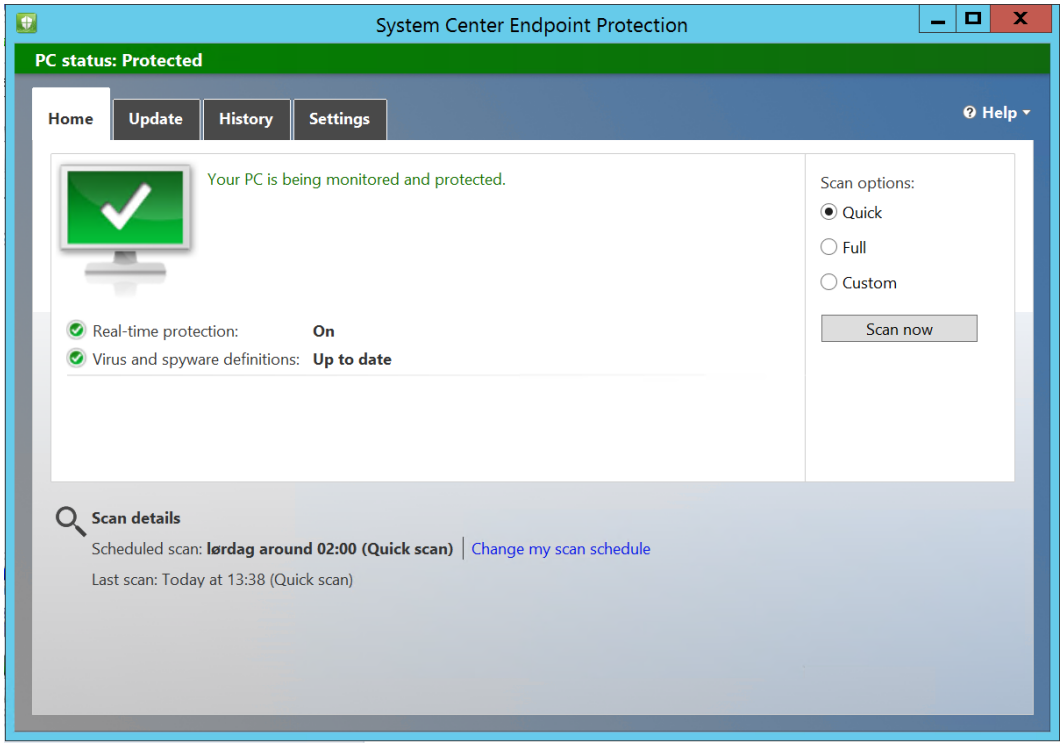
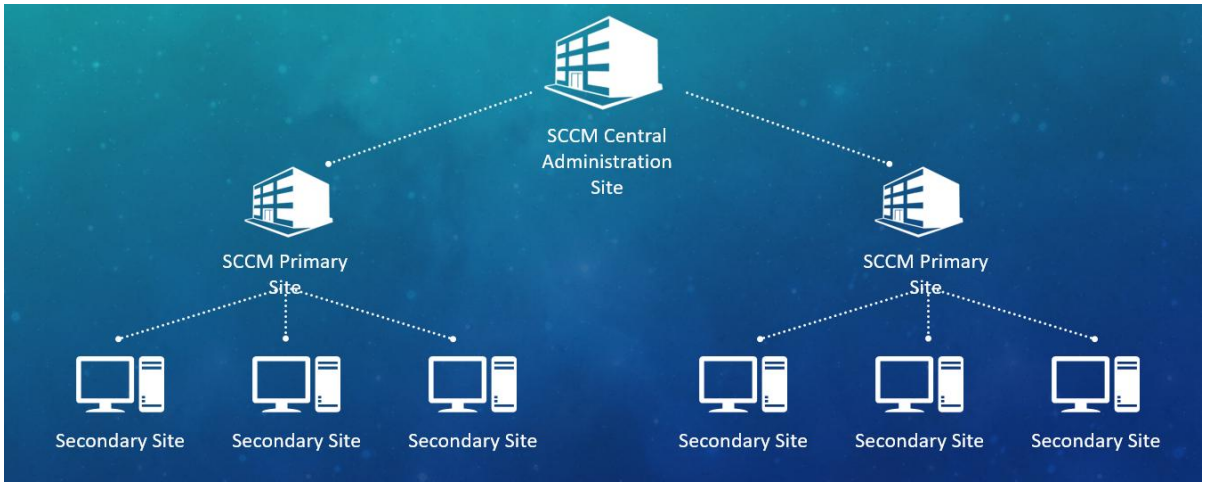
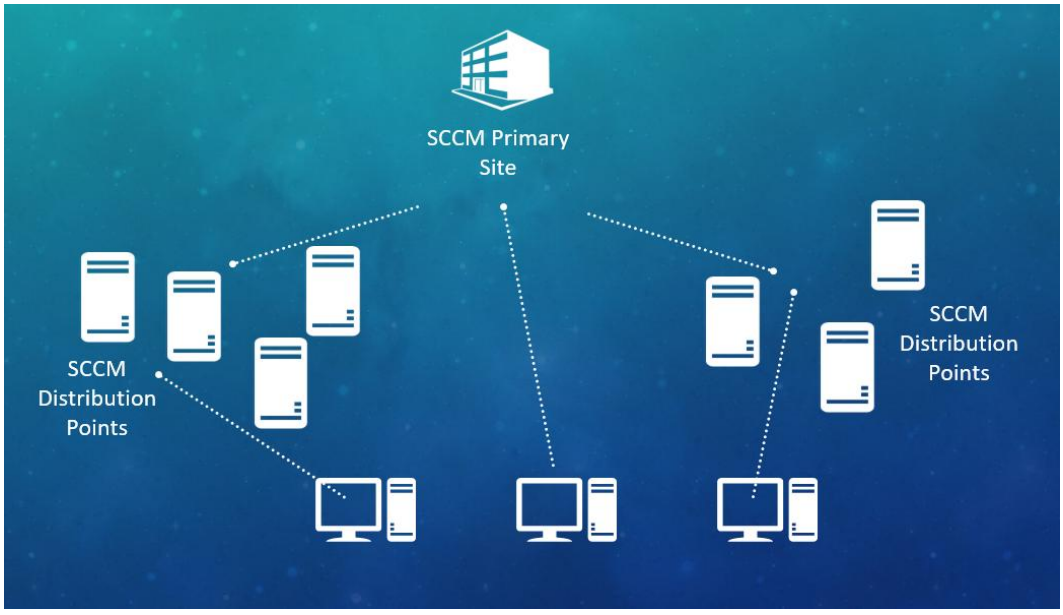
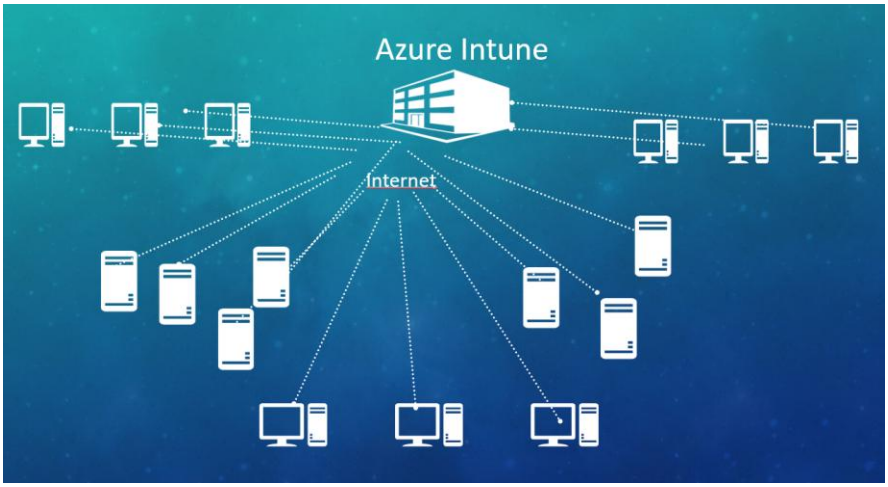
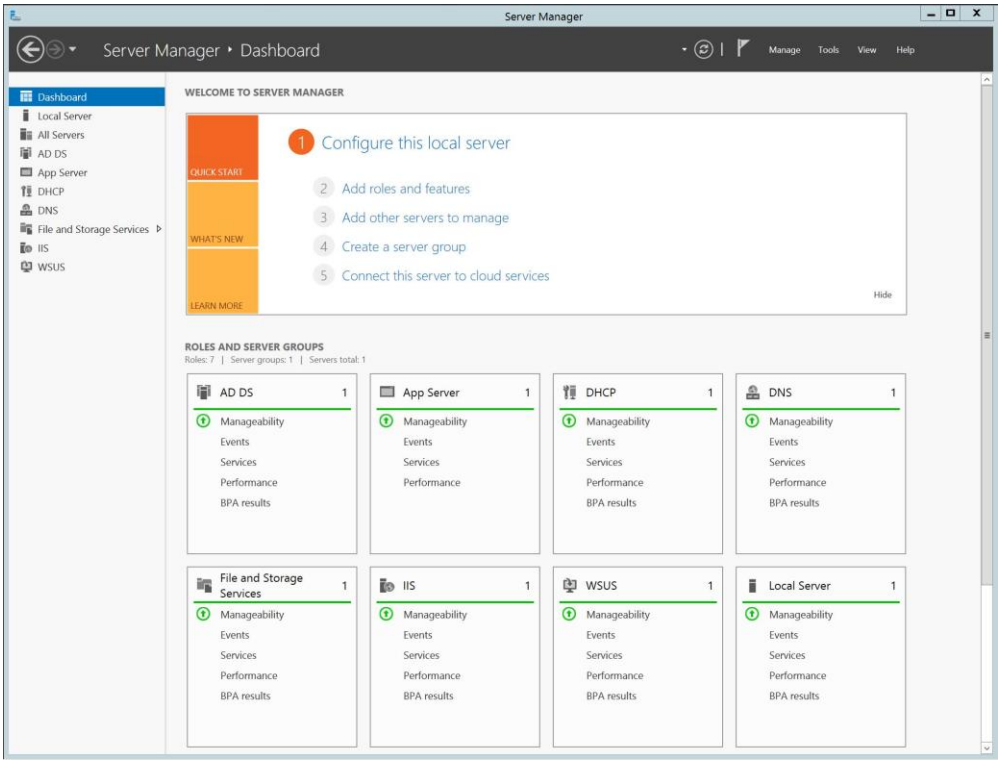
# Chapter 1: Planning and Getting Started with System Center Endpoint Protection

