

GT 4.2.0 MyProxy: User's Guide

DRAFT

GT 4.2.0 MyProxy: User's Guide

DRAFT

Table of Contents

1. Introduction	1
2. Using MyProxy	2
1. Storing a credential in the MyProxy repository	2
2. Retrieving a credential from the MyProxy repository	2
I. Command-line tools	3
myproxy-init	4
myproxy-info	8
myproxy-logon	9
myproxy-store	11
myproxy-retrieve	15
myproxy-destroy	17
myproxy-change-pass-phrase	18
myproxy-admin-adduser	19
myproxy-admin-change-pass	21
myproxy-admin-query	22
myproxy-admin-load-credential	23
myproxy-server	27
3. Debugging	28
1. Debugging GSI authentication problems	28
4. Troubleshooting	29
1. Incorrect system clocks	29
2. Errors	30
Glossary	31

List of Tables

1. myproxy-init options	6
2. myproxy-info options	8
3. myproxy-logon options	10
4. myproxy-store options	13
5. myproxy-retrieve options	16
6. myproxy-destroy options	17
7. myproxy-change-pass-phrase options	18
8. myproxy-admin-adduser options	20
9. myproxy-admin-change-pass options	21
10. myproxy-admin-query options	22
11. myproxy-admin-load-credential options	25
12. myproxy-server options	27
4.1. MyProxy Errors	30

DRAFT

Chapter 1. Introduction

The MyProxy User's Guide provides general end user-oriented information. The major end-user issues are storing and retrieving credentials in the MyProxy repository.

DRAFT

Chapter 2. Using MyProxy

1. Storing a credential in the MyProxy repository

Rather than storing your X.509 credentials (certificate and *private key*) on each machine you use, you can store them in a MyProxy repository and retrieve a *proxy credential* from the MyProxy repository when needed.

To store a credential in the MyProxy repository, run the **myproxy-init** command on a computer where your Grid credentials are located. For example:

```
$ myproxy-init -a -s myproxy.ncsa.uiuc.edu
Your identity: /C=US/O=National Computational Science Alliance/CN=Jim Basney
Enter GRID pass phrase for this identity:
Creating proxy ..... Done
Your proxy is valid until Fri Sep 13 13:52:56 2002
Enter MyProxy Pass Phrase:
Verifying password - Enter MyProxy Pass Phrase:
A proxy valid for 168 hours (7.0 days) for user jbasney now exists on myproxy.ncsa
```

The **myproxy-init** command prompts first for the pass phrase of your private key (similar to **grid-proxy-init**) and then prompts twice for a new pass phrase to use to secure the credentials on the MyProxy server. By default, the credential is stored under your Unix username (jbasney in the example above) for 7 days and can be used to retrieve credentials with 12 hour lifetimes. [Command-line tools](#) below lists all the available options for the myproxy-init command.

2. Retrieving a credential from the MyProxy repository

Once you've stored a credential in the MyProxy repository, you can retrieve a proxy credential whenever you need one with the **myproxy-logon** command. For example:

```
$ myproxy-logon -s myproxy.ncsa.uiuc.edu
Enter MyProxy Pass Phrase:
A proxy has been received for user jbasney in /tmp/x509up_u500
```

The **myproxy-logon** command prompts for the pass phrase you set previously with **myproxy-init**, retrieves a proxy credential for you, and stores it in the correct default location for use with other Globus Toolkit programs. The [Command-line tools](#) lists all the available options for the **myproxy-logon** command.

Command-line tools

DRAFT

Name

myproxy-init -- Store a *proxy credential* for later retrieval

myproxy-init

Tool description

The **myproxy-init** command uploads a credential to a **myproxy-server** for later retrieval. In the default mode, the command first prompts for the user's Grid pass phrase (if needed), which is used to create a proxy credential. The command then prompts for a MyProxy pass phrase, which will be required to later retrieve the credential. The MyProxy pass phrase must be entered a second time for confirmation. A credential with a lifetime of one week (by default) is then delegated to the **myproxy-server** and stored with the given MyProxy pass phrase. Proxy credentials with a default lifetime of 12 hours can then be retrieved by **myproxy-logon** using the MyProxy passphrase. The default behavior can be overridden by options specified below.

The **myproxy-init** command can also upload a credential to a **myproxy-server** to support credential renewal. Renewal allows a trusted service (for example, a batch job scheduler) to obtain a new credential for a user before the existing credential it has for that user expires. The **-R** argument to **myproxy-init** configures the credential for renewal by the specified service. Renewal requires two authentications. The renewing service must authenticate with its own credentials, matching the distinguished name specified by the **-R** argument, and must also authenticate with an existing credential that matches the distinguished name of the stored credential to retrieve a new credential.

