idera™

TOOLS FOR SQL SERVER,
SHAREPOINT, AND POWERSHELL

SharePoint encrypt
User Guide

For Version 1.8

Revision history

Version	Date	Comments required	Approvals required
1.8.0.38	October 30, 2012		

SharePoint encrypt User Guide

October 30, 2012

where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

Table of Contents

Introduction

Thank you for choosing Idera for your security needs and welcome to the Version 1.8 User Guide. Please carefully read 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

We use the following fonts and styles in this document.

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`

Theory of Operation

This section describes how SharePoint encrypt delivers security capabilities to SharePoint servers and content.

Idera's technology enables authorized users with need to know to transparently store and share their content while allowing privileged administrators to manage the SharePoint infrastructure without viewing sensitive content.

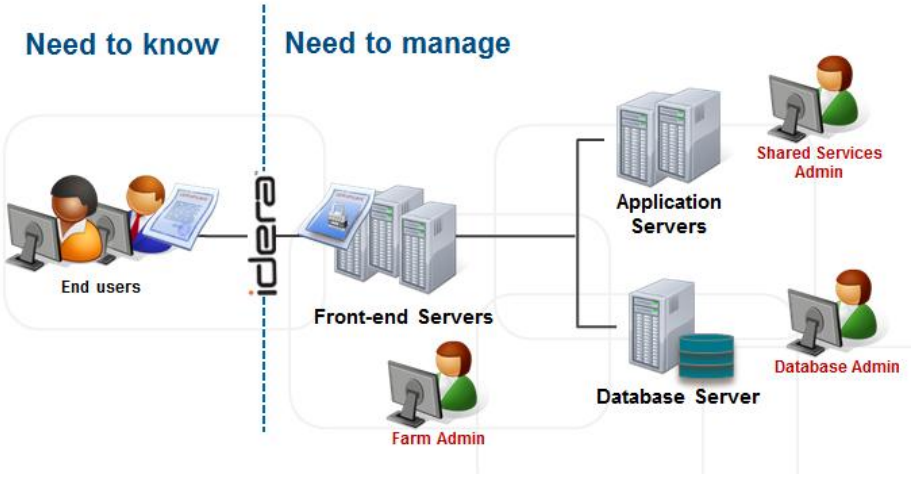


Figure 1 SharePoint encrypt security principle

SharePoint encrypt agent

The SharePoint encrypt service is a software agent that you install on the Web Front End servers in SharePoint farms. The agent software acts as a shim, inserting in the communications software stack to intercept files being checked into and out of SharePoint sites. The agent transparently encrypts files uploaded to the Libraries and, on download, decrypts files based on access control policies. The decision-making for which files to encrypt/decrypt and what keys to utilize is governed by key management policies created and administered on the SharePoint encrypt console as described below.

The SharePoint encrypt service works with the SharePoint encrypt console to manage security policies and encryption keys across multiple Web Front Ends. The figure below shows the relationship.

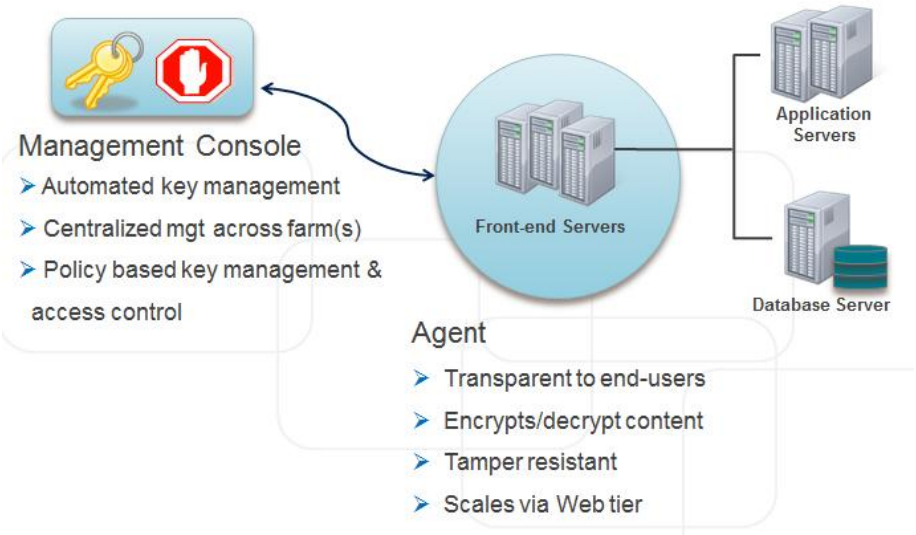


Figure 2 SharePoint encrypt architecture

SharePoint encrypt agent and console

The SharePoint encrypt service requires that a SharePoint encrypt console is available in order to deploy access control policies and keys to each SharePoint Web Front End running the SharePoint encrypt service. In the event that the SharePoint encrypt console is taken offline, or is otherwise unavailable for a time period, each SharePoint encrypt service will continue to operate and to perform encryption/decryption functions.

SharePoint encrypt console

The SharePoint encrypt console software provides management of encryption keys and access control policies across multiple SharePoint sites and Web Front Ends (see limitations for current release above). From the console, security administrators are able to define security policies and to apply them to Document Libraries.

Installation & Upgrades

We recommend installing the Idera SharePoint encrypt Service first and then installing the Idera SharePoint encrypt Console.

Things you will need

	Add the .Net Framework 3.5.1 Features to the server that will host the Idera SharePoint encrypt Console. Also, download and install the .Net Framework 4.0 Server/Development version on the server that will host the Idera SharePoint encrypt Console.
	Download and 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.
	**You will need to install the Idera SharePoint encrypt Console on a server outside the SharePoint farm.** The supported operating systems for the Idera SharePoint encrypt Console are: • Windows Server 2008 • Windows Server 2008 R2 • Windows 7
	**Open TCP Port 5194** on the server hosting the SharePoint encrypt Console and all web fronts end servers in the SharePoint farm that will be running the SharePoint encrypt Service.
	**Domain administrator** privileges are required to install the SharePoint encrypt Service. You will only need local administrator rights if installing on a machine that does not belong to an Active Directory Domain.

A full backup of the content in SharePoint that you want to encrypt.

Do you have a multi-server SharePoint farm?

SharePoint encrypt supports multiple Web Front End servers using a "hub and axle" architecture. The SharePoint encrypt Console will communicate with one SharePoint encrypt Service agent and that agent will communicate the configuration to the other agents in the farm. Before you begin, choose one WFE server to host the "master" SharePoint encrypt Service agent. Install the SharePoint encrypt Service agent on this server before installing on the additional Web Front Ends.

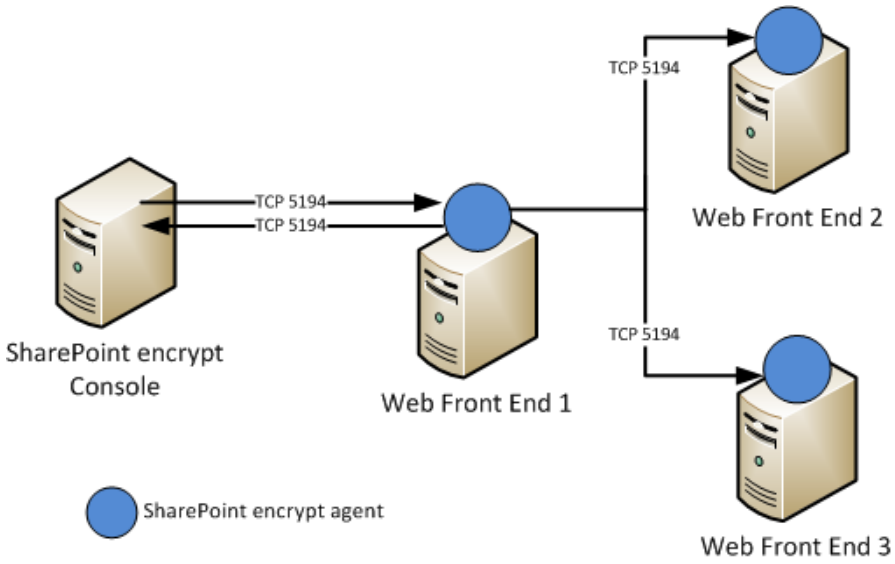


Figure 3 Hub and axle architecture

Permissions for the SharePoint encrypt Service

The SharePoint encrypt Service includes a Windows Service Application (**SharePoint encrypt Service**). You will need to set the logon properties of the service to an account that has elevated privilege to all the web applications that contain information you want to secure. Specifically, the Windows Service Application needs the following permissions:

- Member of the Windows Local Administrators group on each Web Front End (WFE) server
- Member of the SharePoint Farm Administrators group in SharePoint Central Administration
- Database Owner (dbo) rights to the content database(s) that contain information you want to secure

Upgrading the software

1. **Take a backup of the SharePoint encrypt Console configuration!** Follow the steps in the section Maintaining the SharePoint encrypt Console.

2. Lock the SharePoint site collections that have secured data so that users cannot access encrypted content during the upgrade.
3. Stop the SharePoint encrypt Windows Service Applications on the servers running the SharePoint encrypt Console and the SharePoint encrypt Service.
4. If the existing installation of SharePoint encryption is version 1.7, you will need to uninstall 1.7 before applying version 1.8. Upgrading SharePoint encrypt from version 1.8 does not require uninstalling the existing version. See the section Uninstalling for instructions on uninstalling the software. **Do not remove protection or decrypt your files prior to uninstalling.**
5. Follow the instructions below for installing the software.

SharePoint encrypt Service

1. Login into the Web Front End server as a user with Domain administrator privilege.
2. Locate the SharePoint encrypt Service installation program you downloaded.
3. Double-click the installer.
4. The first screen of the installer will prompt you to identify the master SharePoint encrypt Service agent (see Figure below).

