



HyBlue IceLock QuickStart

Overview

IceLock's Untethered Data Security approach takes the guesswork out of configuring and installing powerful data security. The installation process has two steps remaining:

1. Install and run the Customer Configuration Application
2. Install IceLock on each computer and run the Computer Security Application

These steps explained in more detail below will automatically create a comprehensive key system with complete management of keys.

Customer Configuration Application

The file you are now downloading will unpack a number of files including the Customer Creation Application (CCA), the IceLock client installer and IceLock documentation.

The IceLock Customer Configuration process is a simple 5 step process. The steps are:

1. Create a unique Customer Private key
2. Create a unique Customer Public key
3. Create a group of public and private keys for each computer IceLock will be subsequently installed on
4. Send the computer keys to HyBlue's servers for use when you install IceLock on computers
5. Store the Customer Private Key safely for later use.

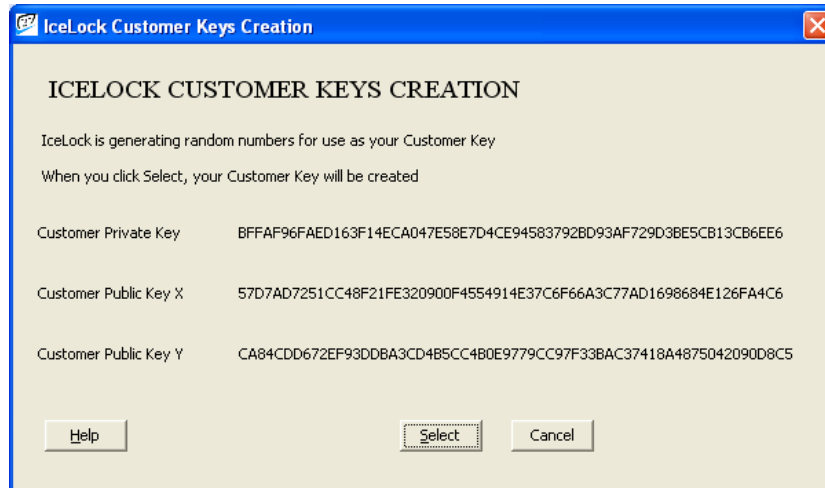
You should run the software first on an administrator's computer to configure the keys for your users.

Simply double click on the file you have downloaded to start. When the files are all unpacked, the CCA will automatically launch and step through the key generation process. The CCA starts with the welcome screen shown below:

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com

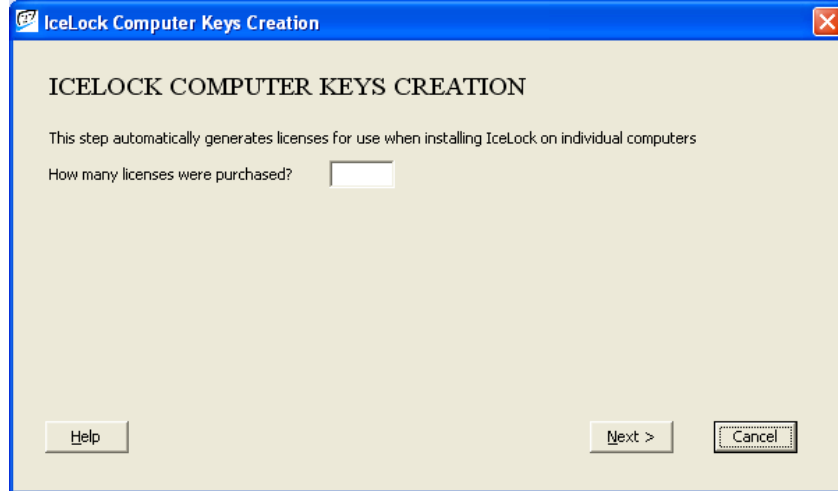


The welcome screen lays out the process. Clicking Next brings up the following screen:



To ensure each customer has a unique set of keys, random numbers are generated continuously until you click Select. Clicking Select assigns the Customer Private and Public keys. You will save the Customer Private Key later; all other keys are stored by HyBlue. After clicking Select, click Next. You will see this screen:

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com



Enter the number of licenses you purchased on this screen and click Next. IceLock will now generate your computer specific keys:



The keys are automatically generated and prepared for uploading to HyBlue's servers. Clicking Next will bring up this screen:

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com

© 2008 HyBlue, Inc. All Rights Reserved. HyBlue and the HyBlue logo are registered trademarks of HyBlue, Inc. All other trademarks and registered trademarks are the property of their respective owners.



To simplify the installation process on each computer, the computer specific keys are stored on HyBlue's servers and automatically assigned each time a new computer is installed. The computer specific keys are protected by the Passphrase you enter here. You will use this Passphrase each time you install IceLock on a computer to verify an authorized installation, however the Passphrase is never used to encrypt data on any computer. Click Next.

You can also specify that every user must use a secondary password. Secondary passwords protect the secure virtual disk in case the Windows password is hacked. Checking the Require Secondary Password mark enforces this higher level of security.

Clicking Next transmits the keys and security preference to HyBlue's servers. You can monitor the progress as shown below:

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com

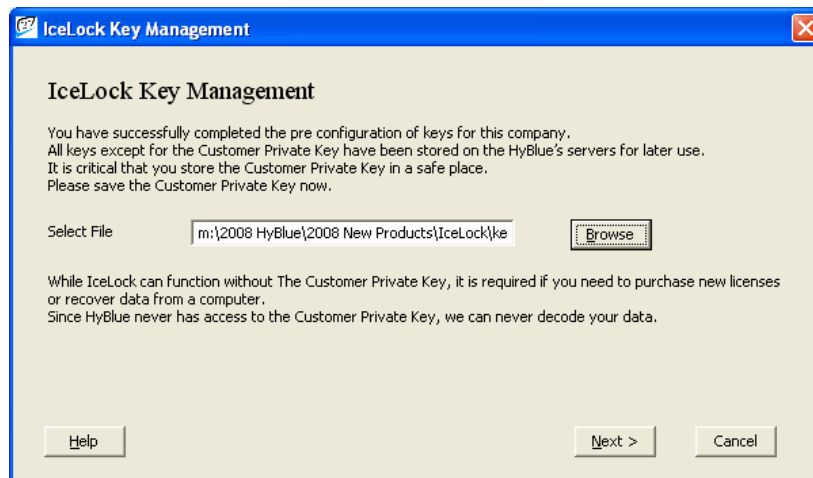
© 2008 HyBlue, Inc. All Rights Reserved. HyBlue and the HyBlue logo are registered trademarks of HyBlue, Inc. All other trademarks and registered trademarks are the property of their respective owners.



The keys have been successfully uploaded to HyBlue's servers and are now available for individual computer installation. Make sure you record the Passphrase for later use. Click Next to continue.

The final configuration step is to store the Customer Private Key safely. This Private Key is never sent to HyBlue which means that HyBlue can never decrypt any of your data or provide a replacement if it is lost. Normal use of IceLock is possible without the Customer Private Key, however, the Private key is required to purchase additional licenses or recover data. It is critical that you keep the Customer Private Key safe. For more information on key storage, see Best Practices for Key Management below.

