APPENDIX A

# Agent Properties

**Revised: March 30, 2012**

The agent.properties file contains the configuration settings for Connector. Typically, properties containing lists do not support the uses of spaces between separators.

**Caution** Before changing the settings of the agent.properties file you should discuss your requirements with customer support. In the worst case, certain settings could lead to Connector effectively blocking all traffic.

| Setting | Description | Default | Alternate |
|---|---|---|---|
| `<exception name>-exception_pattern` | See Host Exceptions, page 4-3. | | `<pattern1> [,<pattern2>...]` |
| `<exception name>-keepalive.enable` | See Host Exceptions, page 4-3. | `TRUE` | `FALSE` |
| `<exception name>-tunnel` | See Host Exceptions, page 4-3. | `FALSE` | `TRUE` |
| `<exception name>-primaryProxy` | See Host Exceptions, page 4-3. | | `<IP address or host name>` |
| `<exception name>-primaryProxyPort` | See Host Exceptions, page 4-3. | | `<port>` |
| `<exception name>-secondaryProxy` | See Host Exceptions, page 4-3. | | `<IP address or host name>` |
| `<exception name>-secondaryProxyPort` | See Host Exceptions, page 4-3. | | `<port>` |
| `<exception name>-tertiaryProxy` | See Host Exceptions, page 4-3. | | `<IP address or host name>` |
| `<exception name>-tertiaryProxyPort` | See Host Exceptions, page 4-3. | | `<port>` |
| `aup.enable` | Enable Acceptable Usage Policy support for Connector in standalone mode. This is not supported in enterprise mode. | `FALSE` | `TRUE` |
| `auth.realm` | The name of the realm that appears in the basic authentication dialog. | | `<realm>` |
| `backlog.size` | Maximum number of connections to queue. | `100 (Windows) 900 (Linux)` | `<number>` |
| `brand.file` | File that applies any branding text. | `branding.properties` | `<filename>` |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| connectorId | A unique string (up to 32 characters in length) used to identify the Connector instance for reporting purposes. The string can contain only alphanumeric characters, hyphens ( - ), and underscores ( _ ). | | <string> |
| defaultUpstreamPort | The value used when upstream ports for primary, secondary, or tertiary upstream proxies are not specified. For example, if secondaryProxy is specified and secondaryProxyPort is not, the defaultUpstreamPort value will be used. | 8080 | <port> |
| domains.<domain> | Comma separated list of domains to be grouped under a single domain for LDAP queries. This will override individual domain settings. | | <domain> |
| elb.buckets | Specifies how many upstream servers Connector should do load balancing to. | 1 | <number> |
| elb.enable | Used to enable enterprise load balancing. | FALSE | TRUE |
| elb.mode | Sets the load balancing policy. | client-ip | host |
| encryptHeaders | Sets whether or not Connector encrypts headers added to a request. Do not change this setting unless explicitly instructed to do so by a support engineer. | TRUE | FALSE |
| encryptionVersion | Sets the headed encoding: 0 - hex, 1 - base-64 encoded and gzipped (smallest but increases CPU load), or 2 - base-64 (larger than 1 but faster) | 2 | 0 |
| groupInclude | Comma separated list of groups to be sent to Cloud Web Security. All other groups (which are not relevant to Web filtering) are excluded. Note the double \ and /. The domain and group only are case insensitive. Wildcards are supported. | all groups | WinNT://<domain>\\<group><br><br>WinNT://<domain*>\\<group*> |
| groupslookup.recursive.depth | The depth for nested groups. A setting of 1 switches off support for nested groups. | 1 | <number> |
| groupslookup.recursive.exclude | A comma separated list of exception groups which should not be included in nesting. | no groups | WinNT://<domain>\\<group> |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| http.failover.alivePoll | Whether to check if the upstream Cloud Web Security proxy server is available. | FALSE | TRUE |
| http.failover.alivePollDelaySec | Delay in seconds between checks. | 30 | <number> |
| http.failover.aliveRepeatsToWhiteList | Number of successful requests before removal from the blacklist. | 1 | <number> |
| http.failover.failPollDelaySec | How often in seconds to poll blacklisted proxy servers. | 3 | <number> |
| http.failover.failRepeatsToBlacklist | Number of failures before adding to blacklist. | 5 | <number> |
| http.failover.numberOfRetriesForResource | Number of retries to count as failure. | 2 | <number> |
| httpAddress | Interface to bind to for HTTP. In workgroup mode, limits Connector to a single interface for use with multi-homed servers. | accept connections on any interface | <IP address> |
| httpPort | The port which Connector listens to for HTTP traffic. | 8080 | <port> |
| icap.generate.random.istag | Enables Connector to respond with random ISTags required by some gateways. | FALSE | TRUE |
| icapAddress | Interface to bind to for ICAP. In workgroup mode, limits Connector to a single interface for use with multi-homed servers. | accept connections on any interface | <IP address> |
| icapPort | The port on which Connector should listen for ICAP traffic. | 1344 | <port> |
| install.mode | Sets workgroup or enterprise mode. | | enterprise.install<br>workgroup.install |
| keepalive.enable | Enabling keep-alive creates persistent connections. This is a requirement for NTLM pass-through. | TRUE | FALSE |