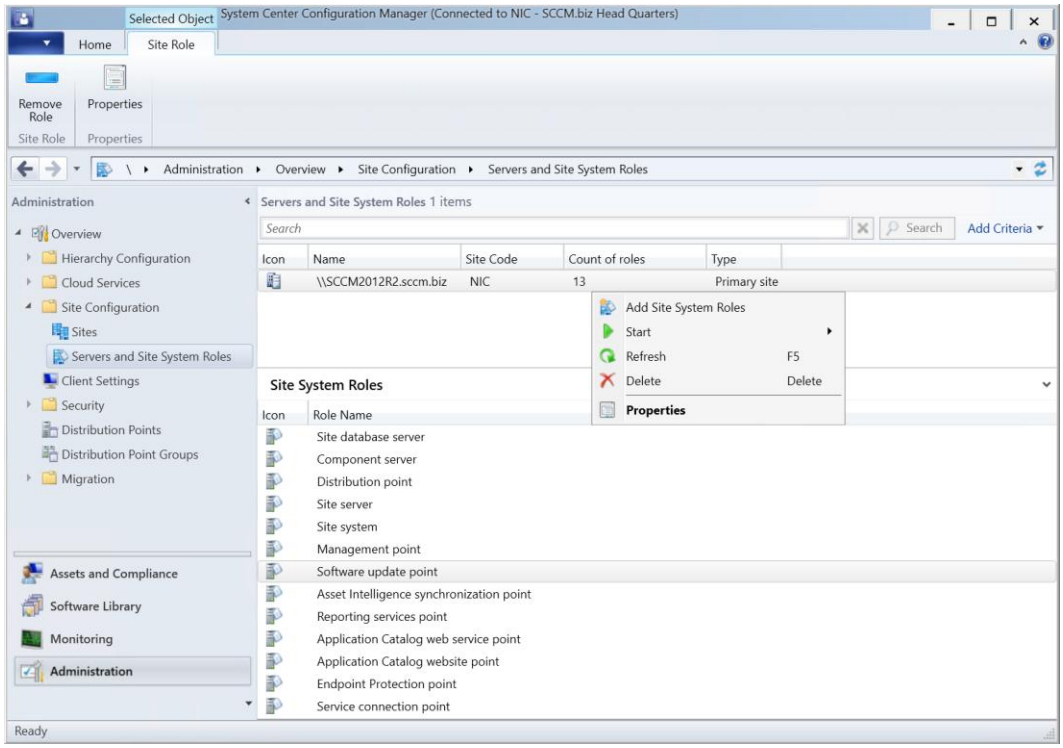


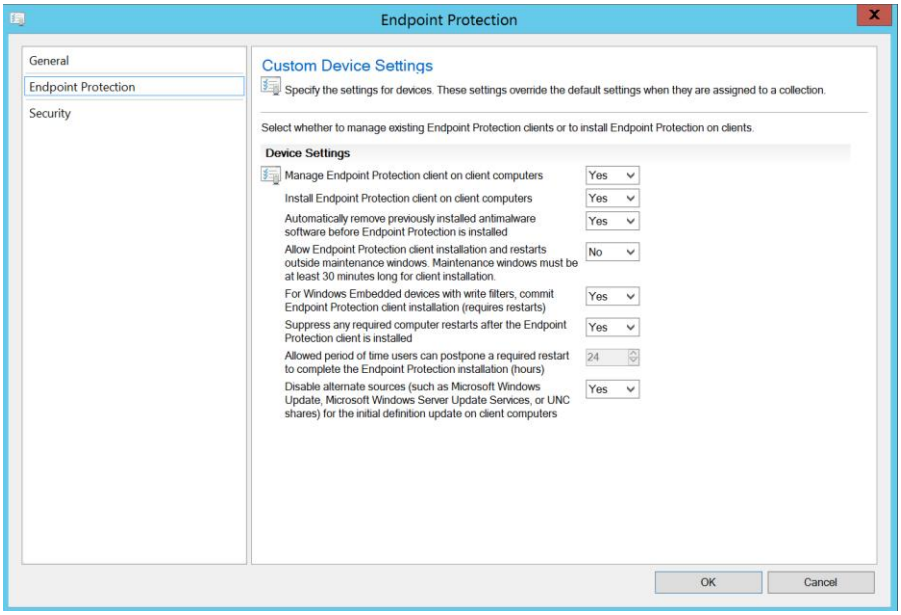

SCCM Central Administration Site
SCCM Primary Site
SCCM Primary Site
Secondary Site
Secondary Site
Secondary Site
Secondary Site
Secondary Site
Secondary Site


SCCM Primary Site
SCCM Distribution Points
SCCM Distribution Points

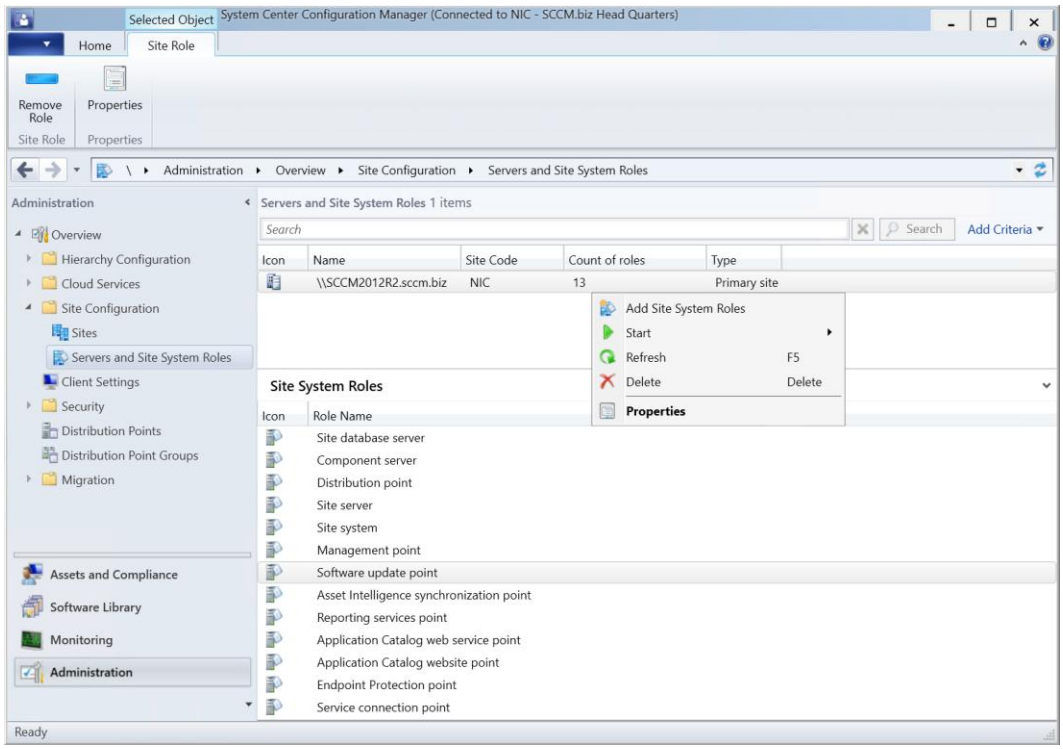

Azure Intune
Internet

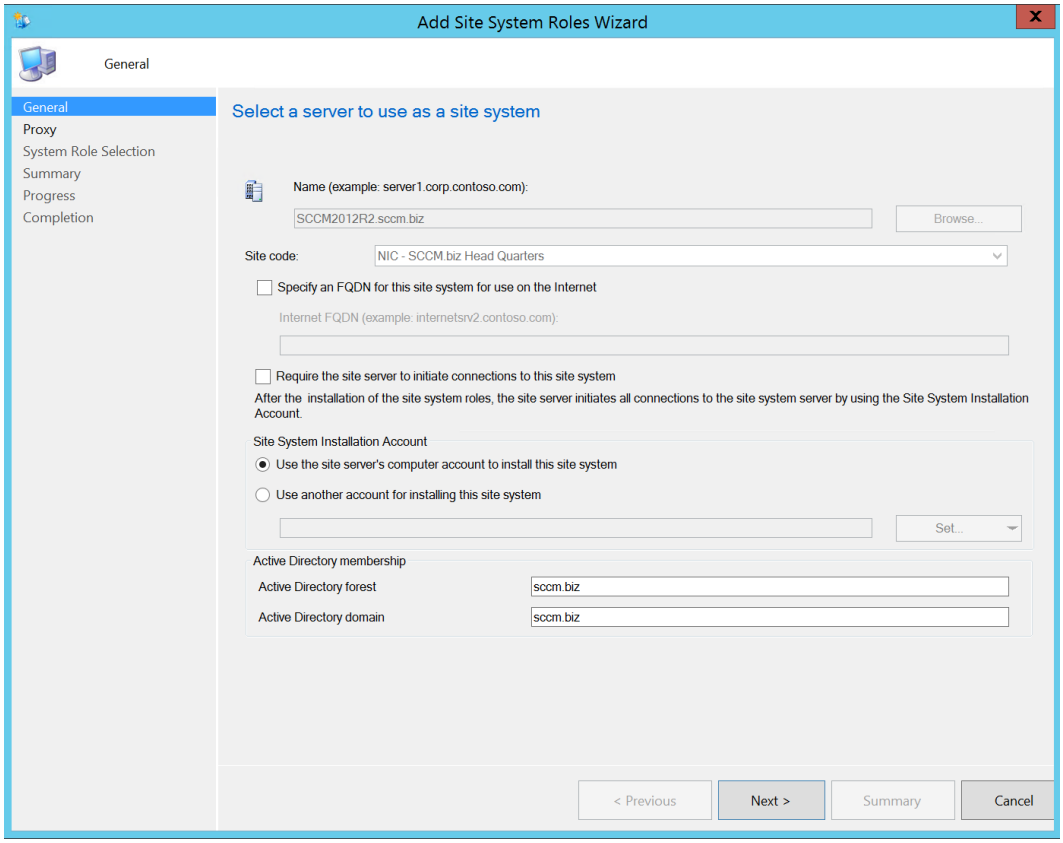

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
App Server
DHCP
DNS
File and Storage Services
IIS
WSUS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 7 | Server groups: 1 | Servers total: 1
AD DS 1
App Server 1
DHCP 1
DNS 1
File and Storage Services 1
IIS 1
WSUS 1
Local Server 1
Manageability
Events
Services
Performance
BPA results

