.Policies v18.1

- Overview
- Contingency Public Keys
    - Changing a Key Name
- Defining Policy
- General Settings
    - FIPS Mode
    - Integration
- Users / Groups
- ZIP File Creation
    - Alternate Data Stream
    - Encryption
        - Algorithm
        - Passphrase
        - Smartkeys
        - Certificates (X.509)
        - Strict Checking Options
        - Signing and Certificate Options
    - OpenPGP File Creation
    - Configuring Passphrase Complexity
    - Configuring Contingency Keys
    - Configuring Contingency Groups
- Outlook Plugin Policy Settings
    - General Settings
    - Recipient Filtering
    - Content Filtering
    - Outlook Plugin Behavior Settings
- MacOS Settings
- Performance Management
    - Agent/Service
- Cloning a Policy

Overview

Before users can use Smartcrypt successfully, system administrators must establish effective data encryption policies. Smartcrypt policies, defined on this tab, are responsible for controlling the end user experience, configuring and locking program options and most importantly, specifying administrative policy keys for use by Audit, Discovery and Data Loss Prevention (DLP) people, processes and technology.

Each client device's agent application checks in with the manager at a standard (configurable) interval. When the client checks in, Smartcrypt Enterprise Manager (SEM) applies any policy changes. Policy order on the Policies page is important; the client agent processes the Policies list from the top down. The agent uses the first one that applies to its particular user. Each policy has a defined scope of users that it applies to. When group policies are applied to a client, those policies always override the site-wide policy. If no policy is defined for a particular user, they will receive the site-wide-default policy.

For example, let's say you want to define a policy that applies to your Admin group, composed of one person from each of your departmental groups (Sales, Executive, Marketing, IT). When you add a new policy, it assumes the top position. For the Admin group policy to be applied to those departmental representatives, you should define the departmental policies first. Otherwise, you can adjust the processing order by dragging policies Up or Down in the Order column. The Site-wide Default policy cannot be re-ordered.

Most policy controls will have four drop-down options:

Option	Description
Allowed (default on)	Option is end user configurable and its default state is on
Allowed (default off)	Option is end user configurable and its default state is off
Required	Option is not end user configurable and has been locked on
Disabled	Option is not end user configurable and has been locked off

Affected policy controls and their default settings are listed in this table.

Section	Control	Default Setting
Alternate Data Streams	Store Alternate Data Streams	Allowed (default off)
Encryption		Allowed (default on)
Encryption	Passphrase	Allowed (default on)

Encryption	Smartkeys	Allowed (default on)
Encryption	Certificates	Allowed (default on)
Signing		Allowed (default on)
OpenPGP File Creation	ASCII Armor	Allowed (default off)
OpenPGP File Creation	Encryption	Allowed (default on)
OpenPGP File Creation	Encryption Passphrase	Allowed (default on)
OpenPGP File Creation	Encryption OpenPGP Key	Allowed (default on)
OpenPGP File Creation	Sign Files	Allowed (default on)
Outlook Plugin Behavior Settings	Exclude Email Signatures	Allowed (default on)
Outlook Plugin Behavior Settings	Prompt Before Zipping	Allowed (default on)
Outlook Plugin Behavior Settings	Auto-search Recipients	Allowed (default on)
Outlook Plugin Behavior Settings	Include Unzip Instructions	Allowed (default on)
Outlook Plugin Behavior Settings	Sign Attachments	Allowed (default off)
Outlook Plugin Behavior Settings	Re-Encrypt Attachments	Allowed (default on)
MacOS Policy Settings	Automatically open extracted items	Allowed (default on)
MacOS Policy Settings	Delete file(s) on encryption	Allowed (default on)
MacOS Policy Settings	Delete archive on decryption	Allowed (default off)

For administrative access to enterprise-wide encrypted content, Smartcrypt supplies two options for customers. Contingency Keys and Contingency Groups. A contingency key is included with any encrypted file created in an organization, and can be opened by anyone with access to the contingency key's private key. A Contingency Group allows all members of that group to open files encrypted by the other group members.

