




New possibilities in latest OfficeScan and OfficeScan plug-in architecture

*Märt Erik
AS Stallion*

Agenda



- New in OfficeScan 10.5
 - » More Active Directory support
 - » New automated client grouping option
 - » Multi-tier Client Trees
 - » WRS integrated with Smart Scan servers
 - » Expanded compliance-assessment reporting
 - » Role options for Update Agents
 - » Application filtering for firewall
 - » Exception lists for device control
 - » Highly granular admin-user access settings
 - » Performance & other incremental enhancements
- OfficeScan plug-ins
 - » IDF - Intrusion Defense Firewall
 - » TMAgent Manager
 - » Trend Micro Mobile Security
 - » Trend Micro Security (for Mac)
 - » Trend Micro Virtual Desktop Support

A large blue rectangular area containing the title text. The background of this area is a blurred image of a person's hands using a computer mouse and keyboard. The text "New features and enhancements in OfficeScan 10.5" is centered in white. Faint, repeating "NB" text is visible in the background of the blue area.

New features and enhancements in OfficeScan 10.5

More Active Directory support



- Expanded Active Directory support for multiple forests and trusted domains
- Version 10.0 allows to specify only Active Directory domain where OfficeScan server belongs.
- In OfficeScan 10.5 it is possible to define multiple Active Directory domains



Administration > Active Directory > Active Directory Integration



Active Directory Integration

Active Directory Domains

Add the Active Directory domains OfficeScan will associate with the client tree.

Encrypt Active Directory Credentials

Specify an encryption key and file path to ensure an additional layer of protection for your Active Directory credentials.

Encryption Key:

Full path and file name:

Specify Authentication Credentials

Specify a credential OfficeScan will use to connect to this Active Directory domain controller.

IMPORTANT: Ensure that the domain credential does not expire.

Username:

Password:

New automated client grouping option

- Different than legacy NetBIOS, AD & DNS options
- Rules based on:
 - **Active Directory scope**
 - IP address range
- Rules can be prioritized, activated & deactivated
- Can schedule domain re-sort/re-creation
- If used:
 - Cannot manually add groups on the Client Management Page
 - Cannot move clients with drag and drop
 - Can still delete groups

Networked Computers > Client Grouping



Client Grouping

Client Grouping

Group clients by:

- ☐ NetBIOS domain
- ☐ Active Directory domain
- ☐ DNS domain
- ☒ Custom client groups

Specify or group clients using Active Directory or IP addresses.

Automatic Client Grouping

Add

Delete

Active Directory

IP Address

	Source	Status	Preview
			Name
			Source
			Destination

Add

Delete

Scheduled Domain Creation

☒ Enable scheduled domain creation

Schedule-based Domain Creation

- ☐ Daily
- ☒ Weekly, every Friday Start time: 17 : 00 (hh:mm)
- ☐ Monthly, on day 01

Networked Computers > Client Grouping > Automatic Client Grouping > Add > Active Directory/ IP Address



Add Grouping Rule

☒ Enable this rule

Define Rule

Rule Name:

Active Directory Source:

Select one or multiple sources that represents the specified group in the OfficeScan

- ☒ xsonnkm.local
 - ☐ Computers
 - ☐ Domain Controllers
 - ☐ Microsoft Exchange Securi...
 - ☐ Users
 - ☒ XsnTestLab01

Client Tree:

Specify one OfficeScan Client Tree that will represent the selected Active Directory

☒ Duplicate Active Directory structure into OfficeScan Client Tree.

