Manage2 API Authentication Methods

To authenticate via the Manage2 API use either HTTP Basic Authentication or key-based authentication.

HTTP Basic Authentication

HTTP Basic Authentication encodes your username and password inside the HTTP request headers. Manage2's PHP and Perl client libraries use HTTP basic authentication over SSL by default.

Client examples

A browser client

To use HTTP Basic Authentication via a browser client, use the browser to send the API call and enter your username and password in the dialog window. The authentication session will remain active in your browser session unless you clear the browser cookies or close the browser window.

The following URL is an example of how to send an API call via a browser client:

```
https://manage2.cpanel.net/XMLlicenseInfo.cgi?output=json
```

A curl client

To use HTTP Basic Authentication via a client script or console, send a *curl* command with your Manage2 username, password, and API call details.

The following *curl* command example uses HTTP Basic Authentication:

```
curl -u user@example.com:secret
https://manage2.cpanel.net/XMLgroupInfo.cgi
```

The Manage2 API Perl library

The following Perl code example uses the Manage2 API Perl library's *cPanelLicensing* module to authenticate via HTTP Basic Authentication:

```
use cPanelLicenses;
my $cpl = cPanelLicensing->new(user => "user\@example.com", pass =>
"secret");
$cpl->fetchGroups();
```

The Manage2 API PHP library

The following PHP code example uses the Manage2 API PHP library's *cPanelLicensing* class to authenticate via HTTP Basic Authentication:

```
require "cpl.inc.php";
$cpl = new cPanelLicensing("user\@example.com", "secret");
$cpl->fetchGroups();
```

Key-based authentication

Key-based authentication grants access to send API calls without your Manage2 username and password. Manage2 authorizes each API key to send API calls from the IP address which you specify.

To create an API key for key-based authentication, perform the following steps:

1. Use the [Manage2 API Functions - Add a Pickup Phrase](#) function to add a pickup passphrase for your Manage2 user and a specific IP address.
2. Use the pickup passphrase from step 1 with the [Manage2 API Functions - Register Key-Based Authentication](#) function to retrieve the 20 character API key. Send that API key via the `apikey` parameter with all subsequent API calls.

Client examples

A browser client

To use key-based authentication via a browser client, use the browser to send the API call and include the `apikey` parameter with your API key.

The following URL is an example of how to send the `apikey` parameter via a browser client:

```
https://manage2.cpanel.net/XMLlicenseInfo.cgi?
output=json&apikey=aFj1fKnYzW5lbD5KXFeVtLsM
```

A curl client

To use key-based authentication via a client script or console, send a *curl* command with your API key and API call details.

```
curl 'https://manage2.cpanel.net/XMLlicenseInfo.cgi?
output=json&apikey=aFj1fKnYzW5lbD5KXFeVtLsM'
```

The Manage2 API Perl library

The following Perl code example uses the Manage2 API Perl library's *cPanelLicensing* module to authenticate via key-based authentication:

```
use cPanelLicenses;
my $cpl = cPanelLicensing->new(apikey => "aFj1fKnYzW5lbD5KXFeVtLsM");
$cpl->fetchGroups();
```

The Manage2 API PHP library

The following PHP code example uses the Manage2 API PHP library's *cPanelLicensing* class to authenticate via key-based authentication:

```
require "cpl.inc.php";
$cpl = new cPanelLicensing(apikey => "aFj1fKnYzW5lbD5KXFeVtLsM");
$cpl->fetchGroups();
```