APPENDIX **B**

Customer Log Messages

This appendix summarizes the various Customer Log messages that the AD Agent can generate (based on the current value of the “logLevel” configurable option) under various functional categories.

You can use the **adacfg options set –logLevel** command to change the “logLevel” setting.

Note Some of these log messages are associated with the “NOTICE” logging level (which falls between the “INFO” and “WARN” levels), but “NOTICE” itself cannot be chosen as a setting for 'logLevel' using the above adacfg command.

The following scale shows the full spectrum of logging levels, in order of increasing verbosity, with “NOTICE” highlighted in Italics font to show that it is not a configurable option for “logLevel,” and “INFO” highlighted in bold face font to show that it is the default setting for “logLevel:”

FATAL < ERROR < WARN < *NOTICE* < **INFO** < DEBUG

Note When you troubleshoot problems, it is often helpful to raise the setting of “logLevel” from its default setting of “INFO” to the most verbose level “DEBUG.” However, this setting can have a negative impact on the performance of the AD Agent. We recommend that you restore the setting of “logLevel” after you have resolved your problems.

Similarly, lowering the “logLevel” from its default setting of “INFO” to a lesser verbose level “WARN” can have a positive impact on the performance of the AD Agent. However, this setting will prevent the output of any “INFO” or “NOTICE” level messages (that can potentially be important for administrative or auditing purposes).

A local archive of historical Customer Log messages is maintained inside the “C:\IBF\radiusServer\runtime\logs\localStore” directory. These log messages are also forwarded to any remote syslog targets that have been configured using the **adacfg syslog create** command.

Table B-1 lists the AD-Agent-specific messages that can be logged to the Customer Logs, with the message code, logging level, message class, message text, and a general description corresponding to each. This is not the full list of all messages that can be generated, and it does not include, for example, generic RADIUS-related messages or other miscellaneous messages.

Table B-1 AD Agent Log Messages

Message Code	Logging Level	Message Class	Message Text	Description
AD Agent Start/Stop				
(a more comprehensive set of messages is logged in the Windows Application Event Log. See Appendix C, "Windows Application Event Logs," for more information.				
31502	INFO	STARTUP-SHUTDOWN	Started Runtime	The "RADIUS Server" subcomponent of the AD Agent has been started.
Configuration Changes				
68000	NOTICE	IBF_CONFIG_CHANGE	Created DC configuration	A domain controller machine has been configured in the AD Agent using the **adacfg dc create** command.
68001	NOTICE	IBF_CONFIG_CHANGE	Deleted DC configuration	A domain controller machine configuration has been removed from the AD Agent using the **adacfg dc erase** command.
68002	NOTICE	IBF_CONFIG_CHANGE	Created RADIUS-client configuration	A client device has been configured in the AD Agent using the **adacfg client create** command.
68003	NOTICE	IBF_CONFIG_CHANGE	Deleted RADIUS-client configuration	A client device configuration has been removed from the AD Agent using the **adacfg client erase** command.
Mapping Updates				
12862	INFO	IBF_RADIUS_SERVER	Updated mapping in Identity Cache	An IP-address-to-user-identity mapping has been added or updated in the internal cache of the AD Agent.
12855	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update due to userLogonTTL	An incoming IP-address-to-user-identity mapping update has been ignored by the AD Agent because the logon time occurred too far in the past (relative to the "userLogonTTL" configurable option).
12856	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update: older than existing mapping	An incoming IP-address-to-user-identity mapping update has been ignored by the AD Agent because the associated logon time was earlier that that of the one currently cached by the AD Agent for the same IP address.

