line switches]	See <u>Command line options</u> below for a list of available options.
<i>Source_URL</i>	Specifies the original URL of the file(s) to be copied.  If this is a directory, all files within that directory will be copied.
<i>Destination_URL</i>	Specifies the URL where you want to copy the files.  If you want to copy multiple files, this must be a directory.



### Note

Any url specifying a directory must end with /.

## URL prefixes

Versions from GT 3.2 and later support the following URL prefixes:

- **file://** (on a local machine only)

- `ftp://`
- `gsiftp://`
- `http://`
- `https://`

Versions from GT 4.2 and later support the following URL prefix (in addition to the above-mentioned URL prefixes):

- `sshftp://`



## Note

We do *not* provide an interactive client similar to the generic FTP client provided with Linux. See the [Interactive Clients](#) section below for information on an interactive client developed by NCSA/NMI/TeraGrid.

## URL formats

URLs can be any valid URL as defined by RFC 1738 that have a [protocol](#) we support. In general, they have the following format: `protocol://host:port/path`.



## Note

If the path ends with a trailing / (i.e. `/path/to/directory/`) it will be considered to be a directory and all files in that directory will be moved. If you want a recursive directory move, you need to add the `-r/-recurse` switch described below.

**Table 1. URL formats**

<code>gsiftp://myhost.mydomain.com:2812/data/foo.dat</code>	Fully specified.
<code>http://myhost.mydomain.com/mywebpage/default.html</code>	Port is not specified; therefore, GridFTP uses protocol default (in this case, 80).
<code>file:///foo.dat</code>	Host is not specified; therefore, GridFTP uses your local host. Port is not specified; therefore, GridFTP uses protocol default (in this case, 80).
<code>file:/foo.dat</code>	This is also valid but is not recommended because, while many servers (including ours) accept this format, it is <i>not</i> RFC conformant and is not recommended.



## Important

For GridFTP (`gsiftp://`) and FTP (`ftp://`), it is legal to specify a user name and password in the the URL as follows:

```
gsiftp://myname:[mypassword]@myhost.mydomain.com/foo.dat
```

If you are using GSI security, then you may specify the username (but you may *not* include the `:` or the password) and the grid-mapfile will be searched to see if that is a valid account mapping for your

distinguished name (DN). If it is found, the *server* will setuid to that account. If not, it will fail. It will NOT fail back to your default account.

If you are using anonymous FTP, the username *must* be one of the usernames listed as a valid anonymous name and the password can be anything.

If you are using password authentication, you must specify both your username and password. **THIS IS HIGHLY DISCOURAGED, AS YOU ARE SENDING YOUR PASSWORD IN THE CLEAR ON THE NETWORK.** This is worse than no security; it is a false illusion of security.

## Command line options

### Informational Options

-help   -usage	Prints help.
-version	Prints the version of this program.
-versions	Prints the versions of all modules that this program uses.
-q   -quiet	Suppresses all output for successful operation.
-vb   -verbose	During the transfer, displays: <ul style="list-style-type: none"> <li>• number of bytes transferred,</li> <li>• performance since the last update (currently every 5 seconds), and</li> <li>• average performance for the whole transfer.</li> </ul>
-dbg   -debugftp	<p>Debugs FTP connections and prints the entire control channel protocol exchange to STDERR.</p> <p>Very useful for debugging. Please provide this any time you are requesting assistance with a globus-url-copy problem.</p>
-list <url>	This option will display a directory listing for the given url.
-nl-bottleneck   -nlb	This option uses NetLogger to estimate speeds of disk and network read/write system calls, and attempt to determine the bottleneck component.



### Note

In order to use this, the server must be configured to enable netlogger bottleneck detection<sup>2</sup>.

### Utility Ease of Use Options

-a   -ascii	Converts the file to/from ASCII format to/from local file format.
-b   -binary	Does not apply any conversion to the files. This option is turned on by default.
-cd   -create-dest	Create destination directories, if needed
-f <i>filename</i>	Reads a list of URL pairs from a filename.

Each line should contain:

*sourceURL destURL*

Enclose URLs with spaces in double quotes ("). Blank lines and lines beginning with the hash sign (#) will be ignored.

-r | -recurse

Copies files in subdirectories.

-rp | -relative-paths

The path portion of ftp urls will be interpreted as relative to the user's starting directory on the server. By default, all paths are root-relative. When this flag is set, the path portion of the ftp url must start with %2F if it designates a root-relative path.

-notpt | -no-third-party-transfers

Turns third-party transfers off (on by default).

Site firewall and/or software configuration may prevent a connection between the two servers (a *third party transfer*). If this is the case, globus-url-copy will "relay" the data. It will do a GET from the source and a PUT to the destination.

This obviously causes a performance penalty but will allow you to complete a transfer you otherwise could not do.

## Reliability Options

-rst | -restart

Restarts failed FTP operations.

-rst-retries <retries>

Specifies the maximum number of times to retry the operation before giving up on the transfer.

Use 0 for infinite.

The default value is 5.

-rst-interval <seconds>

Specifies the interval in seconds to wait after a failure before retrying the transfer.

Use 0 for an exponential backoff.

The default value is 0.

-rst-timeout <seconds>

Specifies the maximum time after a failure to keep retrying.

Use 0 for no timeout.

The default value is 0.

-df <filename> | -dumpfile  
<filename>

Specifies path to the file where untransferred urls will be saved for later restarting. The resulting file is the same format as the -f input file. If the file exists, it will be read and all other url input will be ignored.

-do <filename> | -dump-only  
<filename>

Perform no write operations on the destination. Instead, all files that would be transferred are enumerated and dumped to the specified file. Resulting file is the same format as the -f input file. Note: if you intend to use this file as input

for a future transfer, the `-create-dest` option will be required if any destination directories do not already exist.

`-stall-timeout` | `-st <seconds>`

Specifies how long before cancelling/restarting a transfer with no data movement. Set to 0 to disable. Default is 600 seconds.

## Performance Options

`-tcp-bs <size>` | `-tcp-buffer-size <size>`

Specifies the size (in bytes) of the TCP buffer to be used by the underlying ftp data channels.



### Important

This is critical to good performance over the WAN.

How do I pick a value?

`-p <parallelism>` | `-parallel <parallelism>`

Specifies the number of parallel data connections that should be used.



### Note

This is one of the most commonly used options.

How do I pick a value?

`-bs <block size>` | `-block-size <block size>`

Specifies the size (in bytes) of the buffer to be used by the underlying transfer methods.

`-pp`

Allows pipelining. GridFTP is a command response protocol. A client sends one command and then waits for a "Finished response" before sending another. Adding this overhead on a per-file basis for a large data set partitioned into many small files makes the performance suffer. Pipelining allows the client to have many outstanding, unacknowledged transfer commands at once. Instead of being forced to wait for the "Finished response" message, the client is free to send transfer commands at any time.

`-mc filename source_url`

Transfers a single file to many destinations. Filename is a line-separated list of destination urls. For more information on this option, click [here](#).

Multicasting must be [enabled for use](#) on the server side.



### Warning

This option is EXPERIMENTAL.

`-concurrency` | `-cc`

Specifies the number of concurrent FTP connections to use for multiple transfers.

`-udt`

Uses UDT, a reliable UDP-based transport protocol, for data transfers.



### Note

Note: In order to use this option, the server must be configured to use [UDT](#). For third party transfers, no change is required on the client side. For client-server transfers, you need to enable threading in the

client. To switch to threaded flavor, set the environment variable 'GLOBUS\_THREAD\_MODEL=pthread'.

-fast

Recommended when using GridFTP servers. Use MODE E for all data transfers, including reusing data channels between list and transfer operations.

## Security Related Options

-s <subject> | -subject <subject>

Specifies a subject to match with both the source and destination servers.



### Note

Used when the server does not have access to the host certificate (usually when you are running the server as a user). See [the section called “If you run a GridFTP server by hand...”](#).

-ss <subject> | -source-subject  
<subject>

Specifies a subject to match with the source server.



### Note

Used when the server does not have access to the host certificate (usually when you are running the server as a user). See [the section called “If you run a GridFTP server by hand...”](#).

-ds <subject> | -dest-subject  
<subject>

Specifies a subject to match with the destination server.



### Note

Used when the server does not have access to the host certificate (usually when you are running the server as a user). See [the section called “If you run a GridFTP server by hand...”](#).

-nodcau | -no-data-channel-  
authentication

Turns off data channel authentication for FTP transfers (the default is to authenticate the data channel).



### Warning

We do *not* recommend this option, as it is a security risk.

-dcsafe | -data-channel-safe

Sets data channel protection mode to SAFE.

Otherwise known as *integrity* or *checksumming*.

Guarantees that the data channel has not been altered, though a malicious party may have observed the data.



### Warning

Rarely used as there is a substantial performance penalty.

-dcpriv | -data-channel-private

Sets data channel protection mode to PRIVATE.

The data channel is encrypted and checksummed.

Guarantees that the data channel has not been altered and, if observed, it won't be understandable.

## Warning

VERY rarely used due to the VERY substantial performance penalty.



## Advanced Options

-stripe	Enables striped transfers on supported servers.
-striped-block-size   -sbs	Sets layout mode and blocksize for striped transfers.  If not set, the server defaults will be used.  If set to 0, partitioned mode will be used.  If set to >0, blocked mode will be used, with this setting used as the blocksize.
-t <transfer time in seconds>	Runs the transfer for the specified number of seconds and then ends. Useful for performance testing or forced restart loops.
-ipv6	Uses ipv6 when available.

## Warning

This option is EXPERIMENTAL. Use at your own risk.

-dp   -delayed-pasv	Enables delayed passive.
-g2   -gridftp2	Uses GridFTP v2 protocol enhancements when possible.
-mn   -module-name <gridftp storage module name>	Specifies the backend storage module to use for both the source and destination in a GridFTP transfer.
-mp   -module-parameters <gridftp storage module parameters>	Specifies the backend storage module arguments to use for both the source and destination in a GridFTP transfer.
-smn   -src-module-name <gridftp storage module name>	Specifies the backend storage module to use for the source file in a GridFTP transfer.
-smp   -src-module-parameters <gridftp storage module parameters>	Specifies the backend storage module arguments to use for the source file in a GridFTP transfer.
-dmn   -dst-module-name <gridftp storage module name>	Specifies the backend storage module to use for the destination file in a GridFTP transfer.
-dmp   -dst-module-parameters <gridftp storage module parameters>	Specifies the backend storage module arguments to use for the destination file in a GridFTP transfer.
-aa   -authz-assert <authorization assertion file>	Uses the assertions in the specified file to authorize access to both the source and destination servers.
-saa   -src-authz-assert <authorization assertion file>	Uses the assertions in the specified file to authorize access to the source server.
-daa   -dst-authz-assert <authorization assertion file>	Uses the assertions in the specified file to authorize access to the destination server.

-cache-aa   -cache-authz-assert	Caches the authorization assertion for subsequent transfers.
-cache-saa   -cache-src-authz-assert	Caches the source authorization assertion for subsequent transfers.
-cache-daa   -cache-dst-authz-assert	Caches the destination authorization assertion for subsequent transfers.
-nl-bottleneck   -nlb	Uses NetLogger to estimate speeds of disk and network read/write system calls, and attempt to determine the bottleneck component.  Note: In order to use this, the server must be configured to enable netlogger bottleneck detection.
-src-pipe   -SP <command line>	Sets the source end of a remote transfer to use piped-in input with the given command line.   <b>Warning</b>  Do not use with the <code>-fsstack</code> option.
-dst-pipe   -DP <command line>	Sets the destination end of a remote transfer to write data to then standard input of the program run via the given command line.   <b>Warning</b>  Do not use with the <code>-fsstack</code> option.
-pipe <command line>	Sets both <code>-src-pipe</code> and <code>-dst-pipe</code> to the same value.
-dcstack   -data-channel-stack	Specifies the XIO driver stack for the network on both the source and the destination. Both must be GridFTP servers.
-fsstack   -file-system-stack	Specifies the XIO driver stack for the disk on both the source and the destination. Both must be GridFTP servers.
-src-dcstack   -source-data-channel-stack	Specifies the XIO driver stack for the network on the source GridFTP server.
-src-fsstack   -source-file-system-stack	Specifies the XIO driver stack for the disk on the source GridFTP server.
-dst-dcstack   -dest-data-channel-stack	Specifies the XIO driver stack for the network on the destination GridFTP server.
-dst-fsstack   -dest-file-system-stack	Specifies the XIO driver stack for the disk on the destination GridFTP server.
-cred <path to credentials or proxy file>, -src-cred   -sc <path to credentials or proxy file>, -dst-cred   -dc <path to credentials or proxy file>	Specifies the credentials to use for source, destination, or both FTP connections.
-af <filename>   -alias-file <filename>	Specifies a file that maps logical host aliases to lists of physical hosts. When used with multiple concurrent connections, each connection uses the next host in the list. Each line should either be an alias (noted with the @ symbol), or a hostname[:port]. Currently, only the aliases @source and @destination are valid, and they are used for every source or destination url.



## Synchronization Options

<code>-sync</code>	Only transfer files where the destination does not exist or differs from the source. <code>-sync-level</code> controls how to determine if files differ.
<code>-sync-level &lt;number&gt;</code>	Choose criteria for determining if files differ when performing a sync transfer. Level 0 will only transfer if the destination does not exist. Level 1 will transfer if the size of the destination does not match the size of the source. Level 2 will transfer if the timestamp of the destination is older than the timestamp of the source. Level 3 will perform a checksum of the source and destination and transfer if the checksums do not match. The default sync level is 2.

## Default globus-url-copy usage

A **globus-url-copy** invocation using the **gsiftp** protocol with no options (i.e., using all the defaults) will perform a transfer with the following characteristics:

- binary
- stream mode (which implies no parallelism)
- host default TCP buffer size
- encrypted and checksummed control channel
- an authenticated data channel

## MODES in GridFTP

GridFTP (as well as normal FTP) defines multiple wire protocols, or MODES, for the data channel.

Most normal FTP servers only implement *stream mode* (MODE S), i.e. the bytes flow in order over a single TCP connection. GridFTP defaults to this mode so that it is compatible with normal FTP servers.

However, GridFTP has another MODE, called Extended Block Mode, or *MODE E*. This mode sends the data over the data channel in blocks. Each block consists of 8 bits of flags, a 64 bit integer indicating the offset from the start of the transfer, and a 64 bit integer indicating the length of the block in bytes, followed by a payload of length bytes. Because the offset and length are provided, out of order arrival is acceptable, i.e. the 10th block could arrive before the 9th because you know explicitly where it belongs. This allows us to use multiple TCP channels. If you use the `-p` | `-parallelism` option, **globus-url-copy** automatically puts the servers into MODE E.



### Note

Putting `-p 1` is not the same as no `-p` at all. Both will use a single stream, but the default will use stream mode and `-p 1` will use MODE E.

## If you run a GridFTP server by hand...

If you run a GridFTP server by hand, you will need to explicitly specify the subject name to expect. The `subject` option provides **globus-url-copy** with a way to validate the remote servers with which it is communicating. Not only must the server trust **globus-url-copy**, but **globus-url-copy** must trust that it is talking to the correct server. The validation is done by comparing host DNs or subjects.

If the GridFTP server in question is running under a host certificate then the client assumes a subject name based on the server's canonical DNS name. However, if it was started under a user certificate, as is the case when a server is

started by hand, then the expected subject name must be explicitly stated. This is done with the `-ss`, `-sd`, and `-s` options.

`-ss` Sets the `sourceURL` subject.

`-ds` Sets the `destURL` subject.

`-s` If you use this option alone, it will set both urls to be the same. You can see an example of this usage under the [Troubleshooting](#) section.