   Leave this field blank if either of these conditions applies to this installation:

   1) you are installing on a single server, or,

   2) this installation is for the first of more than one Web Front End server.

   Otherwise **enter the IP address** (hostname will not work) of the Web Front End server that you first installed the SharePoint encrypt Service agent (the master install). For more information, see Do you have a multi-server SharePoint farm?

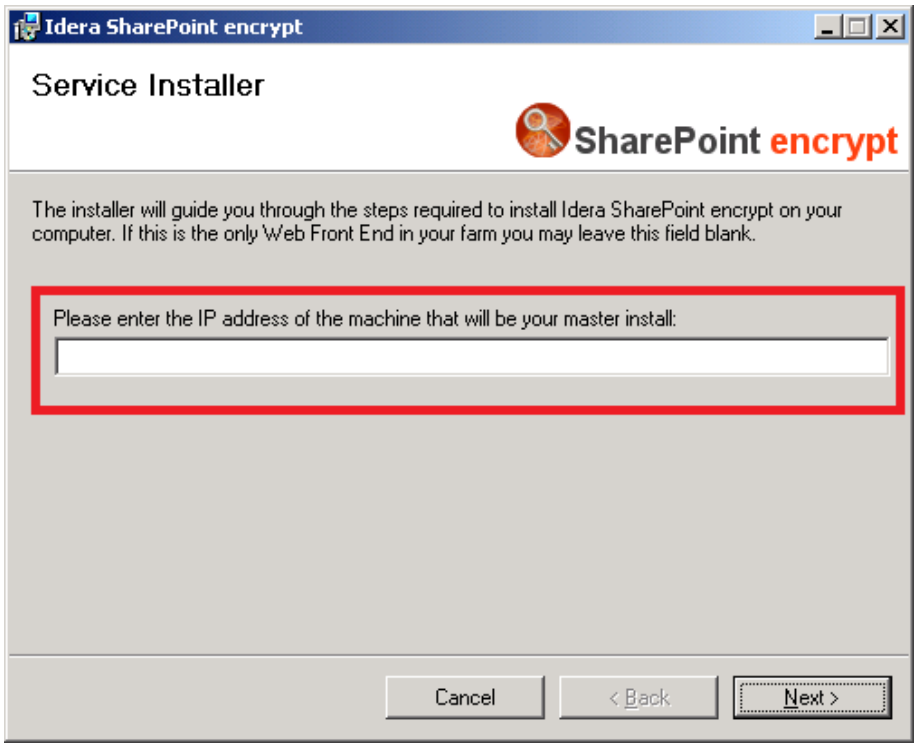


Figure 4 Identify the master SharePoint encrypt Serviceagent

5. Follow the prompts in the installation wizard and accept the license agreement.
6. Follow the remaining onscreen instructions. You will be prompted to configure the credentials for the Windows Service Application of the SharePoint encrypt Service.

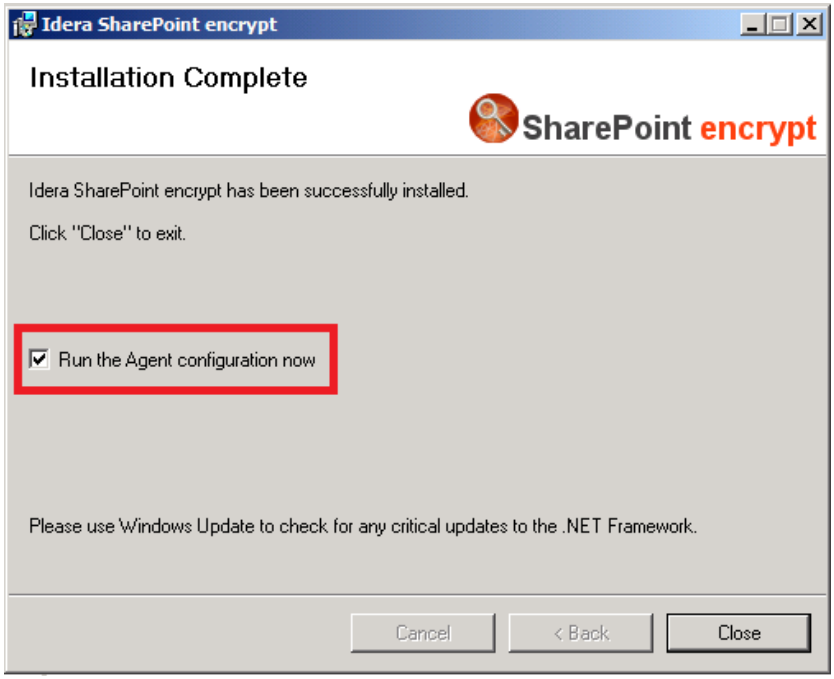


Figure 5 Configure service account

7. The SharePoint encrypt Service Windows Service Application needs to run as a member of the SharePoint Farm Administrators group, a member of the Windows local Administrators group, and have Database Owner (dbo) to the content database(s) that contain information you need to secure. Enter the account username as "DOMAIN\username" for an Active Directory account or ".\username" for local Windows accounts.

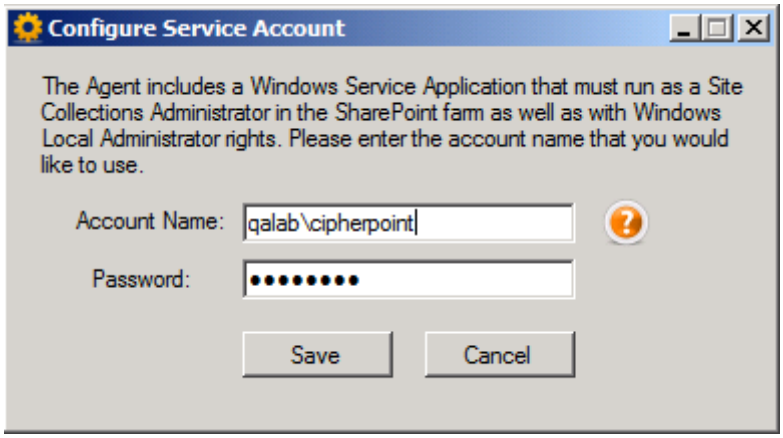


Figure 6 Enter service account credentials

SharePoint encrypt Console

Do not install the SharePoint encrypt Console on a server that is part of your SharePoint farm. Installing the SharePoint encrypt Console on a server in your farm is not a supported configuration. Security best practice for encryption and key management requires storing your data encryption keys separate from your encrypted data, so the SharePoint encrypt Console must be installed on a server outside the SharePoint farm.

1. Login into the server that will host the SharePoint encrypt Console as the administrator.
2. Locate the SharePoint encrypt Console installation program you downloaded.
3. Double-click the installer
4. Follow the onscreen instructions.

Configuration

This section contains instructions for creating and applying encryption and access control policies to protect SharePoint content. You can skip this section if you are evaluating the product using the embedded 14 day trial license.

Product Licensing

If you purchased the product, you will have received an encrypted license file, *license.cpf*, that you need to copy to the SharePoint encrypt Service install folder on **all** of the web front ends in your SharePoint farm.

1. Login into the SharePoint server that has the SharePoint encrypt Service installed.
2. Open Windows Explorer and navigate to *C:\Program Files (x86)\Idera\Idera SharePoint encrypt\Config*
3. Copy the *license.cpf* file you received with your purchase into the folder and overview the existing license file (See figure below).
4. After a few moments, you can view the current license status on the **Control Panel** tab of the SharePoint encrypt Console.

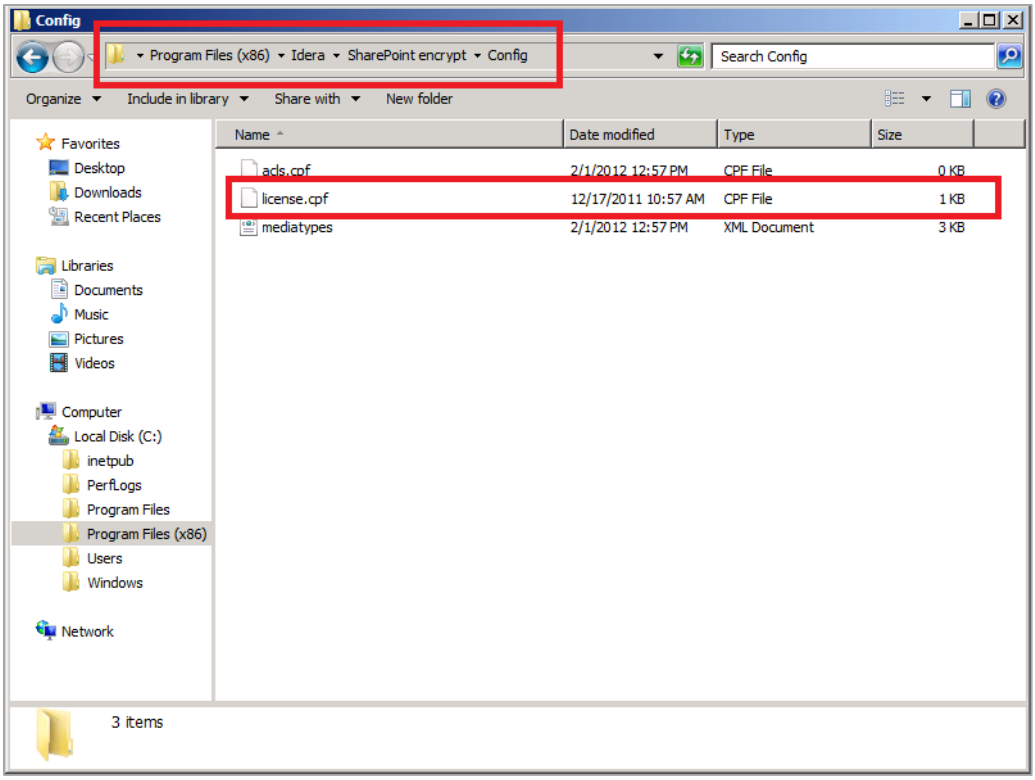


Figure 7 Applying the license file

Verify the SharePoint encrypt Service installation

The SharePoint encrypt Service installer binds the enforcement module to the default web application on port 80. If you have additional or other web application(s) that contain sites you need to protect, follow the steps in this section.

