

Iron Mountain's DataDefense Service Frequently Asked Questions

Software Overview

1. [How can the DataDefense solution protect my company?](#)

The DataDefense software ensures that sensitive data stored on desktops, laptops and tablet PCs will not fall into the wrong hands even if the computer itself does.

2. [How does the DataDefense application work?](#)

DataDefense secures access to sensitive data on your computer by detecting user behaviors which are inconsistent with expected norms, an indicator that unauthorized persons may be attempting to access the device. Once this behavior is detected, sensitive data files are destroyed based on a pre-determined set of rules that cover both location and depth of destruction.

More specifically, files are protected by encryption and destruction. Before your device is ever lost or stolen, the administrator can download pre-set rules which inform the device software to take destructive action under specified conditions. Thus, the device is prepared to protect itself when an unauthorized access attempt occurs. Additionally, if the lost device ever communicates with the server again, the client software can be instructed to immediately destroy sensitive data.

3. [How does the DataDefense product differ from other security products available?](#)

Many security products concentrate on preventing the loss or theft of your computer. Other security products rely on encryption alone to prevent access to data on a lost or stolen device. The DataDefense solution provides data security by encrypting and destroying sensitive data even when you are no longer in possession of the equipment.

4. [Are any of the data or device degradation options available with DataDefense reversible? If so, which ones? How?](#)

For file encryption, only the person who is logged on to the machine and users listed as "Data Recovery Agents" can decrypt files. The certificate and key used for encryption can be exported to a removable storage device and used to recover the files. When the device is put into persistent shutdown, usage can be restored with a proper high-speed connection to the DataDefense server.

5. [Will the DataDefense software be available for export?](#)

Yes.

6. [Does the export restriction of 128-bit encryption affect the DataDefense software?](#)

No. All communications are secured by SSL. Our encryption is based on Microsoft's EFS (Encrypting File System) technology which is built into the operating system. Microsoft ensures EFS is export-compliant by meeting U.S. government controls.

7. [I have multiple operating systems on the same computer and one of the operating systems is not supported by the DataDefense product. How will DataDefense protect my data if the wrong operating system is used to login to the system?](#)

Data files created under the Windows operating system and saved in folders protected by encryption using the DataDefense software will be encrypted and unusable by an intruder using another operating system.

8. How will software updates to the DataDefense client be made?

Software updates and patches to the DataDefense client will be made available automatically through the server.

Installation

1. How long does it take to install the DataDefense software?

Assuming that Iron Mountain will be hosting the DataDefense server, the client software setup and installation takes about 10 minutes.

2. How do I install the DataDefense client software over a dial-up connection?

If you are using dial-up to connect to the internet, do the following:

1. Perform the client installation as described in the welcome letter
2. Restart the Computer.
3. After restart, use the Task Manager to end the process called MonitorConsole.exe.
4. Establish a dial-up connection.
5. Lock the computer (by pressing Ctrl-Alt-Delete and clicking Lock Computer).
6. Use Ctrl-Alt-Delete to log on to the computer (this will automatically restart MonitorConsole.exe and complete the installation).

3. What are the installation requirements for the DataDefense client software?

- o Windows 2000 with Service Pack 4 or later or Windows XP Professional with Service Pack 2 or later
- o Microsoft Windows .Net Framework Version 1.1 or later
- o 10 MB disk space
- o 256 MB of RAM
- o Single user per device
- o Unique machine name
- o Periodic network connection to the Internet

To enable encryption on the device:

- o NTFS formatted drives
- o EFS certificate for the provisioned Windows logon account

For Novell networking environments:

- o Novell Client for Novell Networks 4.9.1

4. How much hard drive space is required to install the DataDefense client software?

Approximately 10MB are required for the client install of DataDefense.

5. What operating systems are supported by the DataDefense client software?

Windows 2000 with Service Pack 4 or later

or

Windows XP Professional with Service Pack 2 or later

6. How much RAM is required to install the DataDefense client software?

A minimum of 256MB of RAM is recommended to install the DataDefense client on your device.