A credential may be used either for retrieval or renewal, but not both. If both are desired, upload a different credential for each use with a different name, using the **-k** option.

The hostname where the **myproxy-server** is running must be specified by either defining the **MYPROXY_SERVER** environment variable or the **-s** option.

By default, **myproxy-init** will create a proxy credential from the user's end-entity credentials at `~/globus/usercert.pem` and `~/globus/userkey.pem` to delegate to the **myproxy-server**. To specify an alternate location for the source certificate and key to delegate, use the **X509_USER_CERT** and **X509_USER_KEY** environment variables. To use a proxy credential as the source of the delegation, set both environment variables to the location of the proxy credential. To delegate a "legacy globus proxy", set the **GT_PROXY_MODE** environment variable to "old".

Command syntax

myproxy-init [options]

Command options

DRAFT

Table 1. myproxy-init options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>hostname</i> , --pshost <i>hostname</i>	Specifies the hostname of the myproxy-server. This option is required if the MYPROXY_SERVER environment variable is not defined. If specified, this option overrides the MYPROXY_SERVER environment variable.
-p <i>port</i> , --psport <i>port</i>	Specifies the TCP port number of the myproxy-server . Default: 7512.
-P, --pidfile <i>path</i>	Specifies a file to write the pid to.
-l, --username	Specifies the MyProxy account under which the credential should be stored. By default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-c <i>hours</i> , --cred_lifetime <i>hours</i>	Specifies the lifetime of the credential stored on the myproxy-server in hours. Specify 0 for the maximum possible lifetime, i.e., the lifetime of the original credential. Default: 1 week (168 hours).
-t <i>hours</i> , --proxy_lifetime <i>hours</i>	Specifies the maximum lifetime of credentials retrieved from the myproxy-server using the stored credential. Default: 12 hours.
-d, --dn_as_username	Use the <i>certificate subject</i> (DN) as the default username, instead of the LOGNAME environment variable.
-a, --allow_anonymous_retrievers	Allow credentials to be retrieved with just pass phrase authentication. By default, only entities with credentials that match the myproxy-server.config default retriever policy may retrieve credentials. This option allows entities without existing credentials to retrieve a credential using pass phrase authentication by including "anonymous" in the set of allowed retrievers. The myproxy-server.config server-wide policy must also allow "anonymous" clients for this option to have an effect.
-A, --allow_anonymous_renewers	Allow credentials to be renewed by any client. Any client with a valid credential with a subject name that matches the stored credential may retrieve a new credential from the MyProxy repository if this option is given. Since this effectively defeats the purpose of proxy credential lifetimes, it is not recommended. It is included only for the sake of completeness.
-r <i>dn</i> , --retrievable_by <i>dn</i>	Allow the specified entity to retrieve credentials. By default, the argument will be matched against the common name (CN) of the client (for example: "Jim Basney"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=Jim Basney") instead.
-R <i>dn</i> , --renewable_by <i>dn</i>	Allow the specified entity to renew credentials. By default, the argument will be matched against the common name (CN) of the client (for example: "condorg/modi4.ncsa.uiuc.edu"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=condorg/modi4.ncsa.uiuc.edu") instead. This option implies -n since passphrase authentication is not used for credential renewal.
-x, --regex_dn_match	Specifies that the DN used by options -r and -R will be matched as a regular expression.

-X, --match_cn_only	Specifies that the DN used by options -r and -R will be matched against the Common Name (CN) of the subject.
-k <i>name</i> , --credname <i>name</i>	Specifies the credential name.
-K <i>description</i>	blank
--creddesc <i>description</i>	Specifies credential description.
-S, --stdin_pass	by default, the command prompts for a passphrase and reads the passphrase from the active tty. When running the command non-interactively, there may be no associated tty. Specifying this option tells the command to read passphrases from standard input without prompts or confirmation.

DRAFT

Name

myproxy-info -- Display information about credentials

myproxy-info

Tool description

The **myproxy-info** command displays information about a user's credentials stored on a **myproxy-server**. The user must have a valid proxy credential as generated by **grid-proxy-init** or retrieved by **myproxy-logon** when running this command.

Command syntax

myproxy-info [options]

Command options

Table 2. myproxy-info options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>hostname</i> , --pshost <i>hostname</i>	Specifies the hostname of the myproxy-server. This option is required if the MYPROXY_SERVER environment variable is not defined. If specified, this option overrides the MYPROXY_SERVER environment variable.
-p <i>port</i> , --psport <i>port</i>	Specifies the TCP port number of the myproxy-server . Default: 7512.
-l <i>name</i> , --username <i>name</i>	Specifies the MyProxy account to query. By default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-d, --dn_as_username	Use the certificate subject (DN) as the default username, instead of the LOGNAME environment variable.

