

Safe Access® Lite Technical Note

Introduction

Safe Access® Lite is a free version of StillSecure's Safe Access, the industry's #1 award-winning Network Access Control (NAC) solution. StillSecure® is offering this solution to the community free of charge in order to:

- Decrease the NAC implementation learning curve and help plan for a successful roll-out
- Realize immediate benefits from NAC without the complications associated with most implementations
- Provide an immediate view into an organization's security posture, device health status, and endpoint policy compliance
- Allow organizations to experiment with NAC easily and cost-effectively without network disruption

StillSecure is offering this solution free of charge and with community forum-based support similar to the following StillSecure solutions:

- Strata Guard® Free
<http://sgfree.stillsecure.com>
- Cobia™
<http://cobia.stillsecure.com>

Please note that there are some differences between Safe Access® Lite and the commercially-supported version. These differences have been detailed in the [Table 1 on page 2](#). StillSecure is hopeful that you will find significant value in Safe Access® Lite and we look forward to interacting with you on the forums.

For further details on Safe Access® Lite please go to:

<http://salite.stillsecure.com>

For further details on the commercial version of Safe Access v5.0 please go to:

<http://www.stillsecure.com/safeaccess>

If you are interested in upgrading from the free version to a commercially supported version, please contact StillSecure at sales@stillsecure.com or 303-381-3830.

We are interested in your feedback! Send us email at:

salite@stillsecure.com

Features

The following table compares the feature differences between Safe Access® Lite and Safe Access:

Table 1: Safe Access® Lite versus Safe Access

| Features | Safe Access® Lite | Safe Access v5.0 |
|--|---|---|
| License | 250 endpoints supported | Hundreds of thousands of endpoints supported |
| Enforcement options | No enforcement. Monitoring only (passive mode). | <ul style="list-style-type: none"> • 802.1X • DHCP • Inline • Specification of: <ul style="list-style-type: none"> – Accessible Services – Devices and Domains for Always Allow Access – Devices and Domains for Always Deny Access |
| High availability | No | Yes |
| Load balancing | No | Yes |
| Multiple server installation | One enforcement server (ES) | Multiple ESs supported |
| Test updates | Yes | Yes |
| Maintenance | Backup from the user interface (UI) Restore from the UI Generate support packages from the UI | Backup from the UI Restore from the UI Generate support packages from the UI |
| Endpoint testing options | Agent-based ActiveX Agentless | Agent-based ActiveX Agentless |
| Configurable end-user screens | Yes | Yes |
| Ability to specify windows credentials | Yes | Yes |
| Ability to specify logging levels | Yes | Yes |
| Ability to specify timeout periods | Yes | Yes |
| Endpoint options | View endpoint activity View test results Search for specific endpoints | View endpoint activity View test results Search for specific endpoints Take action on endpoints |
| Email notification of test alerts | Yes | Yes |

Table 1: Safe Access® Lite versus Safe Access

| Features | Safe Access® Lite | Safe Access v5.0 |
|--------------------------------|---|--|
| Create and edit NAC policies | Ability to specify unsupported operating systems Supports retest frequency Allows assignment of endpoints to clusters Supports selection of tests per NAC policy | Ability to specify unsupported operating systems Supports retest frequency Allows assignment of endpoints to clusters Supports selection of tests per NAC policy Allows specification of test failure actions. Supports specifying inactivity timeout |
| View cluster status | Yes | Yes |
| View enforcement server status | Yes | Yes |
| Generate reports | Yes | Yes |

Installation

Safe Access® Lite is delivered as a 1 GB zip file and can be opened with VMware® player requiring 10 GB of free disk space. System requirements and installation details can be found in the *Implementation Guide* located at:

<http://salite.stillsecure.com>

NOTE

Please ensure that before you power on your virtual machine for Safe Access® Lite that the virtual machine has been allocated at least 512 MB of memory.

