



ConSeal Private Links



[Introduction](#)



[Install/unInstall](#)



[Configuration](#)



[Passwords](#)



[Contacts](#)



[Reference](#)



[Glossary](#)



Introduction

[About ConSeal Private Links \(CPLinks\)](#)

[Comparison of CPLinks and VPN's](#)

[Who can see what I send and download on the Internet?](#)

[How will CPLinks help me?](#)

[What else will help make my communications private?](#)

[Who should not use CPLinks?](#)

Technical

[What kind of traffic can CPLinks send encrypted?](#)

[Why do I need to run ConSeal PC FIREWALL or ConSeal Private Desktop first?](#)



Install/unInstall



ConSeal Private Links (CPLinks) is supported by version 2.0+ of ConSeal PC FIREWALL and ConSeal Private Desktop. It creates a file named PLINK.CPS in the program's installation directory. The unInstall routine will not remove files that were not created during installation, so you will have to delete this file manually for a complete uninstall.



Configuration

To use CPLinks, you make a contact record and then connect. If you are setting up a server that is unattended, you set an "AutoConnect Password" that your contacts will use.

Contacts


A "contact" is another PC that you want to communicate with using CPLinks' encryption. You create the contact record for them, they create a contact record for you and then you both can connect. For more information about creating a contact record, click [here](#).

How to find someone's IP address

There are many ways to find an IP address. If you use IRC to chat, you can use the /DNS command in mIRC and other programs to find a person's IP address. Also, there is a very convenient service at <http://www.selfhost.com> where you can get your own domain free of charge, even if you are connecting to the Internet using a dial-up connection.


Connecting

Once you and your contact have made contact records, either one of you can start the connection.

To do it, you click on the contact entry in the list and then click the "Connect" button: . If CPLinks is not able to connect within 10 seconds, it will pop up a message saying so and the "State" changes from "Connecting" back to "Closed". If it does connect, the "State" changes "Connected".

Disconnecting

Either you or your contact can disconnect at any time. When you are disconnected, any communication you send is once again sent unencrypted. To disconnect, click on the contact

entry in the list and then click the "Disconnect" button: .

Once you are connected to your contact, only you and they can disconnect. The Disconnect signal cannot be spoofed easily by a hacker because it contains a "signature" that is based on session information as well as the Shared Secret, which is known only to you and your contact. This "signature" is verified before disconnecting. A Disconnect signal with an invalid signature is ignored.

CPLinks Password

In order to keep your contact information private, the Contact Records are encrypted on disk. A "CPLinks Password" is required when you first use CPLinks and this Password is used to make the encryption keys for encrypting the Contact List. Every time you run CPLinks, you must enter this Password to be able to access the Contact List. In order to use CPLinks without entering the CPLinks Password, you must set an AutoConnect Password.

AutoConnect Passwords

If you have a service that you want to run unattended, you can choose to enter an "AutoConnect Password". This is a password that your contacts can enter when they connect that allows a

connection to be made without you entering your main CPLinks Password. You must share this password with your contacts.

Configuring ConSeal Private Desktop (CPD)

When CPLinks is run, CPD will prompt you to ask if "PLINK.EXE" should be allowed to communicate. Choose "Yes".

Configuring ConSeal PC FIREWALL

You will need to allow CPLinks' connection traffic through the Firewall. It uses UDP port 4994 for both the remote and local ports. The local address will be "My Address". The remote address depends on how you want to control access. You can set it to one IP address, if you wish to allow just one site to try to connect. You can set it to "All Addresses" so that any IP address may try to connect. CPLinks' own authentication will prevent unauthorized people from connecting. You can set it to a range of addresses by using the mask field as described in the Firewall help.

You can also use the Firewall's Checked Learning Mode to help make this new rule. Run CPLinks and the Firewall will prompt you to allow this new traffic. Choose "Allow".

Making Services available only to CPLinks users

ConSeal PC FIREWALL v2.0 allows rules to apply only to CPLinks-encrypted traffic. For example, you can run an ftp server and make a Firewall rule to allow access to that ftp service only when the traffic is CPLinks-encrypted. Anyone who is not connected cannot access the service. Once they are connected through CPLinks, they can access it. If they are connected and accesses the service and disconnect, they are cut off from the service. This guarantees two things:

- 1) The service is available only to the people who are authorized (CPLinks contacts).
- 2) All traffic to and from this service is always encrypted.