## Note

This is an *unusual* use of the client. Most times you need to specify both URLs.

## How do I choose a value?

### How do I choose a value for the TCP buffer size (`-tcp-bs`) option?

The value you should pick for the TCP buffer size (`-tcp-bs`) depends on how fast you want to go (your bandwidth) and how far you are moving the data (as measured by the Round Trip Time (RTT) or the time it takes a packet to get to the destination and back).

To calculate the value for `-tcp-bs`, use the following formula (this assumes that Mega means  $1000^2$  rather than  $1024^2$ , which is typical for bandwidth):

$$-tcp-bs = \text{bandwidth in Megabits per second (Mbs)} * \text{RTT in milliseconds (ms)} * 1000 / 8$$

As an example, if you are using fast ethernet (100 Mbs) and the RTT was 50 ms it would be:

$$-tcp-bs = 100 * 50 * 1000 / 8 = 625,000 \text{ bytes.}$$

So, how do you come up with values for bandwidth and RTT? To determine RTT, use either ping or traceroute. They both list RTT values.



## Note

You must be on one end of the transfer and ping the other end. This means that if you are doing a third party transfer you have to run the ping or traceroute between the two server hosts, not from your client.

The bandwidth is a little trickier. Any point in the network can be the bottleneck, so you either need to talk with your network engineers to find out what the bottleneck link is or just assume that your host is the bottleneck and use the speed of your network interface card (NIC).



## Note

The value you pick for `-tcp-bs` limits the top speed you can achieve. You will NOT get bandwidth any higher than what you used in the calculation (assuming the RTT is actually what you specified; it varies a little with network conditions). So, if for some reason you want to limit the bandwidth you get, you can do that by judicious choice of `-tcp-bs` values.

So where does this formula come from? Because it uses the bandwidth and the RTT (also known as the latency or delay) it is called the *bandwidth delay product*. The very simple explanation is this: TCP is a reliable protocol. It must save a copy of everything it sends out over the network until the other end acknowledges that it has been received.

As a simple example, if I can put one byte per second onto the network, and it takes 10 seconds for that byte to get there, and 10 seconds for the acknowledgment to get back (RTT = 20 seconds), then I would need at least 20 bytes

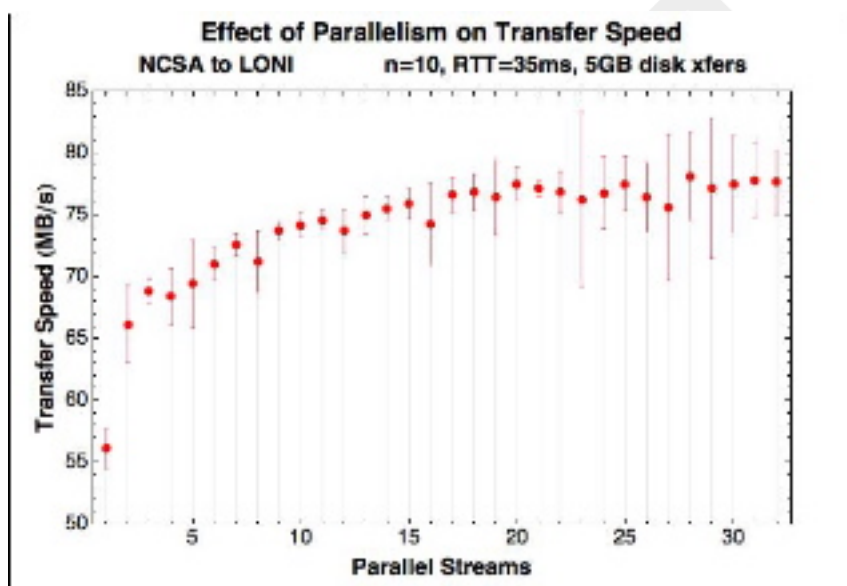
of storage. Then, hopefully, by the time I am ready to send byte 21, I have received an acknowledgement for byte 1 and I can free that space in my buffer. If you want a more detailed explanation, try the following links on TCP tuning:

- [http://www.psc.edu/networking/perf\\_tune.html](http://www.psc.edu/networking/perf_tune.html)
- <http://www.didc.lbl.gov/TCP-tuning/>
- <http://www.ncne.nlanr.net/research/tcp/>

## How do I choose a value for the parallelism (-p) option?

For most instances, using 4 streams is a very good rule of thumb. Unfortunately, there is not a good formula for picking an exact answer. The shape of the graph shown here is very characteristic.

**Figure 1. Effect of Parallel Streams in GridFTP**



You get a strong increase in bandwidth, then a sharp knee, after which additional streams have very little impact. Where this knee is depends on many things, but it is generally between 2 and 10 streams. Higher bandwidth, longer round trip times, and more congestion in the network (which you usually can only guess at based on how applications are behaving) will move the knee higher (more streams needed).

In practice, between 4 and 8 streams are usually sufficient. If things look really bad, try 16 and see how much difference that makes over 8. However, anything above 16, other than for academic interest, is basically wasting resources.

## Limitations

There are no limitations for **globus-url-copy** in GT 6.0.

## Interactive clients for GridFTP

The Globus Project does *not* provide an interactive client for GridFTP. Any normal FTP client will work with a GridFTP server, but it cannot take advantage of the advanced features of GridFTP. The interactive clients listed below take advantage of the advanced features of GridFTP.

There is no endorsement implied by their presence here. We make no assertion as to the quality or appropriateness of these tools, we simply provide this for your convenience. We will *not* answer questions, accept bugs, or in any way shape or form be responsible for these tools, although they should have mechanisms of their own for such things.

UberFTP was developed at the NCSA under the auspices of NMI and TeraGrid:

- NCSA Uberftp only download: <http://dims.ncsa.uiuc.edu/set/uberftp/download.html>
- UberFTP User's Guide: <http://dims.ncsa.uiuc.edu/set/uberftp/userdoc.html>

DRAFT

## Name

globus-gridftp-server — Configures the GridFTP Server

## Synopsis

globus-gridftp-server

## Tool description

**globus-gridftp-server** configures the GridFTP server using a config file and/or commandline options.



### Note

Command line options and configuration file options may both be used, but the command line *overrides* the config file.

The configuration file for the GridFTP *server* is read from the following locations, in the given order. Only the first file found will be loaded:

- Path specified with the `-c <configfile>` command line option.
- `$GLOBUS_LOCATION/etc/gridftp.conf`
- `/etc/grid-security/gridftp.conf`

Options are one per line, with the format:

`<option> <value>`

If the value contains spaces, they should be enclosed in double-quotes ("). Flags or boolean options should only have a value of 0 or 1. Blank lines and lines beginning with `#` are ignored.

For example:

```
port 5000
allow_anonymous 1
anonymous_user bob
banner "Welcome!"
```

## Developer notes

The Globus implementation of the GridFTP *server* draws on:

- three IETF RFCs:
  - RFC 959
  - RFC 2228
  - RFC 2389
- an IETF Draft: MLST-16
- the GridFTP protocol specification, which is Global Grid Forum (GGF) Standard GFD.020.

The command line tools and the *client* library completely hide the details of the protocol from the user and the developer. Unless you choose to use the control library, it is not necessary to have a detailed knowledge of the protocol.

## Command syntax

The basic syntax for **globus-gridftp-server** is:

```
globus-gridftp-server [optional command line switches]
```

To use **globus-gridftp-server** with a config file, make sure to use the `-c <configfile>` option.

## Command line options

The table below lists config file options, associated command line options (if available) and descriptions.



### Note

Any boolean option can be negated on the command line by preceding the specified option with `'-no-'` or `'-n'`.  
example: `-no-cas` or `-nf`.

## Informational Options

<code>help &lt;0 1&gt;, -h, -help</code>	Show usage information and exit. Default value: FALSE
<code>version &lt;0 1&gt;, -v, -version</code>	Show version information for the server and exit. Default value: FALSE
<code>versions &lt;0 1&gt;, -V, -versions</code>	Show version information for <b>all</b> loaded globus libraries and exit. Default value: FALSE

## Modes of Operation

<code>inetd &lt;0 1&gt;, -i, -inetd</code>	Run under an inetd service. Default value: FALSE
<code>daemon &lt;0 1&gt;, -s, -daemon</code>	Run as a daemon. All connections will fork off a new process and setuid if allowed. See <a href="#">Section 4.4.1, “Running in daemon mode”</a> for more information. Default value: TRUE
<code>detach &lt;0 1&gt;, -S, -detach</code>	Run as a background daemon detached from any controlling terminals. See <a href="#">Section 4.4.1, “Running in daemon mode”</a> for more information. Default value: FALSE
<code>ssh, -ssh</code>	Run over a connected ssh session. Default value: not set
<code>exec &lt;string&gt;, -exec &lt;string&gt;</code>	For statically compiled or non-GLOBUS_LOCATION standard binary locations, specify the full path of the server binary here. Only needed when run in <a href="#">daemon mode</a> .

	Default value: not set
<code>chdir &lt;0 1&gt;, -chdir</code>	Change directory when the server starts. This will change directory to the dir specified by the <code>chdir_to</code> option.
	Default value: TRUE
<code>chdir_to &lt;string&gt;, -chdir-to &lt;string&gt;</code>	Directory to <code>chdir</code> to after starting. Will use <code>/</code> if not set.
	Default value: not set
<code>fork &lt;0 1&gt;, -f, -fork</code>	Server will fork for each new connection. Disabling this option is only recommended when debugging. Note that non-forked servers running as 'root' will only accept a single connection and then exit.
	Default value: TRUE
<code>single &lt;0 1&gt;, -1, -single</code>	Exit after a single connection.
	Default value: FALSE
<code>chroot_path &lt;string&gt;, -chroot-path &lt;string&gt;</code>	Path to become the new root after authentication. This path must contain a valid certificate structure, <code>/etc/passwd</code> , and <code>/etc/groups</code> . The command <code>globus-gridftp-server-setup-chroot</code> can help create a suitable directory structure.
	Default value: not set

## Authentication, Authorization, and Security Options

<code>auth_level &lt;number&gt;, -auth-level &lt;number&gt;</code>	<ul style="list-style-type: none"> <li>• 0 = Disables all authorization checks.</li> <li>• 1 = Authorize identity only.</li> <li>• 2 = Authorize all file/resource accesses.</li> </ul> <p>If not set, the GridFTP Server uses level 2 for front ends and level 1 for data nodes.</p> <p>Default value: not set</p>
<code>ipc_allow_from &lt;string&gt;, -ipc-allow-from &lt;string&gt;</code>	<p>Only allow IPC connections (applicable for backend servers in a striped configuration) from these source IP addresses. Specify a comma-separated list of IP address fragments. A match is any IP address that starts with the specified fragment. Example: '192.168.1.' will match and allow a connection from 192.168.1.45. Note that if this option is used, any address not specifically allowed will be denied.</p> <p>Default value: not set</p>
<code>ipc_deny_from &lt;string&gt;, -ipc-deny-from &lt;string&gt;</code>	<p>Deny IPC connections (applicable for backend servers in a striped configuration) from these source IP addresses. Specify a comma-separated list of IP address fragments. A match is any IP address that starts with the specified fragment. Example: '192.168.2.' will match and deny a connection from 192.168.2.45.</p>

	Default value: not set
<code>allow_from &lt;string&gt;, -allow-from &lt;string&gt;</code>	Only allow connections from these source IP addresses. Specify a comma-separated list of IP address fragments. A match is any IP address that starts with the specified fragment. Example: '192.168.1.' will match and allow a connection from 192.168.1.45. Note that if this option is used, any address not specifically allowed will be denied.
	Default value: not set
<code>deny_from &lt;string&gt;, -deny-from &lt;string&gt;</code>	Deny connections from these source IP addresses. Specify a comma-separated list of IP address fragments. A match is any IP address that starts with the specified fragment. Example: '192.168.2.' will match and deny a connection from 192.168.2.45.
	Default value: not set
<code>secure_ipc &lt;0 1&gt;, -si, -secure-ipc</code>	Use GSI security on the IPC channel.
	Default value: TRUE
<code>ipc_auth_mode &lt;string&gt;, -ia &lt;string&gt;, -ipc-auth-mode &lt;string&gt;</code>	Set GSI authorization mode for the IPC connection. Options are one of the following: <ul style="list-style-type: none"> <li>• none</li> <li>• host</li> <li>• self</li> <li>• subject:[subject]</li> </ul>
	Default value: host
<code>allow_anonymous &lt;0 1&gt;, -aa, -allow-anonymous</code>	Allow cleartext anonymous access. If server is running as root, <code>anonymous_user</code> must also be set. Disables IPC security.
	Default value: FALSE
<code>anonymous_names_allowed &lt;string&gt;, -anonymous-names-allowed &lt;string&gt;</code>	Comma-separated list of names to treat as anonymous users when allowing anonymous access. If not set, the default names of 'anonymous' and 'ftp' will be allowed. Use '*' to allow any username.
	Default value: not set
<code>anonymous_user &lt;string&gt;, -anonymous-user &lt;string&gt;</code>	User to setuid to for an anonymous connection. Only applies when running as root.
	Default value: not set
<code>anonymous_group &lt;string&gt;, -anonymous-group &lt;string&gt;</code>	Group to setgid to for an anonymous connection. If not set, the default group of <code>anonymous_user</code> will be used.
	Default value: not set
<code>allow_root, -allow-root</code>	Allow clients to be mapped to the root account.
	Default value: FALSE



<code>pw_file &lt;string&gt;, -password-file &lt;string&gt;</code>	Enable cleartext access and authenticate users against this <code>/etc/passwd</code> formatted file.  Default value: not set
<code>connections_max &lt;number&gt;, -connections-max &lt;number&gt;</code>	Maximum concurrent connections allowed. Only applies when running in <u>daemon mode</u> . Unlimited if not set.  Default value: not set
<code>connections_disabled &lt;0 1&gt;, -connections-disabled</code>	Disable all new connections. Does not affect ongoing connections. This must be set in the configuration file and then a SIGHUP issued to the server in order to reload the configuration.  Default value: FALSE
<code>offline_msg &lt;string&gt;, -offline-msg &lt;string&gt;</code>	Custom message to be displayed to clients when the server is offline via the <code>connections_disabled</code> or <code>connections_max = 0</code> options.  Default value: not set
<code>disable_command_list &lt;string&gt;, -disable-command-list &lt;string&gt;</code>	A comma separated list of client commands that will be disabled.  Default value: not set
<code>authz_callouts, -authz-callouts</code>	Enable the GSI authorization callout framework.  Default value: TRUE
<code>restrict_paths, -rp, -restrict-paths</code>	A comma separated list of full paths that clients may access. Each path may be prefixed by R and/or W, denoting read or write access, otherwise full access is granted. If a given path is a directory, all contents and subdirectories will be given the same access. Order of paths does not matter -- the permissions on the longest matching path will apply. The special character '~' will be replaced by the authenticated user's home directory. Note that if the authenticated user's home directory is not accessible, the home directory and starting path will be set to '/'. By default all paths are allowed, and access control is handled by the OS.  Default value: not set
<code>rp_follow_symlinks, -rp-follow-symlinks</code>	Allow following symlinks that lead to restricted paths.  Default value: FALSE
<code>acl, -em, -acl</code>	A comma separated list of ACL or event modules to load.  Default value: not set

## Logging Options

<code>log_level &lt;string&gt;, -d &lt;string&gt;, -log-level &lt;string&gt;</code>	Log level. A comma-separated list of levels from the following: <ul style="list-style-type: none"> <li>• ERROR</li> <li>• WARN</li> <li>• INFO</li> </ul>
---	---

- DUMP

- ALL

For example:

```
globus-gridftp-server -d error,warn,info
```

You may also specify a numeric level of 1-255.

