idera™

TOOLS FOR SQL SERVER,
SHAREPOINT, AND POWERSHELL

SharePoint encrypt
Release Notes

For Version 1.8

idera™

Revision history

Version	Date	Comments required	Approvals required
1.8.0.42	November 8, 2012		

SharePoint encrypt Release Notes

November 8, 2012

idera™

Table of Contents

Introduction

Thank you for choosing Idera for your security needs and welcome to the Version 1.8.0 Release Notes. Please carefully read the Release Notes and other sections of this documentation. If you require any additional assistance or need to submit any comments about this document please contact us according to the information contained in the Contacts section.

Nomenclature

This document uses the following fonts and styles:.

Table 1 Document nomenclature

Style	Description
Text	**Bold** text indicates the name of a menu option of other graphical user interface (GUI) component.
Text	Text that is **bold and underlined** indicates important information.
Text	Text in *Italics* indicates a file or folder name
“Text”	“Quoted” text indicates a value to enter into a text field or other input. When entering the value do not include the quotation marks.
Text	Underlined text indicates a link to another section of the document, an email address, or website.
`Text`	`Text in Courier New font indicates command line syntax to execute`

Release Notes

Please carefully read this section before attempting to install or configure the Idera software.

Version 1.8.0 introduces the following new features and enhancements. Please see the resolved issues for fixes included in this release. **For all new features, please see the known issues sections.**

- support for encrypting SharePoint lists
- support for SharePoint 2010 Claims-based authentication
- an option to allow SharePoint administrators to view the list of items in a secure List or Library without being able to view encrypted content.
- support for clients running Windows XP
- more granular debugging options
- minor usability enhancements to the SharePoint encrypt Console

SharePoint encrypt Service

Idera SharePoint encrypt is a complete data security solution for Microsoft SharePoint environments. It combines strong encryption and key management to secure sensitive content on SharePoint servers. It allows you to specify optional user access lists that differ from your basic SharePoint permissions setup. The SharePoint encrypt Service keeps files secure from unauthorized users including Windows and SharePoint administrators with privileged user access rights. At the same time, it ensures that authorized users have easy, transparent access to their information.

Supported Platforms

You can use the SharePoint encrypt Service software on the following platforms:

- SharePoint MOSS 2007 SP2 hosted on the following:

- Microsoft Windows Server 2003 , 32-bit edition and 64-bit edition
- Microsoft Windows Server 2003 R2, 32-bit edition and 64-bit edition
- Microsoft Windows Server 2008, 64-bit edition
- Microsoft Windows Server 2008 R2, 64-bit edition
- X86 based processors only. Itanium processors are not supported.

- SharePoint 2010 Standard and SharePoint 2010 Enterprise hosted on the following:
  - Microsoft Windows Server 2008 64-bit edition Original
  - Microsoft Windows Server 2008R2, 64-bit edition
  - X86 based processors only. Itanium processors are not supported.

Product Limitations

- The SharePoint encrypt Service encrypts the following file types. Please contact customer support if you need support for file extensions not listed.
  - ".accdb", ".accde", ".accdt", ".accdr"
  - ".c", ".cpp", ".cs"
  - ".doc"".docx", ".docm", ".dotx", ".dotm"
  - ".mdb"
  - ".pdf",".png",".ppt", ".pptx", ".pptm", ".potx", ".potm", ".ppam", ".ppsx", ".ppsm"
  - ".rtf"
  - ".txt"
  - ".vba"
  - ".xls", ".xlt", ".xlsx", ".xlsm", ".xltx", ".xltm", ".xlsb", ".xlam",".xml"
  - ".zip"

