



**TENABLE**  
Network Security®

## **Patch Management Integration**

January 10, 2012

**(Revision 5)**

---

Copyright © 2002-2012 Tenable Network Security, Inc. Tenable Network Security, Nessus and ProfessionalFeed are registered trademarks of Tenable Network Security, Inc. Tenable, the Tenable logo, the Nessus logo, and/or other Tenable products referenced herein are trademarks of Tenable Network Security, Inc., and may be registered in certain jurisdictions. All other product names, company names, marks, logos, and symbols may be the trademarks of their respective owners.

# Table of Contents

<b>Overview</b> .....	<b>3</b>
Scanning With Multiple Patch Managers.....	3
<b>WSUS</b> .....	<b>3</b>
Creating the Policies .....	3
<i>General</i> .....	4
<i>Credentials</i> .....	4
<i>Plugins</i> .....	4
<i>Preferences</i> .....	5
<b>SCCM</b> .....	<b>8</b>
Creating the Policies .....	8
<i>General</i> .....	8
<i>Credentials</i> .....	9
<i>Plugins</i> .....	9
<i>Preferences</i> .....	10
<b>VMware Go</b> .....	<b>11</b>
Creating the Policies .....	11
<i>General</i> .....	11
<i>Credentials</i> .....	12
<i>Plugins</i> .....	12
<i>Preferences</i> .....	13
<b>Red Hat Network Satellite</b> .....	<b>15</b>
Creating the Policies .....	15
<i>General</i> .....	15
<i>Credentials</i> .....	16
<i>Plugins</i> .....	16
<i>Preferences</i> .....	17
<b>About Tenable Network Security</b> .....	<b>20</b>

## OVERVIEW

Tenable's Unified Security Monitoring (USM) product suite provides great flexibility in scanning methods to better serve our customers' varying scanning requirements and restrictions. Customers can perform passive scanning, active network scans, or scan with credentials for more accurate results with less network bandwidth utilization.

Nessus and SecurityCenter now leverage credentials for the WSUS, SCCM, and VMware Go (formerly Shavlik) patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner.



IT administrators are expected to manage the patch monitoring software themselves and install any agents required by the patch management system on their systems.

## SCANNING WITH MULTIPLE PATCH MANAGERS

If multiple sets of credentials are supplied to Nessus for patch management tools, Nessus will not use all of them. Based on the credentials supplied, Nessus will use the first one available in the following order:

1. Credentials supplied to directly authenticate to the target
2. VMware Go (formerly Shavlik)
3. WSUS
4. SCCM

## WSUS

Windows Server Update Services (WSUS) is available from Microsoft to manage the distribution of updates and hotfixes for Microsoft products. Nessus and SecurityCenter have the ability to query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Nessus or SecurityCenter GUI.

- > If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore WSUS output.
- > The data returned to Nessus by WSUS is only as current as the most recent data that the WSUS server has obtained from its managed hosts.

WSUS scanning is performed using two Nessus plugins:

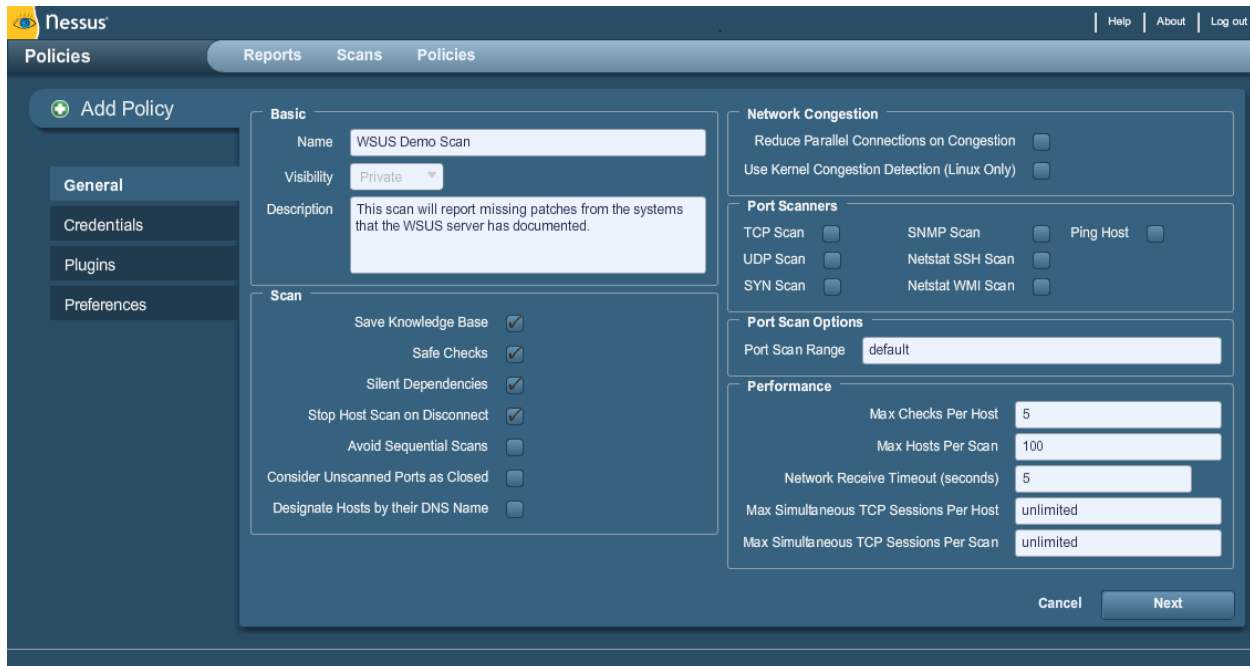
- > wsus\_init\_info.nbin (Plugin ID 57031)
- > wsus\_get\_missing\_updates.nbin (Plugin ID 57032)

## CREATING THE POLICIES

From the Nessus or SecurityCenter web interface, click the "**Policies**" tab and then "**Add**". Directions for each tab under the "**Add Policy**" menu are described in this section.

## General

If WSUS patch management scans are run as part of a normal scan or SMB scan, all port scanning settings can be configured as they would in a typical scan policy.



The screenshot shows the Nessus 'Add Policy' configuration page. The 'Basic' section includes:
 

- Name: WSUS Demo Scan
- Visibility: Private
- Description: This scan will report missing patches from the systems that the WSUS server has documented.

