ECS user guide

1. Prerequisites - Firewall Configuration

- The ECS service is available on Internet. If a firewall or other traffic filtering software or hardware is protecting the ECS client device please ensure that TCP port 443 (SSL) is opened towards Internet.

- For better performance it is also recommended to allow UDP port 4500. The client will automatically try to use the best connection method available.

- For example, if you employ an edge router and a firewall between the Internet and your corporate intranet, you must ensure that port 4500 is enabled on both the router and the firewall and that port 4500 is configured to pass UDP traffic. A firewall will see two connections per user when using ESP; one for the Control Channel on port 443 and one for the data channel on port 4500.

- The main advantage for ESP transport mode is the increase in performance over SSL transport mode.

2. Limitations

- ECS can only be used on standard Windows/Linux/Mac single user PC's (multi user environments like Citrix may not work)

- The ECS-client software does not protect the PC from attacks from e.g. the Internet. No security for the PC itself is included in the ECS service.

- Other installed VPN clients can interfere with the ECS VPN client. Before calling support you need to uninstall other VPN clients to make sure they do not interfere.

- A user-ID can only be used by one user at a time. Multiple sessions with the same user-ID Causes unexpected behaviors and are NOT allowed

3. Installation of client software

Before you start:

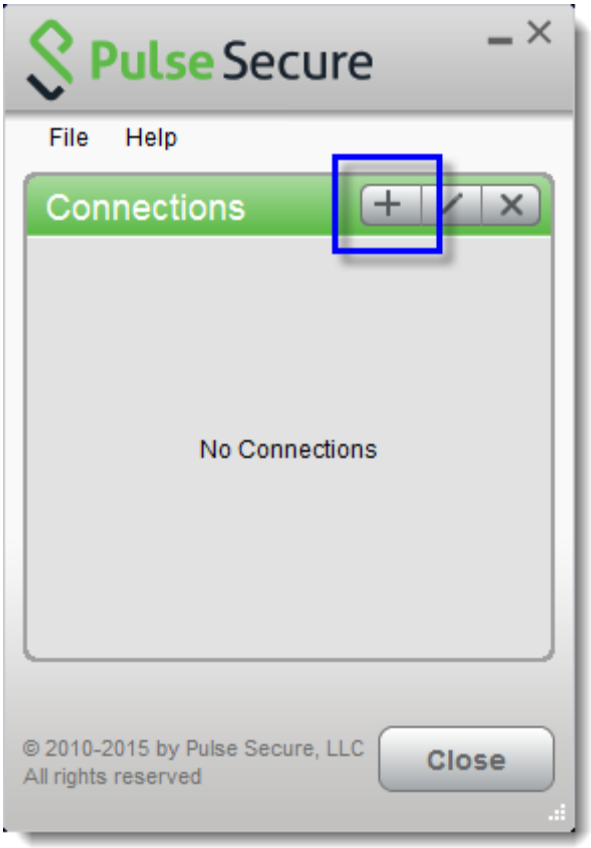
- The installation may require administrator privileges.

3.1. Installation

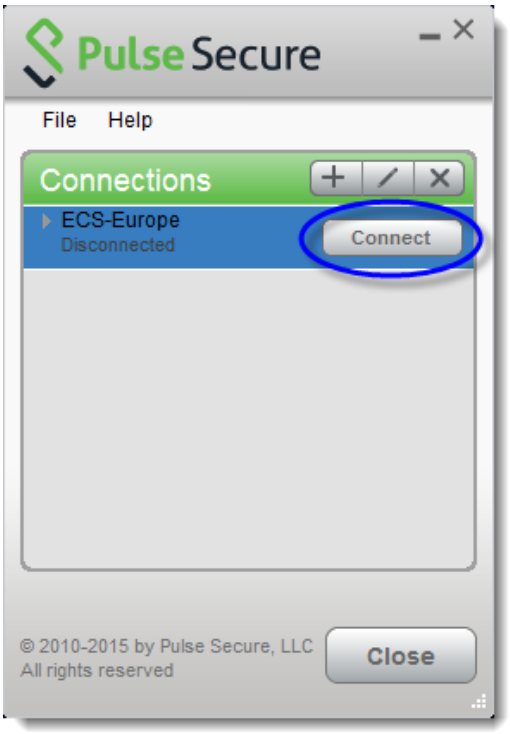
- Client software can be found ***here***
- Select which OS you are running, download and install the application.

When the installation is complete, the Pulse icon will appear in the taskbar. 