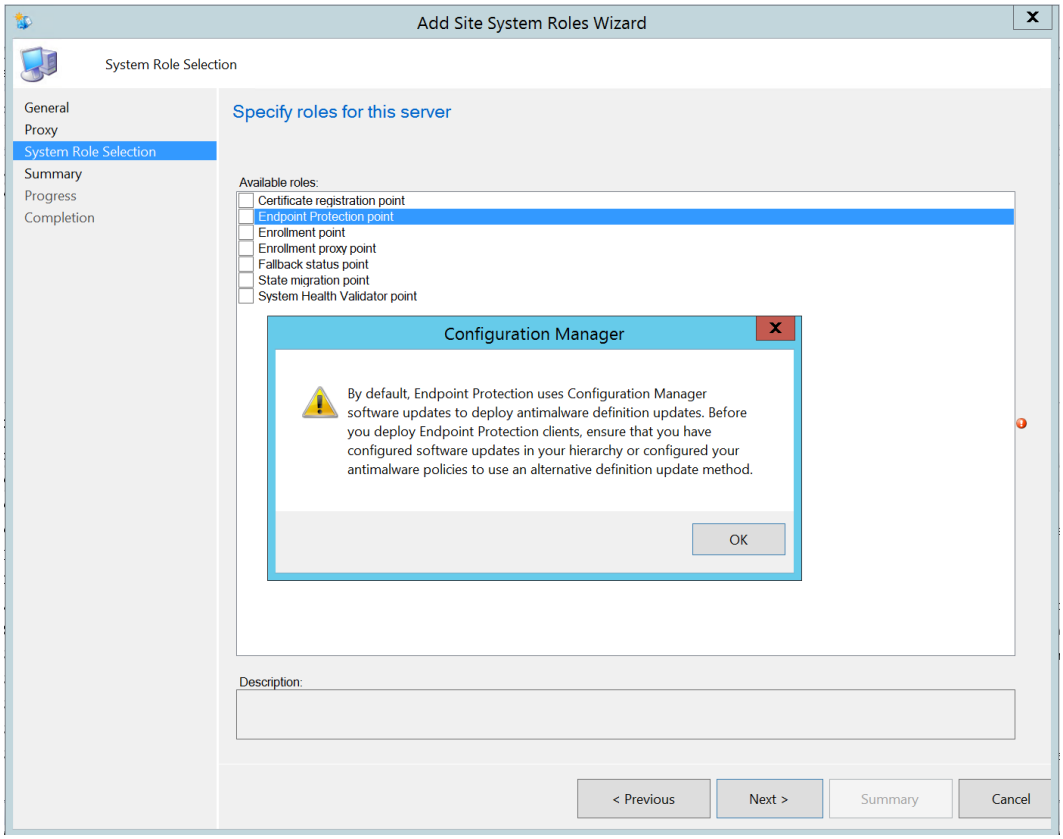

Selected Object
System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration ▸ Overview ▸ Site Configuration ▸ Servers and Site System Roles
Administration
Overview
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Assets and Compliance
Software Library
Monitoring
Administration
Servers and Site System Roles 1 items
Search
Add Criteria
Icon
Name
Site Code
Count of roles
Type
\\SCCM2012R2.sccm.biz
NIC
13
Primary site
Add Site System Roles
Start
Refresh
F5
Delete
Delete
Properties
Site System Roles
Icon
Role Name
Site database server
Component server
Distribution point
Site server
Site system
Management point
Software update point
Asset Intelligence synchronization point
Reporting services point
Application Catalog web service point
Application Catalog website point
Endpoint Protection point
Service connection point
Ready

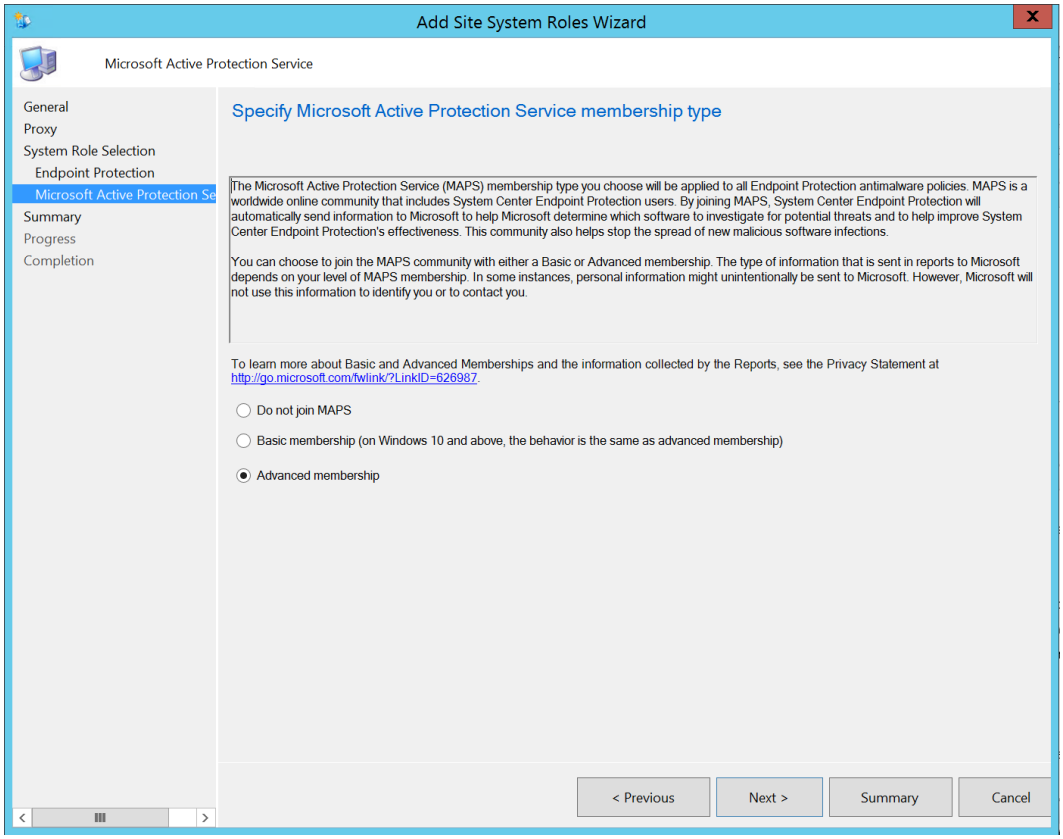

Endpoint Protection
General
Endpoint Protection
Security
Custom Device Settings
Specify the settings for devices. These settings override the default settings when they are assigned to a collection.
Select whether to manage existing Endpoint Protection clients or to install Endpoint Protection on clients.
Device Settings
Manage Endpoint Protection client on client computers
Yes
Install Endpoint Protection client on client computers
Yes
Automatically remove previously installed antimalware software before Endpoint Protection is installed
Yes
Allow Endpoint Protection client installation and restarts outside maintenance windows. Maintenance windows must be at least 30 minutes long for client installation.
No
For Windows Embedded devices with write filters, commit Endpoint Protection client installation (requires restarts)
Yes
Suppress any required computer restarts after the Endpoint Protection client is installed
Yes
Allowed period of time users can postpone a required restart to complete the Endpoint Protection installation (hours)
24
Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial definition update on client computers
Yes
OK
Cancel

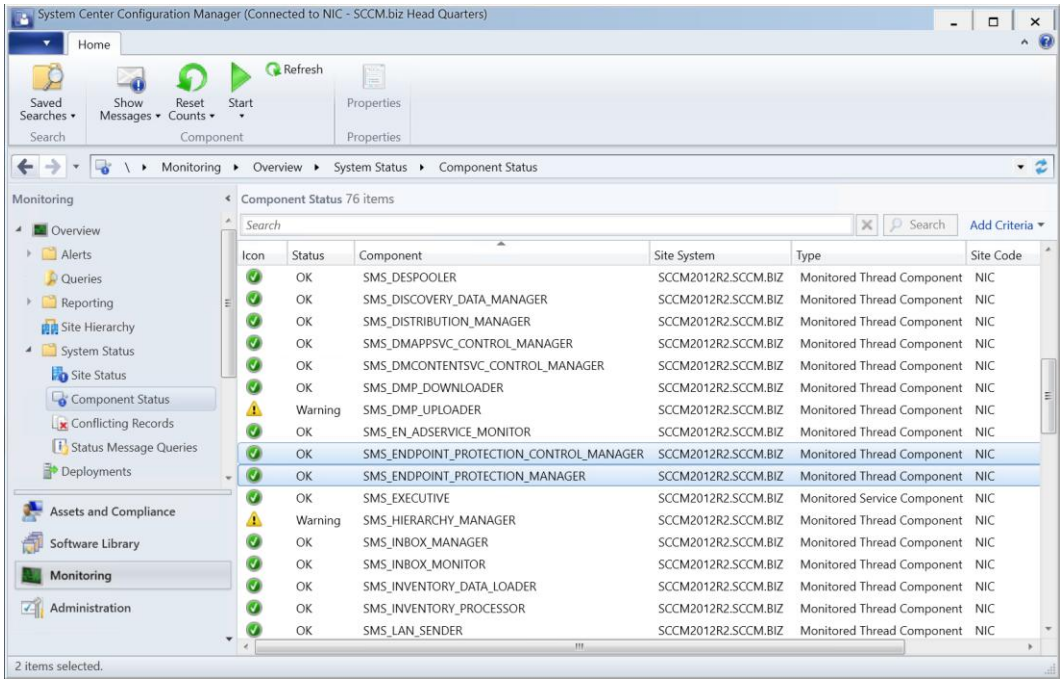
# Chapter 2: Configuring Endpoint Protection in Configuration Manager

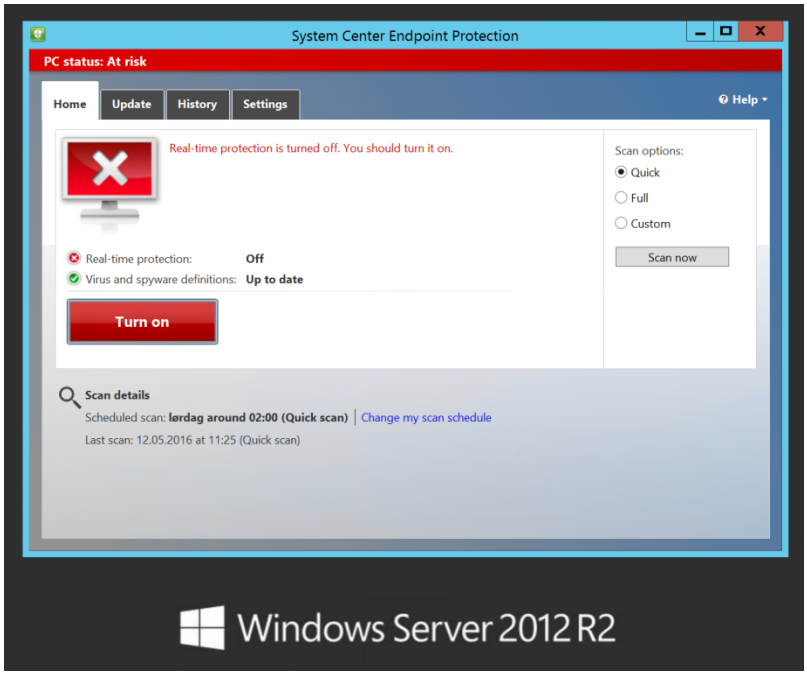


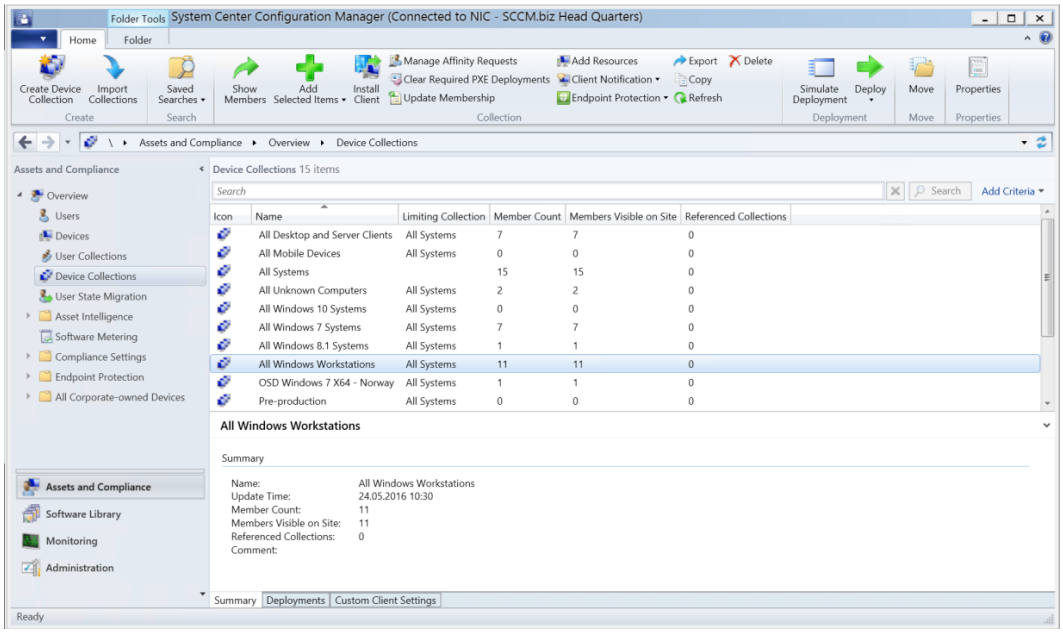

Add Site System Roles Wizard
General
General
Proxy
System Role Selection
Summary
Progress
Completion
Select a server to use as a site system
Name (example: server1.corp.contoso.com):
SCCM2012R2.sccm.biz
Browse...
Site code:
NIC - SCCM.biz Head Quarters
Specify an FQDN for this site system for use on the Internet
Internet FQDN (example: internetsrv2.contoso.com):
Require the site server to initiate connections to this site system
After the installation of the site system roles, the site server initiates all connections to the site system server by using the Site System Installation Account.
Site System Installation Account
Use the site server's computer account to install this site system
Use another account for installing this site system
Set...
Active Directory membership
Active Directory forest
sccm.biz
Active Directory domain
sccm.biz
< Previous
Next >
Summary
Cancel

