Electric Reliability Council of Texas (ERCOT)
Internet Explorer IE 11.x Configuration Guide

Effective: October 01, 2015
## Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/26/2015</td>
<td>1.0</td>
<td>Initial Posted version</td>
<td>Raj Rajagopal</td>
</tr>
<tr>
<td>10/02/2015</td>
<td>1.1</td>
<td>Minor edits</td>
<td>Raj Rajagopal</td>
</tr>
<tr>
<td>10/08/2015</td>
<td>1.2</td>
<td>Update regarding CRR compatibility</td>
<td>Raj Rajagopal</td>
</tr>
</tbody>
</table>
# Contents

1. Introduction .................................................................................. 4
2. Purpose ...................................................................................... 4
2. Scope ......................................................................................... 5
4. Configuration setting for Internet Explorer 11.x ................................. 6
5. Running IE 11.x in Compatibility mode ........................................... 28
6. Running IE 11.x in Enterprise mode ............................................... 30
7. ERCOT Applications URLs to be added to the Enterprise Mode Site List Manager ........................................ 32
8. CRR Bilateral Trade function ....................................................... 33
9. APPENDIX ................................................................................ 34
1. Introduction

The purpose of this document is to provide market participants with information about configuration settings for Microsoft’s Internet Explorer (IE) version 11.x. These configuration settings are expected to provide better compatibility to access ERCOT’s external-facing browser-based applications using IE 11.x. Examples of these applications include the Credit Management Module (CMM), Market Management System (MMS), Congestion Revenue Rights (CRR), and Network Modeling and Management System (NMMS), among others. ERCOT used the configuration settings provided in this document as the baseline to test external-facing browser-based applications using IE 11.x. A list of ERCOT external-facing browser-based applications is included below.

ERCOT’s Enterprise Architecture manages the overall technology lifecycle for browsers, which includes platform compatibility.

2. Purpose

Early this year Microsoft announced the End-of-life policy for IE versions below IE 11:

“Beginning January 12, 2016, only the most current version of Internet Explorer available for a supported operating system will receive technical support and security updates.”

This list of supported operating systems and browser combinations are as follows:

<table>
<thead>
<tr>
<th>Windows Desktop Operating Systems</th>
<th>Internet Explorer Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Vista SP2</td>
<td>Internet Explorer 9</td>
</tr>
<tr>
<td>Windows 7 SP1</td>
<td>Internet Explorer 11</td>
</tr>
<tr>
<td>Windows 8.1 Update</td>
<td>Internet Explorer 11</td>
</tr>
</tbody>
</table>

---

1 Internet Explorer Support Lifecycle Policy [http://support.microsoft.com/gp/Microsoft-Internet-Explorer](http://support.microsoft.com/gp/Microsoft-Internet-Explorer).
ERCOT is publishing this configuration guide in response to the above announcement. The guide provides directions for those market participants that intend to deploy IE 11 in their corporate environment. For market participants who intend to stay with their current browser versions, ERCOT support model for browsers older than 11.x has not changed.

2. **Scope**

The scope of this Guide applies to the following applications:

- Credit Management Module (CMM)
- Market Management System (MMS)
- Congestion Revenue Rights (CRR)
- Outage Scheduler (OS)
- Renewable Energy Credit (REC)
- Retail
  - Market Data transparency
  - MarkeTrak
  - (Create Enrollment)
  - (Create Move In)
  - (Create Move Out)
  - (Delete CSA)
  - (Establish CSA)
  - (Find ESIID)
  - (Find Transactions)
- Market Participant Identify Management (MPIM)
- Mobile Application
- Market Participant Online
- Market Information System (MIS)
  - Application
  - Download
  - Portal
- Eenergy (Siebel UI)
IE 11.x Configuration Guide

- Eservices (Service Requests)
- Eservices (Settlement Disputes)
- ERCOT Portal Online Help
- ERCOT.com
- ETOD
- Extract Subscriber
- LMS (Learning Management System)
- Notice Builder
- PGC Extracts (Extract Subscriber)
- Planning web site
- Report Explorer

3. Identify current browser version

To identify the current browser version do the following:

- Option 1: Go to the page it will display the browser version
  

- Option 2: Open Internet Explorer.
  