Table B-1 AD Agent Log Messages (continued)

Message Code	Logging Level	Message Class	Message Text	Description
12859	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update having timestamp in future	An incoming IP-address-to-user-identity mapping update has been ignored by the AD Agent because the associated logon time is in the future.
12861	INFO	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-update: same time as existing mapping	An incoming IP-address-to-user-identity mapping update has been ignored by the AD Agent because the associated logon time is identical to the one currently cached by the AD Agent for the same IP address and username.
12867	WARN	IBF_RADIUS_SERVER	Approaching stress limit on Identity Cache mapping-updates	AD Agent is approaching its maximum capacity limit on the number of cached mappings. Currently, over 100,000 mappings are cached. If the cache occupancy reaches 200,000 mappings, the AD Agent starts to ignore subsequent incoming mapping updates.
12868	ERROR	IBF_RADIUS_SERVER	Dropped Identity Cache mapping-updates: stress limit exceeded	The AD Agent has reached its maximum capacity limit of 200,000 mappings, and is now ignoring all new incoming mapping updates.
12893	INFO	IBF_RADIUS_SERVER	Deleted mapping in Identity Cache	An IP-address-to-user-identity mapping has been removed from the internal cache of the AD Agent.
Synch Requests				
12869	INFO	IBF_RADIUS_SERVER	Detected Synch request with registration for notifications	A client device has requested to receive a session data snapshot of all mappings currently found in the cache of the AD Agent. The client requests to be registered with the AD Agent for replication.
12860	INFO	IBF_RADIUS_SERVER	Detected Synch request with no registration for notifications	A client device has requested to receive a session data snapshot of all mappings currently found in the cache of the AD Agent. The client does not want to be registered with the AD Agent for replication.

Table B-1 AD Agent Log Messages (continued)

Messag e Code	Logging Level	Message Class	Message Text	Description
12870	INFO	IBF_RADIUS_SERVER	Detected Synch request without change to registration state	A client device has requested to receive a session data snapshot of all mappings currently found in the cache of the AD Agent. The client does not want to change its replication-related state with the AD Agent.
12871	INFO	IBF_RADIUS_SERVER	Detected deregistration Request	A client device has requested not be registered for replication with the AD Agent.
12872	WARN	IBF_RADIUS_SERVER	Approaching capacity limit on max registrations	The AD Agent is approaching its maximum limit on the number of unique client devices that can be simultaneously registered for notification. Currently, over 100 unique client devices can be registered for notification. If this number reaches 120 unique client devices, the AD Agent starts to ignore subsequent incoming requests to register for notification.
12873	ERROR	IBF_RADIUS_SERVER	Dropped registrations: capacity limit exceeded	The AD Agent has reached its maximum limit of 120 unique client devices that can be simultaneously registered for notification, and is now ignoring all new incoming requests to register for notification.
CoA-Based Traffic				
12884	INFO	IBF_RADIUS_SERVER	Sent RADIUS CoA-Request with Notification to PEP	The AD Agent has proactively notified a client device about a mapping that has changed since the time it was provided to that client device. This notification update to the client device is sent using a RADIUS CoA-Request packet.
11223	INFO	Dynamic-Authorization	Received CoA ACK response	The AD Agent has received a RADIUS CoA-ACK packet sent by a client device. The client device acknowledges receipt of the CoA-Request packet sent by the AD Agent.
11224	INFO	Dynamic-Authorization	Received CoA NAK response	The AD Agent has received a RADIUS CoA-NAK packet sent by a client device. The client device acknowledges a problem about a CoA-Request packet sent by the AD Agent.

Table B-1 AD Agent Log Messages (continued)

Message Code	Logging Level	Message Class	Message Text	Description
Session Data Snapshot Transfers				
12878	INFO	IBF_RADIUS_SERVER	Stopping current transfer of session data snapshot	The currently in-progress transfer of a session data snapshot to a client device is being stopped.
12881	INFO	IBF_RADIUS_SERVER	Started transfer of session data snapshot	A new transfer of a session data snapshot to a client device is started. **Note** This log item will be used only for snapshot transfers involving two or more RADIUS packets. The first such packet will be marked with #12881. The last such packet will be marked with #12883. Any packets in between will be marked with #12882.
12882	INFO	IBF_RADIUS_SERVER	Continued transfer of session data snapshot	The currently in-progress transfer of a session data snapshot to a client device is continued. **Note** This log item will be used only for large snapshot transfers involving three or more RADIUS packets. The first such packet will be marked with #12881, and the last such packet will be marked with #12883. All of the packets in between will be marked with #12882.
12883	INFO	IBF_RADIUS_SERVER	Finished transfer of session data snapshot	The transfer of a session data snapshot to a client device has successfully been completed. Very small snapshot transfers, which can fit into a single RADIUS packet will be marked only with this log item (after transfer completion), but not with any #12881 or #12882 log items.
On-Demand Queries				
12864	INFO	IBF_RADIUS_SERVER	Detected On-Demand Entity-Request from PEP	A client device has requested to receive a mapping for a particular IP address (either with or without a request for subsequent notification).
12866	INFO	IBF_RADIUS_SERVER	Could not find identity in Identity Cache	The AD Agent could not find in its cache a mapping having the requested IP address.