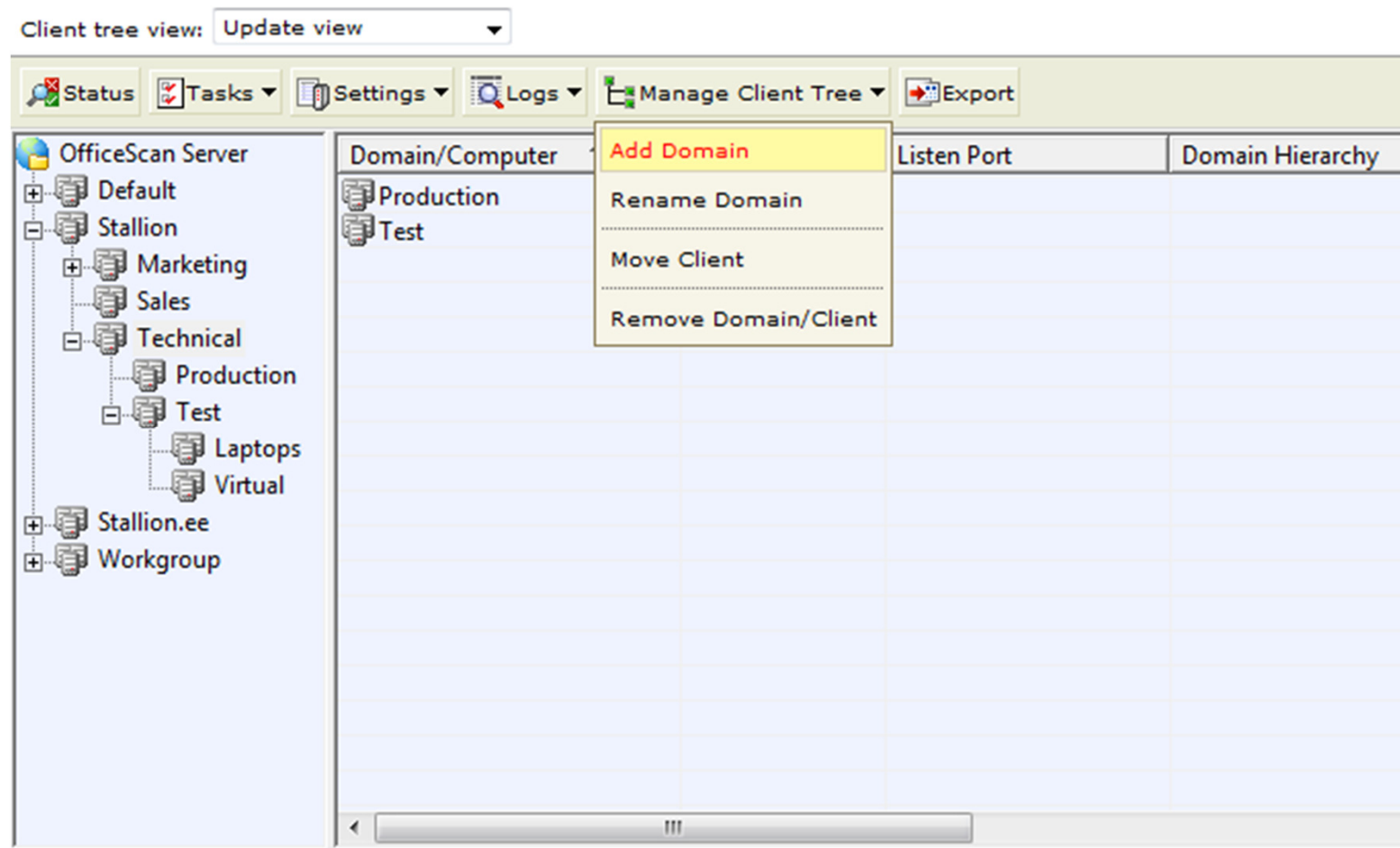
- OfficeScan Server
 - Default
 - Xsonnkm
 - XsnTestLab

<div><div> Add</div><div> Delete</div></div>				
<input type="checkbox"/>	Order	Rule Name	Rule Type	Status
<input type="checkbox"/>	1	Network Administrators	IP Address	
<input type="checkbox"/>	2	Test Lab Mapping	Active Directory	
<input type="checkbox"/>	3	w3 Servers	IP Address	

Multi-tier Client Trees

- In OfficeScan 10.0 and earlier versions domains/ groups could be added only under root domain
- OfficeScan 10.5 allows to create multi-level domain/ group trees

Networked Computers > Client Management > select domain > Manage Client Tree > Add Domain



Web Reputation Service integrated with Smart Scan servers



- OfficeScan 10.0 introduced Smart Scan server
 - In-the-cloud pattern-file query
 - Integrated and standalone Smart Scan servers in your network
- Web Reputation Service requests web pages score from Trend Micro global server in 10.0 and earlier version
- OfficeScan 10.5 integrated Web Reputation Service with Smart Scan server- file and web reputation services both can now be in your network

Smart Protection > Smart Protection Sources > Internal Clients > click on standard list > Launch console



Integrated Smart Protection Server

- ☒ Use Integrated File Reputation Service
- ☒ Use Integrated Web Reputation Service

Client Connection		
Server Mode	Protocol	Server Address
File Reputation	HTTPS	https://10.1.10.20:4345/tmcss/
File Reputation	HTTP	http://10.1.10.20:8082/tmcss/
Web Reputation	HTTP	http://10.1.10.20:5274/

Component Status			
Component	Current Version	Last Update	
Smart Scan Pattern	10388.023.00	07/14/2010 00:39:23	Update Now
Web Blocking List	3.005.00165	07/13/2010 23:38:21	Update Now