| ldap.accountdisabled.attribute | Where a value is specified, the name of the attribute that flags if the user is allowed to browse. A user with a 'disabled' account in the LDAP server is not allowed to browse, even if the correct user name and password are provided at the basic authentication dialog. | | |
| ldap.base.dn | The base DN in the LDAP tree where the query starts. | | ou=People,dc=<company>,dc=com |
| ldap.connect.timeout | Number of milliseconds before connect time-out. | 5000 | <number> |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| ldap.failover.alivePoll | When set to TRUE, the LDAP Resource Manager polls resources to determine if they are available. | FALSE | TRUE |
| ldap.failover.alivePollDelay | The delay in seconds between polling available LDAP resources. | 30 | number |
| ldap.failover.aliveRepeatsToWhitelist | The number of successful repeat attempts to connect to an LDAP server with its status set to unavailable before its status is changed to available. | 1 | <number> |
| ldap.failover.failPollDelay | The delay between attempts to connect to LDAP servers that have had their status changed to unavailable. | 3 | <number> |
| ldap.failover.failRepeatsToBlacklist | Number of failures before the LDAP server's status is changed to unavailable. | 5 | <number> |
| ldap.failover.numberOfRetriesForResource | Number of retries to count as failure. Applied to both the primary and secondary LDAP server. | 2 | <number> |
| ldap.group.attr | The name of the group attribute in the LDAP server configuration. | ou | |
| ldap.group.attr.string.parse | The name of the attribute for parsing out the group name from an LDAP query response. For example, if the response to the group query is ou=mygroup, o=mycompany, l=location then by setting the ldap.group.attr.string.parse to ou you would derive the group name mygroup. | | |
| ldap.read.timeout | Number of milliseconds before read time-out. | 5000 | <number> |
| ldap.type | Type of LDAP in use, either Active Directory or generic. | ad | generic |
| ldap.user.attr | The name of the user attribute in the LDAP server configuration. | uid | |
| ldapRefreshTimeout | The amount of time in milliseconds that Connector should remember a user's group details before querying the LDAP/Active Directory server again. This can greatly reduce the number of requests made via LDAP and increase the speed at which Connector services requests. | 3600000 | <number> |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| licence | Company, Group or User authentication key generated in the portal and used to identify computers where the egress IP has a dynamically assigned IP address. | | <authentication key> |
| local.response.html.file | HTTP error 503 page. | etc/localresponse.html | <relative path from location of agent.properties file> |
| lowercase.user | Make user names lowercase. | FALSE | TRUE |
| ntlm.authenticate | Enables validation of credentials provided by the user's Web browser. | FALSE | TRUE |
| ntlm.dc.primary | Address of the primary Windows Domain Controller. This must be specified if ntlm.authenticate or ntlm.lookup.groups are set to true. | | <IP address or host name> |
| ntlm.dc.secondary | Address of the secondary Windows Domain Controller. | | <IP address or host name> |
| ntlm.dc.tertiary | Address of the tertiary Windows Domain Controller. | | <IP address or host name> |
| ntlm.icap.auth.password | The password that Connector uses when authenticating with an Active Directory/NT4 domain. Used only in ICAP mode. | | <password> |
| ntlm.icap.auth.user | The user name Connector uses to identify itself to an Active Directory/NT4 domain. Used only in ICAP mode. Note the double \ and /. The domain and group only are case insensitive. | | WinNT://<domain>\\<user name> |
| ntlm.lookup.groups | Enables group lookups via NTLM using the Domain Controller. Overrides the LDAP.lookup.groups setting when TRUE. | FALSE | TRUE |
| ntlm.preauth.domain | The domain controller used for SMB signing. The ntlm.preauth settings are required when using Windows Server 2003 or later. | | |
| ntlm.preauth.username | The user name of a normal user of the domain controller. | | |
| ntlm.preauth.password | The password of the user of the domain controller. | | |
| ntlm.timeout | Number of milliseconds before time-out while waiting for a server response. | 10000 | <number> |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| ntlmIpExceptions | Comma separated list of IP addresses (not hostnames) of computers you wish to exclude from NTLM authentication requests. Supports Classless Inter-Domain Routing (CIDR) notation. | | <IP address> |
| onErrorLdapRefreshTimeout | This property is similar to the ldapRefreshTimeout property except that it is used when the LDAP/Active Directory server is unavailable. The length of time specified by this property is relatively short so that the group details for each user will be updated soon after a previously unavailable server comes back online. | 300000 milliseconds | <number> |
| pool.max.size | Maximum number of threads. | 1500 (on Linux you should change this value to 3000) | <number> |
| pool.prestart.corethreads | Create threads on startup. | TRUE | FALSE |
| pool.queue.size | Maximum number of HTTP requests stored in the input queue. | 50 | <number> |