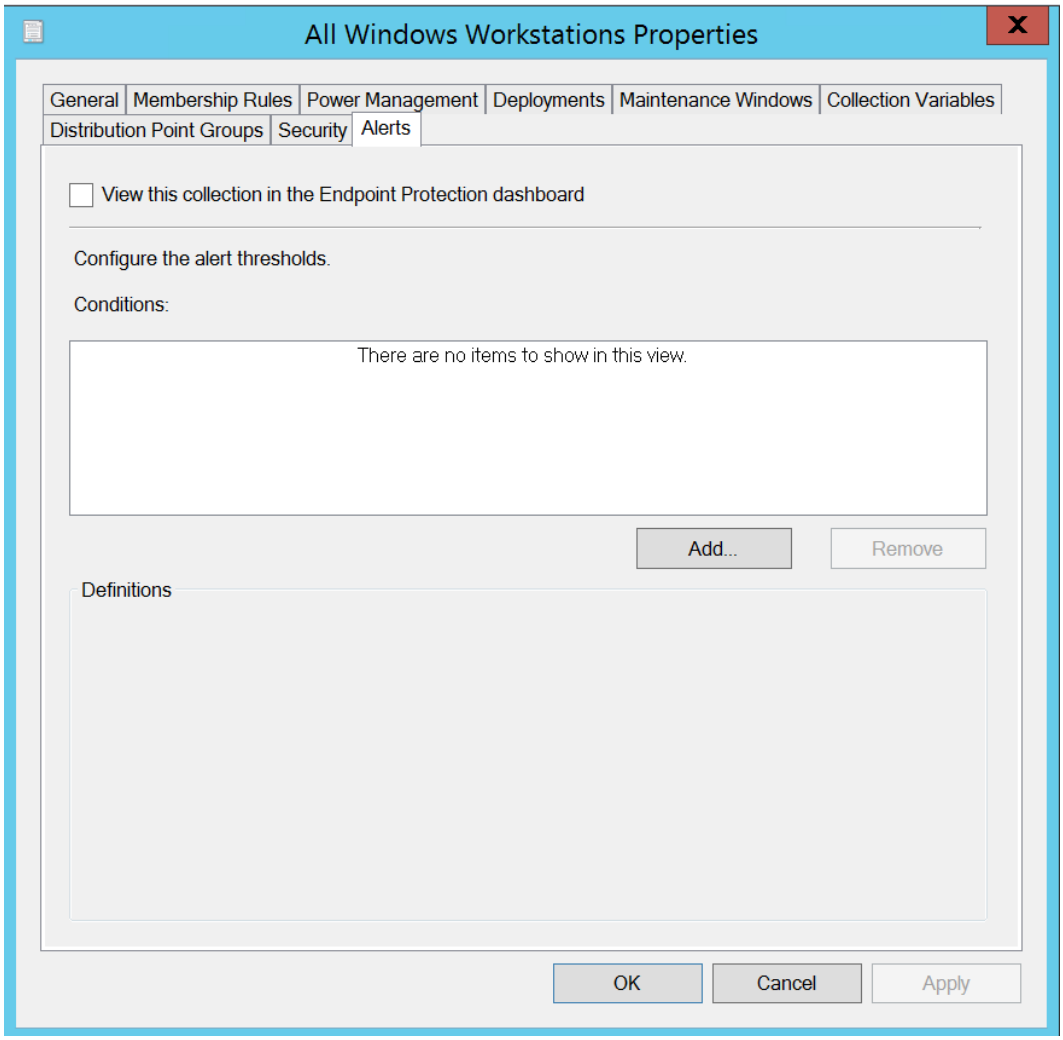

Add Site System Roles Wizard
System Role Selection
General
Proxy
System Role Selection
Summary
Progress
Completion
Specify roles for this server
Available roles:
Certificate registration point
Endpoint Protection point
Enrollment point
Enrollment proxy point
Fallback status point
State migration point
System Health Validator point
Configuration Manager
By default, Endpoint Protection uses Configuration Manager software updates to deploy antimalware definition updates. Before you deploy Endpoint Protection clients, ensure that you have configured software updates in your hierarchy or configured your antimalware policies to use an alternative definition update method.
OK
Description:
< Previous
Next >
Summary
Cancel

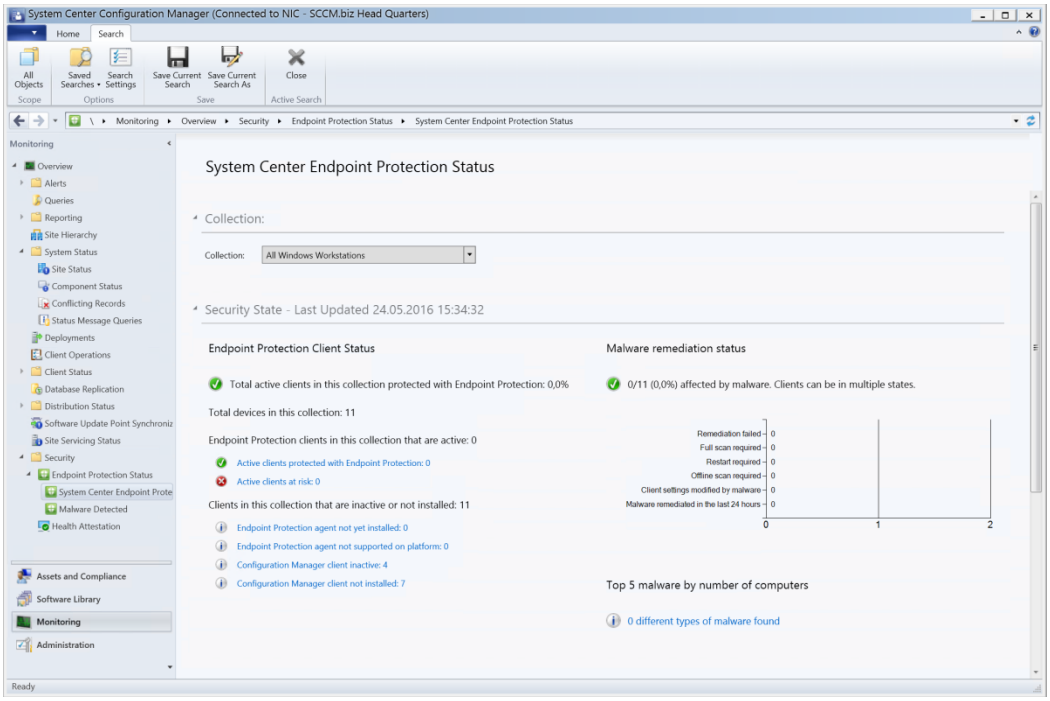

Add Site System Roles Wizard
Microsoft Active Protection Service
General
Proxy
System Role Selection
Endpoint Protection
Microsoft Active Protection Se
Summary
Progress
Completion
Specify Microsoft Active Protection Service membership type
The Microsoft Active Protection Service (MAPS) membership type you choose will be applied to all Endpoint Protection antimalware policies. MAPS is a worldwide online community that includes System Center Endpoint Protection users. By joining MAPS, System Center Endpoint Protection will automatically send information to Microsoft to help Microsoft determine which software to investigate for potential threats and to help improve System Center Endpoint Protection's effectiveness. This community also helps stop the spread of new malicious software infections.
You can choose to join the MAPS community with either a Basic or Advanced membership. The type of information that is sent in reports to Microsoft depends on your level of MAPS membership. In some instances, personal information might unintentionally be sent to Microsoft. However, Microsoft will not use this information to identify you or to contact you.
To learn more about Basic and Advanced Memberships and the information collected by the Reports, see the Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=626987.
Do not join MAPS
Basic membership (on Windows 10 and above, the behavior is the same as advanced membership)
Advanced membership
< Previous
Next >
Summary
Cancel

