OrangeFS Windows Client

OrangeFS Development Team

February 2012

OrangeFS Windows Client

The OrangeFS Windows* Client enables Windows systems to access OrangeFS/PVFS2 file systems. This document will guide you through the installation, operation and configuration of the Client. Complete information about OrangeFS can be located at http://www.orangefs.org.

Contents

Introduction

The Windows Client provides native access to OrangeFS for desktops and servers using Microsoft* Windows.

The Windows Client harnesses the power and speed of OrangeFS, including scale-out storage access from the Windows platform and high-performance parallel computing with full programmatic access via standard parallel programming APIs.

Options for authentication and user mapping include LDAP and X.509 certificates. The Client, which runs as a standard Windows service, supports Windows Vista, Windows 7 and Windows Server 2008 R2 (all editions); x86 and x64.

It enables you to view files though Windows Explorer and the Command Prompt, or you can access files programmatically through standard function calls—like fopen() in C.

Installing the Software

Topics for this section include:

- Preparing for installation
- What to expect
- Running the installation program
- Uninstalling

Preparing for Installation

Important: Please read this section before installation.

Client Requirements

Operating System:

- Windows Vista or Windows 7 (32- and 64-bit versions)
- Windows Server 2008 or Windows Server 2008 R2 (all editions; Server Core installation not currently supported)

Hardware:

- 30MB disk space
- Other requirements dependent on usage; minimum requirements very low

Other:

- You will need to assign a drive letter during installation.
- It is best to run the installer as an administrative user (Administrator, for example).

OrangeFS Requirements

During installation you will be asked to specify the URI of the OrangeFS server to which you will connect. This will require you to know the host name and port number (default is 3334).The format for this entry is provided later in the instructions.

Important: The OrangeFS installation you connect to with the Windows Client must be configured for TCP network protocol.

Authentication Configuration

During installation you will be given three options for user mapping

- `list`
- `certificate`
- `ldap`

The following table summarizes these options:

Options	Description	Best for:	Installation Input	More to do after installation?
`list`	Directly matches one Windows ID with one OrangeFS UID and primary GID.	Simple, smaller installations, trial runs, etc.	Enter one Windows user ID and the OrangeFS (Linux/UNIX-based) UID and primary GID for mapping.	Beyond first user, all others must be entered manually in the `orangefs.cfg` file after installation.
`certificate`	Maps user digital certificate to OrangeFS UID/GID. Our recommended setup is for grid computing which requires CA, proxy and user certificates.	Scientific, large cluster, research, etc.	Specify the location of your user and proxy certificates. This may be either the user's profile directory or custom directory, which you will need to enter...	If your certificates were properly installed and configured before installation, nothing else should be required.

Options	Description	Best for:	Installation Input	More to do after installation?

	IMPORTANT: You will need to have installed and configured your certificates before installation. A recommended method for doing this is included in these instructions.		`c:\users\{userid}`
			OR
			`{cert-dir-prefix}\{userid}`	

`ldap`	Maps user(s) on an LDAP tree to OrangeFS UIDs/GIDs	Windows with Active Directory* or eDirectory*	LDAP inputs, account to sign in, etc.	If all inputs are entered, nothing else should be required.

For more information on user mapping see Client Configuration and User Mapping.

What to Expect

When you complete the installation process, if you have provided all the necessary inputs, the last panel in the installer allows you to select whether to start the client. If you select this option, your system mounts the OrangeFS server you specified and the Windows Client starts. If you are not ready to start the client, you can wait to do it manually when you are ready.

When the installation program is finished, two new directories exist on your Windows system:

New directory	Description
`C:\OrangeFS\Client`	OrangeFS client software, including the client executable (orangefs-client.exe) and two configuration files (`orangefs.cfg, orangefstab`). The two configuration files can be edited for manual configuration, as explained later in this document.
`C:\Program Files\Dokan`	The Dokan* Library, an open source set of files used by the OrangeFS client to mount an OrangeFS server.

In addition to the above, the installation program also adds a few settings to your Windows registry. These settings are automatically removed if you uninstall the client.

