SSProtect :Email

Updated 16.06.15
SSProtect v2.3.8

INTRODUCTION

SSProtect is a distributed cryptosystem designed to protect application data from today's and tomorrow's most advanced electronic threats. The software is easy to deploy and use while maintaining independence from the software, services, and infrastructure decisions you make in addressing your needs.

This Guide describes SSProtect :Email, an Outlook Add-In that utilizes SSProtect to apply protections to email message content. :Email utilizes :Expand, the command line interface that extends SSProtect for third party software integration. Consult SSProtect :Email for details related to programmatic integration.

Getting Help

If at any time you require assistance, you can email Support at support@definisec.com. You can also visit our online support site at https://support.definisec.com. Review *SSProtect Document Index* for guidance finding additional information on other system components.

EMAIL MESSAGE PROTECTION

:Email is an optional component in the *SSProtect* product suite extending protections to Microsoft Outlook Email. *:Email* runs as an Outlook Add-In, and:

- Applies *SSProtect* data protection capabilities to Outlook-based email message items
- Supports both Outlook HTML and so-called, "plain text" message formats
- Protects email messages both at-rest (stored) and in-transit email (communications)
- Utilizes patent-pending optimized cryptographic offloading for secure, efficient protection
- Optionally integrates 2-factor authentication into each attempt to access sensitive messages
- Provides flexible policy configuration designed to guide users through secure transactions
- Stores data mgmt events using *:Assess* to provide data exposure risk information

:Email provides end-to-end email protections for almost every commonly used email system available today without imposing restrictions on message content or functionality.

"Protection By Default" Philosophy

:Email has been designed to provide flexible email message security through policy configuration used to address workflow security. Default procedures are focused on making sure sensitive information retains effective protections unless purposeful user actions are undertaken to remove or change these efforts. The software thus intends to provide a high degree of protection with flexibility to meet the most demanding needs while limiting unintended plaintext exposure.

IMPORTANT: *Please refer to the Message Save section for important details regarding data storage.*

Requirements

:Email is compatible with Outlook 2010 and Outlook 2013 running on Windows 7 or higher. The software works with 32-bit and 64-bit Office installations and with 64-bit Operating Systems. The Add-In utilizes Microsoft .NET; dependencies are handled by the multi-phase installer. It also uses *:Expand* to provide message protection, which is available only when *SSProtect* is running. *SSProtect* automatically starts on login, and it is accessible from the taskbar's notification tray.

Administrators

Administrators do not entertain special privileges with *:Email*, though SSProtect Administrative Panel account configuration governs overall capability. If for example you disable an *SSProtect* account, users will not be able to access protected mail content or send protected messages. Email continues to process as it is outside the scope of *SSProtect* components, thus re-enabling an account at a later time will permit the user to access previously protected items.

If your Organization is already using *SSProtect* but not setup to use *:Email* and you would like to deploy it, contact your DefiniSec Representative; this can be enabled for your Organization and deployed to existing *SSProtect* users in minutes. Once enabled, each *SSProtect* user will on their next login receive the Add-In component required for operation.

INSTALL/UNINSTALL

Installing

SSProtect provides dynamic installation and configuration logic to optimize your environment for features applied by your Administrator. Install *SSProtect* and register using the instructions you receive in email. On first login, *SSProtect* will adjust your environment to match policy settings. As an *:Email* user, you will be prompted to install *:Email*, then the software will launch an independent install package to copy and register the Microsoft Outlook Add-In required for *:Email*. If you do not have the Microsoft .NET Framework installed, you will be prompted to do so.

Once the external installers complete and you register your account, you can start Outlook and begin protecting messages. If you need to re-install *:Email*, you can do so from the *SSProtect Local User Info* dialog reachable from the context menu for SSProtect found in the notification panel. For more information, consult the *SSProtect Guide*, contact your DefiniSec Representative, visit https://support.definisec.com, or email support@definisec.com.