  On the “Help” menu, choose “About Internet Explorer.” It will display the current browser version

4. Configuration setting for Internet Explorer 11.x

The following are minimum recommended settings for Internet Explorer 11.x

Go to “Tools” Menu and choose “Internet Options”
Choose the tab “Security” and click on the button “Custom level”
Under Custom level Enable the the following settings
Security Settings - Internet Zone

- NET Framework-reliant components
  - Permissions for components with manifests
    - Disable
    - High Safety
- Run components not signed with Authenticode
  - Disable
  - Enable
  - Prompt
- Run components signed with Authenticode
  - Disable
  - Enable
  - Prompt
- ActiveX controls and plug-ins
  - Allow ActiveX Filtering
    - Disable
    - Enable

* Takes effect after you restart your computer

Reset custom settings
Reset to: Medium-high (default)
Security Settings - Internet Zone

Settings

- Binary and script behaviors
  - Administrator approved
  - Disable
  - Enable

- Display video and animation on a webpage that does not use
  - Disable
  - Enable

- Download signed ActiveX controls
  - Disable
  - Enable (not secure)
  - Prompt (recommended)

- Download unsigned ActiveX controls
  - Disable (recommended)
  - Enable (not secure)
  - Prompt

* Takes effect after you restart your computer

Reset custom settings

Reset to: Medium-high (default) → Reset...
Optional
The following settings are miscellaneous and are indifferent for browser compatibility.
IE 11.x Configuration Guide

Security Settings - Internet Zone

Settings

- Allow scripting of Microsoft web browser control
  - Disable
  - Enable
- Allow script-initiated windows without size or position constraint
  - Disable
  - Enable
- Allow webpages to use restricted protocols for active content
  - Disable
  - Enable
  - Prompt
- Allow websites to open windows without address or status bar
  - Disable
  - Enable
- Display mixed content
  - Disable
  - Enable

*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium-high (default) ➔ Reset...

OK ➔ Cancel
Security Settings - Internet Zone

Settings

- Display mixed content
  - Disable
  - Enable
  - Prompt

- Don't prompt for client certificate selection when only one certificate is available
  - Disable
  - Enable
  - Prompt

- Drag and drop or copy and paste files
  - Disable
  - Enable
  - Prompt

- Enable MIME Sniffing
  - Disable
  - Enable

- Include local directory path when uploading files to a server

*Note: Takes effect after you restart your computer

Reset custom settings

Reset to: Medium-high (default)
Security Settings - Internet Zone

- Include local directory path when uploading files to a server
  - Disable
  - Enable

- Launching applications and unsafe files
  - Disable
  - Enable (not secure)
  - Prompt (recommended)

- Launching programs and files in an IFRAME
  - Disable
  - Enable (not secure)
  - Prompt (recommended)

- Navigate windows and frames across different domains
  - Disable
  - Enable
  - Prompt

* Takes effect after you restart your computer

Reset custom settings
Reset to: Medium-high (default)
Security Settings - Internet Zone

Settings
- Userdata persistence
  - Disable
  - Enable

- Websites in less privileged web content zone can navigate in
  - Disable
  - Enable
  - Prompt

Scripting
- Active scripting
  - Disable
  - Enable
  - Prompt

- Allow Programmatic clipboard access

*Optional

Reset custom settings
- Reset to: Medium-high (default)

Reset... OK Cancel
IE 11.x Configuration Guide

Security Settings - Internet Zone

Settings
- Allow Programmatic clipboard access
  - Disable
  - Enable
  - Prompt
- Allow status bar updates via script
  - Disable
  - Enable
- Allow websites to prompt for information using scripted window
  - Disable
  - Enable
- Enable XSS filter
  - Disable
  - Enable
- Scripting of Java applets
  - Disable
  - Enable

* Takes effect after you restart your computer

Reset custom settings
Reset to: Medium-high (default)  Reset...
Choose the tab “Advanced” and make the following choices.

 Optional
Internet Options

Settings

- Display a notification about every script error
- Enable automatic crash recovery*
- Enable FTP folder view (outside of Internet Explorer)
- Enable Suggested Sites
- Enable third-party browser extensions*
- Enable visual styles on buttons and controls in webpages
- Go to an intranet site for a single word entry in the Address bar

*Requires restart of computer

Reset Internet Explorer settings

Reset Internet Explorer’s settings to their default condition.

You should only use this if your browser is in an unusable state.

Some settings are managed by your system administrator.

Optional
Optional
Optional
Internet Options

General Security Privacy Content Connections Programs Advanced

Settings

- Enable Integrated Windows Authentication
- Enable native XMLHTTP support
- Enable SmartScreen Filter
- Enable Strict P3P Validation
- Send Do Not Track requests to sites you visit in Internet Explorer
- Use SSL 2.0
- Use SSL 3.0
- Use TLS 1.0
- Use TLS 1.1
- Use TLS 1.2
- Warn about certificate address mismatch
- Warn if changing between secure and not secure mode
- Warn if POST submittal is redirected to a zone that does not match

* Takes effect after you restart your computer

Reset Internet Explorer settings

 Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Some settings are managed by your system administrator.