Name

myproxy-logon -- Retrieve a credential

myproxy-logon

Tool description

The **myproxy-logon** command retrieves a credential from the **myproxy-server** that was previously stored using **myproxy-init**. In the default mode, the command prompts for the MyProxy pass phrase associated with the credential to be retrieved and stores the retrieved credential in the standard location (*/tmp/x509up_u<uid>*).

If the repository contains an end-entity certificate, this command will retrieve an RFC 3820 compliant proxy (also known as "proxy draft compliant impersonation proxy") by default. Set the the GT_PROXY_MODE environment variable to "old" to retrieve a "legacy globus proxy" instead. If the repository contains a *proxy certificate*, the retrieved proxy will always be of the same type as the stored proxy.

The **myproxy-logon** is also available under the name **myproxy-get-delegation** for backward compatibility.

Command syntax

myproxy-logon [options]

Command options

Table 3. myproxy-logon options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>hostname</i> , --pshost <i>hostname</i>	Specifies the hostname of the myproxy-server. This option is required if the MYPROXY_SERVER environment variable is not defined. If specified, this option overrides the MYPROXY_SERVER environment variable.
-p <i>port</i> , --psport <i>port</i>	Specifies the TCP port number of the myproxy-server . Default: 7512.
-l, --username	Specifies the MyProxy account under which the credential to retrieve is stored. By default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-d, --dn_as_username	Use the certificate subject (DN) as the default username, instead of the LOGNAME environment variable. When used with the -a option, the certificate subject of the authorization credential is used. Otherwise, the certificate subject of the default credential is used.
-t <i>hours</i> , --proxy_lifetime <i>hours</i>	Specifies the lifetime of credentials retrieved from the myproxy-server using the stored credential. The resulting lifetime is the shorter of the requested lifetime and the lifetime specified when the credential was stored using myproxy-init . Default: 12 hours.
-o <i>file</i> , --out <i>file</i>	Specifies where the retrieved proxy credential should be stored. If this option is not specified, the proxy credential will be stored in the default location (/tmp/x509up_u<uid>).
-a <i>file</i> , --authorization <i>file</i>	Specifies a credential to be used for authorizing the request instead of a passphrase. When renewing a credential, use this option to specify the existing, valid credential that you want to renew. Renewing a credential generally requires two certificate-based authentications. The client authenticates with its identity, using the credential in the standard location or specified by X509_USER_PROXY or X509_USER_CERT and X509_USER_KEY in addition to authenticating with the existing credential, in the location specified by this option, that it wants to renew.
-k <i>name</i> , --credname <i>name</i>	Specifies the name of the credential that is to be retrieved or renewed.
-S, --stdin_pass	By default, the command prompts for a passphrase and reads the passphrase from the active tty. When running the command non-interactively, there may be no associated tty. Specifying this option tells the command to read passphrases from standard input without prompts or confirmation.

Name

myproxy-store -- Store end-entity credential for later retrieval

myproxy-store

Tool description

The **myproxy-store** command uploads a credential to a **myproxy-server(8)** for later retrieval. Unlike **myproxy-init(1)**, this command transfers the private key over the network (over a private channel). In the default mode, the command will take the credentials found in `~/.globus/usercert.pem` and `~/.globus/userkey.pem` and store them in the **myproxy-server(8)** repository. Proxy credentials with a default lifetime of 12 hours can then be retrieved by **myproxy-logon(1)** using the credential passphrase. The default behavior can be overridden by options specified below.

The hostname where the **myproxy-server(8)** is running must be specified by either defining the `MYPROXY_SERVER` environment variable or the `-s` option.