Disabling and Uninstalling

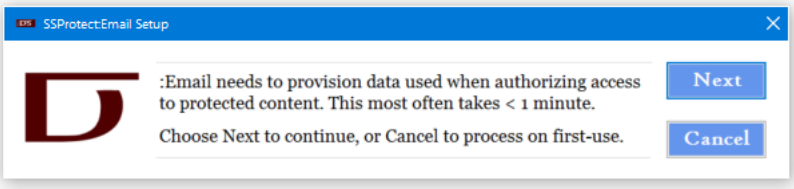
As an Outlook Add-In, there are several ways to disable and/or uninstall the package:

1. From the Outlook Backstage View accessible through the File tab, choose Options then select the Add-Ins panel. From this interface enable and disable *:Email*.
2. Navigate to the Start Menu and choose *:Email* to run the registration package. Choose Unregister to remove the Add-In from Outlook's scope. You can repeat this task and Register the application to re-enable the Add-In. Restart Outlook to apply changes.
3. Uninstall from Add/Remove Programs in the Control Panel; choose *:Email*.

Provisioning

KODiAC Cloud Services tracks *:Email* account configuration data to verify authorized email recipients. When you compose and send a message, *:Email* walks through the recipient list to determine which, if any, of your recipients will not be able to access protected content. *:Email* then takes corrective action for those recipients, based your Policy configuration (summarized in Policy Summary).

In order for *:Email* to retain accuracy in determining authorized collaboration peers, it must share with *KODiAC* internal details Outlook provides at runtime. You will be prompted to authorize this transaction before data is stored. This process is initiated each time you start Outlook with an active *SSProtect* login that has not been previously provisioned. The notification is shown below:

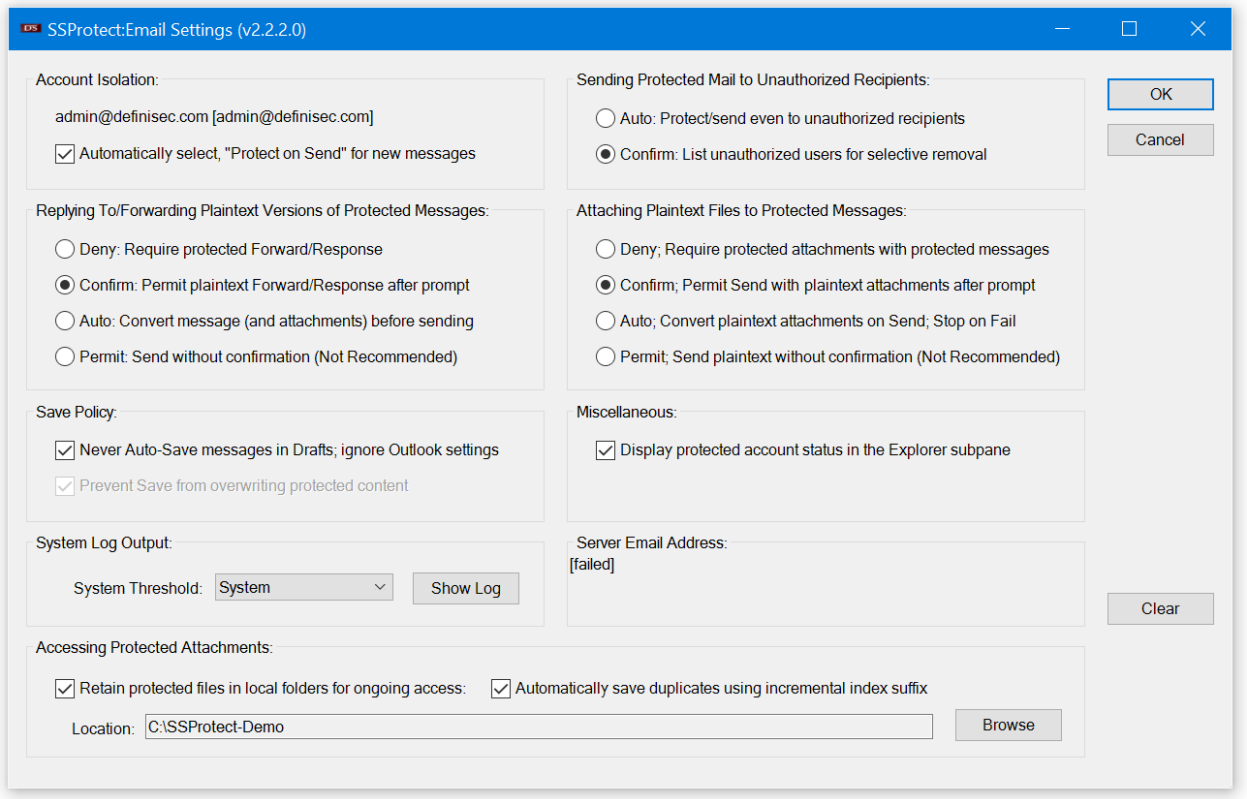


When you see this notification, choose **Next** to provision the account or **Cancel** to defer operation. You will be prompted to login to *SSProtect* and will also need to provide your 2nd factor authentication token.

