
MyProxyClient Documentation

Release 1.4.0

P J Kershaw

February 13, 2015

CONTENTS

1	Examples	3
2	Releases	5
3	Tests	7
3.1	MyProxy Client Module	7
4	Indices and tables	15
	Index	17

This a pure* Python implementation of a client to the MyProxy Credential Management Server (<http://grid.ncsa.uiuc.edu/myproxy/>). It provides both a Python API and a command line interface.

- i.e. MyProxy C client libraries are not required for this package.

It uses pyOpenSSL to make an SSL connection to the server following the messaging interface as outlined in: <http://grid.ncsa.uiuc.edu/myproxy/protocol/>

The code is based on an original program `myproxy_logon` by Tom Uram of ANL.

EXAMPLES

These show how to retrieve a certificate bootstrapping trust in remote service.

API:

```
>>> from myproxy.client import MyProxyClient
>>> myproxy_clnt = MyProxyClient(hostname="myproxy.somewhere.ac.uk")
>>> cert, private_key = myproxy_clnt.logon(username, password, bootstrap=True)
```

Command line interface:

```
$ myproxycient logon -s myproxy.somewhere.ac.uk -l <username> -o creds.pem -b
```


RELEASES

1.4.3

- Fix for SSL to use TLS instead of SSLv3 to address POODLE vulnerability
- Fix for SSL verification for PyOpenSSL version 0.14 - v1.3.1 was broken because it passed the call back method to OpenSSL using verification classes' `__call__` method.

Tested on CentOS 6.4.

1.3.1

- Fix to `MyProxyClient.writeProxyFile` and `MyProxyClient.readProxyFile` to correctly pick-up overridden file setting. Thanks to Nicolas Carenton, IPSL.

Unit test module with test files is in `test/`. See the README in that directory.

Documentation

Sphinx generated documentation is available in `documentation/`. Run the `Makefile` to regenerate if required.

Thanks

- to OMII-UK for funding development of NDG Security (2007-2008)
- Tom Uram who wrote the `myproxy_logon` program on which this package is based.

Contents:

3.1 MyProxy Client Module

class `myproxy.client.MyProxyClient` (*cfgFilePath=None, **prop*)

Bases: `object`

MyProxy client interface

Based on protocol definitions in:

<http://grid.ncsa.uiuc.edu/myproxy/protocol/>

Variables

- **SSL_METHOD** – encryption method used for connecting to MyProxy server - set to TLS version 1
- **MYPROXY_SERVER_ENVVARIABLE** – server environment variable name
- **MYPROXY_SERVER_PORT_ENVVARIABLE** – port environment variable name
- **MYPROXY_SERVER_DN_ENVVARIABLE** – server certificate Distinguished Name environment variable name
- **GLOBUS_LOCATION_ENVVARIABLE** – ‘GLOBUS_LOCATION’ environment variable name
- **GET_CMD** – get command string
- **INFO_CMD** – info command string
- **DESTROY_CMD** – destroy command string
- **CHANGE_PASSPHRASE_CMD** – command string to change cred pass-phrase
- **STORE_CMD** – store command string

- **GET_TRUST_ROOTS_CMD** – get trust roots command string
- **TRUSTED_CERTS_FIELDNAME** – field name in get trust roots response for trusted certificate file names
- **TRUSTED_CERTS_FILEDATA_FIELDNAME_PREFIX** – field name prefix in get trust roots response for trusted certificate file contents
- **HOSTCERT_SUBDIRPATH** – sub-directory path host certificate (as tuple)
- **HOSTKEY_SUBDIRPATH** – sub-directory path to host key (as tuple)
- **PRIKEY_NBITS** – default number of bits for private key generated
- **MESSAGE_DIGEST_TYPE** – message digest type is MD5
- **SERVER_RESP_BLK_SIZE** – block size for retrievals from server
- **MAX_RECV_TRIES** – maximum number of retrievals of size SERVER_RESP_BLK_SIZE before this client gives up
- **DEF_PROXY_FILEPATH** – default location for proxy file to be written to
- **PROXY_FILE_PERMISSIONS** – file permissions returned proxy file is created with
- **PROPERTY_DEFAULTS** – sets permissible element names for MyProxy config file
- **ROOT_USERNAME** – root username - used to determine output directory for trust roots
- **ROOT_TRUSTROOT_DIR** – default trust root directory if running as root user
- **USER_TRUSTROOT_DIR** – default trust root directory for users other than root
- **X509_CERT_DIR_ENVVARNAME** – environment variable name ‘X509_CERT_DIR’, which if set points to the location of the trust roots
- **X509_USER_PROXY_ENVVARNAME** – environment variable name ‘X509_USER_PROXY’ if set points to the output location of the output EEC / Proxy certificate. Not currently used by this class, included for reference only