7. What skills are required to install the DataDefense client software?

You need administration privileges on the client computer to install the software. The client software uses a standard Windows installation package.

8. How can I uninstall the DataDefense client software?

As with most Windows programs, an uninstaller will be included with the DataDefense software. However, if you try to uninstall the application before your client has been deactivated at the server, the uninstall will fail. This prevents a thief from removing the software to disable the DataDefense service.

Those wishing to delete the DataDefense application from their machine must contact the administrator first so that they can deactivate the client device on the server. When this step has been completed, the client software can be uninstalled using the DataDefense uninstaller.

Networking and Servers

1. What is the load on the network when using the DataDefense service?

Each client machine checks in with the DataDefense Server approximately once per hour. This transaction is very light and occurs at different times for each client. Network load scales geometrically as more machines are added. During installation and when new rules are downloaded, the network payload is larger. However, these events occur infrequently and should not significantly impact network traffic.

2. Which network services are used by DataDefense?

Secure .NET web services are used for communication by DataDefense.

Software Operation

1. DataDefense needs the computer name and the user name of a computer before it can operate on that device. How can I tell what the computer name and user name are for my device?

You will need to know your computer's Windows System Name (we call "Machine Name") and User Name in order to install the DataDefense client. These can be found by clicking "Start", "Programs", "Accessories", "System Tools", and then "System Information."

2. How can I change the name of the computer that the DataDefense client will reside on?
 1. Open the Control Panel.
 2. Click on the System icon.
 3. Click on the Computer Name tab.
 4. Click on the Change button.
 5. Enter the new name in the Computer Name field and click OK.

3. Will daylight savings time trigger the DataDefense client to perform an action?

No. The DataDefense software has been written to recognize daylight savings time and will not trigger any client actions.

4. I am traveling to foreign countries and will be using my laptop during the trip. I want to set the time to the current time in whatever country I am in. Will that cause DataDefense activation to occur?

You can protect yourself against DataDefense activation if instead of changing the time on your computer, you change the time zone. In other words, if you have traveled from San Francisco to Denver and want your computer to reflect the new time, change the time zone from Pacific to Mountain. This can be done from the Time Zone tab of the Date and Time icon within the Control Panel.

5. For a machine which has DataDefense installed on it, how can I have data destroyed on this device as soon as possible?

Assuming your company has chosen to use DataDefense's built-in groups and rules, the quickest way to force destruction on a device is to mark it 'Stolen'. Marking the device 'Stolen' will move the device from the 'Active' group into the 'Stolen' group. Once the device checks in, all the built-in destruction rules assigned to the 'Stolen' group will operate on the device.

6. What events trigger a DataDefense client computer to check in with the DataDefense server?

The DataDefense client will check in when any of these events occur:

1. System Startup
 2. New Network Connection
 3. System Shutdown
 4. Login Attempt
 5. Pre-set interval as defined by the administrator
 6. Locking and unlocking of the device
-

7. My users' screensavers automatically locks their computers. If we are running the DataDefense software, will these computers check in when the screensaver locks their systems?

If a screensaver locks the DataDefense device, the device will check back in when the end user successfully logs back on to the system.

8. What happens if the Num Lock or Caps Lock keys are on when a user types in a password during login? Will the DataDefense software trigger any events?

No. The supported Microsoft operating systems offer a safeguard to users who have left the Num Lock or Cap Lock keys on during login. If one of these keys is on during the login process, an error message will be displayed notifying the user of this fact. The end user will not be allowed to continue entering their password until these keys have been turned off.

9. What is the desktop interface for the DataDefense client application?

The DataDefense client does not have a desktop interface. The DataDefense client runs in the background transparently. An administrator must use a web-based interface to set up rules for the client.