Running the Installation Program

To install the OrangeFS Windows Client, you will need the self-extracting installation program, which is available in two versions, depending on your system's processor type (32-bit or 64-bit).

Download and run `orangefs-client-{version}-win32.exe` or `orangefs-client-{version}-win64.exe`. (For example, `orangefs-client-2.8.5.3-win64.exe`.) At this time, you cannot run the 32-bit installer on a 64-bit OS.

Note: It is best to run the installer as an administrative user (Administrator, for example).

1. When the installation program's Welcome dialog displays, click **Next**.
   The next dialog prompts you for an installation location.

2. Use the default location or select a different location and click **Next**.

3. Click **Install** to install the Client.
   The next dialog asks for a file system URI, a mount point and user mapping type.

4. Enter the file system URI, which is the address of any server in the OrangeFS file system you wish to access. The address should include the DNS name/IP address and port number of the OrangeFS file system server, as follows:
   Format: `tcp://{hostname}:{port}/{FS name}`.
   Example: `tcp://myhost.com:3334/pvfs2-fs`. Port 3334 is the default.

5. Enter the **Mount Point**, which, in Windows, is the drive letter (E:-Z:) that will represent the OrangeFS file system to which you have access.

   Select **Auto** if you prefer to use the first available drive letter (starting with E:).

6. Select the type of **User Mapping** you will use.

   If you are not sure, select **List**; the settings can be changed after installation.

   Note: Selecting the `certificate` option for user mapping requires the certificates to have already been generated and placed in appropriate locations to support the Windows Client. If you still need to complete this process, close the installation program for now. When finished with certificate generation, you can restart the installation program.

   Click **Next** to continue.

   The next dialog to display will depend on the type of user mapping you selected.

7. If you selected **List Mapping**, you will need to enter one Windows user ID and the OrangeFS (Linux/UNIX-based) UID and primary GID for mapping. Additional users must be added to the configuration file manually after the installation.

   If you selected **Certificate Mapping**, you are asked to enter the location of your user and proxy certificates. The default is the user profile directory (c:/users/<userid>). Or you may choose another location, which you will enter as the location prefix (<prefix dir>/<userid>).

   If you selected **LDAP Mapping**, a dialog provides three choices for your LDAP implementation (**Active Directory, eDirectory or Custom). S**elect one and click **Next**. In the next dialog that displays, enter the LDAP values OrangeFS requires.

   Note: Depending on which LDAP selection you make, some of the text fields that display in the dialog may already have entries.

   Click **Next** to continue.

The final dialog displays with an option to start the OrangeFS services upon exiting the installation program.

8. Select the check box if you want the client to run and mount the OrangeFS server you specified as soon as the installation program closes.

   Leave the checkbox unselected if your configuration is not complete, and you can manually start the OrangeFS client services later.

   Click **Finish** to complete the installation.

Uninstalling the Client

To uninstall the Windows Client from your computer:

1. Open the **Control Panel** and click **Programs and Features**.
2. Locate and select the **OrangeFS Client** item, and click the **Uninstall** button above.
3. Follow the uninstaller steps to remove the Client.
4. Remove configuration files under `C:\OrangeFS\Client` (by default).

Using the Client

Topic categories for this section include:

- Interfacing with OrangeFS
- Running the Client
- Understanding Security
- Getting/Generating Certificates

Interfacing with OrangeFS

When the Windows Client is running on your computer, the OrangeFS file system appears as a removable drive at the drive letter (E:-Z:). This drive letter, which was specified during installation, is a setting in the configuration file and can be changed. For more information, see Client Configuration.

You can interact with files and directories in the file system in the same way as local files. For example, they can be viewed in Windows Explorer, listed in the Command Prompt or accessed using program API functions, such as `fopen`.

Note: Currently the Client can only mount one OrangeFS file system at a time.

One limitation is that files cannot be created in Explorer--only directories can. To create a file, you need to use the application that corresponds to its file type and save it to the file system.