The next screen stores the Customer Private Key to a location you specify:

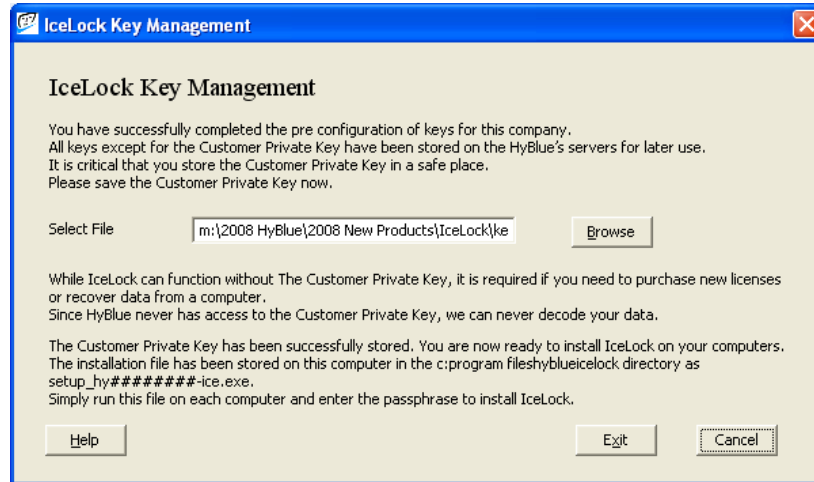


HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com



Browse to a location and store the Private Key.

When you see this screen:



The IceLock configuration is complete and ready to install IceLock on individual computers.

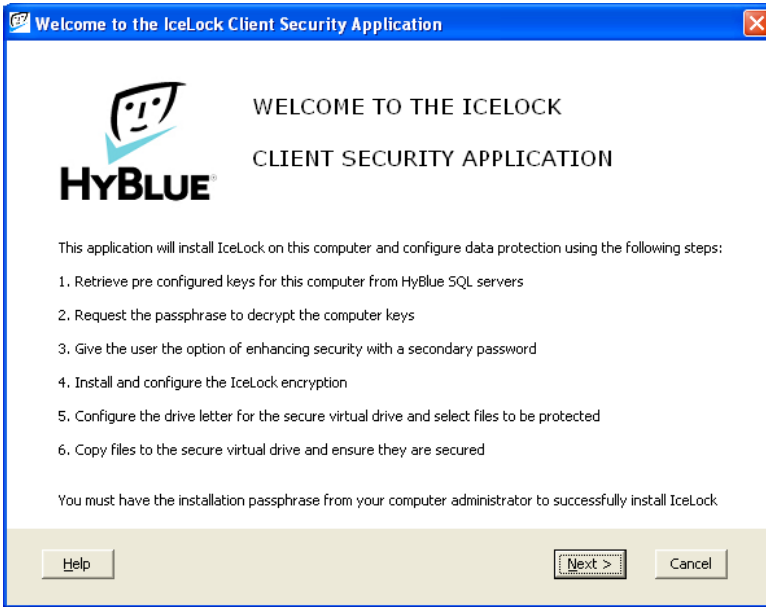
Computer Installation

To install IceLock, each computer must run the setup file stored which was stored in the C:\Program Files\HyBlue\IceLock directory during the CCA operation. The file will be named setup_hy#####-ice-win.exe where ##### is a unique number identifying each customer. Please do not rename the file.

This file should be copied to a convenient network share location or copied to some portable media to take to each computer. The installation requires the computer to be online but is not dependent on Active Directory.

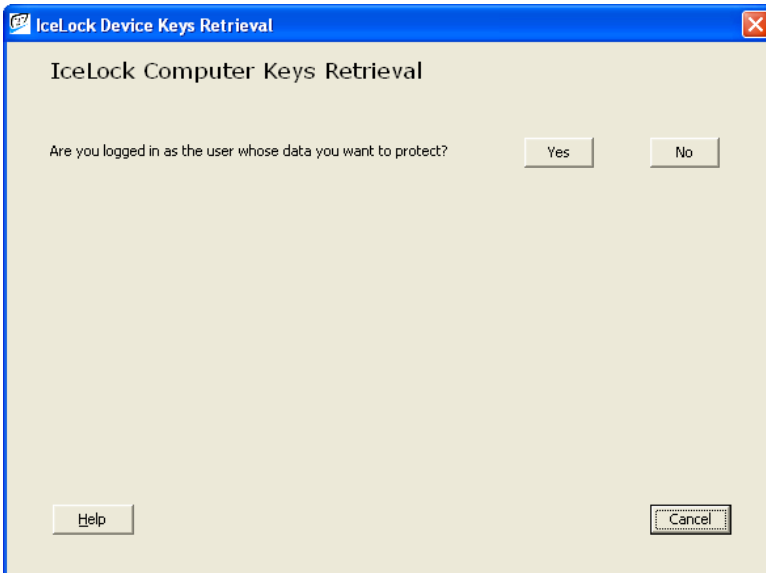
The installation unpacks the files and then displays the Computer Security Application welcome screen shown below:

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com



Click Next to start the configuration process. If all of the licenses purchase have been used, you will be taken to a web page where you can purchase of more licenses.

Since IceLock is user centric, you must be logged in as the correct user. This screen ensures you are logged in correctly:



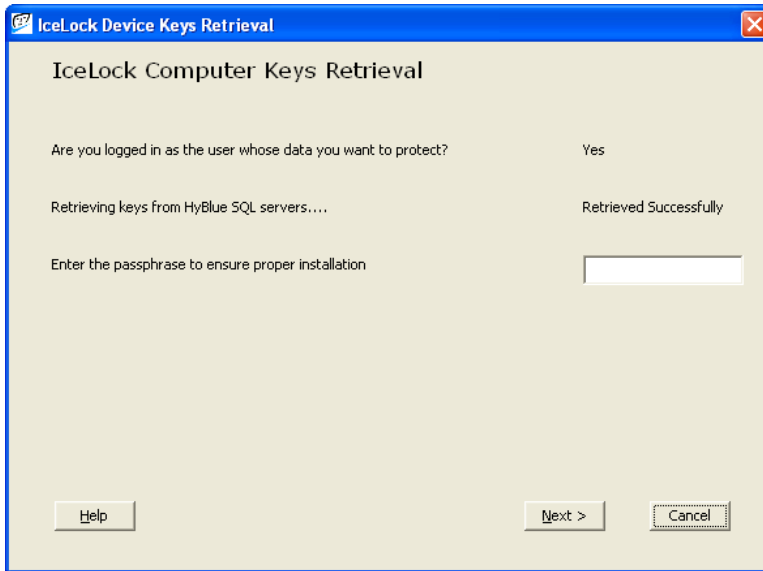
HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com

© 2008 HyBlue, Inc. All Rights Reserved. HyBlue and the HyBlue logo are registered trademarks of HyBlue, Inc. All other trademarks and registered trademarks are the property of their respective owners.



If you are not logged in correctly, please click No, then End. Logout and log back in and the CSA will automatically start again.

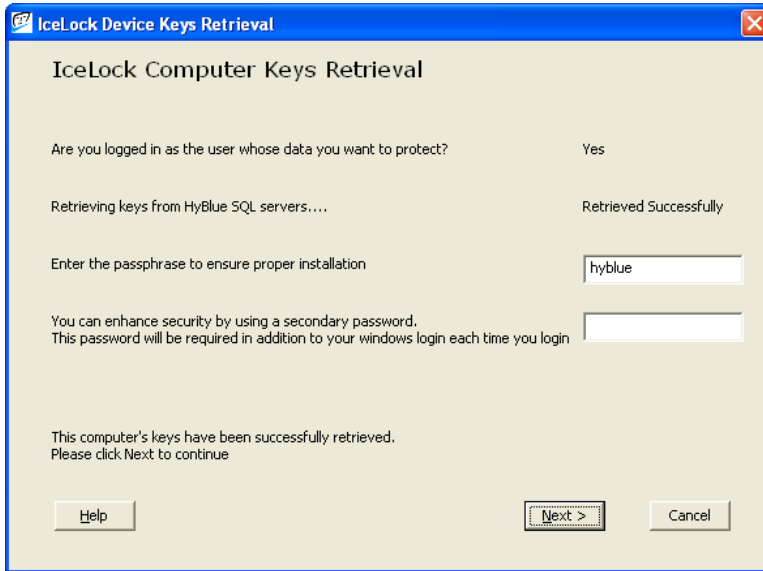
The CSA downloads a set of keys for this computer and requests the installation passphrase that was created during configuration with the CCA. Remember, this phrase is not used to encrypt any computer data, only to authenticate the installation and decrypt these keys. Please enter the passphrase as shown:



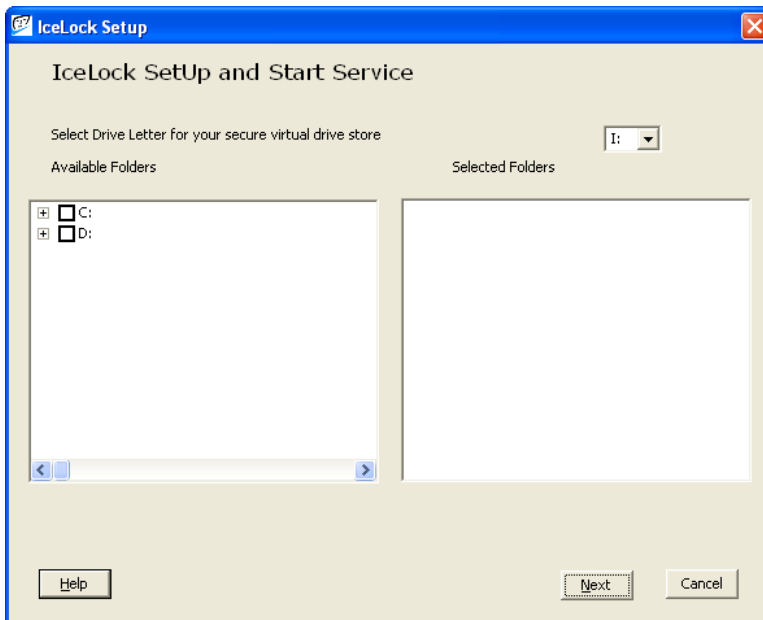
If you selected mandatory secondary passwords while running the CCA, the user must enter a secondary password to proceed. If you did not select mandatory, the user can optionally select a secondary password. The secondary password extends IceLock's protection by requiring another password once the user is logged in to access the secure virtual disk. Secondary passwords can be added at a later time.

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com

© 2008 HyBlue, Inc. All Rights Reserved. HyBlue and the HyBlue logo are registered trademarks of HyBlue, Inc. All other trademarks and registered trademarks are the property of their respective owners.



Next you are asked which drive letter to use for the secure virtual disk. The default drive is I, but can be changed to any available drive letter. Once this is done, the CSA automatically scans the C disk for data files and recommends directories that should be protected. By default the "My Documents" directory is suggested. You can select other drives and directories as needed. Additionally, OST/PST and swapfiles are automatically encrypted in place by IceLock.



HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com



Once you have confirmed the data you want protected, the CSA measures how much disk space is used by those files and suggests a partition size twice as large as the existing data. If there is not enough space on the hard disk you will be warned to create more space or you can enter a smaller size for the partition. You can override the size selection as well.

When you accept the partition size, the partition is automatically created, named and formatted. After formatting the files selected are copied over to the secure disk.

When the copy process is complete, you are shown a side by side listing of the files and directories from the original location and those in the secure virtual disk. You can view all files protected or select to show only the difference between the source and destination. Once you have confirmed that data files were copied correctly, the original data files are erased using a multi pass erase for security.

[insert image]

If the My Documents folder was included, the registry is updated to point to the new drive location for My Documents.

The computer is now protected with IceLock.

Using IceLock

IceLock is designed to be easy to use and not intrude on normal computer use. Simply open files the way you normally do; from inside an application or from Explorer.