Contingency Public Keys

Contingency keys enable an organization to decrypt files encrypted by anyone in the organization, whether the files were passphrase-encrypted or were encrypted for specific recipients.

Contingency keys are third-party OpenPGP or X.509 formatted public keys that will be automatically included in every encryption operation performed by Smartcrypt. These can be keys that you generate outside of the Smartcrypt ecosystem in accordance with your organization's security policy.

Whether the files are password-encrypted or encrypted for specific recipient public keys, contingency keys provide a safeguard to be sure that important information belonging to the organization does not become inaccessible because no one in the organization can decrypt it.

Contingency keys must use RSA-2048 (or stronger) encryption. To add a contingency key to Smartcrypt Enterprise Manager (SEM) for use in a Policy:

1. Go to ***Archive > Policies***.
2. Click **Add** in the Contingency Public Keys section.
3. Browse your system for the public key file.
4. Click **Upload**.

When you need to open a file encrypted with a contingency key, be sure the private key is accessible.

Changing a Key Name

SEM uses the key file name to identify the Contingency Key. If you wish to change this Name, click **Edit** and type in the new Name.

Defining Policy

Smartcrypt provides a default Site-wide Default policy that Admins can edit. To add a group policy, you enter a similar form, but you will need to define the Group that the policy applies to.

General Settings

These settings regulate how often clients must connect with connect with Smartcrypt Enterprise Manager (SEM) for different purposes.

Setting	Description
Name	The name of the policy (such as "Legal Group" or "Accounting"). If you don't name the policy, SEM will describe the Policy with a date and timestamp. **Note**: You cannot edit the name of Site-wide Default policy.
Authentication Check Interval (minutes)	How often an agent re-authenticates with the Smartcrypt Manager (in minutes). Default: 15 minutes. Edit the field to change this interval.
Offline Access Limit (hours)	Smartcrypt agents cache encryption keys they have access to on the systems they run on. If an agent loses connection with the manager (For example, the user's AD account has been disabled and the agent can no longer log in) this is the maximum time (in hours) the agent will keep the keys before it automatically purges them from that device. Default: 24 hours. Edit the field to change this interval. **Note**: Keys will be re-synced if / when the device is successfully re-authenticated.
Allow Smartcrypt Mobile App Access	Enables or disables the ability to use Smartcrypt for iOS or Smartcrypt for Android for the specific user set defined in the policy. Default: Enabled.
Reset Client Defaults	Checking this box will reset any existing policy on any Smartcrypt client device before applying this new policy.

FIPS Mode

FIPS is an abbreviation for Federal Information Processing Standards, a set of standards for information processing in federal agencies in the United States. In FIPS 140 mode, encryption and decryption are done using only encryption and hashing algorithms that have been validated for compliance with FIPS 140-2 security requirements for cryptographic modules by NIST (National Institute of Standards and Technology), a branch of the US government.

Click your preferred FIPS compliance options. Your selection will turn a bright blue; this is the default for clients that this policy applies to. The site-wide policy by default displays all the options, allowing clients to change from the default. To enforce just one selection (such as **Use FIPS 140 Mode**), delete the remaining options.

Note: FIPS mode is not supported on MacOS X.

FIPS Setting	Description
Prefer fastest available algorithms	Use the fastest version of the Advanced Encryption Standard (AES) available on the system. This is the default.
Use FIPS 140 mode	Use only FIPS-validated algorithms to encrypt or decrypt files, email messages, and email attachments.
Use FIPS-validated algorithms; allow AE extraction	Always choose FIPS-validated algorithms for encryption and decryption, but allow unzipping files encrypted with the AE-2 algorithm used by some compression applications.
Prefer FIPS validated algorithms	Choose FIPS-validated algorithms over others, but does not require them.