Running the Client

Two Windows Services must be started to run the OrangeFS Windows Client:

- DokanMounter
- OrangeFS Client

These services are accessed in the Windows Services utility. To open the Services utility, get into the **Control Panel** and click **Administrative Tools** > **Services**. You should see the two services (named above) included in the console listing.

To start (or stop) a service, right-click the service and select the desired action.

The DokanMounter should be started first. This service is tied to the Dokan Library, which is the third-party software included with your installation. DokanMounter enables the Windows Client to mount the file system transparently.

The two services are set to start automatically any time the system is restarted. To change this setting, right-click the service and select **Properties**.

> **Note:** If you have reason to stop the Windows Client service, it is normally not necessary to also stop the DokanMounter service.

Understanding Security

Security is enforced by mapping the Windows user ID to an OrangeFS Linux/UNIX-based UID. The user ID then has permissions to files and directories based on the OrangeFS UID. New files and directories created on Windows will have the mapped UID as owner, the mapped primary GID as group, and permissions mask 755 (`rwxr-xr-x`) by default. You may mark the file as read-only on Windows to remove owner write permissions.

Note: The default permissions mask may be changed with the `new-file-perms` and `new-dir-perms` configuration file keywords; see “Working wih the orangefs.cfg file” below.

Level of security will also depend on the the type of user mapping your Windows Client is configured for. The three types of user mapping are

- **List** Directly matches one Windows ID with one OrangeFS UID and primary GID.
- **Certificate** Maps user digital certificate to OrangeFS UID/GID. Our recommended setup is for grid computing which requires CA, proxy and user certificates
- **LDAP** Maps user(s) on an LDAP tree, such as Active Directory or eDirectory, to OrangeFS UIDs/GIDs

For more information, see “User Mapping.”

Getting (or Generating) New Certificates

Note: This task only applies if your Windows Client is using Certificates for user mapping.

If your Windows Client is configured for certificate mapping, this will likely involve three types of certificates (CA, proxy, user). Usually, these certificates are created and installed by your administrator. However, since all certificates have expiration dates, you may need new ones regenerated from time to time while using the Windows Client.

Depending on your setup, you may need to request new certificates from your administrator or he or she may provide you with instructions for doing it yourself.

Of the three types of certificates mentioned earlier, the proxy certificate will generally need to be renewed more often than the other two. Depending on your administrative policies, the time before a proxy certificate expires can average anywhere from 6 hours to two weeks.

Client Administration

Topic categories for this section include:

- Configuration
- User Mapping
- Installing and Using Globus Toolkit (certificates only)
- Troubleshooting
- Source Code

Configuration

Two configuration files exist for the OrangeFS Client:

- `orangefstab`
- `orangefs.cfg`

Both files are located in the OrangeFS installation directory (`c:\orangefs\client`). They are text files that can be edited.

The `orangefstab` file contains only one line entry, which is the URI address of the OrangeFS server to be mounted for Windows Client access.

The `orangefs.cfg` file can contain a wide range of settings, including:

- The drive letter on your Windows system that is associated with OrangeFS
- The user mapping option your client is configured for (`list`, `certificate`, `ldap`)
- Various additional settings for each of the user mapping options
- Debug settings for logging and troubleshooting

For more information, including correct syntax, on adding and modifying line entries in these files, see “Client Configuration.”

Note: Because the configuration files can be altered to change security information, only administrative users should be able to change them (For security information, see your Windows documentation.)

Working with the orangefstab file

The `orangefstab` file uses the same format as Linux/UNIX mtab (file system mounting) files. On Windows, only the file system URI is of real importance.

Here is a sample line entry in `orangefstab`:

```
tcp://orangefs.acme.com:3334/pvfs2-fs /mnt/pvfs2 pvfs2 defaults,noauto 0 0
```

Since only one file system can be mounted, only one line can be used.

The first field is the important one. It is a URI that specifies an OrangeFS file system server. The format is `tcp://{hostname}:{port}/{FS name}`. The only protocol supported on Windows is TCP. The default port is 3334. The file system name can be determined from the server configuration file (default is `pvfs2-fs`).

