



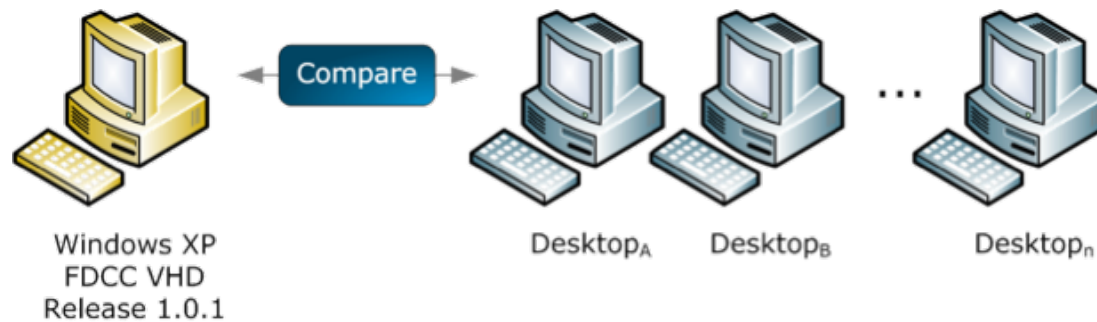
SignaCert

## Proving FDCC Compliance

Using SignaCert Verify to Assess Desktop State

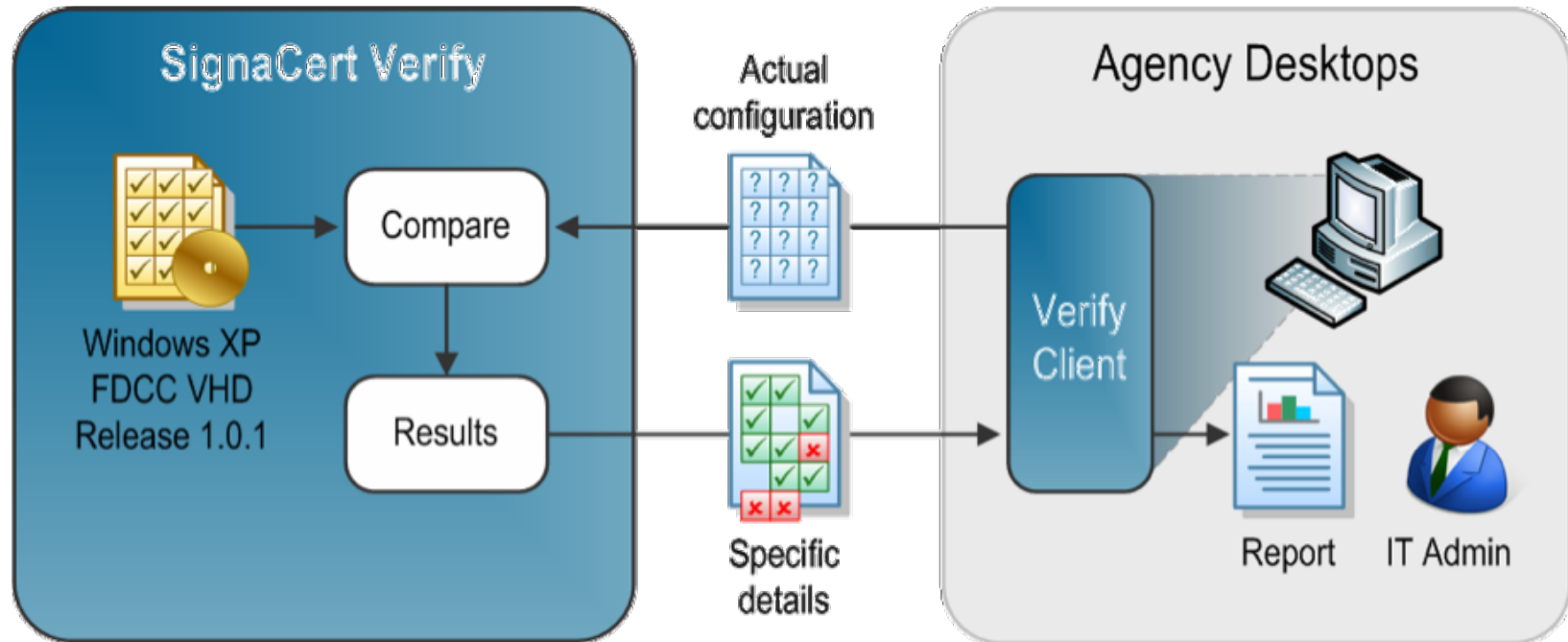
December 2007

Compare agency desktops with published FDCC reference



## Benefits:

- Definitively prove devices are in compliance
- Identify which aren't and get details about specific deviations
- Automate a time-consuming and error-prone process
- An independent control process that speeds efforts to achieve compliance



- Summary information
  - Count of files added by product
  - Count of modified and removed files
- Detailed deviations
  - Full path/filename for each deviation
  - Grouped by product

## FDCC Compliance Verification Report

|                        |                                   |
|------------------------|-----------------------------------|
| <b>Device:</b>         | pester.signacert.com              |
| <b>Policy Name:</b>    | Windows XP FDCC VHD Release 1.0.1 |
| <b>Run Time:</b>       | 01-05-2007 12:56:16.734 pm        |
| <b>Compliant Files</b> | 72,987                            |
| <b>Deviations:</b>     | 621                               |

### Deviations Summary

This section describes the types of deviations found grouped by product and indicating the number of items found.

| Product Name                      | Deviation Type | Count |
|-----------------------------------|----------------|-------|
| Yahoo Messenger                   | Added          | 57    |
| Xnobi 0.9                         | Added          | 27    |
| Skype                             | Added          | 157   |
| Windows XP FDCC VHD Release 1.0.1 | Modified       | 4     |
| Windows XP FDCC VHD Release 1.0.1 | Removed        | 52    |

### Detailed Deviations

This section lists each of deviations found grouped by product. The table indicates the type and the path to the specific deviation. indicating the number of items found.

| Yahoo Messenger                 |                |
|---------------------------------|----------------|
| Path\File                       | Deviation Type |
| C:\WINDOWS\system32\%ncsp\$.inf | Added          |