- The SharePoint encrypt Service **does not** encrypt files of the following types:
    - .aspx
    - .css
    - .gif
    - .jpg, .jpeg, .js
    - .png
- The SharePoint encrypt solution cannot encrypt the following List types
    - Discussion Board
    - Survey
    - Tasks
- The SharePoint encrypt Service will only encrypt text-based columns in a List such as Notes, Single line of text, Multiple lines of text, etc. This limitation is to avoid having to change the format of the column (e.g. a "Number" column must be converted to "Single line of text" since any encrypted value is a string).
- The SharePoint encrypt Service does not support encrypting InfoPath forms that are submitted to a web service.
- Content from encrypted files does not appear in search results - unless the document title is meaningful to the criteria. This means that you cannot search for the contents of an encrypted file. By design, search routines are not able to access the documents while they are encrypted.
- Excel files encrypted by the SharePoint encrypt Service are not compatible with SharePoint Excel Web Services. You can instead edit the file directly in Excel or check out and download the Excel file to make your changes to the file.
- The SharePoint encrypt Service cannot decrypt files that are accessed via the SharePoint API. (47, 111)

Known Issues

- SharePoint encrypt does not support Forms-Based Authentication in SharePoint/MOSS 2007. (J156)
- You must install the Windows Identity Framework on each of the SharePoint Web Front Ends if you are using SharePoint 2010 Claims or Forms Based Authentication (CBA, FBA) and you intend to create CipherPoint access control lists that contain Active Directory Groups. (700)
- By default, the SharePoint encrypt Service installer binds the agent to port 80. If you want to protect a site on a different port number or you have multiple web applications on port 80, please see Verify the SharePoint encrypt Service Installation in the User Guide. (136)
- You must install the SharePoint encrypt Service using Domain Administrator rights when installing on a Windows Server host that is part of an Active Directory domain. (314)
- After editing an encrypted Microsoft Office document with clients running Windows XP and Office 2007, the new version of the file will not be re-encrypted in real-time. The file will get encrypted a short time after saving it to the secured library. This issue does not occur with clients running either a newer operating systems or MS Office 2010. (681)
- With SharePoint 2007, encrypted InfoPath forms will not be decrypted when users access the form using the InfoPath client. To work-around this issue, either edit the InfoPath form in browser-enabled mode or download the form and edit it offline. (683)
- When building a Specify Users policy for a web application that uses Windows Live ID, use the Unique ID values instead of the account names. For example, build the access control list using the value 000300081234@live.com instead of jsmith@live.com. Under some situations, both values will be available in the SharePoint encrypt Console. (624)
- With the 'Allow View' option enabled, an administrator can open a secured document library in Windows Explorer and attempt to delete a file. The file will not be removed but the user will not get a permission denied or other error message. (689)

- If you create a document workspace from a file in a protected library, the workspace does not inherit the protection of the originating location. You need to create an additional rule in the SharePoint encrypt Console to secure the new workspace after you create it. (85)
- The SharePoint encrypt Service only encrypts the current file version. Old revisions of files are not encrypted automatically.
- Unauthorized users can view the list of files in secured libraries when the users browse the library with a web part. The contents of encrypted files are inaccessible even if the file names are visible. (141)
- You cannot use URLs that are not specified in the Alternate Access Mappings to access content in protected libraries. You should make sure that the short and fully qualified hostnames are properly configured in the AAM settings when appropriate. (198)
- If a library has the SharePoint setting **Require content approval for all submitted items** enabled then any existing files will be checked out after protecting a library for the first time. (J120)
- The SharePoint encrypt Service will deny all access requests if you apply a Specify Users access control list that contains no entries. This is by design. (402)
- If a file or list item is encrypted with a deactivated encryption key an authorized user may download or view the file or item but the SharePoint encrypt Service will not, due to policy, decrypt the content. The SharePoint encrypt Console will display a severity two message to indicate a denied access request to deactivated data. (499)

Resolved Issues

- Previous, a client computer running Microsoft Windows XP could no directly edit an Office document stored in a protected SharePoint library. (189)
- The document check-in screen would not appear after you upload a file to a secured library. Users will now receive the check-in prompt, as expected. (223)