Default value: ERROR

```
log_module <string>, -
log-module <string>
```

Indicates the `globus_logging` module that will be loaded. If not set, the default `stdio` module will be used and the logfile options (see next option) will apply.

Built-in modules are `stdio` and `syslog`. Log module options may be set by specifying `module:opt1=val1:opt2=val2`. Available options for the built-in modules are:

- `interval` - Indicates buffer flush interval. Default is 5 seconds. A 0 second flush interval will disable periodic flushing, and the buffer will only flush when it is full.
- `buffer` - Indicates buffer size. Default is 64k. A value of 0k will disable buffering and all messages will be written immediately.

Example:

```
-log-module stdio:buffer=4096:interval=10
```

Default value: not set

```
log_single <string>,
-l <string>, -logfile
<string>
```

Indicates the path of a single file to which you want to log all activity. If neither this option nor `log_unique` is set, logs will be written to `stderr`, unless the execution mode is detached, or `inetd`, in which case logging will be disabled.



## Note

You have to provide full path

Default value: not set

```
log_unique <string>,
-L <string>, -logdir
<string>
```

Partial path to which `gridftp.(pid).log` will be appended to construct the log filename. Example:

```
-L /var/log/gridftp/
```

will create a separate log (`/var/log/gridftp/gridftp.xxxx.log`) for each process (which is normally each new *client* session). If neither this option nor `log_single` is set, logs will be written to `stderr`, unless the execution mode is detached, or `inetd`, in which case logging will be disabled.



## Note

You have to provide full path

`log_transfer <string>`  
`, -Z <string>, -log-`  
`transfer <string>`

Default value: not set

Log NetLogger-style info for each transfer into this file.



## Note

You have to provide full path

Default value: not set

Example: DATE=20050520163008.306532 HOST=localhost PROG=globus-gridftp-server NL.EVNT=FTP\_INFO START=20050520163008.305913 USER=ftp FILE=/etc/group BUFFER=0 BLOCK=262144 NBYTES=542 VOLUME=/ STREAMS=1 STRIPES=1 DEST=[127.0.0.1] TYPE=RETR CODE=226

Time format is YYYYMMDDHHMMSS.UUUUUU (microsecs).

- DATE: time the transfer completed.
- START: time the transfer started.
- HOST: hostname of the server.
- USER: username on the host that transferred the file.
- BUFFER: tcp buffer size (if 0 system defaults were used).
- BLOCK: the size of the data block read from the disk and posted to the network.
- NBYTES: the total number of bytes transferred.
- VOLUME: the disk partition where the transfer file is stored.
- STREAMS: the number of parallel TCP streams used in the transfer.
- STRIPES: the number of stripes used on this end of the transfer.
- DEST: the destination host.
- TYPE: the transfer type, RETR is a send and STOR is a receive (ftp 959 commands).
- CODE: the FTP rfc959 completion code of the transfer. 226 indicates success, 5xx or 4xx are failure codes.

`log_filemode <string>`,  
`-log-filemode <string>`

File access permissions of log files. Should be an octal number such as 0644 (the leading 0 is required).

Default value: not set

`disable_usage_stats`  
`<0|1>, -disable-usage-`  
`stats`

Disable transmission of per-transfer usage statistics. See the [Usage Statistics](#)<sup>1</sup> section in the online documentation for more information.

Default value: FALSE

usage\_stats\_target  
 <string>, -usage-stats-  
 target <string>

Comma-separated list of contact strings for usage statistics listeners. The format of <string> is host:port.

Default value: usage-stats.globus.org:4810

**Example:**

-usage-stats-target usage-stats.globus.org:4810,usage-stats.uc.t

In this example, the usage statistics will be transmitted to the default Globus target (usage-stats.globus.org:4810) and another target (usage-stats.uc.teragrid.org:5920).

The usage stats sent to a particular receiver may be customized by configuring it with a taglist (host:port!taglist) The taglist is a list of characters that each correspond to a usage stats tag. When this option is unset, stats are reported to usage-stats.globus.org:4810. If you set your own receiver, and wish to continue reporting to the Globus receiver, you will need to add it manually. The list of available tags follow. Tags marked \* are reported by default.

- \*(e) START - start time of transfer
- \*(E) END - end time of transfer
- \*(v) VER - version string of gridftp server
- \*(b) BUFFER - tcp buffer size used for transfer
- \*(B) BLOCK - disk blocksize used for transfer
- \*(N) NBYTES - number of bytes transferred
- \*(s) STREAMS - number of parallel streams used
- \*(S) STRIPES - number of stripes used
- \*(t) TYPE - transfer command: RETR, STOR, LIST, etc
- \*(c) CODE - ftp result code (226 = success, 5xx = fail)
- \*(D) DSI - DSI module in use
- \*(A) EM - event modules in use
- \*(T) SCHEME - ftp, gsiftp, sshftp, etc. (client supplied)
- \*(a) APP - guc, rft, generic library app, etc. (client supplied)
- \*(V) APPVER - version string of above. (client supplied)
- (f) FILE - name of file/data transferred
- (i) CLIENTIP - ip address of host running client (control channel)
- (I) DATAIP - ip address of source/dest host of data (data channel)
- (u) USER - local user name the transfer was performed as

- (d) USERDN - DN that was mapped to user id
- (C) CONFID - ID defined by -usage-stats-id config option
- (U) SESSID - unique id that can be used to match transfers in a session and transfers across source/dest of a third party transfer. (client supplied)

usage\_stats\_id <string> Identifying tag to include in usage statistics data.  
 , -usage-stats-id  
 <string> Default value: not set

## Single and Striped Remote Data Node Options

remote\_nodes <string> Comma-separated list of remote node contact strings. See [Remote data-nodes and striped operations](#) and [Separation of processes for higher security](#) for examples of using this option.

Default value: not set

data\_node <0|1>, -dn, -data-node This server is a back end data node. See [Separation of processes for higher security](#) for an example of using this option.

Default value: FALSE

stripe\_blocksize <number>, -sbs <number> Size in bytes of sequential data that each stripe will transfer.  
 , -stripe-blocksize  
 <number> Default value: 1048576

stripe\_count <number>, Number of stripes to use per transfer when this server controls that number.  
 -stripe-count <number> If remote nodes are statically configured (via -r or remote\_nodes), this will be set to that number of nodes, otherwise the default is 1.

Default value: not set

stripe\_layout <number> Stripe layout. 1 = Partitioned, 2 = Blocked.  
 , -sl <number>, -stripe-  
 layout <number> Default value: 2

stripe\_blocksize\_locked <0|1>, -stripe- Do not allow client to override stripe blocksize with the **OPTS RETR**  
 blocksize-locked; command.

Default value: FALSE

stripe\_layout\_locked <0|1>, -stripe-layout- Do not allow client to override stripe layout with the **OPTS RETR** command.  
 locked Default value: FALSE

## Disk Options

blocksize <number>, - Size in bytes of data blocks to read from disk before posting to the network.  
 bs <number>, -blocksize  
 <number> Default value: 262144

sync\_writes <0|1>, - Flush disk writes before sending a restart marker. This attempts to ensure that  
 sync-writes the range specified in the restart marker has actually been committed to disk.

This option will probably impact performance and may result in different behavior on different storage systems. See the man page for **sync()** for more information.

Default value: FALSE

`use_home_dirs` , `-use-home-dirs`

Set the startup directory to the authenticated users home dir.

Default value: TRUE

`perms <string>` , `-perms <string>`

Set the default permissions for created files. Should be an octal number such as 0644. The default is 0644. Note: If umask is set it will affect this setting -- i.e. if the umask is 0002 and this setting is 0666, the resulting files will be created with permissions of 0664.

Default value: not set

`file_timeout <number>` , `-file-timeout <number>`

Timeout in seconds for all disk accesses. A value of 0 disables the timeout.

Default value: not set

## Network Options

`port <number>` , `-p <number>` , `-port <number>`

Port on which a front end will listen for client control channel connections or on which a data node will listen for connections from a front end. If not set, a random port will be chosen and printed via the logging mechanism. See [Remote data-nodes and striped operations](#) and [Separation of processes for higher security](#) for examples of using this option.

Default value: not set

`control_interface <string>` , `-control-interface <string>`

Hostname or IP address of the interface to listen for control connections on. If not set, will listen on all interfaces.

Default value: not set

`data_interface <string>` , `-data-interface <string>`

Hostname or IP address of the interface to use for data connections. If not set will use the current control interface.

Default value: not set

`ipc_interface <string>` , `-ipc-interface <string>`

Hostname or IP address of the interface to use for IPC connections. If not set, will listen on all interfaces.

Default value: not set

`hostname <string>` , `-hostname <string>`

Effectively sets the above `control_interface`, `data_interface` and `ipc_interface` options.

Default value: not set

`ipc_port <number>` , `-ipc-port <number>`

Port on which the front end will listen for data node connections.

Default value: not set

`control_preauth_timeout <number>` , `-control-`

Time in seconds to allow a client to remain connected to the control channel without activity before authenticating.

preauth-timeout <number>	Default value: 120
control_idle_timeout <number>; -control-idle-timeout <number>	Time in seconds to allow a client to remain connected to the control channel without activity.  Default value: 600
ipc_idle_timeout <number>, -ipc-idle-timeout <number>	Idle time in seconds before an unused IPC connection will close.  Default value: 900
ipc_connect_timeout <number>, -ipc-connect-timeout <number>	Time in seconds before cancelling an attempted IPC connection.  Default value: 60
port_range <string>, -port-range <string>	Port range to use for incoming connections. The format is "startport,endport". This, along with -data-interface, can be used to enable operation behind a firewall and/or when NAT is involved. This is the same as setting the environment variable GLOBUS_TCP_PORT_RANGE.  Default value: not set

## User Messages

banner <string>, - banner <string>	Message that is displayed to the client before authentication.  Default value: not set
banner_file <string>, - banner-file <string>	Read banner message from this file.  Default value: not set
banner_terse <0 1>, - banner-terse	When this is set, the minimum allowed banner message will be displayed to unauthenticated clients.  Default value: FALSE
banner_append <0 1>, - banner-append	When this is set, the message set in the 'banner' or 'banner_file' option will be appended to the default banner message rather than replacing it.  Default value: FALSE
login_msg <string>, - login-msg <string>	Message that is displayed to the client after authentication.  Default value: not set
login_msg_file <string> , -login-msg-file <string>	Read login message from this file.  Default value: not set

## Module Options

load_dsi_module <string>, -dsi <string>	Load this Data Storage Interface module. File and remote modules are defined by the server. If not set, the file module is loaded, unless the remote option is specified, in which case the remote module is loaded. An additional
--	--

	configuration string can be passed to the DSI using the format [module name]:[configuration string]. The format of the configuration string is defined by the DSI being loaded.
	Default value: not set
allowed_modules <string>, -allowed-modules <string>	Comma-separated list of ERET/ESTO modules to allow and, optionally, specify an alias for. Example:  -allowed-modules module1,alias2:module2,module3  (module2 will be loaded when a client asks for alias2).
	Default value: not set
dc_whitelist <string>, -dc-whitelist <string>	A comma separated list of drivers allowed on the network stack.
	Default value: not set
fs_whitelist <string>, -fs-whitelist <string>	A comma separated list of drivers allowed on the disk stack.
	Default value: not set
popen_whitelist <string>, -popen-whitelist <string>	A comma separated list of programs that the popen driver is allowed to execute, when used on the network or disk stack. An alias may also be specified, so that a client does not need to specify the full path. Format is [alias:]prog,[alias:]prog. example: /bin/gzip,tar:/bin/tar
	Default value: not set
dc_default <string>, - dc-default <string>	A comma separated list of XIO drivers and options representing the default network stack. Format is of each driver entry is driver1[:opt1=val1;opt2=val2;...]. The bottom of the stack, the transport driver, is always first.
	Default value: not set
fs_default <string>, - fs-default <string>	A comma separated list of XIO drivers and options representing the default disk stack. Format is of each driver entry is driver1[:opt1=val1;opt2=val2;...]. The bottom of the stack, the transport driver, is always first.
	Default value: not set

## Other Options

configfile <string>, -c <string>	Path to configuration file that should be loaded. Otherwise will attempt to load \$GLOBUS_LOCATION/etc/gridftp.conf and /etc/grid-security/gridftp.conf.
-------------------------------------	--



### Note

You have to provide full path

	Default value: not set
config_dir <string>, -C <string>	Path to directory holding configuration files that should be loaded. Files will be loaded in alphabetical order, and in the event of duplicate parameters the



	last loaded file will take precedence. Note that the main configuration file, if one exists, will always be loaded last.
	Default value: not set
<code>config_base_path</code> <code>&lt;string&gt;, -config-base-path &lt;string&gt;</code>	Base path to use when config and log path options are not full paths. By default this is the current directory when the process is started.
	Default value: not set
<code>debug &lt;0 1&gt;, -debug</code>	Set options that make the server easier to debug. Forces no-fork, no-chdir, and allows core dumps on bad signals instead of exiting cleanly. Not recommended for production servers. Note that non-forked servers running as root will only accept a single connection and then exit.
	Default value: FALSE
<code>pidfile &lt;string&gt;, -pidfile &lt;string&gt;</code>	Write PID of the GridFTP server to this path. May contain variable references to <code>\${localstatedir}</code>
	Default value: not set



## Warning

Any FLAG can be negated by prepending `-no` or `-n` to the command line option.

## Limitations

For transfers using parallel data transport streams and for transfers using multiple computers at each end, the direction of the connection on the data channels must go from the sending to the receiving side. For more information about this limitations see <http://www.ogf.org/documents/GFD.20.pdf>.

Globus GridFTP server does not run on windows

# GRAM5 Commands

## Table of Contents

globus-fork-starter .....	54
globus-gatekeeper-admin .....	56
globus-gatekeeper .....	57
globus-gram-audit .....	60
globus-job-cancel .....	61
globus-job-clean .....	62
globus-job-get-output .....	63
globus-job-manager .....	65
globus-job-run .....	70
globus-job-status .....	73
globus-job-submit .....	75
globus-personal-gatekeeper .....	78
globus-rvf-check .....	80
globus-rvf-edit .....	81
globus-scheduler-event-generator-admin .....	82
globus-scheduler-event-generator .....	83
globusrun .....	84

## Name

globus-fork-starter — Start and monitor a fork job

## Synopsis

globus-fork-starter

## Description

The **globus-fork-starter** program is executes jobs specified on its standard input stream, recording the job state changes to a file defined in the `$GLOBUS_LOCATION/etc/globus-fork.conf` configuration file. It runs until its standard input stream is closed and all jobs it is managing have terminated. The log generated by this program can be used by the SEG to provide job state changes and exit codes to the GRAM service. The **globus-fork-starter** program is typically started by the fork GRAM module.

The **globus-fork-starter** program expects its input to be a series of task definitions, separated by the newline character, each representing a separate job. Each task definition contains a number of fields, separated by the colon character. The first field is always the literal string `100` indicating the message format, the second field is a unique job tag that will be distinguish the reply from this program when multiple jobs are submitted. The rest of fields contain attribute bindings. The supported attributes are:

<code>directory</code>	Working directory of the job
<code>environment</code>	Comma-separated list of strings defining environment variables. The form of these strings is <code>var=value</code>
<code>count</code>	Number of processes to start
<code>executable</code>	Full path to the executable to run
<code>arguments</code>	Comma-separated list of command-line arguments for the job
<code>stdin</code>	Full path to a file containing the input of the job
<code>stdout</code>	Full path to a file to write the output of the job to
<code>stderr</code>	Full path to a file to write the error stream of the job

Within each field, the following characters may be escaped by preceding them with the backslash character:

- backslash (\)
- semicolon (;)
- comma (,)
- equal (=)

Additionally, newline can be represented within a field by using the escape sequence `\n`.

