

Edge IE Mode Compatibility Registry Settings

Internal Workaround Reference and Consolidated Registry Configuration

October 2026

Contents

Edge IE Mode Compatibility Registry Settings	1
Background / Source	1
Included Files	2
Recommended Usage	2
Option A - Troubleshoot only the Edge IE Mode compatibility issue	2
Option B - Apply only settings that match the actual symptom	2
Option C - Reproduce our internal Infra package	3
Manual Import	3
Important Security Notes	3
02_Compatibility_View.reg	3
04_Allow_All_Cookies.reg	3
05_Security_Zones.reg	4
03_Trusted_Sites.reg	4
Verification After Import	4
Suggested Troubleshooting Method	4
Rollback / Recovery	4
Scope and Disclaimer	5
Appendix: Consolidated Registry Configuration	6
Consolidated Edge IE Mode Registry Settings	6
01 - Allow Pop-ups	6
Notes	6
02 - Compatibility View / Browser Emulation	6
Notes	7
03 - Trusted Sites / Zone Mapping	7
Notes	8
04 - Allow All Cookies	8
Security note	9
05 - Security Zone Settings	9
Security note	10
Applying the Full Internal Package	10

Edge IE Mode Compatibility Registry Settings

Background / Source

Our company encountered a similar compatibility issue when using legacy web applications through **Microsoft Edge IE Mode**.

As part of the internal troubleshooting process, our Infrastructure (Infra) team provided a **self-extracting installation package** containing the registry settings documented in this repository. The package automatically imported

the included .reg files for the current Windows user.

After applying the package, colleagues who had previously experienced the Edge / IE Mode issue reported that the affected legacy application could be used normally again. One confirmed working environment was:

- **Microsoft Edge:** 154.0.4258.48

This is an important practical result, but it should **not** be interpreted as confirmation that Microsoft Edge 154 officially fixed the underlying IE Mode issue. The observed recovery may be caused by one or more compatibility, security-zone, cookie, pop-up, or browser-emulation settings restored by these registry entries.

Important: These registry settings were prepared for our company's internal environment. They are **not** a **universal Microsoft fix**, and not every setting will be required or appropriate in another organization. Review each setting against your own legacy application, security requirements, Group Policy, trusted-site configuration, and IE Mode deployment before importing it.

Included Files

File	Purpose	Typical reason to use it
01_Allow_Popups.reg	Adjusts IE pop-up behavior	Legacy application uses window.open() , print windows, or child forms
02_Compatibility_View.reg	Enables Compatibility View / browser-emulation behavior	Legacy page requires older IE rendering behavior
03_Trusted_Sites.reg	Configures IE security-zone mapping behavior and provides templates for trusted sites	Application must be treated as a Trusted Site
04_Allow_All_Cookies.reg	Relaxes cookie restrictions in Zones 1, 2, and 3	Login/session/cookie behavior is failing
05_Security_Zones.reg	Relaxes selected security settings in Trusted Sites (Zone 2)	Legacy application requires ActiveX, scripting, downloads, or integrated login
setup.bat	Imports all five .reg files in sequence	Internal package / controlled deployment only
reg.md	Consolidated reference containing all registry entries	Review, audit, comparison, or manual extraction

Recommended Usage

Option A - Troubleshoot only the Edge IE Mode compatibility issue

If the primary symptom is the same as ours - a legacy application no longer behaving correctly in Edge IE Mode - start by reviewing:

02_Compatibility_View.reg

This file contains the Compatibility View / Browser Emulation settings and is the most directly related to the behavior we observed.

Do **not** assume the other registry files are required.