Table B-1 AD Agent Log Messages (continued)

Message Code	Logging Level	Message Class	Message Text	Description
Keepalive Requests				
12885	INFO	IBF_RADIUS_SERVER	Detected Keepalive Request from PEP	A client device has sent a keepalive request to the AD Agent.
Domain Status Queries				
12890	INFO	IBF_RADIUS_SERVER	Prepared Domain Status Query-Response	The AD Agent has prepared, and is about to send, a response to a client device that has requested the AD Agent's connectivity status with regard to a specific Active Directory domain.
Domain Controller Status Tracking				
12892	INFO	IBF_AD_MONITOR	ActiveDirectory domain controller status changed	The AD Agent has detected a change in the up/down status of a domain controller machine.
Miscellaneous				
12888	WARN	IBF_RADIUS_SERVER	Internal Warning	The AD Agent has experienced an internal problem.
12889	ERROR	IBF_RADIUS_SERVER	Internal Error	The AD Agent has experienced an internal problem.
General Pass/Fail Status (each such log entry refers to corresponding entries having an identical value for their associated 'IbfSessionID' attribute.)				
5200	NOTICE	Passed-Attempt	IBF request succeeded	AD Agent has been able to successfully process a request (a Synch Request, an On-Demand Query, a Keepalive Request, or a Domain Status Query) previously received from a client device.
5400	NOTICE	Failed-Attempt	IBF request failed	AD Agent has been unable to successfully process a request (a Synch Request, an On-Demand Query, a Keepalive Request, or a Domain Status Query) previously received from a client device, due to a reason encoded in the value of the 'FailureReason' attribute. In this or any other similar (but generic) 'Failed-Attempt' log entry, possible 'FailureReason' codes are presented in the next subsection of this table.

Table B-1 AD Agent Log Messages (continued)

Message Code	Logging Level	Message Class	Message Text	Description
5405	NOTICE	Failed-Attempt	RADIUS Request dropped	AD Agent has received a RADIUS packet, but is silently dropping it, due to a reason encoded in the value of the 'FailureReason' attribute. In this or any other similar (but generic) 'Failed-Attempt' log entry, possible 'FailureReason' codes are presented in the next subsection of this table.
5413	NOTICE	Failed-Attempt	RADIUS Accounting-Request dropped	AD Agent has received a RADIUS Accounting-Request packet, but is silently dropping it, due to a reason encoded in the value of the 'FailureReason' attribute. In this or any other similar (but generic) 'Failed-Attempt' log entry, possible 'FailureReason' codes are presented in the next subsection of this table.
Potential 'FailureReason' Messages				
(any 'FailureReason' code specified in a 'Failed-Attempt' log entry but not found in this subsection of the table should be regarded as an internal AD Agent error.)				
11007	DEBUG	RADIUS	Could not locate Network Device or AAA Client	A RADIUS packet has been received from an IP address not associated with any currently-configured client devices. Make sure that this device is configured, using 'adacfg client create'.
11011	WARN	RADIUS	RADIUS listener failed	Could not open one or more of the UDP ports used for receiving RADIUS requests. Make sure that no other processes on the AD Agent machine are using ports 1812, 1813, 1645, or 1646.
11012	ERROR	RADIUS	RADIUS packet contains invalid header	A RADIUS packet having an invalid header has been received. Make sure that the client device is compatible with AD Agent and is functioning properly.
11013	INFO	RADIUS	RADIUS packet already in the process	An incoming RADIUS request has been ignored by AD Agent, because it is a duplicate of another previously received packet that is currently being processed.
11014	ERROR	RADIUS	RADIUS packet contains invalid attribute(s)	A RADIUS packet having invalid attributes has been received. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly.