For each job the **globus-fork-starter** processes, it replies by writing a single line to standard output. The replies again consist of a number of fields separated by the semicolon character.

For a successful job start, the first field of the reply is the literal `101`, the second field is the tag from the input, and the third field is a comma-separated list of SEG job identifiers which consist the concatenation of a UUID and a process id. The **globus-fork-starter** program will write state changes to the SEG log using these job identifiers.

For a failure, the first field of the reply is the literal 102, the second field is the tag from the input, the third field is the integer representation of a GRAM error code, and the fourth field is a string explaining the error.

## ENVIRONMENT

If the following variables affect the execution of **globus-fork-starter**

**GLOBUS\_LOCATION** Path to Globus Toolkit installation. This is used to locate the `globus-fork.conf` configuration file.

## Files

`$GLOBUS_LOCATION/etc/  
globus-fork.conf` Path to fork SEG configuration file.

DRAFT

## Name

globus-gatekeeper-admin — Manage globus-gatekeeper services

## Synopsis

```
globus-gatekeeper-admin [-h]
```

```
globus-gatekeeper-admin [-l] [-n NAME]
```

```
globus-gatekeeper-admin [-e SERVICE] [-n NAME]
```

```
globus-gatekeeper-admin [-E]
```

```
globus-gatekeeper-admin [-d SERVICE]
```

## Description

The **globus-gatekeeper-admin** program manages service entries which are used by the **globus-gatekeeper** to execute services. Service entries are located in the `/etc/grid-services` directory. The **globus-gatekeeper-admin** can list, enable, or disable specific services, or set a service as the default. The `-h` command-line option shows a brief usage message.

## Listing services

The `-l` command-line option to **globus-gatekeeper-admin** will cause it to list all of the services which are available to be run by the **globus-gatekeeper**. In the output, the service name will be followed by its status in brackets. Possible status strings are `ENABLED`, `DISABLED`, and `ALIAS to NAME`, where *NAME* is another service name.

If the `-n NAME` is used, then only information about the service named *NAME* is printed.

## Enabling services

The `-e SERVICE` command-line option to **globus-gatekeeper-admin** will cause it to enable a service so that it may be run by the **globus-gatekeeper**.

If the `-n NAME` option is used as well, then the service will be enabled with the alias *NAME*.

## Enabling a default service

The `-E` command-line option to **globus-gatekeeper-admin** will cause it to enable a service alias with the name `jobmanager`. The **globus-gatekeeper-admin** program will choose the first service it finds as the default. To enable a particular service as the default, use the `-e` parameter described above with the `-n` parameter.

## Disabling services

The `-d SERVICE` command-line option to **globus-gatekeeper-admin** will cause it to disable a service so that it may not be run by the **globus-gatekeeper**. All aliases to a disabled service are also disabled.

## Files

`/etc/grid-services`

Default location of enabled gatekeeper service descriptions.

## Name

globus-gatekeeper — Authorize and execute a grid service on behalf of a user

## Synopsis

```
globus-gatekeeper [-help]
[-conf PARAMETER_FILE]
[-test] [ -d | -debug ]
{ -inetd | -f }
[ -p PORT | -port PORT ]
[-home PATH] [ -l LOGFILE | -logfile LOGFILE ] [-lf LOG_FACILITY]
[-acctfile ACCTFILE]
[-e LIBEXECDIR]
[-launch_method { fork_and_exit | fork_and_wait | dont_fork } ]
[-grid_services SERVICEDIR]
[-globusid GLOBUSID]
[-gridmap GRIDMAP]
[-x509_cert_dir TRUSTED_CERT_DIR]
[-x509_cert_file TRUSTED_CERT_FILE]
[-x509_user_cert CERT_PATH]
[-x509_user_key KEY_PATH]
[-x509_user_proxy PROXY_PATH]
[-k]
[-globusmap KMAP]
[-pidfile PIDFILE]
```

## Description

The **globus-gatekeeper** program is a meta-server similar to **inetd** or **xinetd** that starts other services after authenticating a TCP connection using GSSAPI and mapping the client's credential to a local account.

The most common use for the **globus-gatekeeper** program is to start instances of the globus-job-manager(8) service. A single **globus-gatekeeper** deployment can handle multiple different service configurations by having entries in the `/etc/grid-services` directory.

Typically, users interact with the **globus-gatekeeper** program via client applications such as globusrun(1), **globus-job-submit**, or tools such as CoG jglobus or Condor-G.

The full set of command-line options to **globus-gatekeeper** consists of:

-help	Display a help message to standard error and exit
-conf <i>PARAMETER_FILE</i>	Load configuration parameters from <i>PARAMETER_FILE</i> . The parameters in that file are treated as additional command-line options.
-test	Parse the configuration file and print out the POSIX user id of the <b>globus-gatekeeper</b> process, service home directory, service execution directory, and X.509 subject name and then exits.
-d, -debug	Run the <b>globus-gatekeeper</b> process in the foreground.
-inetd	Flag to indicate that the <b>globus-gatekeeper</b> process was started via <b>inetd</b> or a similar super-server. If this flag is set and the <b>globus-gatekeeper</b> was not started via <b>inetd</b> , a warning will be printed in the gatekeeper log.

-f	Flag to indicate that the <b>globus-gatekeeper</b> process should run in the foreground. This flag has no effect when the <b>globus-gatekeeper</b> is started via inetd.
-p <i>PORT</i> , -port <i>PORT</i>	Listen for connections on the TCP/IP port <i>PORT</i> . This option has no effect if the <b>globus-gatekeeper</b> is started via inetd or a similar service. If not specified and the gatekeeper is running as root, the default of 2119 is used. Otherwise, the gatekeeper defaults to an ephemeral port.
-home <i>PATH</i>	Sets the gatekeeper deployment directory to <i>PATH</i> . This is used to interpret relative paths for accounting files, libexecdir, certificate paths, and also to set the GLOBUS_LOCATION environment variable in the service environment. If not specified, the gatekeeper looks for service executables in /usr/sbin, configuration in /etc, and writes logs and accounting files to /var/log.
-l <i>LOGFILE</i> , -logfile <i>LOGFILE</i>	Write log entries to <i>LOGFILE</i> . If <i>LOGFILE</i> is equal to logoff or LOGOFF, then logging will be disabled, both to file and to syslog.
-lf <i>LOG_FACILITY</i>	Open syslog using the <i>LOG_FACILITY</i> . If not specified, LOG_DAEMON will be used as the default when using syslog.
-acctfile <i>ACCTFILE</i>	Set the path to write accounting records to <i>ACCTFILE</i> . If not set, records will be written to the log file.
-e <i>LIBEXECDIR</i>	Look for service executables in <i>LIBEXECDIR</i> . If not specified, the sbin subdirectory of the parameter to -home is used, or /usr/sbin if that is not set.
-launch_method fork_and_exit fork_and_wait dont_fork dont_exit	Determine how to launch services. The method may be either dont_fork (the service runs completely independently of the gatekeeper, which exits after creating the new service process), fork_and_wait (the service is run in a separate process from the gatekeeper but the gatekeeper does not exit until the service terminates), or dont_fork, where the gatekeeper process becomes the service process via the exec ( ) system call.
-grid_services <i>SERVICEDIR</i>	Look for service descriptions in <i>SERVICEDIR</i> .
-globusid <i>GLOBUSID</i>	Sets the GLOBUSID environment variable to <i>GLOBUSID</i> . This variable is used to construct the gatekeeper contact string if it can not be parsed from the service credential.
-gridmap <i>GRIDMAP</i>	Use the file at <i>GRIDMAP</i> to map GSSAPI names to POSIX user names.
-x509_cert_dir <i>TRUSTED_CERT_DIR</i>	Use the directory <i>TRUSTED_CERT_DIR</i> to locate trusted CA X.509 certificates. The gatekeeper sets the environment variable X509_CERT_DIR to this value.
-x509_user_cert <i>CERT_PATH</i>	Read the service X.509 certificate from <i>CERT_PATH</i> . The gatekeeper sets the X509_USER_CERT environment variable to this value.
-x509_user_key <i>KEY_PATH</i>	Read the private key for the service from <i>KEY_PATH</i> . The gatekeeper sets the X509_USER_KEY environment variable to this value.
-x509_user_proxy <i>PROXY_PATH</i>	Read the X.509 proxy certificate from <i>PROXY_PATH</i> . The gatekeeper sets the X509_USER_PROXY environment variable to this value.

<code>-k</code>	Use the <b>globus-k5</b> command to acquire Kerberos 5 credentials before starting the service.
<code>-globusmap <i>KMAP</i></code>	Use <i>KMAP</i> as the path to the Grid credential to kerberos initialization mapping file.
<code>-pidfile <i>PIDFILE</i></code>	Write the process id of the <b>globus-gatekeeper</b> to the file named by <i>PIDFILE</i> .

## ENVIRONMENT

If the following variables affect the execution of **globus-gatekeeper**:

<code>X509_CERT_DIR</code>	Directory containing X.509 trust anchors and signing policy files.
<code>X509_USER_PROXY</code>	Path to file containing an X.509 proxy.
<code>X509_USER_CERT</code>	Path to file containing an X.509 user certificate.
<code>X509_USER_KEY</code>	Path to file containing an X.509 user key.
<code>GLOBUS_LOCATION</code>	Default path to gatekeeper service files.

## Files

<code>/etc/grid-services/<i>SERVICENAME</i></code>	Service configuration for <i>SERVICENAME</i> .
<code>/etc/grid-security/grid-mapfile</code>	Default file mapping Grid identities to POSIX identities.
<code>/etc/globusmap</code>	Default file mapping Grid identities to Kerberos 5 principals.
<code>/etc/globus-nologin</code>	File to disable the <b>globus-gatekeeper</b> program.
<code>/var/log/globus-gatekeeper.log</code>	Default gatekeeper log.

## See also

globus-k5(8), globusrun(1), globus-job-manager(8)



## Name

globus-gram-audit — Load GRAM4 and GRAM5 audit records into a database

## Synopsis

```
globus-gram-audit [--conf CONFIG_FILE] [--create] | [--update=OLD-VERSION]] [--check] [--delete] [--audit-directory AUDITDIR] [--quiet]
```

## Description

The **globus-gram-audit** program loads audit records to an SQL-based database. It reads `$GLOBUS_LOCATION/etc/globus-job-manager.conf` by default to determine the audit directory and then uploads all files in that directory that contain valid audit records to the database configured by the **globus\_gram\_job\_manager\_auditing\_setup\_scripts** package. If the upload completes successfully, the audit files will be removed.

The full set of command-line options to **globus-gram-audit** consist of:

<code>--conf <i>CONFIG_FILE</i></code>	Use <i>CONFIG_FILE</i> instead of the default from the configuration file for audit database configuration.
<code>--check</code>	Check whether the insertion of a record was successful by querying the database after inserting the records. This is used in tests.
<code>--delete</code>	Delete audit records from the database right after inserting them. This is used in tests to avoid filling the database with test records.
<code>--audit-directory <i>DIR</i></code>	Look for audit records in <i>DIR</i> , instead of looking in the directory specified in the job manager configuration. This is used in tests to control which records are loaded to the database and then deleted.
<code>--query <i>SQL</i></code>	Perform the given <i>SQL</i> query on the audit database. This uses the database information from the configuration file to determine how to contact the database.
<code>--quiet</code>	Reduce the amount of output for common operations.

## FILES

The **globus-gram-audit** uses the following files (paths relative to `$GLOBUS_LOCATION`).

<code>etc/globus-gram-job-manager.conf</code>	GRAM5 job manager configuration. It includes the default path to the audit directory
<code>etc/globus-gram-audit.conf</code>	Audit configuration. It includes the information needed to contact the audit database.

## Name

`globus-job-cancel` — Cancel a GRAM batch job

## Synopsis

```
globus-job-cancel [ -f | -force ] [ -q | -quiet ] JOBID
```

```
globus-job-cancel [-help] [-usage] [-version] [-versions]
```

## Description

The **globus-job-cancel** program cancels the job named by *JOBID*. Any cached files associated with the job will remain until **globus-job-clean** is executed for the job.

By default, **globus-job-cancel** prompts the user prior to canceling the job. This behavior can be overridden by specifying the `-f` or `-force` command-line options.

## Options

The full set of options to **globus-job-cancel** are:

`-help`, `-usage`    Display a help message to standard error and exit.

`-version`    Display the software version of the **globus-job-cancel** program to standard output.

`-version`    Display the software version of the **globus-job-cancel** program including DiRT information to standard output.

`-force`, `-f`    Do not prompt to confirm job cancel and clean-up.

`-quiet`, `-q`    Do not print diagnostics for succesful cancel. Implies `-f`.

## ENVIRONMENT

If the following variables affect the execution of **globus-job-cancel**.

`X509_USER_PROXY`    Path to proxy credential.

`X509_CERT_DIR`    Path to trusted certificate directory.

## Name

**globus-job-clean** — Cancel and clean up a GRAM batch job

## Synopsis

```
globus-job-clean [ -r RESOURCE | -resource RESOURCE ]
[ -f | -force ] [ -q | -quiet ] JOBID
```

```
globus-job-clean [-help] [-usage] [-version] [-versions]
```

## Description

The **globus-job-clean** program cancels the job named by *JOBID* if it is still running, and then removes any cached files on the GRAM service node related to that job. In order to do the file clean up, it submits a job which removes the cache files. By default this cleanup job is submitted to the default GRAM resource running on the same host as the job. This behavior can be controlled by specifying a resource manager contact string as the parameter to the `-r` or `-resource` option.

By default, **globus-job-clean** prompts the user prior to canceling the job. This behavior can be overridden by specifying the `-f` or `-force` command-line options.

## Options

The full set of options to **globus-job-clean** are:

<code>-help, -usage</code>	Display a help message to standard error and exit.
<code>-version</code>	Display the software version of the <b>globus-job-clean</b> program to standard output.
<code>-version</code>	Display the software version of the <b>globus-job-clean</b> program including DiRT information to standard output.
<code>-resource <i>RESOURCE</i>, -r <i>RESOURCE</i></code>	Submit the clean-up job to the resource named by <i>RESOURCE</i> instead of the default GRAM service on the same host as the job contact.
<code>-force, -f</code>	Do not prompt to confirm job cancel and clean-up.
<code>-quiet, -q</code>	Do not print diagnostics for succesful clean-up. Implies <code>-f</code>

## ENVIRONMENT

If the following variables affect the execution of **globus-job-clean**.

<code>X509_USER_PROXY</code>	Path to proxy credential.
<code>X509_CERT_DIR</code>	Path to trusted certificate directory.

## Name

**globus-job-get-output** — Retrieve the output and error streams from a GRAM job

## Synopsis

```
globus-job-get-output [ -r RESOURCE | -resource RESOURCE ]
[ -out | -err ] [ -t LINES | -tail LINES ] [ -follow LINES | -f LINES ] JOBID
```

```
globus-job-get-output [-help] [-usage] [-version] [-versions]
```

## Description

The **globus-job-get-output** program retrieves the output and error streams of the job named by *JOBID*. By default, **globus-job-get-output** will retrieve all output and error data from the job and display them to its own output and error streams. Other behavior can be controlled by using command-line options. The data retrieval is implemented by submitting another job which simply displays the contents of the first job's output and error streams. By default this retrieval job is submitted to the default GRAM resource running on the same host as the job. This behavior can be controlled by specifying a particular resource manager contact string as the *RESOURCE* parameter to the *-r* or *-resource* option.