This operation only takes a few seconds, at which point you are then returned to Outlook for further processing. If the process fails, your account will retry this operation when the information is necessary, which is most likely the next time you send information.

The status of this operation is shown in the *Settings* dialog, under the *Server Email Address* identifier. If this shows *[failed]*, this operation did not succeed. Reset by choosing **Clear**. The next time the information is required, :Email will retry.

The *Settings* dialog, with a failed provisioning result, is shown on the following page.



Note that this is unique to each individual email account, since each is associated with a different *SSProtect* account. As you change files and use different email addresses, you will work through provisioning steps required for each account. You will not be notified again unless your email address is changed, or other mail server configuration details are modified. The procedure is the same – it will update your data accordingly.

PROTECTING EMAIL

The general procedure for using Outlook does not change. There are caveats associated with protecting data, though the procedure is simple and straightforward. There are numerous options that allow you to control various aspects of operation, covered in subsequent sections. All are designed to provide flexibility beyond the basic default configuration, which is designed to retain a protected workflow for messages and message attachments. Policy specialization allows you to make adjustments for nuances associated with your operating dynamics.

IMPORTANT: *SSProtect'ed email messages use HTML format to carry embedded objects and advanced formatting. If in the Trust Center Settings you have configured Outlook to read messages in plaintext format, conversion will fail and you will not be able to access decrypted content.*

Sending a Protected Message

Compose a New Message to an SSProtect Organization peer or Trusted Third Party using your email account associated with *SSProtect*. Check, *Protect On Send* in the ribbon bar, then Send.

Opening a Protected Message

When you receive a protected message and open it, *SSProtect* will prompt you for required credentials based on your account settings. Once you authenticate, the message is decrypted and presented to you in its' original form. When you close the message, it returns to encrypted form. By default you are not able to completely overwrite encrypted content. See In-Place Protection.

NOTE: *You must open the message in order to convert to plaintext; the preview panel will only show the encrypted/encoded information. Double-click to open and acknowledge any SSProtect prompts.*

Operational Flexibility

The *:Email* policy options are, by default, suitable for most situations. It's best to start with the defaults and make modifications as they become relevant, taking on each piece individually. The following walkthrough shows you how to use :Email and answer, *What happens if you…*

1. …send a message from an email account that doesn't match your *SSProtect* user?
2. …send a protected message to recipients not authorized to read it?
3. …attach unprotected files to a protected message?
4. …reply to or forward a protected message in unprotected format?

Procedure

1. Start Outlook

   SSProtect is configured to start when you login to Windows. If you have modified this behavior, Outlook will attempt to start *SSProtect* at startup.

   Status is given by the Explorer *:Email* ribbon control group, which updates when you close a message and at other times; this is not a real-time indicator. See SSProtect Concurrency.

2. Select New Email to create a new message

   Every Outlook account you use provisions data with *KODiAC Cloud Services* for access authorization. This data is specific to the recognition that collaborative peers have access to protected content – it does not govern access to protected content, and does not have any impact on protection effectiveness.

   Until you properly provision each Outlook account, others will not see you as a peer with authorized access. For some, this is a matter of inconvenience when sending protected messages – they will be prompted that you do not have authorization to access content, but they can override stipulations and force delivery. For others, this is not possible due to their policy configuration – which prohibits any kind of protected sharing until the matter is resolved.

   For this reason, proper provisioning is critical. For more information, see Provisioning.

3. Check/uncheck *Protect On Send* as desired

   Protect On Send is set by your Default Protected Send policy setting. If you intend to protect this message, you must start from the Account that matches your *SSProtect* configuration and check this option; it will not be available from other accounts. See Protective Scope.

4. Enter your recipients

   When you Send a protected message, your Settings dictate handling for recipients not authorized to access your SSProtect content. See Recipient Processing.

5. Type a subject line

   :Email does not currently offer the ability to obfuscate the Subject line in any way.

6. Edit the email body text using HTML or Plain Text format; Rich Text is not supported.

   HTML uses special processing for embedded objects. See Inline Attachments.

7. Add attachments

   :Email does not by default protect attachments added to protected messages. See File Attachments.

