Ten Best Practices and Considerations for Securing Reflection Desktop

Following these best practices for securing Reflection Desktop will help you design a secure terminal emulation solution.

Guide

www.microfocus.com/opentext

Solution Guide

opentext™

Security is top of mind in every enterprise organization. There's simply too much at stake to ignore any applications used for key business functions. Mainframe applications often house data that's critical to the business, but organizations are sometimes unsure of the best approach for protecting this data because it's daunting to think of having to update some legacy applications. The good news is there is a solution—Reflection Desktop—that simplifies the process of protecting systems of record on host systems. Now you can make your host applications comply with regulatory mandates and internal security initiatives without making expensive changes on the host side.

These best practices include high-level recommendations and considerations. For more detailed information about the security features OpenText™ Reflection Desktop supports, see:

- Secure Connections in the Reflection Desktop Help Guide
- The Reflection Desktop Deployment Guide

Bring your host systems back into the security fold without jeopardizing business operations.

1. Monitor Security Alerts

OpenText™ regularly publishes security alerts in knowledge base articles at Security Alerts—Reflection Desktop.

2. Secure Connections with the Highest Level of TLS

Reflection Desktop supports TLS 1.3, the latest and most secure version.

3. Use the Strongest Available Encryption Ciphers

Disable less secure cipher suites and enable those you consider to be more secure. See SSL/TLS Security Properties Dialog Box.

4. Stay Current with Versioning

Staying current with major new releases, service packs and updates ensures you deploy the latest security patches and fixes to your end-users.

The Host Connectivity team makes each new version of Reflection Desktop more secure than the last. A dedicated staff of senior engineers evaluate all security alerts and incorporate updates in the next versions.

OpenText™ Development teams use a Secure Development Lifecycle process, where ongoing training and product review ensures our software has no security vulnerabilities, and all new features are developed with security in mind.

5. Use Certificates Securely

Configure Reflection Desktop to prevent security risks associated with certificates.

- Enable the "Retrieve and validate certificate chains" setting in the SSL/TLS Security Properties Dialog. This setting specifies whether certificates presented for host authentication are valid and signed by a trusted CA. Disabling this option can make connections vulnerable to man-in-the-middle attacks, and risks compromising connection security. See SSL/TLS Security Properties Dialog Box.
- Consider disabling connections for the Windows certificate store. Reflection applications can be configured to only authenticate certificates in the Reflection or Windows stores. Disabling use of the Windows certificate store ensures greater control over which certificates are used for authentication. Certificates are easily added to the Windows store, and you will not need them all. Disabling the Windows store ensures that only certificates imported into the Reflection store are used for host authentication. See Enable or disable the use of the windows Certificate store.

6. Control Access to Product Features

Limit access to settings and controls, and consider custom templates with locked down settings so users must use security settings, such as the latest TLS versions, when creating new sessions.

Access to almost any of the Reflection settings or controls can be restricted to prevent users from changing values. This simplifies support requirements and helps resolve security concerns. Users cannot change settings unless elevated to administrator access level.

Access to almost every Reflection Desktop feature can be enabled or disabled via two different options—Microsoft Group Policy or Reflection *.ACCESS files, which administrators can create with Reflection Desktop administrative tools and then deployed with the product. See Control Access to "Lock Down" Settings and Controls.

Control Access

Lock down or disable potentially insecure features, such as users accessing programming and macro languages to record, write and distribute automation code that includes user IDs and passwords, creating a security risk.

- Use the Reflection Group policy settings, as documented in Technical Information Document 7024743, and Control Access to Settings and Controls with Microsoft Group Policy to disable specific features and create more secure user environments.
- Alternatively, create and deploy .ACCESS files from the Reflection Desktop administrative tools to lock down specific settings. See Control Access to Settings and Controls with Reflection Administrative Tools.

Set up Session Templates

Control the types of sessions users create by deploying session templates with pre-configured settings. For example, create templates with pre-configured SSL/TLS settings and then lock them down Group Policy or Reflection Desktop administrative tools. See Set up Session Templates.

7. Configure the Reflection Desktop Trust Center to Protect Data and Information Privacy

Use the Trust Center to protect your working environment from information theft, and your data from potential damage from non-trusted sources. Configure settings to protect these data and information types:

Trusted Locations

This is a directory designated as a secure file source. By default, Reflection users can only open documents from directories specified as trusted locations and are prevented from opening untrusted documents outside them.

Information Privacy

To ensure host applications can adhere to regulations like GDPR, PCI DSS, HIPAA, CCPA, configure Reflection Desktop to protect sensitive data such as credit card Primary Account Numbers (PANs), phone numbers, and US Social Security numbers. Information Privacy ensures that sensitive data is not displayed on the screen and productivity features, such as Screen History require secure connections and redact PANs in logs.

API and Macro Security

Configure Trust Center settings within the Reflection Desktop API and macros to:

- Enable or disable the Reflection Desktop .NET API.
- Determine if Reflection legacy macros are supported.
- Specify what happens when an action restricted through group policy or .ACCESS files, is initiated through a macro or API call. See Protecting Data and Information Privacy.

8. Do Not Save Passwords in Macros

Including user IDs or passwords in macros or other automation code creates a security risk, so Reflection Desktop automatically adds a prompt dialog box to a VBA (Visual Basic for Applications) macro, instead of the password, to prevent security risks.

See: Technical Information Document 7024220

9. Manage Host Sessions Using a Centralized Management Server

Use the OpenText™ Host Access Management and Security Server (MSS), a separately available product, to centrally manage, secure, and monitor users' access to host connections during Reflection sessions.

- This centralized management server will grant or deny access based on group or role, help to quickly apply security updates and configuration changes, and make post-install adjustments on the fly. Use MSS to easily configure and lock down large numbers of desktops. See Use a Centralized Management Server.
- Use the OpenText™ MSS Advanced Authentication Add-on to configure a multi-factor authentication solution to create additional protection for sensitive data by adding more advanced authentication to the username and password. Advanced Authentication works on diverse platforms and uses different types of authenticators such as Fingerprint, Card, and OTP. Advanced Authentication. It provides a single authentication framework to ensure secure access to every device with minimal administration. See OpenText Advanced Authentication.

Connect with Us
OpenText CEO Mark Barrenechea's blog

- Using the Automated Sign-On for Mainframe Add-On, users can authenticate to a front-end system using a modern form of authentication, such as a smart card, certificate, LDAP password, Kerberos, etc, and be automatically logged on to a z/OS mainframe application. See Set up Automated Sign-On for Mainframe Sessions.

10. Encrypt Session Documents

Encrypt 3270, 5250, and Open Systems session documents to protect them against unauthorized changes. Encryption effectively scrambles the data in a session document. For best results, use document encryption in conjunction with the encryption options in Reflection Permissions Manager. See Encrypt a Session File.

Additional Security Features

Multiple security features protect your personal data and prevent it being read by unauthorized users.

- Reflection Desktop software does not store host usernames or passwords anywhere in the configuration files.
- Reflection Workspace logs do not capture host usernames or passwords.

Conclusion

Many organizations have made the securing of legacy applications a lower priority. With data breaches at an all-time high and expected to continue, putting off securing legacy applications is no longer an option for enterprise organizations. Luckily, Reflection Desktop provides modern capabilities that enterprise organizations can use to protect sensitive data, prevent the loss of data, and comply with the most stringent security requirements.

Learn more at
www.microfocus.com/opentext

opentext™