Command syntax

myproxy-store [options]

DRAFT

Command options

DRAFT

Table 4. myproxy-store options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>hostname</i> , --pshost <i>hostname</i>	Specifies the hostname of the myproxy-server. This option is required if the MYPROXY_SERVER environment variable is not defined. If specified, this option overrides the MYPROXY_SERVER environment variable.
-p <i>port</i> , --psport <i>port</i>	Specifies the TCP port number of the myproxy-server(8) . Default: 7512.
-l, --username	Specifies the MyProxy account under which the credential should be stored. by default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-c <i>filename</i> , --certfile <i>filename</i>	Specifies the filename of the source certificate. This is a required parameter.
-y <i>filename</i> , --keyfile <i>filename</i>	Specifies the filename of the source private key. This is a required parameter.
-t <i>hours</i> , --proxy_lifetime <i>hours</i>	Specifies the maximum lifetime of credentials retrieved from the myproxy-server(8) using the stored credential. Default: 12 hours
-d, --dn_as_username	Use the certificate subject (DN) as the default username, instead of the LOGNAME environment variable.
-a, --allow_anonymous_retrievers	Allow credentials to be retrieved with just pass phrase authentication. by default, only entities with credentials that match the myproxy-server.config(5) default retriever policy may retrieve credentials. This option allows entities without existing credentials to retrieve a credential using pass phrase authentication by including "anonymous" in the set of allowed retrievers. The myproxy-server.config(5) server-wide policy must also allow "anonymous" clients for this option to have an effect.
-A, --allow_anonymous_renewers	Allow credentials to be renewed by any client. Any client with a valid credential with a subject name that matches the stored credential may retrieve a new credential from the MyProxy repository if this option is given. Since this effectively defeats the purpose of proxy credential lifetimes, it is not recommended. It is included only for sake of completeness.
-r <i>dn</i> , --retrievable_by <i>dn</i>	Allow the specified entity to retrieve credentials. by default, the argument will be matched against the common name (CN) of the client (for example: "Jim Basney"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=Jim Basney") instead.
-E <i>dn</i> , --retrieve_key <i>dn</i>	Allow the specified entity to retrieve end-entity credentials. by default, the argument will be matched against the common name (CN) of the client (for example: "Jim Basney"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=Jim Basney") instead.

-R <i>dn</i> , --renewable_by <i>dn</i>	Allow the specified entity to renew credentials. by default, the argument will be matched against the common name (CN) of the client (for example: "condorg/modi4.ncsa.uiuc.edu"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=condorg/modi4.ncsa.uiuc.edu") instead. This option implies -n since passphrase authentication is not used for credential renewal.
-x, --regex_dn_match	Specifies that the DN used by options -r and -R will be matched as a regular expression.
-X, --match_cn_only	Specifies that the DN used by options -r and -R will be matched against the Common Name (CN) of the subject.
-k <i>name</i> , --credname <i>name</i>	Specifies the credential name.
-K <i>description</i> , --creddesc <i>description</i>	Specifies credential description.

Name

myproxy-retrieve -- Retrieve an end-entity credential

myproxy-retrieve

Tool description

The **myproxy-retrieve** command retrieves a credential directly from the **myproxy-server(8)** that was previously stored using **myproxy-init(1)** or **myproxy-store(1)**. Unlike **myproxy-logon(1)**, this command transfers the *private key* in the repository over the network (over a private channel). To obtain a proxy credential, we recommend using **myproxy-logon(1)** instead.

In the default mode, the command prompts for the pass phrase associated with the credential to be retrieved and stores the retrieved credential in the standard location (`~/.globus/usercert.pem` and `~/.globus/userkey.pem`). You could then run **grid-proxy-init** to create a proxy credential from the retrieved credentials.

Command syntax

myproxy-retrieve [options]

Command options

Table 5. myproxy-retrieve options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>hostname</i> , --pshost <i>hostname</i>	Specifies the hostname of the myproxy-server. This option is required if the MYPROXY_SERVER environment variable is not defined. If specified, this option overrides the MYPROXY_SERVER environment variable.
-p <i>port</i> , --psport <i>port</i>	Specifies the TCP port number of the myproxy-server(8) . Default: 7512.
-l, --username	Specifies the MyProxy account under which the credential to retrieve is stored. by default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-d, --dn_as_username	Use the certificate subject (DN) as the default username, instead of the LOGNAME environment variable. When used with the -a option, the certificate subject of the authorization credential is used. Otherwise, the certificate subject of the default credential is used.
-t <i>hours</i> , --proxy_lifetime <i>hours</i>	Specifies the lifetime of credentials retrieved from the myproxy-server(8) using the stored credential. The resulting lifetime is the shorter of the requested lifetime and the lifetime specified when the credential was stored using myproxy-init(1) . Default: 12 hours.
-c <i>filename</i> , --certfile <i>filename</i>	Specifies the filename of where the certificate will be stored.
-y <i>filename</i> , --keyfile <i>filename</i>	Specifies the filename of where the private key will be stored.
-a <i>file</i> , --authorization <i>file</i>	Specifies a credential to be used for authorizing the request instead of a passphrase. When renewing a credential, use this option to specify the existing, valid credential that you want to renew. Renewing a credential generally requires two certificate-based authentications. The client authenticates with its identity, using the credential in the standard location or specified by X509_USER_PROXY or X509_USER_CERT and X509_USER_KEY in addition to authenticating with the existing credential, in the location specified by this option, that it wants to renew.
-k <i>name</i> , --credname <i>name</i>	Specifies the name of the credential that is to be retrieved or renewed.
-S, --stdin_pass	By default, the command prompts for a passphrase and reads the passphrase from the active tty. When running the command non- interactively, there may be no associated tty. Specifying this option tells the command to read passphrases from standard input without prompts or confirmation.