Integration

If your user receives a ZIP archive with a single file in it, often they will want to open and read the zipped file without having to extract (decompress) it first. With the Integration section, administrators can define a set of file extensions that will automatically open. A default set of extensions, including Microsoft Office files, PDF and graphics files, are included.

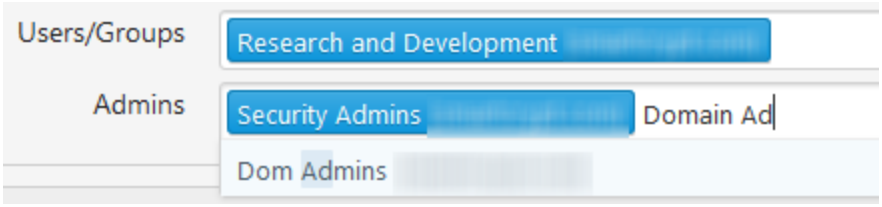
To add a file type to the list, type the extension into the edit box. You'll be asked to confirm the addition.

To remove a file type from the list, select the extension by clicking the box and press **Delete**. You may undo the choice.

Users / Groups

Use these settings to define who is subject to this Group Policy.

Setting	Description
Users /Groups	List of Active Directory users and groups for which this policy should apply. **Note**: If a user is defined in more than one policy, the first one in the policy list will be applied.
Admins	List of Active Directory users and groups that are allowed to control and modify this policy. **Note**: If a user is defined that is not currently a Sys Admin, the user will be added to the SEM Admins list configured as a Security Admin.



Note: The Smartcrypt Manager will query Active Directory to auto-complete an entry.

ZIP File Creation

Set encryption and signing policies for creating ZIP archives with the following.

Alternate Data Stream

In a sense, a file is a stream of data stored on a hard drive. When you open a file, the stream takes up space in a computer's memory. On modern Windows computers using the NTFS file system, individual files can contain multiple data streams. The content of a file is one data stream, but the same file can contain one or more alternate data streams. In the relatively rare instance that an alternate stream is created, it usually contains additional information about a file. For example, when Internet Explorer downloads a file from the Internet, it adds an alternate stream noting that the file originated outside the local network. Smartcrypt always retains this stream in archives. These streams are not common, but can add size to a file.

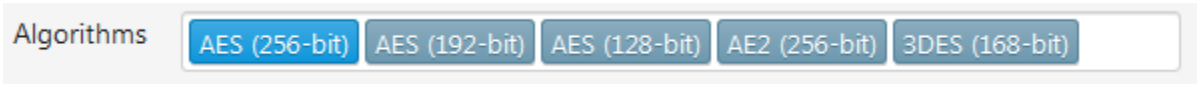
Setting	Description
Store Alternate Data Streams	Preserve the alternate data stream of a file during compression. Default setting: Allowed (default off)
Restore Alternate Data Streams	Re-apply the alternate data stream of a file when extracting. Default: None

Encryption

Administrators can choose whether to require every ZIP archive to be encrypted, and whether to allow users to Skip encrypting files on a case-by-case basis. Default: Allowed (default on)

Algorithm

Smartcrypt supports AES in several key lengths as well as AE2 (256-bit) and 3DES (168-bit). By default, Smartcrypt uses the strongest available algorithm and key length (AES-256). This displays in bright blue. Other allowed key lengths are displayed in a grayer blue. Admins can delete any algorithm to prevent its use.