 The 'Scan' section includes several checkboxes:
 

- Save Knowledge Base:
- Safe Checks:
- Silent Dependencies:
- Stop Host Scan on Disconnect:
- Avoid Sequential Scans:
- Consider Unscanned Ports as Closed:
- Designate Hosts by their DNS Name:

 The 'Network Congestion' section includes:
 

- Reduce Parallel Connections on Congestion:
- Use Kernel Congestion Detection (Linux Only):

 The 'Port Scanners' section includes:
 

- TCP Scan:
- UDP Scan:
- SYN Scan:
- SNMP Scan:
- Netstat SSH Scan:
- Netstat WMI Scan:
- Ping Host:

 The 'Port Scan Options' section includes:
 

- Port Scan Range: default

 The 'Performance' section includes:
 

- Max Checks Per Host: 5
- Max Hosts Per Scan: 100
- Network Receive Timeout (seconds): 5
- Max Simultaneous TCP Sessions Per Host: unlimited
- Max Simultaneous TCP Sessions Per Scan: unlimited

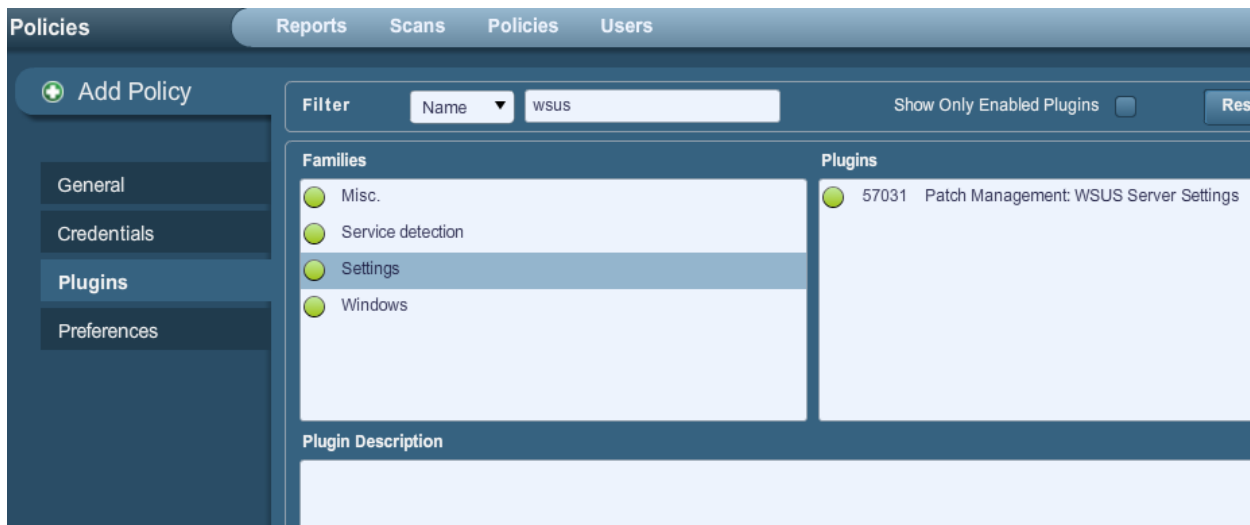
 Buttons for 'Cancel' and 'Next' are visible at the bottom right.

## Credentials

Because Nessus does not rely on the system being managed by WSUS to report patch management issues, credentials for the target systems do not need to be used in the scan policy.

## Plugins

At least three specific plugins must be enabled for the WSUS patch management scans to run. These plugins can easily be found by searching for "WSUS" or "Patch Management" on the plugin filtering configuration page:



The screenshot shows the Nessus 'Filter' configuration page. The 'Filter' section includes:
 

- Name: wsus
- Show Only Enabled Plugins:

 The 'Families' section lists:
 

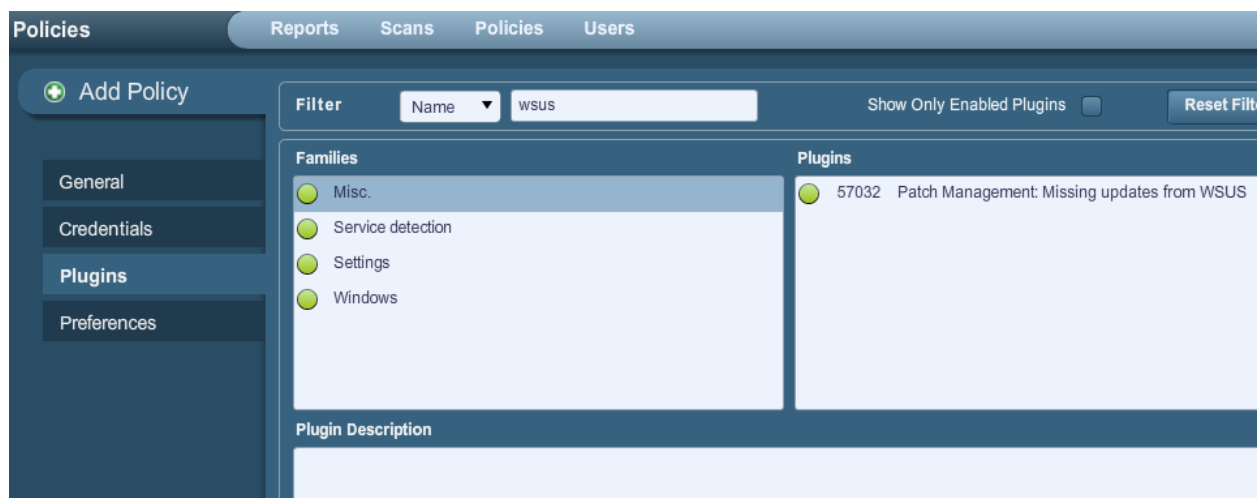
- Misc.
- Service detection
- Settings
- Windows

 The 'Plugins' section lists:
 

- 57031 Patch Management: WSUS Server Settings

 The 'Plugin Description' section is currently empty.

## Patch Management: WSUS Server Settings



## Patch Management: Missing updates from WSUS



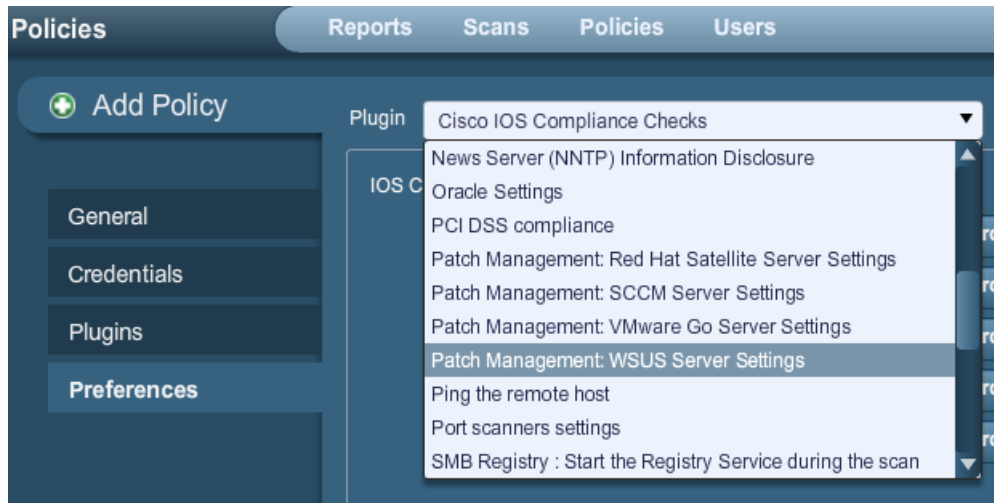
## Windows : Microsoft Bulletins

### Preferences

Credentials for the WSUS server must be provided for WSUS scanning to work properly.