Passwords

CPLinks Password

In order to keep your contact information private, the Contact Records are encrypted on disk. A "CPLinks Password" is required when you first use CPLinks and this Password is used to encrypt the Contact List on disk. Every time you run CPLinks, you must enter this Password to be able to access the Contact List. If you want to allow people to connect to you without having you enter the CPLinks Password, you must set an AutoConnect Password and give it to your contacts.

AutoConnect Passwords

If you have a service that you want to run unattended, you can choose to set an "AutoConnect Password". This is a password that your contacts can enter which will allow them to connect and it saves you from having to enter your CPLinks Password every time. You must share this password with your contacts.



If you set the AutoConnect Password and share it with contacts, you must ensure that nobody can get your Configuration File, named PLINK.CPS. This means your computer must be physically secure, so nobody else can use it. It also means you must ensure that nobody can access the file through a network connection. If you cannot ensure this level of security, do not use the AutoConnect Password feature.



Contacts

A "contact" is another PC that you want to communicate with using CPLinks' encryption. You create the contact record for them, they create a contact record for you and then you both can connect.

Click here for more information about:



[Creating a Contact Record](#)



[Editing a Contact Record](#)



[Deleting a Contact Record](#)



[Exporting a Contact Record](#)



[Importing a Contact Record](#)



[Connecting to a Contact](#)



[Disconnecting from a Contact](#)

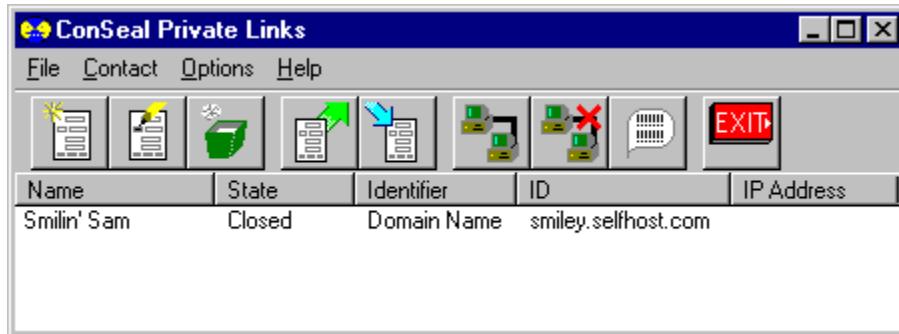


[Messaging a Contact](#)



[When is traffic encrypted?](#)

Reference







There are two main functions performed by the program: contact record management and connection management. There is also a menu option for getting additional help from CPLinks

Contact Records

Contact records can be added by creating or importing. It is easiest to have one person create a record and export it to the other, so they can import it. A connection cannot be made if the names and Shared Secret are not entered correctly. Records can be edited and removed.

Buttons for managing contact records are:

-  [Creating a new Contact Record](#)
-  [Editing a Contact Record](#)
-  [Deleting a Contact Record](#)
-  [Exporting a Contact Record](#)
-  [Importing a Contact Record](#)

Connecting and Disconnecting

Click on a contact and use the menu or Connect button to connect. Once you are connected, all the information your computers send to each other is encrypted. Once you disconnect, the information may be readable by other computers.

Buttons for managing connections are:

-  [Connecting to a Contact](#)



[Disconnecting from a Contact](#)



[Sending a Message to a Contact](#)

Unattended Connections

To automate an unattended system, you can use the "AutoConnect Password" feature. This is a password given to contacts to let them connect when you haven't entered your "CPLinks Password" yourself. This is useful for systems that must operate from bootup without user involvement. To set the AutoConnect Password, click Options/Unattended Connections.

Additional Help

To help with setup, there is a menu item called "Options/Tell me what's wrong". When you select this option, CPLinks provides more messages to help you understand why connections are not working.



Glossary

Under construction.



About ConSeal Private Links (CPLinks)

ConSeal Private Links is a PC-PC VPN (Virtual Private Network).