OK Cancel Apply
5. Running IE 11.x in Compatibility mode

The Internet Explorer browsers have a feature called “Compatibility View” which helps content written in older versions of the browser to render properly in the current version of the browser. In IE 8 this feature was available as a button on the address bar. In IE 11.x this button was deprecated (due to the introduction of X-UA-Compatible tags). However, the compatibility feature still remains in IE 11.x. If there are problems rendering certain ERCOT external applications, enable “Compatibility View” as follows:

1. Open Internet Explorer 11.x
2. Click “Tools”
3. Choose “Compatibility View”
In the Compatibility View Settings box, add the website URL, and then click Add. This turns on Compatibility View for this single website, for this specific computer.
6. Running IE 11.x in Enterprise mode

Enterprise Mode is a compatibility mode that runs on Internet Explorer 11 on Windows 8.1 Update and Windows 7 devices. IE 11 with Enterprise Mode allows websites to render using a modified browser configuration that emulates Internet Explorer 8. This addresses some of the common compatibility problems for applications written on older versions of Internet Explorer. Microsoft notes that with IE 11 in Enterprise Mode, users can take advantage of the newer features of IE 11 while achieving better compatibility with older browser versions.

6.1 System Requirements for running in Enterprise Mode

Enterprise Mode works on Internet Explorer 11 running on Windows 8.1 Update, Windows Server 2012 R2, Windows 7 SP1, or Windows Server 2008 R2 with SP1.

6.2 Turning on Enterprise Mode

Enterprise mode uses sitelist to determine which websites to render in compatibility mode. Before site lists can be used Enterprise Mode must be turned on and set up the system for centralized control. The sitelist is stored either centrally or is stored locally if the centralized file location is unavailable. There are two ways to turn on Enterprise Mode: (a) Using Enterprise Mode Group Policy and (b) Using registry edits.

6.3 Turning on Enterprise Mode using Group Policy

Open Group Policy editor and go to the Administrative Templates\Windows Components\Internet Explorer\Use the Enterprise Mode IE website list setting.

Turning this setting on also requires you to create and store a site list. For more information about creating your site list, see Add sites to the Enterprise Mode site list using the Enterprise Mode Site List Manager or Add multiple sites to the Enterprise Mode site list using a file and Enterprise Mode Site List Manager.

6.4 The Enterprise Mode Site List Manager

The Enterprise Mode Site List Manager tool is used to add individual website domains and domain paths and to specify whether the site renders using Enterprise Mode or the default mode. To add a site to the Site List Manager do the following:
6.5 Adding a site to compatibility list

1. In the Enterprise Mode Site List Manager tool, click **Add**.
2. Type the URL for the website that’s experiencing compatibility problems, like `<domain>.com` or `<domain>.com/<path>` into the **URL** box.
   You don’t need to include the http:// or https:// designation. The tool will automatically try both versions during validation.
3. Type any comments about the website into the **Notes about URL** box.
   Administrators can only see comments while they’re in this tool.
4. Pick **IE7 Enterprise Mode**, **IE8 Enterprise Mode**, or the appropriate document mode for sites that must be rendered using the emulation of a previous version of IE, or pick **Default IE** if the site should use the latest version of IE.
5. Click **Save** to validate your website and to add it to the site list for your enterprise.
   If your site passes validation, it’s added to the global compatibility list. If the site doesn’t pass validation, you’ll get an error message explaining the problem. You’ll then be able to either cancel the site or ignore the validation problem and add it to your list anyway.
6. On the **File** menu, go to where you want to save the file, and then click **Save to XML**.
   You can save the file locally or to a network share. However, you must make sure you deploy it to the location specified in your registry key. For more information about the registry key, see **Turn on local control and logging for Enterprise Mode**.
7. ERCOT Applications URLs to be added to the Enterprise Mode Site List Manager

ERCOT recommends adding the following sites to the IE 11 site List Manager:

- www.ercot.com
- cmm.ercot.com/login.jsp
- mis.ercot.com
- mis.ercot.com/crr/mui/ListAllUserMessage.do
- mis.ercot.com/marketrk/tmtrack.dll
- mis.ercot.com/MODWeb/Login.aspx
- crr.ercot.com
8. CRR Bilateral Trade function

The CRR application bilateral trading pages support only JRE1.6, which may not work under IE11. This issue will be addressed in Release 6 scheduled for December 2015. However, full JRE1.7 support is not scheduled until late 2016 for CRR.
9. APPENDIX
Steps to Export/Import ERCOT Digital Certificates

Market participants use digital certificates to authenticate access to external applications. If you currently have a digital certificate in a version of browser other than IE 11, that certificate has to be imported to IE 11. The following pages show how to export existing digital certificates to IE 11.
In order to keep your certificate safe, a password is required. Remember your password as you will need it to import your certificate. Once created, click “Next”.

Name the certificate, give it a meaningful name and save it to a location you can remember, as you will need to go back this location to import. Click “Next”.

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click next.

---

File to Import

Specify the file you want to import.

File name: [Input field]

Note: More than one certificate can be stored in a single file in the following formats:
- Personal Information Exchange - PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SSM)

Learn more about certificate file formats
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:
- **Certificate Store Selected by User:** Personal
- **Content:** PFX
- **File Name:** C:/User/imizar/Dc

The import was successful.