Web Reputation Service Approved/Blocked List		
Import	Export	1
Rule Name		Coverage
Import	Export	#

Update Settings	
Update Schedule	
<input checked="" type="checkbox"/> Enable scheduled updates	
<input checked="" type="radio"/> Hourly	
<input type="radio"/> Every 15 minutes	
Update Source	
<input checked="" type="radio"/> Trend Micro ActiveUpdate Server	(http://osce10-icss-p.activeupdate.trendmicro.com/activeupdate)
<input type="radio"/> Other update source:	<input type="text" value="http://"/>

Expanded compliance-assessment reporting



- OfficeScan 10.5 allows to make „clients installed or nor installed“ compliance reports based on Active Directory and also IP addresses
- Expanded Compliance Reporting ensures that computers which are part of the OfficeScan client tree:
 - have correct services
 - have latest components
 - have consistent settings
 - successfully perform scanning

Security Compliance > Compliance Assessment > Compliance Report > choose domain from Client Tree Scope and press Assess



Compliance Report Help

Services **Components** Scan Compliance Settings

Computers with Inconsistent Component Versions

Components	Computers
Smart Scan Agent Pattern	0
Virus Pattern	4
IntelliTrap Pattern	1
IntelliTrap Exception Pattern	2
Virus Scan Engine	0
Spyware Pattern	2
Spyware Active-monitoring Pattern	2
Spyware Scan Engine	0
Virus Cleanup Template	1
Virus Cleanup Engine	0
Common Firewall Pattern	0
Common Firewall Driver	0
Behavior Monitoring Driver	1

Client Tree Scope Assess

Select the root or a specific domain and click Assess to generate the latest data from the client tree.

