GOV.UK

Guidance

# Browser Security Guidance: Microsoft Internet Explorer Mobile

Published

**Contents**

This ALPHA guidance is applicable to devices running Internet Explorer on Windows Phone 8.1 in line with the EUD Platform Security Guidance, which this guidance builds on. This guidance was tested on a Nokia Lumia 630 running Windows Phone 8.1.

## 1. Usage scenario

Internet Explorer will be used to access a variety of web services including:

- accessing Intranet services hosted on an enterprise-provided OFFICIAL network
- accessing enterprise cloud services sourced from the Digital Marketplace
- accessing other Internet services and web resource

To support these scenarios, the following architectural choices are recommended:

- All data should be routed through a secure enterprise VPN to ensure the confidentiality and integrity of traffic intended for the enterprise Intranet
- All Internet data should be routed through an enterprise-hosted proxy to benefit from enterprise protective monitoring and logging solutions

## 2. Summary of browser security

This browser has been assessed against each of the 12 security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the browser can best satisfy the security recommendations for more details about how each of the security recommendations is met.

| Recommendation | Rationale |
|---|---|
| Protecting data-in-transit | Internet Explorer Mobile 11 does not support configuration to disable cryptographic cipher suites HTTPS enhancements such as HSTS, certificate pinning and OSCP checks are not supported<br>[!] Users can override certificate warnings |
| Protecting data-at-rest | There is no option to automatically delete sensitive data Cached data and passwords rely on the platform's data-at-rest protection |
| Enabling authentication | Built-in authentication schemes cannot be disabled for cleartext channels |
| Protecting privacy | [!]Search terms and URIs typed into the address bar are sent to Bing over an unencrypted connection |
| Plugin and renderer sandboxing | |
| Plugin and site whitelisting | |
| Malicious code detection and prevention | Content Security Policy is not supported<br>There is no differentiation between Internet sites and Intranet sites |
| Security policy enforcement | [!] All browser security configurations can be disabled by the user<br>Internet Explorer Mobile 11 cannot be centrally configured - devices must be configured manually |
| External peripheral and sensitive API protection | |
| Update policy | [!] The browser is updated infrequently as part of the platform, and so does not receive the same security patches as the desktop version |
| Event collection for enterprise analysis | [!] There is no facility for the enterprise to log or collect security-related events |
| Active scripting | The browser does not allow scripting to be disabled |

## 2.1 Significant risks

The following significant risks have been identified

- All browser security configurations can be disabled by the user placing a heavy reliance on procedural controls. Many features of Internet Explorer Mobile are enabled by default and unconfigurable, however there is potential for the user to weaken privacy controls and disable anti-malware
- The browser is only updated when Windows Mobile itself is patched. This is less frequent than the Internet Explorer patching cycle on desktop platforms, resulting in Internet Explorer Mobile being susceptible to publically known vulnerabilities until the next available platform update
- Search terms and web site addresses typed into the address bar are sent to Bing over an unencrypted connection, allowing both the vendor, network operators and any man-in-the-middle attackers to aggregate potentially personal information
- Built-in authentication schemes such as basic and digest cannot be disabled for unencrypted requests. There is a risk that credentials sent using these methods could be stolen via a man-in-the-middle attack
- Credentials and temporarily cached sensitive data rely on the native encryption feature of Windows Phone. Device Encryption has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured full disk encryption products. Without assurance there is a risk that data stored on the device could be compromised
- Internet Explorer 11 Mobile does not support configuration to disable cryptographic cipher suites. If a vulnerability is discovered in a particular cryptographic cypher, users may be under increased risk as they will believe their encrypted traffic is protected appropriately
- HTTPS warning pages can be bypassed by the user. The browser does not support HSTS, certificate pinning or OSCP checks. There is a risk that secure connections may be subject to a man in the middle attack using a forged certificate
- There is no differentiation or explicit separation between Intranet and Internet web pages. Intranet sites that are vulnerable to cross-site-scripting and cross-site-request-forgery are not protected from malicious Internet websites. There is no built-in protection against cross-site scripting attacks.
- Internet Explorer does not provide any built-in mechanism for logging events for enterprise analysis. It is therefore not possible to determine whether installations adhere to security policies, nor alert on security events such as on-screen security warnings or browser crashes

# 3. How the browser can best satisfy the security recommendations

## 3.1 Protecting data-in-transit

Configure a gateway web proxy to ensure that all Internet traffic is routed through the enterprise for inspection and logging. Use the platform’s data-in-transit protection to securely route all Intranet traffic back to the enterprise and provide access to the proxy.

## 3.2 Protecting data-at-rest

Use the platform’s data-at-rest protection to encrypt profile data and temporary files. If required, users can manually delete temporary data and cached credentials after accessing sensitive sites.

## 3.3 Enabling authentication

Deploy enterprise client authentication certificates to the browser if required.

## 3.4 Protecting privacy

Turn off features that collect data such as browsing history, typed URLs and location data to submit to Microsoft. Configure Data Sense so that it does not request compressed content from the Microsoft cloud.

The SmartScreen filter can be disabled if the trade-off between privacy and security is not acceptable.

## 3.5 Plugin and renderer sandboxing

This requirement is met by the browser without additional configuration.

## 3.6 Plugin and site whitelisting

Deploy a site whitelist on the web proxy if required.

## 3.7 Malicious code detection and prevention

Use the Microsoft SmartScreen cloud service to detect known malicious sites and downloads.