Passphrase

Setting to control whether or not passphrase based encryption is allowed. Default: Allowed (default on)

Smartkeys

Default: Allowed (default on)

In addition to the basic usage settings, these options are available when Smartkeys are allowed:

Setting	Description
Allow users to create Smartkeys	Users can create and define recipients of Smartkeys. Default: Enabled
Allow users to delete Smartkeys	Users can delete Smartkeys they have created. Default: Disabled
Allow encryption with user's private Smartkey	Data can be encrypted with a private Smartkey issued with an account. **Note**: Files encrypted with private Smartkeys are not decryptable by contingency keys or contingency group members. Default: Enabled
Allow encryption using Smartkeys owned by other individuals (besides community keys)	Data can be encrypted with a Smartkey owned by another user. **Note**: "Another User" may be a Smartcrypt user outside of your organization. Default: Enabled

Certificates (X.509)

Default: Allowed (default on)

If you allow users to employ public key encryption In addition to Smartkeys, check the appropriate box to configure these options:

Setting	Description
Allow X.509 Certificates	Users can encrypt with X.509 personal certificates
Allow OpenPGP Keys	Users can encrypt with OpenPGP keys
Perform Strict checking	Strict checking identifies certificates that are valid and designated for encryption. See next section for Strict Checking Options.
Filter Issuer (CN)	If you wish to only see certificates created by a specific certificate authority, type the complete issuer's name in this box. You'll find this information in the Details tab of Certificate Properties. Look for the **Issued by** section in the Details tab, and type everything after **CN=**. For example, if all your company's certificates are issued by COMODO, type (no quotes) "COMODO Client Authentication and Secure Email CA" in this box.
Filter Subject (OU)	If you wish to only see certificates issued to someone in a specific organization, type the complete Organizational Unit (OU) name in this box. You'll find this information in the Details tab of Certificate Properties. Look for the **Issued to** section in the Details tab, and type everything after **OU=**. For example, if all your company's certificates have an OU of Corporate Secure Email, type (no quotes) "Corporate Secure Email" in this box
Check certificate revocation	This option causes Smartcrypt to warn you if a selected certificate to add a signature appears on an accessible list of certificates that have been revoked. If strict checking is also turned on, Smartcrypt does not use a revoked certificate. You must first download a list of revoked certificates from a certificate authority to use this option.

Strict Checking Options

Option	Description
Check Key Usage	Check the purpose for which the certificate is designated (encryption or signing).
Check Time Validity	Check whether the current date is within the valid range of dates for the certificate
Check Time Nesting	Check whether the period of validity of the certificate does not extend past the dates when the issuer certificate is valid. For example, if the issuer certificate is valid from February 1, 2015, to January 31, 2018, the date range during which the selected certificate is supposed to be valid does not begin before February 1, 2015, or end after January 31, 2018.

Signing and Certificate Options

Default: Allowed (default on)

Option	Description
Signature Algorithm	The signature algorithm creates a hash value for the file to be signed. The hash value uniquely represents the file: any change to the file gives it a different hash value. Comparing the hash value of the file when it was signed with the file's current hash value reveals whether the file has been changed. Smartcrypt uses the SHA2 hash algorithm at 256-bit strength by default. Stronger versions (384- and 512-bit) of SHA2 are also available. Click the button to approve the use of either of these algorithms. **Note**: You may allow the use of the MD5 or SHA1 algorithms by clicking in a blank space on this line. These algorithms are deprecated for signing keys, and not recommended.

Perform Strict checking	Strict checking identifies certificates that are valid and designated for encryption. See Strict Checking Options.
Filter Issuer (CN)	If you wish to only see certificates created by a specific certificate authority, type the complete issuer's name in this box. You'll find this information in the Details tab of Certificate Properties. Look for the **Issued by** section in the Details tab, and type everything after **CN=**. For example, if all your company's certificates are issued by COMODO, type (no quotes) "COMODO Client Authentication and Secure Email CA" in this box.
Filter Subject (OU)	If you wish to only see certificates issued to someone in a specific organization, type the complete Organizational Unit (OU) name in this box. You'll find this information in the Details tab of Certificate Properties. Look for the **Issued to** section in the Details tab, and type everything after **OU=**. For example, if all your company's certificates have an OU of Corporate Secure Email, type (no quotes) "Corporate Secure Email" in this box
Check certificate revocation	This option causes Smartcrypt to warn you if a selected certificate to add a signature appears on an accessible list of certificates that have been revoked. If strict checking is also turned on, Smartcrypt does not use a revoked certificate. You must first download a list of revoked certificates from a certificate authority to use this option.
Check certificate revocation when verifying	Check whether an X.509 certificate has been revoked that has been used to sign or encrypt any file in the archive or the archive itself

OpenPGP File Creation

OpenPGP File Creation is optional in Smartcrypt. If you want to permit clients to create OpenPGP files, check **Allow OpenPGP file creation**.