Credential	Description
<b>WSUS Server</b>	WSUS IP address or system name
<b>WSUS Port</b>	Port WSUS is running on (Typically TCP 80 or 443)
<b>WSUS Username</b>	WSUS admin username
<b>WSUS Password</b>	WSUS admin password

In the "Preferences" pane, select "**Patch Management: WSUS Server Settings**" from the Plugin drop-down menu:



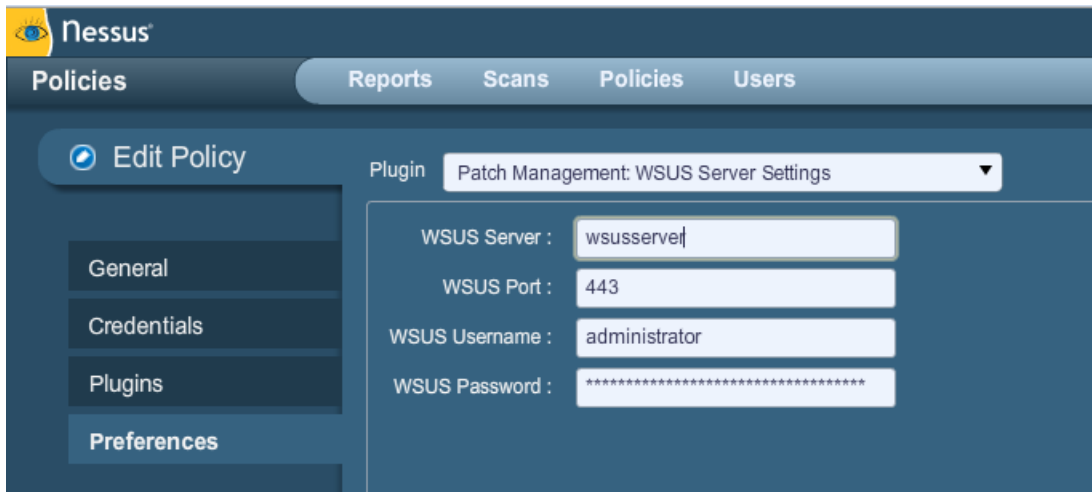
**Policies** | Reports | Scans | Policies | Users

**+ Add Policy**

General  
Credentials  
Plugins  
**Preferences**

Plugin: Cisco IOS Compliance Checks

- News Server (NNTP) Information Disclosure
- Oracle Settings
- PCI DSS compliance
- Patch Management: Red Hat Satellite Server Settings
- Patch Management: SCCM Server Settings
- Patch Management: WSUS Server Settings**
- Patch Management: VMware Go Server Settings
- Ping the remote host
- Port scanners settings
- SMB Registry : Start the Registry Service during the scan



**Nessus**

**Policies** | Reports | Scans | Policies | Users

**⌚ Edit Policy**

General  
Credentials  
Plugins  
**Preferences**

Plugin: Patch Management: WSUS Server Settings

WSUS Server : wsusserver|

WSUS Port : 443

WSUS Username : administrator

WSUS Password : \*\*\*\*\*

The screenshot shows the Nessus Reports interface. The top navigation bar includes 'Reports', 'Scans', 'Policies', and 'Users'. The main content area displays a report for 'wsus 7.46-49' with a severity of 'High'. The report details include:

- Plugin ID:** 51904
- Port / Service:** cifs (445/tcp)
- Plugin Name:** MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)
- Synopsis:** The FTP service running on the remote host has a memory corruption vulnerability.
- Description:** The IIS FTP service running on the remote host has a heap buffer overflow vulnerability. The 'TELNET\_STREAM\_CONTEXT::OnSendData' function fails to properly sanitize user input, resulting in a buffer overflow. An unauthenticated, remote attacker can exploit this to execute arbitrary code.
- Solution:** Microsoft has released a set of patches for Windows Vista, 2008, 2008 R2, and 7: <http://www.microsoft.com/technet/security/bulletin/ms11-004.mspx>
- Risk Factor:** Critical
- CVSS Base Score:** 10.0 (CVSS2#AV:N/AC:L/Au:N/C:I/CIA:C)
- CVSS Temporal Score:** 7.8 (CVSS2#E:POC/RL:OF/RC:C)
- Plugin Output:** The host is missing KB 2489256 according to WSUS. (A red arrow points to this line.)
- CVE:** CVE-2010-3972
- BID:** 45542
- Xref:** OSVDB:70167, EDB-ID:15803, MSFT:MS11-004
- Vulnerability Publication Date:** 2010/12/21

## SCCM

System Center Configuration Manager (SCCM) is available from Microsoft to manage large groups of Windows-based systems. Nessus has the ability to query SCCM to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the Nessus or SecurityCenter GUI.

- > If the credentialed check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore SCCM output.
- > The data returned by SCCM is only as current as the most recent data that the SCCM server has obtained from its managed hosts.

SCCM scanning is performed using two Nessus plugins:

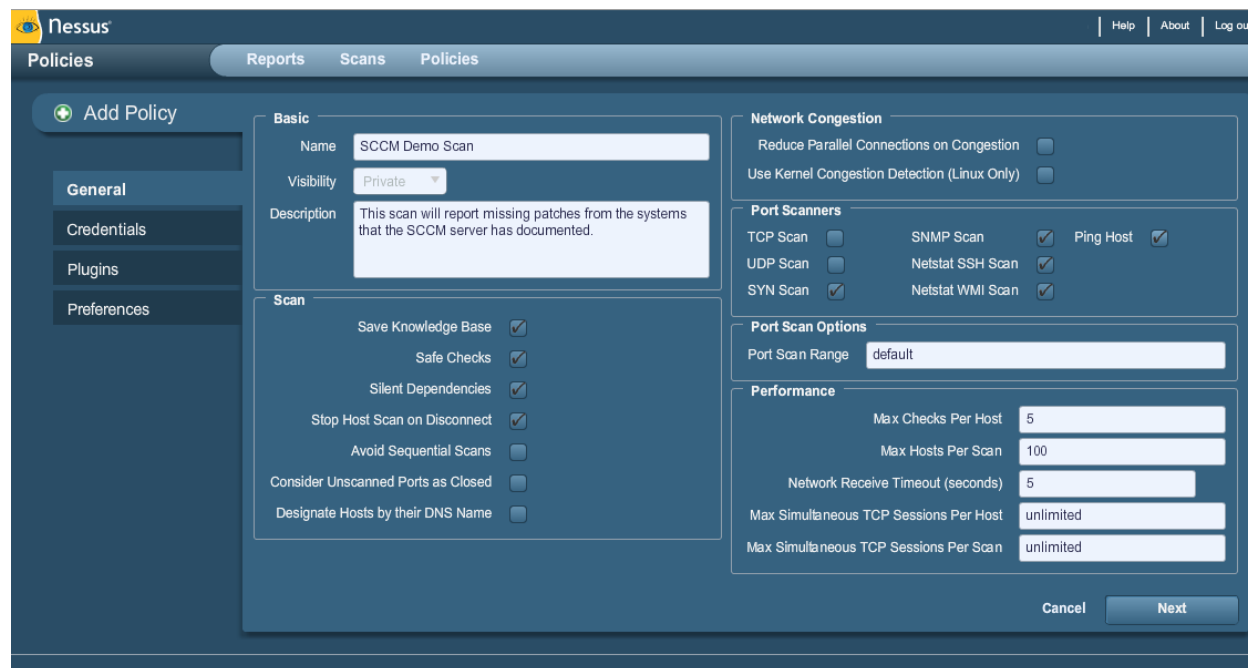
- > sccm\_init\_info.nbin (Plugin ID 57029)
- > sccm\_get\_missing\_updates.nbin (Plugin ID 57030)

## CREATING THE POLICIES

From the Nessus or SecurityCenter web interface, click the **"Policies"** tab and then **"Add"**. Directions for each tab under the **"Add Policy"** menu are described in this section.