Name

myproxy-destroy -- Remove a credential from the repository

myproxy-destroy

Tool description

The **myproxy-destroy** command removes a credential from the **myproxy-server** that was previously stored using **myproxy-init**. The user must have a valid proxy credential as generated by **grid-proxy-init** or retrieved by **myproxy-logout** when running this command.

Command syntax

myproxy-destroy [options]

Command options

Table 6. myproxy-destroy options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>hostname</i> , --pshost <i>hostname</i>	Specifies the hostname of the myproxy-server. This option is required if the MYPROXY_SERVER environment variable is not defined. If specified, this option overrides the MYPROXY_SERVER environment variable.
-p <i>port</i> , --psport <i>port</i>	Specifies the TCP port number of the myproxy-server . Default: 7512.
-l, --username	Specifies the MyProxy account under which the credential to destroy is stored. By default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-d, --dn_as_username	Use the certificate subject (DN) as the default username, instead of the LOGNAME environment variable.
-k <i>name</i> , --credname <i>name</i>	Specifies name of the credential to be destroyed.

Name

myproxy-change-pass-phrase -- Change a credential's passphrase

myproxy-change-pass-phrase

Tool description

The **myproxy-change-pass-phrase** command changes the passphrase under which a credential is protected in the MyProxy repository. The command first prompts for the current passphrase for the credential, then prompts twice for the new passphrase. Only the credential owner can change a credential's passphrase. The user must have a valid proxy credential as generated by **grid-proxy-init** or retrieved by **myproxy-logon** when running this command.

Command syntax

myproxy-change-pass-phrase [options]

Command options

Table 7. myproxy-change-pass-phrase options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>hostname</i> , --pshost <i>hostname</i>	Specifies the hostname of the myproxy-server. This option is required if the MYPROXY_SERVER environment variable is not defined. If specified, this option overrides the MYPROXY_SERVER environment variable.
-p <i>port</i> , --psport <i>port</i>	Specifies the TCP port number of the myproxy-server . Default: 7512.
-l, --username	Specifies the MyProxy account under which the credential should be stored. by default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-d, --dn_as_username	Use the certificate subject (DN) as the default username, instead of the LOGNAME environment variable.
-k <i>name</i> , --credname <i>name</i>	Specifies the credential name.
-S, --stdin_pass	by default, the command prompts for a passphrase and reads the passphrase from the active tty. When running the command noninteractively, there may be no associated tty. Specifying this option tells the command to read passphrases from standard input without prompts or confirmation.

Name

myproxy-admin-adduser -- Add a new *user credential*

myproxy-admin-adduser

Tool description

The **myproxy-admin-adduser** command creates a new credential for a user and loads it into the MyProxy repository. It is a **perl** script that runs **grid-cert-request** (a standard Globus Toolkit program) and **grid-ca-sign** (from the Globus Simple CA package) to create the credential and then runs **myproxy-admin-load-credential** to load the credential into the MyProxy repository. The command prompts for the common name to be included in the new certificate (if the **-c** argument is not specified), the Globus Simple CA key password for signing the certificate, the MyProxy username (if the **-l** or **-d** arguments are not specified), and the MyProxy passphrase for the credential. Most of the command-line options for this command are passed directly to the **myproxy-admin-load-credential** command. The Globus Simple CA must be configured before using this command.

Command syntax

myproxy-admin-adduser [options]