10. When a user logs on to a device which has the DataDefense client installed on it, an error message says that the security log is full and that an administrator needs to clear the log files. What does this mean and why did it happen? How do I clear the security log?

Some users who have the DataDefense client installed on their computer will generate enough security events over time to fill up the Windows security log. This is especially true if the end user spends time testing various rules scenarios.

To clear the security log, one must have administrative privileges on the device. Most end users do. Once an administrator is logged on to the device, they can clear the security log by:

1. Click Start.
2. Click Control Panel.
3. Click on the Administrative Tools icon.
4. Click on the Event viewer icon. This will bring up the event logs of the computer.
5. Click once on the Security Log to highlight it.
6. Click on the Action menu and select Clear All Events.

If you would like to prevent the log from filling as quickly in the future, with Security log highlighted, click on Properties in the Action menu. Here you can adjust the size of the log. Make it larger so that it fills slower. You can also select how it will overwrite entries in the log. To avoid problems, especially during testing, one can select to have events overwritten if needed.

11. With DataDefense, can I set a threshold for check-in time so that I can execute different rules based on how long it has been since someone has checked in?

Yes, thresholds for check-in times are included with the product.

Encryption

1. Is EFS's (Encrypting File System) 128k encryption sufficient for my device?

In general, the answer is yes. The default algorithm for Windows 2000 and Windows XP is DESX (128k). If the enterprise wishes to employ more powerful encryption, the Windows XP operating system includes support for Advanced Encryption Standard (AES) using a 256-bit key (this is the default algorithm for Windows XP Service Pack 2 and Windows Server 2003). For users requiring greater symmetric key strength with a FIPS 140-1 compliant algorithm, the 3DES algorithm can also be enabled.

2. I can still open the file(s) encrypted by DataDefense using the appropriate applications. How can I tell if my files are truly encrypted?

In both Windows 2000 and Windows XP Professional, the original user that set the encryption bit will be able to seamlessly open the file – even without unsetting the encryption bit.

To validate whether a file is really encrypted, create a copy of the encrypted file, unset the encryption bit of the copy and copy both files to some other media (diskette, shared network drive, USB flash, etc.). Now, attempt to open the files as a different user (than the one that created/encrypted) the files. The unencrypted version should open normally while the encrypted version will generate an error message telling you that you do not have access privileges.

For Windows XP Professional only, you can tell if a file is encrypted if the file name shows up with a green tint in the directory listing of the Windows Explorer. Again, the end user who encrypted the file will be able to open it seamlessly.

3. Some of our computers are shared by two users and the device is protected by DataDefense. Why can't one user access another user's files on this computer?

More than likely, the other user's files are encrypted. The key to decrypt a file is unique for each user on the computer. Therefore, only the user who encrypted the file will be able to view that file.

The user who encrypts a file can allow additional users to view the file as well. To do this:

1. Right-click on the file that you want to add an additional user to and select Properties.
2. Click on the Advanced button.
3. Click on the Details button in the Compress or Encrypt Attributes group. This will open a new window.
4. In the new window, click on the Add button.
5. Highlight the person that you wish to add and then press the OK button. In most cases you will probably have to do a search for the person that you are trying to add.

For additional help on encryption, see Microsoft's documentation for EFS.

4. Does DataDefense offer support for any other forms of encryption besides EFS?

DataDefense does not prohibit an end user from using some other form of encryption to protect their data files. The caveat is that DataDefense cannot initiate these other forms of encryption at this time.

5. How can I learn more about Microsoft's Encrypting File System (EFS)?

See Microsoft's website for more information:

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/encrypt_overview.msp

Rules

1. What rules are available with the DataDefense software?

There are six types of rules you can create with DataDefense, each with their own purpose.

- o Invalid Login
- o Date and Time
- o Out of Contact
- o Unrecoverable
- o Device is Lost
- o Device is Stolen

Additionally, DataDefense provides Built-In Rules by pre-configuring device settings for each of these rules (except Date and Time).