### General

If SCCM patch management scans are run as part of a normal scan or SMB scan, all port scanning settings can be configured as they would in a typical scan policy.



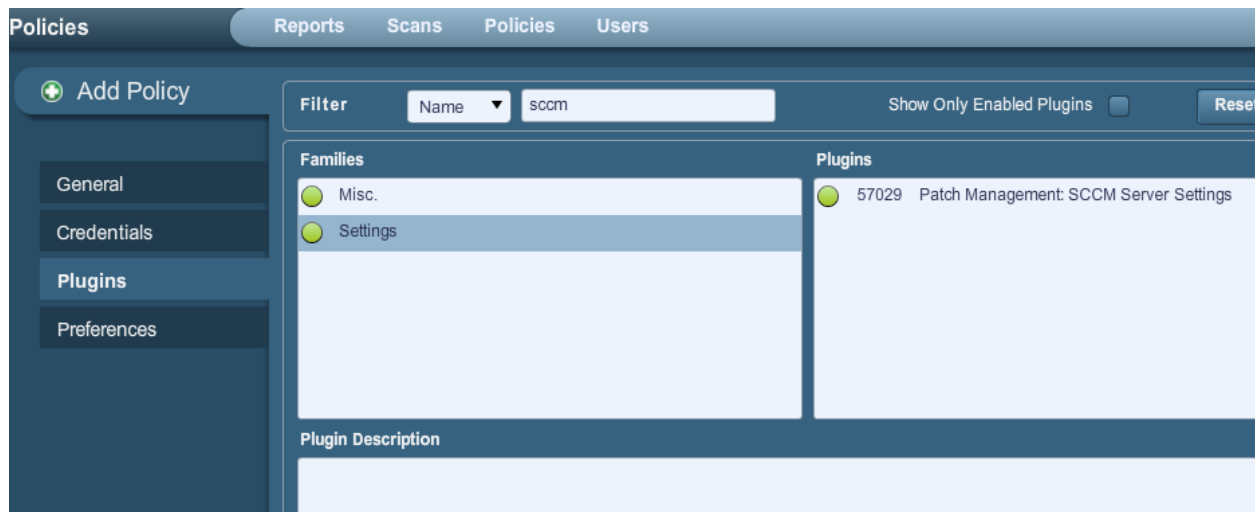


## Credentials

Because Nessus scans do not rely on the system being managed by SCCM to report patch management issues, credentials for the target systems do not need to be used in the scan policy.

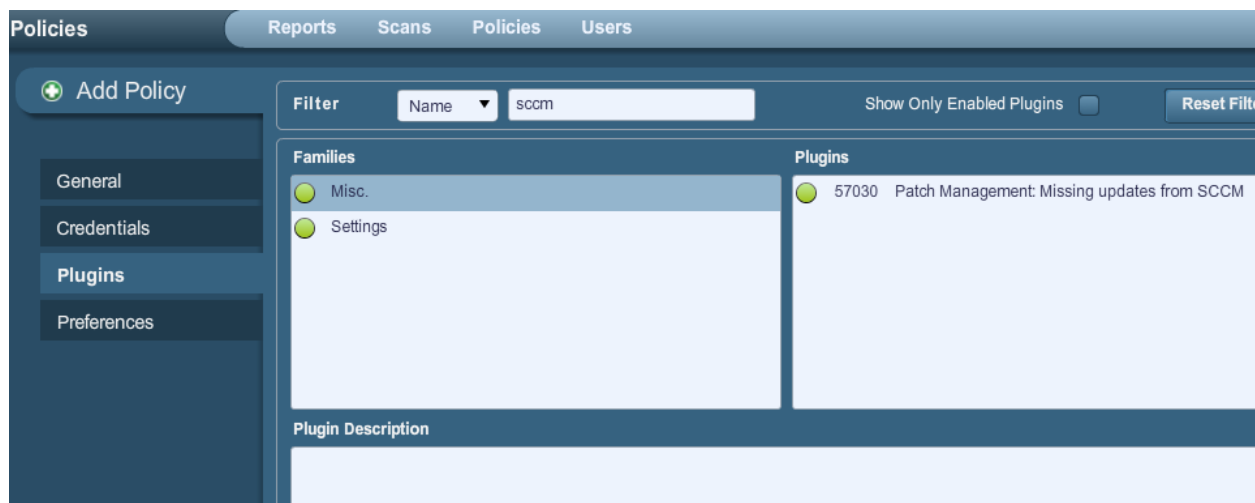
## Plugins

At least three specific plugins must be enabled for the SCCM patch management scans to run. These plugins can easily be found by searching for "SCCM" or "Patch Management" on the plugin filtering configuration page:



The screenshot shows the Nessus interface for configuring a scan policy. The 'Policies' tab is active, and the 'Plugins' sub-tab is selected in the left sidebar. A search filter is applied with the name 'sccm'. The search results are displayed in two columns: 'Families' and 'Plugins'. The 'Families' column lists 'Misc.' and 'Settings'. The 'Plugins' column lists a single plugin: '57029 Patch Management: SCCM Server Settings'. Below the search results is a 'Plugin Description' section.

### Patch Management: SCCM Server Settings



The screenshot shows the Nessus interface for configuring a scan policy. The 'Policies' tab is active, and the 'Plugins' sub-tab is selected in the left sidebar. A search filter is applied with the name 'sccm'. The search results are displayed in two columns: 'Families' and 'Plugins'. The 'Families' column lists 'Misc.' and 'Settings'. The 'Plugins' column lists a single plugin: '57030 Patch Management: Missing updates from SCCM'. Below the search results is a 'Plugin Description' section.

