ESET Tech Center

Enterprise Server known issues

Anish | ESET Nederland - 2018-01-23 - Comments (0) - ESET Endpoint Encryption

The following is a list of known issues with the Enterprise Server which have been reported to us by customers.

Issues

Version 2.9.0

JavaScript error performing Active Directory test

Version 2.8.0

Cannot upload SSL Certificate
Cannot click Update Worksation Details button from FDE wizard

Version 2.7.1

Cannot login when 'Must Change Password' is set on login

Version 2.6.2

Cannot upload own SSL certificate
Cannot delete user as licence is still being downloaded
Cannot see the changed FDE login password

Version 2.6.0

Enterprise Server crashes when restarted, or crashes when a user logs in
Cannot adopt a Full Disk Encrypted workstation

Issues

Version 2.9.0

JavaScript error performing Active Directory Test

When performing an Active Directory test, you may encounter a JavaScript error similar to the image below. The error may be slightly different on different

browsers running different JavaScript engines. This image below is from Internet Explorer 11.

Cause

The reason for the error is that the test was successful in contacting the domain, but no user records were found. The DESlock+ Enterprise Server assumes at least one record will be returned from a test. But if no records are returned, that s the list of users is empty (or null) then the error is thrown when trying to examine the list.

Resolution

Try changing the search parameters to ensure that user records are returned from the search and thus will be displayed in the test dialog.

Affected versions

Issue not present	
Issue present	2.9.0
Issue resolved	2.9.2

Version 2.8.0

Cannot upload SSL Certificate

You may experience problems uploading an SSL certificate into the Enterprise Server. If this is a new certificate the configuration will be rolled back. However if this is an update to a pre-existing certificate then Apache will fail to restart the Enterprise Server will remain inaccessible. This only affects certificate upload and not the self signed certificates created by the Enterprise Server.

Cause

The DESlock+ Enterprise Server uses an include file call ApacheSSL.conf to configure SSL. However when this file is written after a certificate upload the wrong paths are emitted into the file. Specifically the entry SSLCertificateKeyFile and SSLCertificateChainFile will be incorrect. The SSLCertificateKeyFile will reference the certificate file itself. And if you are

not using an intermediate certificate then the SSLCertificateChainFile will reference the previous signing root certificate.

Resolution

The file will need to be edited manually to correct the paths. After this Apache can be started.

Affected versions

Issue not present	
Issue present	2.8.0 (and earlier)
Issue resolved	2.9.0

Cannot click Update Worksation Details button from FDE wizard

A JavaScript error may be displayed when a user attempts to click the Update Workstation Details button from within the Full Disk Encryption (FDE) wizard cards.

Cause

The issue is caused by a coding error.

Resolution

There is no resolution to this issue, it will be resolved in the next version. However the workaround is to request workstation details from the workstation tool menu instead.

Affected versions

Issue not present	2.7.7 (and earlier)
Issue present	2.8.0
Issue resolved	Unresolved

Version 2.7.1

Cannot login when "Must Change Password" is set on login

A JavaScript error may be displayed when a user attempts to login to the Enterprise Server if the "Must Change Password" flag is set and the server will fail to successfully prompt the user for a new password.

Cause

This issue can occur if the password policy is increased causing an existing login with a non-compliant password to be forced to change their password. Alternatively the flag may have been applied to the login manually via the Enterprise Server control panel.

Resolution

If another login can be used to access the Enterprise Server, the "Must Change Password" flag can be removed from the login, or the password policy or login password can be changed so they are mutually compatible. If no other login exists then contact DESlock+ for guidance.

Affected versions

Issue not present	2.6.2 (and earlier)
Issue present	2.7.0 and 2.7.1
Issue resolved	2.7.2 (and later)

Version 2.6.2

Cannot upload own SSL certificate

There is an issue when attempting to upload your own certificate into the Enterprise Server Apache Server SSL Configuration window. After selecting the files, and clicking Upload, a javascript error will be displayed and the browser window will be refreshed before it is possible to continue.

Cause

The issue is caused by a coding error.

Resolution

If you wish you use your own certificate then you should configure the SSL with the built in self signed certificate (use the **Create New Certificate** if necessary). Once complete, you should manually edit the **ApacheSSL.conf** file in the Enterprise Server program files folder and edit the directives **SSLCertificateFile** and **SSLCertificateKeyFile** to the locations of the files you wish to use.