The following default values are used:

- Hostname – localhost.localdomain
- Timezone – US/New-York
- Root password – safeaccess

Monitor (Passive) Mode

Safe Access® Lite is designed to monitor anything that attempts to connect to your network. The industry-standard term for *monitor mode* is *passive mode*. So, whenever you are reading this document (or other NAC documents), just remember that references to passive mode means monitor only.

TIP

Computers and devices (but not switches or routers) are referred to as endpoints in this document.

Passive mode is an alternative to the quarantine or enforcement methods available in the commercial version of Safe Access. Passive mode uses Ethernet device eth0 for monitoring endpoint traffic on the local subnet. It is designed to test endpoints but does no actual quarantining. Because no quarantine methods are enabled in Safe Access® Lite there is no risk of accidentally quarantining endpoints while gathering compliance baseline data. The following diagrams show the two deployment options for Safe Access® Lite.

Figure 1: Option 1, Passive Mode, Simple DHCP

Safe Access in Passive Mode listens to broadcast traffic from devices on a network segment and tests them using domain credentials silently. End-users are not aware that they are being tested and are unable to be quarantined.

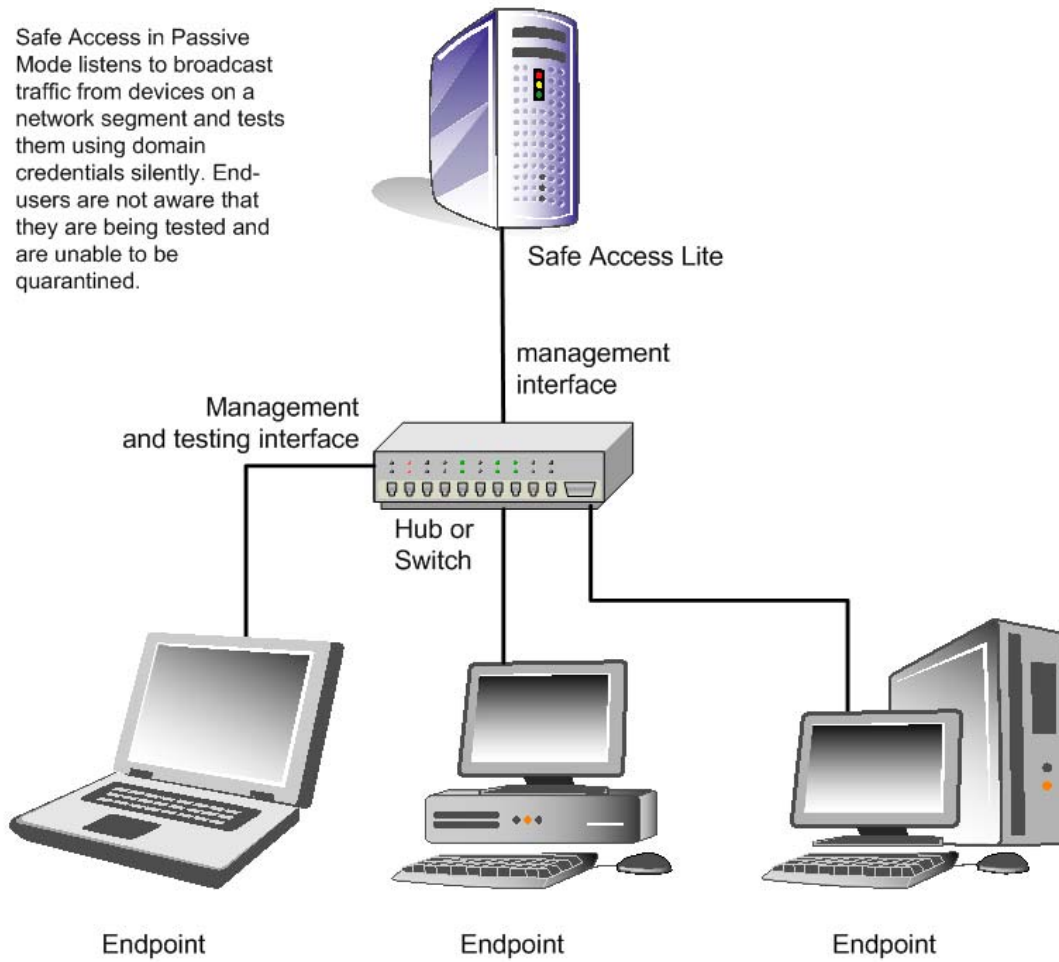
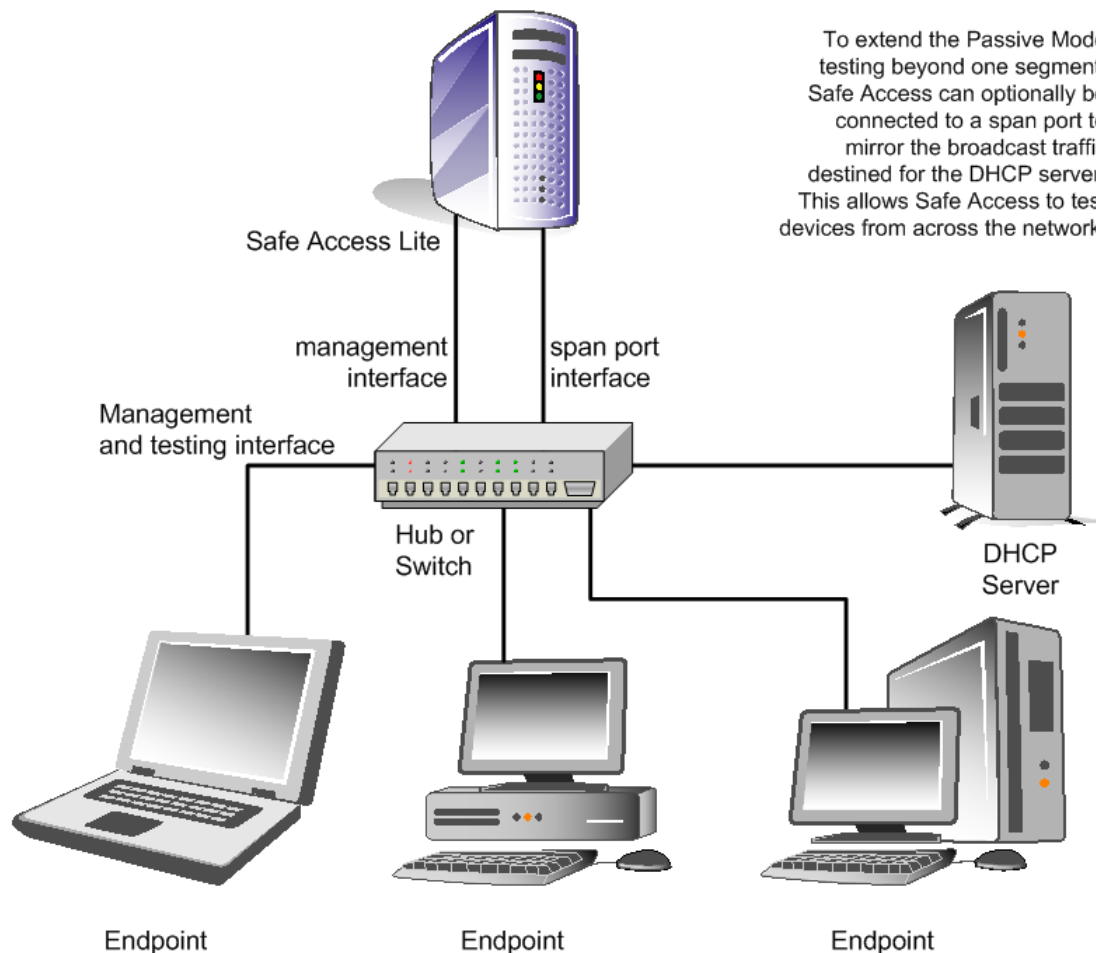


Figure 2: Option 2, Passive Mode, Using Span Port for DHCP




User Interface

The Safe Access® Lite user interface is the same user interface as in the commercial version with the following exceptions:

- All endpoints monitored in passive mode show as **Granted Access**
- Differences in the user interface are described in the following sections:
 - “Endpoint Activity” on page 6
 - “NAC Policies Basic Settings” on page 7
 - “NAC Policies Tests” on page 8
 - “Cluster Access Mode” on page 9
 - “Quarantine Method” on page 10

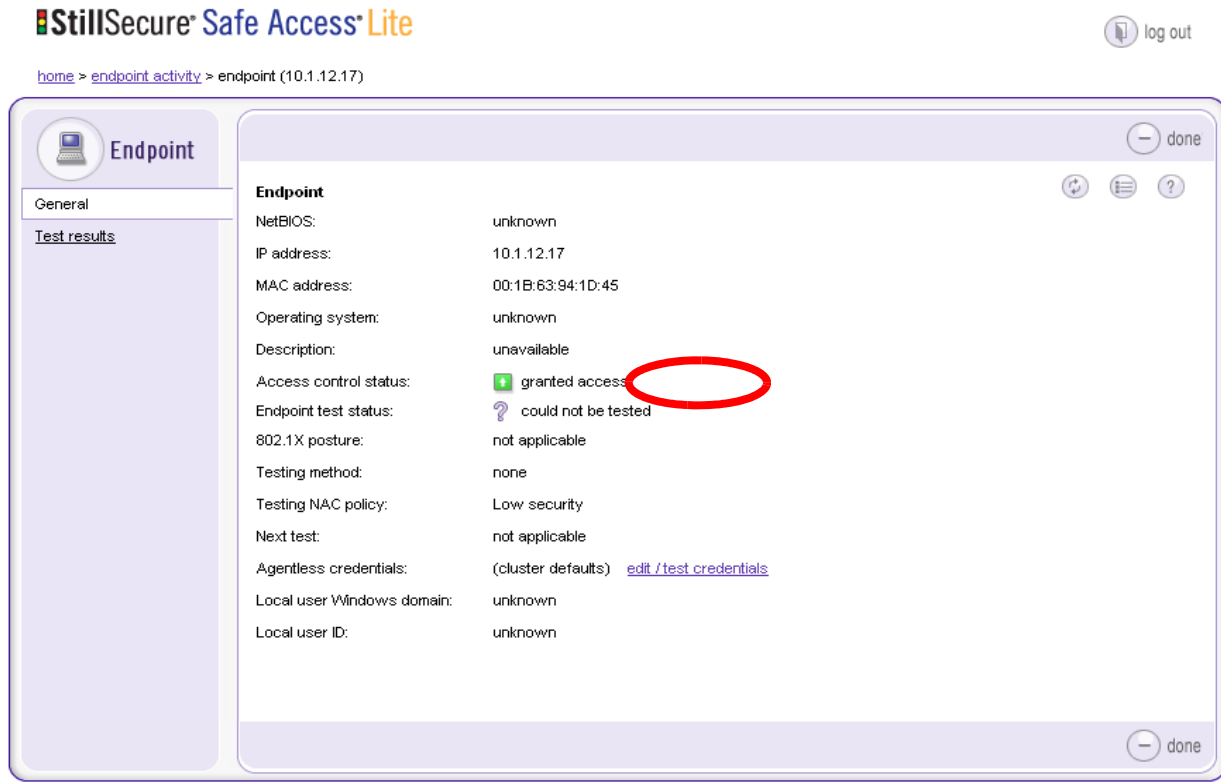
Endpoint Activity

To view the Endpoint activity window:

 Home >> Endpoint activity

Click on a **netbios** name. The **Endpoint** window appears.

Figure 3: Endpoint, General Window




Copyright © 2002-2007 StillSecure®. All rights reserved. 5.0-80006.

The Safe Access® Lite **Endpoint** window does not have the **change access** option next to the **Access control status**.