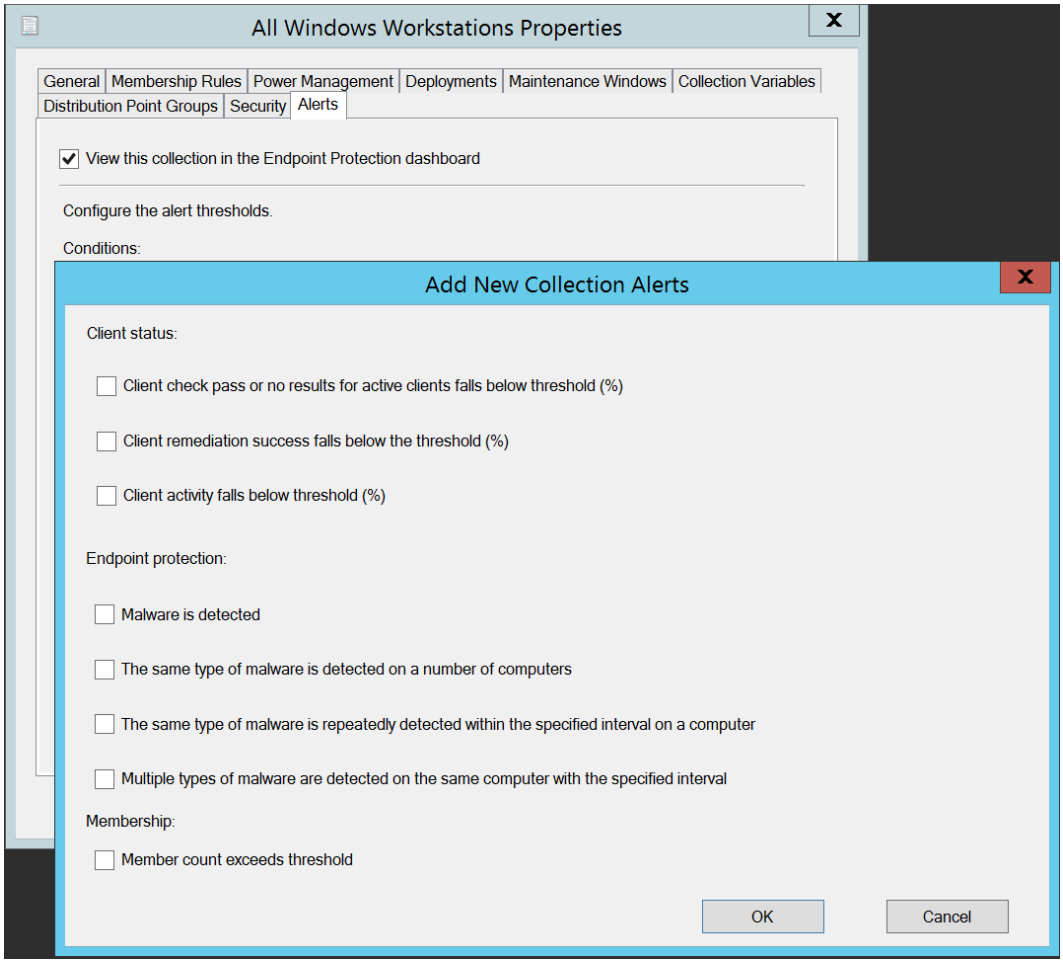

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Saved Searches
Show Messages
Reset Counts
Start
Refresh
Properties
Search
Component
Properties
Monitoring ▸ Overview ▸ System Status ▸ Component Status
Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Site Status
Component Status
Conflicting Records
Status Message Queries
Deployments
Assets and Compliance
Software Library
Monitoring
Administration
Component Status 76 items
Search
Add Criteria
Icon | Status | Component | Site System | Type | Site Code
OK | SMS_DESPOOLER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_DISCOVERY_DATA_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_DISTRIBUTION_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_DMAPPSVC_CONTROL_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_DMCONTENTSVC_CONTROL_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_DMP_DOWNLOADER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
Warning | SMS_DMP_UPLOADER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_EN_ADSERVICE_MONITOR | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_ENDPOINT_PROTECTION_CONTROL_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_ENDPOINT_PROTECTION_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_EXECUTIVE | SCCM2012R2.SCCM.BIZ | Monitored Service Component | NIC
Warning | SMS_HIERARCHY_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_INBOX_MANAGER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_INBOX_MONITOR | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_INVENTORY_DATA_LOADER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_INVENTORY_PROCESSOR | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
OK | SMS_LAN_SENDER | SCCM2012R2.SCCM.BIZ | Monitored Thread Component | NIC
2 items selected.

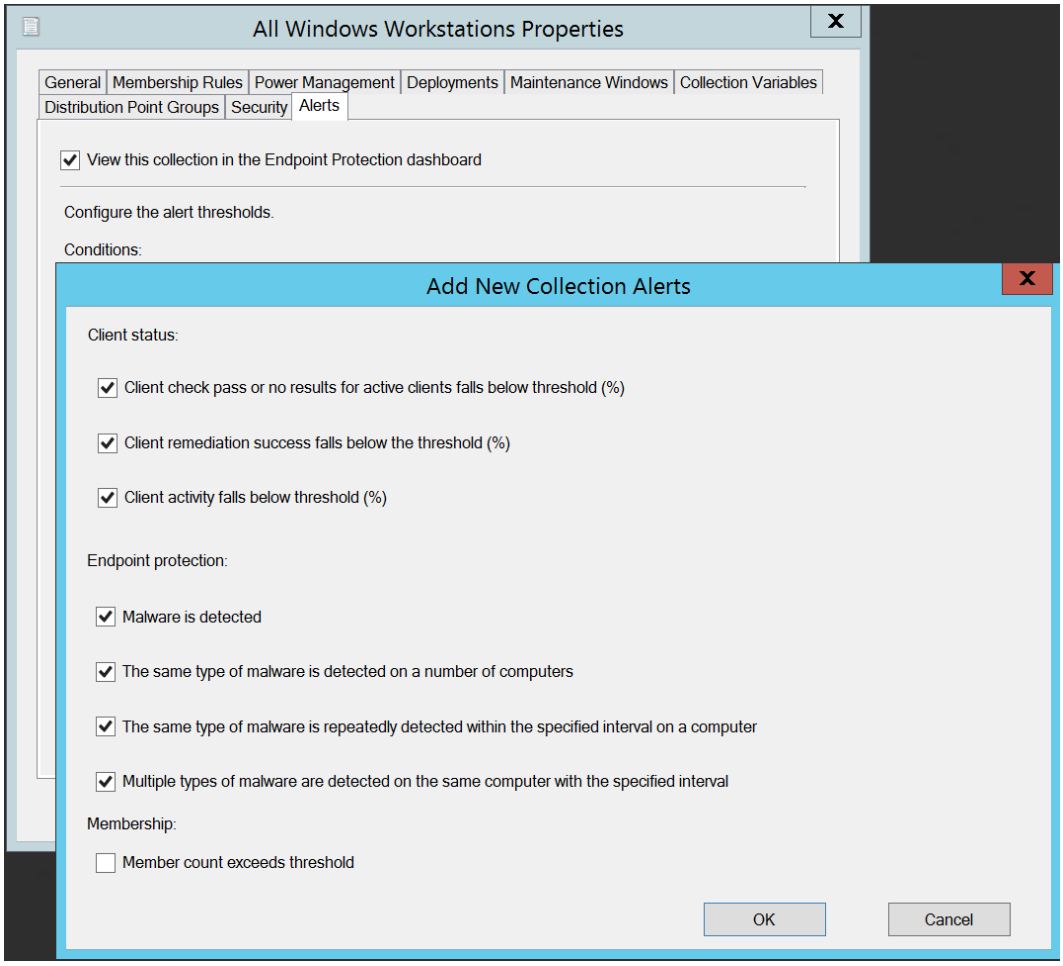

System Center Endpoint Protection
PC status: At risk
Home
Update
History
Settings
Help
Real-time protection is turned off. You should turn it on.
Scan options:
Quick
Full
Custom
Scan now
Real-time protection: Off
Virus and spyware definitions: Up to date
Turn on
Scan details
Scheduled scan: lørdag around 02:00 (Quick scan) | Change my scan schedule
Last scan: 12.05.2016 at 11:25 (Quick scan)
Windows Server 2012 R2

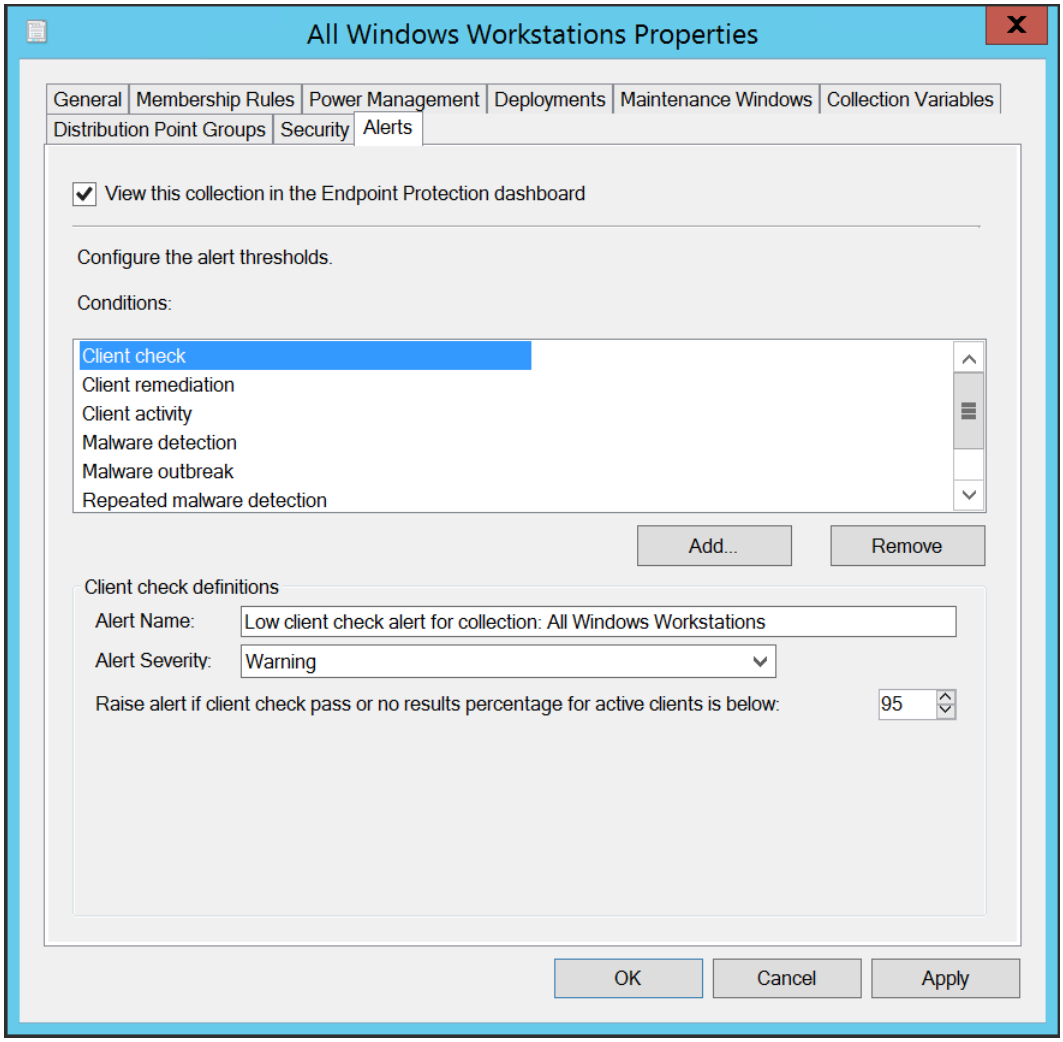

Folder Tools
System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Folder
Create Device Collection
Import Collections
Create
Saved Searches
Search
Show Members
Add Selected Items
Install Client
Manage Affinity Requests
Clear Required PXE Deployments
Update Membership
Add Resources
Client Notification
Endpoint Protection
Export
Copy
Refresh
Delete
Collection
Simulate Deployment
Deploy
Deployment
Move
Move
Properties
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Device Collections
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Device Collections 15 items
Search
Search
Add Criteria
Icon
Name
Limiting Collection
Member Count
Members Visible on Site
Referenced Collections
All Desktop and Server Clients All Systems 7 7 0
All Mobile Devices All Systems 0 0 0
All Systems 15 15 0
All Unknown Computers All Systems 2 2 0
All Windows 10 Systems All Systems 0 0 0
All Windows 7 Systems All Systems 7 7 0
All Windows 8.1 Systems All Systems 1 1 0
All Windows Workstations All Systems 11 11 0
OSD Windows 7 X64 - Norway All Systems 1 1 0
Pre-production All Systems 0 0 0
All Windows Workstations
Summary
Name: All Windows Workstations
Update Time: 24.05.2016 10:30
Member Count: 11
Members Visible on Site: 11
Referenced Collections: 0
Comment:
Summary
Deployments
Custom Client Settings
Ready