- ☒ OfficeScan Server
- ☐ Workgroup
- ☐ Default

Last query: OfficeScan... 11/09/2010 22:11:04

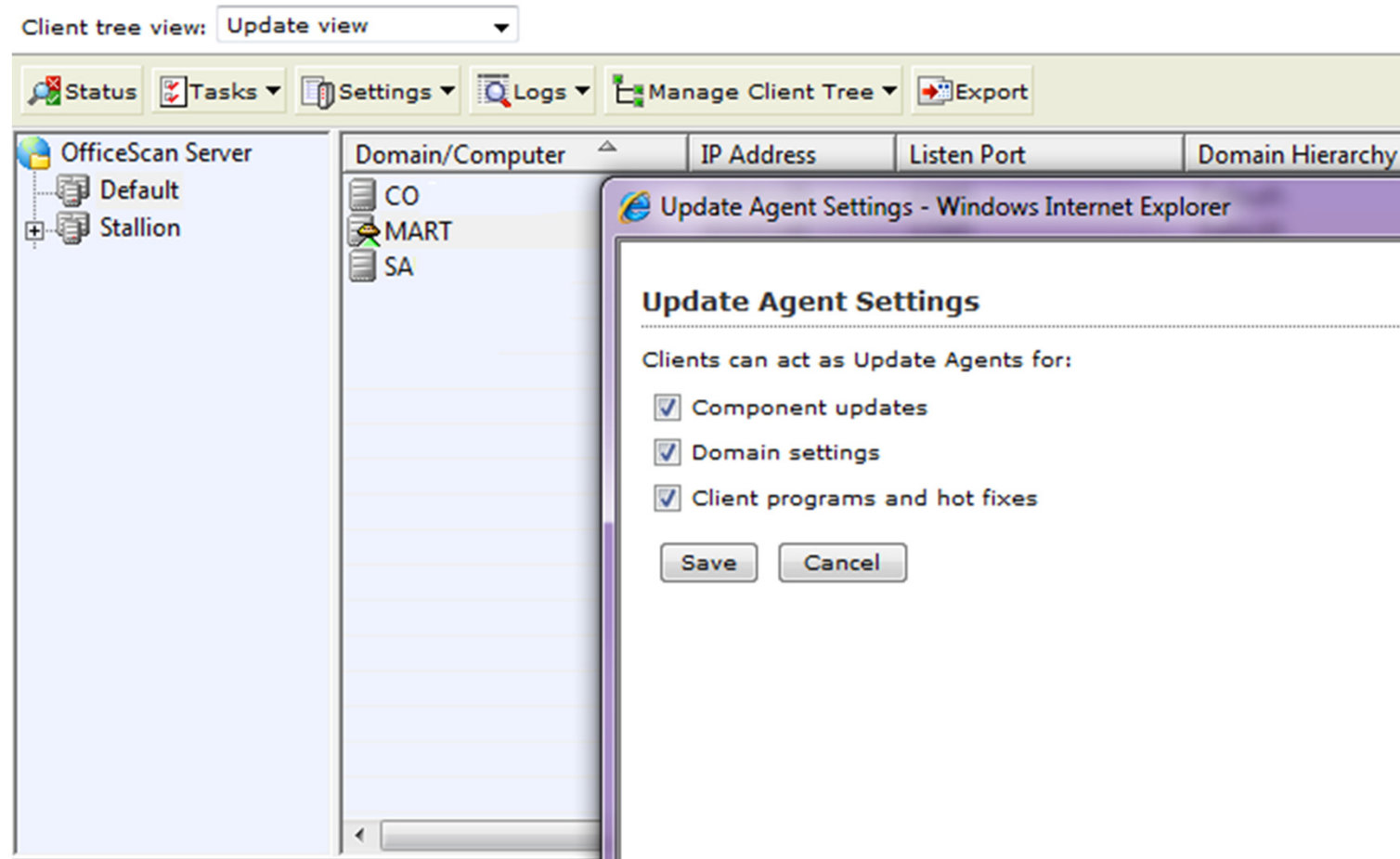
Update Now Export 1-5 of 5 page 1 of 1

Computer Name	OfficeScan Domain	Connection Status	Components
CO	Default\	online	Virus Pattern
KU	Workgroup\	offline	Virus Pattern, Spyware Pattern, Spyware Active-monitoring Pattern
SA	Default\	online	Program Version
ST.	Workgroup\	offline	Virus Pattern, IntelliTrap Pattern, IntelliTrap Exception Pattern, Spyware Pattern, Spyware Active-monitoring Pattern, Virus Cleanup Template
PC	Default\	online	Virus Pattern, IntelliTrap Exception Pattern, Behavior Monitoring Driver

Role options for Update Agents

- Update agents:
 - Offload the update process from OfficeScan
 - Decrease LAN and WAN backbone traffic
- Update agent hierarchy
 - OfficeScan server distributes to update agents
 - Update agents distribute to clients
- In OfficeScan 10.5 it is possible to choose what update agents distribute
 - Component updates
 - Domain settings
 - Client programs and hot fixes

Networked Computers > Client Management > choose computer > Settings > Update Agent Settings



Application filtering for firewall



- Added feature to the client firewall that allows to block or allow network traffic based on the application



Networked Computers > Firewall > Policies > Add > under Exception section press Add > Application: section



Edit Exception

Firewall Policies > Edit Policy > Edit Exception

Exception	
Name:	<input type="text" value="Putty"/>
Application:	<div><div><input type="radio"/> All applications</div><div><input checked="" type="radio"/> Specify application full path:<div><input type="text" value="C:\Users\Mart\Desktop\PUTTY.EXE"/><div>For example, C:\Program Files\app.exe</div></div></div><div><input type="radio"/> Specify application registry key:<div>Key: <input type="text" value="HKEY_LOCAL_MACHINE"/><div>Subkey: <input type="text"/><div>For example, SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\test.exe\</div></div></div></div></div> <div>Value name: <input checked="" type="checkbox"/> Use default value name <input type="text"/></div>
Action:	<div><input checked="" type="radio"/> Allow network traffic</div> <div><input type="radio"/> Allow and log network traffic</div> <div><input type="radio"/> Deny network traffic</div>
Direction:	<div><input checked="" type="checkbox"/> Inbound</div> <div><input checked="" type="checkbox"/> Outbound</div>
Protocol:	<input type="text" value="TCP/UDP"/>
Port(s):	<div><div><input checked="" type="radio"/> All ports</div><div><input type="radio"/> Range:<div>From: <input type="text"/><div>To: <input type="text"/></div></div></div><div><input type="radio"/> Specific port numbers:<div><input type="text"/><div>(Use a comma to separate port numbers)</div></div></div></div>
IP address(es):	<div><div><input checked="" type="radio"/> All IP addresses</div><div><input type="radio"/> Single IP address:<div>IP: <input type="text"/></div></div></div>

Exception lists for device control



- Two types of exceptions:
 - Approved Application List
 - Applications in this list are exempt from Device Control policies and have full access to external storage devices and network resources
 - Executable Program List
 - Applications in this list can be run from external storage devices, but do not have access to external devices.



Networked Computers > Client Management > choose domain/ group or computer > Settings > Device Control Settings > Exceptions section



☒ Enable Device Control

☐ Block AutoRun function on USB devices

Device	Description	Permissions
USB devices	Includes all kinds of storage devices, except floppy and optical disks, that connect through a USB interface	No Access
Optical disks	Storage media read by internal or external drives using lasers; commonly in CD or DVD format	Full Control
Floppy disks	Flexible magnetic disks typically enclosed in rigid 3 1/2-inch cases and read by external or built-in drives	Full Control
Network resources	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

Exceptions

Provide digital signatures or the program full file path and name. Items added to the Device Access List will be exempt from Device Control policies and have full access to external storage devices and network resources. Items added to the External Programs List can run from external storage devices but with limited access. Separate entries with a semicolon (;).