caCertDir

trust roots directory containing PEM encoded CA certificates to validate MyProxy server certificate

changePassphrase (*username, passphrase, newPassphrase, sslCertFile=None, sslKeyFile=None, sslKeyFilePassphrase=None*)

change pass-phrase protecting the credentials for a given username

Raises

- **MyProxyClientGetError** –
- **MyProxyClientRetrieveError** –

Parameters

- **username** – username of credential
- **passphrase** – existing pass-phrase for credential
- **newPassphrase** – new pass-phrase to replace the existing one.
- **sslCertFile** – certificate used for client authentication with the MyProxy server SSL connection. This ID will be set as the owner of the stored credentials. Only the owner can later remove credentials with myproxy-destroy or the destroy method. If not set, this argument defaults to \$GLOBUS_LOCATION/etc/hostcert.pem
- **sslKeyFile** – corresponding private key file. See explanation for sslCertFile

- **sslKeyFilePassphrase** – passphrase for sslKeyFile. Omit if the private key is not password protected.

Returns none

destroy (*username*, *sslCertFile=None*, *sslKeyFile=None*, *sslKeyFilePassphrase=None*)
destroy credentials from the server for a given username

Raises

- **MyProxyClientGetError** –
- **MyProxyClientRetrieveError** –

Parameters

- **username** – username selected for credential
- **sslCertFile** – certificate used for client authentication with the MyProxy server SSL connection. This ID will be set as the owner of the stored credentials. Only the owner can later remove credentials with myproxy-destroy or the destroy method. If not set, this argument defaults to \$GLOBUS_LOCATION/etc/hostcert.pem
- **sslKeyFile** – corresponding private key file. See explanation for sslCertFile
- **sslKeyFilePassphrase** – passphrase for sslKeyFile. Omit if the private key is not password protected.

Returns none

getDelegation (**arg*, ***kw*)
Retrieve proxy cert for user - same as logon

getTrustRoots (*username=''*, *passphrase=''*, *writeToCACertDir=False*, *bootstrap=False*)
Get trust roots for the given MyProxy server

Parameters

- **username** (*basestring*) – username (optional)
- **passphrase** (*basestring*) – pass-phrase (optional)
- **writeToCACertDir** (*bool*) – if set to True, write the retrieved trust roots out to the directory specified by the “caCertDir” attribute
- **bootstrap** (*bool*) – If set to True, bootstrap trust roots i.e. connect to MyProxy server without verification of the server’s SSL certificate against any CA certificates. Set to False, for default behaviour: verify server SSL certificate against CA certificates held in location set by the “caCertDir” attribute.

Returns trust root files as a dictionary keyed by file name with each item value set to the file contents

Return type dict

hostname
hostname of MyProxy server

info (*username*, *sslCertFile=None*, *sslKeyFile=None*, *sslKeyFilePassphrase=None*)
return True/False whether credentials exist on the server for a given username

Raises

- **MyProxyClientGetError** –
- **MyProxyClientRetrieveError** –

Parameters

- **username** (*string*) – username selected for credential
- **sslCertFile** (*string*) – certificate used for client authentication with the MyProxy server SSL connection. This ID will be set as the owner of the stored credentials. Only the owner can later remove credentials with myproxy-destroy or the destroy method. If not set, this argument defaults to \$GLOBUS_LOCATION/etc/hostcert.pem
- **sslKeyFile** (*string*) – corresponding private key file. See explanation for sslCertFile
- **sslKeyFilePassphrase** (*string*) – passphrase for sslKeyFile. Omit if the private key is not password protected.

classmethod locateClientCredentials (*enableTmpFileLoc=False*)

Find the location of a client certificate and private key to use to authenticate with the server based on the various default locations that MyProxy/Globus support