8. Choose Send to deliver the message:

   a. If you have addressed recipients that *:Email* will not authorize to access your information, your Settings will dictate handling. See Recipient Processing.

   b. If you have attached plaintext files, Settings dictate handling. See File Attachments.

   c. If you are replying to or forwarding a protected message with an unprotected message, your Settings will dictate handling. See Reply and Forward Processing.

9. Respond to *SSProtect* authorization requirements

   Enter your *SSProtect* password and/or provide your 2nd factor authentication token as prompted. With authorization, your email is protected then sent.

10. Navigate to your Sent Items folder to review your protected message.

    By default, Outlook keeps a copy of your outgoing messages in the Sent Items folder.

Default Protected Send

If most of your messages will be protected, have *:Email* automatically protect messages by checking, *Protect items on send* in the *Account Isolation* group in Settings.

SSProtect Concurrency

For *:Email* to process protected messages, *SSProtect* must be running. You are able to compose and send unprotected messages even with the account being protected by *SSProtect*, though you cannot send protected messages or access protected data when *SSProtect* is not available.

SSProtect Explorer Status Indicator

Outlook automatically starts *SSProtect* on startup, if possible. The Explorer ribbon contains an *:Email* control group holding Settings and About buttons and also a status button labeled :Email Active or :Email Inactive, depending on state at startup.

Status changes as *SSProtect* starts and stops, and updates when you open and close messages. If *SSProtect* is not running, click on :Email Inactive and *:Email* will attempt to start it for you.

Protective Scope

:Email does not apply to all message, only those associated with *SSProtect* email addresses. When you create or open a message for an account that is active in SSProtect, the ribbon *:Email* control group will have an :Email Active status under the About button. This tells you that the message can be protected, and your Settings will apply as you work.

When you create or open an email from a different *:Email* account, this indicator will not be present and all controls except Settings and About will be disabled.

Note that this indicator is not dynamic during the lifetime of the message; if *SSProtect* is running when you create or open a message from your *:Email* account, and during editing it closes, the indicator will not change. You will be notified of the missing state when you attempt to send, if necessary. You will not lose data; you will be returned to the message to recover your work.

Explorer Status Subpane

Along with the Active and Inactive indication, you have the option of displaying an Explorer subpane that contains the status of *SSProtect*. This will show you the active account, which can facilitate efficient navigation when you use multiple *SSProtect* accounts and multiple *:Email* accounts at the same time.

The display pane can be enabled and disabled in Settings, *Display protected account status in the Explorer subpane checkbox*.

Recipient Processing

When you address recipients, it's not always easy to know who is authorized to receive protected content. When you Send, *:Email* will determine the set of unauthorized users, if any, and present them to you for review if your related Setting is Confirm – else it will send to your list.

Enumerating Authorized Recipients

Authorized users are those provisioned in your Organization or granted Third Party Trust status by Administrators and Delegates. Users cannot enumerate this list. Administrators and Delegates can by accessing Administer Users in *SSProtect*.

Unauthorized User Receipt

Unauthorized users will see protected messages the same way they are initially presented to you in your Sent Items folder (before you open and access plaintext). Unauthorized users cannot access your protected messages, though if they are later provisioned as a member of your Organization or a Third Party Trust, they will be able to decrypt previously received messages.

Unauthorized Recipient Policy Setting

In the Settings dialog, change *Protected Mail to Unauthorized Resources* to one of the following:

Auto: protected email is automatically sent to all recipients – valid or not

Confirm: you are prompted with unauthorized users and given choices on how to proceed

If you choose Confirm, and you attempt to Send a protected message to one or more unauthorized users, you will be prompted to choose one of three possibilities:

Yes: Remove unauthorized users and send the message

No: Send the message to all users, authorized and unauthorized

Cancel: Return to the message for further modification

Unprotected messages, and those from other accounts, do not trigger this rule.

Attaching Files to Outgoing Messages

File attachments are handled independent of message text. When you attach files to your message, *:Email* determines at that time whether the attachment is an SSProtect'ed file or plaintext. This status is held for processing when you Send, at which point your Settings determine behavior.

Policy Options

In the Settings dialog, change *Attaching Plaintext Files to Protected Messages* to one of the following:

Deny: never permit plaintext attachments – you will receive an error on Send if you try

Confirm: you are prompted and can permit or deny Send processing as desired

Auto: this will automatically convert plaintext attachments, one by one – each requires 2FA*

Permit: *:Email* will automatically send your message independent of attachment state

Permit is not recommended, it's easy to accidentally attach plaintext files to protected messages.

