

## Safe Access upgrade provides the ability to test and control Vista endpoints

### Description

---

After upgrade, Vista endpoints are testable and will no longer be controlled by the NAC policy preference regarding unsupported OSs.

If NAC policies have been configured to allow access for unsupported OSs, Some Vista endpoints that were previously allowed may now be testable and potentially fail testing, preventing access.

If NAC policies have been configured to deny access for unsupported OSs, Some Vista endpoints that were previously denied access may now be testable and potentially pass testing, granting access.

### Affected Products, Versions

---

This condition exists in the following software versions:

Safe Access: 5.0-4181, 5.0-4391

### Impact

---

Vista endpoints may fail testing and be quarantined, where previously they were allowed access within the NAC policy as an unsupported OS.

Vista endpoints may pass testing and be granted access, where previously they were quarantined within the NAC policy as an unsupported OS.

### Solution

---

After the upgrade manually test Vista endpoints to verify their compliance status.

### Step by Step

---

1. For each Vista endpoint on the network connect with a web browser to manually test.

Open a web browser and visit **https://<SafeAccess>:89** where <SafeAccess> is the IP or DNS name of the Safe Access Management Server (MS).

2. Complete testing

Follow the directions in the web browser to test the endpoint

3. Remediate identified issues

Follow the directions for failed tests or correct using your organizations best practices.

4. Retest the endpoint

After remediation, retest the endpoint to verify the situation has been corrected

5. Repeat for other Vista endpoints

Repeat the test for at least a representative sample of Vista endpoints to be comfortable with the test results.

Copyright © 2002-2008 StillSecure®. All rights reserved.

StillSecure®, the StillSecure logo, Safe Access®, Strata Guard®, VAM®, Cobia™ and the Cobia logo are trademarks or registered trademarks of StillSecure. Additional StillSecure trademarks or registered marks can be found at <http://www.stillsecure.com/company/copyright.php>. All other brands, company names, product names, trademarks or service marks referenced in this material are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by StillSecure.

StillSecure's trademarks, registered trademarks or trade dress may not be used in connection with any product or service that is not the property of StillSecure, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits StillSecure. The products and services described in this material may not be available in all regions.

This StillSecure® software product includes open-source software components. StillSecure conforms to the terms and conditions that govern the use of the open source components included in this product. Users of this product have the right to access the open source code and view all applicable terms and conditions governing open source component usage. Visit <http://www.stillsecure.com/opensource> to access open source code, applicable terms and conditions, and related information.