1. Login into the SharePoint server that has the SharePoint encrypt Service installed.
2. Open Windows Explorer and navigate to *C:\inetpub\wwwroot\wss\VirtualDirectories*
3. Open the folder that corresponds to the web application that contains the site(s) you will need to protect (e.g. *80*, *extranet.foo.com*)

4. Open the *web.config* file in Windows Notepad and search for the text "CipherPoint"

   If you find no entries then continue to the next step. Otherwise, please go to the following section.

5. Make a copy of the *web.config* file
6. For SharePoint 2007 installations
   a. Search the *web.config* file for "<httpmodules>"
   b. At the end of the <httpmodules> section add the following line

```
<add name="CipherPointLens"
type="CipherPoint.CipherPointLens, CipherPointLens,
Version=1.8.0.42, Culture=neutral, PublicKeyTo-
ken=7e06dcf310e66293" />
```

   c. Save your changes
7. For SharePoint 2010 installations
   a. Search the *web.config* file for "<modules"
   b. At the end of the <modules RunALL…> section add the following lines

```
<add name="CipherPointLens"
type="CipherPoint.CipherPointLens, CipherPointLens,
Version=1.8.0.42, Culture=neutral, PublicKeyTo-
ken=7e06dcf310e66293" />
<remove name="OutputCache" />
```

   c. Save your changes
8. If you modified a *web.config* file then open a command window As Administrator and restart IIS using the following command:

```
iisreset/noforce
```

Permissions to the installation folder

Each administrator of the SharePoint encrypt Console will need read and write privileges to the installation folder and the registry key in order to access and modify configurations.

1. Login into the server that has the SharePoint encrypt Console installation.

2. Open Windows Explorer and navigate to *C:\Program Files (x86)*
3. Right click the folder *Idera* and select **Properties**
4. Click the Security tab and review the permissions. The Windows accounts for each administrator of the SharePoint encrypt Console will need read and write permissions to this folder.
5. Click the **Edit…** button to modify the permissions of the folder.
6. Click the **Add…** button and add the users that will need to access the console.
7. Click the **OK** button to the return to the Permissions window
8. Select the users that you added in step 6 and enable the **Modify** check box.
9. Click the **Apply** button to save the changes and then click the **OK** button to close the permissions window.

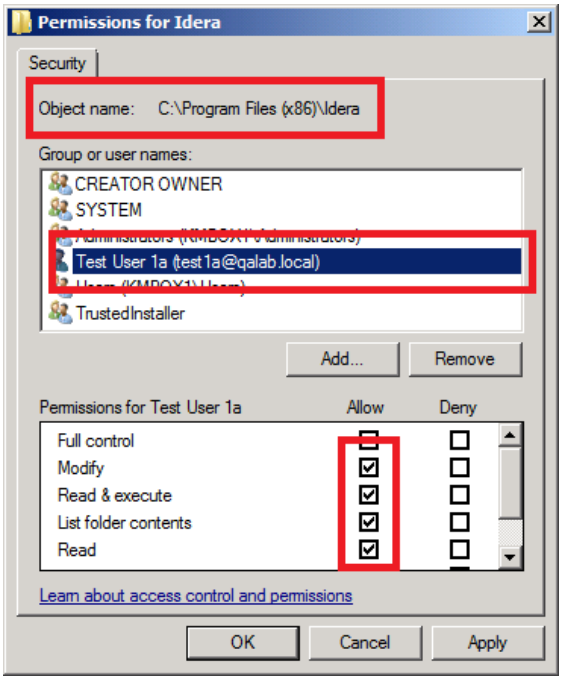


Figure 8 Setting permissions on the SharePoint encrypt Console install folder

10. Click the Windows Start button and select **Run…**

11. Type "regedit" in the **Open:** text box and click the **Ok** button
12. In the Windows Registry Editor navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node*
13. Right click the *CipherPoint* key and select **Permissions…**
14. Click the **Add…** button and add the same users as in Step 6 above
15. Click the **OK** button
16. Select the users that you added in Step 14 and in the **Permissions for Users** box enable the **Allow** checkbox for **Full Control**
17. Click the **OK** button to save the permissions

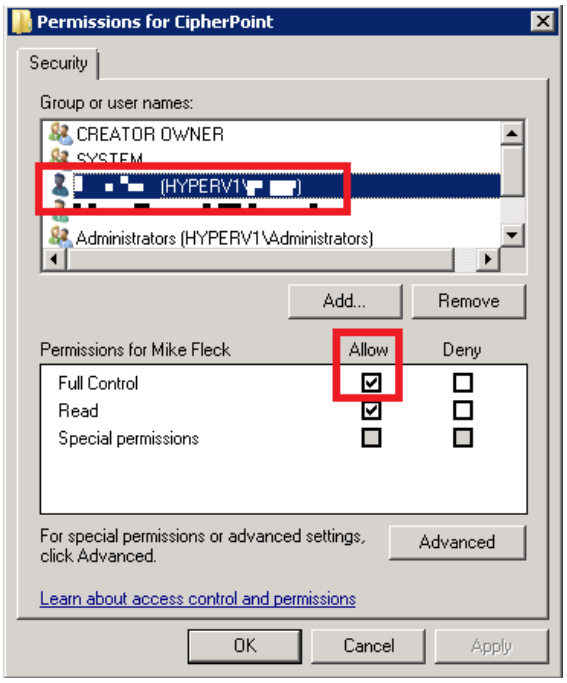


Figure 9 Setting Registry permissions

Setup the SharePoint encrypt Console

1. Login into the server that has the SharePoint encrypt Consoleinstallation.
2. Click the Windows **Start** button and go to **All Programs -> Idera** and click the **Idera SharePoint encrypt - Console** icon.

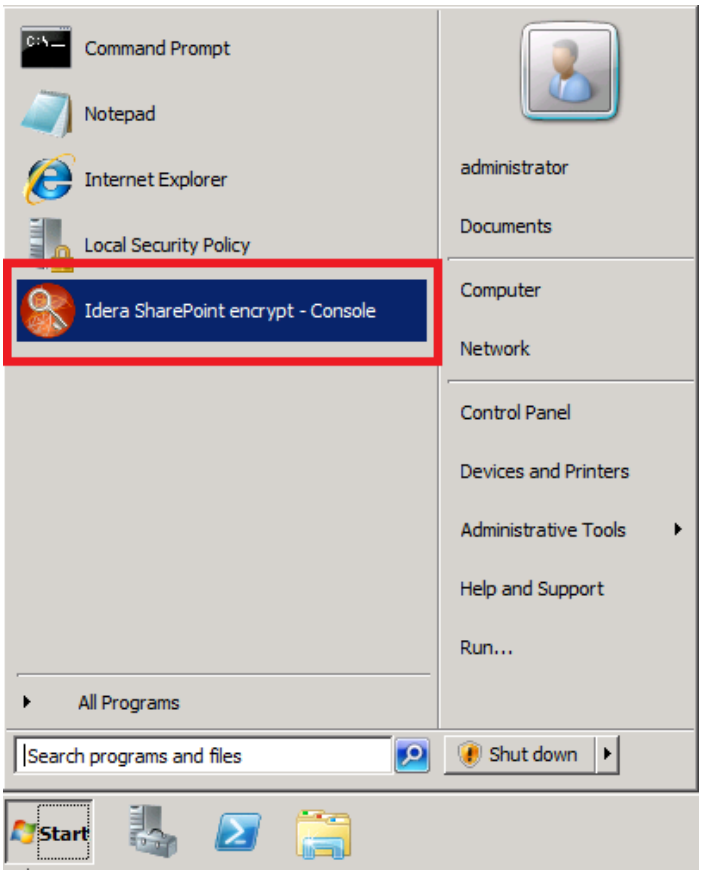


Figure 10 Launching the SharePoint encrypt Console

3. You will receive a prompt to create an administrative login.

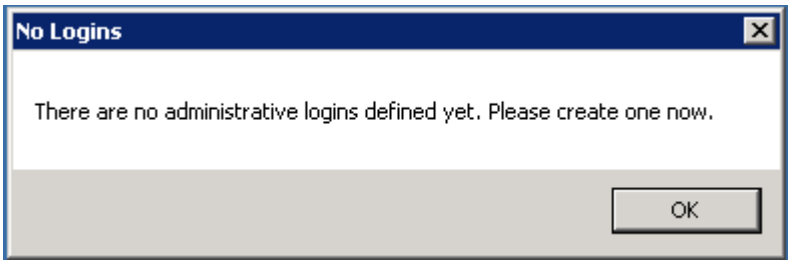


Figure 11 No administrator accounts exist

4. Click the **OK** button and create an administrator account on the following form. The **Username** cannot be greater than 10 charac-

ters. The password must be at least 8 characters long and contain at least one letter, at least one number, and at least one special character.

5. Login using the account you created in the previous step. If this is the first time you have run the SharePoint encrypt Console you will receive a prompt to register a SharePoint encrypt Service.