When you are connected to another PC in your Contact List, all the information you send and receive is encrypted. And this works for all applications that can communicate over the Internet, without modification. People cannot read what you are sending and cannot even be sure what kind of information you are sending: email, web browsing, file transfers, voice over IP, etc. While companies are linking networks with server-server and client-server VPN's, CPLinks is a "client-client" VPN, combining strong encryption and privacy with unparalleled flexibility and ease-of-use.

CPLinks has an important advantage over public key VPN's. By design, you and your contact are the only people who can decrypt what is sent. No need to trust a central site that must protect its server. With CPLinks, as long as you don't reveal your Shared Secrets, your link is safe.

Some uses for CPLinks:

- 1) Put a server (e.g. email, website, ftp) on the Internet where users must use CPLinks to reach it. With ConSeal PC FIREWALL and CPLinks on the server, only users with CPLinks connections can reach that service. All others are blocked and can't even see the service is there.
- 2) Chat with ICQ or IRC/DCC in complete privacy.
- 3) Encrypt voice-over-IP (VoIP) for private telephone calls.
- 4) Cable modem users whose Internet connection can be snooped by others in their area.
- 5) Ever wonder if your neighbors, ISP, or government are monitoring your Internet use? With CPLinks, they are shut out.

Limitations of CPLinks:

- 1) CPLinks only works with other sites that have CPLinks installed.
- 2) When using CPLinks for sending encrypted mail, remember that CPLinks encrypts the information during transmission and decrypts it at the receiving CPLinks platform. Any routing after that is "in clear" unless otherwise protected.



Comparison of CPLinks and VPN's

ConSeal Private Links (CPLinks) is a PC-PC VPN. Traditional VPN's, such as ConSeal VPN (a separate product), allow access to a network on the other end. CPLinks provides encrypted communications to the PC you are connected with. It does not support routing to other systems. The rule of thumb is:

If you can talk to a computer without CPLinks, you can talk to it encrypted with CPLinks.

ConSeal VPN

- client-server
- provides access to remote networks
- strong authentication, based on shared secrets
- supports strong encryption
- entire IP packet encrypted, hiding traffic type
- tunneled using TCP to prevent replay
- encryption keys can be tumbled
- not IPsec compliant (the mirage of VPN standardization), will be in the future
- client supports one VPN connection at a time

ConSeal Private Links

- client-client
- No
- Yes
- Yes
- Yes
- No (tunneled using UDP)
- No
- No (will be in the future)
- supports many connections at a time



Who can see what I send and download on the Internet?

The messages your computer sends are relayed through many "hops" before they reach their destination. Often it is a computer that routes the data packets. All these computers are networked together in what we call the Internet.

Each computer that relays a data packet can look at the message inside. Also, any computer on the same network segment can "listen" to the data packets that are going to neighboring computers and eavesdrop. On some (not all) cable modem connections, your neighbors can "listen" and get the data packets that others are sending, just as if they are on the same local area network (LAN). This shows that there are a lot of people in a position to monitor you while you use the Internet.

In comparison, telephone calls are more private. Most telephone companies recognize a person's right to privacy and rarely (in Canada and the US at least) listen to calls without a police warrant. Since your telephone call is routed through company equipment, you can have a measure of trust that they are not abusing their position. Cell phones and microwave towers broadcast your call for all to hear, so these are two notable exceptions.

Data on the Internet, however, is not limited to telephone company (or ISP) equipment. It can be relayed through universities, government sites, foreign countries and you have no say in this. Nor do you have a reliable method of knowing how it is routed, since the path can change from moment to moment. This anarchy in design means you are trusting complete strangers who have made no promise to you of privacy.

This design works because there is too much traffic on the Internet for (human) snoopers to read, but with the advent of computers being able to sift through messages looking for particular topics, it is now well within the capability of many countries to scan world-wide email systematically. Also, they can just as easily monitor chats using ICQ, IRC and other communication software.

You cannot use the Internet without the possibility of being monitored.

To address this, you can encrypt email so the receiver has to decrypt it. If you use direct chats (ICQ or IRC/DCC), then **CPLinks will encrypt that conversation right from your computer to theirs.**

How will CPLinks help me?

