ESET Tech Center

Knowledgebase > ESET Endpoint Encryption > What is password policy?

What is password policy?

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

When a workstation is managed by an Enterprise Server, the administrator can specify requirements of passwords specified by users. This allows them to ensure secure passwords are used and that security compliance is met.

The Password Policy is specified as part of the **Group Policy** within the Enterprise Server. Please see the following article for details on modifying the Group policy as required, the settings relating to password quality are within the **Password Policy** section: KB251 - How do I modify group policy?

Key-File and Encrypted Container Passwords

When the DESlock+ software requests the user specifies a password a progress bar will be coloured from red to green as they type to indicate their progress towards meeting the password requirements. Only when the progress bar has filled and is green in colour has the password met the specified policy and will allow the user to continue through the process.

When specifying passwords if the mouse pointer is hovered over the Password Policy bar a tooltip dialog will display detailing the policy requirements and which of those requirements have been reached by the current entry.

There are some examples of this behaviour below:

Changing the users Key-File password (Password Policy not met)

Encrypting a file using a password for encryption (Password Policy met)

Full Disk Encryption

When specifying Full Disk Encryption passwords within the Enterprise Server, at the point of starting encryption the Password Policy is enforced. If the policy has not been met the encryption wizard will not progress and a red circle with an exclamation mark will appear indicating that Password Policy has not been met. If the user hovers their mouse pointer over this icon a tooltip will appear explaining the requirements.

It should be noted that the Password Policy applied for Full Disk Encryption logins is set at the time of encryption starting on the Workstation. Modifications to the Password Policy once encryption has been initiated will not apply to Full Disk Encryption password changes.

In order to apply a new Password Policy in this situation you will need to update the policy, decrypt then re-encrypt the machine. Therefore it is good practice to ensure Password Policy is decided upon before deploying Full Disk Encryption.

The Password Policy will also affect the quality of the generated recovery login passwords which are used if a user forgets their Full Disk Encryption password. The interface for this process includes a password quality bar but unlike the other interfaces does not include a mouse hover option. There are more details of the recovery process itself here: KB143 - How do I reset a managed user's Full Disk Encryption password?

Related Articles

KB252 - What are Workstation and Group Policy?

Keywords: audit