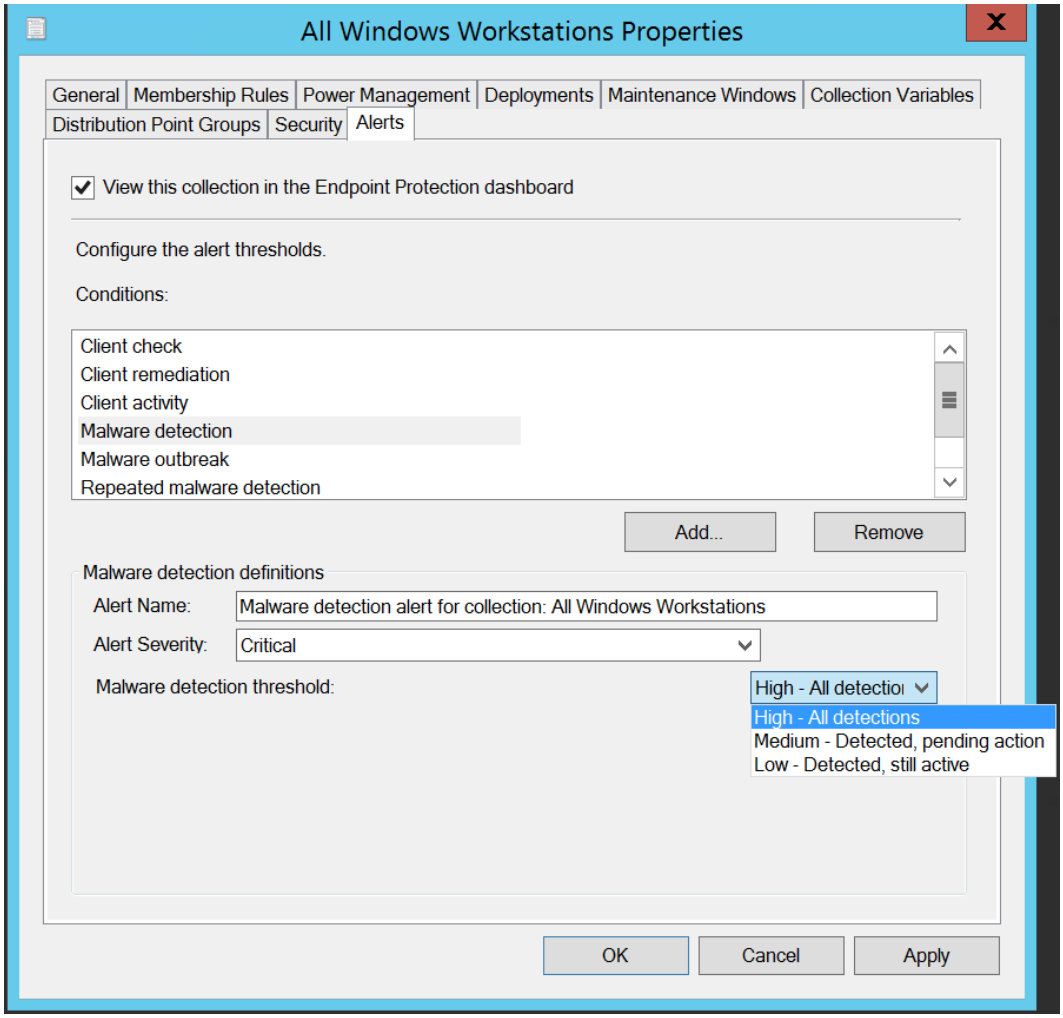

All Windows Workstations Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
There are no items to show in this view.
Add...
Remove
Definitions
OK
Cancel
Apply

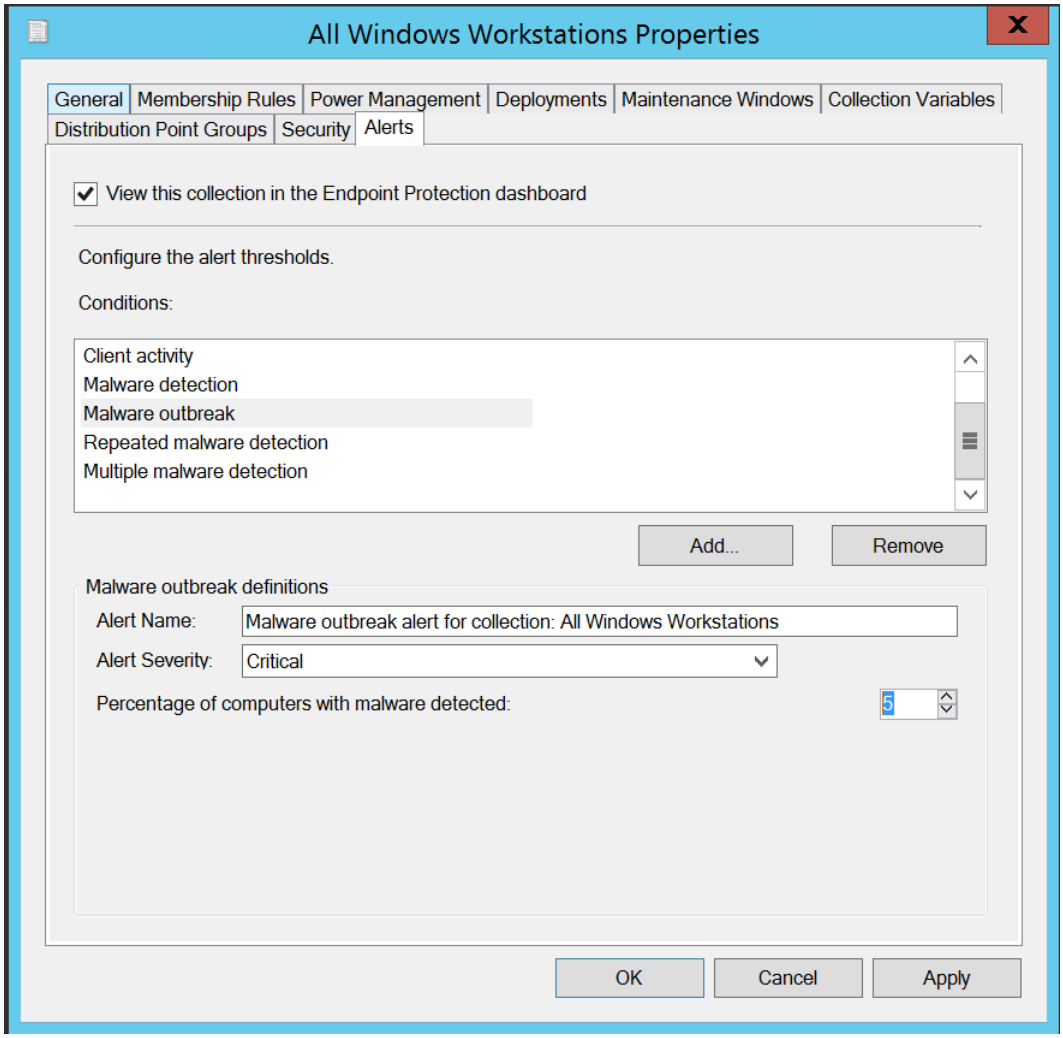

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Search
All Objects
Saved Searches
Search Settings
Save Current Search
Save Current Search As
Close
Scope
Options
Save
Active Search
Monitoring ▸ Overview ▸ Security ▸ Endpoint Protection Status ▸ System Center Endpoint Protection Status
Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Site Status
Component Status
Conflicting Records
Status Message Queries
Deployments
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchroniz
Site Servicing Status
Security
Endpoint Protection Status
System Center Endpoint Prote
Malware Detected
Health Attestation
Assets and Compliance
Software Library
Monitoring
Administration
System Center Endpoint Protection Status
Collection:
Collection: All Windows Workstations
Security State - Last Updated 24.05.2016 15:34:32
Endpoint Protection Client Status
Total active clients in this collection protected with Endpoint Protection: 0,0%
Total devices in this collection: 11
Endpoint Protection clients in this collection that are active: 0
Active clients protected with Endpoint Protection: 0
Active clients at risk: 0
Clients in this collection that are inactive or not installed: 11
Endpoint Protection agent not yet installed: 0
Endpoint Protection agent not supported on platform: 0
Configuration Manager client inactive: 4
Configuration Manager client not installed: 7
Malware remediation status
0/11 (0,0%) affected by malware. Clients can be in multiple states.
Remediation failed 0
Full scan required 0
Restart required 0
Offline scan required 0
Client settings modified by malware 0
Malware remediated in the last 24 hours 0
0
1
2
Top 5 malware by number of computers
0 different types of malware found
Ready

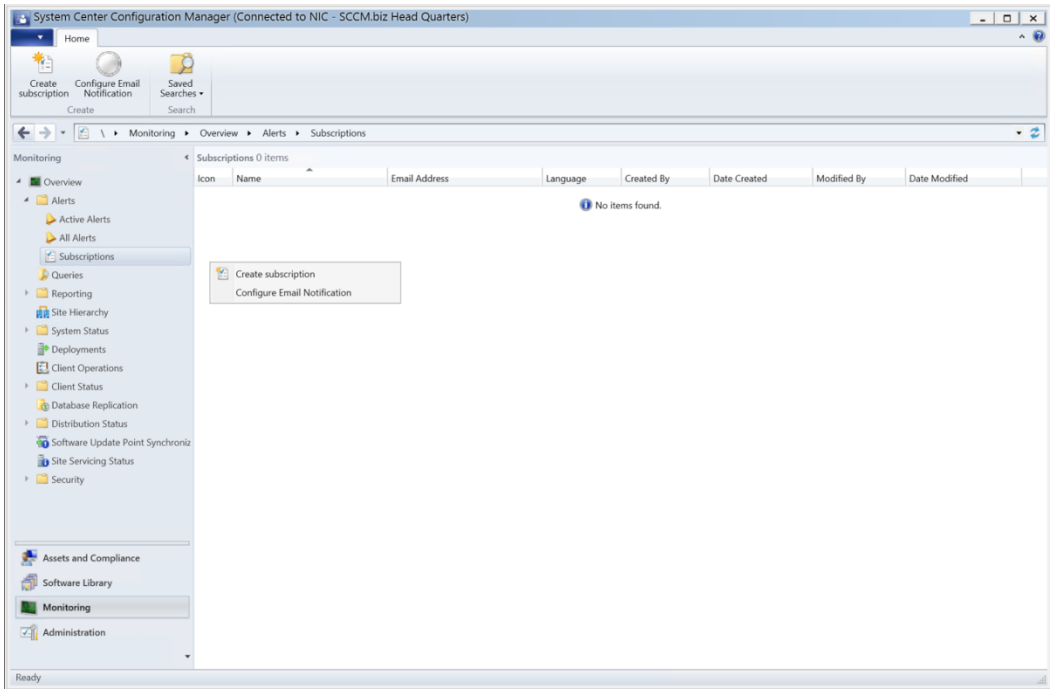

All Windows Workstations Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
Add New Collection Alerts
Client status:
Client check pass or no results for active clients falls below threshold (%)
Client remediation success falls below the threshold (%)
Client activity falls below threshold (%)
Endpoint protection:
Malware is detected
The same type of malware is detected on a number of computers
The same type of malware is repeatedly detected within the specified interval on a computer
Multiple types of malware are detected on the same computer with the specified interval
Membership:
Member count exceeds threshold
OK
Cancel