Option B - Apply only settings that match the actual symptom

Use the following as a guide:

Symptom	Registry file(s) to review
IE Mode page renders incorrectly / legacy JavaScript fails	02_Compatibility_View.reg
Pop-up windows are blocked	01_Allow_Popups.reg
Application must run in Trusted Sites	03_Trusted_Sites.reg
Login state or session cookies are lost	03_Trusted_Sites.reg, 04_Allow_All_Cookies.reg
ActiveX control cannot load	03_Trusted_Sites.reg, 05_Security_Zones.reg
File download or legacy download prompt is blocked	03_Trusted_Sites.reg, 05_Security_Zones.reg
Windows Integrated Authentication / automatic login is required	03_Trusted_Sites.reg, 05_Security_Zones.reg

Option C - Reproduce our internal Infra package

If your organization has reviewed all settings and intentionally wants to reproduce the same full import sequence:

1. Place all five **.reg** files and **setup.bat** in the same folder.
2. Review and customize any domain/IP entries before deployment.
3. Run **setup.bat**.
4. Fully close all Microsoft Edge windows.
5. Start Edge again and test the affected site in IE Mode.
6. Confirm the Edge version with **edge://settings/help**.
7. Verify that the legacy application's required functions work correctly.

The supplied batch file imports all five registry files silently with **regedit /s**.

Manual Import

Each **.reg** file can also be applied independently:

1. Review the file in a text editor.
2. Confirm that the registry path and values are appropriate for your environment.
3. Double-click the selected **.reg** file, or import it using Registry Editor.
4. Close all Edge windows.
5. Reopen Edge and retest the site in IE Mode.

These settings are written under **HKEY_CURRENT_USER**, so they apply to the current Windows user rather than every user on the device.

Important Security Notes

02_Compatibility_View.reg

AllSitesCompatibilityMode=1 enables Compatibility View broadly. This may affect sites other than the intended legacy application. If possible, prefer a targeted configuration after the root cause is confirmed.

04_Allow_All_Cookies.reg

This file permits first-party, third-party, and persistent cookies in:

- Zone 1 - Local Intranet
- Zone 2 - Trusted Sites
- Zone 3 - Internet

This is broader than many organizations will want. If the application only requires relaxed cookie handling in Trusted Sites, consider limiting the change to Zone 2.

05_Security_Zones.reg

This file changes **Trusted Sites (Zone 2)** security settings and enables or relaxes several legacy capabilities, including:

- ActiveX controls
- Signed ActiveX download
- Unsigned ActiveX download
- Active scripting
- Java applet scripting
- Automatic logon with the current username/password
- File download behavior
- Launching applications and unsafe files

These settings may significantly reduce browser security for any site assigned to Zone 2. They should only be used after security review and only when the target application genuinely requires them.

03_Trusted_Sites.reg

The supplied file contains example domain/IP entries only. Replace example values with the actual approved application hostnames or IP addresses before using Trusted Sites mappings.

Verification After Import

After applying the selected settings:

1. Fully exit Microsoft Edge, including background Edge processes if necessary.
2. Reopen Edge.
3. Confirm the affected page is opening in IE Mode.
4. Test the exact function that previously failed.
5. Record the Edge version and Windows version/build.
6. If testing different registry files individually, change only one group at a time so the effective setting can be identified.

For our internal case, users who previously experienced the issue reported normal operation after the Infra registry package was applied, including on Edge 154.0.4258.48.

Suggested Troubleshooting Method

For external teams trying to identify the minimum required fix, use a controlled A/B approach:

1. Reproduce the issue on an affected workstation.
2. Export or document the current relevant registry values.
3. Apply 02_Compatibility_View.reg first.
4. Restart Edge and retest.
5. Only if the issue remains, evaluate the other files based on the actual symptom.
6. Avoid importing all security-relaxation settings unless they are demonstrably required.

This makes it easier to determine whether the effective change is Compatibility View itself or another legacy IE security/privacy setting.

Rollback / Recovery

Before deployment, it is recommended to export the affected registry keys or create an organization-approved rollback package.

Because these files overwrite specific values rather than recording their previous state, there is no single generic rollback `.reg` file that can safely restore every machine to its prior configuration.

Possible recovery methods include:

- Restore previously exported registry values.
- Reapply the organization's Group Policy / MDM browser-security baseline.
- Reset the corresponding Internet Options / IE security-zone settings where appropriate.

Do not rely on a generic reset when the workstation is managed by corporate Group Policy; consult the responsible Infra/Security team.