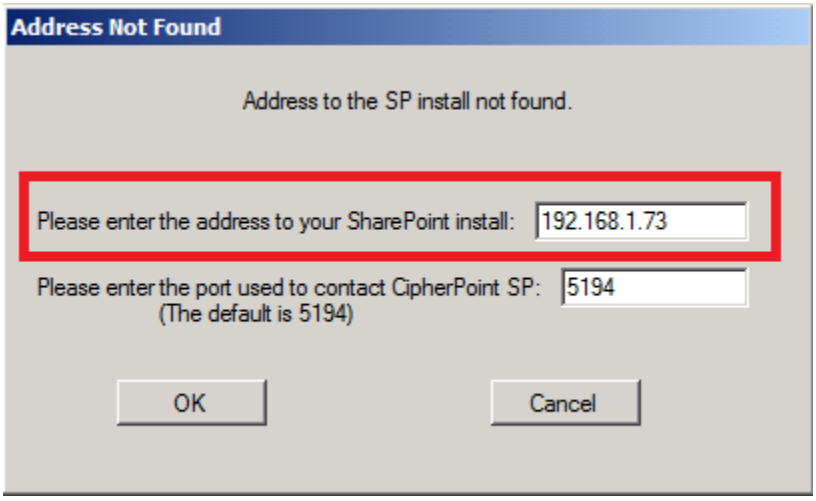


Figure 12 Specifying the master Web Front End

7. Enter the IP address or hostname of the master Web Front End server in the text entry box labeled **Please enter the IP address of the WFE you have designated as the master** according to the instructions in the section Do you have a multi-server SharePoint farm?. The WFE must already have the SharePoint encrypt Service installed.
8. Leave the port number as the default value (5194).
9. Click **OK**.

Configuration and Deployment of Security Policies

Now that SharePoint encrypt components are installed, there are four important steps needed before the product is fully functional in your SharePoint farm. These include retrieving the SharePoint topology, creating key management policies to match your information security

and compliance requirements, building access control policies to be used within your SharePoint farm, and finally selecting the portions of your SharePoint topology to be protected, and applying the key management and access control policies to the protected parts of the topology.

Retrieve SharePoint Topology

1. In the SharePoint encrypt Console click the tab labeled **Control Panel**.
2. Click the **Get Topology** button. The button will remain disabled until the topology information has been read from SharePoint and received by the Console.
3. When the **Get Topology** button is no longer disabled, click the **Logs** tab and check if the SharePoint encrypt Service reported any errors when connecting to the SharePoint farm.
    a. The most common error condition is that the Windows Service Application for the SharePoint encrypt Service does not have the necessary permissions to connect to the SharePoint farm and retrieve the list of web applications and other contents. Please see the section Permissions for the SharePoint encrypt Service for more details on the permissions required by the SharePoint encrypt Service.
    b. If there are no errors, click the **Portals** tab and verify that the expected list of web applications is visible. Note, the Console will not display the Central Administration site or other administrative SharePoint sites.

The default behavior for SharePoint encrypt is to request the SharePoint topology on-demand. When you click the **Get Topology** button in the **Control Panel** tab, SharePoint encrypt will request the list of Web Applications. As you expand a Web Application in the Topology window on the **Portals** tab, SharePoint encrypt will request the Site Collections in that Web Application. If this on-demand approach does not give you the response time that you would like then you can disable the on-demand functionality by enabling the **Load Full Topology** checkbox on the **Control Panel** tab. Not that this will cause SharePoint encrypt to request ALL the Lists and Libraries in all Sites across all Site Collections. This process could take several minutes up to over

an hour for very large environments.

Figure 13 Changing the behavior of Get Topology

Creating Key Management Policies

Idera has designed SharePoint encrypt Console to eliminate the complexity of encryption key management. We will use two common information security compliance requirements as the basis for learning how to create and configure SharePoint encrypt Console Key Management policies.

PCI DSS Policy Example

4. In the SharePoint encrypt Console click the tab labeled **Key Management**.
5. Click the **New** button at the bottom of the Key Management panel
6. Enter "PCI_DSS" in the **Policy Name** field.
7. Select **AES – 256 bits** from the **Algorithm** pull down list.

8. Increment the **Change Every** value to **1**. This value will instruct SharePoint encrypt to create a new data encryption key every year.
9. Increment the **Keep Keys** for value to **7**. This value will instruct SharePoint encrypt to deactivate old encryption keys 7 years after they have been replaced by a new key. Setting this value to 0 indicates the encryption key never expires.
10. Compare your entries with the Figure below and click **Save** after you have validated your input.

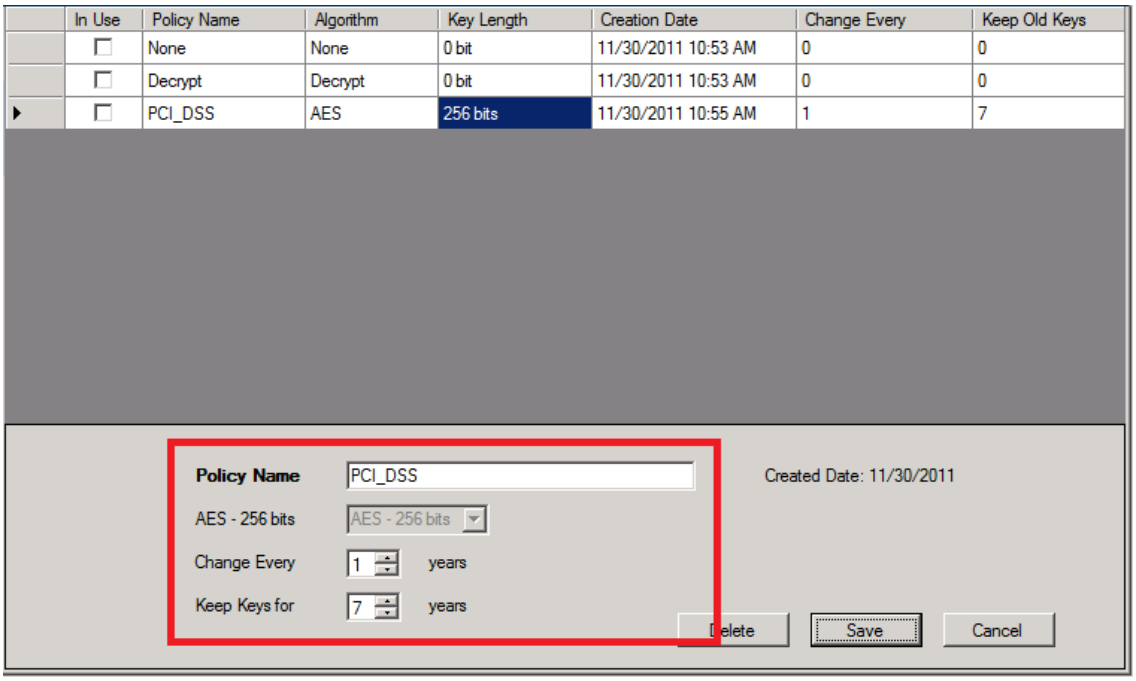


Figure 14 Sample PCI DSS key management policy

HIPAA/HITECH Policy Example

1. In the SharePoint encrypt Console click the tab labeled **Key Management**.
2. Click the **New** button at the bottom of the Key Management panel
3. Enter "HIPAA_HITECH" in the **Policy Name** field.

4. Select **AES – 256 bits** from the **Algorithm** pull down list.
5. Increment the **Change Every** value to **2**. This value will instruct SharePoint encrypt to issue a new data encryption key every two years.
6. Increment the **Keep Keys** for value to **0**. This value will instruct SharePoint encrypt to never expire old encryption keys since you always want medical records to be available.
7. Compare your entries with the Figure below and click **Save** once you have validated your input.