The second field is the internal UNIX-style mount point. This value should be the same for all clients (Windows or Linux/UNIX). The other fields should be left as-is above.

Working with the orangefs.cfg file

The bulk of the Windows Client configuration information is contained in `orangefs.cfg`. This is a text file that contains line entries in the following format:

```
{keyword} [option value]
```

You can also specify comments using the # character:

```
# This is a comment.
```

Keyword: mount

The first essential keyword to discuss is `mount`. This keyword is used to specify the drive letter that is associated with the mounted OrangeFS server.
Example:

```
mount O:
```

This example will mount the file system on O: drive. (You must include the colon.) If the mount keyword is not used, the first alphabetically available drive, starting with E:, is used.

Keyword: user-mode

The `user-mode` keyword selects the user mapping mode. It **must** be included in the file, or the Client will not start. The option value must be `list`, `certificate` or `LDAP`.
Example:

```
user-mode list
```

For more on user mapping keywords, see “User Mapping”.

Keywords: new-file-perms, new-dir-perms

The `new-file-perms` and `new-dir-perms` keywords change the initial permissions mask of newly created files and directories. If these keywords are not present, the permissions mask is 755 (`rwxr-xr-x`).

Note: For information on the permissions mask, see the Linux/UNIX `chmod` man page.

The keywords are used with an octal integer value representing the permissions mask.
Examples:

```
new-file-perms 644
new-dir-perms 700
```

The first example will cause new files to be created with “`rw-r--r--`“ permissions. The second will create directories with “`rwx------`“ permissions.

Note: While you can set the “sticky bit” in OrangeFS, it has no affect.

Important: You should always ensure that the owner of the file has read permissions to their own files (mask 400), and read and execute permissions to their own directories (mask 500). Otherwise a user will not be able to read these files and directories after creation.

Keywords: debug, debug-file, debug-stderr

Finally, the `debug`, `debug-file` and `debug-stderr` keywords are used to log detailed debugging information. If you specify the `debug` keyword by itself, Client-related messages are recorded in `orangefs.log` in the installation directory (`C:\OrangeFS\Client`) by default.

You can change the name and location of the log file by using the `debug-file` keyword:

```
debug-file C:\Temp\myfile.log
```

You can also use any of the debugging flags available with OrangeFS. For a list of these flags, see the OrangeFS system documentation. The Client flag is `win_client`. With this line:

```
debug win_client io msgpair
```

...you would record debugging information about the Client, I/O and message pair operations.

The `debug-stderr` keyword is used with no option value, and causes debugging messages to be printed to the console. This keyword is only useful if `orangefs-client.exe` is running as a normal executable (not as a service).

Keywords for User Mapping

There are many more keywords that are specific to the user mapping mode you choose for the Windows Client. For detailed discussion of these keywords, see User Mapping.

Keyword Table

The following table lists all available keywords for the orangefs.cfg file. Note that it does not include the option values available for each keyword. See individual keyword discussions for those details.

Keyword	Description
`mount`	Sets Windows drive letter that represents OrangeFS file system.
`user-mode`	Sets the authentication/security method used to map Windows user accounts with OrangeFS user accounts.
`list`	One of the three user-modes. Directly matches one Windows ID with one OrangeFS UID and primary GID.
`user`	Defines a user who is mapped in list mode. A separate line using this keyword is required for each user.
`certificate`	One of three user-modes. Maps user digital certificate to OrangeFS UID/GID.
`ca-path`	Path to file for CA (Certificate Authority) certificate.
`cert-dir-prefix`	Specifies the location of your user certificates if the user's default profile directory is not being used. Specify a path to a directory.
`ldap`	One of the three user-modes. Enables Windows user ID to be looked up in an identity directory that supports LDAP. Examples: Active Directory and eDirectory.
`ldap-host`	Sets the host computer running ldap.
`ldap-bind-dn`	Sets a user DN to bind to.
`ldap-bind-password`	Sets a user password.
`ldap-search-root`	Specifies the DN of the directory container object where searches should begin.
`ldap-search-class`	Specifies object class that the user object must be.
`ldap-search-scope`	Sets the scope of user searches.
`ldap-naming-attr`	Sets the attribute on the user object that must exactly match the Windows user ID.