## Options

The full set of options to **globus-job-get-output** are:

<i>-help</i> , <i>-usage</i>	Display a help message to standard error and exit.
<i>-version</i>	Display the software version of the <b>globus-job-get-output</b> program to standard output.
<i>-version</i>	Display the software version of the <b>globus-job-get-output</b> program including DiRT information to standard output.
<i>-resource RESOURCE</i> , <i>-r RESOURCE</i>	Submit the retrieval job to the resource named by <i>RESOURCE</i> instead of the default GRAM service on the same host as the job contact.
<i>-out</i>	Retrieve only the standard output stream of the job. The default is to retrieve both standard output and standard error.
<i>-err</i>	Retrieve only the standard error stream of the job. The default is to retrieve both standard output and standard error.
<i>-tail LINES</i> , <i>-t LINES</i>	Print only the last <i>LINES</i> count lines of output from the data streams being retrieved. By default, the entire output and error file data is retrieved. This option can not be used along with the <i>-f</i> or <i>-follow</i> options.
<i>-follow LINES</i> , <i>-f LINES</i>	Print the last <i>LINES</i> count lines of output from the data streams being retrieved and then wait until canceled, printing any subsequent job output that occurs. By default, the entire output and error file data is retrieved. This option can not be used along with the <i>-t</i> or <i>-tail</i> options.

## ENVIRONMENT

If the following variables affect the execution of **globus-job-get-output**.

X509\_USER\_PROXY Path to proxy credential.

X509\_CERT\_DIR Path to trusted certificate directory.

DRAFT

# Name

globus-job-manager — Execute and monitor jobs

## Synopsis

```
globus-job-manager {-type LRM} [-conf CONFIG_PATH] [-help] [-globus-host-manufacturer
MANUFACTURER] [-globus-host-cputype CPUTYPE] [-globus-host-osname OSNAME] [-globus-host-osversion
OSVERSION] [-globus-gatekeeper-host HOST] [-globus-gatekeeper-port PORT] [-globus-gatekeeper-subject
SUBJECT] [-home GLOBUS_LOCATION] [-target-globus-location TARGET_GLOBUS_LOCATION] [-condor-
arch ARCH] [-condor-os OS] [-history HISTORY_DIRECTORY] [-scratch-dir-base SCRATCH_DIRECTORY]
[-enable-syslog] [-stdio-log LOG_DIRECTORY] [-log-pattern PATTERN] [-log-levels LEVELS] [-state-file-dir
STATE_DIRECTORY] [-globus-tcp-port-range PORT_RANGE] [-globus-tcp-source-range SOURCE_RANGE] [-
x509-cert-dir TRUSTED_CERTIFICATE_DIRECTORY] [-cache-location GASS_CACHE_DIRECTORY] [-k] [-
extra-envvars VAR=VAL, . . .] [-seg-module SEG_MODULE] [-audit-directory AUDIT_DIRECTORY] [-globus-
toolkit-version TOOLKIT_VERSION] [-disable-streaming] [-disable-usagestats] [-usagestats-targets TARGET] [-
service-tag SERVICE_TAG]
```

## Description

The **globus-job-manager** program is a service which starts and controls GRAM jobs which are executed by a local resource management system, such as LSF or Condor. The **globus-job-manager** program is typically started by the **globus-gatekeeper** program and not directly by a user. It runs until all jobs it is managing have terminated or its delegated credentials have expired.

Typically, users interact with the **globus-job-manager** program via client applications such as **globusrun**, **globus-job-submit**, or tools such as CoG jglobus or Condor-G.

The full set of command-line options to **globus-job-manager** consists of:

-help	Display a help message to standard error and exit
-type <i>LRM</i>	Execute jobs using the local resource manager named <i>LRM</i> .
-conf <i>CONFIG_PATH</i>	Read additional command-line arguments from the file <i>CONFIG_PATH</i> . If present, this must be the first command-line argument to the <b>globus-job-manager</b> program.
-globus-host-manufacturer <i>MANUFACTURER</i>	Indicate the manufacturer of the system which the jobs will execute on. This parameter sets the value of the \$( GLOBUS_HOST_MANUFACTURER ) RSL substitution to <i>MANUFACTURER</i>
-globus-host-cputype <i>CPUTYPE</i>	Indicate the CPU type of the system which the jobs will execute on. This parameter sets the value of the \$( GLOBUS_HOST_CPUTYPE ) RSL substitution to <i>CPUTYPE</i>
-globus-host-osname <i>OSNAME</i>	Indicate the operating system type of the system which the jobs will execute on. This parameter sets the value of the \$( GLOBUS_HOST_OSNAME ) RSL substitution to <i>OSNAME</i>
-globus-host-osversion <i>OSVERSION</i>	Indicate the operating system version of the system which the jobs will execute on. This parameter sets the value of the \$( GLOBUS_HOST_OSVERSION ) RSL substitution to <i>OSVERSION</i>
-globus-gatekeeper-host <i>HOST</i>	Indicate the host name of the machine which the job was submitted to. This parameter sets the value of the \$( GLOBUS_GATEKEEPER_HOST ) RSL substitution to <i>HOST</i>

<code>-globus-gatekeeper-port</code> <i>PORT</i>	Indicate the TCP port number of gatekeeper to which jobs are submitted to. This parameter sets the value of the <code>\$(GLOBUS_GATEKEEPER_PORT)</code> RSL substitution to <i>PORT</i> .
<code>-globus-gatekeeper-subject</code> <i>SUBJECT</i>	Indicate the X.509 identity of the gatekeeper to which jobs are submitted to. This parameter sets the value of the <code>\$(GLOBUS_GATEKEEPER_SUBJECT)</code> RSL substitution to <i>SUBJECT</i> .
<code>-home</code> <i>GLOBUS_LOCATION</i>	Indicate the path where the Globus Toolkit(r) is installed on the service node. This is used by the job manager to locate its support and configuration files.
<code>-target-globus-location</code> <i>TARGET_GLOBUS_LOCATION</i>	Indicate the path where the Globus Toolkit(r) is installed on the execution host. If this is omitted, the value specified as a parameter to <code>-home</code> is used. This parameter sets the value of the <code>\$(GLOBUS_LOCATION)</code> RSL substitution to <i>TARGET_GLOBUS_LOCATION</i> .
<code>-history</code> <i>HISTORY_DIRECTORY</i>	Configure the job manager to write job history files to <i>HISTORY_DIRECTORY</i> . These files are described in the FILES section below.
<code>-scratch-dir-base</code> <i>SCRATCH_DIRECTORY</i>	Configure the job manager to use <i>SCRATCH_DIRECTORY</i> as the default scratch directory root if a relative path is specified in the job RSL's <code>scratch_dir</code> attribute.
<code>-enable-syslog</code>	Configure the job manager to write log messages via syslog. Logging is further controlled by the argument to the <code>-log-levels</code> parameter described below.
<code>-log-pattern</code> <i>PATTERN</i>	Configure the job manager to write log messages to files named by the string <i>PATTERN</i> . The <i>PATTERN</i> string may contain job-independent RSL substitutions such as <code>\$(HOME)</code> , <code>\$(LOGNAME)</code> , etc, as well as the special RSL substitution <code>\$(DATE)</code> which will be resolved at log time to the date in YYYYMMDD form.
<code>-stdio-log</code> <i>LOG_DIRECTORY</i>	Configure the job manager to write log messages to files in the <i>LOG_DIRECTORY</i> directory. This is a backward-compatible parameter, equivalent to <code>-log-pattern LOG_DIRECTORY/gram_\$(DATE).log</code> .
<code>-log-levels</code> <i>LEVELS</i>	Configure the job manager to write log messages of certain levels to syslog and/or log files. The available log levels are FATAL, ERROR, WARN, INFO, DEBUG, and TRACE. Multiple values can be combined with the <code> </code> character. The default value of logging when enabled is FATAL   ERROR.
<code>-state-file-dir</code> <i>STATE_DIRECTORY</i>	Configure the job manager to write state files to <i>STATE_DIRECTORY</i> . If not specified, the job manager uses the default of <code>\$(GLOBUS_LOCATION)/tmp/gram_job_state/</code> . This directory must be writable by all users and be on a file system which supports POSIX advisory file locks.
<code>-globus-tcp-port-range</code> <i>PORT_RANGE</i>	Configure the job manager to restrict its TCP/IP communication to use ports in the range described by <i>PORT_RANGE</i> . This value is also made available in the job environment via the <code>GLOBUS_TCP_PORT_RANGE</code> environment variable.
<code>-globus-tcp-source-range</code> <i>SOURCE_RANGE</i>	Configure the job manager to restrict its TCP/IP communication to use source ports in the range described by <i>SOURCE_RANGE</i> . This value is also made

	available in the job environment via the <code>GLOBUS_TCP_SOURCE_RANGE</code> environment variable.
<code>-x509-cert-dir</code> <code>TRUSTED_CERTIFICATE_DIRECTORY</code>	Configure the job manager to search <code>TRUSTED_CERTIFICATE_DIRECTORY</code> for its list of trusted CA certificates and their signing policies. This value is also made available in the job environment via the <code>X509_CERT_DIR</code> environment variable.
<code>-cache-location</code> <code>GASS_CACHE_DIRECTORY</code>	Configure the job manager to use the path <code>GASS_CACHE_DIRECTORY</code> for its temporary GASS-cache files. This value is also made available in the job environment via the <code>GLOBUS_GASS_CACHE_DEFAULT</code> environment variable.
<code>-k</code>	Configure the job manager to assume it is using Kerberos for authentication instead of X.509 certificates. This disables some certificate-specific processing in the job manager.
<code>-extra-envvars</code> <code>VAR=VAL,...</code>	Configure the job manager to define a set of environment variables in the job environment beyond those defined in the base job environment. The format of the parameter to this argument is a comma-separated sequence of <code>VAR=VAL</code> pairs, where <code>VAR</code> is the variable name and <code>VAL</code> is the variable's value. If the value is not specified, then the value of the variable in the job manager's environment is used. This option may be present multiple times on the command-line or the job manager configuration file to append multiple environment settings.
<code>-seg-module</code> <code>SEG_MODULE</code>	Configure the job manager to use the schedule event generator module named by <code>SEG_MODULE</code> to detect job state changes events from the local resource manager, in place of the less efficient polling operations used in GT2. To use this, one instance of the <b>globus-job-manager-event-generator</b> must be running to process events for the LRM into a generic format that the job manager can parse.
<code>-audit-directory</code> <code>AUDIT_DIRECTORY</code>	Configure the job manager to write audit records to the directory named by <code>AUDIT_DIRECTORY</code> . This records can be loaded into a database using the <b>globus-gram-audit</b> program.
<code>-globus-toolkit-version</code> <code>TOOLKIT_VERSION</code>	Configure the job manager to use <code>TOOLKIT_VERSION</code> as the version for audit and usage stats records.
<code>-service-tag</code> <code>SERVICE_TAG</code>	Configure the job manager to use <code>SERVICE_TAG</code> as a unique identifier to allow multiple GRAM instances to use the same job state directories without interfering with each other's jobs. If not set, the value <code>untagged</code> will be used.
<code>-disable-streaming</code>	Configure the job manager to disable file streaming. This is propagated to the LRM script interface but has no effect in GRAM5.
<code>-disable-usagestats</code>	Disable sending of any usage stats data, even if <code>-usagestats-targets</code> is present in the configuration.
<code>-usagestats-targets</code> <code>TARGET</code>	Send usage packets to a data collection service for analysis. The <code>TARGET</code> string consists of a comma-separated list of <code>HOST:PORT</code> combinations, each containing an optional list of data to send. See <a href="#">Usage Stats Packets</a> <sup>1</sup> for more information about the tags. Special tag strings of <code>all</code> (which enables all tags) and <code>default</code> may be used, or a sequence of characters for the various tags.



	If this option is not present in the configuration, then the default of usage-stats.globus.org:4810 is used.
<code>-condor-arch ARCH</code>	Set the architecture specification for condor jobs to be <i>ARCH</i> in job classified ads generated by the GRAM5 condor LRM script. This is required for the condor LRM but ignored for all others.
<code>-condor-os OS</code>	Set the operating system specification for condor jobs to be <i>OS</i> in job classified ads generated by the GRAM5 condor LRM script. This is required for the condor LRM but ignored for all others.

## Environment

If the following variables affect the execution of **globus-job-manager**

HOME	User's home directory.
LOGNAME	User's name.
JOBMANAGER_SYSLOG_ID	String to prepend to syslog audit messages.
JOBMANAGER_SYSLOG_FAC	Facility to log syslog audit messages as.
JOBMANAGER_SYSLOG_LVL	Priority level to use for syslog audit messages.
GATEKEEPER_JM_ID	Job manager ID to be used in syslog audit records.
GATEKEEPER_PEER	Peer information to be used in syslog audit records
GLOBUS_ID	Credential information to be used in syslog audit records
GLOBUS_JOB_MANAGER_SLEEP	Time (in seconds) to sleep when the job manager is started. [For debugging purposes only]
GRID_SECURITY_HTTP_BODY_FD	File descriptor of an open file which contains the initial job request and to which the initial job reply should be sent. This file descriptor is inherited from the <b>globus-gatekeeper</b> .
X509_USER_PROXY	Path to the X.509 user proxy which was delegated by the client to the <b>globus-gatekeeper</b> program to be used by the job manager.
GRID_SECURITY_CONTEXT_FD	File descriptor containing an exported security context that the job manager should use to reply to the client which submitted the job.
GLOBUS_USAGE_TARGETS	Default list of usagestats services to send usage packets to.
GLOBUS_TCP_PORT_RANGE	Default range of allowed TCP ports to listen on. The <code>-globus-tcp-port-range</code> command-line option overrides this.
GLOBUS_TCP_SOURCE_RANGE	Default range of allowed TCP ports to bind to. The <code>-globus-tcp-source-range</code> command-line option overrides this.

## Files

<code>\$HOME/.globus/job/HOSTNAME/LRM.TAG.red</code>	Job manager delegated user credential.
--	--

<code>\$HOME/.globus/ job/HOSTNAME/ LRM.TAG.lock</code>	Job manager state lock file.
<code>\$HOME/.globus/ job/HOSTNAME/LRM.TAG.pid</code>	Job manager pid file.
<code>\$HOME/.globus/ job/HOSTNAME/ LRM.TAG.sock</code>	Job manager socket for inter-job manager communications.
<code>\$HOME/.globus/ job/HOSTNAME/JOB_ID/</code>	Job-specific state directory.
<code>\$HOME/.globus/ job/HOSTNAME/JOB_ID/ stdin</code>	Standard input which has been staged from a remote URL.
<code>\$HOME/.globus/ job/HOSTNAME/JOB_ID/ stdout</code>	Standard output which will be staged from a remote URL.
<code>\$HOME/.globus/ job/HOSTNAME/JOB_ID/ stderr</code>	Standard error which will be staged from a remote URL.
<code>\$HOME/.globus/ job/HOSTNAME/JOB_ID/ x509_user_proxy</code>	Job-specific delegated credential.
<code>\$GLOBUS_LOCATION/ tmp/gram_job_state/ job.HOSTNAME.JOB_ID</code>	Job state file.
<code>\$GLOBUS_LOCATION/ tmp/gram_job_state/ job.HOSTNAME.JOB_ID.lock</code>	Job state lock file. In most cases this will be a symlink to the job manager lock file.
<code>\$GLOBUS_LOCATION/etc/ globus-job-manager.conf</code>	Default location of the global job manager configuration file.
<code>\$GLOBUS_LOCATION/ etc/grid-services/ jobmanager-LRM</code>	Default location of the LRM-specific gatekeeper configuration file.
<code>\$GLOBUS_LOCATION/ etc/globus/gram/job-- manager.rvf</code>	Default location of the site-specific job manager RSL validation file.
<code>\$GLOBUS_LOCATION/etc/ globus/gram/lrm.rvf</code>	Default location of the site-specific job manager RSL validation file for the named lrm.