DRAFT

Command options

Table 8. myproxy-admin-adduser options

-h	Displays command usage text and exits.
-u	Displays command usage text and exits.
-c <i>cn</i>	Specifies the Common Name for the new credential (for example: "Jim Basney").
-s <i>dir</i>	Specifies the location of the credential storage directory. The directory must be accessible only by the user running the myproxy-server process for security reasons. Default: /var/myproxy or \$GLOBUS_LOCATION/var/myproxy.
-l <i>username</i>	Specifies the MyProxy account under which the credential should be stored.
-t <i>hours</i>	Specifies the maximum lifetime of credentials retrieved from the myproxy-server using the stored credential. Default: 12 hours.
-n	Disables passphrase authentication for the stored credential. If specified, the command will not prompt for a passphrase, the credential will not be encrypted by a passphrase in the repository, and the credential will not be retrievable using passphrase authentication with myproxy-logon . This option is used for storing renewable credentials and is implied by -R .
-d	Use the certificate subject (DN) as the username.
-a	Allow credentials to be retrieved with just pass phrase authentication. by default, only entities with credentials that match the myproxy-server.config default retriever policy may retrieve credentials. This option allows entities without existing credentials to retrieve a credential using pass phrase authentication by including "anonymous" in the set of allowed retrievers. The myproxy-server.config server-wide policy must also allow "anonymous" clients for this option to have an effect.
-A	Allow credentials to be renewed by any client. Any client with a valid credential with a subject name that matches the stored credential may retrieve a new credential from the MyProxy repository if this option is given. Since this effectively defeats the purpose of proxy credential lifetimes, it is not recommended. It is included only for sake of completeness.
-r <i>dn</i>	Allow the specified entity to retrieve credentials. By default, the argument will be matched against the common name (CN) of the client (for example: "Jim Basney"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=Jim Basney") instead.
-R <i>dn</i>	Allow the specified entity to renew credentials. By default, the argument will be matched against the common name (CN) of the client (for example: "condorg/modi4.ncsa.uiuc.edu"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=condorg/modi4.ncsa.uiuc.edu") instead. This option implies -n since passphrase authentication is not used for credential renewal.
-x	Specifies that the DN used by options -r and -R will be matched as a regular expression.
-X	Specifies that the DN used by options -r and -R will be matched against the Common Name (CN) of the subject.
-k <i>name</i>	Specifies the credential name.
-K <i>description</i>	Specifies credential description.

Name

myproxy-admin-change-pass -- Change credential passphrase

myproxy-admin-change-pass

Tool description

The **myproxy-admin-change-pass** command changes the passphrase used to encrypt a credential in the MyProxy repository. The command first prompts for the current passphrase for the credential, then prompts twice for the new passphrase. If an empty passphrase is given, the credential will not be encrypted. It accesses the repository directly and must be run on the machine where the **myproxy-server** is installed from the account that owns the repository.

Command syntax

myproxy-admin-change-pass [options]

Command options

Table 9. myproxy-admin-change-pass options

-h	Displays command usage text and exits.
-u	Displays command usage text and exits.
-s <i>dir</i>	Specifies the location of the credential storage directory. The directory must be accessible only by the user running the myproxy-server process for security reasons. Default: /var/myproxy or \$GLOBUS_LOCATION/var/myproxy.
-l <i>username</i>	Specifies the MyProxy account under which the credential should be stored.
-k <i>name</i>	Specifies the credential name.
-S, --stdin_pass	by default, the command prompts for a passphrase and reads the passphrase from the active tty. When running the command non-interactively, there may be no associated tty. Specifying this option tells the command to read passphrases from standard input without prompts or confirmation.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.

Name

myproxy-admin-query -- Query repository contents

myproxy-admin-query

Tool description

The **myproxy-admin-query** command displays information about the credentials stored in the MyProxy repository. It can also be used to remove credentials from the repository. It accesses the repository directly and must be run on the machine where the **myproxy-server** is installed from the account that owns the repository.

Command syntax

myproxy-admin-query [options]

Command options

Table 10. myproxy-admin-query options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-l <i>name</i> , --username <i>name</i>	Returns information on credentials for a single username. By default, the command returns information on all credentials for all usernames.
-k <i>name</i> , --credname <i>name</i>	Returns information on the credentials with the specified name.
-e <i>hours</i> , --expiring_in <i>hours</i>	Returns information on credentials with remaining lifetime less than the specified number of hours. For example, -e 0 will return all expired credentials.
-t <i>hours</i> , --time_left <i>hours</i>	Returns information on credentials with remaining lifetime greater than the specified number of hours.
-s <i>dir</i> , --storage <i>dir</i>	Specifies the location of the credential storage directory. The directory must be accessible only by the user running the myproxy-server process for security reasons. Default: /var/myproxy or \$GLOBUS_LOCA-TION/var/myproxy.
-r, --remove	Remove the credentials matching the query from the repository. For example, <i>myproxy-admin-query -e 0 -r</i> will remove all expired credentials from the repository.
-L ' <i>msg</i> ', --lock ' <i>msg</i> '	Places the credentials matching the query under an administrative lock and specifies a message to be returned on access attempts. Be sure to put the message in quotes so it is captured as one argument to the command.
-U, --unlock	Removes any administrative locks for the credentials matching the query.