Keyword	Description
ldap-uid-attr	Specifies the attributes which store the OrangeFS UID.
ldap-gid-attr	Specifies the attributes which store the OrangeFS GID.
new-file-perms	Specifies the permissions mask that new OrangeFS files will have.
new-dir-perms	Specifies the permissions mask that new OrangeFS directories will have.
debug	Specifies for all client-related messages to bee logged in orangefs.log.
debug-file	Sets a custom name and location of log file used for debugging (in place of orangefs.log).
debug-stderr	Sets all debuggin messages to print to console. Works only when the executable, orangefs-client, is run (rather than running the service).

User Mapping

The Client maps Windows user IDs to OrangeFS Linux/UNIX-based UIDs for authentication. The `user-mode` keyword in `orangefs.cfg` specifies the type of user mapping. There are three modes of user mapping, detailed below.

List Mapping

This simple form of mapping allows you to list Windows user IDs and their corresponding OrangeFS UIDs and primary GIDs. The list is created in `orangefs.cfg`. Here is the format of each line:

```
user {Windows User ID} {UID}:{GID}
```

Example:

```
user ofsuser 500:100
```

Lines specifying users must come after the line containing the `user-mode` keyword.

File operations originating from the specified Windows user ID will be carried out on OrangeFS as the specified UID.

Certificate Mapping

This topic includes:

- A summary of the currently supported approach to certificate mapping for the Windows Client, including the supported software package for implementing this approach
- The three types of certificates that must be in place before configuring the Windows Client for certificate mapping
- The configuration settings for certificate mapping that can be set in `orangefs.cfg`, either during installation or manually.

Important: This topic ***does not*** discuss how to create certificates. For notes on the mechanics of generating certificates, see “Notes on Installing and Using Globus Toolkit.”

Certificates for Grid-Computing

With OrangeFS, the use of certificates for user mapping and security is often associated with grid computing. Therefore, the OrangeFS team chose to support the certificate generation capabilities of Globus Toolkit (an open source utilities package for grid computing) in its early implementation of the Windows Client.

Specifically, the Globus Toolkit components used to generate certificates for the Windows Client are MyProxy and SimpleCA.

If you choose the `certificate` option for user mapping, the certificates will need to already have been generated and placed in their appropriate locations. For more information on meeting these certificate requirements for Windows Client, see "Notes on Installing and Using Globus Toolkit."

Future releases of the Windows Client will accommodate alternatives to certificates generated by Globus Toolkit. Until then, if you wish to implement a certificate solution other than the one used here, please contact Technical Support.

Certificate Requirements

The Client uses X.509 certificates to identify users. The certificates contain the UID and GID to be used on the OrangeFS server. Because OrangeFS currently expects trusted clients, the certificates *do not provide true security*. However, they will limit the actions of typical users, such as deleting files they do not own. Note that support for untrusted clients will be added to OrangeFS in an upcoming release.

Three types of certificates must be in place for the Windows Client:

- CA (certificate authority)
- proxy
- user

The following table describes each type.

Type	Example Name	Default Location on Windows Client	Default location on Globus Toolkit System
CA	`cacert.pem`	`C:\OrangeFS\Client\CA`	`{home}/.globus/cacert.pem` ...where `home` is the home directory of the user who installed SimpleCA, typically `root`.
Proxy	`cert.0`	`C:\Users\{userid}`	`/tmp/x509up_u250` (for UID 250)
User	`cert.1, cert.2 ...`	`C:\Users\{userid}`	`{home}/.globus/usercert.pem`

Configuration File

There are two configuration file keywords associated with the `certificate` option for user mapping: `ca-path` and `cert-dir-prefix`.

