Portal Transition Guide for Modernized e-File (MeF)

Introduction

The purpose of this guide is to assist software developers, transmitters, and states in the transition of MeF to the new Integrated Enterprise Portal (IEP). The MeF application version and current supported schemas will not change as part of this migration. This is a technical publication and is not intended for tax preparers. The transition to the new portal (IEP) should be transparent to tax preparers and taxpayers.

IRS is in the process of completing a multi-year upgrade to the on-line portal infrastructure. The earlier infrastructure has served the IRS, its partners, and taxpayers well. With the success of IRS.gov, the portal applications and other interactive applications, the demands on the portal infrastructure significantly increased. In order to continue to meet the expanding on-line portal needs, the IRS portal infrastructure needed a significant upgrade. The new service based infrastructure will allow the IRS to support the portal needs for the foreseeable future.

Some of the benefits of the new IRS portal infrastructure:

- One-stop, Web-based services to internal and external users.
- Enhanced secure and reliable portals with a modernized portal design and increased systems capacity.
- Keeps IRS information current and accurate with near real-time updates of more than 110,000 forms, publications, news items, rules, and articles.
- Meets demand from the public taxpayer for information and resources, and from the tax preparer population for support for resources and submissions.
- Improves user experience for both taxpayers and tax preparers by making information and materials easy to find and obtain.
- Offers self-service options for taxpayers and tax preparers for information and publications.
- Reduces paper and person-to-person interactions between the IRS and the public taxpayer/tax preparer to complete a tax transaction.
- Taxpayers and tax preparers can more easily find and obtain information and material without calling the IRS.
- Supports tax preparer submissions.

The first phase of the IRS portal upgrade was the transition to a new IRS.gov in August 2012. The second phase supports all registered user applications and was implemented over the Labor Day weekend of August 31st through September 2nd, 2013, with full operation on September 3rd, 2013.

Revision History

Version Number	Summary of Changes	Changes Marked
1.0	Initial Draft	No
1.1	Information added to the “Certification Location” section	No
1.2	Added a “Troubleshooting Guidance” Section. Clarified Hours of Operation that IEP is available.	No
1.3	Clarification on IFA URL behavior. Added IFA information to the “Troubleshooting Guidance” Section	No
1.4	Added more details to the Timeline. Included additional information the “Troubleshooting Guidance” section	No
1.5	Removed the information about ATS testing. Included information about cookie changes.	Yes
1.6	Updated Cookie Information	Yes

Information Highlights

- The MeF Production and ATS environment migrated to the new portal (IEP) and became *fully operational* to all software developers, transmitters and states on Tuesday, September 3rd, 2013 at 12:00 p.m. ET. The MeF application version and current supported schemas did not change.

- The new portal (IEP) requires new public SSL certificates for establishing the SSL connection. Your software or browser configurations may be set up to automatically download these certificates when it connects to the new portal (IEP) the first time. Information on where you can manually download them is located in the Technical Guidelines section below.

- A2A toolkit users (SDK and client application) were also impacted by these changes. Please read the Technical Guidelines section below for more details.

Technical Guidelines

Enterprise Firewall Configuration:

If clients must connect through enterprise firewalls which restrict their outbound connections by IP address please send an email to the MeF Mailbox at mefmailbox@irs.gov . Please include your DNS information and whether you support IPv6 or IPv4.

Caches:

Our recommendation is to clear cache information on your devices; desktop, server, browser, laptop etc.

Certificate location:

The new portal (IEP) has a different server certificates for establishing the SSL connection than the previous portal (RUP) did. Your software or browser configurations may be set up to automatically download these certificates when it connects to IEP the first time. If you need to manually download the certificates for the testing period and production they are available on the MeF User Guide & Publications .

The certificates are in a ZIP folder with the file extension *.txt. If you need to convert them to another file type (*.cer, *.crt, *.pem, etc) in order to upload them to your server you can rename the certificates to the necessary file type.

A2A Toolkit Users:

The new portal (IEP) server certificates need to be added to the A2A Toolkit Trust Store.