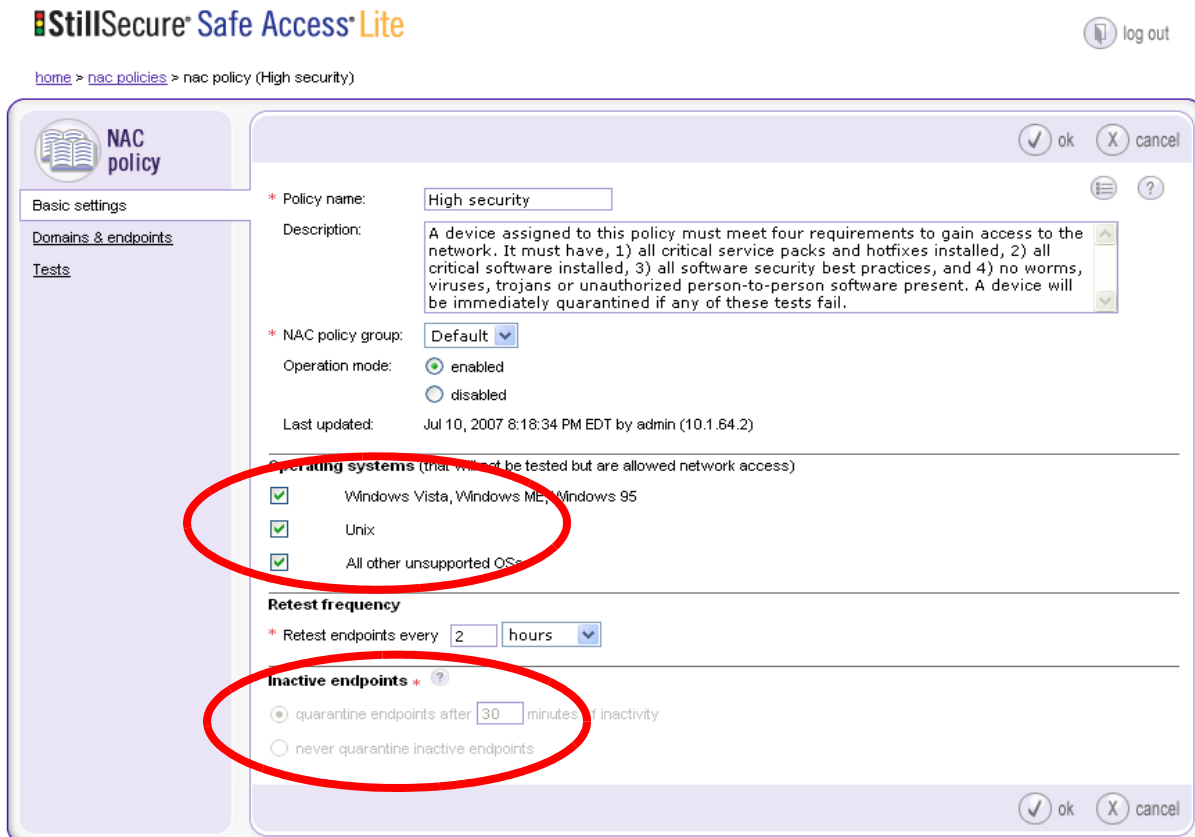
NAC Policies Basic Settings

To view the NAC policy window:

 Home >> NAC policy

Click on a NAC policy. The **NAC policy** window appears.

Figure 4: NAC Policy, Basic Settings Window



Copyright © 2002-2007 StillSecure®. All rights reserved. 5.0-60006.

The Safe Access® Lite **NAC policy** window has the following differences:

- All **Operating systems** are checked as not tested but allowed network access.
- The **Inactive endpoints** options are disabled

