Smartpoint Policies

- Overview
- Adding a Smartpoint Policy
    - Actions
    - Application Exceptions
        - Application Pattern
        - Users
        - Action
- Editing a Smartpoint Policy
- Deleting a Smartpoint Policy

Overview

A Smartpoint policy is a set of rules which tell the Smartcrypt agent how to operate. You may add, edit or delete Smartpoint policies in the Smartcrypt Enterprise Manager.

Adding a Smartpoint Policy

1. Login to the Smartcrypt Enterprise Manager (SEM).
2. Go to **TDE > Policies**. A list of existing Smartpoint policies will be displayed.
3. Click **Add**.
4. (Optional) Choose a descriptive **Name** for the Policy.
5. Choose a Default **Action**.
6. Identify users for, "Selectable By" that you'd like to have associated with this policy. Users/groups entered here that are part of the TDE Group can choose this key for their Smartpoints.
7. Identify any individual exceptions to the Default Action in the **Application Exceptions**.
8. Click **Save** to add the policy.

Actions

A default action represents how TDE will respond to access attempts by all system processes and users not specifically called out in the Application Exception list below, for this Smartpoint.

Action	Description
Encrypt /Decrypt	Files are transparently encrypted / decrypted *Best used for applications and users that are authorized to encrypt / decrypt data in this location.*
Raw	Files are presented in whatever form they have been stored. They can be either in an encrypted or decrypted state *Best used for backup agent software and to verify encryption is functioning*
Deny	If someone in the group that this policy applies to tries to open this file, it won't open, and the user receives an error message. *Best used as a catch-all for unnamed authorized processes or for calling out a specific process that you do not want accessing the file system location defined in the Smartpoint*

Application Exceptions

Application Pattern

Application Pattern identifies individual exceptions to the default action. Each pattern you define acts as a rule. A pattern can only be an application or "SYSTEM;" it cannot be a file type. "SYSTEM" refers to files a user on a different device accesses by connecting to a network. A good example would be any file located within a folder shared over a network.

An example of a pattern would be **lmsword.exe*. The "**l*" searches and locates the application on your device. Every file opened in Microsoft Word on the TDE agent that uses this Smartpoint policy will act in correspondence with the selected action for the pattern.

Users

User identifies a user to match with an exception to the default action. A user can be a local user on the computer, a Windows domain account, or even the SID of a windows user object. A user can be combined with a pattern to apply a rule to both the pattern and the user, or can be used by itself.

An example of a typical configuration would be combining the *SYSTEM* pattern with *Authenticated Users* and the *Encrypt/Decrypt* action on a file server to allow any authenticated Windows users to access data on a file share.

Action

The available actions you may choose from are the same as the default action options. This chosen action represents how the identified pattern responds.

Editing a Smartpoint Policy

You may update a Smartpoint policy within the *Smartpoint Policies* tab by selecting **Edit** located to the right of the Smartpoint policy you wish to edit. The changes will be reflected immediately on any TDE agent to which the Smartpoint policy applies.

Deleting a Smartpoint Policy

You may delete a Smartpoint policy within the *Smartpoint Policies* tab by selecting **Delete** located to the right of the Smartpoint policy you wish to delete.

**** IMPORTANT: If a Smartpoint Policy is in use by a Smartpoint, it cannot be deleted.**