Apple is deprecating an older API used by ESMC MDM, upgrade now to keep your iOS devices manageable

2020-10-05 - Steef | ESET Nederland - Comments (0) - Customer Advisories

News

The Apple Push Notification service (APNs) will no longer support the legacy binary protocol as of November 2020.

What to expect

The ESET Security Management Center (ESMC) Mobile Device Management (MDM) component uses the APNs communication protocol for the management of iOS devices. All ESMC MDM components older than version 7.2.11.3 rely on the old binary API part of the APNs protocol. In November 2020, when the binary API part of the APNs protocol is deprecated, users with an MDM component on a version older than version 7.2.11.3 will lose the ability to manage iOS devices.

To work properly, ESMC MDM version 7.2.11.3 requires a new network port (2197). For more information on network requirements, refer to the Ports used > **ESMC MDC Machine** section of the ESMC Installation/Upgrade Online Help guide.

FAQ

- **What should I do to preserve the full connectivity and functionality of iOS devices managed by ESMC MDM?**

Prior to the November 2020 deadline, upgrade the ESMC MDM component to version 7.2.11.3. If required, execute the certificate exchange process.

- **What if I upgraded my ESMC MDM component to version 7.2.11.3 after the November 2020 deadline?**

If the ESMC MDM component is upgraded after the November 2020 deadline the managed iOS devices should restore the connectivity and functionality when the upgrade process is finished.



Important!

Users who use a self-signed HTTPS certificate for the management of iOS devices with ESMC MDM might lose connectivity if the MDM HTTPS certificate is exchanged after the November 2020 deadline before the ESMC MDM component upgrade process is finished. We recommend you execute the HTTPS certificate exchange after the ESMC MDM component upgrade process is finished. If you are unable to perform the HTTPS certificate exchange before the November 2020 deadline, continue with the ESMC MDM component upgrade process.

Can I still use my self-signed certificate signed by ESMC CA after the November 2020 deadline?

Yes. You can still use the self-signed certificate signed by ESMC CA after the November 2020 deadline. However, there is a potential loss of connectivity if the HTTPS certificate exchange is executed without the MDM upgraded to version 7.2.11.3.

What will happen if I execute the HTTPS certificate exchange without upgrading the MDM component after the November 2020 deadline?

If the user has self-signed the HTTPS certificate and executes the HTTPS certificate exchange before upgrading the ESMC MDM component to version 7.2.11.3 after the November 2020 deadline, iOS devices can lose connectivity. This occurs because the iOS device is unable to exchange trust with the MDM component due to the MDM component's inability to notify the iOS device via the old APNs protocol.

What if I use a third-party HTTP certificate trusted by Apple and upgrade my ESMC MDM component after the November 2020 deadline?

Managed devices will automatically reconnect to the MDM component when the ESMC MDM upgrade to version 7.2.11.3 is complete.