



ProtectFile 3.6.0 Release Notes

Version: 3.06.00, Build 8
Release Notes Issue Date: 09/19/2008
Last Updated: 04/02/2008

Product Description

ProtectFile is an encryption application that enables protection of sensitive data. This protection can be applied selectively to single or multiple directories, either locally or on a server.

Version Summary

Release Description

This release adds support for Vista installations and includes several bug fixes.

New Features and Enhancements

This release includes support for ProtectFile on 32-bit Vista operating systems.

Released Components

ProtectFile for Windows 2000/XP/Server 2003/Vista:

Supported Platforms for Client Management (on Server)

- Windows 2003 Server, Service Pack 2

Supported Platforms for Client Management (on Server)

- Windows Server 2003, Service Pack 2

Supported Platforms for Client

- Windows 2000 Pro, Service Pack 4
- Windows Server 2003, Service Pack 2
- Windows XP Home, Service Pack 3
- Windows XP Pro, Service Pack 3
- Windows Vista 32-bit, Service Pack 1

Advisory Notes

- ProtectFile can utilize smart cards and tokens to provide two-factor authentication and to protect sensitive information in the user configuration on client machines and in the ProtectFile Management Console (MC) database.

Most Cryptographic Service Providers (CSPs) provided by the smart card manufacturers implement the functionality required by ProtectFile. Please refer to the specific smart card manufacturer's documentation for instructions on installation of their runtime environment (RTE) and associated utilities. Refer to the *ProtectFile Administration Guide* for details on a number of CSP and PKCS#11 configuration settings.

The following table provides an overview of the tokens and smart cards supported by this ProtectFile release. Not all tokens and smart cards are covered in the regression tests of each release. If you experience problems, contact SafeNet Support.

| Model | Information |
|---|--|
| SafeNet Borderless Security Smart Card 330 | SafeNet CIP Utilities BSEC 7.1.1_0006 1024- and 2048-bit RSA keys supported |
| SafeNet iKey 2032 | SafeNet CIP Utilities BSEC 7.1.1_0006 1024- and 2048-bit RSA keys supported |
| Aladdin eToken R2 | "eToken Base Cryptographic Provider", RTE 3.65 (4.5 for Vista) |
| Aladdin eToken Pro | "eToken Base Cryptographic Provider", RTE 3.65 (4.5 for Vista) |
| Other supported smart cards include: <ul style="list-style-type: none"> • ActivCard Gold • A-Trust • CryptoVision • Infineon SICRYPT • RSA Passage • Schlumberger Cyberflex • Siemens CardOS • Spyrus Rosetta | |

- ProtectFile Business PKCS#11 version is not supported in this version.
- Moving files into an unregistered domain/envelope with the **AccessControl** parameter set to 2 or 3 (Remote Access allowed) results in the file being moved into the domain without being encrypted. This file will appear corrupted when opened by a user with the domain registered. This file can be reconstructed by disabling the driver and copying/moving it out of the domain.
- Issues may arise when mixing the use of FQDN and NETBIOS naming conventions when mapping drives or creating envelopes on DFS links. Logging off and restarting ProtectFile will resolve this issue.
- When using tokens/smart cards to authenticate in a PKI environment, the token/smart card must be available for use when any modification to the envelope status and/or network configuration has changed.

- Network configuration changes include a change in the client's drive mappings and/or a change in the active target of a DFS link/root. In these cases, ProtectFile needs to verify the client still has access. To do so, require the token/smart card to be available and logged in. The **PKITimeOutBehaviour** setting of 1 (Ignore Timeout) is not supported in this environment and should not be applied.
- ProtectFile Premium envelopes created or removed in folders that can be accessed while offline (i.e., offline folders) must be created or removed while the folder is online. If envelopes are created or removed while the folder is offline, the envelope tag file may not be replicated correctly.
- Do not use the DFS root folder to map DFS shares. Ensuring that the mapping is to a DFS link in the DFS root or below will ensure that ProtectFile is able to correctly resolve the DFS path.
- The ProtectFile GINA logon for ProtectFile Business with PKCS #11 tokens may stall if the supplied token does not contain any keys.
- To access domains on mapped network drives which become available after ProtectFile has started, double-click on the ProtectFile system tray icon and re-enter the password.
- If a program resides within a domain, and the program is launched from the startup folder or the *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run* registry key, then the access control feature for that domain or envelope must be disabled.
- When creating a user profile with a transport key for ProtectFile business (CSP version), a previously created transport key must be selected. Selecting the **Automatic** option can cause ProtectFile failures when attempting to logon with the user token.
- Automatic domain creation on a shared network folder fails silently if a user does not have permission to write to the shared folder.
- After migration from ProtectFile Business to Premium, single DES envelopes may be incorrectly shown as 3DES envelopes in the **Envelope/View** dialog.
- The PKI recovery agent is defined in the registry setting:
HKEY_LOCAL_MACHINE\Software\Eracom\ProtectFile\Policy\RecoverAgent. If the recovery agent user is changed or removed from the PKI directory, this registry entry must be manually updated to reflect the change.
- When using token logon in conjunction with Windows Remote Desktop, the logon container name is advertised differently by the CSP when logging on to the same machine via Remote Desktop. The logon container name is stored in the user's profile after the first logon, which leads to authentication failures when logging on to a machine locally and remotely.
- When specifying a script file on the Protect File command line, the fully qualified name should be used or the script file should reside in the same folder as the ProtectFile executable (ProtectF.exe).
- When specifying exclusions in a script with the **CreateEnvelope** command, the '!' character is used as an exclusion separator character. Therefore, you cannot use the '!' character in the name of any exclusions.
- Protect File will log all parsing and functional errors when processing scripts. However, if the warning level is set to greater than 0, the user will only be notified that parsing errors have occurred. If any functional errors occur (such as failing to find a certificate to add a user), these errors will be logged, but the user will not be notified.
- The Trend Micro OfficeScan Real Time Scan feature fails to detect viruses in encrypted files when the files are on a remote machine and are accessed over the network.