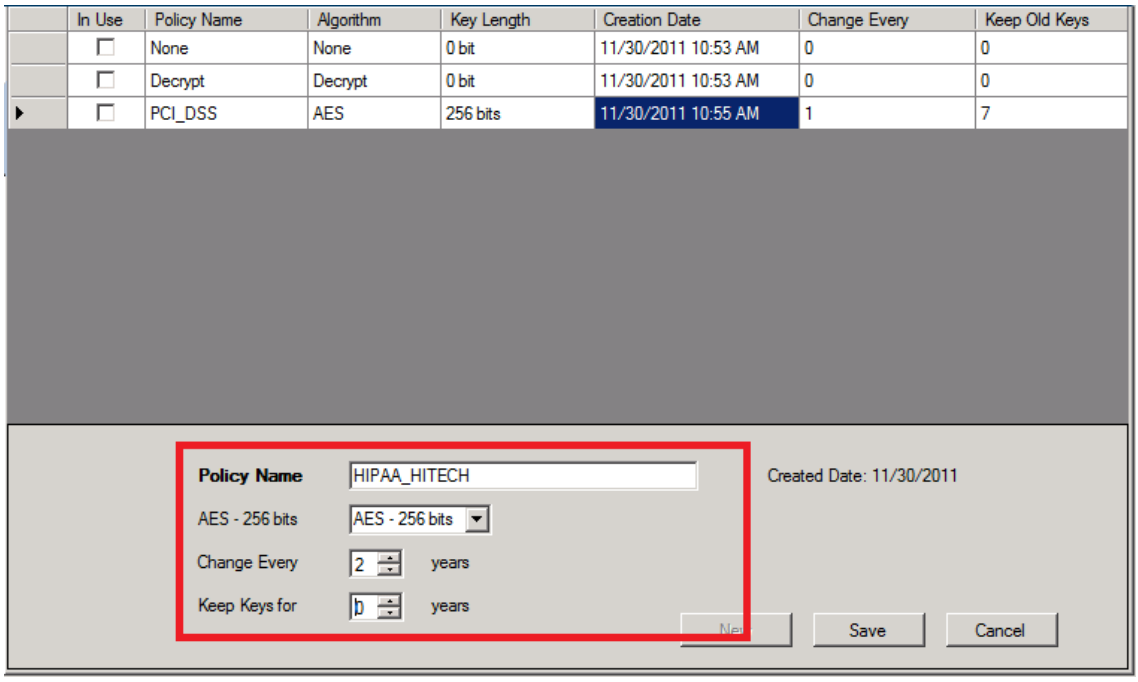


Figure 15 Sample HIPAA HITECH key management policy

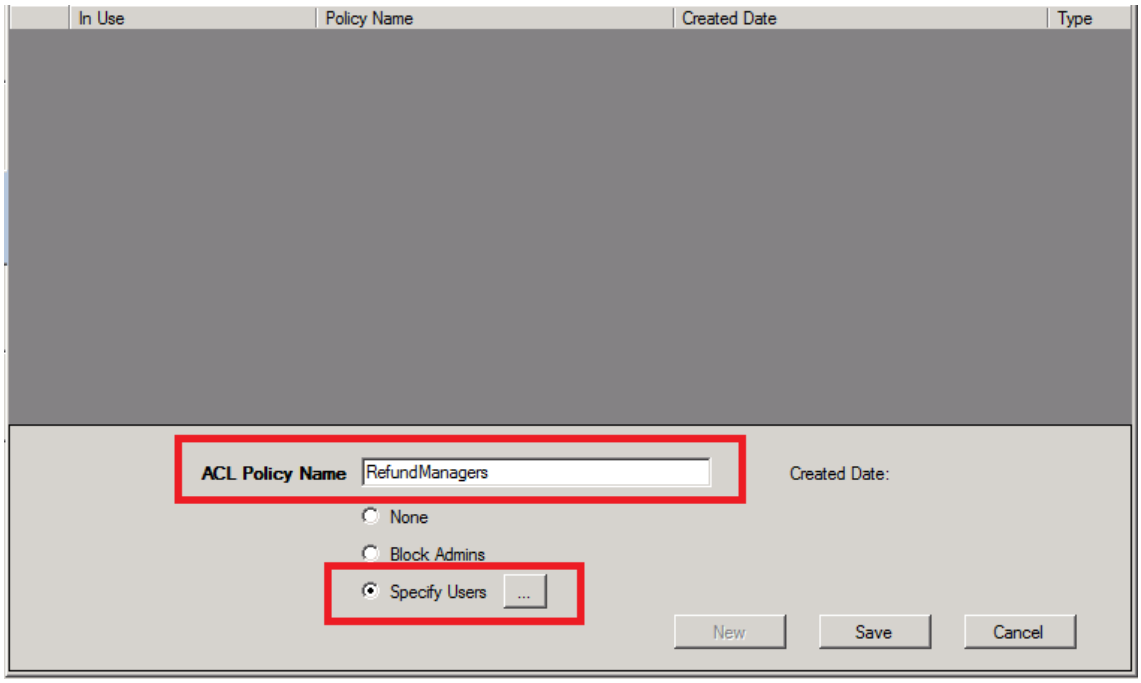
Access Controls

There are three different access control options that can be selected and applied to your SharePoint topology.

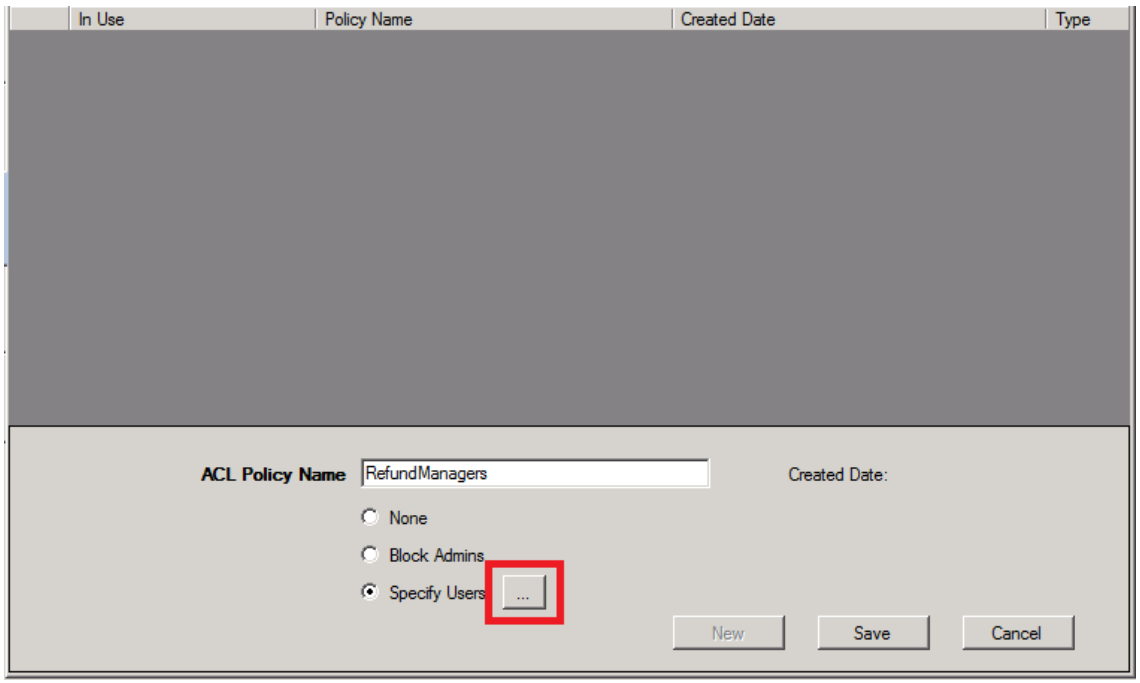
- **None** – SharePoint encrypt will not provide additional access controls. Native SharePoint permissions are the only access control mechanism and SharePoint encrypt provides encryption and decryption of content for all users.
- **Block Admins** – SharePoint encrypt will deny access to any user that has an administrative role (Farm Administrator, Site Collection Administrator, Shared Services Administrator, or System Administrator) defined within SharePoint. All other SharePoint permissions are unaffected. This approach provides a basic level of protection against a malicious user with administrative privilege. For example, a farm administrator can still create a new, non-administrative user and add that user as a site contributor to get access.
- **Specify Users** – SharePoint encrypt provides two different access control policies that allow you to specify certain users or groups to include or exclude.
    - **Inclusion Lists** identify the users or groups that may access a protected Library. Use this option to tightly control which users may access and decrypt content in a protected Library. Any new membership assigned in SharePoint will also have to be added to the SharePoint encrypt Access Control policy.
    - **Exclusion Lists** identify the users or groups that CANNOT access a protected Library. These user or groups do not need to have existing permissions assigned in SharePoint.

Create a new Access Control policy

1. In the SharePoint encrypt Console click the tab labeled **Access Controls**.
2. Click the **New** button at the bottom of the Access Controls panel
3. Name the policy by entering a name ("RefundManagers" in the example below) in the **ACL Policy Name** field.



4. Select the **Specify Users** radio option and click the browse button to view the list of site members.



5. Leave **Policy Type** set to the default value (**Inclusion list**).

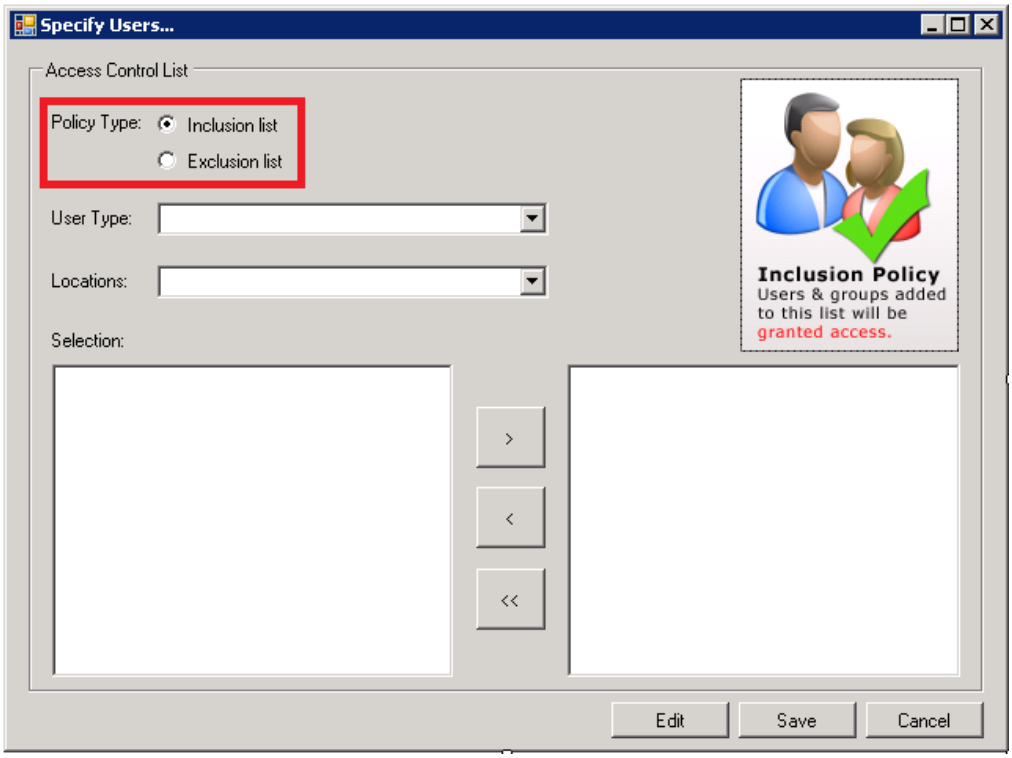


Figure 16 Access Control Policy Type

6. Select **SharePoint** in the **User Type** drop-down list.
7. Use the **Locations** drop-down list to select the SharePoint site from which you want to use to import user and group names.
8. In the **Selection** field click the names of the users or groups you want to add to the policy then click **>** to add the users or groups.