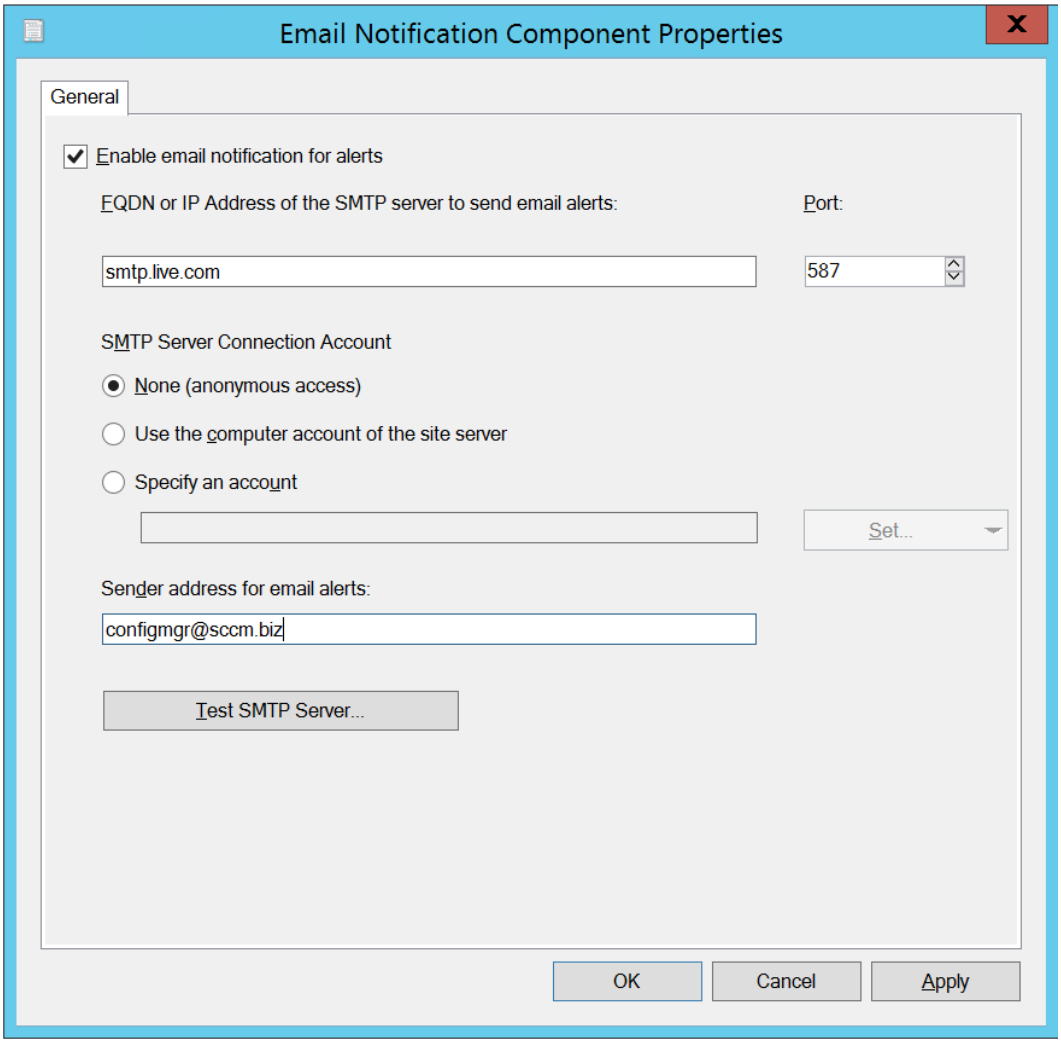

All Windows Workstations Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
Add New Collection Alerts
Client status:
Client check pass or no results for active clients falls below threshold (%)
Client remediation success falls below the threshold (%)
Client activity falls below threshold (%)
Endpoint protection:
Malware is detected
The same type of malware is detected on a number of computers
The same type of malware is repeatedly detected within the specified interval on a computer
Multiple types of malware are detected on the same computer with the specified interval
Membership:
Member count exceeds threshold
OK
Cancel

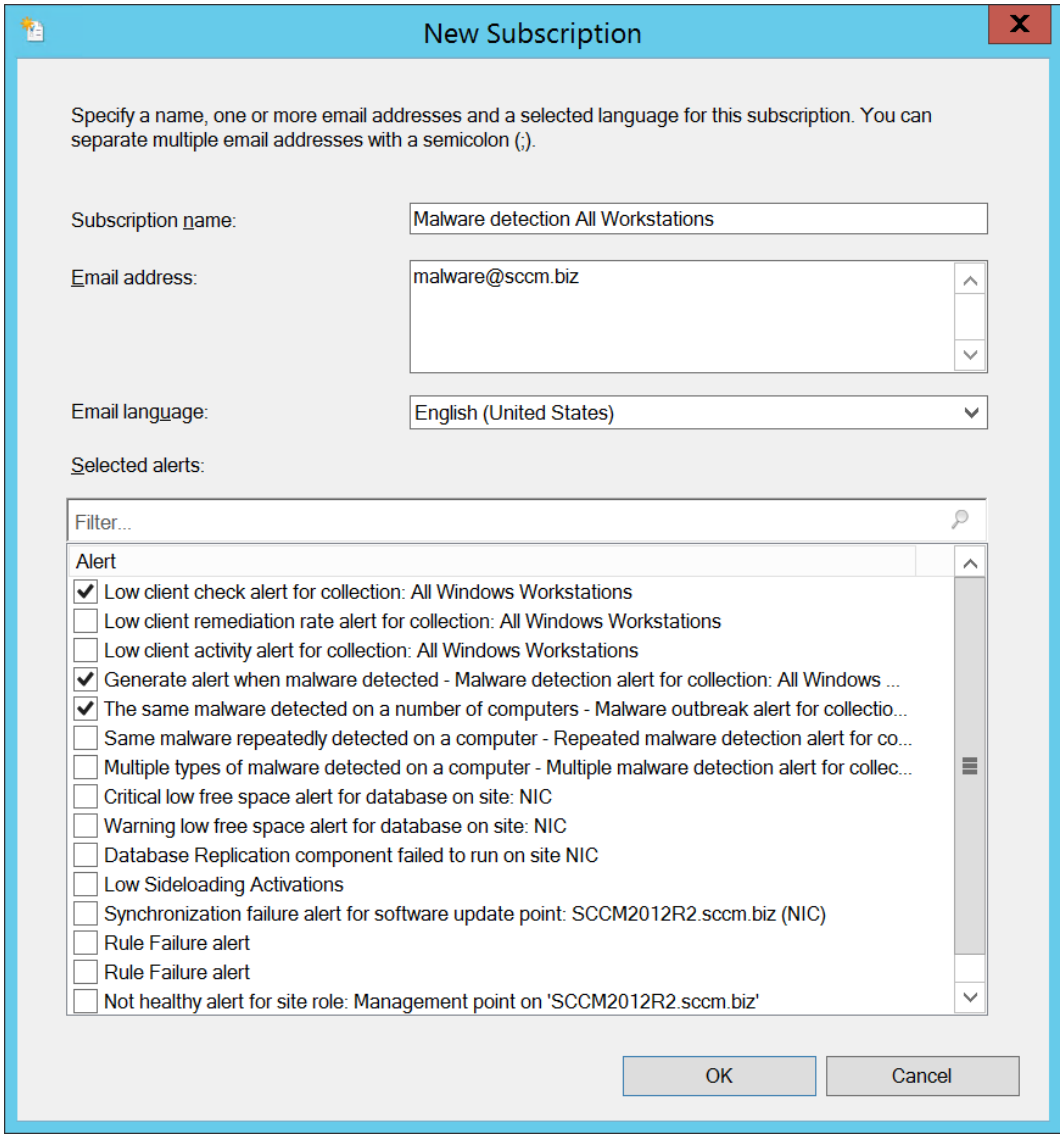

All Windows Workstations Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
Client check
Client remediation
Client activity
Malware detection
Malware outbreak
Repeated malware detection
Add...
Remove
Client check definitions
Alert Name:
Low client check alert for collection: All Windows Workstations
Alert Severity:
Warning
Raise alert if client check pass or no results percentage for active clients is below:
95
OK
Cancel
Apply

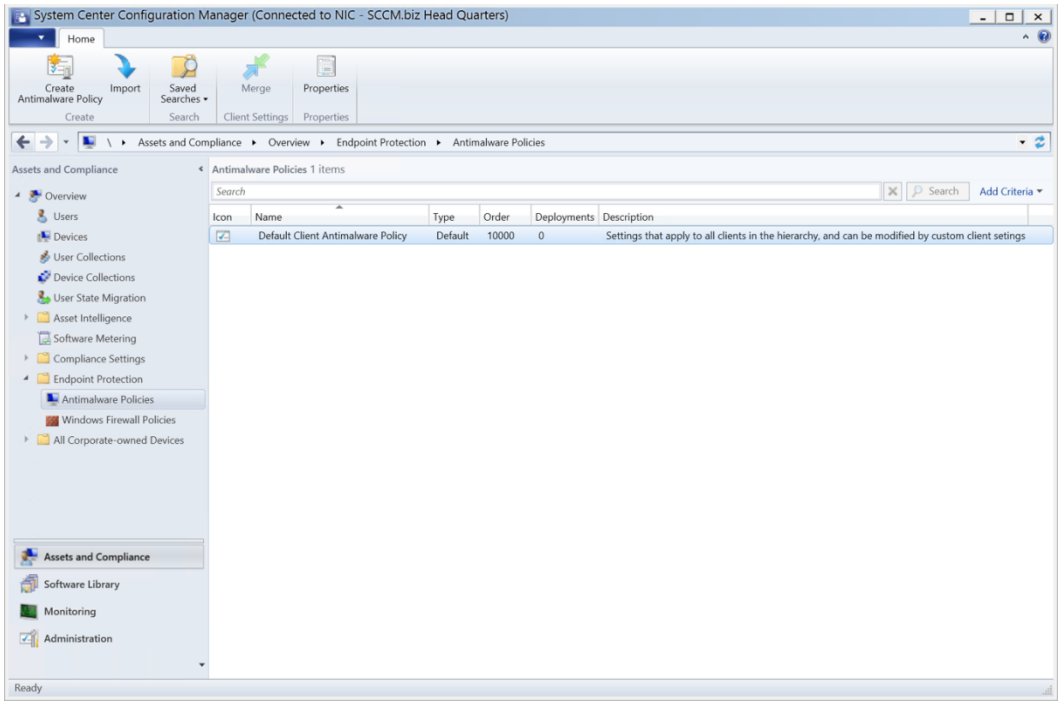

All Windows Workstations Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
Client check
Client remediation
Client activity
Malware detection
Malware outbreak
Repeated malware detection
Add...
Remove
Malware detection definitions
Alert Name:
Malware detection alert for collection: All Windows Workstations
Alert Severity:
Critical
Malware detection threshold:
High - All detectio
High - All detections
Medium - Detected, pending action
Low - Detected, still active
OK
Cancel
Apply