Scope and Disclaimer

This package documents a **company-specific workaround/configuration that was observed to restore functionality** in our environment.

It does not establish which individual registry value is the root-cause fix, and it is not evidence that Microsoft has officially resolved the Edge IE Mode regression.

Organizations reusing these settings should determine the smallest required configuration and validate it against their own security policy before deployment.

Appendix: Consolidated Registry Configuration

Consolidated Edge IE Mode Registry Settings

This document combines the contents of the five registry files supplied in the internal Infra compatibility package.

Source / context: Our company experienced a similar Microsoft Edge IE Mode compatibility issue. Infra provided a self-extracting package containing these registry settings. After installation, affected colleagues reported that the legacy application worked normally again, including on Edge 154.0.4258.48.

Do not treat this as a universal fix. These values were prepared for our corporate environment. Some settings are broad and security-sensitive. Review each section and apply only what is appropriate for your environment.

01 - Allow Pop-ups

Source file: 01_Allow_Popups.reg

Windows Registry Editor Version 5.00

```
; =====
; Allow Pop-ups
; Disable the IE pop-up blocker and allow selected domains
; =====

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows]
"PopupMgr"=dword:00000000
"PlaySound"=dword:00000001
"UseSecBand"=dword:00000001
"BlockUserInit"=dword:00000000
"UseTimerMethod"=dword:00000000
"UseHooks"=dword:00000001
"AllowHTTPS"=dword:00000000
"BlockControls"=dword:00000000

; Add domains that must be allowed to open pop-up windows here.
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows\Allow]
; Example: allow *.example.com
; "*.example.com"=hex:00,00
; Example: allow a specific IP
; "10.0.0.100"=hex:
```

Notes

This modifies pop-up handling for the current user. Use it only when the legacy application depends on new windows, child forms, report/print windows, or similar behavior.

02 - Compatibility View / Browser Emulation

Source file: 02_Compatibility_View.reg

Windows Registry Editor Version 5.00

```
; =====
; Compatibility View / Browser Emulation
; Legacy IE rendering compatibility settings
```

```
; =====

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation]
; Disable TLD automatic updates
"TLDDUpdates"=dword:00000000
"UnattendLoaded"=dword:00000001
"CVListTTL"=dword:00000001

; Enable Compatibility View for all sites - key setting
"AllSitesCompatibilityMode"=dword:00000001

; Enable Compatibility View for intranet sites
"IntranetCompatibilityMode"=dword:00000001

; Do not enable Compatibility View for Local Machine pages
"LocalMachineCompatibilityMode"=dword:00000000

; Disable the Microsoft Compatibility List override
"MSCompatibilityMode"=dword:00000000

; Automatic layout recovery
"AutomaticLayoutRecovery"=dword:00000001

; Compatibility cache
"StaleCompatCache"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation\LowMic]
"StaleCompatCache"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation\PolicyList]

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation\PPB]
"AllowLocationInPP"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation\QuirksPolicyList]
```

Notes

This is the section most directly related to the Compatibility View behavior observed in our Edge IE Mode investigation.

AllSitesCompatibilityMode=1 has broad scope. Do not assume it is appropriate for every environment or every legacy site.

03 - Trusted Sites / Zone Mapping

Source file: 03_Trusted_Sites.reg

Windows Registry Editor Version 5.00

```
; =====
; Trusted Sites
; Configure IE security-zone mapping behavior
; Zone values: 0=Local Machine, 1=Local Intranet,
;               2=Trusted Sites, 3=Internet, 4=Restricted Sites
; =====
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap]
"UNCAsIntranet"=dword:00000001
"AutoDetect"=dword:00000001
"ProxyBypass"=dword:00000001
"IntranetName"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains]
@=""

; Example: add all subdomains of example.com to Trusted Sites
; [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\example.com]
; "*"=dword:00000002
;
; [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\example.com]
; "http"=dword:00000002
; "https"=dword:00000002

; Example: add a specific IP to Trusted Sites
; [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\192.168.1.1]
; "http"=dword:00000002
; "https"=dword:00000002

; Example: add a specific subdomain/path mapping
; [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\example.com]
; "http"=dword:00000002
; "https"=dword:00000002
```

Notes

The supplied file contains sample domain/IP mappings only. Replace examples with approved real values if Trusted Sites assignment is required.