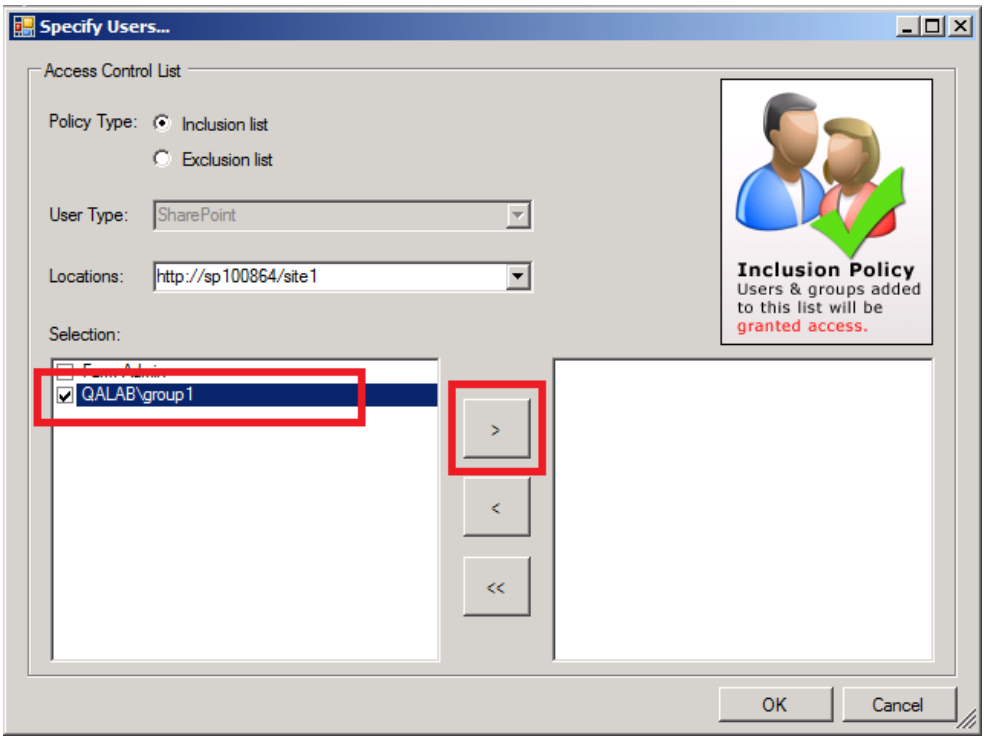


Figure 17 Building the Access Control List

9. Click the **OK** button to return to the main panel.
10. Click the **Save** button to save your new policy.

Securing a Library

Before you begin make sure you have created at least one Key Management policy and at least one Access Control policy. Upon completion of the steps in this section the solution will also begin encrypt any existing files in the protected library. We recommend you perform these steps in accordance with your organization's change management procedures if you are working in a production environment.

1. **Take a full backup of the library or libraries you want to protect before proceeding.**
2. In the SharePoint encrypt Console click the tab labeled **Portals**.

3. Use the tree view in the left side of the panel to browse the site(s) and select the Library you want to protect.
4. Use the list in the middle of the panel to select the Access Control policy you want to apply to the Library.
5. Use the list on the right side of the panel to select the Key Management policy you want to apply to the Library.
6. Click the **Save** button to apply the selected combination of policies to the topology item.

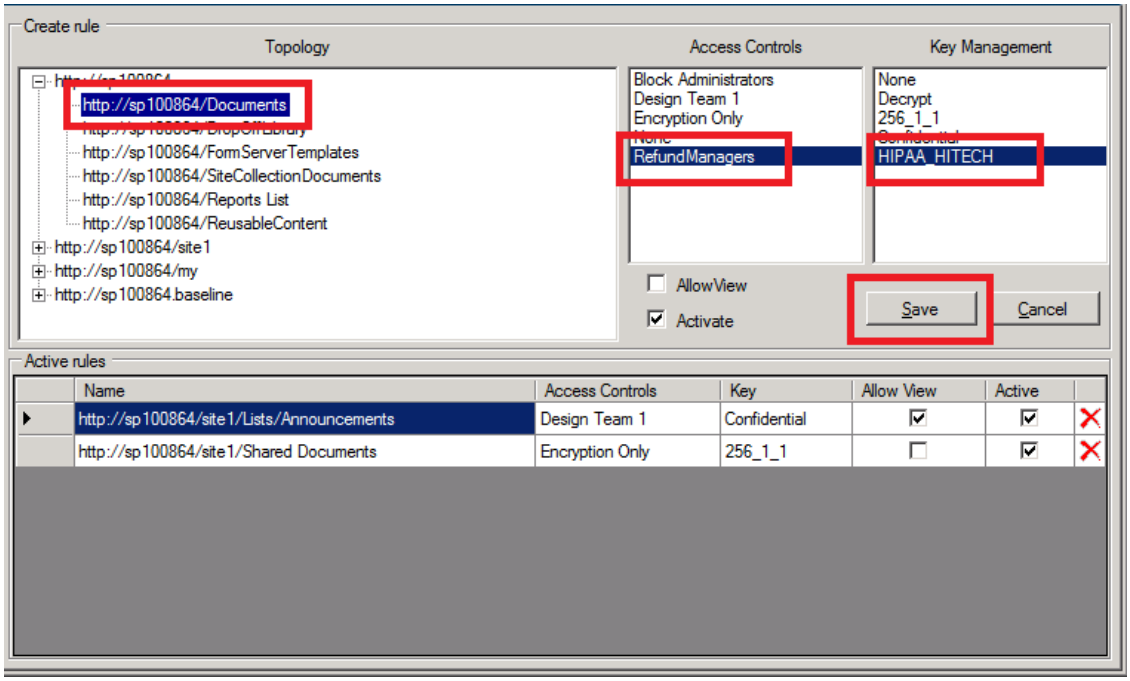


Figure 18 Protecting a SharePoint document library

7. You have now applied key management and access control policies to a SharePoint library. SharePoint encrypt will now secure the selected Library according to the encryption and access control rules contained in the policies.

The Allow View option

The Allow View rule option allows SharePoint encrypt Console administrators to permit limited access by SharePoint administrators to

secured locations. This option is disabled by default. When this option is enabled, a SharePoint administrator that would otherwise be denied **all** access to a List of Library may view the items in the List or Library but he will not be able to open files and any encrypted List items will remain encrypted.

To enable or disable the Allow View option:

1. In the SharePoint encrypt Console click the **Portals** tab to view the current list of security rules
2. In the **Active rules** window click the **Allow View** checkbox to enable or disable the AllowView option

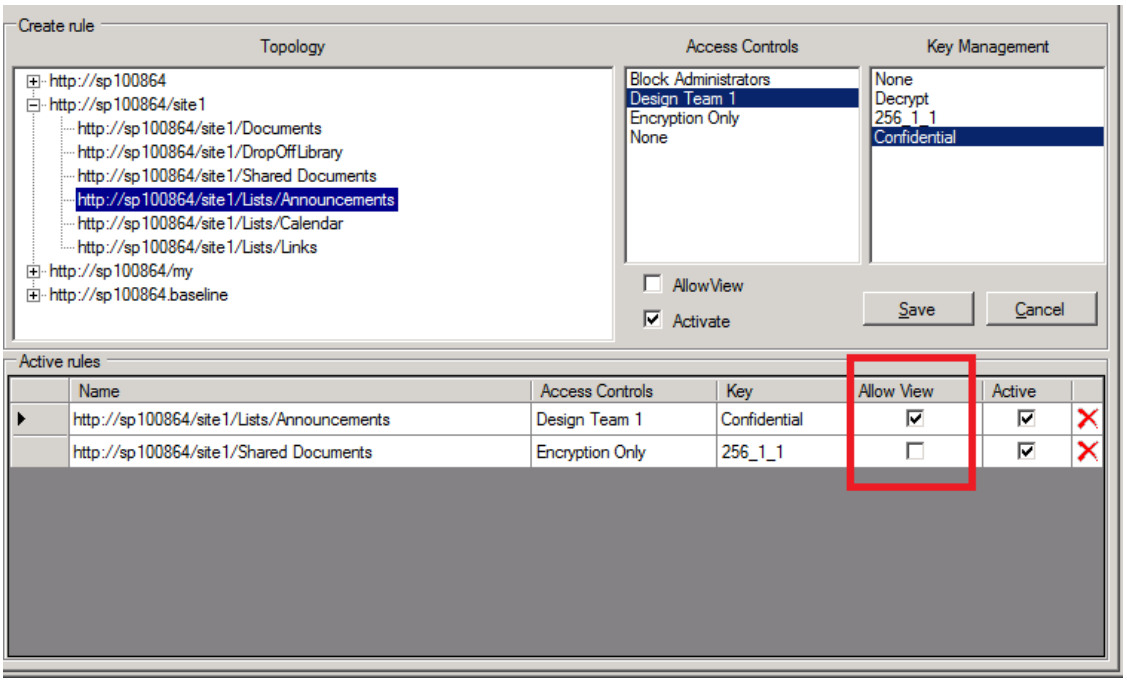


Figure 19 Managing the Allow View option

Working with Audit Logs

Idera SharePoint encrypt uses the following severity levels to categorize different messages. The audit messages are stored in the Share-

Point encrypt Console log file and are also written to the Windows Application Event log on the server running the SharePoint encrypt Console.

Severity	Description
One	Reserved for decryption of a protected library.
Two	Communication errors between the SharePoint encrypt Console and SharePoint encrypt Service
Three	Denied user access requests
Four	Authorized read or download requests
Five	<not used>
Informational	Authorized edit or upload operations. Also non-interactive operations such as initial encryption of a protected library.

Log messages will come from the following event sources:

Source	Description
Manager	Audit messages generated by activity on the SharePoint encrypt Console and Windows service application.
Agent	Audit messages generated by the module of the SharePoint encrypt Service that enforces policies and the Windows service application.

To view the current list of events:

1. In the SharePoint encrypt Console click the **Logs** tab to view the available log messages.
2. Double-click a row to view an individual log entry
3. To filter the logs select the message source from the combination box and enter text in the edit box. Click the **Search** button to apply the filter.