To get started simply login into your computer. If you did not setup to use a secondary password, the secure virtual disk will automatically load and your data is available. If you configured a secondary password, you will be asked to enter that password and your data is available.

IceLock Management

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com

© 2008 HyBlue, Inc. All Rights Reserved. HyBlue and the HyBlue logo are registered trademarks of HyBlue, Inc. All other trademarks and registered trademarks are the property of their respective owners.



IceLock's online management lets you control a computer's response to potential unauthorized use. From HyBlue's web portal you can select a variety of settings that are automatically downloaded to each computer you own.

The table below shows the settings available, their default setting and the range of settings:

| Setting | Default Value | Minimum Value | Maximum Value | Function |
|------------------------------------|---------------|---------------|---------------|--|
| Action to take if computer stolen | Delete Key | | Delete Data | This determines if the encryption key is deleted when a stolen computer comes online. Deleting the Key is a recoverable selection. Deleting Data will delete all protected data. |
| Login Failures before key deletion | 5 | 3 | 9 | This is for both Windows login and secondary key login if used. The technician is notified if the computer is online, the technician needs to re-enable login after this occurs. |
| Days offline before key removal | 21 | 5 | 99 | The computer will automatically delete the key if offline more than this value. If the device comes back online and is not listed as stolen it automatically resets the key to allow use |
| | | | | |

Key Management Best Practices

In traditional encryption systems a great deal of time and effort is expended to ensure that keys are implemented correctly, tracked, inventoried and secured. IceLock removes this burden with the exception of one critical component.

The Customer Private Key is generated by the CCA when first setting up a new customer. While this key is not required during normal use of IceLock it is critical in two specific instances.

1. Adding new keys to the system. If 100 keys were originally purchased and 50 new keys are required, the private key must be accessed by the CCA to generate the new device keys.
2. Data recovery. The IceLock system allows network administrators to recover data from a secure virtual disk by linking the Customer Private Key to specific public keys available from HyBlue. This allows recovery of data if a computer cannot boot, in many circumstances, as well as

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com



recovery when an employee leaves and doesn't share their secondary password.

The Customer Private Key must be stored by the customer as it is never shared with HyBlue. By not sharing the key with HyBlue, the risk of compromise from HyBlue or someone who compromises HyBlue is removed.

Key Management in the case of IceLock becomes simply keeping a copy of the Customer Private Key safe and with the customer. It should not be shared with anyone, it should be stored in a safe electronic location or locations for the customer. Since the key is simply a long alpha numeric string it can also be printed out and saved in hard copy. It is tedious entering such a key but it can be done so having a paper backup locked in the company files is a good last ditch backup.

To summarize, key management is greatly simplified with HyBlue IceLock. There is a data file that should be stored by each customer. This file should be stored in a safe electronic location either a floppy disk or CD. The file can also be printed out and filed in a safe location at the customer's office as a last ditch backup.

With these backup solutions in place, adding new licenses or recovering data becomes a very simple operation.

Troubleshooting and Support

While every effort has been made to create a quick and easy installation process, there are certain issues which are known to create problems during the installation. HyBlue maintains a support site at <https://www.hyblue.com/CustomerTools/support.aspx>. You need to be logged in to access this site.

Thank you for using HyBlue's services. If you are running a free trial, you will be notified as the trial is coming to a close so that you can register your software and continue to use IceLock. If you are an existing customer, you will be invoiced for computers that are on the system as of the 1st of the next month.

If you have further questions on the installation of HyBlue software, please contact HyBlue Support at 206.838.7238 or support@hyblue.com.

HyBlue Inc. 5 West Harrison, First Floor. Seattle, WA 98119
206.838.1907, Sales@HyBlue.com www.HyBlue.com

© 2008 HyBlue, Inc. All Rights Reserved. HyBlue and the HyBlue logo are registered trademarks of HyBlue, Inc. All other trademarks and registered trademarks are the property of their respective owners.