Option	Description
ASCII Armor	ASCII armor (also known as Radix-64) is a character format that creates an ASCII character stream that could be used in transferring OpenPGP files through transport mechanisms that can only handle character data (for example, email body text). Default: Allowed (default off)
Encryption	You have the option to allow users to create OpenPGP files AND disable Encryption. The default is Allowed (default on).
Encryption Algorithm	Smartcrypt offers the choice of the algorithms shown below. Different key lengths are supported for the Advanced Encryption Standard (AES) algorithm. In general, the longer the key, the stronger the encryption. Encryption also takes slightly longer in proportion to the length of the key.

Algorithm	Description
AES	The standard algorithm adopted by the U.S. federal government and in widespread use in banking and credit card operations.
CAST5	This algorithm is the default algorithm for many popular OpenPGP clients.
IDEA	This is an optional algorithm in the OpenPGP standard, used in many OpenPGP clients.

Passphrase	Default: Allowed (default on)
OpenPGP Key	Default: Allowed (default on)
Sign Files	Default: Allowed (default on)
Sign Files Algorithm	Smartcrypt uses the SHA2 hash algorithm at 256-bit strength by default. Stronger versions (384- and 512-bit) of SHA2 are also available. Click the button to approve the use of either of these algorithms. **Note**: You may allow the use of the MD5 or SHA1 algorithms by clicking in a blank space on this line. These algorithms are deprecated for signing keys, and not recommended.

Configuring Passphrase Complexity

To secure passphrase-encrypted files, use passphrases that are long enough and are not easy to guess. Smartcrypt helps administrators set requirements for both minimum and maximum passphrase lengths. Check the **Enforce passphrase complexity rules** box to do this.

For example, you can require a minimum passphrase length of 15 characters, or even 260 characters, instead of the default minimum of eight. Whenever your user encrypts with a passphrase, Smartcrypt enforces your rules by rejecting any proposed passphrase that does not comply.

You define these requirements after checking the box:

Requirement	What it means
Minimum Length	The minimum number of characters that a passphrase must contain. Passphrases shorter than this are rejected. Longer passphrases are harder to guess. You can require a minimum length as great as 260 characters. Default is 8 characters.
Maximum Length	The maximum number of characters that a passphrase can contain. Passphrases longer than this are rejected. Default is 250 characters. You can assign a maximum length as great as 260 characters.
Maximum Repeats	Sets the maximum number of adjacent, case-sensitive occurrences of the same character. A setting of 1 allows no repetitions. A setting of 2 allows two adjacent occurrences, and so on. A setting of 0 (the default) turns the option off and allows all repetitions. For example, a setting of 2 disallows a passphrase that contains aaa but allows aAa or a1a2a.
Minimum Lowercase	Minimum number of lower case alphabetical characters a passphrase requires. Default is 0.
Minimum Uppercase	Minimum number of upper case alphabetical characters a passphrase requires. Default is 0.
Minimum Digits	Minimum number of digits (integers 0-9) a passphrase requires. Default is 0.
Minimum Symbols	Minimum number of special characters a passphrase requires. By default a special character is defined as any non-alphanumeric character. Examples include `@#$%''*()_-+={}&&:;<>,.?/\`~!"* ^[]` Default is 0.
Placement rules	These rules restricts certain character types from being used as the FIRST character or LAST character of a passphrase. Use the drop-down menu next to the relevant character type (Lowercase, Uppercase, Digits, or Symbols).Choices include: **Setting** / **Description** **Prohibit in first or last position** — Rejects the selected passphrase if the selected character type starts or ends the passphrase. **Prohibit if only in first or last position** — Rejects the selected passphrase if the selected character type starts or ends the passphrase, and does not appear elsewhere in the passphrase. By default, Smartcrypt does not check for placement.