If you wish to store the CA certificate in a non-default location on the Windows Client, you can add a line entry to `orangefs.cfg` that begins with the `ca-path` keyword, followed by the custom directory location, as follows:

```
ca-path {path}
```

Example: `ca-path C:\Certificates\OrangeFS\CA`

If you wish to store the user and proxy certificates in a non-default location on the Windows Client, you can add a line entry to `orangefs.cfg` that begins with the `cert-dir-prefix` keyword, followed by a path to a directory.

```
cert-dir-prefix <path to directory>
```

Example: `cert-dir-prefix C:\Certificates\OrangeFS`

When the Client attempts to locate the proxy and user certificates for a user, it will append the userid as a directory name to the cert-dir-prefix. For example, user bsmith's certificates should be placed in `C:\Certificates\OrangeFS\bsmith\` using the cert-dir-prefix above.

LDAP Mapping

LDAP (Lightweight Directory Access Protocol) mapping allows the Windows user ID to be looked up in an identity directory that supports LDAP. Example LDAP directories include Microsoft Windows Active Directory and Novell* eDirectory. Consult your directory documentation for information on LDAP.

LDAP options are specified in `orangefs.cfg`. The keywords described below must follow the `user-mode ldap` line entry.

Connecting over LDAP

First you must specify the host computer running LDAP. This is done with the `ldap-host` keyword in the following format:

```
ldap-host ldap[s]://{hostname}:{port}
```

If `ldaps` is specified, a secure connection is used; otherwise, the connection is plain text. The default secure port is 636, and the default plain text port is 389, but you may alter the port as shown above. Example:

```
ldap-host ldaps://myldaphost.acme.com:1636
```

You may bind to the directory anonymously if it allows, or you may specify a user and password with the `ldap-bind-dn` and `ldap-bind-password` keywords:

```
ldap-bind-dn {bind (login) user DN}
ldap-bind-password {password}
```

Example:

```
ldap-bind-dn cn=orangefs-user,ou=special,o=acme
ldap-bind-password S3crt!
```

Because the password is stored in plain text in the configuration file, you must give the binding user minimal rights to the directory. For more information, see "LDAP Security" below.

Search Options

The Client will search LDAP for the Windows user ID making the file system request. The search options configure how the directory will be searched.

First, the `ldap-search-root` keyword specifies the DN of the directory container object where the search should begin.

```
ldap-search-root ou=cluster-users,o=acme
```

The `ldap-search-scope` keyword can be one of either `onelevel` or `subtree`. If `onelevel` is specified, only the object specified with `ldap-search-root` is searched—no descendant

objects (sub-containers) are searched. If `subtree` is specified, the object specified with `ldap-search-root` is searched along with all descendant objects. The default is `onelevel`.

```
ldap-search-root subtree
```

The Client will form an LDAP search string in the form:

```
(&(objectClass={ldap-search-class})({ldap-naming-attr}={Windows user ID}))
```

The `ldap-search-class` keyword specifies the object class that the user object must be. Typical values are `User` or `inetOrgPerson`.

```
ldap-search-class User
```

The `ldap-naming-attr` keyword indicates the attribute on the user object that must exactly match the Windows user ID. Consult your documentation for whether the comparison is case-sensitive (typically it is not). Typical values might be `cn` or `name`.

```
ldap-naming-attr cn
```

Attribute Options

The `ldap-uid-attr` and `ldap-gid-attr` keywords specify the attributes which store the OrangeFS UID and primary GID respectively. The Client retrieves these values for use on the file system.

```
ldap-uid-attr uidNumber
ldap-gid-attr gidNumber
```

LDAP Security

Because the LDAP binding password is stored as plain text, you must give the binding user minimal rights to the LDAP directory. Alternatively, minimal rights can be given to users who bind anonymously—no password is stored in this case. Here are rights to consider:

- Rights to search objects in the search root and below
- Rights to read the object class, naming attribute, UID attribute and GID attribute from searchable objects
- No write/delete/administrator rights

For performance, UID/GID credentials are cached for a time after lookup. If rights need to be revoked, the OrangeFS Client service should be restarted.

You should also use an encrypted connection to LDAP if possible, by specifying `ldaps` in the host URI.