| C:\WINDOWS\system32\%ncsp\$.inf | Added          |



**Results**—Provide details about the state of compliance for a given device. Reports indicate whether a device is an exact match or if and what deviations were found.



**Exact Match**—Desktops that match the FDCC exactly, down to the file level are considered an exact match.



**Modified**—Verify can detect files that have changed, even if they have the same filename, size and path.

**Action: Restore files to original state!**



**Removed**—Because actual findings are compared with a published reference, Verify can detect files that have been removed from a desktop.

**Action: Replace original files!**



**Added**—Files found that aren't specified by the reference are considered added files.

**Action: Remove the added files!**

- Replaces / augments manual auditing process
  - Reduce time spent by as much as 80% [swag-need some more]
- Identifying specific deviations allows rapid remediation
  - Reduce diagnoses (what is non-compliant) by as much as 80% [swag-need some more]
  - Spend more time fixing rather than finding problems
- Identify common sources of non-compliance
  - What applications/processes cause problems
  - Put preventative controls in place for those processes

- **Identify found files**—Typically added files are part of a patch, hotfix, or other intentional adhoc effort. Verify can identify all Microsoft patches related to Windows XP and Vista as well as many commercial applications.
- **Improved control**—Detailed information of what is on desktops allows faster, more accurate remediation
- **Improved availability**—Determine what's at risk before failures occur



Customers requiring verification of tens or even hundreds of desktops require a more scalable solution

1. Customer configures client for broad deployment
  - Proxy settings
  - SNMP, SMTP, and/or write to logs
2. Deployed and trigger client via SMS or other EMS tool
3. Verification request sent to Verify ETS for comparison with the reference
4. Results are returned to the client and results are written per customer configuration