- Previously, SharePoint encrypt Service encryption capabilities did not interoperate with SharePoint Lists.
- SharePoint encrypt now supports claims-based authentication in SharePoint 2010 installations. (335)
- Users could not use the **New Document** button in the SharePoint ribbon to add new content to a secured library. (5)
- The SharePoint System Account would be denied access even if that account were authorized using a Specify Users access control policy. The user of the SharePoint System Account in ACL policies is now fully supported. (528)
- The SharePoint encrypt Service will now encrypt a published document. (522)
- The SharePoint encrypt Service will enforce Specify Users policies that rely on nested Active Directory groups. For performance reasons, however, the access control processing will only traverse 3 levels of nested groups. (J117, 526)

SharePoint encrypt Console

SharePoint encrypt Console provides advanced key and security management capabilities for SharePoint encrypt Service.

Supported Platforms

You can use the SharePoint encrypt Console on the following platforms:

- Microsoft Windows 7 64-bit edition
- Microsoft Windows Server 2008 64-bit edition
- Microsoft Windows Server 2008 R2 64-bit edition
- X86 based processors only. Itanium processors are not supported.

Product Limitations

- The SharePoint encrypt Console does not support the following features. These features will be available in a future release.

- You cannot manage multiple farms from a single SharePoint encrypt Console.(100)

Known Issues

- SharePoint encrypt solution does not support Forms-Based Authentication in SharePoint/MOSS 2007. (J156)
- When running the SharePoint encrypt Console for the first time, the Console administrator will receive an error that the Topology file is missing. Click the **Get Topology** button on the **Control Panel** tab request the list of topology items (e.g. web applications, site collections, sites) from the SharePoint farm. (782)
- The On some systems, the SharePoint encrypt Console may not be able to read the pre-existing logs file after upgrading to 1.8.0. To resolve this issue either delete the file *C:\Program Files (x86)\Idera\SharePoint encrypt\log.xml* or simply restore the log.xml file from the copy you made prior to upgrading. (635)
- A user must have access permission for the SharePoint encrypt Console installation folder and registry to run SharePoint encrypt Console. (234)
- If you refresh or filter the logs in the **Logs** tab on the SharePoint encrypt Console, a null reference exception can appear. This error appears due to a bug in the DataGridView control. If the error appears, wait a few moments and refresh or filter again. You can also navigate to a different tab, and then return to the **Logs** tab. (310)
- The SharePoint encrypt Console does not allow account names longer than 10 characters. (373)
- The SharePoint encrypt Console may crash if you install it on a virtual machine that was restored from snapshot. This occurs due to resource issues on the hypervisor. If this happens, uninstall and reinstall SharePoint encrypt Console. (409)
- The SharePoint encrypt Console will not display trusted domains in the **Location** drop-down when browsing Active Directory to create a Specify Users access control policy. (J111)
- When attempting to browse a domain that is unavailable, the SharePoint encrypt Console may erroneously report that the

logged on Windows account does not have permissions to the domain. (J117)

- If the SharePoint encrypt Console and SharePoint encrypt Service host systems use different time zone settings there will be a delay in validating the license file. Please make sure that the SharePoint encrypt Console host server uses the same time zone setting as the servers in the SharePoint farm. (J102)
- When using a license file that was created prior to the release of version 1.8.0, the number of allowed Web Front End servers will be displayed as "Unlimited" in the Control Panel tab in the SharePoint encrypt Console. (532)

Resolved Issues

- You can enter a hostname or IP address when SharePoint encrypt Console prompts you to register a SharePoint encrypt Service even though registration by hostname is not allowed. (142)
- The solution would retrieve SharePoint topology (list of sites, users, etc.) on regular intervals which could result in high resource utilization on farms with a large number of site collections. The SharePoint encrypt Console now only requests topology after the initial installation of the software and then when a SharePoint encrypt Console administrator clicks the **Get Topology** button the **Control Panel** tab. (368,591)
- On some systems the SharePoint encrypt Console would fail to load a new license file. (581)
- The SharePoint encrypt Console would not install on non-US versions of the Windows operating system under certain conditions. (481, J82)

Contacts

You can reach Idera technical support via phone or email.

support@idera.com

(713) 523-4433