Name

`myproxy-admin-load-credential --` Directly load repository

`myproxy-admin-load-credential`

Tool description

The **myproxy-admin-load-credential** command stores a credential directly in the local MyProxy repository. It must be run from the account that owns the repository. Many of the options are similar to **myproxy-init**. However, unlike **myproxy-init**, **myproxy-admin-load-credential** does not create a proxy from the source credential but instead directly loads a copy of the source credential into the repository. The pass phrase of the source credential is unchanged. Use **myproxy-admin-change-pass** to change the pass phrase after the credential is stored if desired. Proxy credentials with a default lifetime of 12 hours can then be retrieved by **myproxy-logon** using the MyProxy passphrase. The command's behavior is controlled by the following options.

Command syntax

`myproxy-admin-load-credential [options]`

DRAFT

Command options

DRAFT

Table 11. myproxy-admin-load-credential options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-s <i>dir</i> , --storage <i>dir</i>	Specifies the location of the credential storage directory. The directory must be accessible only by the user running the myproxy-server process for security reasons. Default: /var/myproxy or \$GLOBUS_LOCATION/var/myproxy
-c <i>filename</i> , --certfile <i>filename</i>	Specifies the filename of the source certificate. This is a required parameter.
-y <i>filename</i> , --keyfile <i>filename</i>	Specifies the filename of the source private key. This is a required parameter.
-l <i>username</i> , --username <i>user-name</i>	Specifies the MyProxy account under which the credential should be stored. by default, the command uses the value of the LOGNAME environment variable. Use this option to specify a different account username on the MyProxy server. The MyProxy username need not correspond to a real Unix username.
-t <i>hours</i> , --proxy_lifetime <i>hours</i>	Specifies the maximum lifetime of credentials retrieved from the myproxy-server using the stored credential. Default: 12 hours.
-d, --dn_as_username	Use the certificate subject (DN) as the username.
-a, --allow_anonymous_retrievers	Allow credentials to be retrieved with just pass phrase authentication. by default, only entities with credentials that match the myproxy-server.config default retriever policy may retrieve credentials. This option allows entities without existing credentials to retrieve a credential using pass phrase authentication by including "anonymous" in the set of allowed retrievers. The myproxy-server.config server-wide policy must also allow "anonymous" clients for this option to have an effect.
-A, --allow_anonymous_renewers	Allow credentials to be renewed by any client. Any client with a valid credential with a subject name that matches the stored credential may retrieve a new credential from the MyProxy repository if this option is given. Since this effectively defeats the purpose of proxy credential lifetimes, it is not recommended. It is included only for sake of completeness.
-r <i>dn</i> , --retrievable_by <i>dn</i>	Allow the specified entity to retrieve credentials. By default, the argument will be matched against the common name (CN) of the client (for example: "Jim Basney"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=Jim Basney") instead.
-R <i>dn</i> , --renewable_by <i>dn</i>	Allow the specified entity to renew credentials. By default, the argument will be matched against the common name (CN) of the client (for example: "condorg/modi4.ncsa.uiuc.edu"). Specify -x before this option to match against the full distinguished name (DN) (for example: "/C=US/O=National Computational Science Alliance/CN=condorg/modi4.ncsa.uiuc.edu") instead.
-x, --regex_dn_match	Specifies that the DN used by options -r and -R will be matched as a regular expression.
-X, --match_cn_only	Specifies that the DN used by options -r and -R will be matched against the Common Name (CN) of the subject.
-k <i>name</i> , --credname <i>name</i>	Specifies the credential name.

<i>-K description, --creddesc de- scription</i>	Specifies credential description.
---	-----------------------------------

DRAFT

Name

myproxy-server -- Store credentials in an online repository

myproxy-server

Tool description

The **myproxy-server** is a server that runs on a trusted, secure host and manages a database of security credentials for use from remote sites. The **myproxy-init** program stores credentials with associated policies that specify credential lifetimes and who is authorized to retrieve credentials. The **myproxy-server.config** file sets server-wide policies that are used in conjunction with the policies set by **myproxy-init** to control who is authorized to store and retrieve credentials.