4. To remove the filter delete the text from the edit box and click the **Search** button.

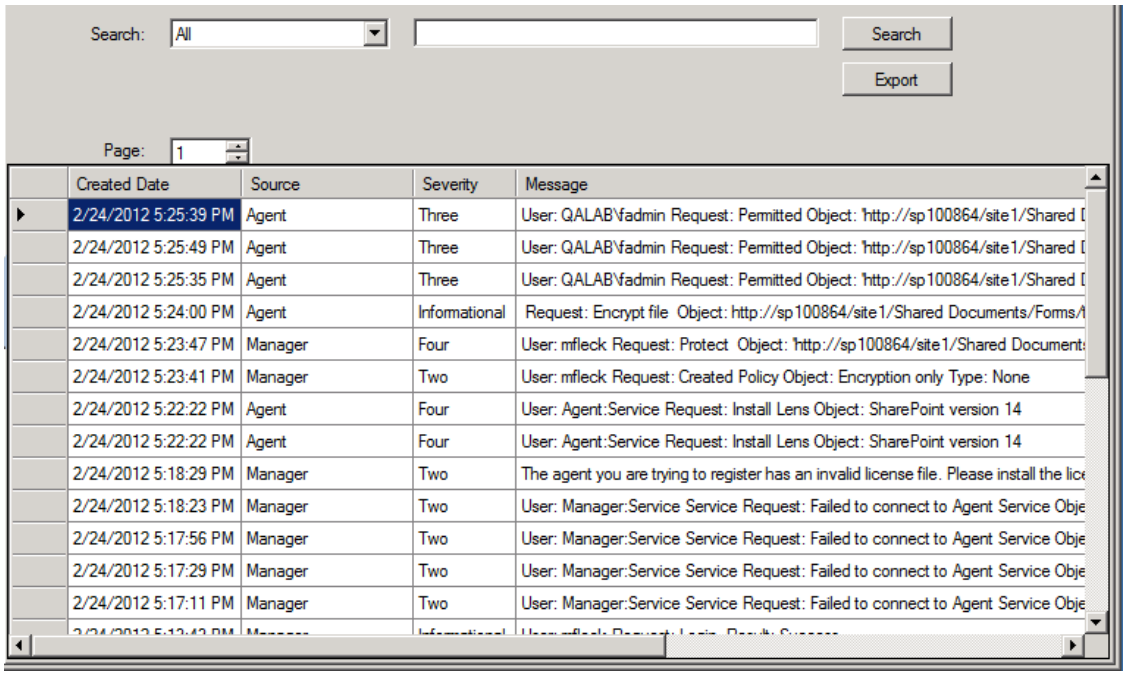


Figure 20 SharePoint encrypt log messages

Removing Protection

Before you begin make sure you have created at least one Key Management policy and at least one Access Control policy.

1. In the SharePoint encrypt Console click the tab labeled **Portals**.
2. In the list of **Active rules**, click the red **X** icon to the right of the library you want to stop protecting.

   After a few moments the SharePoint encrypt Service will stop applying the access control and key management policies to the affected document library. All existing files, however, are **still encrypted**. If you want to decrypt all the files in the library continue to the next step.

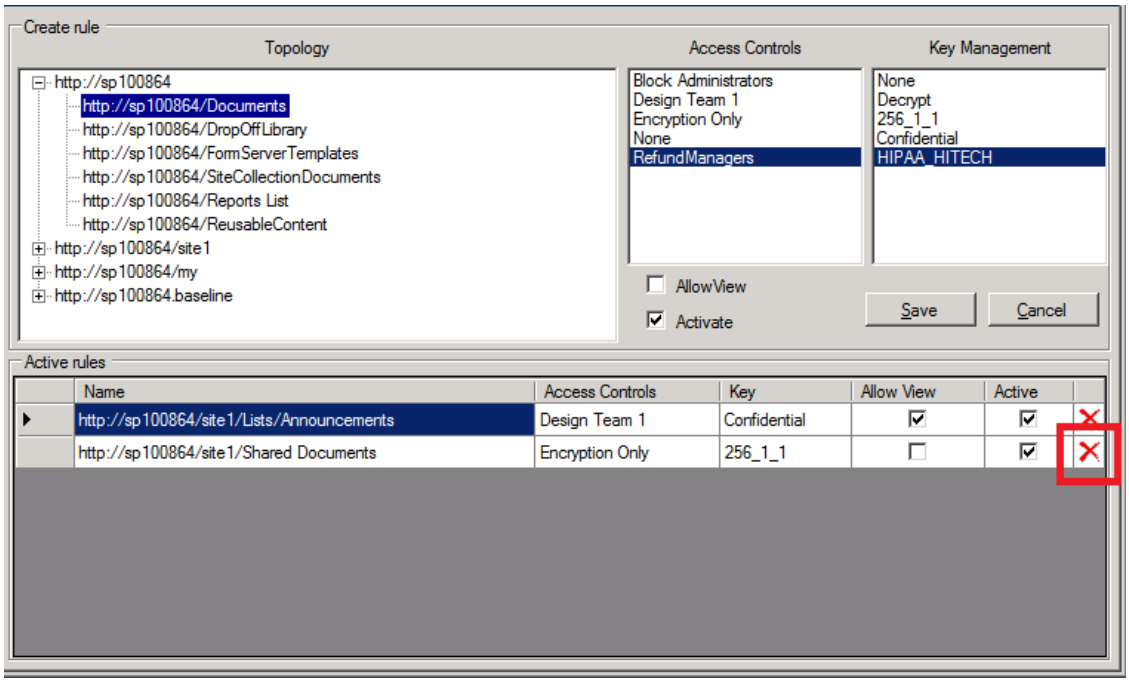


Figure 21 Deleting protection

3. To decrypt all encrypted files in a library select the library that contains the encrypted files, select an appropriate access control policy, and select the **Decrypt** key management policy.
4. Click the **Save** button

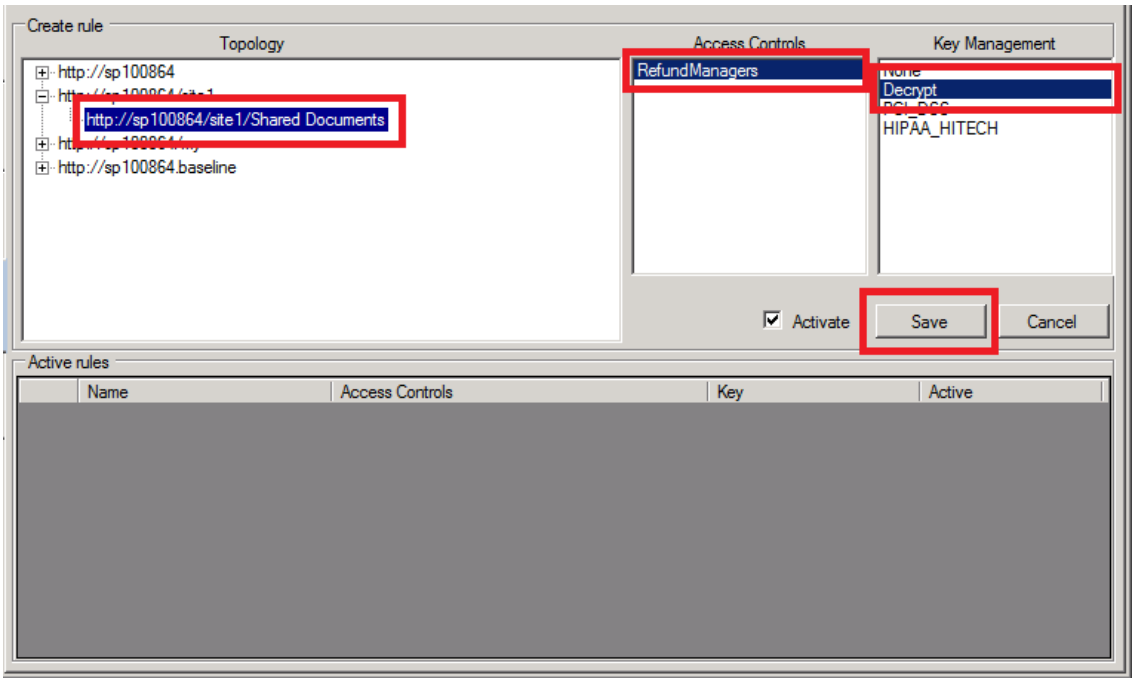


Figure 22 Decrypting files in a library

5. Review the events in the **Logs** tab for information on the current status of the decryption process.
6. The rule applying the **Decrypt** policy will automatically be removed when the decryption process is complete.

Uninstalling

Before uninstalling the product make sure you have decrypted your files and/or archived the Data Encryption Keys and Master Encryption Key according to the steps in the Removing Protection and Maintaining the SharePoint encrypt Console sections, respectively. If you fail to perform these steps before uninstalling the product your **encrypted information may become permanently inaccessible.**

Use the following steps to uninstall SharePoint encrypt. **When uninstalling the SharePoint encrypt Console read and follow all prompts very carefully.**

1) Click the Windows **Start** button and select **Control Panel**

2) Click **Uninstall a Program**

3) Select the program you want to uninstall and click the **Uninstall** button

Figure 23 Remove or keep SharePoint encrypt files

4) If you are uninstalling the SharePoint encrypt Console you will be prompted to delete or leave the configuration files. If you click **Yes**, **you will delete all the data encryption keys**.

5) You may need to manually delete the SharePoint encrypt Service entries in the *web.config* files. Please read the section Verify the SharePoint encrypt Service installation for more details.

Maintaining the SharePoint encrypt Console

SharePoint encrypt uses two types of encryption keys. The encryption keys generated and applied to secure information in SharePoint are Data Encryption Keys. There is also a Master Encryption Key that is used to secure the Data Encryption Keys and the other sensitive configuration items.

Protecting the Data Encryption Keys

Archive the SharePoint encrypt Console data encryption keys and configuration files daily. Use your existing backup software to archive the XML files in *C:\Program Files (x86)\Idera\Idera SharePoint encrypt*.

