ESET Tech Center

Knowledgebase > ESET Endpoint Encryption > Configuring Managed users with no local storage access (Roaming Facility)

Configuring Managed users with no local storage access (Roaming Facility)

Anish | ESET Nederland - 2018-01-30 - Comments (0) - ESET Endpoint Encryption

When a user activates their machine with the Enterprise Server the process updates the HKEY_CURRENT_USER branch of the registry with their activation details and a file known as the Key-file is created within their Windows user profile for storage of encryption keys and licencing information.

If you are working in an environment where the users ability to write data to the system or registry is restricted then you can make use of the roaming facility in DESlock+ to ensure the activation details and users encryption keys are stored on a network path.

This method can also be used to elimiate the requirement for a user to activate on every PC they use.

This guide assumes you are using Enterprise Server v2.4.5 or later and Client Install v4.5.4 or later.

To enable this within your Enterprise Server do the following :

Note - Configuring the clients in this manner will not allow the use of Full Disk Encryption on the machines.

Select the **Workstations** branch of the tree (or create a new branch to apply policy to if you do not wish to use the new settings globally).
Select **Workstation Policy** as pictured below.
Select the items detailed in the list below and then click the the **Details** button to edit their settings as specified :

Key-File Settings\Key-File Location Type - **Specified Path**
Key-File Settings\Key-File Location - *Path to the users home storage e.g. Z:\*
Advanced Options\Force Roaming Mode - **Yes**
Advanced Options\Keep Settings With Key-File - **Yes**
Advanced Options\Force RDS Mandatory Profile Mode - **Yes**

The policy changes detailed above cannot be pushed across the network to the clients, instead you will need to update clients by using the **Download**

Settings File button to obtain a registry file to update existing installs or download an install with the new settings merged using the following steps.

Select **Organisation:***ORGANISATION_NAME*.
Select the **Client Installs** tab. Select the install package in the list appropriate for your target system.
Click the **Download Merged Install** button.
Select the Policy you have updated with the new settings and click **Download**.

Activate the users as normal by generating an activation code and entering it into the client. Note when the users workstations will appear in the Enterprise Server **Remote Desktop Services** branch with a **TS_** prefixed identifier.

When the user first activates, two files will be created in the path pointed to by their Key-File Location path, these are named **tokenstore.dat**(Key-file) and **tokenstore.usr** (registry settings).

When the user moves to a second machine the settings and activation data will already be loaded from the network path and they will not be required to activate again.