- A user may end up with encrypted data in registered envelopes or get immediately deregistered from an envelope just created. This can occur when a user is using multiple certificates issued on different tokens and smart cards or different machines when using software CSPs. This occurs because ProtectFile will select the certificate with the latest effective date for envelope encryption, and might therefore not have access to the corresponding private key.
- When using DFS shares with ProtectFile Business CSP licenses, it may be necessary to periodically log in as the domain password user associated with the token or smart card.

Resolved Issues

| Severity | Classification | Definition |
|----------|----------------|---------------------------------|
| C | Critical | No reasonable workaround exists |
| H | High | Reasonable workaround exists |
| M | Medium | Medium level priority problems |
| L | Low | Lowest level priority problems |

| Issues resolved in this release | | |
|---------------------------------|----------|--|
| Issue | Severity | Synopsis |
| 32716 | M | More accurate viewing of large number of domains/envelopes |
| 33405 | M | Improved LDAP functionality with registry entries |
| 36146 | M | |
| 35592 | H | Enhanced ProtectFile silent installation regarding the "GINA" msi argument |
| 38812 | M | ScrCtrl.exe utility improvement |
| 40098 | L | Better handling of file date/time when updating envelope.sys |
| 40239 | H | DFS Folder can be renamed in offline mode |
| 41460 | H | Greatly improved efficiency when handling very large files |
| 41482 | H | Enhanced capabilities with multiple certificates on a token or smart card |
| 41946 | L | Improved administration dialog regarding users |
| 42143 | M | PFGINA with Management Console – enhanced recovery handling |
| 42269 | H | PFGINA with Management Console – improved password synchronization |

Known Issues and Workarounds

| Known issues from this release | | |
|--------------------------------|----------|---|
| Issue | Severity | Synopsis |
| 37189 | M | Summary: Installing Protect File with invalid license keys could give the message: "Can not find dll or other derived DLL. Process will terminate!" Workaround: Remove and reinstall Protect File using valid license keys. |
| 31905 | M | Summary: Deleting a user profile using the Master Console did not delete the local cached copy (secondary profile). Since the secondary profile still existed, the user login occurred. Workaround: The user's secondary profile must be removed manually by selecting the file and deleting it. |
| 33059 | L | The same folder can be added as an 'Exclusion' with UNC path and mapped path. |
| 33102 | L | A limited user does not have access to view exclusions. |
| 33470 | H | Summary: Removing an existing domain removes exclusions inside that domain. Workaround: Copy information within the exclusion to an alternate location. |
| 33500 | L | Protect file allows a user to login if a certificate has expired. |
| 33836 | M | Summary: A limited user in Protect File cannot administer own domain. Workaround: The domain can be administered by an administrator. |
| 33988 | L | Summary: An incorrect message ID displayed when a Register Domain action is cancelled. Workaround: Acknowledge the message and continue. |
| 34305 | L | Summary: Protect File Premium fails after removing an envelope with more than 2 GB of data. Workaround: Deregister the added envelope by selecting Envelope > De-Register . |

Publications

The publications associated with this release are:

- ProtectFile Administration Guide, 007769-001 (Rev C, August 2008)
- ProtectFile Business User Guide, 007771-001 (Rev C, August 2008)
- ProtectFile Management Console Tutorial, 008031-001 (Rev B, August 2008)
- ProtectFile Management Console User Guide, 007772-001 (Rev B, August 2008)
- ProtectFile Premium User Guide, 007770-001 (Rev C, August 2008)