

TROUBLESHOOTING

Guide

Common Troubleshooting Issues in Spy Sweeper Enterprise

- **Firewall Configurations:**
 - Spy Sweeper requires TCP ports 50001-50003 be opened for normal communications between client and server. The Server requires port 50000 be opened to receive communications from the client. Additionally, if you are running your communication in SSL mode 50020-50023 must be opened for communications.

- **Client Deployment:** (if a customer is having issues while using the client deployment feature in their environment)
 - Occasionally it is necessary to credential the Admin Console service to ensure that the deployment feature is allowed to function within a more secured network. To accomplish this simply set the Webroot admin console service to log on as a domain administrator for the duration of the deployment.

 - File and Print Sharing must be not only enabled but allowed in windows firewall for the client deployment component to function correctly.

 - Netbios must be enabled within the customer's network for the client deployment function to see all workstations within an environment. Additionally, if the network passes across a switch or router that does not support netbios hops, the client deployment component will not see any machines on the other side of that switch or router.

- **Client Update issues:**
 - Often customers will report that their clients are not receiving updates. This can often be due to an assumption on their part that updates will be automatically assigned "out of the box". To resolve this check within *Manage Desktop Applications* → *Spy Sweeper* → *Update Spy Sweeper* and ensure that they have the correct settings placed in Manual and Automatic Install.
 - Ports being blocked or another application is running on Webroot ports. This is usually a firewall related issue, but occasionally customers are running an application that uses one of the Webroot ports.

- **Client polling issues:**
 - Clients require a non-specified and randomized interval to check in after installation. During this time customers can become impatient and inquire why the client has not shown in Client Management. This is best addressed PRE-Deployment with a quick explanation of the client behavior. Should it be necessary to force a client to immediately check in you can add an entry to the client registry under *HKLM\SOFTWARE\Webroot\Enterprise\Commagent*. Add a DWORD value of 'fp' (without quotes) and set its value to hexadecimal 2. Then cycle the Webroot commagent service to force the client to immediately poll into the server.

- **Proxy Servers and Microsoft ISA:**
 - It is essential that a customer be informed that we pass http traffic through TCP ports and any internal monitoring of traffic within a network by a proxy server will intercept this communication unless those ports are excluded.
 - Microsoft ISA server will occasionally intercept traffic between the Webroot update servers and the admin console, effectively breaking the update process. The ISA server must be fully patched and configured to ignore traffic coming from the admin console on port 443 to allow successful communications.

- **Common Conflicts:**
 - There is a known and well documented conflict between Spy Sweeper Enterprise and McAfee 8.0i. McAfee has identified this as an issue in their software conflicting with multiple vendors and is issuing a patch to resolve this. Currently, McAfee support will release the beta version of this patch to Webroot customers on request.
 - Symantec ver. 10 with the anti-spyware components enabled occasionally conflicts with Spy Sweeper Enterprise. Again this is quickly resolved by adding exclusions for the Webroot folders on both the clients and server.