[MS-OIDCE]: OpenID Connect 1.0 Protocol Extensions

This topic lists the Errata found in [MS-OIDCE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V4.0 – 2017/09/15.

Errata Published*	Description
2017/09/18	Several sections in this document were updated to show that, with KB 4038801, the OpenID Connect 1.0 Protocol Extensions on Windows Server 2016 implement OpenID Connect Front-Channel Logout instead of OpenID Connect Session Management. In Section 1.2.1, Normative References, the following references were added: [MSKB-4038801] Microsoft Corporation, "September 19, 2017 - KB4038801", https://support.microsoft.com/help/4038801 [OIDCFrontChanLO] Jones, M., "OpenID Connect Front-Channel Logout 1.0 - draft 02", January 2017, http://openid.net/specs/openid-connect-frontchannel-1_0.html In Section 1.5, Prerequisites/Preconditions, the citation to [OIDCSession] was replaced with a citation to [OIDCFrontChanLO], and normative language and a behavior note were added to [OIDCSession] support. Changed from: The OpenID Connect 1.0 Protocol Extensions define extensions to [OIDCCore], [OIDCSession], and [OIDCDiscovery]. The following prerequisites are required for implementing the OpenID Connect 1.0 Protocol Extensions: - The REQUIRED parts of [OIDCCore] and [OIDCDiscovery] have been implemented on the AD FS server. - The REQUIRED parts for RP-Initiated Logout, as defined in [OIDCSession] section 5, have been implemented on the AD FS server. Changed to: The OpenID Connect 1.0 Protocol Extensions define extensions to [OIDCCore], [OIDCFrontChanLO], and [OIDCDiscovery]. The following prerequisites are required for implementing the OpenID Connect 1.0 Protocol Extensions: - The REQUIRED parts of [OIDCCore] and [OIDCDiscovery] have been implemented on the AD FS server. - The REQUIRED parts for RP-Initiated Logout, as defined in [OIDCSession] section 5, SHOULD<1> have been implemented on the AD FS server. <1> Section 1.5: Only Windows Server 2016 with [MSKB-4019472] installed but without [MSKB-4038801] installed and Windows Server v1709 implement the REQUIRED parts for RP-Initiated Logout as defined in [OIDCSession] section 5.

Errata Published*	Description
	In Section 2.2.3.2, OpenID Provider Metadata, the citation to [OIDCSession] was replaced with a citation to [OIDCFrontChanLO]. The existing product behavior note was updated. A new note was added for additional metadata fields, along with a product behavior note describing their context. Changed from: OpenID Provider Metadata provides information about the OpenID connect provider, as described in [OIDCDiscovery] section 3. Note: The end_session_endpoint metadata field defined in the [OIDCSession] section 2.1 is required for the OpenID Connect 1.0 Protocol Extensions.<2> ... <2> Section 2.2.3.2: Windows implementations of the AD FS server can be configured in an implementation-specific way to either return or not return the end_session_endpoint metadata. Changed to: OpenID Provider Metadata provides information about the OpenID connect provider, as described in [OIDCDiscovery] section 3. Note: - The end_session_endpoint metadata field defined in [OIDCFrontChanLO] section 4 is required for the OpenID Connect 1.0 Protocol Extensions.<3> - The frontchannel_logout_supported and frontchannel_logout_session_supported metadata fields defined in the [OIDCFrontChanLO] section 3 are required for the OpenID Connect 1.0 Protocol Extensions.<4> ... <3> Section 2.2.3.2: In Windows Server 2016 with [MSKB-4019472] installed but without [MSKB-4038801] installed and in Windows Server v1709, the AD FS server can be configured in an implementation-specific way to either return or not return the end_session_endpoint metadata. <4> Section 2.2.3.2: Windows Server 2016 without [MSKB-4038801] installed and Windows Server v1709 do not support [OIDCFrontChanLO]. In Section 3.1.5.4, Logout endpoint (/logout), the citation to [OIDCSession] was replaced with a citation to [OIDCFrontChanLO], and the existing product behavior note was updated. Changed from: As defined in the [OIDCSession] section 5, the Logout endpoint logs out the user from the AD FS server. The following HTTP methods are allowed to be performed on this endpoint.<5> ... <5> Section 3.1.5.4: Windows Client operating systems (Windows 10 v1511 and later) do not implement the extensions to OpenID Connect Session Management. Changed to: As defined in the [OIDCFrontChanLO] section 4, the Logout endpoint logs out the user from the AD FS server. The following HTTP methods are allowed to be performed on this endpoint.<7> ...

Errata Published*	Description
	<7> Section 3.1.5.4: Logout support in Windows Server 2016 without [MSKB-4038801] installed and in Windows Server v1709 is limited to OpenID Connect Session Management ([OIDCSession], specifically, section 5). Windows Client operating systems (Windows 10 v1511 and later) do not implement the extensions to OpenID Connect Session Management or OpenID Connect Front-Channel Logout. In Section 3.2.5.4 Logout endpoint (/logout), the citation to [OIDCSession] was replaced with a citation to [OIDCFrontChanLO], and the existing product behavior note was updated. Changed from: As defined in [OIDCSession] section 5, the Logout endpoint logs out the user from the AD FS server. The following HTTP methods are allowed to be performed on this endpoint.<9> ... <9> Section 3.2.5.4: The Logout endpoint is not supported on Windows Server 2016 unless [MSKB-4019472] is installed. Changed to: As defined in [OIDCFrontChanLO] section 4, the Logout endpoint logs out the user from the AD FS server. The following HTTP methods are allowed to be performed on this endpoint.<11> ... <11> Section 3.2.5.4: The following support information applies to the Logout endpoint: - The Logout endpoint is not supported on Windows Server 2016 unless [MSKB-4019472] is installed. - The Logout endpoint is implemented as OpenID Connect Session Management ([OIDCSession], specifically, section 5) in Windows Server 2016 with [MSKB-4019472] installed but without [MSKB-4038801] installed. - The Logout endpoint is implemented as OpenID Connect Session Management ([OIDCSession], specifically, section 5) in Windows Server v1709. - The Logout endpoint is implemented as OpenID Connect Front-Channel Logout ([OIDCFrontChanLO]) in Windows Server 2016 with [MSKB-4038801] installed. - - - - - - - - - - - - - - - - - - In several sections, the citation to [OIDCSession] was replaced with a citation to [OIDCFrontChanLO], as shown below. In the following sections, changed "[OIDCSession]" to "[OIDCFrontChanLO]": - 3.1.5, Message Processing Events and Sequencing Rules - 3.2.5, Message Processing Events and Sequencing Rules In the following sections, changed "[OIDCSession] section 5" to "[OIDCFrontChanLO] section 4": - 3.1.5.4.1.1, Request Body - 3.1.5.4.1.2, Response Body - 3.1.5.4.1.3, Processing Details - 3.2.5.4.1.1, Request Body

Errata Published*	Description
	- 3.2.5.4.1.2, Response Body - 3.2.5.4.1.3, Processing Details In Section 4.2, Example OpenID Provider Configuration Response, fields were added to the example. Changed from: ... "access_token_issuer":"https://server.example.com", "microsoft_multi_refresh_token":true } Changed to: ... "access_token_issuer":"https://server.example.com", "microsoft_multi_refresh_token":true, "end_session_endpoint":"https://server.example.com/logout", "frontchannel_logout_supported":true, "frontchannel_logout_session_supported":true }

*Date format: YYYY/MM/DD