* - Note that each attachment requires its own second factor authentication step, which means several attachments in a single email end up prompting you for several 2nd factor authentication actions, if relevant. This will in the future be consolidated, but for now you will have to perform any acknowledge one for each file – and then once again for the message itself.

Attachments on Disk

When you attach a file to a message, the source is not exposed to the Add-In. In order to work with the file, *:Email* saves it to a temporary location then removes it when it's no longer needed. This may be immediately after a message is discarded, or only after Outlook is shutdown. This folder is chosen by using the Location given in the Settings dialog, and as described in the next section. However, outbound attachments are written to a subfolder to insure they do not collide, in name, with attachments associated with incoming messages.

Any conversion that's performed on send is performed in these files. When a plaintext attachment is converted, it is saved to disk, removed from the message, converted with *SSProtect*, then re-added. The disk-stored item is then deleted. The subfolder to the given Location is removed on Outlook exit.

Accessing Attachments in Received Messages

There are several configuration items that give you fine-tuned control over the way attachments are handled. But first, it's important to understand how attachments work before applying this to the policy options.

Operation

When you open a message with an attachment, viewing the attachment results in copying the file to a cache folder on disk, then using that file location. You may notice this when you use Outlook without *:Email* and try to Save As with any attachment you open. However, *SSProtect* specifically protects this folder from outside access to insure that interim plaintext content passing through this folder isn't exposed to the outside world.

As such, *:Email* uses a different folder for processing attachments, and you must specify a location for these actions. By default, this is your local Windows profile's *My Documents* folder, usually accessible from a *Library* shortcut in Explorer. You can change this to use any folder *SSProtect* works with.

When you open a single attachment multiple times, the attachment has to refer to what's already stored on disk, or has to save the attachment again then re-open it. Outlook uses the latter approach, and *:Email* does the same. This means any changes you make before closing get overwritten the next time you access the same attachment – or one with the same name from a different message.

To better manage this procedure, *:Email* provides a way to automatically save message attachments using a numbered suffix that increase with each save operation. This allows you to revisit the folder and pull information from the modified files anytime you wish.

Policy Options

The following options, available in the Settings dialog, provide control over message attachment behavior:

Retain protected files in local folder for ongoing access

This tells *:Email* not to remove saved attachments when you shutdown Outlook. Thus, any message attachment you opened will remain in your chosen Folder. Else, these are deleted when you exit.

Automatically save duplicates using incremental index suffix

Rather than prompt you if you open the same attachment twice, *:Email* will append `-1`, `-2`, `-3`, etc. to the filename. For example, `attachment.txt`, `attachment-1.txt`, `attachment-2.txt`, etc. If you don't select this option, opening the same attachment multiple times overwrites the original. Thus, if you access the attachment and make changes, opening it again overwrites those changes.

Location

This determines the Folder you use when attachments are saved, as noted in the previous text.

Attachment Location

As noted, the Location determines where saved attachments are stored, and they can be indexed to remain unique. A subfolder is used as a temporary working folder when saving an attachment for conversion prior to re-attachment and delivery.

The content in these folders should remain consistent and available for you throughout the lifetime of multiple Outlook sessions. You should however go through the files' contents and pull changes you need to a different working area as soon as possible, then remove the file that you no longer need. This work area may not always retain data integrity and it's a better habit to work in your own independently managed folders than try and integrate your work with the logic :Email is applying, which will undoubtedly change.

As a matter of practice, try not to rely upon the attachment folder except for local changes and data that you copy from the* Location *folder on an as-needed basis. Outlook does not empty the contents of this folder when you configure it for retained storage. As such ***you will need to manually remove items over time***, else the folder will become increasingly difficult to work with.

Inline Attachments

HTML formatted messages often include embedded objects with links. Different mail systems take different approaches despite prevalent use. Incompatibilities still exist in certain cases, which is seen when receiving a Winmail.dat attachment in a non-Outlook mail system.

:Email handles embedded HTML objects when protecting messages. Their content is read from the original message and included in the protected data stream for reconstruction when an authorized user accesses the message.