Command syntax

myproxy-server [options]

Command options

Table 12. myproxy-server options

-h, --help	Displays command usage text and exits.
-u, --usage	Displays command usage text and exits.
-v, --verbose	Enables verbose debugging output to the terminal.
-V, --version	Displays version information and exits.
-d, --debug	Run the server in debug mode. In this mode, the server will run in the foreground, will accept one connection, write log messages to the terminal while processing the incoming request, and exit after completing one request.
-p <i>port</i> , --port <i>port</i>	Specifies the TCP port number that the myproxy-server should listen on. Default: 7512.
-c <i>file</i> , --config <i>file</i>	Specifies the location of the myproxy-server configuration file. Default: /etc/myproxy-server.config or \$GLOBUS_LOCATION/etc/myproxy-server.config.
-s <i>dir</i> , --storage <i>dir</i>	Specifies the location of the credential storage directory. The directory must be accessible only by the user running the myproxy-server process for security reasons. Default: /var/myproxy or \$GLOBUS_LOCATION/var/myproxy.

Chapter 3. Debugging

In addition to the following, there is more debugging information in [Chapter 4, Testing](#) and [Chapter 6, Debugging](#) in the MyProxy Admin Guide.

1. Debugging GSI authentication problems

To debug GSI authentication problems, run

```
grid-proxy-init -debug -verify
```

from the terminal where you run the MyProxy clients, and run

```
grid-proxy-init -debug -verify -cert /etc/grid-security/hostcert.pem -key /etc/grid-security/hostkey.pem
```

as root on the myproxy-server machine (assuming you run the myproxy-server as root).

DRAFT

Chapter 4. Troubleshooting

For a list of common errors in GT, see [Error Codes](#).

1. Incorrect system clocks

The most common cause of MyProxy authentication problems is incorrect system clocks. GSI authentication is very sensitive to clock skew. Make sure your system clock is accurate (for example, by running [NTP](#)¹) and your timezone is set correctly.

¹ <http://www.ntp.org/>

2. Errors

Table 4.1. MyProxy Errors

Error Code	Definition	Possible Solutions
MyProxy server name does not match expected name	<p>This error appears as a mutual authentication failure or a server authentication failure, and the error message should list two names: the expected name of the MyProxy server and the actual authenticated name.</p> <p>By default, the MyProxy clients expect the MyProxy server to be running with a host certificate that matches the target hostname. This error can occur when running the MyProxy server under a non-host certificate or if the server is running on a machine with multiple hostnames.</p> <p>The MyProxy clients authenticate the identity of the MyProxy server to avoid sending passphrases and credentials to rogue servers.</p> <p>If the expected name contains an IP address, your system is unable to do a reverse lookup on that address to get the canonical hostname of the server, indicating either a problem with that machine's DNS record or a problem with the resolver on your system.</p>	<p>If the server name shown in the error message is acceptable, set the <code>MYPROXY_SERVER_DN</code> environment variable to that name to resolve the problem.</p>
Error in <code>bind()</code> : Address already in use	<p>This error indicates that the <code>myproxy-server</code> port (default: 7512) is in use by another process, probably another <code>myproxy-server</code> instance. You cannot run multiple instances of the <code>myproxy-server</code> on the same network port.</p>	<p>If you want to run multiple instances of the <code>myproxy-server</code> on a machine, you can specify different ports with the <code>-p</code> option, and then give the same <code>-p</code> option to the MyProxy commands to tell them to use the <code>myproxy-server</code> on that port.</p>
grid-proxy-init failed	<p>This error indicates that the <code>grid-proxy-init</code> command failed when <code>myproxy-init</code> attempted to run it, which implies a problem with the underlying Globus installation.</p>	<p>Run <code>grid-proxy-init -debug -verify</code> for more information.</p>
User not authorized	<p>An error from the <code>myproxy-server</code> saying you are "not authorized" to complete an operation typically indicates that the <code>myproxy-server.config</code> file settings are restricting your access to the <code>myproxy-server</code>. It is possible that the <code>myproxy-server</code> is running with the default <code>myproxy-server.config</code> file, which does not authorize any operations.</p>	<p>See Configuring for more information.</p>

Glossary

C

certificate subject An identifier for the certificate owner, e.g. `"/DC=org/DC=doegrids/OU=People/CN=John Doe 123456"`. The subject is part of the information the CA binds to a public key when creating a certificate.

P

private key The private part of a key pair. Depending on the type of certificate the key corresponds to it may typically be found in `$HOME/.globus/userkey.pem` (for user certificates), `/etc/grid-security/hostkey.pem` (for host certificates) or `/etc/grid-security/<service>/<service>key.pem` (for service certificates).

For more information on possible private key locations see [this](#).

proxy certificate A short lived certificate issued using a EEC. A proxy certificate typically has the same effective subject as the EEC that issued it and can thus be used in its place. GSI uses proxy certificates for single sign on and delegation of rights to other entities.

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

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.

U

user credentials The combination of a user certificate and its corresponding private key.