CPLinks encrypts what you send through the Internet. When you connect to another CPLinks user, all the traffic you send back and forth is private. It supports all Internet programs simultaneously and without modification. Also, you can have more than one private connection at a time. You can have a DCC chat in IRC while transferring a file from another CPLinks-protected site.

What else will help make my communications private?

There are two other broad categories of privacy tools: VPN's and data encryption.

VPN's (Virtual Private Networks)

Currently, VPN's are used to link home users to their office network or to connect remote sites, such as offices in different cities. When a home user connects through a VPN, all the computers in the office are now accessible, as if the user were in the office, right on the network. Signal 9's ConSeal VPN offers this capability. Also, two ConSeal servers can be used to link whole office networks.

CPLinks does not make a remote network available. It is a "client-client" design, in that it links two end users. It can be used to link many clients to a single server, however and if that server acts as a proxy, then it can make more services available to these clients, such as email.

Data Encryption

Applications can add encryption to keep the information private during transfer. Encrypted email is a good example. You can encrypt the message you send for it to be decrypted by the receiver. Also, data files can be encrypted before sending and decrypted when they are received.

CPLinks encrypt the information during transmission but it is decrypted by the far end.

Therefore, it could only be used to protect email if the far end were the email server. If the far end were just another step along the way, the email would be unencrypted and readable the rest of the way.

What kind of traffic can CPLinks send encrypted?

CPLinks can encrypt all IP traffic. IP is the Internet Protocol, so that means CPLinks can encrypt any traffic you can currently send over the Internet.

CPLinks cannot encrypt other type of traffic that could be sent through an internal network, such as IPX or NetBEUI.

Why do I need to run ConSeal PC FIREWALL or ConSeal Private Desktop first?

Plink has been designed as an add-on feature in the ConSeal suite of security products. It is designed to work closely with either ConSeal PC FIREWALL or ConSeal Private Desktop. It is not designed to run by itself. Without CPD or the Firewall running, CPLinks can connect but not send or receive encrypted traffic.

If you do not want to use packet filtering, you can:

- 1) In ConSeal PC FIREWALL, click **Rules** to see the "Control" page and unselect the "Firewall Up" option, or
- 2) In ConSeal Private Desktop, choose "Allow Everything".

Who should not use CPLinks?

You should not use CPLinks if it is against the laws of your country or if your employer has forbidden the use of encryption.



Creating a Contact Record

The dialog box titled "Contact Information" has the following fields and values:

- Contact Name: Bob
- Domain Name: bob.selfhost.com
- Shared Secret: a phrase that nobody can guess
- My Name: Alice

Buttons: OK, Cancel, Help

Alice's contact record for Bob

The dialog box titled "Contact Information" has the following fields and values:

- Contact Name: Alice
- Domain Name: alice.selfhost.com
- Shared Secret: a phrase that nobody can guess
- My Name: Bob

Buttons: OK, Cancel, Help

Bob's contact record for Alice

Both you and the person at the other computer make a contact record that allows you both to connect. In the diagram above, two people, Alice and Bob, are making contact records.

Contact Name: Alice puts in "Bob" for the contact name and Bob puts in "Alice". This name is not case-sensitive, so if Bob put "alice" or "ALICE", it would be OK.

IP Address, Domain Name or Any Address: If they had fixed IP addresses, they could put them in directly (IP Address is ...) but for this example, Alice and Bob are using dial-up where they have a different IP address every time they connect. So, they use the service at <http://www.selfhost.com> to get a domain name assigned when they are online. That way, CPLinks can find their IP address and connect them. If Alice were hosting a server for many people to connect to, then she could put "Any Address", since the IP address of the system that is connected is never known or needed.

Shared Secret: They enter exactly the same thing here. The Shared Secret is used to make the encryption keys so, ultimately, the privacy of their communication relies on nobody else learning or guessing this secret information. This secret phrase is case-sensitive, which means Alice and Bob must use exactly the same characters. If Alice typed "A phrase.." and Bob typed "a phrase..", they could not connect, because the "A" and "a" are not considered the same.