☒ Device Access list

☐ External Programs list

Device Access List

C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Highly granular admin-user access settings



- Delegate tasks to child domains to restrict administrative users to specific tasks without interfering with parent domains
- Limit the presentation of the management console
- Define roles that allow administrative users to focus only on their specific responsibilities
- Assign “view only” access to pages without granting an administrator the ability to modify the associated configuration parameters

Administration > User Roles > Add



Select Domains*:

*Required fields

Role Permissions

Specify the menu items that this newly created role can see or configure from either the main menu or the client management tree drop-down menus.

Global Menu Items

Client Management Menu Items

Specify the menu items that this newly created role can see or configure from the client management tree drop-down menus. Not selecting an option not display when the user role logs on to the OfficeScan web console.

Client Tree Scope	Available Menu Items	View	Configure
<input type="checkbox"/> OfficeScan Server	Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Default	Tasks	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Workgroup	Scan Now	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Client Uninstallation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Spyware/Grayware Restore	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Virus/Malware Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Spyware/Grayware Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Firewall Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Web Reputation Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Behavior Monitoring Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Device Control Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Delete Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Manage Client Tree	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Add Domain	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Rename Domain	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Move Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Sort Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Performance & other incremental enhancements



- For example:
 - More granular Web reputation settings which now allow to configure web reputation policies and assign them to one, several, or all OfficeScan clients
 - Added controls for scan settings for clients with the privilege to configure scan exclusions



A blue-tinted background image showing a person's hands using a computer mouse and keyboard. The image is overlaid with a semi-transparent blue rectangle containing the title text. Faint, repeating text "NB" is visible in the background.

OfficeScan plug-in architecture

Open OfficeScan management console > Plug-in Manager



Scan Now for All Domains

Update Server Now

Summary

Security Compliance

Networked Computers

Smart Protection

Updates

Logs

Cisco NAC

Notifications

Administration

Tools

Plug-in Manager

TREND MICRO
SMART
PROTECTION
NETWORK

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:

- Ensure that the Plug-in Manager version is 1.0.3151 or later. Please upgrade Plug-in Manager first if its version is earlier than 1.0.3151.
- Read the installation guide and release notes. Click [here](#) to download these documents.

Manage Program

Current version: 1.2.2266

Uninstall

TMAgent Manager

The Threat Management Agent (TMAgent) Manager is a plug-in program that utilizes the OfficeScan™ server architecture to easily deploy and manage TMAgents. TMAgent Manager can manage the list of Threat Mitigator servers, deploy TMAgent to endpoints, and uninstall the TMAgent Manager client and TMAgent. Once the endpoints finish installing TMAgent, Threat Mitigator will be able to communicate and enforce endpoint policies.

This version of TMAgent Manager uses TMAgent 2.7.1058.

Manage Program

Available version: 1.0.1065

Download (7.06MB)

Trend Micro Mobile Security

Trend Micro Mobile Security for Enterprise v5.5 allows the OfficeScan server to manage Mobile Device Agents installed on mobile devices. Also, it allows you to 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 malware from infecting mobile devices.

WARNING: TMMS Encryption functionality for Symbian S60 mobile devices will be lost if you upgrade to TMMS 5.5.

Manage Program

Available version: 5.5.1105

Upgrade

Current version: 5.1.1077

Uninstall

Trend Micro Security (for Mac)

Trend Micro Security (for Mac) delivers immediate protection from malware targeting Mac OS and other operating systems in heterogeneous environments. Trend Micro Smart Protection Network enables real-time correlated threat intelligence and proactive Web threat protection. This flexible solution integrates seamlessly into Mac OS for easy of administration and a positive user experience.

Please refer to the release notes and Administrator's Guide for installation requirements and details. Click [here](#) to download these documents.