| pool.start.size | Minimum number of threads created on startup. | 250 | <number> |
| primaryProxy | The primary Cloud Web Security proxy included in your provisioning email. | | <IP address or host name> |
| primaryProxyPort | The primary Cloud Web Security proxy port included in your provisioning email. | | <port> |
| primaryProxyType | Sets whether SSL tunneling is enabled for the primary proxy. | PLAIN | SSL |
| providerUrl[.primary] | The primary LDAP/Active Directory server queried by Connector. The .primary part of the property is optional. | | ldap://<IPaddress or host name>:3268 |
| providerUrl.secondary | The secondary LDAP/Active Directory server queried by Connector. | | ldap://<IP address or host name>:3268 |
| publicKeyFile | The location of the public key used to encrypt headers. Do not change this setting unless explicitlyinstructed to do so by a support engineer. | etc/publicKey.txt | <relative path from location of agent.properties file> |
| read.timeout.downstream | Number of milliseconds before downstream read time-out. | 10000 | <number> |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| read.timeout.upstream | Number of milliseconds before upstream read time-out. | 182000 | <number> |
| secondaryProxy | The secondary Cloud Web Security proxy included in your provisioning email. | | <IP address or host name> |
| secondaryProxyPort | The secondary Cloud Web Security proxy port included in your provisioning email. | | <port> |
| secondaryProxyType | Sets whether SSL tunneling is enabled for the secondary proxy. | PLAIN | SSL |
| securityAuthentication[.primary] | LDAP security strength. The .primary part of the property is optional. | none | simplestrong |
| securityAuthentication.secondary | LDAP security strength. | none | simplestrong |
| securityCredentials[.primary] | The password for the primary account Connector uses when authenticating with an LDAP/Active Directory server. The .primary part of the property is optional. | | <password> |
| securityCredentials.secondary | The password for the secondary account Connector uses when authenticating with an LDAP/Active Directory server. | | <password> |
| securityPrincipal[.primary] | The primary user name Connector uses to identify itself to an LDAP/Active Directory server. The .primary part of the property is optional. | | cc=<user name>, cn=users, dc=<company>,dc=com |
| securityPrincipal.secondary | The secondary user name Connector uses to identify itself to an LDAP/Active Directory server. | | cc=<user name>, cn=users, dc=<company>,dc=com |
| skip.wmp.authentication | Skip NTLM authentication for Windows Media Player. | FALSE | TRUE |
| sslTunnelTimeout | The number of milliseconds for which Connector should keep SSL tunnel requests open. | 60000 | <number> |
| system.telemetry | Comma-separated list of system properties to include in the XSD header when upload.stas is TRUE. | os.name, os.version | <system property>[, <system property>] |
| tertiaryProxy | The tertiary Cloud Web Security proxy included in your provisioning email. | | <IP address or host name> |
| tertiaryProxyPort | The tertiary Cloud Web Security proxy port included in your provisioning email. | | <port> |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| tertiaryProxyType | Sets whether SSL tunneling is enabled for the tertiary proxy. | PLAIN | SSL |
| upload.stats | Whether to send statistics (connection time, total connections, running time, thread count, OS name, and OS version) to Cloud Web Security. | TRUE | FALSE |
| upstream.connect.timeout | Number of milliseconds before upstream connection time-out. | 3000 | <number> |
| useBasic | Whether or not to use basic authentication. | FALSE | TRUE |
| useHttp | Tells Connector whether or not to run in workgroup mode. It enables Connector to act as a simple Web proxy server, listening to all user web requests. If set to true, useIcap must be set to false. | FALSE | TRUE |
| useIcap | Whether or not to listen for Web requests using ICAP. Used with ISA Server and ICAP compatible gateways. If set to true, useHttp must be set to false. | FALSE | TRUE |
| useISA2000 | Specifies if ISA 2000 Server is in use. | FALSE | TRUE |
| useISA2004 | Specifies if ISA Server 2004/2006 is in use. | FALSE | TRUE |
| useLdap | Whether or not Connector should use LDAP to query Active Directory for the groups of which the user is a member. | FALSE | TRUE |
| UseLdapResourceManager | The LDAP Resource Manager, handles failovers from the primary LDAP server to the secondary LDAP server. You must not modify this value unless instructed to do so by customer support. | TRUE | FALSE |
| useNtlm | Enables Connector to collect users' internal IP addresses and user names using the NTLM authentication protocol. In most cases this authentication is transparent to the user. | FALSE | TRUE |

| Setting | Description | Default | Alternate |
|---|---|---|---|
| user.agent.skip.authentication | Enable user agent string matching. | FALSE | TRUE |
| user.agent.skip.authentication.regexp | When user.agent.skip.authentication is TRUE, skip authentication for user agent strings matching a regular expression, for example ( Chrome \| Safari 1\\.\\d). Note, if this is left blank when user.agent.skip.authentication is TRUE authentication will be effectively switched off for all sites. | | <regular expression> |