### Patch Management: Missing updates from SCCM



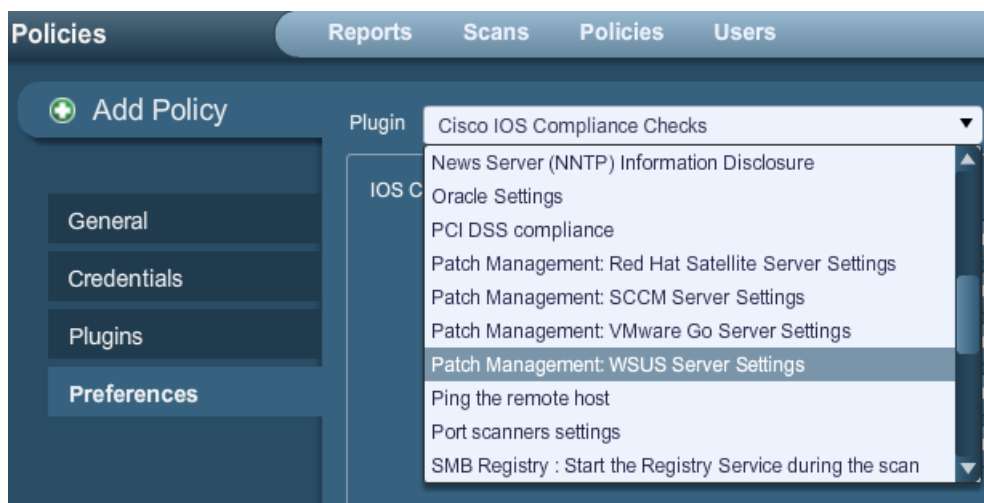
### Windows : Microsoft Bulletins

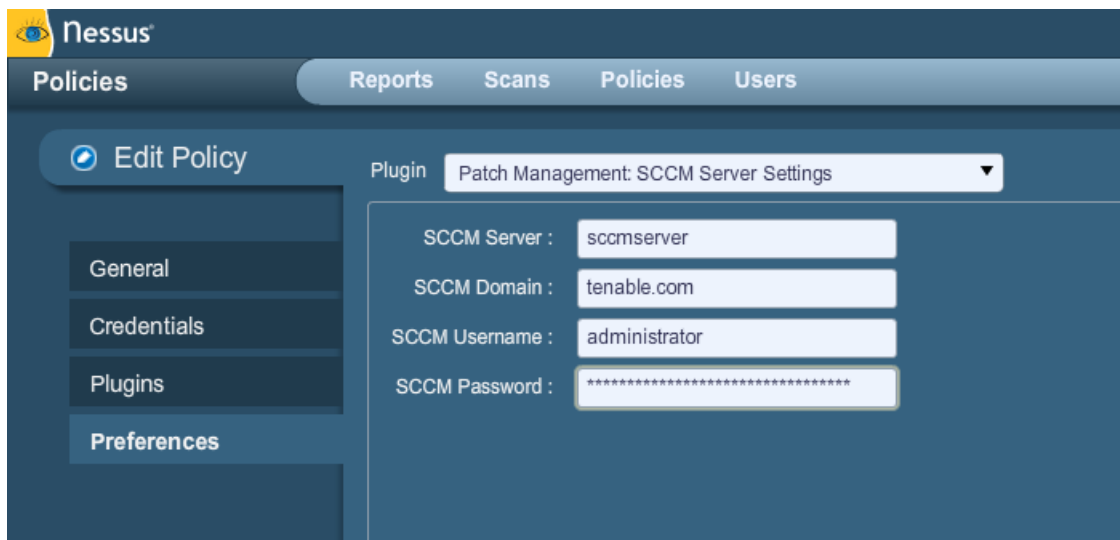
#### Preferences

Credentials for the SCCM server must be provided for SCCM scanning to work properly.

Credential	Description
<b>SCCM Server</b>	SCCM IP address or system name
<b>SCCM Domain</b>	The domain the SCCM server is a part of
<b>SCCM Username</b>	SCCM admin username
<b>SCCM Password</b>	SCCM admin password

In the “**Preferences**” pane, select “**Patch Management: SCCM Server Settings**” from the Plugin drop-down menu:





## VMWARE GO

VMware Go (formerly known as Shavlik) is a cloud-based service that checks the patch compliance status of an organization's systems. Nessus and SecurityCenter have the ability to query VMware Go to verify whether or not patches are installed on systems managed by VMware Go and display the patch information through the Nessus or SecurityCenter GUI.

- The VMware Go plugin never makes a direct connection to the target system; it instead connects to the VMware Go server specified to query the host about patch status.
- Outbound access to the VMware Go management server is required.
- SMB credentials are given priority; VMware Go is not used on a host when a valid SMB account is given.
- The organization using VMware Go is responsible for installing the VMware Go agents on their hosts.
- The data returned to Nessus by VMware Go is only as current as the most recent data that the VMware Go.

VMware Go scanning is performed using three Nessus plugins:

- shavlik\_settings.nbin (Plugin ID: 57026)
- shavlik\_host\_info.nbin (Plugin ID 57027)
- shavlik\_missing\_patches.nbin (Plugin ID 57028)

## CREATING THE POLICIES

From the Nessus or SecurityCenter web interface, click the "**Policies**" tab and then "**Add**". Directions for each tab under the Add Policy menu are described in this section.

### *General*

If VMware Go patch management scans are run as part of a normal scan or SMB scan, all port scanning settings can be configured as they would in a typical scan policy.

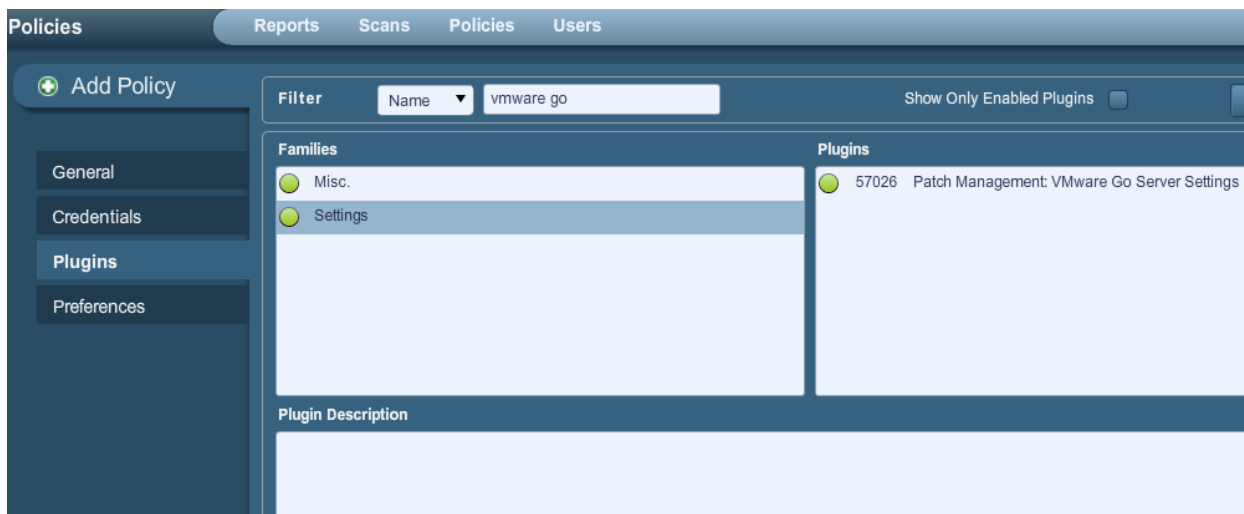
<b>Basic</b> Name: VMware Go test Visibility: Private Description:		<b>Network Congestion</b> Reduce Parallel Connections on Congestion <input type="checkbox"/> Use Kernel Congestion Detection (Linux Only) <input type="checkbox"/>	
<b>Scan</b> Save Knowledge Base <input type="checkbox"/> Safe Checks <input checked="" type="checkbox"/> Silent Dependencies <input checked="" type="checkbox"/> Stop Host Scan on Disconnect <input type="checkbox"/> Avoid Sequential Scans <input type="checkbox"/> Consider Unscanned Ports as Closed <input type="checkbox"/> Designate Hosts by their DNS Name <input type="checkbox"/>		<b>Port Scanners</b> TCP Scan <input type="checkbox"/> SNMP Scan <input checked="" type="checkbox"/> Ping Host <input checked="" type="checkbox"/> UDP Scan <input type="checkbox"/> Netstat SSH Scan <input checked="" type="checkbox"/> SYN Scan <input checked="" type="checkbox"/> Netstat WMI Scan <input checked="" type="checkbox"/>	
		<b>Port Scan Options</b> Port Scan Range: default	
		<b>Performance</b> Max Checks Per Host: 5 Max Hosts Per Scan: 100 Network Receive Timeout (seconds): 5 Max Simultaneous TCP Sessions Per Host: unlimited Max Simultaneous TCP Sessions Per Scan: unlimited	
		Cancel <b>Next</b>	

### Credentials

Because VMware Go scans do not rely on the system being managed to report patch management issues, credentials for the systems do not need to be used in the scan policy.

