Endpoint Management Security Administrator guide

Overview

This guide focuses on the tasks that need to be performed by the administrator who is responsible for security. This includes concepts such as SSL management and others.

Securing File Upload

OpenText™ Endpoint Management allows customers to upload, and transfer or distribute files as part of various features in the product. The upload and distribution of files is performed "as is" and without applying additional protection measures. OpenText encourages customers to apply relevant protection measures as per their security policy to protect against risks associated with uploading, transferring, or distributing files through Endpoint Management. By not implementing relevant protection measures, the devices in the customer's environment may be exposed to increased security risks. You understand and agree to assume all associated risks and hold OpenText harmless for the same. It remains at all times the customer’s sole responsibility to assess its own regulatory and business requirements. OpenText does not represent or warrant that its products comply with any specific legal or regulatory standards applicable to the customer in conducting the customer's business.

Console Helper

The files uploaded using the Console Helper are scanned for viruses, but the scan does not support the following:

- If the file is a compressed archive (such as a ZIP file), the files inside the archive will not be scanned for viruses.
- If the file is larger than 2 GB.

Uploaded files are encrypted while in the cloud but are stored as plain text at the destination location on the assigned endpoints. Once installed on the endpoints, the protection of the files becomes the customer's responsibility. If necessary, customers can encrypt files containing sensitive information before uploading.

Securing Enrollment Token

As a best practice and to secure the system, ensure that you adhere to the following points when creating the Enrollment Token:

- **Token:** The token is auto generated and consists of 32 characters. Save and securely distribute the enrollment token to prevent unauthorized devices from being registered into the zone. Any compromise of this key could allow unauthorized or incorrect devices to be registered in the zone.
- **Usage Limit:** You can set a higher usage limit. However, the chances of a token being compromised increase as its usage limit increases. Therefore, ensure that it is as low as possible.
- **Token Expiry Date:** You can set a longer validity period. However, the chances of a token being compromised increase as its validity period increases. Therefore, ensure that it is as short as possible.

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/en-us/legal.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.