Protecting the Master Encryption Key

Archive the Master Encryption Key after the first installation of the SharePoint encrypt Console and, optionally, whenever you change the SharePoint encrypt Console administrators.

The SharePoint encrypt Console uses the Master Encryption Key to encrypt the Data Encryption Keys (i.e. the cryptographic keys used to secure information in SharePoint) as well as other sensitive configuration items.

You will need at least two SharePoint encrypt Console administrator accounts to archive the Master Encryption Key.

1. In the SharePoint encrypt Console click the **Control Panel** tab
2. Click the **Backup MEK** button.
3. Click the account names of the two or three administrator accounts. These administrators will **all** have to enter their passwords in order to restore the Master Encryption Key.
4. After you have selected two administrator accounts, click the **Select Users** button.
5. Click the **Browse** button to select the destination location for the Master Encryption Key archive file.

6. Click the **Backup MEK** button to archive the Master Encryption Key.
7. The file *Backup_MEK2Adm.xml* will be created in the location you specified above. Archive this file to multiple locations.

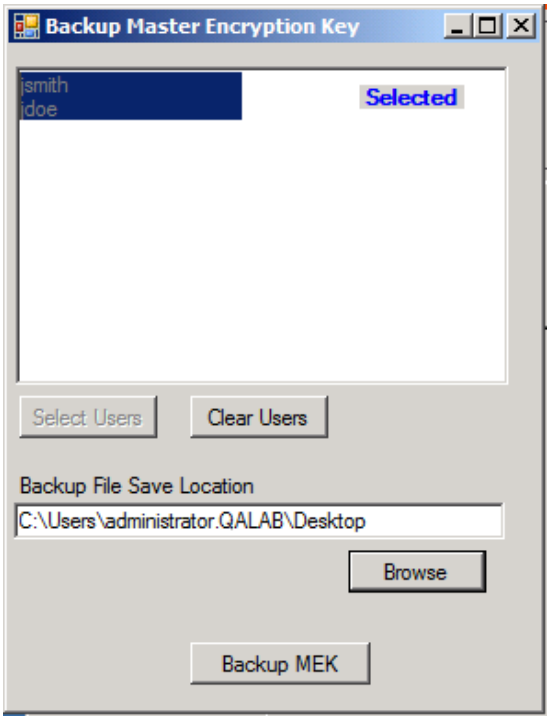


Figure 24 Backup the Master Encryption Key

Recovering the SharePoint encrypt Console

To recover from a failure, simply install the SharePoint encrypt Console on a new server and restore the archived XML configuration files and data encryption keys to the new installation location. Then you need to restore the Master Encryption Key so that the contents of the encrypted configuration files can be decrypted by the SharePoint encrypt Console.

1. Restore the Master Encryption Key backup file (*Backup_MEK2Adm.xml*) created in the previous section to the new SharePoint encrypt Console server.

2. Restore the XML configuration files to the SharePoint encrypt Console installation path *C:\Program Files(x86)\Idera\Idera SharePoint encrypt*
3. Launch the SharePoint encrypt Console and you will receive an error message due to a failure to decrypt the XML files. This is expected behavior.

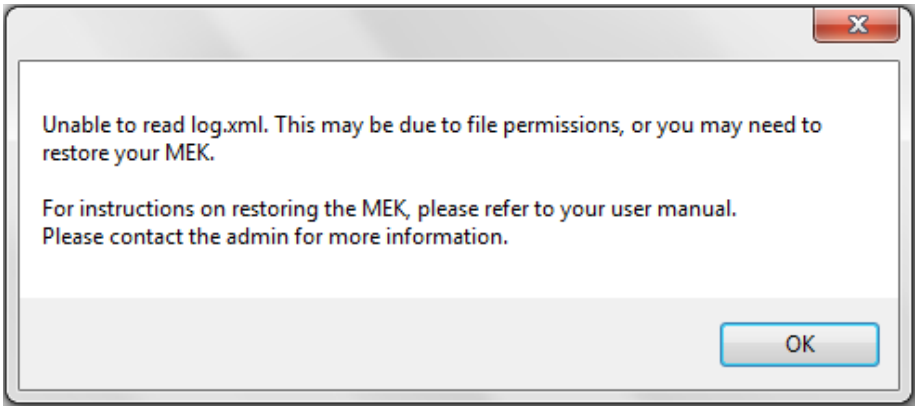


Figure 25 Error due to incorrect Master Encryption Key

4. In the SharePoint encrypt Console click the **Control Panel** tab.
5. Click the **Restore MEK** button.

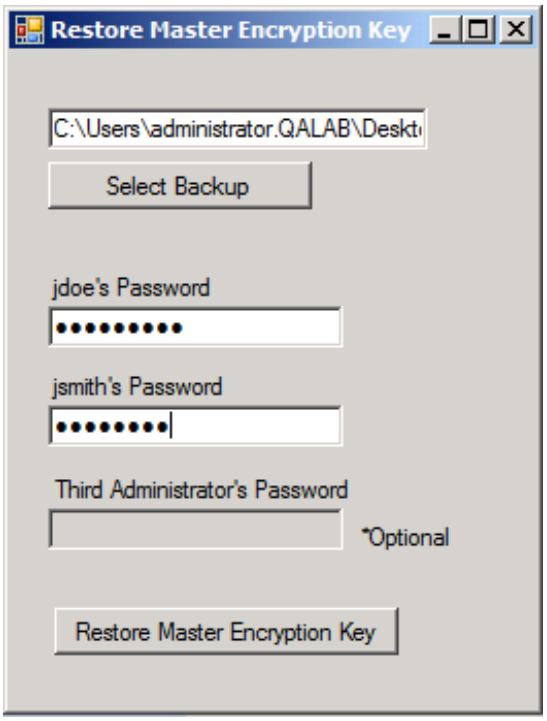


Figure 26 Restoring the Master Encryption Key

6. Click the **Select Backup** button and browse to the Master Encryption Key archive file you copied in Step 1.
7. Enter the password for each of the administrator accounts in the corresponding text fields.
8. Click the **Restore Master Key** button

You can now apply any restored or new Key Management and Access Control policies to your information and SharePoint encrypt will automatically retrieve the correct Data Encryption Keys.

Licensing Explained

You may view the current license status in the **Control Panel** tab of the SharePoint encrypt Console. Below is an explanation of each field in the licensing section.

Figure 27 License status

Field Name	Description
Customer Name	The name of the organization that purchased the product license.
Product license type	• "Demo" license will allow full product functionality for a 2 week period • "Enterprise" licenses allow full product functionality • "Standard" licenses allow full product functionality for a limited number of web front end servers
Number of WFEs allowed	The number of SharePoint encrypt Service agent licenses purchased.
Number of WFEs in farm	The number of Web Front End servers and Application servers discovered by the agent.

License expires on	The date that the product license expires (not applicable to Perpetually licenses)
Agent IP Address	The IP address of the master Web Front End agent.

License expiration

When a license expires you will not be able to make any changes to your security configuration. The product will continue to enforce the existing security rules.

Please see the Contacts section if you need to renew your product license or require assistance decommissioning the software.

Troubleshooting

If you have any problems related to the product, the steps below are helpful to isolate the issue. We recommend you follow the steps in the order provided.

Verify the installation

1. If users receive HTTP error 403 when accessing a protected library on a Windows Server 2003 then re-install the SharePoint encrypt Service using an account that has Domain Administrator rights.
2. Verify that the *web.config* files for the appropriate web applications have been modified to include the SharePoint encrypt Service.
3. Verify that the SharePoint and SQL Server services are running on the servers in the SharePoint farm.
4. Verify the Windows Service Applications for SharePoint encrypt Console and SharePoint encrypt Service are running on each of the servers.
5. Restart IIS after installing the SharePoint encrypt Service using the command in a Windows Command Prompt.

   ```
   iisreset/restart
   ```

6. Make sure the login account for SharePoint encrypt Service Windows Service Application has the correct permissions according to the section Permissions for the SharePoint encrypt Service.
7. Restart the SharePoint encrypt Service and SharePoint encrypt Console Windows Service Applications using the Windows Services Console (Start->Run->services.msc).

Test Network Connectivity

8. Issue the following command using the **Windows Command Prompt** from the server running the SharePoint encrypt Service. If the telnet client cannot connect to the remote port then make sure the Windows Firewall has been configured to allow inbound and

outbound traffic on TCP port 5194.

```
telnet [hostname/IP of SharePoint encrypt Con-
sole] 5194
```

9. Issue the following command using the **Windows Command Prompt** from the server running the SharePoint encrypt Console. If the telnet client cannot connect to the remote port then make sure the Windows Firewall has been configured to allow inbound and outbound traffic on TCP port 5194.

```
telnet [hostname/IP of SharePoint encrypt Ser-
vice] 5194
```

10. To enable debug logging change one or more of the registry keys below to "true" based on which component of the product you need to troubleshoot. All the keys below are in *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\CipherPoint*

Value	Component
"DEBUG_AGENT_S"	the SharePoint encrypt Service Windows Service Application on the Web Front Enter (WFE) server.
"DEBUG_LENS"	the SharePoint encrypt Service security module on the WFE server.
"DEBUG_COMMON"	communication libraries on either the WFE or the server running the SharePoint encrypt Console
"DEBUG_CONSOLE"	the SharePoint encrypt Console
"DEBUG_CONSOLE_S"	the SharePoint encrypt Console Windows Service Application

The debug logs are written the following locations:

a. *C:\Program Files(x86)\Idera\Idera SharePoint encrypt\Idera SharePoint encrypt Debug Log.txt* on the server that is running the SharePoint encrypt Service.

b. *C:\Program Files(x86)\Idera\Idera SharePoint encrypt\Ider SharePoint encrypt Debug Log.txt* on the server that is running the SharePoint encrypt Console.

Contacts

You can reach Idera technical support via phone or email.

support@idera.com

(713) 523-4433