Unresolved Inline Attachments

Outlook provides safeguards against automatically downloading external message content. This is evident when you see, "*Click here to download pictures. To help protect your privacy, Outlook prevented automatic download…*". If you do not click this reference to download content before replying to or forwarding the message, the references appear as unprotected attachments. As a result, if you try and deliver a protected message, your *Attaching Plaintext Files to Protected Messages* Setting will dictate subsequent behavior. This can sometimes lead to a confusing prompt that plaintext attachments are included with an HTML message that has not yet been processed. These artifacts are transmitted with the protected message but as plaintext attachments, but not displayed on the recipient's machine until he/she authorizes rendering by using the associated Outlook controls.

Reply and Forward Processing

You can determine how to manage replies and forwarding actions with protected content from the Settings dialog by changing *Replying to or Forwarding Protected Messages* to one of the following:

Deny: error on Send if you reply to or forward a protected message in plaintext format

Confirm: permit plaintext reply to or forward of protected messages only after confirmation

Auto: convert on Send if you reply to or forward a protected message in plaintext format

Permit: send even if you reply to or forward a protected message in plaintext format

We do not recommend Permit; it is easy to open a protected message, edit, and forget to protect before replying or forwarding.

ACCESSING EMAIL

:Email automatically prompts you for authorization when you open a protected message. After you review its' content and choose to close, the plaintext content is replaced with the encoded ciphertext to insure unauthorized local access is mitigated. This behavior can be changed (below).

Accessing protected attachments requires policy settings to match your system's dynamic performance. See Additional Settings.

In-Place Protection

Opened messages include two ribbon control commands – *Protect Now* and *Release Protection*. Apply protections to any message item in any folder with *Protect Now* and take advantage of the same protections *:Email* provides to incoming and outgoing content.

Release Protection removes protections and stores the mail item in plaintext. Attachments are stored in `My Documents\SSProtectEmail`, however are not removed if/when you delete the mail item.

Saving Protected Messages

Store plaintext from protected content by using the Release Protection feature. If you open a protected message and convert to plaintext, ***Save will not give you an error but will not store the plaintext in any of your Outlook folders***.

However, if you Forward or Reply To protected content that you have accessed in plaintext form, your plaintext state will be stored in the Drafts folder (or the folder you have configured via Outlook settings) but the original ciphertext content remains with the original item you opened. If you navigate to the Draft folder and Discard changes, the original message in protected form remains.

When using :Email, you will be prompted to save your changes anytime you close a new, reply, or forwarded message item – even if you have not made any local chances. As noted above, plaintext goes in the Draft (or other configured target) folder while any original item retains ciphertext in its original location.

Auto-Save Policy

Outlook's Auto-Save policy can, after a period of idle time, saves a draft of an open message. *:Email* can stop this behavior when you choose *Never Auto-Save message drafts* in the *Save Policy* group of the Settings dialog.

REPLY ALL AND FORWARDING

When protecting a message, you can determine whether or not recipients are allowed to Reply All and/or Forward the message when accessed by an authorized recipient. Use the Ribbon Control Group to activate, "Disable Replay All" and/or "Disable Forward". These controls are either presented as checkboxes you can check, with descriptive text, or with an icon that represents the setting.

When a recipient receives a protected message with Reply All disabled, the Reply All button will be gray. Similarly, if Forwarding is disabled, the Forward button will be gray. Keyboard shortcuts for these actions will also be disabled.

Working Around Reply All and Forwarding Policy

SSProtect has been designed to provide a default protected workflow but does not seek to make it impossible for users to deviate. This flexibility avoids the all too common set of workarounds end-users always find ways to employ, which either defeat the entire purpose of the control or, in some cases, create a scenario that is higher risk than not having any protective controls applied in the first place.

If you must use Reply All or Forward with a message configured to preclude such action, Release Protections to convert the item to an unmanaged, unprotected state then utilize the re-enabled Reply All and/or Forward buttons as necessary.

NOTE: *Though it is possible to enforce the continued disabled state of both Reply All and Forward after protections have been removed, as noted in the preceding text, the decision to remove Reply All and Forwarding policy selection when protections are released retains consistency and avoids workarounds end-users will employ to avoid such limitations (such as not using protections at all to avoid this inconvenience).*

POLICY SUMMARY

:Email provides Policy Settings to govern application behavior. "Default" behaviors that minimize the possibility of human error can have a tremendous impact on the security posture of a system or organization. Proper utilization of these features more closely aligns the software with its' original design purpose.

System Logs

The following describes the policies associated with, and operation of, the logging mechanism.

