REST API

OpenVPN Access Server

The OpenVPN Access Server now supports a Web Services API called REST that can be used to fetch a client configuration file from the Access Server.

The curl command can be used to easily access this API as follows:

curl -u USERNAME:PASSWORD https://ACCESS_SERVER:CWS_PORT/rest/METHOD

Any generic HTTPS client tool (including even a web browser) can be used to access the API -- curl is just used here as an example. Whatever method is used, the USERNAME:PASSWORD pair should be passed to the API using HTTP Basic Auth.

Replace the above variables in the curl command as follows:

USERNAME -- the username of the Access Server user for whom a configuration file is sought.

PASSWORD -- the password of the Access Server user for whom a configuration file is sought.

ACCESS_SERVER -- the domain name or public IP address of the Access Server.

CWS_PORT -- the port that the client web server is listening on. Usually 443 but may be different based on the specific Access Server configuration. This is normally the same port that you would use to connect to the Client Web Server UI.

METHOD -- use "GetUserlogin" to get an OpenVPN client configuration file that will require a username and password to connect to the Access Server. Use "GetAutologin" to get an OpenVPN configuration file that will authenticate with the Access Server using only a client certificate, with no username and password required. This is idea for unattended clients such as routers, servers, or appliances.

***Note** that for Autologin configurations, the user (specified by USERNAME) must have the Autologin permission enabled in the User Permissions page of the Access Server Admin UI.

- *On success*, the web services API will return the OpenVPN client configuration file as content-type text/plain.

- *On error*, an error message will be returned as content-type text/xml. These are some of the common error returns:

Authentication failed (bad USERNAME or PASSWORD):

<?xml version="1.0" encoding="UTF-8"?>

<Error>

<Type>Authorization Required</Type>

<Synopsis>REST method failed</Synopsis>

<Message><Fault 9007: 'AUTH_FAILED: Server Agent XML method requires authentication'></Message>

</Error>

User does not have permission to use an Autologin profile:

<?xml version="1.0" encoding="UTF-8"?>

<Error>

<Type>Internal Server Error</Type>

<Synopsis>REST method failed</Synopsis>

<Message><Fault 9000: "NEED_AUTOLOGIN: User 'USERNAME' lacks autologin privilege"></Message>

</Error>

Keep in mind that when using curl as the HTTPS client, curl will require that the Access Server web server uses a trusted certificate, such as a commercial web certificate. If your Access Server uses a self-signed CA, then it would be advisable to make this certificate available to curl, or whatever HTTPS client you are using.

The Access Server web CA certificate is stored here:

/usr/local/openvpn_as/etc/web-ssl/ca.crt

and can be specified to curl using the following option:

--cacert ca.crt

It is also possible to instruct curl to disable web server certificate verification using the -k option, but this should be discouraged for security reasons.

*Also note that the OpenVPN client configuration files obtained from the Access Server require ***OpenVPN 2.1.***