Parameters **enableTmpFileLoc** (*bool*) – enable setting based on /tmp/x509up_<uid>, defaults to False

Returns private key and certificate file location to use based on the current environment

Return type tuple

login (*username, passphrase, credname=None, lifetime=None, keyPair=None, certReq=None, nBitsForKey=4096, bootstrap=False, updateTrustRoots=False, authnGetTrustRootsCall=False, sslCertFile=None, sslKeyFile=None, sslKeyFilePassphrase=None*)

Retrieve a proxy credential from a MyProxy server

Exceptions: MyProxyClientGetError, MyProxyClientRetrieveError

Parameters

- **username** (*basestring*) – username of credential
- **passphrase** (*basestring*) – pass-phrase for private key of credential held on server
- **credname** (*string / None type*) – optional credential name - provides additional means to specify credential to be retrieved
- **lifetime** (*int*) – lifetime for generated certificate
- **keyPair** (*OpenSSL.crypto.PKey*) – Public/Private key pair. This is ignored if a certificate request is passed via the certReq keyword
- **certReq** (*string*) – ASN1 format certificate request, if none set, one is created along with a key pair
- **nBitsForKey** (*int*) – number of bits to use when generating key pair, defaults to the PRIKEY_NBITS class variable setting. This keyword is ignored if a key pair is passed in from an external source via the keyPair keyword
- **bootstrap** (*bool*) – If set to True, bootstrap trust roots i.e. connect to MyProxy server without verification of the server's SSL certificate against any CA certificates. Set to False, for default behaviour: verify server SSL certificate against CA certificates held in location set by the "caCertDir" attribute. If bootstrap is set, updateTrustRoots will be forced to True also
- **updateTrustRoots** (*bool*) – set to True to update the trust roots
- **authnGetTrustRootsCall** (*bool*) – pass username and password to getTrustRoots call. getTrustRoots is invoked if the "updateTrustRoots" or "bootstrap" keywords are set. This is not recommended for bootstrap since in this case the server is NOT authenticated by this client.

- **sslCertFile** – applies to SSL client based authentication - alternative to username/pass-phrase based. This certificate is used for authentication with MyProxy server over the SSL connection. If not set, this argument defaults to \$GLOBUS_LOCATION/etc/hostcert.pem
- **sslKeyFile** – corresponding private key file. See explanation for sslCertFile
- **sslKeyFilePassphrase** – passphrase for sslKeyFile. Omit if the private key is not password protected.

Return type tuple

Returns credentials as strings in PEM format: the user certificate, its private key and the issuing certificate. The issuing certificate is only set if the user certificate is a proxy

openSSLConfFilePath

file path for OpenSSL config file

openSSLConfig

OpenSSLConfig object

parseConfig (*cfg, section='DEFAULT'*)

Extract parameters from _cfg config object

port

Port number for MyProxy server

proxyCertLifetime

Default proxy cert. lifetime (seconds) used in logon request

proxyCertMaxLifetime

Default max. lifetime allowed for Proxy Certificate retrieved - used by store method

put (*username, passphrase, userCertFile, userKeyFile, lifetime=None, sslCertFile=None, sslKeyFile=None, sslKeyFilePassphrase=None*)

Store a proxy credential on the server

Unfortunately this method is not implemented as it requires the creation of a proxy certificate by the client but PyOpenSSL doesn't currently support the required proxyCertInfo X.509 certificate extension

Raises NotImplementedError see above

Parameters

- **username** (*string*) – username selected for new credential
- **passphrase** (*string*) – pass-phrase for new credential. This will be used by the server to authenticate later requests. It must be at least 6 characters. The server may impose other restrictions too depending on its configuration.
- **certFile** (*string*) – user's X.509 proxy certificate in PEM format
- **keyFile** (*string*) – equivalent private key file in PEM format
- **sslCertFile** (*string*) – certificate used for client authentication with the MyProxy server SSL connection. If not set, this argument defaults to \$GLOBUS_LOCATION/etc/hostcert.pem
- **sslKeyFile** (*string*) – corresponding private key file. See explanation for sslCertFile
- **sslKeyFilePassphrase** (*string*) – passphrase for sslKeyFile. Omit if the private key is not password protected.
- **lifetime** (*int / None*) – the maximum lifetime allowed for retrieved proxy credentials in seconds. defaults to proxyCertMaxLifetime attribute value

classmethod readProxyFile (*filePath=None*)

Read proxy cert file following the format used by myproxy-logon - proxy, cert, private key, user cert.

