ESET Tech Center

Can I install DESlock+ remotely?

Anish | ESET Nederland - 2018-03-07 - Comments (0) - ESET Endpoint Encryption

It is possible to install the DESlock+ software remotely using remote access software such as Team Viewer, LogMeIn etc. This may be useful if for instance you are offering a managed service or you have employees that work outside of the office. However there are a few things to keep in mind if you are considering this which are detailed below.

> The remote connection software being used may not provide support for interaction with the UAC prompts which are displayed by Windows during some operations of the DESlock+ client software including installation. This would mean the user will need to accept the UAC prompt themselves.
> The software stores configuration data in the users Windows profile, so you will need to login as them when activating the system or making changes that affect their key-file.
> The installation process, uninstallation process and the start of Full Disk Encryption with Safe Start enabled will require that Windows is restarted during the process.
> While it is possible to manage individual machines using the software in a standalone capacity, it is much easier to manage machines remotely by using an Enterprise Server as detailed here: DESlock+ Enterprise Server Centralised Management
> If you intend to use the Full Disk Encryption feature of DESlock+, starting the system once encrypted will require the user at the machine enters their credentials, it will not be possible to do this remotely using remote connection software. If you have not already done so it would be worth running through the process on a local machine so you have an understanding of the interface the user will need to use to boot the system.
> Should there be a problem with the Windows installation or encryption process preventing the machine from starting then recovery facilities require booting from prepared ISO files to perform the decryption. Details of this can be found here: KB210 - How do I decrypt a managed system that is unable to start Windows?.
> It is recommended that Safe Start is used when starting Full Disk Encryption to detect errors that might stop the machine from booting. There are more details of Safe Start here: KB177 - What is DESlock+ Full Disk Encryption Safe Start
> It is not possible to use the Enterprise Server Push Install method to remote machines that are not on your network. You can however obtain an MSI installation package to run on the system detailed here: KB217 - How do I download a merged install for installation on a Workstation?

If the machine is not part of your normal network infrastructure and backup procedures then a separate backup should be taken before commencing encryption.
When controlled by an Enterprise Server, the full disk encryption system has a password recovery facility built in so you can provide the user with access to the system again should they forget their password. There are details of this here: KB143 - How do I reset a managed user's Full Disk Encryption password.

Related Articles

KB308 - Managing multiple sites from a single Enterprise Server

Keywords: team viewer, teamviewer, remote desktop connection, rdp, gotomeeting, gotoassist, vnc