## See Also

globusrun(1), globus-gatekeeper(8), globus-personal-gatekeeper(1), globus-gram-audit(8)

## Name

globus-job-run — Execute a job using GRAM

## Synopsis

```
globus-job-run [-dumpysl] [-dryrun] [-verify]
[-file ARGUMENT_FILE]
SERVICE_CONTACT
[ -np PROCESSES | -count PROCESSES ]
[ -m MAX_TIME | -maxtime MAX_TIME ]
[ -p PROJECT | -project PROJECT ]
[ -q QUEUE | -queue QUEUE ]
[ -d DIRECTORY | -directory DIRECTORY ] [-env NAME=VALUE]...
[-stdin [ -l | -s ] STDIN_FILE ] [-stdout [ -l | -s ] STDOUT_FILE ] [-stderr [ -l | -s ] STDERR_FILE ]
[-x RSL_CLAUSE]
[ -l | -s ] EXECUTABLE [ARGUMENT...]
```

```
globus-job-run [-help] [-usage] [-version] [-versions]
```

## Description

The **globus-job-run** program constructs a job description from its command-line options and then submits the job to the GRAM service running at *SERVICE\_CONTACT*. The executable and arguments to the executable are provided on the command-line after all other options. Note that the `-dumpysl`, `-dryrun`, `-verify`, and `-file` command-line options must occur before the first non-option argument, the *SERVICE\_CONTACT*.

The **globus-job-run** provides similar functionality to **globusrun** in that it allows interactive start-up of GRAM jobs. However, unlike **globusrun**, it uses command-line parameters to define the job instead of RSL expressions.

## Options

The full set of options to **globus-job-run** are:

<code>-help, -usage</code>	Display a help message to standard error and exit.
<code>-version</code>	Display the software version of the <b>globus-job-run</b> program to standard output.
<code>-version</code>	Display the software version of the <b>globus-job-run</b> program including DiRT information to standard output.
<code>-dumpysl</code>	Translate the command-line options to <b>globus-job-run</b> into an RSL expression that can be used with tools such as <b>globusrun</b> .
<code>-dryrun</code>	Submit the job request to the GRAM service with the <code>dryrun</code> option enabled. When this option is used, the GRAM service prepares to execute the job but stops before submitting the job to the LRM. This can be used to diagnose some problems such as missing files.
<code>-verify</code>	Submit the job request to the GRAM service with the <code>dryrun</code> option enabled and then without it enabled if the <code>dryrun</code> is successful.
<code>-file ARGUMENT_FILE</code>	Read additional command-line options from <i>ARGUMENT_FILE</i> .

<code>-np PROCESSES, -count PROCESSES</code>	Start <i>PROCESSES</i> instances of the executable as a single job.
<code>-m MAX_TIME, -maxtime MAX_TIME</code>	Schedule the job to run for a maximum of <i>MAX_TIME</i> minutes.
<code>-p PROJECT, -project PROJECT</code>	Request that the job use the allocation <i>PROJECT</i> when submitting the job to the LRM.
<code>-q QUEUE, -queue QUEUE</code>	Request that the job be submitted to the LRM using the named <i>QUEUE</i> .
<code>-d DIRECTORY, -directory DIRECTORY</code>	Run the job in the directory named by <i>DIRECTORY</i> . Input and output files will be interpreted relative to this directory. This directory must exist on the file system on the LRM-managed resource. If not specified, the job will run in the home directory of the user the job is running as.
<code>-env NAME=VALUE</code>	Define an environment variable named by <i>NAME</i> with the value <i>VALUE</i> in the job environment. This option may be specified multiple times to define multiple environment variables.
<code>-stdin [-l   -s] STDIN_FILE</code>	Use the file named by <i>STDIN_FILE</i> as the standard input of the job. If the <code>-l</code> option is specified, then this file is interpreted to be on a file system local to the LRM. If the <code>-s</code> option is specified, then this file is interpreted to be on the file system where <b>globus-job-run</b> is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.
<code>-stdout [-l   -s] STDOUT_FILE</code>	Use the file named by <i>STDOUT_FILE</i> as the destination for the standard output of the job. If the <code>-l</code> option is specified, then this file is interpreted to be on a file system local to the LRM. If the <code>-s</code> option is specified, then this file is interpreted to be on the file system where <b>globus-job-run</b> is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.
<code>-stderr [-l   -s] STDERR_FILE</code>	Use the file named by <i>STDERR_FILE</i> as the destination for the standard error of the job. If the <code>-l</code> option is specified, then this file is interpreted to be on a file system local to the LRM. If the <code>-s</code> option is specified, then this file is interpreted to be on the file system where <b>globus-job-run</b> is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.
<code>-x RSL_CLAUSE</code>	Add a set of custom RSL attributes described by <i>RSL_CLAUSE</i> to the job description. The clause must be an RSL conjunction and may contain one or more attributes. This can be used to include attributes which can not be defined by other command-line options of <b>globus-job-run</b> .
<code>-l</code>	When included outside the context of <code>-stdin</code> , <code>-stdout</code> , or <code>-stderr</code> command-line options, <code>-l</code> option alters the interpretation of the executable path. If the <code>-l</code> option is specified, then the executable is interpreted to be on a file system local to the LRM.
<code>-s</code>	When included outside the context of <code>-stdin</code> , <code>-stdout</code> , or <code>-stderr</code> command-line options, <code>-s</code> option alters the interpretation of the executable path. If the <code>-s</code> option is specified, then the executable is interpreted to be on the file system where <b>globus-job-run</b> is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.

## ENVIRONMENT

If the following variables affect the execution of **globus-job-run**.

X509\_USER\_PROXY Path to proxy credential.

X509\_CERT\_DIR Path to trusted certificate directory.

## See Also

globusrun(1), globus-job-submit(1), globus-job-clean(1), globus-job-get-output(1), globus-job-cancel(1)

DRAFT

## Name

globus-job-status — Check the status of a GRAM5 job

## Synopsis

globus-job-status *JOBID*

globus-job-status [-help] [-usage] [-version] [-versions]

## Description

The **globus-job-status** program checks the status of a GRAM job by sending a status request to the job manager contact for that job specified by the *JOBID* parameter. If successful, it will print the job status to standard output. The states supported by **globus-job-status** are:

PENDING	The job has been submitted to the LRM but has not yet begun execution.
ACTIVE	The job has begun execution.
FAILED	The job has failed.
SUSPENDED	The job is currently suspended by the LRM.
DONE	The job has completed.
UNSUBMITTED	The job has been accepted by GRAM, but not yet submitted to the LRM.
STAGE_IN	The job has been accepted by GRAM and is currently staging files prior to being submitted to the LRM.
STAGE_OUT	The job has completed execution and is currently staging files from the service node to other http, GASS, or GridFTP servers.

## Options

The full set of options to **globus-job-status** are:

- help, -usage Display a help message to standard error and exit.
- version Display the software version of the **globus-job-status** program to standard output.
- versions Display the software version of the **globus-job-status** program including DiRT information to standard output.

## ENVIRONMENT

If the following variables affect the execution of **globus-job-status**.

X509\_USER\_PROXY Path to proxy credential.

X509\_CERT\_DIR Path to trusted certificate directory.

## Bugs

The **globus-job-status** program can not distinguish between the case of the job manager terminating for any reason and the job being in the `DONE` state.

## See Also

`globusrun(1)`

DRAFT

## Name

globus-job-submit — Submit a batch job using GRAM

## Synopsis

```
globus-job-submit [-dumprsl] [-dryrun] [-verify]
[-file ARGUMENT_FILE]
SERVICE_CONTACT
[ -np PROCESSES | -count PROCESSES ]
[ -m MAX_TIME | -maxtime MAX_TIME ]
[ -p PROJECT | -project PROJECT ]
[ -q QUEUE | -queue QUEUE ]
[ -d DIRECTORY | -directory DIRECTORY ] [-env NAME=VALUE]...
[-stdin [ -l | -s ] STDIN_FILE ] [-stdout [ -l | -s ] STDOUT_FILE ] [-stderr [ -l | -s ] STDERR_FILE ]
[-x RSL_CLAUSE]
[ -l | -s ] EXECUTABLE [ARGUMENT...]
```

```
globus-job-submit [-help] [-usage] [-version] [-versions]
```

## Description

The **globus-job-submit** program constructs a job description from its command-line options and then submits the job to the GRAM service running at *SERVICE\_CONTACT*. The executable and arguments to the executable are provided on the command-line after all other options. Note that the *-dumprsl*, *-dryrun*, *-verify*, and *-file* command-line options must occur before the first non-option argument, the *SERVICE\_CONTACT*.

The **globus-job-submit** provides similar functionality to **globusrun** in that it allows batch submission of GRAM jobs. However, unlike **globusrun**, it uses command-line parameters to define the job instead of RSL expressions.

To retrieve the output and error streams of the job, use the program **globus-job-get-output**. To reclaim resources used by the job by deleting cached files and job state, use the program **globus-job-clean**. To cancel a batch job submitted by **globus-job-submit**, use the program **globus-job-cancel**.

## Options

The full set of options to **globus-job-submit** are:

<i>-help</i> , <i>-usage</i>	Display a help message to standard error and exit.
<i>-version</i>	Display the software version of the <b>globus-job-submit</b> program to standard output.
<i>-versions</i>	Display the software version of the <b>globus-job-submit</b> program including DiRT information to standard output.
<i>-dumprsl</i>	Translate the command-line options to <b>globus-job-submit</b> into an RSL expression that can be used with tools such as <b>globusrun</b> .
<i>-dryrun</i>	Submit the job request to the GRAM service with the <i>dryrun</i> option enabled. When this option is used, the GRAM service prepares to execute the job but stops before submitting the job to the LRM. This can be used to diagnose some problems such as missing files.
<i>-verify</i>	Submit the job request to the GRAM service with the <i>dryrun</i> option enabled and then without it enabled if the <i>dryrun</i> is successful.



<code>-file ARGUMENT_FILE</code>	Read additional command-line options from <i>ARGUMENT_FILE</i> .
<code>-np PROCESSES, -count PROCESSES</code>	Start <i>PROCESSES</i> instances of the executable as a single job.
<code>-m MAX_TIME, -maxtime MAX_TIME</code>	Schedule the job to run for a maximum of <i>MAX_TIME</i> minutes.
<code>-p PROJECT, -project PROJECT</code>	Request that the job use the allocation <i>PROJECT</i> when submitting the job to the LRM.
<code>-q QUEUE, -queue QUEUE</code>	Request that the job be submitted to the LRM using the named <i>QUEUE</i> .
<code>-d DIRECTORY, -directory DIRECTORY</code>	Run the job in the directory named by <i>DIRECTORY</i> . Input and output files will be interpreted relative to this directory. This directory must exist on the file system on the LRM-managed resource. If not specified, the job will run in the home directory of the user the job is running as.
<code>-env NAME=VALUE</code>	Define an environment variable named by <i>NAME</i> with the value <i>VALUE</i> in the job environment. This option may be specified multiple times to define multiple environment variables.
<code>-stdin [-l   -s] STDIN_FILE</code>	Use the file named by <i>STDIN_FILE</i> as the standard input of the job. If the <code>-l</code> option is specified, then this file is interpreted to be on a file system local to the LRM. If the <code>-s</code> option is specified, then this file is interpreted to be on the file system where <b>globus-job-submit</b> is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.
<code>-stdout [-l   -s] STDOUT_FILE</code>	Use the file named by <i>STDOUT_FILE</i> as the destination for the standard output of the job. If the <code>-l</code> option is specified, then this file is interpreted to be on a file system local to the LRM. If the <code>-s</code> option is specified, then this file is interpreted to be on the file system where <b>globus-job-submit</b> is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.
<code>-stderr [-l   -s] STDERR_FILE</code>	Use the file named by <i>STDERR_FILE</i> as the destination for the standard error of the job. If the <code>-l</code> option is specified, then this file is interpreted to be on a file system local to the LRM. If the <code>-s</code> option is specified, then this file is interpreted to be on the file system where <b>globus-job-submit</b> is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.
<code>-x RSL_CLAUSE</code>	Add a set of custom RSL attributes described by <i>RSL_CLAUSE</i> to the job description. The clause must be an RSL conjunction and may contain one or more attributes. This can be used to include attributes which can not be defined by other command-line options of <b>globus-job-submit</b> .
<code>-l</code>	When included outside the context of <code>-stdin</code> , <code>-stdout</code> , or <code>-stderr</code> command-line options, <code>-l</code> option alters the interpretation of the executable path. If the <code>-l</code> option is specified, then the executable is interpreted to be on a file system local to the LRM.
<code>-s</code>	When included outside the context of <code>-stdin</code> , <code>-stdout</code> , or <code>-stderr</code> command-line options, <code>-s</code> option alters the interpretation of the executable path. If the <code>-s</code> option is specified, then the executable is interpreted to be on

the file system where **globus-job-run** is being executed, and the file will be staged via GASS. If neither is specified, the local behavior is assumed.

## ENVIRONMENT

If the following variables affect the execution of **globus-job-submit**.

`X509_USER_PROXY` Path to proxy credential.

`X509_CERT_DIR` Path to trusted certificate directory.

## See Also

`globusrun(1)`, `globus-job-run(1)`, `globus-job-clean(1)`, `globus-job-get-output(1)`, `globus-job-cancel(1)`

DRAFT

## Name

**globus-personal-gatekeeper** — Manage a user's personal gatekeeper daemon

## Synopsis

```
globus-personal-gatekeeper [-help] [-usage] [-version] [-versions] [-list] [-directory CONTACT]
```

```
globus-personal-gatekeeper [-debug] {-start} [-jmttype LRM] [-auditdir AUDIT_DIRECTORY] [-port PORT] [-log[=DIRECTORY]] [-seg] [-acctfile ACCOUNTING_FILE]
```

```
globus-personal-gatekeeper [-killall] [-kill]
```

## Description

The **globus-personal-gatekeeper** command is a utility which manages a gatekeeper and job manager service for a single user. Depending on the command-line arguments it will operate in one of several modes. In the first set of arguments indicated in the synopsis, the program provides information about the **globus-personal-gatekeeper** command or about instances of the **globus-personal-gatekeeper** that are running currently. The second set of arguments indicated in the synopsis provide control over starting a new **globus-personal-gatekeeper** instance. The final set of arguments provide control for terminating one or more **globus-personal-gatekeeper** instances.

The **-start** mode will create a new subdirectory of `$HOME/.globus` and write the configuration files needed to start a **globus-gatekeeper** daemon which will invoke the **globus-job-manager** service when new authenticated connections are made to its service port. The **globus-personal-gatekeeper** then exits, printing the contact string for the new gatekeeper prefixed by `GRAM contact:` to standard output. In addition to the arguments described above, any arguments described in **globus-job-manager(8)** can be appended to the command-line and will be added to the job manager configuration for the service started by the **globus-gatekeeper**.

The new **globus-gatekeeper** will continue to run in the background until killed by invoking **globus-personal-gatekeeper** with the **-kill** or **-killall** argument. When killed, it will kill the **globus-gatekeeper** and **globus-job-manager** processes, remove state files and configuration data, and then exit. Jobs which are running when the personal gatekeeper is killed will continue to run, but their job directory will be destroyed so they may fail in the LRM.