### Plugins

Make sure the plugin **"Patch Management: VMware Go Server Settings"** is selected under **"Plugins"** -> **"Families"** -> **"Settings"**:



The screenshot shows the 'Policies' management interface. A search filter is set to 'vmware go'. Under the 'Families' column, 'Settings' is selected. Under the 'Plugins' column, '57026 Patch Management: VMware Go Server Settings' is selected. The left sidebar shows navigation options: General, Credentials, Plugins, and Preferences.

### Patch Management: VMware Go Server Settings



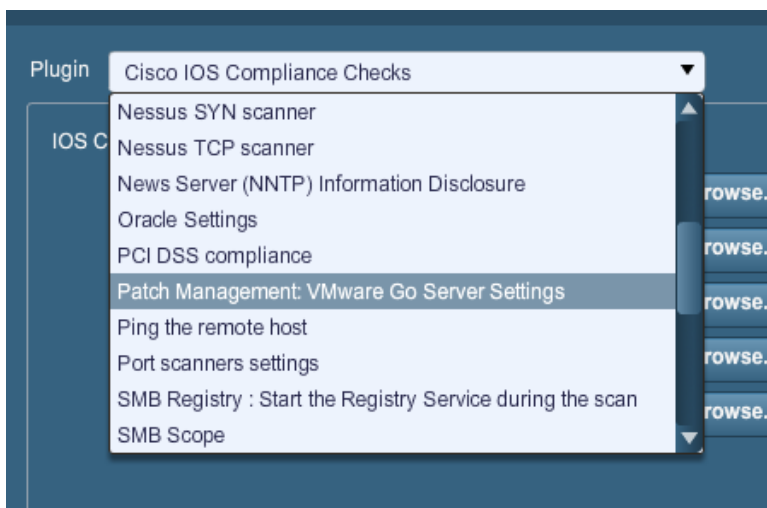
### Patch Management: Missing updates from VMware Go

#### Preferences

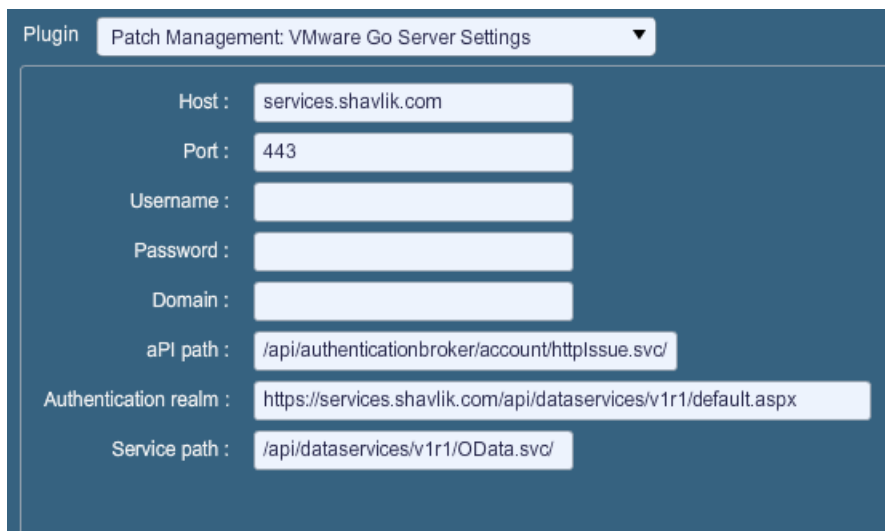
Credentials for the VMware Go server must be provided for scanning to work properly.

Credential	Description
<b>VMware Go Server</b>	VMware Go IP address or system name
<b>VMware Go Domain</b>	The VMware cloud-specified domain the VMware Go server is a part of
<b>VMware Go Username</b>	VMware Go admin username
<b>VMware Go Password</b>	VMware Go admin password

In the "Preferences" pane, select "Patch Management: VMware Go Server Settings" from the Plugin drop-down menu:



The following settings pane will be displayed:



Plugin: Patch Management: VMware Go Server Settings

Host: services.shavlik.com

Port: 443

Username: [Empty]

Password: [Empty]

Domain: [Empty]

aPI path: /api/authenticationbroker/account/httpissue.svc/

Authentication realm: https://services.shavlik.com/api/dataservices/v1r1/default.aspx

Service path: /api/dataservices/v1r1/OData.svc/

Once valid VMware Go credentials have been provided, any of the standard Windows checks will produce output similar to the following:



**Families**

- Ubuntu Local Security Checks
- VMware ESX Local Security Checks
- Web Servers
- Windows
- Windows : Microsoft Bulletins**
- Windows : User management

**Plugins**

- 35221 MS08-078: Microsoft Internet Explorer Security Update
- 35362 MS09-001: Microsoft Windows SMB Vulnerabilities Ren
- 35361 MS09-001: Vulnerabilities in SMB Could Allow Remote
- 35630 MS09-002: Cumulative Security Update for Internet Ex
- 35631 MS09-003: Vulnerabilities in Microsoft Exchange Could
- 35632 MS09-004: Vulnerability in Microsoft SQL Server Could
- 35633 MS09-005: Vulnerabilities in Microsoft Office Visio Cou



**Plugin ID:** 35632      **Port / Service:** cifs (445/tcp)      **Severity:** High

**Plugin Name:** MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)

Microsoft has released a set of patches for SQL Server 2000 and 2005 :  
<http://technet.microsoft.com/en-us/security/bulletin/ms09-004>

**Risk Factor:** High

**CVSS Base Score**  
 9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

**CVSS Temporal Score**  
 7.4 (CVSS2#E:F/RL:OF/RC:C)

**Plugin Output**  
 The host is missing the patch / patches for MS09-004 according to VMware Go.

**CVE**  
 CVE-2008-5416

**BID**  
 32710

## RED HAT NETWORK SATELLITE

Red Hat Satellite is a systems management platform for Linux-based systems. Nessus and SecurityCenter have the ability to query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information through the Nessus or SecurityCenter GUI.

Although not supported by Tenable, the RHN Satellite plugin will also work with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk has the capability of managing distributions based on Red Hat (RHEL, CentOS, Fedora) and SuSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

- > If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore RHN Satellite output.
- > The data returned to Nessus by RHN Satellite is only as current as the most recent data that the Satellite server has obtained from its managed hosts.