Cookies:

IEP has introduced a new "DC" cookie that is used for site stickiness by the IEP architecture. JSESSION cookie is the other cookie that is being passed with the request but it's not new to IEP. Both DC and JSESSION cookies are being passed to clients on Login Service Request and required to pass back with all service requests within the session. There are some issues noted with .NET framework with passing multiple cookies. MeF can provide sample code snippets to help developers deal with those issues. Please contact the MEF Mailbox @ mefmailbox@irs.gov to get the code snippets.

The IEP will need the following information in the HTTP Headers of the Client Requests:

1. IEP adds 2 very important cookies to a HTTP Request. These will be part of the HTTP Header for that SOAP/HTTP Web Service.
2. The first Cookie is "JSESSIONID" cookie. Used for internal server stickiness.
3. The second Cookie is the "dc" cookie. This will help the web services to be routed to the correct SITE (Data Center).
4. In the IRS web services the Login and Logout (and all the web services executed in between this Login and Logout) are tightly coupled meaning that it is not just the SAML token but also that they need to be executed in the same SITE. So for this reason they can be considered as one multi services transaction. The "dc" cookie helps IEP to route these service to the same SITE as the Login.
5. The "dc" Cookie will be sent back on the Login response (and all subsequent request) and can be found in the HTTP Header. This cookie needs to be sent back in the subsequent Client Requests.
6. The "dc" Cookie will also be sent back on Get Service and if this Get service used to persist this particular session for reuse then it is expected that the subsequent requests do sent the cookies back in their HTTP header.
7. The IEP also sets a few other Cookies, it is preferred that all Cookies set by IEP should be returned by the toolkit, however, the "dc" and "JSESSIONID" are the most critical ones
8. It is preferred that the 2 IEP cookies be sent back in the subsequent Requests' HTTP header as is, meaning 2 separate cookies, the way they were received.
9. If the Clients are unable to send multiple cookies in their HTTP header due to limitations from their frameworks then they should send back all the name-value pairs from both the cookies (as they received) in a single cookie properly formatted and all the name-value pairs from both the received cookies separated by semi-colons. Some frameworks might separate the cookie name-value pairs using a comma (,) that is not acceptable.
10. The A2A clients should not modify the cookie values or remove them.

Please note: This only affects A2A clients and has no affect on the IFA clients. As a short-term measure, the IRS has implemented a fix where all traffic is being diverted to one site. This will help alleviate the session limit reached issue experienced by some clients. Once the cookie solution is implemented by the externals, we will remove this short-term fix. We expect the externals to make all cookies related coding changes before the start of the 2014 filing season.

A2A Toolkit Clients: The new version of the A2A toolkit (v4.0) which is due late October is coded to pass back the cookies properly.

Troubleshooting Guidance:

A2A

Certificate Validation Error

- On a Windows Server 2003-based, Windows XP-based, or an older version computer, you cannot obtain certificates from a Windows Server 2008-based certification authority (CA). In this case, you receive an event for the certificate autoenrollment operation "Automatic certificate enrollment for local system failed to enroll for one Computer2008 certificate (0x80092009). Cannot find the requested object." You may also get a warning that the "The remote server presented a certificate that did not validate, due to RemoteCertificateChainErrors" when you try to establish the SSL connection.

  If you experience these symptoms please make sure that you install the hotfix that will allow you obtain the certificates. For example, if you are running Windows Server 2003 the hotfix that has worked for some transmitters was http://support.microsoft.com/kb/968730?wa=wsignin1.0

Importing SSL Certificates into a Java Keystore

- Software developers who use the Java Keystore on a UNIX based operating system will need to import the new IEP SSL certificate into it. You can add them using the standard Java "keystore – import" option. **Note:** This information is applicable to A2A Toolkit users who use Java SDK since they are also using the cacerts file for their trust store.

IFA

Certificate Warning Messages

- When you navigate to the URL to test IEP, listed in the Technical Guidelines section, your web browser may ask if you want to trust the certificate presented before displaying the Login website.

  You may also get a warning when you try to download a file. For example, the message for Internet Explorer says "There is a problem with this website's security certificate. The security certificate presented by this website was issued for a different website's address. Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server. We recommend that you close this webpage and do not continue to this website."

  If you receive this message you need to import the certificates into your browser. If you do not have permission to import these certificates on your workstation contact your system administrator. The location of these certificates is listed the Technical Guidelines section.