Return type tuple

Returns tuple containing proxy cert, private key, user cert

serverDN

Distinguished Name for MyProxy Server Certificate

setDefaultCACertDir ()

Make default trust root setting - the directory containing the CA certificates for verifying the MyProxy server's SSL certificate.

The setting is made by using standard Globus defined locations and environment variable settings

ssl_verification

Class with a method which is passed to the SSL context to verify the peer (MyProxy server) certificate in the SSL handshake between this client and the MyProxy server

store (*username, passphrase, certFile, keyFile, sslCertFile=None, sslKeyFile=None, sslKey-FilePassphrase=None, lifetime=None, force=True*)

Upload credentials to the server

Raises

- **MyProxyClientGetError** –
- **MyProxyClientRetrieveError** –

Parameters

- **username** (*string*) – username selected for new credential
- **passphrase** (*string*) – pass-phrase for new credential. This is the pass phrase which protects keyfile.
- **certFile** (*string*) – user's X.509 certificate in PEM format
- **keyFile** (*string*) – equivalent private key file in PEM format
- **sslCertFile** (*string*) – certificate used for client authentication with the MyProxy server SSL connection. This ID will be set as the owner of the stored credentials. Only the owner can later remove credentials with myproxy-destroy or the destroy method. If not set, this argument defaults to \$GLOBUS_LOCATION/etc/hostcert.pem or if this is not set, certFile
- **sslKeyFile** (*string*) – corresponding private key file. See explanation for sslCertFile
- **sslKeyFilePassphrase** (*string*) – passphrase for sslKeyFile. Omit if the private key is not password protected. Nb. keyFile is expected to be passphrase protected as this will be the passphrase used for logon / getDelegation.
- **force** – set to True to overwrite any existing creds with the same username. If, force=False a check is made with a call to info. If creds already, exist exit without proceeding

classmethod writeProxyFile (*proxyCert, proxyPriKey, userX509Cert, filePath=None*)

Write out proxy cert to file in the same way as myproxy-logon - proxy cert, private key, user cert. Nb. output from logon can be passed direct into this method

Parameters

- **proxyCert** (*string*) – proxy certificate
- **proxyPriKey** (*string*) – private key for proxy

- **userX509Cert** (*string*) – user certificate which issued the proxy
- **filePath** (*string*) – set to override the default filePath

INDICES AND TABLES

- *genindex*
- *search*

C

caCertDir (myproxy.client.MyProxyClient attribute), 8
 changePassphrase() (myproxy.client.MyProxyClient method), 8

D

destroy() (myproxy.client.MyProxyClient method), 9

G

getDelegation() (myproxy.client.MyProxyClient method), 9
 getTrustRoots() (myproxy.client.MyProxyClient method), 9

H

hostname (myproxy.client.MyProxyClient attribute), 9

I

info() (myproxy.client.MyProxyClient method), 9

L

locateClientCredentials()
 (myproxy.client.MyProxyClient class method),
 10
 logon() (myproxy.client.MyProxyClient method), 10

M

MyProxyClient (class in myproxy.client), 7

O

openSSLConfFilePath (myproxy.client.MyProxyClient attribute), 11
 openSSLConfig (myproxy.client.MyProxyClient attribute), 11

P

parseConfig() (myproxy.client.MyProxyClient method),
 11
 port (myproxy.client.MyProxyClient attribute), 11
 proxyCertLifetime (myproxy.client.MyProxyClient attribute), 11

proxyCertMaxLifetime (myproxy.client.MyProxyClient attribute), 11
 put() (myproxy.client.MyProxyClient method), 11

R

readProxyFile() (myproxy.client.MyProxyClient class method), 11

S

serverDN (myproxy.client.MyProxyClient attribute), 12
 setDefaultCACertDir() (myproxy.client.MyProxyClient method), 12
 ssl_verification (myproxy.client.MyProxyClient attribute), 12
 store() (myproxy.client.MyProxyClient method), 12

W

writeProxyFile() (myproxy.client.MyProxyClient class method), 12