Satellite scanning is performed using two Nessus plugins:

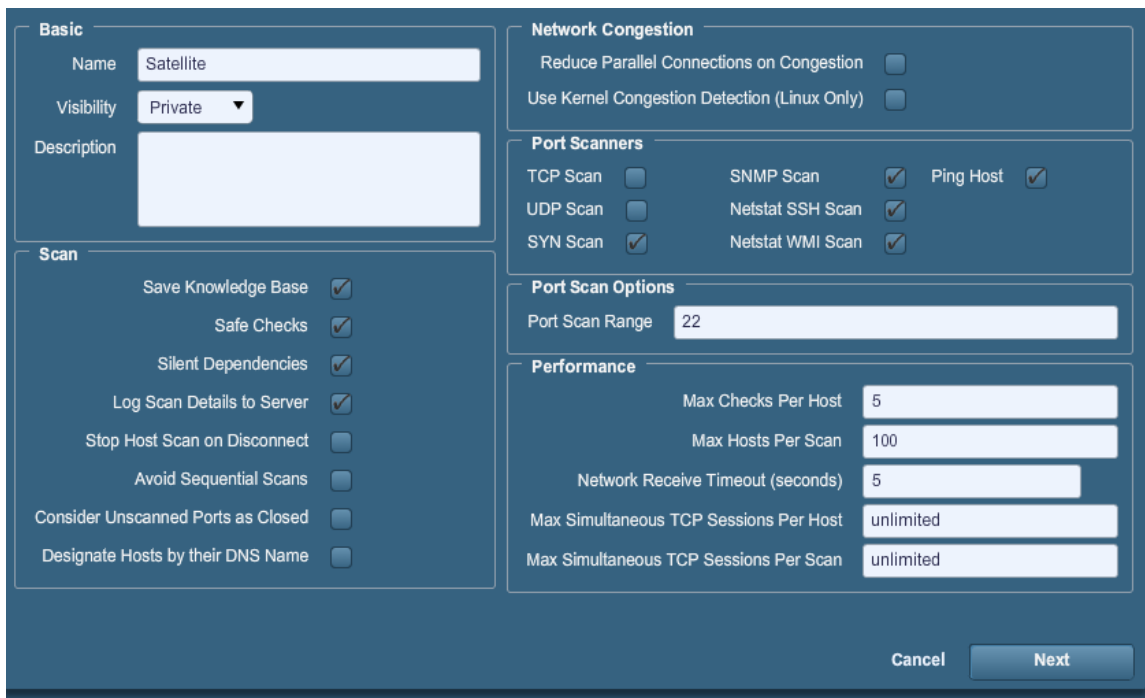
- > satellite\_settings.nbin (Plugin ID 57063)
- > satellite\_get\_managed\_hosts.nbin (Plugin ID 57064)
- > satellite\_get\_packages.nbin (Plugin ID 57065)
- > satellite\_get\_schedule.nbin (Plugin ID 57066)
- > satellite\_get\_system\_info.nbin (Plugin ID 57067)

## CREATING THE POLICIES

From the Nessus or SecurityCenter web interface, click the **"Policies"** tab and then **"Add"**. Directions for each tab under the **"Add Policy"** menu are described in this section.

### *General*

If RHN Satellite patch management scans are run as part of a normal scan, all port scanning settings can be configured as they would in a typical scan policy.



The screenshot shows a configuration window for a scan named "Satellite". The interface is divided into several sections:

- Basic:** Name: Satellite; Visibility: Private; Description: (empty text area).
- Scan:** A list of checkboxes for scan options: Save Knowledge Base (checked), Safe Checks (checked), Silent Dependencies (checked), Log Scan Details to Server (checked), Stop Host Scan on Disconnect (unchecked), Avoid Sequential Scans (unchecked), Consider Unscanned Ports as Closed (unchecked), and Designate Hosts by their DNS Name (unchecked).
- Network Congestion:** Reduce Parallel Connections on Congestion (unchecked), Use Kernel Congestion Detection (Linux Only) (unchecked).
- Port Scanners:** TCP Scan (unchecked), UDP Scan (unchecked), SYN Scan (checked), SNMP Scan (checked), Netstat SSH Scan (checked), Netstat WMI Scan (checked), Ping Host (checked).
- Port Scan Options:** Port Scan Range: 22.
- Performance:** Max Checks Per Host: 5; Max Hosts Per Scan: 100; Network Receive Timeout (seconds): 5; Max Simultaneous TCP Sessions Per Host: unlimited; Max Simultaneous TCP Sessions Per Scan: unlimited.

Buttons for "Cancel" and "Next" are located at the bottom right of the window.

### **Credentials**

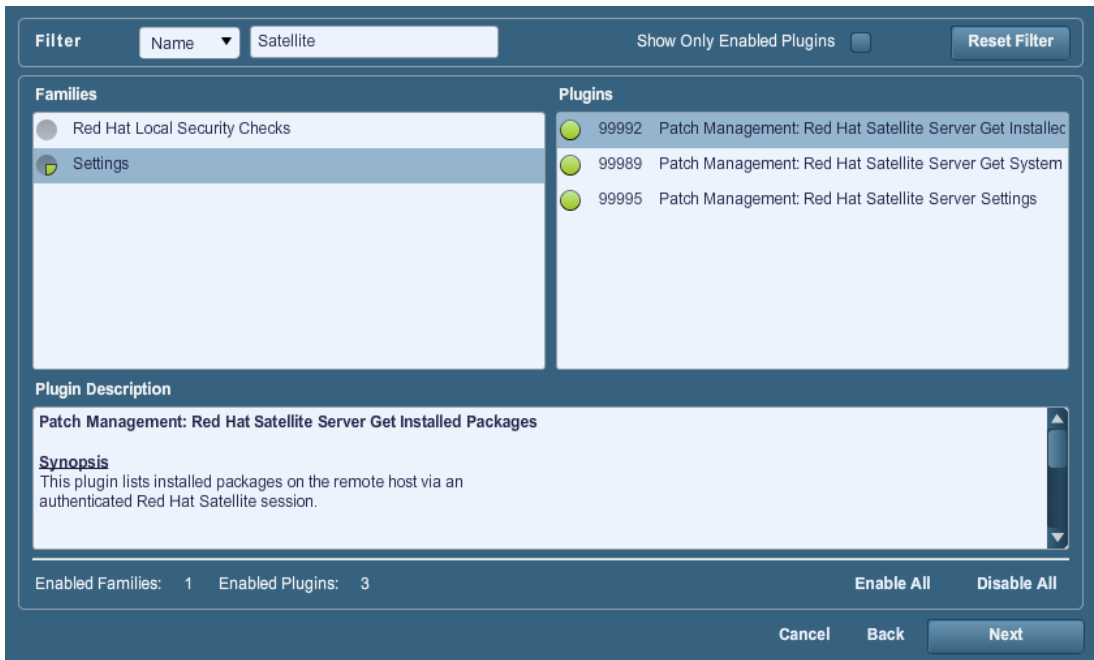
Because RHN Satellite scans do not rely on the system being managed to report patch management issues, credentials for the systems do not need to be used in the scan policy.