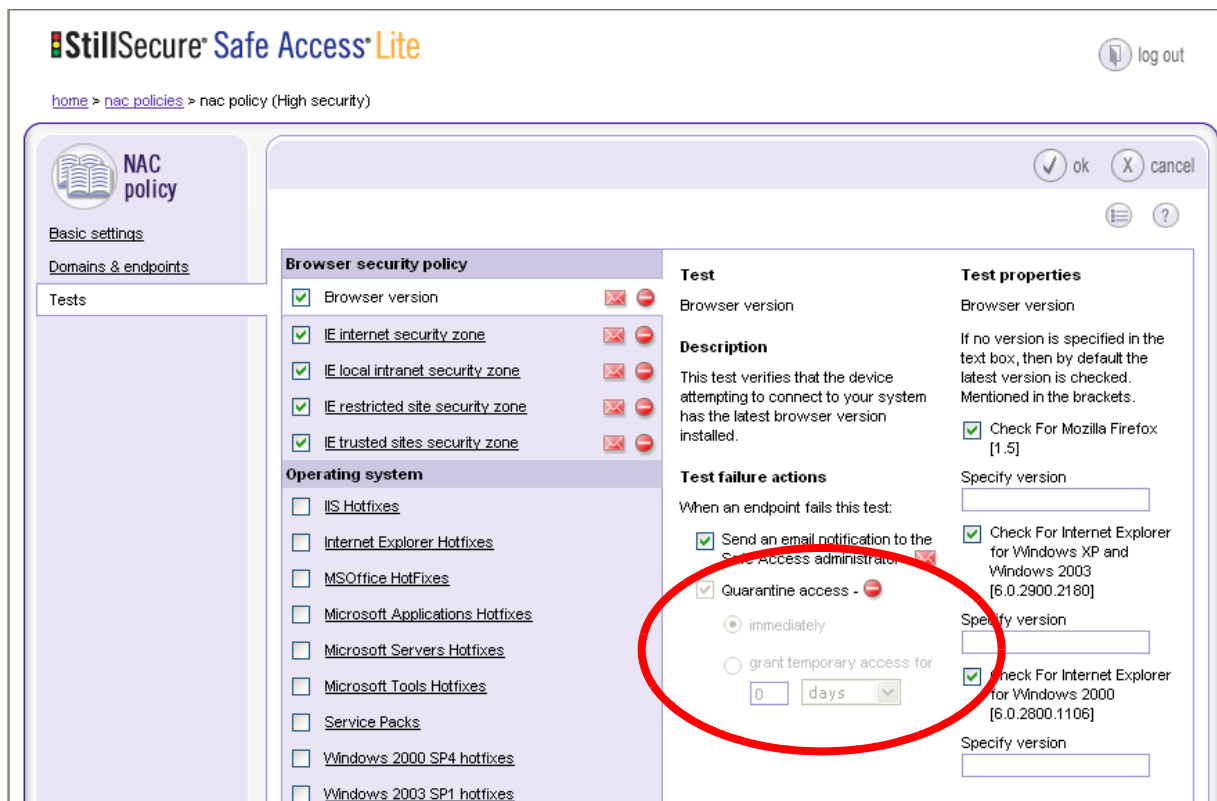
NAC Policies Tests

To view the NAC policy window:

Home >> NAC policy

- 1 Click on a **NAC policy**. The **NAC policy** window appears.
- 2 Select the **Tests** menu option.

Figure 5: NAC Policy, Tests Window



The Safe Access® Lite window shows the **Quarantine access** options are disabled (grayed out).