Table B-1 AD Agent Log Messages (continued)

Message Code	Logging Level	Message Class	Message Text	Description
11021	ERROR	RADIUS	RADIUS could not decipher password. packet missing necessary attributes	A RADIUS packet having a password that could not be deciphered has been received. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly. Make sure that the same RADIUS shared secret has been properly configured, both in the client device and in AD Agent.
11029	WARN	RADIUS	Unsupported RADIUS packet type	A RADIUS packet having an invalid packet type has been received. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly.
11030	WARN	RADIUS	Pre-parsing of the RADIUS packet failed	An invalid RADIUS packet has been received. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly.
11031	WARN	RADIUS	RADIUS packet type is not a valid Request	A RADIUS response packet has been received when a RADIUS request packet was expected. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly.
11036	ERROR	RADIUS	The Message-Authenticator RADIUS attribute is invalid.	A RADIUS packet having an invalid Message-Authenticator attribute has been received. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly. Make sure that the same RADIUS shared secret has been properly configured, both in the client device and in AD Agent.
11037	ERROR	RADIUS	Dropped accounting request received via unsupported port.	A RADIUS Accounting-Request packet was received via an unsupported UDP port number. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly.

Table B-1 AD Agent Log Messages (continued)

Message Code	Logging Level	Message Class	Message Text	Description
11038	ERROR	RADIUS	RADIUS Accounting-Request header contains invalid Authenticator field.	A RADIUS Accounting-Request packet having an invalid Authenticator field in its packet header has been received. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly. Make sure that the same RADIUS shared secret has been properly configured, both in the client device and in AD Agent.
11039	INFO	RADIUS	RADIUS authentication request rejected due to critical logging error	An internal logging-related error has been detected, possibly due to lack of sufficient available disk space.
11040	INFO	RADIUS	RADIUS accounting request dropped due to critical logging error.	An internal logging-related error has been detected, possibly due to lack of sufficient available disk space.
11050	WARN	RADIUS	RADIUS request dropped due to system overload	An internal logging-related error has been detected, possibly due to lack of sufficient available disk space.
11052	ERROR	RADIUS	Authentication request dropped due to unsupported port number	A RADIUS request packet was received via an unsupported UDP port number. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly.
11053	WARN	RADIUS	Invalid attributes in outgoing radius packet - possibly some attributes exceeded their size limit	An internal has caused an outgoing RADIUS response packet to be invalid, possibly because the size of the packet as a whole, or of one of its associated attributes, had exceeded the maximum limit.
11103	ERROR	RADIUS-Client	RADIUS-Client encountered error during processing flow	An internal error has been detected during the processing of an incoming RADIUS packet. Make sure that the client device is compatible with AD Agent, has been configured properly, and is functioning properly. Make sure that the same RADIUS shared secret has been properly configured, both in the client device and in AD Agent.

Table B-1 AD Agent Log Messages (continued)

Message Code	Logging Level	Message Class	Message Text	Description
11213	WARN	Dynamic-Authorization	No response received from Network Access Device: lost communication with notification subscriber	AD Agent has not received any acknowledgement packet (positive or negative) from a client device to which it has previously sent a CoA-Request packet. AD Agent assumes that communication with this client device has been lost, and will set its status to 'Out-Of-Sync'.
11214	WARN	Dynamic-Authorization	An invalid response received from Network Access Device: lost communication with notification subscriber	AD Agent has received an invalid response from a client device to which it has previously sent a CoA-Request packet. AD Agent assumes that communication with this client device has been lost, and will set its status to 'Out-Of-Sync'.
32006	WARN	Logging	Could not log to critical logger	An internal logging-related error has been detected, possibly due to lack of sufficient available disk space.
32016	FATAL	Logging	System reached low disk space limit	Sufficient disk space is not available.