## 3.8 Security policy enforcement

Internet Explorer settings cannot be configured or enforced using an MDM or ActiveSync.

## 3.9 External peripheral and sensitive API protection

This requirement is met by the browser without additional configuration.

## 3.10 Update policy

Updates are applied to the browser when the phone itself is updated.

## 3.11 Event collection for enterprise analysis

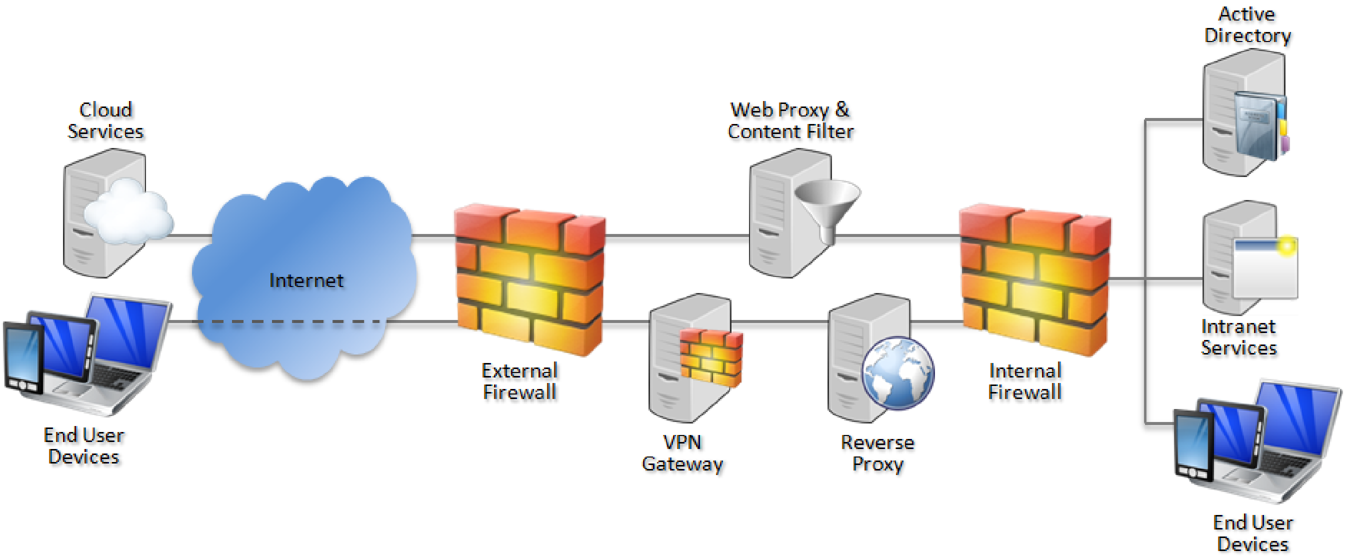
There is no facility for collecting logs or security events for enterprise analysis.

## 3.12 Active scripting

This requirement is met by the browser without additional configuration.

# 4. Network Architecture

Deploy a DMZ web proxy in an architecture based on the Internet Gateway Architectural Pattern. The following network diagram describes the recommended architecture for this browser. The proxy/content filter includes user and machine request logging, anti-malware and content inspection components.



**Recommended network architecture for deployments of Microsoft Internet Explorer Mobile on Windows Phone**

# 5. Deployment process

The following steps should be followed to prepare the enterprise infrastructure for hosting a deployment of the browser and provision it to end user devices.

1. Procure, deploy and configure network components, including a web proxy/content filter and remote access VPN.
2. Provision Windows Phone in line with the EUD Platform Security Guidance.

3. Set up the browser configuration on each device in accordance with the settings later in this guidance.

# 6. Recommended configuration

The following changes need to be made using the Settings app on the device.

| Setting | Value |
|---|---|
| Get suggestions from Bing as I type | Off |
| Reduce data use by sending URLs to the Data Sense service | Off |
| Send browsing history to Microsoft | Off |
| Use SmartScreen Filter to help protect against unsafe websites | On |
| Send a Do Not Track request to websites you visit | On |
| Cookies from websites and apps | Block some |
| Reduce data use by sending URLs to the Data Sense service | Off |

# 7. Enterprise Considerations

## 7.1 SmartScreen filter

Microsoft SmartScreen filter is a security feature that aims to protect against phishing websites and malicious downloads. It works by sending the full addresses of webpages to Microsoft. If Microsoft reports that the page is unsafe, the page or file will not be downloaded or displayed to protect the user against malware and data theft.

Microsoft encrypts the addresses before sending them over the Internet to ensure that they are protected over the Internet, and tries to filter addresses to remove personal information where possible. Nevertheless it is feasible that personal or sensitive data may be sent and processed. SmartScreen filter can be disabled entirely if the trade-off between privacy and security is not acceptable.

## 7.2 Data sense

The data sense feature reduces the amount of data used to send webpages to the device. It works by sending web requests to non-encrypted sites both to the actual web site and to Microsoft. If Microsoft has a copy of the page and determines that it can be well compressed the page is served by Microsoft instead of the original web site.

Microsoft encrypts the addresses before sending them over the Internet to ensure that they are protected over the Internet, and tries to filter addresses to remove sensitive information where possible. A unique ID is used to track the usage of each device. It is feasible that personal or sensitive data may be sent and processed and correlated with other web browsing by that user. Data sense can be entirely disabled using the configuration above. If data sense is disabled, the phone will still retrieve mobile versions of websites optimised for smaller screens where available.

# Legal information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it.