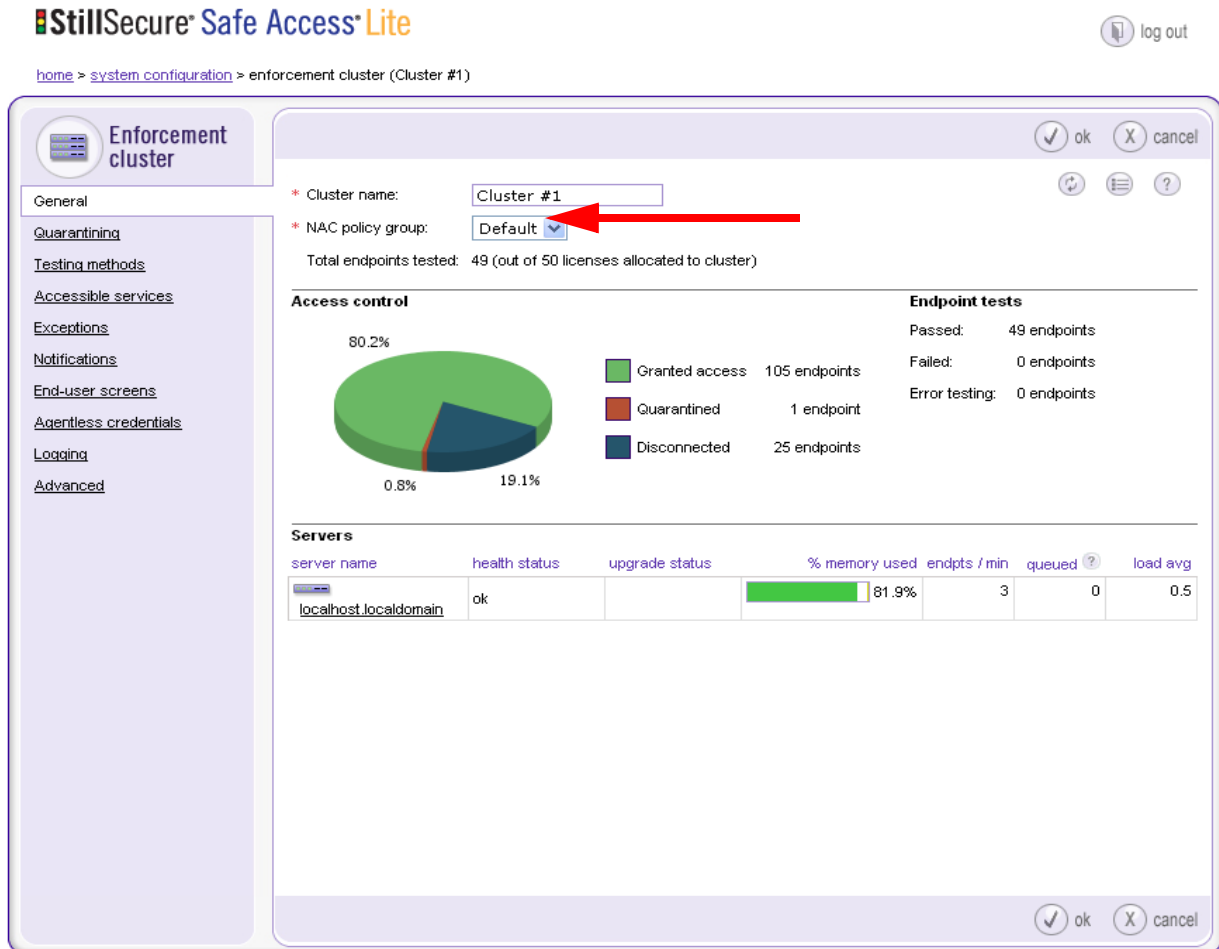
Cluster Access Mode

To view the Enforcement cluster window:

 Home >> System configuration

Click on an Enforcement cluster. The Enforcement cluster window appears.

Figure 6: Enforcement Cluster, General Window



home > system configuration > enforcement cluster (Cluster #1)

log out

Enforcement cluster

General

* Cluster name: Cluster #1

* NAC policy group: Default

Total endpoints tested: 49 (out of 50 licenses allocated to cluster)

Access control

80.2% 19.1% 0.8%

- Granted access 105 endpoints
- Quarantined 1 endpoint
- Disconnected 25 endpoints

Endpoint tests

Passed: 49 endpoints
Failed: 0 endpoints
Error testing: 0 endpoints

Servers

| server name | health status | upgrade status | % memory used | endpts / min | queued | load avg |
|-----------------------|---------------|----------------|---------------|--------------|--------|----------|
| localhost.localdomain | ok | | 81.9% | 3 | 0 | 0.5 |

Copyright © 2002-2007 StillSecure®. All rights reserved. 5.0-60006.