### **Plugins**

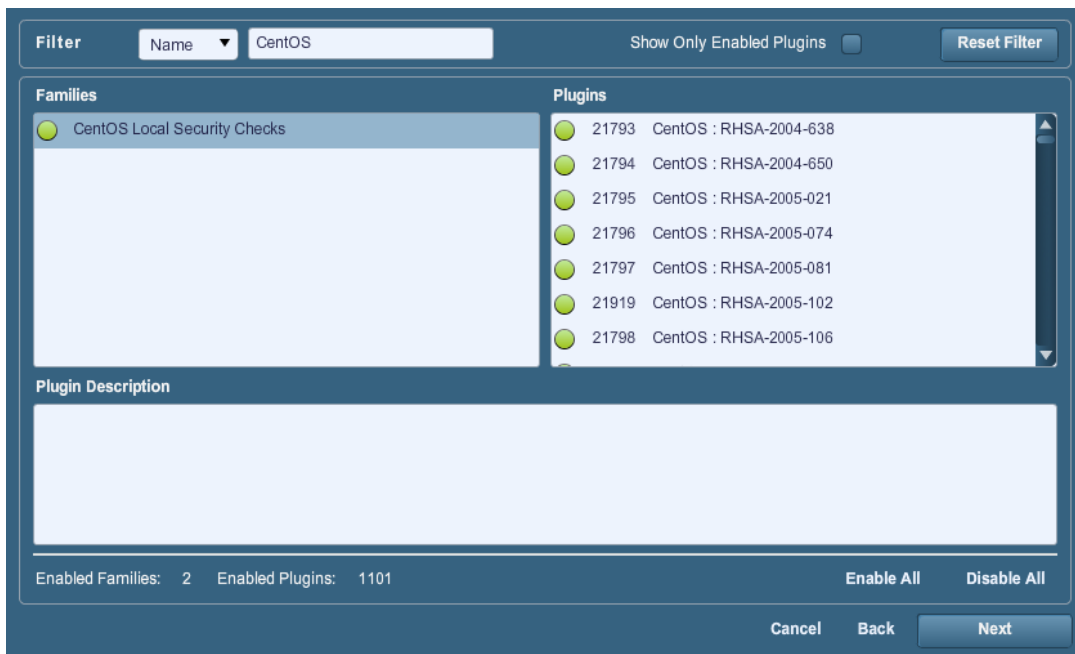
Make sure the following plugins are enabled under **"Plugins"** -> **"Families"** -> **"Settings"**:

- > Patch Management: Red Hat Satellite Server Get Installed Packages
- > Patch Management: Red Hat Satellite Server Get System
- > Patch Management: Red Hat Satellite Server Settings





In addition, enable the local operating system security check plugins of your choice. Nessus currently supports Red Hat Enterprise Server, Fedora, OpenSUSE, and CentOS in conjunction with the Red Hat Satellite Server plugins:



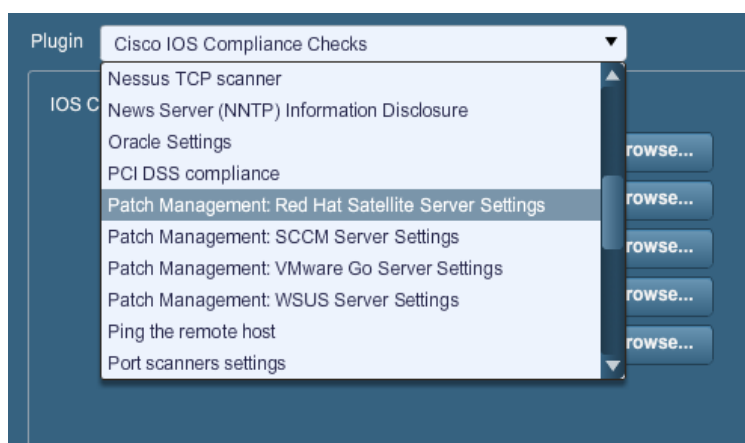
### Preferences

Credentials for the RHN Satellite server must be provided for scanning to work properly.

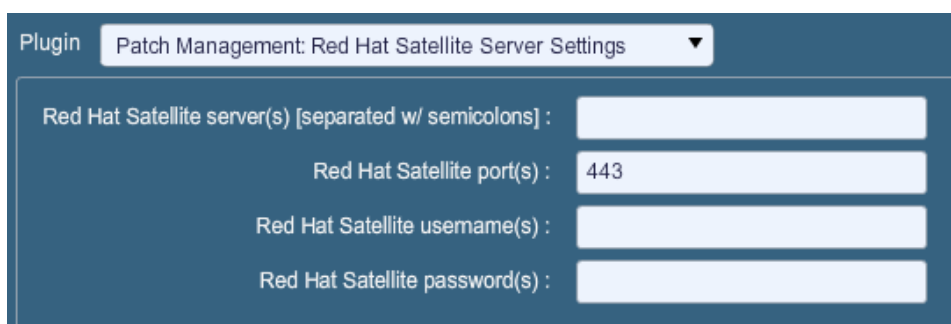
Credential	Description
------------	-------------

<b>Red Hat Satellite server(s)</b>	RHN Satellite IP address or system name
<b>Red Hat Satellite port(s)</b>	Port Satellite is running on (Typically TCP 80 or 443)
<b>Red Hat Satellite username(s)</b>	Satellite username
<b>Red Hat Satellite password(s)</b>	Satellite password

In the “**Preferences**” pane, select “**Patch Management: Red Hat Satellite Server Settings**” from the Plugin drop-down menu:



Enter the host, port, user, and password for your Satellite server:



Run the scan. The results of the scan will show which local checks fired:

228  0 / tcp List Detail 22 results

Plugin ID	Name	Port	Severity
99992	Patch Management: Red Hat Satellite Server Get Installed Packages	general/tcp	Low
99989	Patch Management: Red Hat Satellite Server Get System Information	general/tcp	Low
38896	CentOS : RHSA-2009-0411	general/tcp	Low
35310	CentOS : RHSA-2009-0004	general/tcp	Low
50804	CentOS : RHSA-2010-0819	general/tcp	High
53434	CentOS : RHSA-2011-0436	general/tcp	High
51146	CentOS : RHSA-2010-0978	general/tcp	High
48303	CentOS : RHSA-2010-0616	general/tcp	High
43658	CentOS : RHSA-2007-0964	general/tcp	Low
44677	CentOS : RHSA-2010-0108	general/tcp	Low
44097	CentOS : RHSA-2010-0054	general/tcp	Low
43734	CentOS : RHSA-2009-0361	general/tcp	Low
43798	CentOS : RHSA-2009-1471	general/tcp	Low
34463	CentOS : RHSA-2008-0946	general/tcp	Low
43785	CentOS : RHSA-2009-1335	general/tcp	Low
43726	CentOS : RHSA-2009-0013	general/tcp	Low
51885	CentOS : RHSA-2011-0170	general/tcp	High
47739	CentOS : RHSA-2010-0528	general/tcp	High

## **ABOUT TENABLE NETWORK SECURITY**

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit <http://www.tenable.com/>.

**Tenable Network Security, Inc.**  
7063 Columbia Gateway Drive  
Suite 100  
Columbia, MD 21046  
410.872.0555  
[www.tenable.com](http://www.tenable.com)