My Name: This is the name you are known by. In the example, Alice puts her name and Bob puts his. You don't have to use your real name. Also, you don't have to use the same name as you used in other contact records. You do have to share this name with your contact, however, so they can use it as the **Contact Name** in their record. This name is not case-sensitive, so if Bob put "bob" or "BOB", it would be OK.



Editing a Contact Record

Contact Name

Domain Name is

Shared Secret


My Name

To edit a contact, highlight the entry in the Contact List and then click the Edit button: .

For a description of what must be entered, click [here](#). To save changes, click OK. Click Cancel to close the Contact Information window without saving the changes.




Deleting a Contact Record

To delete a Contact Record, highlight the entry in the Contact List and then click the "Remove contact" button:  .



Connecting to a Contact


Once you and your contact have made Contact Records, either one of you can start the connection (as long as the Contact Record contains the IP Address or Domain Name). To

connect, highlight the entry in the Contact List and then click the "Connect" button: . The "State" will change to "Connecting". If CPLinks is not able to connect within 10 seconds, it will pop up a message saying so and the "State" changes from "Connecting" back to "Closed". If it does connect, the "State" changes "Connected".



Disconnecting from a Contact


Either you or your contact can disconnect at any time. When you are disconnected, any communication you send is once again sent unencrypted. To disconnect, highlight the contact

entry in the list and then click the "Disconnect" button: .

Once you are connected to your contact, only you and they can disconnect. The Disconnect signal cannot be spoofed easily by a hacker because it contains a "signature" that is based on session information as well as the Shared Secret, which is known only to you and your contact. This "signature" is verified before disconnecting. A Disconnect signal with an invalid "signature" is ignored.



Messaging a Contact

You can send messages to your Contact once you are connected. To do this, click on the "Send Message" button: . Type in a short text message (less than 438 letters) and click the OK button to send it. It will appear as a small popup window on your contact's screen.


When is traffic encrypted?

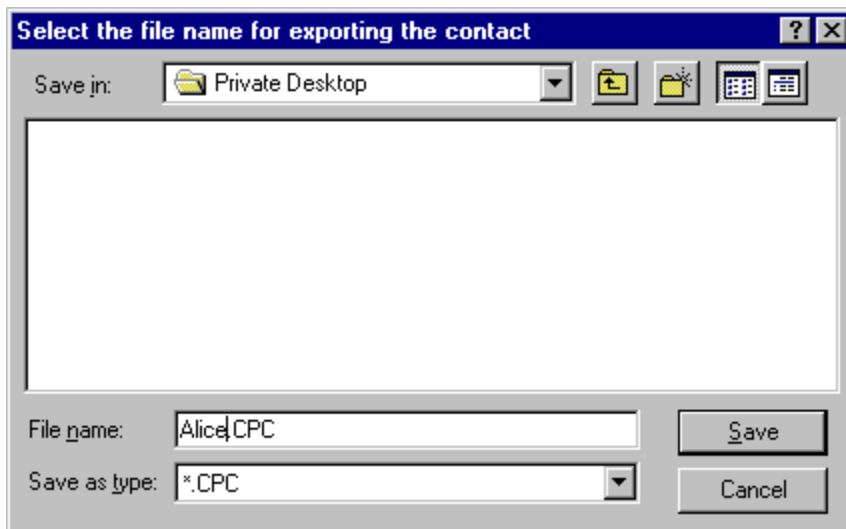
Traffic to and from your contact is encrypted when CPLinks shows the status as "Connected". At any other time, it is sent "in the clear". The applications you are using will probably continue to communicate if you disconnect in CPLinks (unless a ConSeal PC FIREWALL rule allows a service only through a CPLinks-encrypted link).



Exporting a Contact Record

The easiest way for two people to share contact information is for one person to create it and send it to the other. If Alice makes a contact record for Bob, she can export it so that Bob can [import](#) it. Once they each have a contact record for the other, they can connect.

To export a contact, highlight the entry in the Contact List and then click the Export button:  . You are prompted to choose a file name to save it in:



You can choose any file name you like, but CPLinks uses the name you choose for yourself in the Contact Record. The name is limited to 8 characters, so if you used the name "Alice N. Wonderland", the proposed file name will be "Alice_N.CPC".