The full set of command-line options to **globus-personal-gatekeeper** consists of:

<b>-help, -usage</b>	Print command-line option summary and exit
<b>-version</b>	Print software version
<b>-versions</b>	Print software version including DiRT information
<b>-list</b>	Print a list of all currently running personal gatekeepers. These entries will be printed one per line.
<b>-directory <i>CONTACT</i></b>	Print the configuration directory for the personal gatekeeper with the contact string <i>CONTACT</i> .
<b>-debug</b>	Print additional debugging information when starting a personal gatekeeper. This option is ignored in other modes.
<b>-start</b>	Start a new personal gatekeeper process.
<b>-jmttype <i>LRM</i></b>	Use <i>LRM</i> as the local resource manager interface. If not provided when starting a personal gatekeeper, the job manager will use the default <code>fork</code> LRM.

<code>-auditdir AUDIT_DIRECTORY</code>	Write audit report files to <i>AUDIT_DIRECTORY</i> . If not provided, the job manager will not write any audit files.
<code>-port PORT</code>	Listen for gatekeeper TCP/IP connections on the port <i>PORT</i> . If not provided, the gatekeeper will let the operating system choose.
<code>-log[=DIRECTORY]</code>	Write job manager log files to <i>DIRECTORY</i> . If <i>DIRECTORY</i> is omitted, the default of <i>\$HOME</i> will be used. If this option is not present, the job manager will not write any log files.
<code>-seg</code>	Try to use the SEG mechanism to receive job state change information, instead of polling for these. These require either the system administrator or the user to run an instance of the <b>globus-job-manager-event-generator</b> program for the LRM specified by the <code>-jmttype</code> option.
<code>-acctfile ACCOUNTING_FILE</code>	Write gatekeeper accounting entries to <i>ACCOUNTING_FILE</i> . If not provided, no accounting records are written.

## Examples

This example shows the output when starting a new personal gatekeeper which will schedule jobs via the *lsf* LRM, with debugging enabled.

```
% globus-personal-gatekeeper -start -jmttype lsf
```

```
verifying setup...
```

```
done.
```

```
GRAM contact: personal-grid.example.org:57846:/DC=org/DC=example/CN=Joe User
```

This example shows the output when listing the current active personal gatekeepers.

```
% globus-personal-gatekeeper -list
```

```
personal-grid.example.org:57846:/DC=org/DC=example/CN=Joe User
```

This example shows the output when querying the configuration directory for the above personal gatekeeper.

```
% globus-personal-gatekeeper -directory "personal-grid.example.org:57846:/DC=org/DC=example/CN=Joe User"
```

```
/home/juser/.globus/.personal-gatekeeper.personal-grid.example.org.1337
```

```
% globus-personal-gatekeeper -kill "personal-grid.example.org:57846:/DC=org/DC=example/CN=Joe User"
```

```
killing gatekeeper: "personal-grid.example.org:57846:/DC=org/DC=example/CN=Joe User"
```

## See Also

globusrun(1), globus-job-manager(8), globus-gatekeeper(8)

## Name

globus-rvf-check — Edit a GRAM5 RSL validation file

## Synopsis

```
globus-rvf-check [-h] [-help]
```

```
globus-rvf-check [-d] {FILENAME...}
```

## Description

The **globus-rvf-check** command is a utility which checks the syntax of a RSL validation file, and prints out parse errors when encountered. It can also parse the RVF file contents and then dump file's contents to stdout, after canonicalizing values and quoting. The exit code of **globus-rvf-check** is 0 if all files specified on the command line exist and have no parse errors.

The full set of command-line options to **globus-rvf-check** consists of:

-h, -        Print command-line option summary and exit  
help, --  
help

-d        Dump the RVF contents to stdout. In the output, Each file which is parsed will be prefixed by an RVF comment which contains the input filename. If not specified, **globus-rvf-check** just prints a diagnostic message to standard output indicating whether the file could be parsed.

## Name

globus-rvf-edit — Edit a GRAM5 RSL validation file

## Synopsis

```
globus-rvf-edit [-h]
```

```
globus-rvf-edit [[-s] | [-l LRM] | [-f PATH]]
```

## Description

The **globus-rvf-edit** command is a utility which opens the default editor on a specified RSL validation file, and then, when editing completes, runs the **globus-rvf-check** command to verify that the RVF file syntax is correct. If a parse error occurs, the user will be given an option to rerun the editor or discard the modifications.

The full set of command-line options to **globus-rvf-edit** consists of:

- h            Print command-line option summary and exit
- s            Edit of the site-specific RVF file, which provides override values applicable to all LRMs installed on the system.
- l *LRM*      Edit the site-specific LRM overrides for the LRM named by the *LRM* parameter to the option.
- f *PATH*     Edit the RVF file located at *PATH*

## Name

globus-scheduler-event-generator-admin — Manage SEG modules

## Synopsis

```
globus-scheduler-event-generator-admin [-h]
```

```
globus-scheduler-event-generator-admin [-l]
```

```
globus-scheduler-event-generator-admin [-e MODULE]
```

```
globus-scheduler-event-generator-admin [-d MODULE]
```

## Description

The **globus-scheduler-event-generator-admin** program manages SEG modules which are used by the **globus-scheduler-event-generator** to monitor a local resource manager or batch system for events. The **globus-scheduler-event-generator-admin** can list, enable, or disable specific SEG modules. The `-h` command-line option shows a brief usage message.

## Listing SEG Modules

The `-l` command-line option to **globus-scheduler-event-generator-admin** will cause it to list all of the SEG modules which are available to be run by the **globus-scheduler-event-generator**. In the output, the service name will be followed by its status in brackets. Possible status strings are `ENABLED` and `DISABLED`.

## Enabling SEG Modules

The `-e MODULE` command-line option to **globus-scheduler-event-generator-admin** will cause it to enable the module so that the init script for the **globus-scheduler-event-generator** will run it.

## Disabling SEG Modules

The `-d MODULE` command-line option to **globus-scheduler-event-generator-admin** will cause it to disable the module so that it will not be started by the **globus-scheduler-event-generator** init script.

## Files

`/etc/globus/scheduler-event-generator`      Default location of enabled SEG modules.

## See Also

globus-scheduler-event-generator(8)

## Name

globus-scheduler-event-generator — Process LRM events into a common format for use with GRAM

## Synopsis

```
globus-scheduler-event-generator -s LRM  
[-t TIMESTAMP] [-d DIRECTORY]  
[-b] [-p PIDFILE]
```

## Description

The **globus-scheduler-event-generator** program processes information from a local resource manager to generate LRM-independent events which GRAM can use to track job state changes. Typically, the **globus-scheduler-event-generator** is started at system boot time for all LRM adapters which have been installed. The only required parameter to **globus-scheduler-event-generator** is `-s LRM`, which indicates what LRM-specific module to load. A list of available modules can be found by using the **globus-scheduler-event-generator-admin -l** command.

Other options control how the **globus-scheduler-event-generator** program runs and where its output goes. These options are:

- `-t TIMESTAMP` Start processing events which start at *TIMESTAMP* in seconds since the UNIX epoch. If not present, the **globus-scheduler-event-generator** will process events from the time it was started, and not look for historical events.
- `-d DIRECTORY` Write the event log to files in *DIRECTORY*, instead of printing them to standard output. Within *DIRECTORY*, logs will be named by the time when they were created in *YYYYMMDD* format.
- `-b` Run the **globus-scheduler-event-generator** program in the background.
- `-p PIDFILE` Write the process-id of **globus-scheduler-event-generator** to *PIDFILE*.

## Files

`/var/lib/globus/globus-seg-LRM/YYYYMMDD` LRM-independent event log generated by **globus-scheduler-event-generator**

## See Also

globus-scheduler-event-generator-admin(8), globus-job-manager(8)



## Name

globusrun — Execute and manage jobs via GRAM

## Synopsis

```
globusrun [-help] [-usage] [-version] [-versions]
```

```
globusrun { -p | -parse }
{ -f RSL_FILENAME | -file RSL_FILENAME | RSL_SPECIFICATION }
```

```
globusrun [-n] [-no-interrupt]
{ -r RESOURCE_CONTACT | -resource RESOURCE_CONTACT }
{ -a | -authenticate-only }
```

```
globusrun [-n] [-no-interrupt]
{ -r RESOURCE_CONTACT | -resource RESOURCE_CONTACT }
{ -j | -jobmanager-version }
```

```
globusrun [-n] [-no-interrupt] { -k | -kill } {JOB_ID}
```

```
globusrun [-n] [-no-interrupt] [-full-proxy] [-D] { -y | -refresh-proxy } {JOB_ID}
```

```
globusrun { -status } {JOB_ID}
```

```
globusrun [-q] [-quiet] [-o] [-output-enable] [-s] [-server] [-w] [-write-allow] [-n] [-no-interrupt] [-b] [-batch] [-F]
[-fast-batch] [-full-proxy] [-D] [-d] [-dryrun]
{ -r RESOURCE_CONTACT | -resource RESOURCE_CONTACT }
{ -f RSL_FILENAME | -file RSL_FILENAME | RSL_SPECIFICATION }
```

## Description

The **globusrun** program for submits and manages jobs run on a local or remote job host. The jobs are controlled by the **globus-job-manager** program which interfaces with a local resource manager that schedules and executes the job.

The **globusrun** program can be run in a number of different modes chosen by command-line options.

When **-help**, **-usage**, **-version**, or **-versions** command-line options are used, **globusrun** will print out diagnostic information and then exit.

When the **-p** or **-parse** command-line option is present, **globusrun** will verify the syntax of the RSL specification and then terminate. If the syntax is valid, **globusrun** will print out the string "RSL Parsed Successfully. . ." and exit with a zero exit code; otherwise, it will print an error message and terminate with a non-zero exit code.

When the **-a** or **-authenticate-only** command-line option is present, **globusrun** will verify that the service named by *RESOURCE\_CONTACT* exists and the client's credentials are granted permission to access that service. If authentication is successful, **globusrun** will display the string "GRAM Authentication test successful" and exit with a zero exit code; otherwise it will print an explanation of the problem and will with a non-zero exit code.

When the **-j** or **-jobmanager-version** command-line option is present, **globusrun** will attempt to determine the software version that the service named by *RESOURCE\_CONTACT* is running. If successful, it will display both the Toolkit version and the Job Manager package version and exit with a zero exit code; otherwise, it will print an explanation of the problem and exit with a non-zero exit code.

When the `-k` or `-kill` command-line option is present, **globusrun** will attempt to terminate the job named by `JOB_ID`. If successful, **globusrun** will exit with zero; otherwise it will display an explanation of the problem and exit with a non-zero exit code.

When the `-y` or `-refresh-proxy` command-line option is present, **globusrun** will attempt to delegate a new X.509 proxy to the job manager which is managing the job named by `JOB_ID`. If successful, **globusrun** will exit with zero; otherwise it will display an explanation of the problem and exit with a non-zero exit code. This behavior can be modified by the `-full-proxy` or `-D` command-line options to enable full proxy delegation. The default is limited proxy delegation.

When the `-status` command-line option is present, **globusrun** will attempt to determine the current state of the job. If successful, the state will be printed to standard output and **globusrun** will exit with a zero exit code; otherwise, a description of the error will be displayed and it will exit with a non-zero exit code.

Otherwise, **globusrun** will submit the job to a GRAM service. By default, **globusrun** waits until the job has terminated or failed before exiting, displaying information about job state changes and at exit time, the job exit code if it is provided by the GRAM service.

The **globusrun** program can also function as a GASS file server to allow the **globus-job-manager** program to stage files to and from the machine on which **globusrun** is executed to the GRAM service node. This behavior is controlled by the `-s`, `-o`, and `-w` command-line options.

Jobs submitted by **globusrun** can be monitored interactively or detached. To have **globusrun** detach from the GRAM service after submitting the job, use the `-b` or `-F` command-line options.

## Options

The full set of options to **globusrun** consist of:

<code>-help</code>	Display a help message to standard error and exit.
<code>-usage</code>	Display a one-line usage summary to standard error and exit.
<code>-version</code>	Display the software version of <b>globusrun</b> to standard error and exit.
<code>-versions</code>	Display the software version of all modules used by <b>globusrun</b> (including DiRT information) to standard error and then exit.
<code>-p, -parse</code>	Do a parse check on the job specification and print diagnostics. If a parse error occurs, <b>globusrun</b> exits with a non-zero exit code.
<code>-f RSL_FILENAME, -file RSL_FILENAME</code>	Read job specification from the file named by <code>RSL_FILENAME</code> .
<code>-n, -no-interrupt</code>	Disable handling of the SIGINT signal, so that the interrupt character (typically <b>Control+C</b> ) causes <b>globusrun</b> to terminate without canceling the job.
<code>-r RESOURCE_CONTACT, -resource RESOURCE_CONTACT</code>	Submit the request to the resource specified by <code>RESOURCE_CONTACT</code> . A resource may be specified in the following ways: <ul style="list-style-type: none"> <li>• <code>HOST</code></li> <li>• <code>HOST:PORT</code></li> <li>• <code>HOST:PORT/SERVICE</code></li> </ul>

- *HOST/SERVICE*
- *HOST:/SERVICE*
- *HOST::SUBJECT*
- *HOST:PORT:SUBJECT*
- *HOST/SERVICE:SUBJECT*
- *HOST:/SERVICE:SUBJECT*
- *HOST:PORT/SERVICE:SUBJECT*

If any of *PORT*, *SERVICE*, or *SUBJECT* is omitted, the defaults of 2811, jobmanager, and host@HOST are used respectively.

-j, -jobmanager-version	Print the software version being run by the service running at <i>RESOURCE_CONTACT</i> .
-k <i>JOB_ID</i> , -kill <i>JOB_ID</i>	Kill the job named by <i>JOB_ID</i>
-D, -full-proxy	Delegate a full impersonation proxy to the service. By default, a limited proxy is delegated when needed.
-y, -refresh-proxy	Delegate a new proxy to the service processing <i>JOB_ID</i> .
-status	Display the current status of the job named by <i>JOB_ID</i> .
-q, -quiet	Do not display job state change or exit code information.
-o, -output-enable	Start a GASS server within the <b>globusrun</b> application that allows access to its standard output and standard error streams only. Also, augment the <i>RSL_SPECIFICATION</i> with a definition of the GLOBUSRUN_GASS_URL RSL substitution and add <i>stdout</i> and <i>stderr</i> clauses which redirect the output and error streams of the job to the output and error streams of the interactive <b>globusrun</b> command. If this is specified, then <b>globusrun</b> acts as though the -q were also specified.
-s, -server	Start a GASS server within the <b>globusrun</b> application that allows access to its standard output and standard error streams for writing and any file local the the <b>globusrun</b> invocation for reading. Also, augment the <i>RSL_SPECIFICATION</i> with a definition of the GLOBUSRUN_GASS_URL RSL substitution and add <i>stdout</i> and <i>stderr</i> clauses which redirect the output and error streams of the job to the output and error streams of the interactive <b>globusrun</b> command. If this is specified, then <b>globusrun</b> acts as though the -q were also specified.
-w, -write-allow	Start a GASS server within the <b>globusrun</b> application that allows access to its standard output and standard error streams for writing and any file local the the <b>globusrun</b> invocation for reading or writing. Also, augment the <i>RSL_SPECIFICATION</i> with a definition of the GLOBUSRUN_GASS_URL RSL substitution and add <i>stdout</i> and <i>stderr</i> clauses which redirect the output and error streams of the job to the output and error streams of the interactive <b>globusrun</b> command. If this is specified, then <b>globusrun</b> acts as though the -q were also specified.

