Novell®

ZENworks™
Endpoint Security Management 3.2

Release Notes

June 26, 2007

Contents

Section 1 - Overview

1.1 Document Purpose

The purpose of this document is to detail the new features and known issues for ZENworks Endpoint Security Management (ESM) version 3.2. This document supports **ESM 3.2.461**, and subsequent releases.

1.2 Background

ZENworks Endpoint Security Management 3.2 is the initial release of Endpoint Security Management and is based on Senforce's Endpoint Security Suite 3.2. Compared to the previous release of Endpoint Security Suite, this version increases the product's capabilities in the areas of alerts monitoring, storage device security, communications port control, firewall, and wireless management, as well as improves reporting, management, and general usability.

1.3 Documentation

Product documentation is available in the ZENworks Endpoint Security Management Documentation page: http://www.novell.com/documentation/zesm32/index.html

Available manuals for this release are:

- ZENworks ESM Installation and Quick-Start Guide
- ZENworks ESM Administrator's Manual
- ZENworks Security Client User's Manual

Documentation for ZENworks ESM 3.2 is available in PDF format. To view, use Adobe Acrobat Reader. Acrobat Reader is available free at: http://www.adobe.com/products/acrobat/readstep2.html.

Section 2 - Installation and Licensing

2.1 Installation and Licensing

The ZENworks ESM Installation and Quick-start Guide is included with the ESM documentation. Guidelines for requirements and installation procedures are included.

Licenses are sent separately and should be installed as described in the information sent along with the product license file.

Section 3 - New Features in this Release

3.1 Alerts Monitoring

Alerts monitoring ensures that any attempts to compromise corporate security policies are reported in the Management Console. This allows the ESM Administrator to know of potential problems and take any appropriate remedial actions. The Alerts dashboard is completely configurable, granting total control over when and how frequently alerts are triggered.

Alerts monitoring is available for the following areas:

- **Client Integrity** - notifies of unremediated integrity test results
- **Communication Port Security** - notifies of potential port scan attempts
- **Data Protection** - notifies of files that are copied to removable storage devices within a one day period
- **Security Client Configuration** - notifies of incorrect security client versions and incorrect policies
- **Security Client Tampering** - notifies of user hack attempts, uninstall attempts and usage of the override password
- **Wireless Security** - notifies of unsecure access points, both detected and connected to by the end-user

3.2 Uninstall Password Control

Administrators can enforce uninstall passwords through a policy update. Uninstall passwords can be enabled, updated, or disabled per policy.

3.3 Client Self Defense Control by Policy

Administrators can enable or disable Client Self Defense by policy, by checking or unchecking a box in the main Global Policy settings.

3.4 Antivirus Definition File Checks by Age

Antivirus file exists checks can now be determined by file age, rather than just by file date.