Smart Connect Release Notes

Smart Connect v1.4 release notes

The v1.4 release of the Smart Connect agent for Web Security addresses a number of reported issues and incremental functionality requests.

Table 1-1 What's new in the v1.4 Smart Connect agent

Feature	Description
CSP replacement feature	For customers with a 100% Smart Connect agent deployment throughout their organization. The CSP Replacement feature sends user authentication details to the Web Security infrastructure when that user is connected to the corporate LAN. This feature delivers a change to the `agentconfigure.xml`. The default value is now set at `YES <enable_onlan_saucer>`.
Support for primary CSP	You can now nominate a primary upstream proxy for the agent to connect to the infrastructure while the user is on the corporate LAN. The previous `upstream_proxy` configuration setting had two properties: `address` and `port`. A new `isprimary` property is added in this release. The value for `isprimary` can be set to `true` or `false`. If an `upstream_proxy` is defined as primary, it is set at a higher priority than the non-primary `upstream_proxies` that have the same scores.
Start up speed of Smart Connect agent	Previously, the Smart Connect agent tested all available routes and picked the most responsive. The agent now sets a timeout when it selects the route. The default timeout is 20 seconds. You can configure this setting in `agentconfigure.xml`. For example: `<chooseproxy_timeout>10</chooseproxy_timeout>` sets the timeout to 10 seconds. In this example, Smart Connect selects the route within 10 seconds. If there is no response within 10 seconds, the Smart Connect agent checks every 500ms until every possible route returns a timeout (after 1 minute) or a response is received.
Limit on log file size	Smart Connect v1.4 addresses an issue where Squid log files can be set to on without limitation under certain circumstances. This fix comprises two changes: • The agent sets the default log level to `INFO` from `WARN` • The agent renames `agent.log` to `agent.log.bak` whenever the file size is more than 10M. Then the agent starts a new log file.
Header files can contain spaces	The Smart Connect parser now supports header names that contain spaces.
Rebranding	This version removes references to the *MessageLabs* brand name.

For further information on Smart Connect, see Help on Web Roaming.

Smart Connect v1.3 release notes

The v1.3 release of the Smart Connect agent for Web Security addresses a number of reported issues and incremental functionality requests.

Not all customers need to upgrade to Smart Connect v1.3. While we recommend that you deploy the latest version of the Smart Connect agent, if you use a previous version you are entitled to support. However, if you experience any issues that can be resolved by moving to v1.3, we request that you upgrade to the latest version.

If you are provisioned with the Web Security Smart Connect roaming service, you can download Smart Connect v1.3 from the portal. You must uninstall the previous version of the Smart Connect agent and install the new version.

Table 1-2 What's new in the v1.3 Smart Connect agent

Feature	Description
Improved compatibility with third-party endpoint security products	The Smart Connect agent can now identify a user (domain\username) who is logged in using an alternative method that obscures their user name. For example, the user name can be obscured by a third-party endpoint product. Some products (such as Trend Micro's OfficeScan) appear under a system account instead of providing the end-user information. In previous versions, the lack of availability of end-user information prevented the Smart Connect user from authenticating properly. A configuration option in the Smart Connect agent now lets you gather the information from an alternative source. A description of the new `user_session_override` parameter is described in the table: New configuration parameters
More consistent performance when you connect from various corporate LAN locations	When the user is on the corporate LAN (`onLAN` status), multiple proxy entries may be listed in the agent configuration file. In this case, the Smart Connect v1.3 agent selects the upstream proxy that provides the best performance response.
Better Web site compatibility	Smart Connect v1.3 addresses compatibility issues with some Web sites that had previously resulted in agent crashes.
Diagnostics for non-standard port configurations	Smart Connect v1.3 fixes a defect whereby diagnostic pages were not loaded properly if the configured port number was something other than 80.

Not all customers need to upgrade to Smart Connect v1.3. While we recommend that you deploy the latest version of the Smart Connect agent, if you use a previous version you are entitled to support. However, if you experience any issues that can be resolved by moving to v1.3, we request that you upgrade to the latest version.

If you are provisioned with the Web Security Smart Connect roaming service, you can download Smart Connect v1.3 from the portal. You must uninstall the previous version of the Smart Connect agent and install the new version.

Table 1-3 **New configuration parameters**

Parameter	Default	Values	Description
`user_session_override`	`No`	`Yes` or `No`	By default, the Smart Connect agent determines the user ID by capturing the `user-id` of the process that initiates connections to the agent. In some cases, the user ID is reported as `NT AUTHORITY\SYSTEM` instead of the ID of the end user. For example, this situation may occur when you use a third-party antivirus product and the antivirus product intercepts the connections. Setting the`user_session_override` parameter to "TRUE" forces the Smart Connect agent to use the logged-on user's name instead of the default method. Use this parameter if you see `NT AUTHORITY\SYSTEM` user IDs in your reports.

For further information on Smart Connect, see Help on Web Roaming.

Upgrading Smart Connect

Not all customers need to upgrade to Smart Connect v1.4. While we recommend that you deploy the latest version of the Smart Connect agent, if you use a previous version you are entitled to support. However, if you experience any issues that can be resolved by moving to v1.4, we request that you upgrade to the latest version.

If you are provisioned with the Web Security Smart Connect roaming service, you can download Smart Connect v1.4 from the portal. You must uninstall the previous version of the Smart Connect agent and install the new version.

For further information on Smart Connect, see Help on Web Roaming.