- System Log Output: Information is stored in a log file that can be used for troubleshooting. There are 8 levels: Trace, Debug, Warning, Error, Info, Severe, Critical, and System. When you choose, "less verbose" levels are included; choosing Error includes Info, Severe, Critical, System.

  The log holds a single day's events. Choose Show Log to launch (Notepad.exe) and view content in:

  ```
  C:\ProgramData\DefiniSec\SSProtect\SSProtect_Email.log
  C:\ProgramData\DefiniSec\SSProtect\SSProtect_Email-previous.log
  ```

  The previous day's information is updated after midnight each day, and the current day's log is reset.

  When you change the System Threshold, output changes go into effect for resources as they are created.

NOTE: *Data logging has a noticeable impact on performance. We recommend leaving this setting at* Critical *except when troubleshooting a specific problem. Don't forget to reset.*

Procedure Settings

These settings are discussed in the Procedure walkthrough.

- Protect items on Send: If you typically send protected email from your *:Email* account, set this and you can manually override by unchecking, "Protect on send" when composing email.
- Unauthorized Recipients: It's easy to compose an email to a large audience then send it in protected format, not realizing some members will not be able to ready it. You can have the software ignore this dynamic and send protected email anyway, or it can prompt you with the list of users that are not

authorized and permit you to automatically remove them, ignore and continue with protected email, or back up and change your recipient list or even whether or not the email should be protected.

- Protected Reply: The software can prevent you from sending an unintended plaintext response to a protected item. This happens quite frequently and as a safeguard offers simple yet high-value protection against common operations.
- Plaintext Attachments: It's easy to lose track of disparate system protections, and *SSProtect* utilizes cooperative components to provide a consistent interface for all target materials. When replying to protected email, it's sometimes easy to lose track of whether or not the response should be protected, and the software can be configured to not only prevent plaintext responses to protected items (above), but can also make sure you only include protected attachments. At present, *:Email* will warn you of any inconsistency, and in the future will be able to apply individual file protections on your behalf.
- Never Auto-Save: The software can be configured to deny Outlook Auto-Save behavior despite Outlook configuration to the contrary. This way, while responding to a sensitive, protected email (and thus authoring a plaintext response), an interruption that pulls you away from your computer for more than a few minutes won't result in storage of sensitive interim plaintext materials in email Folders. These events can go undetected for long periods of time, exposing critical data to anyone that gains temporary access to your computer.
- Disable save on close: When you open a protected message, its' content is replaced with plaintext thus prompting you to save changes on close. Use this (recommended) to skip.
- Prevent Save from overwriting: You cannot save plaintext messages that are the result of converting protected content for editing and/or review. This is the automatically enforced setting which insures all protected data, accessed by default, returns to its' protected state.
- Display status in the Explorer subpane: Because *SSProtect* is active for a single account at one time, and because Outlook manages multiple accounts concurrently, *:Email* displays a small box with a message and the abbreviated DefiniSec logo at the bottom of your message list indicating which account is being managed. Remember that this is not a real-time display, and changes only on certain events. Future releases will address these static gaps.
- Server Email Address: This is the server address your account uses to identify itself to others. If this says [failure] or similar, use the Clear button to reset it and force a reconfiguration.
- Retain protected files: This option keeps Outlook from removing any attachments that you have opened from within email messages. Every time you open a message, it overwrites any pre-existing instance of the same filename, even if the file is different and from a different message, but uses the same filename.
- Automatically save duplicates: This option tells :Email to save each attachment using a unique filename. This uses an upward counting number as a suffix to the filename (before the extension) so you can make changes to a file you access directly from a message, then return to it in the filesystem to recover the data.

RESTRICTIONS ON TEMPORARY ITEMS

You will not be able to view protected messages in a local browser session despite the note Outlook provides in certain circumstances. When you attempt to do this Outlook saves the message in a `.mht` file then renders this in Internet Explorer. *SSProtect* restricts access to the secure temporary attachments folder that Outlook uses for these items, thus IE fails to render the data. This is done to prevent malicious applications from accessing temporary Outlook data files in various cases.

OFFICE 365 INTEGRATION

As of version v2.3.0, our team is investigating integration with Office 365 on the web. At this point in time, no decisions have been finalized through the goal is to provide similar if not the same functionality available using the desktop Outlook client when using the Outlook Web Access. Stay tuned to our website and support pages (https://www.definisec.com and https://support.definisec.com) for notification of plans and releases.