- Open the application and add an ECS connection



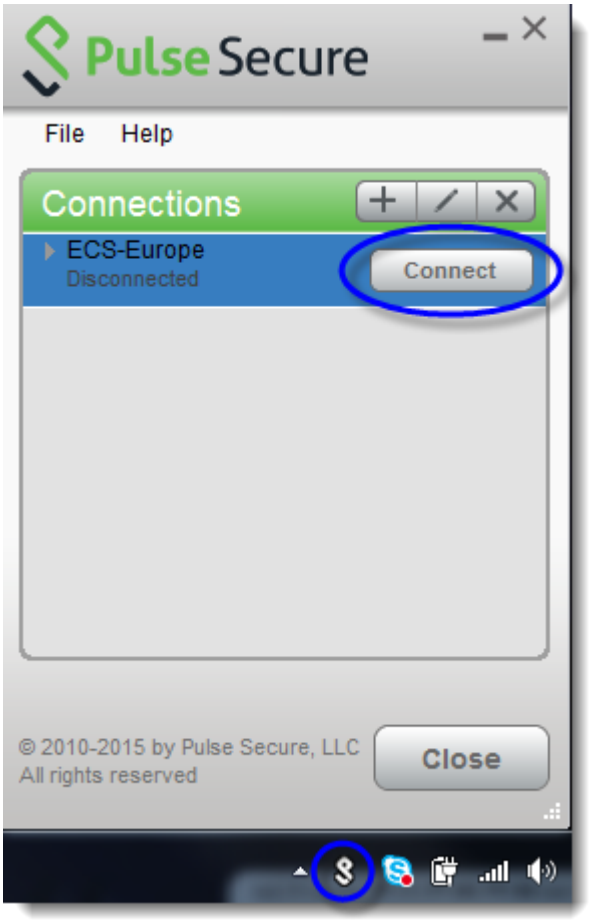
- Add your connection URL (https://xxxx.com) and save the connection. You should have received that information by mail from HCL support team or your contractor.
- In this use case we have added a connection called ECS-Europe.

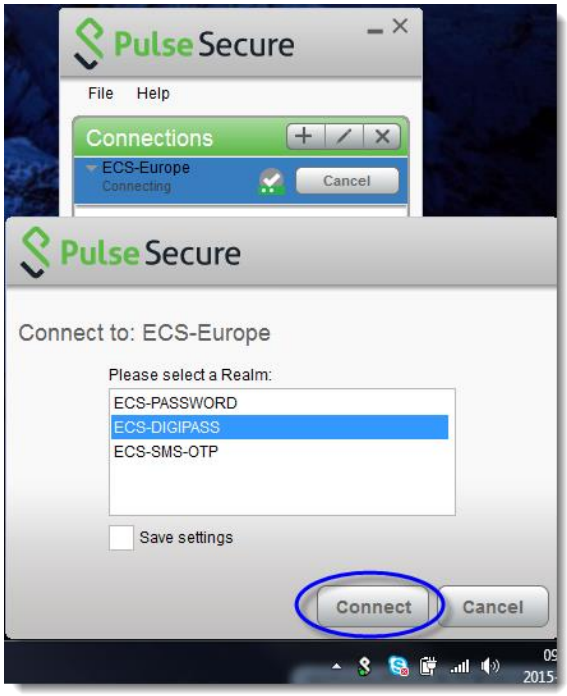


4. How to use ECS

4.1. Connect

- Open the Pulse Secure application, and click connect


Pulse Secure
File Help
Connections
ECS-Europe
Disconnected
Connect
© 2010-2015 by Pulse Secure, LLC
All rights reserved
Close


Pulse Secure
File Help
Connections
ECS-Europe
Connecting
Cancel
Pulse Secure
Connect to: ECS-Europe
Please select a Realm:
ECS-PASSWORD
ECS-DIGIPASS
ECS-SMS-OTP
Save settings
Connect
Cancel

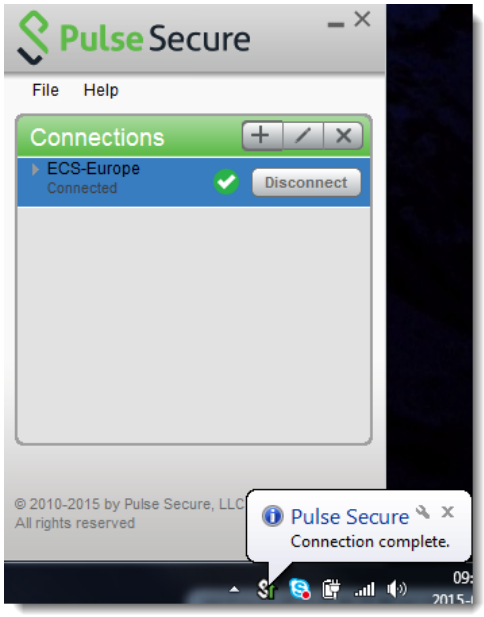
- If you have been told to use one time passwords using Digipass or SMS-OTP, you shall select ECS-DIGIPASS or ECS-SMS-OTP option.