Configuring Contingency Keys

Choose from a list of existing contingency keys associated with this installation.

To define a contingency key, return to the main Policies page and click **Add New Contingency Key**.

Configuring Contingency Groups

A Contingency Group allows all members of that group to open files encrypted by the other group members. Choose from a list of Active Directory users to define Smartcrypt users that will be able to decrypt all information encrypted by users in this policy.

Outlook Plugin Policy Settings

The Smartcrypt Desktop application on Windows has a plugin that can run to control encryption operations for outgoing email in Outlook. There are several policies that dictate the use and control of the encryption settings.

Check the **Enforce Outlook Integration** box to set policy options for the Smartcrypt Outlook Plugin. The following options will display.

General Settings

Setting	Description

Smartcrypt Plugin Actions

This allows for control on the default and available actions from the Smartcrypt Outlook Plugin. The default option displays in bright blue. Other allowed actions are displayed in a grayer blue. Admins can delete actions to prevent there use.

Action	Description
Encrypt Message body and attachments	Including this option allows users to send an email that is an email body encrypted email. The only part of the message that is not encrypted into a .zip archive is the subject line. This will require the recipient to use a email mime (.eml) viewer to read the original message. This is the most secure option, but also the most obtrusive to your normal email workflow.
Encrypt Attachments only	Including this option allows users to send an email and ignore the body of the email message, and only encrypt the attachments to the email. The attachments will be gathered and included in 1 zip archive and then encrypted.
Compress attachments only	Including this option allows users to send an email and ignore the body of the email message, and only compress the attachments to the email. The attachments will be gathered and included in 1 zip archive and then compress, but not encrypted.
Skip Actions	Including this option allows users to send an email that bypasses the Smartcrypt Outlook Plugin. If this bypass is not desired, the option should be removed from the list of available actions.

Extensions to Include

Defining extensions in the extensions to include creates a small subset of extensions that will be considered by the Smartcrypt Plugin when performing **Compress attachments only** and **Encrypt Attachments only** actions.

Example

Setup - The policy is set to include extensions ".pdf"

User Action - The user sends an email with a .PDF and attached the the email

Smartcrypt Outlook Plugin Option Selected	Action	Description
Encrypt Message body and attachments	Email body, and all attachments encrypted.	Since email body encryption encrypts the body and attachments, the extension filters are ignored and the body and attachments are encrypted.
Encrypt Attachments only	PDF is added to encrypted archive.	Since there is a direct match on the extension in the email, the attachment is encrypted by Smartcrypt.
Compress attachments only	PDF is added to compressed archive.	Since there is a direct match on the extension in the email, the attachment is compressed by Smartcrypt.

User Action - The user sends an email with a .PNG and attached the the email

Smartcrypt Outlook Plugin Option Selected	Action	Description
Encrypt Message body and attachments	Email body, and all attachments encrypted.	Since email body encryption encrypts the body and attachments, the extension filters are ignored and the body and attachments are encrypted.
Encrypt Attachments only	No action.	No direct match on extension, no actions taken.
Compress attachments only	No action.	No direct match on extension, no actions taken.

<table>
<tr><td>Extension to exclude</td><td>Defining extensions in the extensions to exclude creates a small subset of extensions that will be ignored by the Smartcrypt Plugin when performing "Compress attachments only" and "Encrypt Attachments only" actions.