04 - Allow All Cookies

Source file: 04_Allow_All_Cookies.reg

Windows Registry Editor Version 5.00

```
; =====
; Allow All Cookies
; Enables advanced privacy override and relaxes cookie handling
; for legacy applications that depend on IE cookie behavior
; =====

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
; Enable advanced privacy override
"PrivacyAdvanced"=dword:00000001

; Disable zone-crossing warnings
"WarnonZoneCrossing"=dword:00000000

; Allow normal caching behavior for SSL pages
"DisableCachingOfSSLPages"=dword:00000000

; Zone 2 - Trusted Sites
; 1A02: first-party cookies
```

```
; 1A06: third-party cookies
; 1A10: persistent/non-session cookies
; Values: 0=Allow, 1=Prompt, 3=Block

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2]
"1A02"=dword:00000000
"1A06"=dword:00000000
"1A10"=dword:00000000

; Zone 3 - Internet
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]
"1A02"=dword:00000000
"1A06"=dword:00000000
"1A10"=dword:00000000

; Zone 1 - Local Intranet
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1]
"1A02"=dword:00000000
"1A06"=dword:00000000
"1A10"=dword:00000000
```

Security note

This change affects Zones 1, 2, and 3. In particular, changing Zone 3 means the cookie behavior can affect general Internet sites, not only the target legacy application.

If the application only requires relaxed cookies in Trusted Sites, consider limiting the change to Zone 2.

05 - Security Zone Settings

Source file: 05_Security_Zones.reg

Windows Registry Editor Version 5.00

```
; =====
; Security Zone Settings
; Relaxes selected settings for Zone 2 - Trusted Sites
; =====

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2]
; ActiveX controls
; 1200: Run ActiveX controls and plug-ins (0=Enable)
"1200"=dword:00000000

; 1405: Script ActiveX controls marked safe for scripting (0=Enable)
"1405"=dword:00000000

; 1001: Download signed ActiveX controls (0=Enable)
"1001"=dword:00000000

; 1004: Download unsigned ActiveX controls (0=Enable, 1=Prompt, 3=Disable)
"1004"=dword:00000000

; Scripting
; 1400: Active scripting (0=Enable)
"1400"=dword:00000000
```

```
; 1402: Scripting of Java applets (0=Enable)
"1402"=dword:00000000

; Other
; 1A00: Logon (0x20000 = automatic logon with current username/password)
"1A00"=dword:00020000

; 1608: Allow META REFRESH (0=Enable)
"1608"=dword:00000000

; 1609: Allow script-initiated windows without size/position constraints (1=Enable)
"1609"=dword:00000001

; 2200: Automatic prompting for file downloads (0=Enable)
"2200"=dword:00000000

; 2201: File download (0=Enable)
"2201"=dword:00000000

; 1806: Launching applications and unsafe files (0=Enable)
"1806"=dword:00000000
```

Security note

This section intentionally relaxes several legacy browser-security controls in **Trusted Sites (Zone 2)**. In particular, it enables unsigned ActiveX download and launching applications/unsafe files.

Do not deploy this section broadly unless the target legacy application requires it and the configuration has been reviewed by the organization's Infra/Security team.

Applying the Full Internal Package

The original `setup.bat` performs the following sequence:

```
regedit /s "01_Allow_Popups.reg"
regedit /s "02_Compatibility_View.reg"
regedit /s "03_Trusted_Sites.reg"
regedit /s "04_Allow_All_Cookies.reg"
regedit /s "05_Security_Zones.reg"
```

The package writes to `HKEY_CURRENT_USER`.

For another organization, importing all five files should **not** be the default approach. Review the settings first and apply only those required for the observed symptoms and approved by the organization's security policy.