2. What are the possible consequences of a rule violation when using the DataDefense software?

There are five actions taken when thresholds are reached based upon escalating risk:

1. Warning message (optional)
2. Shutdown
3. Persistent Shutdown
4. Encryption key destruction
5. Data elimination

3. How can I make the DataDefense client delete all files inside of a folder?

When adding a location for the DataDefense delete action to work upon, add a *.* to the end of the directory path. The asterisk character is the equivalent of the wild card character in the Windows operating system. If you don't include the *.* in the directory path, you will still be deleting all the files within the folder, but you will also delete the folder itself.

4. How can I make the DataDefense client delete all files inside of a folder and the folder itself?

When adding a location for the DataDefense delete action to work upon, end the chosen directory path with a backslash. If you include the *.* character set or any kind of file designation after the backslash, only those files will be deleted and the folder itself will be left alone.

5. My DataDefense account is hosted with Iron Mountain. How do I access the DataDefense server to change or update the rules for my account?

Authorized administrators can access their administrative account via the DataDefense web interface. A user ID and password will be needed to access the devices, groups, data sets, and rules that the administrator is responsible for.

Security and Settings

1. Is DataDefense susceptible to SAM (Security Account Manager) attacks?

No. If you are using a device which meets the operating system requirements for DataDefense (Windows 2000 or XP), then the SAM file will be encrypted. Our recommendation is to upgrade to Windows 2000 or XP and enable Microsoft's Encrypting File System (EFS). This would prevent someone from accessing the encrypted files even if they used a utility to delete the SAM file.

2. What is a SAM (Security Account Manager) attack? How does upgrading my operating system help prevent such an attack?

The SAM (Security Accounts Manager) database stores hashed copies of users passwords. A SAM attack is the attempt to recover the passwords of the users from the SAM database.

On older operating systems, the SAM is not encrypted and accepts the user's hashed password instead of the password itself. By upgrading the operating system to Windows 2000 or XP, the users' passwords will be hashed in the SAM database and the database will be encrypted. In addition, Windows 2000 and XP will not accept the hashed password as a valid password entry.

3. One of the trigger events for DataDefense is when the device does not check in according to schedule. If someone stole the computer and did not connect to the network or Internet, eventually data destruction would be initiated based upon elapsed time. Why couldn't the thief just set the clock back to keep DataDefense from destroying the data?

DataDefense automatically triggers data destruction if the time, date, or year is significantly modified.

4. What happens when a machine is booted from a floppy? Will this beat the DataDefense software?

Booting your computer from a floppy disk will not circumvent the Possession Status Mechanisms (PSM) that is in place.

5. DataDefense offers overwrite capability from one to eight times. How many times should sensitive corporate data be overwritten before it is safe from hackers?

The US Department of Defense standard is seven times, but some corporations see this as excessive.

Each time you overwrite a bit, you have a 25% chance of scrambling any one specific path to reconstruct the data. The minimum number of times you need to overwrite a bit to destroy all bits is four times. The odds of at least one path never getting touched in four consecutive wipes are 42%. The odds, however, of recovering large sequential chains of data are much lower.

6. Let's say I have triggered a file deletion process on my machine protected with the DataDefense product. What happens if I shut off the computer while it is performing the file(s) deletion?

The next time the device is turned on, DataDefense will continue the deletion process where it left off.



About Iron Mountain

1. How do I contact Iron Mountain?

You can contact us through our website at:

www.ironmountain.com

Use the web forms to reach the department you are interested in contacting.

Or call us at 800-899-IRON

2. What kind of support does Iron Mountain offer for its products and services?

Iron Mountain offers live technical support 24 x 7 x 365 at 800-888-2774 or system.support@ironmountain.com

3. How much does it cost for support for Iron Mountain products and services?

Technical support is free of charge provided you have purchased an Iron Mountain product or service.