<u>Example</u>

Setup - The policy is set to exclude extensions ".pdf"

User Action - The user sends an email with a .PDF and attached the the email

<table>
<tr><th>Smartcrypt Outlook Plugin Option Selected</th><th>Action</th><th>Description</th></tr>
<tr><td>Encrypt Message body and attachments</td><td>Email body, and all attachments encrypted.</td><td>Since email body encryption encrypts the body and attachments, the extension filters are ignored and the body and attachments are encrypted.</td></tr>
<tr><td>Encrypt Attachments only</td><td>No action.</td><td>Direct match on extension, no actions taken because extension is set to be excluded.</td></tr>
<tr><td>Compress attachments only</td><td>No action.</td><td>Direct match on extension, no actions taken because extension is set to be excluded.</td></tr>
</table>

User Action - The user sends an email with a .PNG and attached the the email

<table>
<tr><th>Smartcrypt Outlook Plugin Option Selected</th><th>Action</th><th>Description</th></tr>
<tr><td>Encrypt Message body and attachments</td><td>Email body, and all attachments encrypted.</td><td>Since email body encryption encrypts the body and attachments, the extension filters are ignored and the body and attachments are encrypted.</td></tr>
<tr><td>Encrypt Attachments only</td><td>PNG is added to encrypted archive.</td><td>No direct match on extension, the attachment is encrypted by Smartcrypt.</td></tr>
<tr><td>Compress attachments only</td><td>PNG is added to compressed archive.</td><td>No direct match on extension, the attachment is compressed by Smartcrypt.</td></tr>
</table>
</td></tr>
<tr><td>Exclude Email Signature</td><td>If this option is enabled, text and pictures included in the signature element in an email will not be included in the archive and will appear in plain text in the email. Default: Allowed (default on)</td></tr>
</table>

Recipient Filtering

Recipient filtering allows for specific rules to apply based on who the email is being sent to. The Smartcrypt Outlook Plugin can scan the To, and Carbon Copy (CC) fields and mandate certain Smartcrypt Outlook Plugin actions occur based on recipients.

To enable recipient filtering, type the email address to filter in the field next to the action you want done. Use wildcards to identify multiple addresses, as you see in the following example.

Example Recipient Filtering Rules

Smartcrypt Outlook Plugin Option	Email List
Email Body Encryption	legal@pkware.com
Encrypt Attachments	
Compress Attachments	
Skip Actions	*@pkware.com

In this example, any email addressed to legal@pkware.com will automatically apply the action to encrypt message body and attachments, regardless of what the user has selected.

An email to any other @pkware.com email address will skip all processing. In this example, all internal email to @pkware.com except to the legal mailbox would be un-encrypted, and un-compressed.

Content Filtering

Content filtering allows you to mandate a Smart Filter Bundle for Discovery purposes. Click in the **Discovery Filter** field, and use the drop-down menu to display the current list of Smart Filter Bundles (defined on the Discovery page). Select a filter bundle, or leave it blank.

Check **Override Recipient Filtering** to resolve conflicts between the actions mandated by the Discovery Filter and the actions mandated by the Recipient Filter.

Outlook Plugin Behavior Settings

The Outlook Plugin has some basic behaviors that trigger a different user experience. The same 4-state drop down options apply here as well (Allowed On, Allowed Off, Required, Disabled) to the following options:

Behavior Option	Description
Prompt Before Zipping	There is another dialog that the Plugin can open to select user controlled options for Smartcrypt. This is useful when sending email outside of outlook (from a "send an email option" in other applications). Default: Allowed (default on).
Auto-search Recipients	Auto-Search Recipients will look at the users existing Smartkeys are try to pick a Smartkey that all recipients have access to. If a Smartkey is not found, a new only can be created with all recipients included on the email message. Default: Allowed (default on).
Include Unzip Instructions	Smartcrypt can include a plain text (non encrypted) document with instructions on how to decrypt the attachment. Default: Allowed (default on).
Instructions	Text added here will be provided in a text file that is sent out automatically when a user sends an encrypted attachment. This text can be plaintext or HTML formatted. **Note**: This is not used when email body encryption is activated or when discovery filter override recipient filtering is not checked.
Sign Attachments	The zip archive produced by Smartcrypt can be automatically signed with a digital certificate (when present). Default: Allowed (default off).
Re-Encrypt Attachments	Users can change the encryption on existing ZIP archives attached to an email message. This option must be set if you want Smartcrypt to encrypt existing archives. Default: Allowed (default on).
Default ZIP Name	Smartcrypt gives the same, generic name to all ZIP file attachments that contain multiple files. In this field, specify the generic name to use. When you zip a single attached file, ordinarily the ZIP file is named after the attached file itself. For example, if the attached file is *my_file.docx*, Smartcrypt names the ZIP file *my_file.zip*. (Exception: If the Security option to Encrypt file names is set, the generic name is always used.) Following the **Default ZIP Name**, you can also define an alternate three-character extension for ZIP archives. Some networks have security settings that prevent file attachments with the ZIP extension from being sent or received. Use this feature if this is an issue for you or your recipient

If a standard name is required for all ZIP attachments (to possible be allowed through a mail gateway or to skip some other processing), a standard name can be defined as well by entering a name in the **Default Zip Name** field.

MacOS Settings

Setting	Description
Extract file location(s)	By default, Smartcrypt extracts compressed files in the same directory as the original archive. If another file with the same name is located in that same directory in Finder, the newly-extracted file is added as a copy of the original file. This setting allows you to select a new default folder, or be prompted for a destination folder each time you open an archive. Choose from these options: • Original archive folder (default) • Your **Desktop** • **Other** folder. This option opens a Finder box. Choose any folder for all extracted files to be extracted to. • **Prompt for folder**. When you select this option, you will be asked where to put the extracted files each time you extract an archive with Smartcrypt.

Extract email attachment location(s)	By default, Smartcrypt extracts compressed files in the same directory as the original archive. If another file with the same name is located in that same directory in Finder, the newly-extracted file is added as a copy of the original file. This setting allows you to select a new default folder, or be prompted for a destination folder each time you open an archive. Choose from these options: • Original archive folder (default) • Your **Desktop** • **Other** folder. This option opens a Finder box. Choose any folder for all extracted files to be extracted to. • **Prompt for folder**. When you select this option, you will be asked where to put the extracted files each time you extract an archive with Smartcrypt.
File select action option(s)	Define what happens when a user selects an archive. **Extract Archive**: Unzip the files in the archive in Finder. **View Archive**: Display the files in a Smartcrypt window.
Automatically open extracted items	When the user extracts file(s) from an archive, open them in the associated application. Default: Allowed (default on).
Delete file(s) on encryption	When a file is encrypted, the unencrypted file is removed from the system. Default: Allowed (default on).
Delete archive on decryption	When files are decrypted (encryption is removed), the encrypted archive is deleted. Default: Allowed (default off).

Performance Management

Agent/Service

This setting can be enabled from the support page

Setting	Description
Max Worker Count	The minimum number of worker threads when using the default optimal worker count algorithm. Default: 12
Min Worker Count	The maximum number of worker threads when using the default optimal worker count algorithm Default: 2
Worker Job Sleep (ms)	The amount of time to sleep after a job is finished (successes AND failures). Default: 0

Cloning a Policy

Administrators can develop very finely-grained policies. Policies can be applied to individual users and groups, defined narrowly or widely. As an administrator, you might find that an effective set of permissions for one group simply do not work for one group. In cases where administrators want to tweak some policy settings for some users, you can *Clone* a policy to copy all its settings in a separate policy. You can then use the cloned policy as a template for the clone. When you have completed changing the settings in the clone, save the changes.

In the User and Group Policies section, click **Clone** to the right of the Policy you want to serve as the template for your new version. The new policy is named "Policy cloned from *<original policy name>* at *<timestamp>*.

You can then Edit the cloned policy as you would any other.

Note: You do not need to clone the Site-wide Default policy. It is the template for any new policy.