Manage Program

Available version: 1.5.5028

Download (149.30MB)

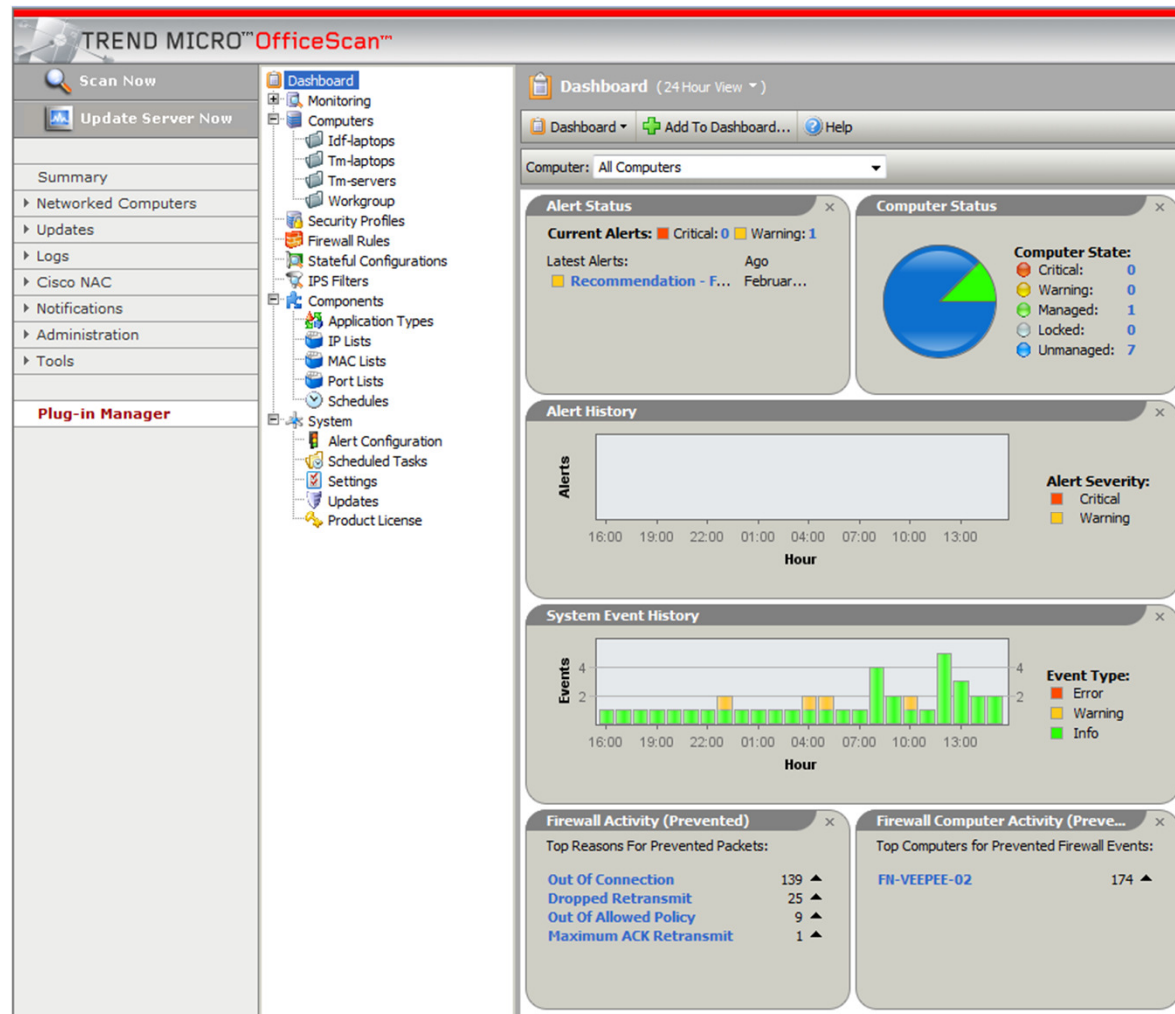
Trend Micro Virtual Desktop Support

IDF - Intrusion Defense Firewall



- IDF is a host intrusion defense system that plugs in to existing OfficeScan solution
- It supplements OfficeScan clients with advanced firewall, virtual patching features and provides deep packet inspection, along with advanced application vulnerability protection
- IDF allows to create and manage comprehensive intrusion defense security policies, track threats, and log actions taken in response to these threats

IDF - management console



IDF - firewall



- Sophisticated, bi-directional stateful firewall, provides complete support for all network protocols. Firewall Rules are fully configurable to allow or deny traffic on a per-interface basis, and restrict communication to allowed IP or MAC addresses.

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

IDF - virtual patching



- Virtual patching is a host-based security capability that shields applications from vulnerabilities until permanent corrections from procedures such as patch management and software maintenance can be applied.
- Virtual patching operates on network streams, inspecting inbound traffic and shielding applications from exploits, even though the vulnerability has not been permanently patched

IDF - virtual patching



- 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

The screenshot shows the 'IPS Filters' application window. The title bar reads 'IPS Filters (By Issued)' and the status bar indicates 'Page 1 of 13'. The window contains a table with the following columns: Name, Application Type, Priority, Severity, Mode, Type, and CVE. The table lists 32 filters, with the 10th filter, '1003287 - LinkedIn Browser Toolbar A...', highlighted in blue. The filters include various applications like Microsoft Windows Server, Mozilla Firefox, and Adobe Acrobat, with different severity levels and modes.