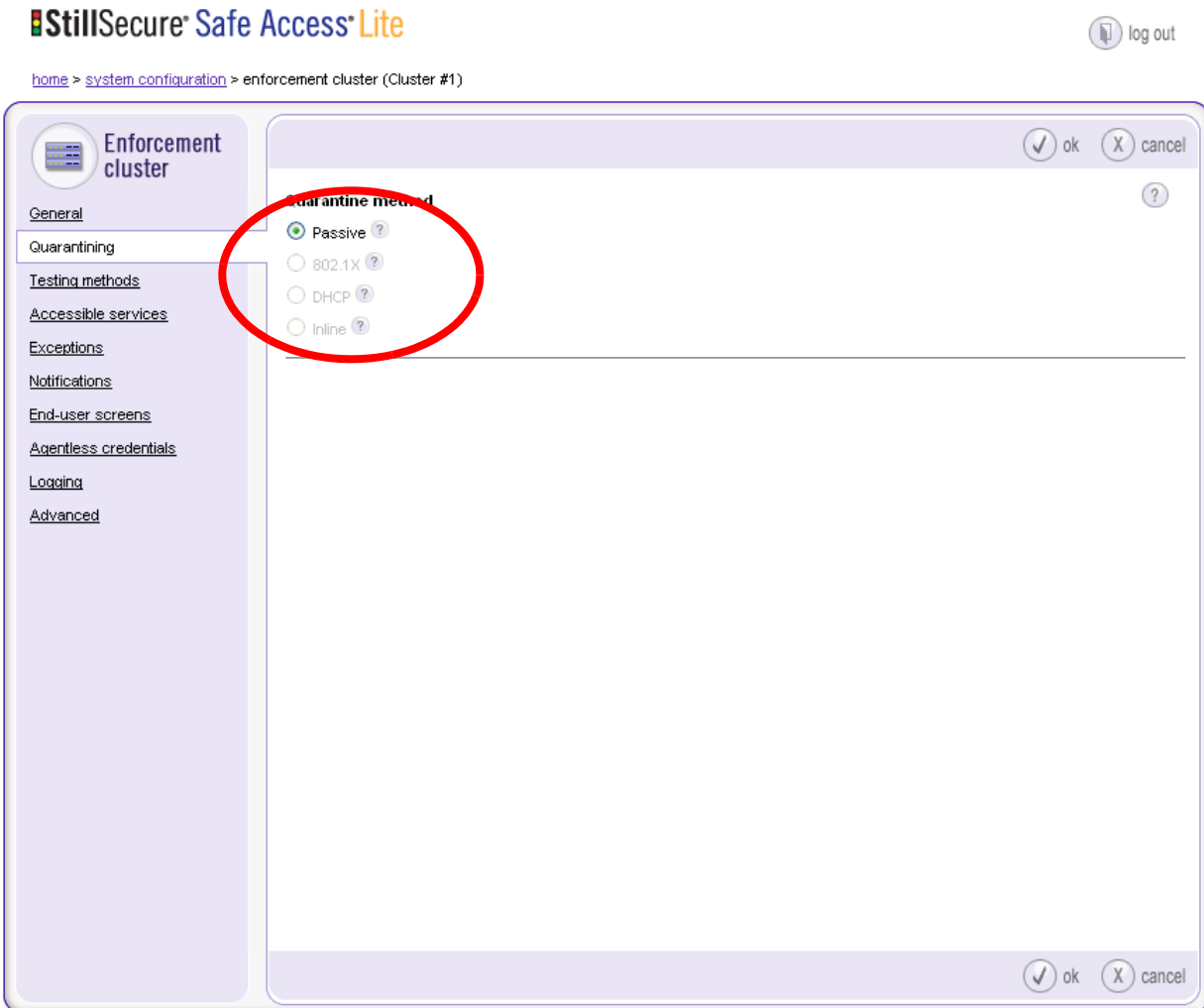
The Safe Access® Lite window shows that there are no access mode radio buttons listed under the cluster name.

Quarantine Method

To view the Quarantining window:

 Home >> System configuration >> Quarantining

Figure 7: System Configuration, Quarantining Window



Copyright © 2002-2007 StillSecure®. All rights reserved. 5.0-60006.

The Safe Access® Lite window has the following differences:

- Passive mode is enabled
- All other modes are disabled (grayed out)