Notes on Installing and Using Globus Toolkit

This section provides supplementary information about Globus Toolkit. The information only applies to Windows Clients that use the certificates mode for user mapping.

With OrangeFS, the use of certificates for user mapping and security is often associated with grid computing. Therefore, the OrangeFS team chose to support the certificate generation capabilities of Globus Toolkit (an open source utilities package for grid computing) in its early implementation of the Windows Client.

Note: Future releases will accommodate alternatives to the Globus Toolkit approach. Until then, if you wish to implement a certificate solution other than the one described here, please contact Technical Support.

Whether you are new to Globus Toolkit or you have already installed it for certificate generation, the guidelines and suggestions in this section will ensure optimal certificate configuration for the Windows Client.

Introduction

The Client can use X.509 certificates to identify users. The certificates contain the UID and GID to be used on the OrangeFS server. Because OrangeFS currently expects trusted clients, the certificates *do not provide true security*. However, they will limit the actions of typical users, such as deleting files they do not own. Note that support for untrusted clients will be added to OrangeFS in an upcoming release.

Identifying Certificate Format

The certificate that identifies the OrangeFS user is called the identifying certificate. It is a proxy certificate, which allows authorization on behalf of an "end entity," in this case a user. This user is represented by a user certificate.

Proxy certificates contain authorization information in a data field known as a policy. For the Client, the policy is a UTF-8 string in the form `{UID}/{GID}`. For OpenSSL, the proxy specification for UID 250 and primary GID 100 looks like:

```
language=id-ppl-anyLanguage
pathlen=0
policy=text:250/100
```

More information on generating this certificate is provided below.

Certificates and Validation

The identifying certificate is only useful if it can be validated against its signing certificate. The signing certificate may also need to be validated against the certificate that signed it, and so on, forming a certificate chain. Ultimately, the chain must end at the trusted, self-signed certificate of a certificate authority (CA).

Installing Globus Toolkit

Install Globus Toolkit on one of the OrangeFS servers or another Linux system that shares the same user information (UIDs/GIDs).

Installation instructions for Globus Toolkit can be obtained at `http://www.globus.org/toolkit/docs/latest-stable/`. The Quickstart instructions will provide a default configuration for MyProxy, including a CA called `SimpleCA`.

There are many different security options that can be configured. For example, a third-party certificate authority may be used. As long as the identifying certificate follows the format above, the client will accept the certificate.

Locating the CA Certificate

If `SimpleCA` is being used, the default CA certificate is `{home}/.globus/cacert.pem`, where `$HOME` is the home directory of the user who installed SimpleCA, typically `root`.
If a third-party CA is being used, the certificate will be located in an implementation-dependent location. The security administrator of the grid should be able to locate the file.

The CA certificate needs to be copied to the Client system after installing the Client. For the location of the file, see "Client Certificate Locations" below.

Using Grid-based certification

To use grid-based certification, the user must first have a user certificate. To obtain this certificate, the user runs `grid-cert-request` to generate a certificate request file. At that time, the user specifies the certificate pass phrase. This file is then e-mailed (for example) to the CA organization, where a human agent will review the request and return a user certificate signed by the CA certificate. The certificate will be stored in `{home}/.globus/usercert.pem`. If the grid installation is using `SimpleCA`, the certificate request can be processed by a local administrator using the `grid-ca-sign` command.

The `grid-proxy-init` command can then be used to obtain a proxy certificate. A file (`cert-policy`, for example) should be created to contain the policy text, which is formatted `{UID}/{GID}`. The file would contain `250/100` for a user with UID 250 and GID 100. The `grid-proxy-init` command can be used to generate the proxy certificate with our example `cert-policy` file, as follows:

```
grid-proxy-init -policy cert-policy -pl id-ppl-anyLanguage
```

The user enters the certificate pass phrase and the proxy certificate is generated. To simplify this command, the OrangeFS installation package includes the script `Tools\pvfs2-grid-proxy-init.sh`. This will generate the policy file and run `grid-proxy-init`. The resulting proxy certificate is stored by default at `/tmp/x509up_u{UID}`. *Example*: `/tmp/x509up_u250` for UID 250.