Affected versions

Issue not present	2.6.0
Issue present	2.6.1 and 2.6.2
Issue resolved	Unresolved

Cannot delete user as licence is still being downloaded

The Enterprise Server will block attempts to delete a user. This behaviour is intentional because due to the way the licence resync works and if you delete the user while this process is occurring then it can leave the Enterprise Server or licensing server in an invalid state. When a resync is started, a flag is put on the user to prevent delete and then removed at the end of the resync.

However there are certain situations where this flag can be set on, but not then removed. And this prevents the user from being deleted even after the resync has completed.

Resolution

If you are certain than a resync is not currently in progress, the simplest way to remove the flag is to start a full resync. Please see: http://support.deslock.com/KB76. Please ensure that when the final box appears, you check the "Perform a full resync when this window is closed" item. Wait for this resync to fully complete and then retry the delete.

If the licence cannot be resynced for some reason, then it is possible to edit the database manually to remove the flag - contact DESlock+ for guidance.

Affected versions

Issue not present	2.5.8 (and earlier)
Issue present	2.6.0 to 2.6.2
Issue resolved	2.7.0 (and later)

Cannot see the changed FDE login password

When you enter a new FDE login password, the change will take effect on the client machine however when you come to view it in the Enterprise Server it will remain as an old password.

Cause

If you are using Google Chrome as the web browser to access your Emterprise Server, you may have selected the option to 'save passwords'. Due to how Chrome fills in login details it will display the password you have saved into the Enterprise Server giving the impression it is what you have entered. However the pasword you entered will be stored in the database which is passed to the client.

Version 2.6.0

Enterprise Server crashes when restarted, or crashes when a user logs in

There are two known issues which can cause the Enterprise Server to crash either when starting or when a user logs into the console. Both of these crashes can be resolved with an SQL script available from DESlock+ Support, but this does not resolve the underlying problem and the crash can reoccur.

Cause 1

A [change in the ODBC driver](#) in the SQL Native Client 2012 mean that "sync errors" from the Enterprise Server service (dlpadm) could fail to be read by the Enterprise Console service (dlpecsrv). This resulted in the service crashing. Sync errors are generally there to indicate problems the dlpadm service has, most often these would indicate transient network problems so could be ingnored.

Resolution

The crash can be resolved by removing the records from the table, using the script from DESlock+ Support. You can prevent further causes of this crash by reverting to a previous SQL Native Client version - contact DESlock+ for guidance.

Affected versions

Issue not present	2.5.7 (and earlier)
Issue present	2.5.8 to 2.6.0 (inclusive) if using SQL Native Client 2012
Issue resolved	2.6.1 (and later)

Cause 2

Each time a DESlock+ client workstation performs an update from an Enterprise Server it returns a status packet. This packet contains system information such as disk layout, connected USB devices, and other information necessary for the Enterprise Server or useful for diagnostics. This information can be seen in the "Extended Information" tab of a workstation within the Enterprise Server.

However, when the workstation is activly performing Full Disk Encryption and sending progress information the system information is handled differently.

In this instance any UTF8 encoded text within this block may begin to grow exponentially. Likely sources of this data include, but are not limited to, an non US English operating system with localized USB device names. Also different versions of the DESlock+ client software may return data differently.

Usually this behaviour cause a problem because the progress would only be read once an hour and might never grow sufficiently large to pose a problem. But if the workstation remains encrypting for a long time, and if the Enterprise

Server Proxy Syncs frequently during the duration then this growth of data could eventually cause the service to crash.

Resolution

The problem can be mitigated by requesting [updated workstation information](#) during encryption, or posting any other command, which will request a new system information block and will reset any growth caused by the FDE progress status reports.

Affected versions

Issue not present	2.4.5 (and earlier)
Issue present	2.5.0 to 2.6.0 (inclusive) behaviour dependant in DESlock+ client version
Issue resolved	2.6.1 (and later)

Cannot adopt a Full Disk Encrypted workstation

If a workstation is already encrypted when it is first activated into an Enterprise Server (such as a client that was originall installed standalone) then it will appear as an unmanaged workstation. At this point the option to adopt this workstation into the Enteprise Server is offered. However this may produce an error "This workstation does not have any activated users with a Full Disk Encryption (FDE) supported licence. An FDE supported licence is required for this operation. (0xC0130105)".

Resolution

There is no workaround for this issue and either the workstation must stay unmanaged until the new version is applied or you must decrypt the workstation using a [Recovery CD](#) and then re-encrypt it within the Enterprise Server.

Affected versions

Issue not present	2.5.8 (and earlier)
Issue present	2.6.0

Issue resolved	2.6.1 (and later)

Keywords: enterprise server known issues