<code>-b, -batch</code>	Terminate after submitting the job to the GRAM service. The <b>globusrun</b> program will exit after the job hits any of the following states: <code>PENDING</code> , <code>ACTIVE</code> , <code>FAILED</code> , or <code>DONE</code> . The GASS-related options can be used to stage input files, but standard output, standard error, and file staging after the job completes will not be processed.
<code>-F, -fast-batch</code>	Terminate after submitting the job to the GRAM service. The <b>globusrun</b> program will exit after it receives a reply from the service. The <code>JOB_ID</code> will be displayed to standard output before terminating so that the job can be checked with the <code>-status</code> command-line option or modified by the <code>-refresh-proxy</code> or <code>-kill</code> command-line options.
<code>-d, -dryrun</code>	Submit the job with the <code>dryrun</code> attribute set to true. When this is done, the job manager will prepare to start the job but start short of submitting it to the service. This can be used to detect problems with the <i>RSL_SPECIFICATION</i> .

## Environment

If the following variables affect the execution of **globusrun**

`X509_USER_PROXY` Path to proxy credential.

`X509_CERT_DIR` Path to trusted certificate directory.

## Bugs

The **globusrun** program assumes any failure to contact the job means the job has terminated. In fact, this may be due to the **globus-job-manager** program exiting after all jobs it is managing have reached the `DONE` or `FAILED` states. In order to reliably detect job termination, the `two_phase` RSL attribute should be used.

## See Also

`globus-job-submit(1)`, `globus-job-run(1)`, `globus-job-clean(1)`, `globus-job-get-output(1)`, `globus-job-cancel(1)`

# GSI-OpenSSH Commands

The `(1)`, `(1)`, and `(1)` commands provide the same interfaces as the standard OpenSSH `ssh`, `scp`, and `sftp` commands, respectively, with the added ability to perform X.509 *proxy credential* authentication and delegation.

## Table of Contents

<code>gsissh</code> .....	89
<code>gsiscp</code> .....	90
<code>gsisftp</code> .....	91

DRAFT

## Name

`gsissh` — Secure remote login

## Synopsis

`gsissh`

## Tool description

Use the *gsissh* command to securely login to a remote machine.

## Command syntax

`gsissh [-l login_name] hostname | user@hostname [command]`

DRAFT

## Name

*gsiscp* — Secure remote file copy

## Synopsis

*gsiscp*

## Tool description

Use the *gsiscp* command to securely copy files to or from a remote machine.

## Command syntax

*gsiscp* [-P port] [[user@]host1:]file1 [...] [[user@]host2:]destfile

DRAFT

## Name

`gsisftp` — Secure file transfer

## Synopsis

`gsisftp`

## Tool description

The *gsisftp* command provides an interactive interface for transferring files to and from remote machines.

## Command syntax

*gsisftp* [[user@]host[:dir[/]]]

DRAFT



# Simple CA Commands

## Table of Contents

grid-ca-create .....	93
grid-ca-package .....	95
grid-ca-sign .....	97

DRAFT

## Name

grid-ca-create — Create a CA to sign certificates for use on a grid

## Synopsis

```
grid-ca-create [-help] [-h] [-usage] [-version] [-versions]
```

```
grid-ca-create [-force] [-noint] [-dir DIRECTORY]
[-subject SUBJECT] [-email ADDRESS] [-days DAYS] [-pass PASSWORD]
[-nobuild] [-g] [-b]
[-openssl-help] [OPENSSL-OPTIONS]
```

## Description

The **grid-ca-create** program creates a self-signed CA certificate and related files needed to use the CA with other Globus tools. The **grid-ca-create** program prompts for information to use to generate the CA certificate, but the prompts may be avoided by using the command line options.

By default, the **grid-ca-create** program creates the self-signed CA certificate, installs it on the current machine in its trusted certificate directory, and creates a source tarball which can be used to generate an RPM package for the CA. If the RPM package is installed on a machine, users on that machine can create certificate requests for user, host, or service identity certificates to be signed by the CA certificate generated by running **grid-ca-create**.

If run as a privileged user, the **grid-ca-create** program creates the CA certificate and support files in `${localstatedir}/lib/globus/simple_ca` and the CA certificate and signing policy are installed in the `/etc/grid-security` directory. Otherwise, the files are created in the `${HOME}/.globus/simpleCA` directory.

The full set of command-line options to **grid-ca-create** follows. In addition to these, unknown options will be passed to the **openssl** command when creating the self-signed certificate.

<code>-help, -h, -usage</code>	Display the command-line options to <b>grid-ca-create</b> and exit.
<code>-version, -versions</code>	Display the version number of the <b>grid-ca-create</b> command. The second form includes more details.
<code>-force</code>	Overwrite existing CA in the destination directory if one exists
<code>-noint</code>	Run in non-interactive mode. This will choose defaults for parameters or those specified on the command line without prompting. This option also implies <code>-force</code> .
<code>-dir DIRECTORY</code>	Create the CA in <i>DIRECTORY</i> . The <i>DIRECTORY</i> must not exist prior to running <b>grid-ca-create</b> .
<code>-subject SUBJECT</code>	Use <i>SUBJECT</i> as the subject name of the self-signed CA to create. If this is not specified on the command-line, <b>grid-ca-create</b> will default to using the subject name <i>cn=Globus Simple CA, ou=\$HOSTNAME, ou=GlobusTest, o=Grid</i> .
<code>-email ADDRESS</code>	Use <i>ADDRESS</i> as the email address of the CA. The default instructions generated by <b>grid-ca-create</b> tell users to mail the certificate request to this address. If this is not specified on the command-line, <b>grid-ca-create</b> will default to the <code>\$LOGNAME@\$HOSTNAME</code>
<code>-days DAYS</code>	Set the default lifetime of the self-signed CA certificate to <i>DAYS</i> . If not set, the <b>grid-ca-create</b> program will default to 1825 days (5 years).

- `-pass PASSWORD`      Use the string *PASSWORD* to protect the CA's private key. This is useful for automating Simple CA, but may make it easier to compromise the CA if someone obtains a shell on the machine storing the CA's private key.
- `-nobuild`                Disable building a source tarball for distributing the CA's public information to other machines. The source tarball can be created later by using the **grid-ca-package** command.
- `-g`                        Create a binary GPT package containing the new CA's public information. The package will be created in the current working directory. This package can be deployed by with the **gpt-install** tool.
- `-b`                        Create a binary GPT package containing the new CA's public information that is backward-compatible with GPT 3.2. Packages created in this manner will work with Globus Toolkit 2.0.0-5.0.x.

## Examples

Create a simple CA in `$HOME/SimpleCA`

```
% grid-ca-create -noint -dir $HOME/SimpleCA
```

```
C e r t i f i c a t e     A u t h o r i t y     S e t u p
```

```
This script will setup a Certificate Authority for signing Globus
users certificates. It will also generate a simple CA package
that can be distributed to the users of the CA.
```

```
The CA information about the certificates it distributes will
be kept in:
```

```
/home/juser/SimpleCA
```

```
The unique subject name for this CA is:
```

```
cn=Globus Simple CA, ou=simpleCA-grid.example.org, ou=GlobusTest, o=Grid
```

```
Insufficient permissions to install CA into the trusted certificate
directory (tried ${sysconfdir}/grid-security/certificates and
${datadir}/certificates)
```

```
Creating RPM source tarball... done
```

```
globus_simple_ca_0146c503.tar.gz
```

## Environment Variables

The following environment variables affect the execution of **grid-ca-create**:

`GLOBUS_LOCATION`    Non-standard installation path of the Globus toolkit.

## See Also

`grid-cert-request(1)`, `grid-ca-sign(1)`, `grid-default-ca(1)`, `grid-ca-package(1)`

## Name

`grid-ca-package` — Prepare a CA certificate, configuration, and policy for distribution

## Synopsis

```
grid-ca-package [-help] [-h] [-usage] [-version] [-versions]
```

```
grid-ca-package [[-ca HASH] | [-cadir SIMPLECADIR]] [-g] [-b] [-r] [-d]
```

## Description

The **grid-ca-package** utility creates a tarball containing an RPM spec file and the files needed to use a CA with grid tools. It optionally will also create a GPT package for distributing a CA.

By default, the **grid-ca-package** utility displays a list of installed grid CA and prompts for which CA to package. It then creates a tarball containing the CA certificate, signing policy, CA configuration files, and an spec script to generate a binary RPM package containing the CA. If the CA hash is known prior to running **grid-ca-package**, it may provided as an argument to the `-ca` parameter to avoid prompting. **grid-ca-package** may also be used to package a SimpleCA directory, using the `-cadir` parameter.

In addition to generating a spec script and tarball, **grid-ca-package** creates a GPT package if either the `-g` or `-b` options are used on the command-line. These packages may be used to distribute a CA and configuration to systems which do not support RPM packages.

The **grid-ca-package** utility writes the package tarballs to the current working directory.

The full set of command-line options to **grid-ca-package** follows.

<code>-help, -h, -usage</code>	Display the command-line options to <b>grid-ca-package</b> and exit.
<code>-version, -versions</code>	Display the version number of the <b>grid-ca-package</b> command. The second form includes more details.
<code>-ca <i>CA</i></code>	Use the CA whose name matches the hash string <i>CA</i> . When invoked with this option, <b>grid-ca-package</b> runs non-interactively.
<code>-cadir <i>SIMPLECADIR</i></code>	Use the SimpleCA located in <i>SIMPLECADIR</i> When invoked with this option, <b>grid-ca-package</b> runs non-interactively.
<code>-g</code>	Create a GPT binary package in addition to the RPM script tarball. This package may be installed on other systems using the <b>gpt-install</b> program.
<code>-b</code>	Create a GPT binary package with GPT metadata located in the path expected by GPT 3.2 (used in Globus 2.0.0-5.0.x) instead of <code>\${datadir}/globus/packages</code> as used in Globus 5.2.x. This option overrides the <code>-g</code> command-line option.
<code>-r</code>	Create a binary RPM package for the CA. This option currently only works on RPM-based distributions.
<code>-d</code>	Create a binary Debian package for the CA. This option currently only works on Debian-based distributions.

## Examples

Package a Simple CA with hash 0146c503

```
% grid-ca-package -ca 0146c503  
Creating RPM source tarball... done  
  globus_simple_ca_0146c503.tar.gz
```

## Environment Variables

The following environment variables affect the execution of **grid-ca-package**:

**GLOBUS\_LOCATION** Non-standard installation path of the Globus toolkit.

## See Also

grid-cert-request(1), grid-ca-sign(1), grid-default-ca(1), grid-ca-create(1)

DRAFT

## Name

grid-ca-sign — Sign a certificate with a SimpleCA for use on a grid

## Synopsis

```
grid-ca-sign [-help] [-h] [-usage] [-version] [-versions]
```

```
grid-ca-sign -in REQUEST -out CERTIFICATE
[-force] [-dir DIRECTORY]
[-openssl-help] [OPENSSL-OPTIONS]
```

## Description

The **grid-ca-sign** program signs a certificate based on a request file with a CA certificate created by **grid-ca-create**. The new certificate is written to a file. If the CA has already signed a certificate with the same subject name as contained in the certificate request, it will refuse to sign the new request unless the `-force` option is provided on the command-line.

If run as a privileged user, **grid-ca-sign** uses the CA certificate and configuration located in `${localstatedir}/lib/globus/simple_ca` to sign the certificate. For a non-privileged user, **grid-ca-sign** uses the CA certificate and configuration located in `$HOME/.globus/simpleCA`. The **grid-ca-sign** program can use a different CA configuration and certificate by using the `-dir` option.

The full set of command-line options to **grid-ca-sign** follows. In addition to these, unknown options will be passed to the **openssl** command when creating the self-signed certificate.

<code>-help, -h, -usage</code>	Display the command-line options to <b>grid-ca-sign</b> and exit.
<code>-version, -versions</code>	Display the version number of the <b>grid-ca-sign</b> command. The second form includes details about the package containing <b>grid-ca-sign</b> .
<code>-in REQUEST</code>	Sign the request contained in the <i>REQUEST</i> file.
<code>-out CERTIFICATE</code>	Write the signed request to the <i>CERTIFICATE</i> file.
<code>-force</code>	Revoke any previously issued certificate with the same subject name as in the certificate request and issue a new certificate. Otherwise, <b>grid-ca-sign</b> will refuse to sign the request.
<code>-dir DIRECTORY</code>	Sign the certificate using the Simple CA certificate and configuration located in <i>DIRECTORY</i> instead of the default.
<code>-openssl-help</code>	Print the command-line options available for the <b>openssl ca</b> command.

## Examples

Sign a certificate request using the simple CA in `$HOME/SimpleCA`

```
% grid-ca-sign -in usercert_request.pem -out usercert.pem -dir $HOME/SimpleCA
```

To sign the request  
please enter the password for the CA key:

The new signed certificate is at: `/home/juser/.globus/simpleCA/newcerts/01.pem`

## Environment Variables

The following environment variables affect the execution of **grid-ca-sign**:

`GLOBUS_LOCATION` Non-standard installation path of the Globus toolkit.

## See Also

`grid-cert-request(1)`, `grid-ca-create(1)`, `grid-default-ca(1)`, `grid-ca-package(1)`

DRAFT

# Glossary

## C

**client** A process that sends commands and receives responses. Note that in GridFTP, the client may or may not take part in the actual movement of data.

## E

**extended block mode (MODE E)** MODE E is a critical GridFTP components because it allows for out of order reception of data. This in turn, means we can send the data down multiple paths and do not need to worry if one of the paths is slower than the others and the data arrives out of order. This enables parallelism and striping within GridFTP. In MODE E, a series of “blocks” are sent over the data channel. Each block consists of:

- an 8 bit flag field,
- a 64 bit field indicating the offset in the transfer,
- and a 64 bit field indicating the length of the payload,
- followed by length bytes of payload.

Note that since the offset and length are included in the block, out of order reception is possible, as long as the receiving side can handle it, either via something like a seek on a file, or via some application level buffering and ordering logic that will wait for the out of order blocks.

## P

**proxy credentials** The combination of a proxy certificate and its corresponding private key. GSI typically stores proxy credentials in `/tmp/x509up_u<uid>`, where `<uid>` is the user id of the proxy owner.

## S

**server** A process that receives commands and sends responses to those commands. Since it is a server or service, and it receives commands, it must be listening on a port somewhere to receive the commands. Both FTP and GridFTP have IANA registered ports. For FTP it is port 21, for GridFTP it is port 2811. This is normally handled via `inetd` or `xinetd` on Unix variants. However, it is also possible to implement a daemon that listens on the specified port. This is described more fully in in the Architecture section of the GridFTP Developer's Guide.

**stream mode (MODE S)** The only mode normally implemented for FTP is MODE S. This is simply sending each byte, one after another over the socket in order, with no application level framing of any kind. This is the default and is what a standard FTP server will use. This is also the default for GridFTP.



# T

## third party transfers

In the simplest terms, a third party transfer moves a file between two GridFTP servers.

The following is a more detailed, programmatic description.

In a third party transfer, there are three entities involved. The client, who will only orchestrate, but not actually take place in the data transfer, and two servers one of which will be sending data to the other. This scenario is common in Grid applications where you may wish to stage data from a data store somewhere to a supercomputer you have reserved. The commands are quite similar to the client/server transfer. However, now the client must establish two control channels, one to each server. He will then choose one to listen, and send it the PASV command. When it responds with the IP/port it is listening on, the client will send that IP/port as part of the PORT command to the other server. This will cause the second server to connect to the first server, rather than the client. To initiate the actual movement of the data, the client then sends the RETR filename command to the server that will read from disk and write to the network (the sending server) and will send the STOR filename command to the other server which will read from the network and write to the disk (the receiving server).

See Also [client/server transfer](#).