After selecting a file name, you are asked to supply your address and to choose whether to include the Shared Secret in this exported record:



Since your copy of a Contact Record contains the Address of the person you want to connect with, the record you export to them should contain your Address, if you want them to be able to connect to you. If you are always the one to initiate the connection and if you may be connecting

from a different IP address every time, then you should leave it set to "Any Address". Otherwise, you should replace "Any Address" with "IP Address" and choose your IP address from the popup list on the right, or you should choose "Domain Name" and enter your domain name, for example "alice.selfhost.com".


Consider carefully whether you want to include the Shared Secret in the record you export. All the security of your connection relies on this being kept private, so you shouldn't simply send it in email, for example. If you can send the export record securely, then it makes sense to include the Shared Secret. Some methods of sending the exported record are:

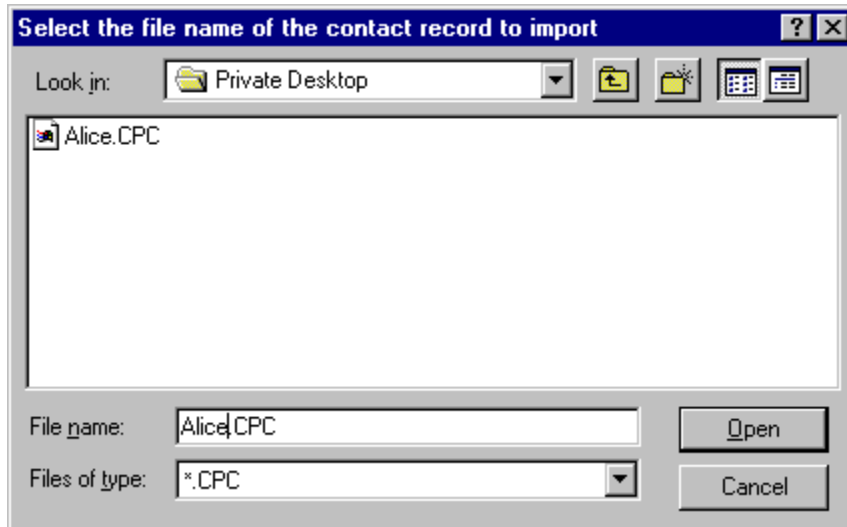
- 1) Encrypted email
- 2) As an encrypted file, sent as an attachment in email.

You can send the export record unencrypted if it does not contain the Shared Secret. You could give the contact the Shared Secret over the telephone, if you consider it safe.



Importing a Contact Record

To import a Contact Record, click the Import button: . You are prompted to choose the file containing the record:



Once you choose the file, the record will appear in your Contact List, with the name of your contact appearing in the first column ("Name" column).

You should edit the record to check that the Shared Secret is set. If it is not, then you should get it from your contact and enter. Also, check to see if the record shows "Any Address", "IP Address" or "Domain Name". If this record is to allow people to connect from anywhere, then it should show "Any Address". This means you won't be able to initiate the connection, however, since the record doesn't indicate how to find the contact. If you need to initiate the connection, you will need your contact's IP address or domain name. They can find this by clicking on Help/What is my IP address in the CPLinks menu.

Edvard Munch, *The Scream*.
This picture indicates comments
for the highly security-conscious.

Shared Secret

The Shared Secret is used by CPLinks during connections to generate encryption keys. It is very important that you and your contact keep it secret because anyone knowing it can use it to decrypt the encrypted traffic. It is recommended that you change your Shared Secret regularly, just as you would change a password.

The Shared Secret should be a string of letters and numbers, much like a password. You should not use one or two words or names or anything that could be guessed. It is recommended that you make it more than 10 characters, using numbers of other keyboard characters than letters.

The Shared Secret is case-sensitive. That is, upper case (capitol) letters are considered different than lower case (small) letters.



A guessable Shared Secret can be the weakest point for a snooper to target. If they can guess it, it is possible for them to decrypt your messages. The longer the Shared Secret, the better.



It is actually a lot of work to guess and then decrypt messages. The caution above is to guide you into safe practises.

Buddha

This picture indicates comments
that remind you not to worry.

