

Microsoft Network Access Protection

Abstract

This document describes the level of support of Microsoft Network Access Protection (NAP) on networks built with Enterasys products.

Microsoft Network Access Protection

Microsoft NAP is a policy enforcement technology built natively into the Windows Vista and Windows Server 2008 operating systems that enables customers to better protect network assets from unhealthy computers by enforcing compliance with network health policies.

Microsoft NAP client is embedded into Windows Vista. Note that the Microsoft NAP client has been enhanced in Windows Vista SP1. The Microsoft NAP client will also be available for Windows XP with the release of Windows XP SP3.

Microsoft NAP server component is part of Microsoft Network Policy Server (NPS), available exclusively on Windows Server 2008. Note that NAP can be deployed in a mixed Windows Server 2003/2008 environment, with NPS services running on Windows Server 2008 and other services like AD, CA, etc running on Windows Server 2003.

Microsoft NAP / Enterasys Security Enabled Infrastructure

Enterasys has been testing Microsoft NAP in conjunction with Enterasys switches (Matrix N-Series and SecureStack) for more than a year, leveraging 802.1X authentication and Policy/VLAN enforcement. Note that Microsoft is also running NAP testing with Enterasys switches (Matrix N-Series NSA switch) in their own lab in Redmond, WA, USA. Enterasys' value added switch features like Multi-User 802.1X Authentication, Dynamic Policy Assignment (role-based networking), Dynamic VLAN Assignment (RFC 3580), VLAN-to-Policy Mapping and related management are greatly facilitating and enhancing Microsoft NAP deployments.

Here's a [press release](#) published on February 7, 2007 when Windows Server 2008 was still in Beta 2 stage (it was called "Windows Server Longhorn" at the time).

The following table lists the hardware platforms which have been explicitly tested to support Microsoft NAP, along with the associated firmware versions.

Hardware Platform	Firmware Version
SecureStack A2	2.01.00
SecureStack B2	4.01.01
SecureStack B3	1.01.01
SecureStack C2	5.01.01
SecureStack C3	1.01.01
Matrix DFE-G	6.01.01
Matrix DFE-P	6.01.01
Matrix DFE-D	6.01.01

Microsoft NAP / Enterasys NAC

Enterasys currently support Microsoft NAP deployments on the top of an Enterasys security-enabled infrastructure running 802.1X authentication. Enterasys NAC (both inline and out-of-band) supports transparently NAP operations in such environments (from a “pre-connect” perspective). Enterasys also provides post-connect assessment for all devices connected on a network, which would “deviate” from standard behavior, leveraging IDP and NBAD technologies.

Enterasys is currently working on further integrating Microsoft NAP and Enterasys NAC (Network Access Control) technologies. Enterasys NAC will be able to leverage Microsoft NAP as a client-based assessment technology, providing further control and visibility of NAP-enabled devices, as well as supporting non NAP-enabled devices by leveraging other assessment technologies. Health status and location of all devices connected to the network will be consolidated in one view and tracked for audit/historization purposes. Identity of such devices as well as users logged onto those devices can also be tracked.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2007 Enterasys Networks, Inc. All rights reserved. Enterasys is a registered trademark. Secure Networks is a trademark of Enterasys Networks. All other products or services referenced herein are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

Microsoft®