Name	Application Type	Priority	Severity	Mode	Type	CVE
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

TMAgent Manager

(new in OfficeScan 10.5)



TMAgent Manager

The Threat Management Agent (TMAgent) Manager is a plug-in program that utilizes the OfficeScan™ server architecture to easily and manage TMAgents. TMAgent Manager can manage the list of Threat Mitigator servers, deploy TMAgent to endpoints, and uninstall the TMAgent Manager client and TMAgent. Once the endpoints finish installing TMAgent, Threat Mitigator will be able to communicate and enforce endpoint policies.

This version of TMAgent Manager uses TMAgent 2.7.1058.



Manage Program

Available version: 1.0.1065

Download

(7.06MB)

Trend Micro Mobile Security



- Trend Micro Mobile Security protects smartphones and PDAs from infections and attacks.
- Anti-malware features block viruses, worms, trojans and SMS text message spam
- Built-in firewall and Intrusion Detection System protects against hackers, intrusions and DoS attacks- potential threats to the increasing number of WiFi- enabled mobile devices

Trend Micro Mobile Security



Status summary as of 11/10/2010 18:10:39

Device Registration Status



Registered: 0
Unregistered: 0
Total managed devices: 0

0 SMS message(s) in queue

Message type	Message Number	Action
Registration	0	Delete
Component Update	0	Delete
Policy Update	0	Delete

⚠ No SMS Sender is configured. [Configure Now.](#)

⚠ Unable to reach server. [Verify Now.](#)

Device Update Status

Anti-Malware Components	Current Version	Up-to-date	Out-of-date	Update Rate
Malware Pattern for Windows Mobile 5/6	1.129.00	0	0	<input type="text"/> 0.0%
Malware Pattern for Symbian OS 9.x S60 3 rd /5 th Edition	1.195.00	0	0	<input type="text"/> 0.0%
Malware Scan Engine for Windows Mobile 5/6	7.460-1035	0	0	<input type="text"/> 0.0%
Malware Scan Engine for Symbian OS 9.x S60 3 rd /5 th Edition	7.460-1043	0	0	<input type="text"/> 0.0%
Program	Current Version	Upgraded	Not Upgraded	Upgrade Rate
Mobile Device Agent for Windows Mobile 5/6 - Pocket PC, Pocket PC Phone / Classic, Professional	5.5.0.1151	0	0	<input type="text"/> 0.0%
Mobile Device Agent for Windows Mobile 5/6 - Smartphone / Standard	5.5.0.1151	0	0	<input type="text"/> 0.0%
Mobile Device Agent for Symbian OS 9.x S60 3 rd /5 th Edition	5.5.0.1036	0	0	<input type="text"/> 0.0%

Trend Micro Security (for Mac)



- Management of up to 1 000 Mac endpoints
- Standard AV technology
 - Detection and blocking of malware
- Uses also Web Reputation
- Seamless integration into MacOS
- Supports
 - Mac OS™ X version 10.4.11 (Tiger™) or later
 - Mac OS X version 10.5.5 (Leopard™) or later

Trend Micro Security (for Mac)



Trend Micro OfficeScan™

Current server:

Scan Now
Update Server Now

Summary
Security Compliance
+ Networked Computers
+ Smart Scan
+ Updates
+ Logs
+ Cisco NAC
+ Notifications
+ Administration
+ Tools

Plug-in Manager

Trend Micro Security for Mac

Summary | Client Management | Server Updates | Notifications | Administration

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: [] [Search]

Tasks Settings Logs Manage Client Tree 1 - 2 of 2 Page 1 of 1

Computer	Computer Location	Connection Status	Security Risks	Web Threats
James-iMac-G3	Internal	Online	0	0
tw-jamesolmac	External	Offline	0	0

Number of client(s): 2

Real-time Scan Settings

☒ Enable Real-time Scan

Target Action

☒ Use ActiveAction

☐ Use the same action for all security risk types
(If you choose Clean, specify the second action Trend Micro Security will take if cleaning fails)

Type	1st Action	2nd Action
All Types	Clean	Quarantine

☒ Display a notification message on the client computer when virus/malware is detected.