This certificate must be transferred to the Client system, along with the user certificate (see above). For the file location, see “Client Certificate Locations” below. The proxy certificate must be renamed `cert.0`, and the user certificate `cert.1`.

Delegating Identities for Clusters

The use of identifying proxy certificates allows the identity of the user to be separated from the actual Windows user ID making a file system request. This ability is useful for clusters.

For example, a user has Windows user ID JSmith. However, when he executes a job on a cluster node, the job scheduler uses Windows user ID ClusterUser.

The system administrator would set the certificate directory prefix to `C:\ClusterWork`. A directory called `ClusterUser` would be created under `ClusterWork`. The job scheduler would transfer certificates to the `C:\ClusterWork\ClusterUser` directory. When `ClusterUser` makes file system requests, it will use JSmith’s certificates, so requests will be made using JSmith’s UID on the file system. When a different user uses the node, that user’s certificates will be used.

Certificate Expiration and Renewal

For performance, the Client caches the OrangeFS user identity (UID/GID) until the proxy certificate expires. By default, Globus Toolkit proxy certificates expire after 12 hours. If jobs requiring more time are expected, a means for the user to renew the certificate should be provided.

One way to do this is to have the user to run `grid-proxy-init` again. This will overwrite the current proxy. Then the new proxy certificate can be transferred to the Client system (overwriting the current certificate) without interrupting the current job.

Client Certificate Locations

The certificates are stored as PEM-format files on the Client system. The identifying certificate's name is `cert.0`. Because the identifying certificate is associated with a Windows user, by default it is stored in its user's profile directory. On most systems this is `C:\Users\{username}`.
Example: `C:\Users\jsmith`

Alternatively, a certificate `prefix` directory can be specified in the client configuration file, by default `C:\OrangeFS\Client\orangefs.cfg`. Use the `cert-dir-prefix` keyword to specify this directory. The user's username will be appended as a directory name to the prefix directory. Here's an example configuration file statement:

```
cert-dir-prefix M:\OrangeFS Users
```

For user jsmith, the identifying certificate will be `M:\OrangeFS Users\jsmith\cert.0`.

The identifying certificate must be verified by its end-entity (sometimes called a user) certificate. This certificate should be placed in the same directory as the identifying certificate, with the name `cert.1`. Additional intermediate certificates can be placed in the same directory with names `cert.2`, `cert.3`, and so on.

The CA certificate is placed in the OrangeFS CA directory with the name `cacert.pem`. By default this is `C:\OrangeFS\Client\CA\cacert.pem`. This path can be changed in the configuration file using the `ca-path` directive in the configuration file:

```
ca-path M:\OrangeFS Certificates\orangefs-cacert.pem
```

If this certificate changes, the Client service must be restarted.

Troubleshooting

To troubleshoot problems, check the Application Event Log in the Event Viewer utility. You can also turn on detailed debugging (see the next section).

As mentioned earlier, startup errors will be logged to the Windows Event Log.

The configuration file has some strict requirements, so if there is a problem the Client will log an error to Event Log and exit. The event message should give an exact explanation of the problem with the configuration file. Correct the problem and restart the OrangeFS Client service.

Make sure network connectivity is available between the Client system and the server(s) hosting OrangeFS. Check firewall settings and network access lists.

For information about the `debug` and related keywords, see the earlier section, "General Configuration." The generated file `orangefs.log` can be used to diagnose problems. A file named `service.log` is also created in the installation directory when debugging is enabled, and can provide more detail on startup errors.

Note that many debug messages are low-level and require extensive knowledge of OrangeFS/PVFS2 to interpret. For more information, consult the OrangeFS and PVFS2 system documentation.

Free and commercial support is available at http://orangefs.org.

Source Code

The intention of the OrangeFS team is to provide all source code needed for building the Client. Instructions on obtaining source code using subversion, a source control program, are available at http://orangefs.org. Build instructions will be released at a later date.