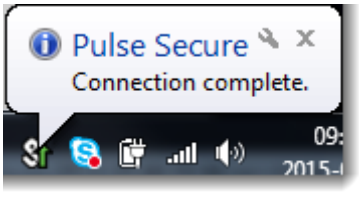
- Press the Connect button.

- Fill in the username and password/Digipass password, and press Connect.

If you login with SMS-OTP, a new window will be displayed to enter the OTPpassword, which you have received in your phone.

- The green sign indicates that you have a safe tunnel to the ECS gateway. The tunnel will only permit traffic to the resources that you are registered for. Traffic to all other resources will be sent out to the local network as usual (split tunneling).

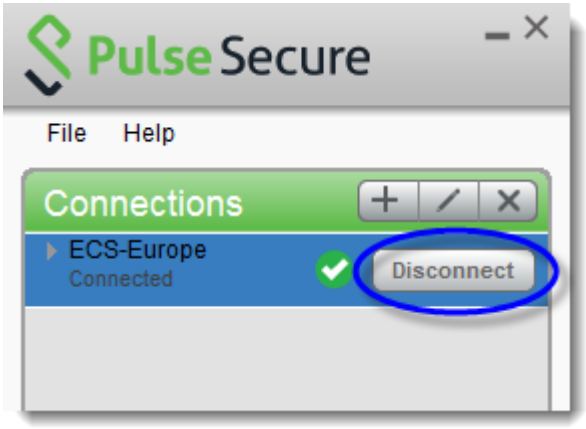




- You are able to resolve Internet as well as internal DNS names when connected.
- Start your applications or tools that you want to use. Traffic to all resources that you are allowed to reach will be sent down the secure tunnel to the ECS gateway and then further to the final destination.

4.2. Disconnect

Press the Disconnect button to log off and end the secure session.



5. Troubleshooting

5.1. Access denied – Invalid username or password

If you recently have received a new password make sure that you have changed the *initial password*. If you are using SMS-OTP to login, also ensure that your phone number is *registered* on your user account. If you are using hardware token and the onetime password does not work the token may not be properly *assigned* to your user account. You have to contact ECS support to sort this out.

5.2. SMS-OTP is not appearing

Note that the phone number format we register at the authentication server must meet the international notation (E.123) e.g. +22 607 1234567.
As a first act please read and if possible perform this step by step guide.
If the problem still persist:
There are many reasons why SMS-OTP does not work very well in certain countries or mobile networks but fortunately in many cases that problem is workable.
First and foremost you need to check that your telephone supplier is listed on mobile networks supported by Mideye.

If your supplier is found on the list above feel free to contact our SMS-OTP provider **Mideye** support and ask them what is happening with my SMS-OTP (they only need to know you phone number, that's all).
If it was not listed above you should ask them for help anyway because that is the only way to resolve the issue because of you most likely cannot change your telephone network supplier out of hand. The point is that **Mideye** support team has access to advanced tools and therefore able to resolve most of the SMS issues very quickly.
If you still are facing problems with SMS-OTP please contact ECS support.

5.3. Mideye+ for smart phones

Once the issue has been resolved (meaning you are able to receive atleast one SMS-OTP) and you are using **smartphone** it's strongly recommended to install Mideye+ as soon as possible. One SMS is still needed for activation of the app though.
The main idea of **Mideye+** is that it is primarily **passing the traffic to data channel** (mobile or Wi-Fi) which makes login less sensitive for SMS delays and other SMS delivery issues. On top of that **Mideye+** works in offline mode (as a token) as well. You simply set your smart phone in flight mode and use **manual signature** feature which is very useful at poor mobile coverage situations.

5.4. I cannot generate onetime password with my hardware token

Make sure that you have required pin code for your token. If the code is not available please contact ECS support.

5.5. I cannot reach my server through ECS

Ensure that correct IP, port and protocol is ordered for your ECS-group. If something is missing please contact the person who has placed the ECS order or ECS support.

5.6. I cannot reach my server through ECS, even though everything is correct in the ECS-group (IP, port and protocol), and my server is listening on correct port.

A firewall opening may be required in this case, depending on the circumstances. Please contact ECS support to investigate the need for a firewall opening request.

5.7. I can reach my server through ECS, but cannot login to the server

ECS only provides a communication link to the server, not the login itself. Please contact the server owner or contractor, you may need help with your credentials on that server.

5.8. I cannot reach out to VPN gateway from my company intranet

Ensure that your local firewall policies allows communication towards Internet via following port numbers and protocols:
TCP-port 264 and 443
UDP-port 500 and 2746