Save Cancel

VDI - Virtual Desktop Infrastructure Support

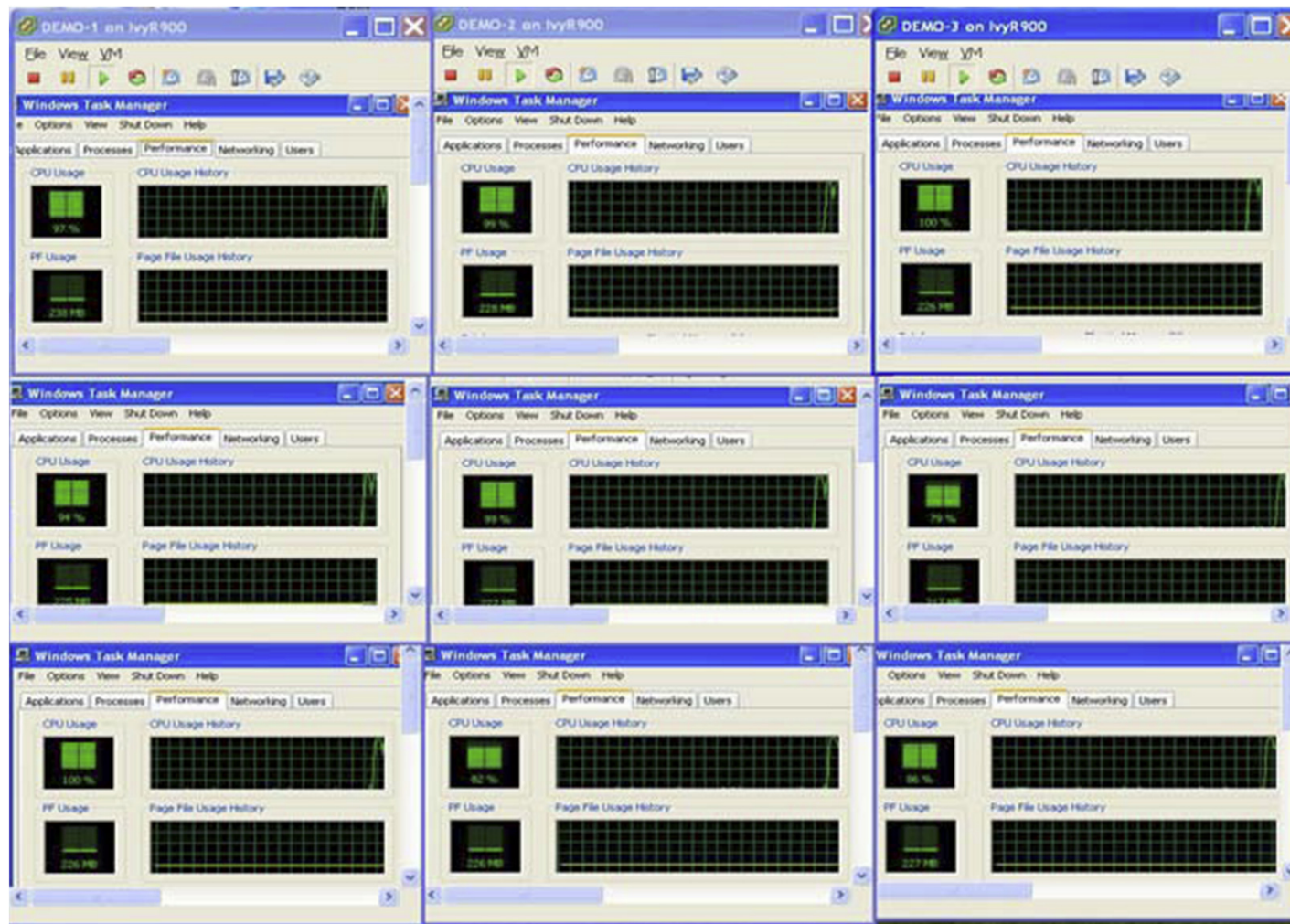
(new in OfficeScan 10.5)



- Simultaneous activity can overload VM platforms
- Plugin serializes OfficeScan client activity
 - Full system scans
 - Component updates



Impact of Simultaneous Scanning



Results of Sequencing Activity



Simple, Straightforward Configuration



Virtual Desktop Infrastructure Settings



Specify guest operating systems using virtual desktops to regulate the number of OfficeScan clients that performs scanning and updates in a single server.

[View License Information](#)

Virtual Desktop Management Method

- ☒ VMware vCenter™ Server
☐ Citrix XenServer™

VMware vCenter Server Connection Setting 1

☒ Enable this connection

vCenter server IP address:

Username:

Password:

☐ Use proxy to connect to this vCenter server

Proxy server name or IP address:

Port:

Proxy server authentication:

Username:

Password:

Test connection

Add new vCenter connection

Save Cancel



Thank you!