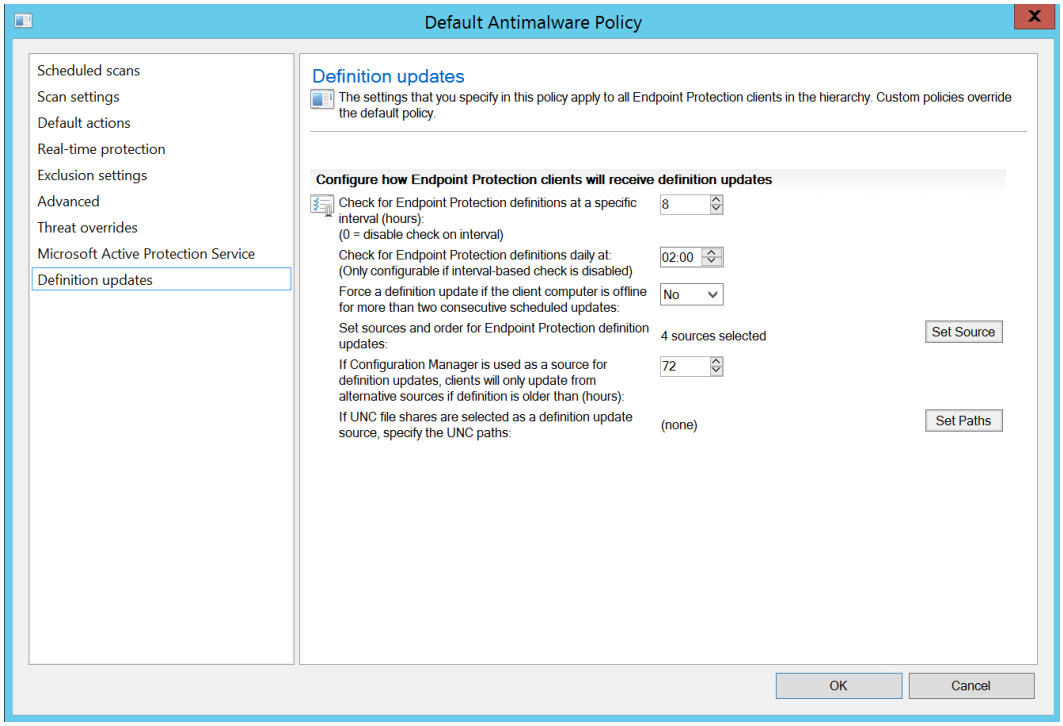

All Windows Workstations Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
Client activity
Malware detection
Malware outbreak
Repeated malware detection
Multiple malware detection
Add...
Remove
Malware outbreak definitions
Alert Name:
Malware outbreak alert for collection: All Windows Workstations
Alert Severity:
Critical
Percentage of computers with malware detected:
5
OK
Cancel
Apply

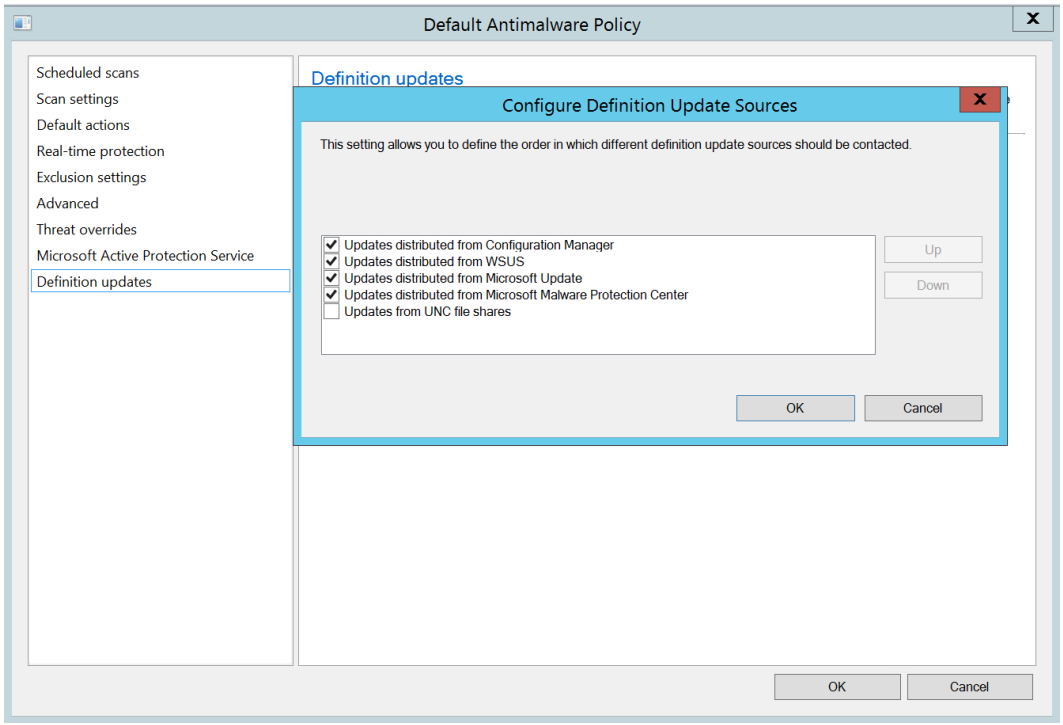

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create subscription
Configure Email Notification
Saved Searches
Create
Search
Monitoring ▸ Overview ▸ Alerts ▸ Subscriptions
Monitoring
Overview
Alerts
Active Alerts
All Alerts
Subscriptions
Queries
Reporting
Site Hierarchy
System Status
Deployments
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchroniz
Site Servicing Status
Security
Assets and Compliance
Software Library
Monitoring
Administration
Subscriptions 0 items
Icon
Name
Email Address
Language
Created By
Date Created
Modified By
Date Modified
No items found.
Create subscription
Configure Email Notification
Ready

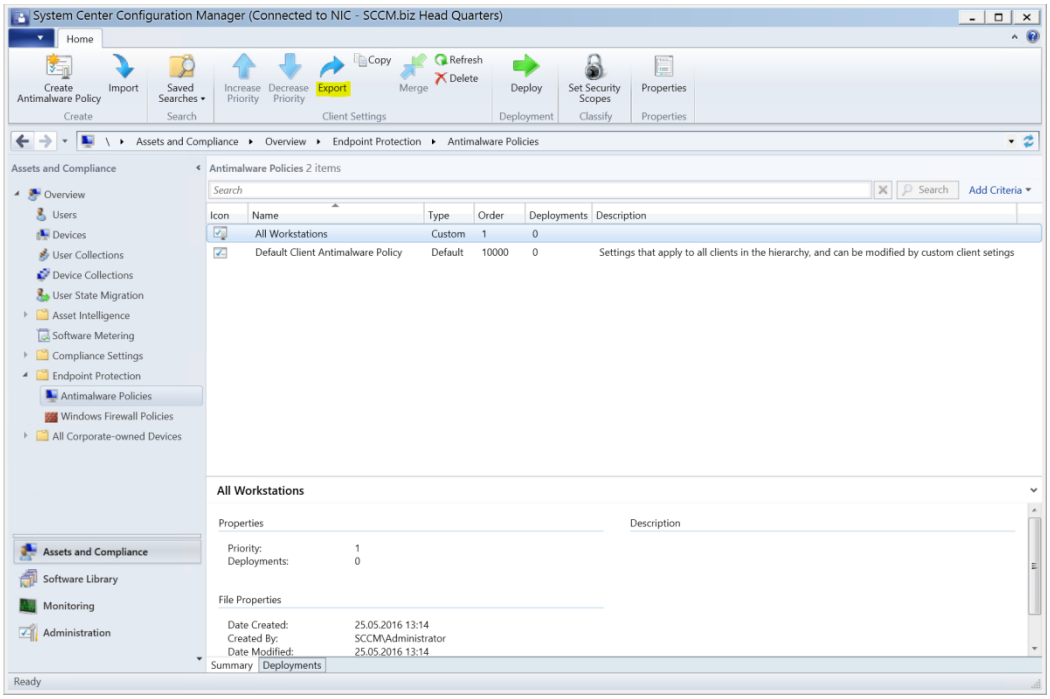

Email Notification Component Properties
General
Enable email notification for alerts
FQDN or IP Address of the SMTP server to send email alerts:
Port:
smtp.live.com
587
SMTP Server Connection Account
None (anonymous access)
Use the computer account of the site server
Specify an account
Set...
Sender address for email alerts:
configmgr@sccm.biz
Test SMTP Server...
OK
Cancel
Apply


New Subscription
Specify a name, one or more email addresses and a selected language for this subscription. You can separate multiple email addresses with a semicolon (;).
Subscription name:
Malware detection All Workstations
Email address:
malware@sccm.biz
Email language:
English (United States)
Selected alerts:
Filter...
Alert
Low client check alert for collection: All Windows Workstations
Low client remediation rate alert for collection: All Windows Workstations
Low client activity alert for collection: All Windows Workstations
Generate alert when malware detected - Malware detection alert for collection: All Windows ...
The same malware detected on a number of computers - Malware outbreak alert for collectio...
Same malware repeatedly detected on a computer - Repeated malware detection alert for co...
Multiple types of malware detected on a computer - Multiple malware detection alert for collec...
Critical low free space alert for database on site: NIC
Warning low free space alert for database on site: NIC
Database Replication component failed to run on site NIC
Low Sideloading Activations
Synchronization failure alert for software update point: SCCM2012R2.sccm.biz (NIC)
Rule Failure alert
Rule Failure alert
Not healthy alert for site role: Management point on 'SCCM2012R2.sccm.biz'
OK
Cancel

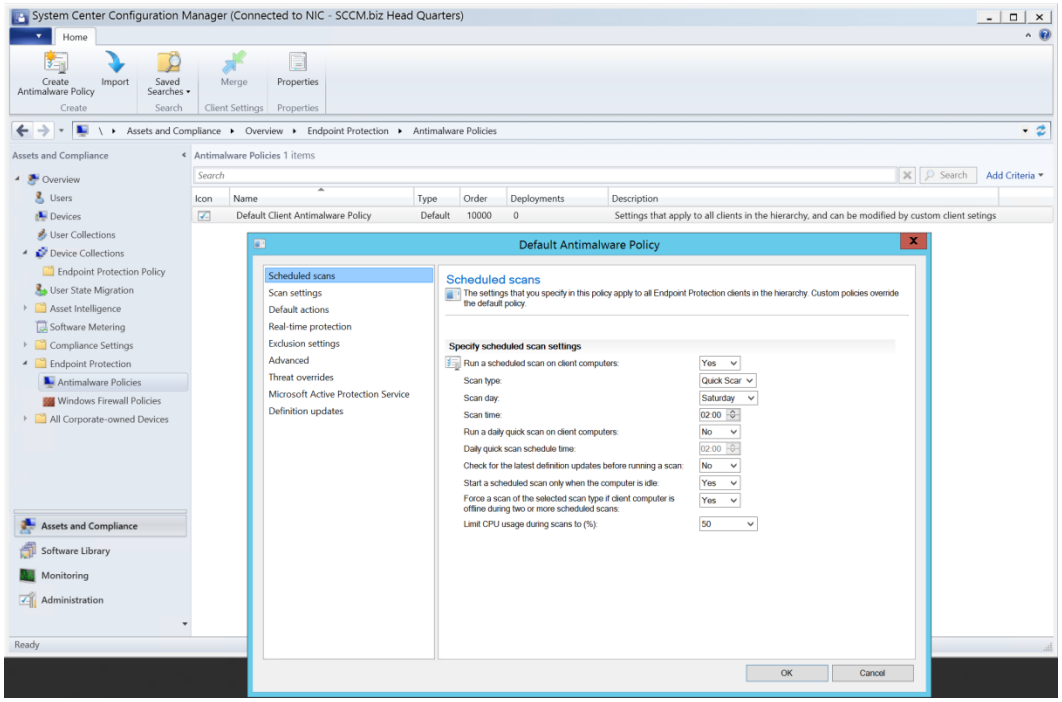

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Antimalware Policy
Import
Saved Searches
Merge
Properties
Create
Search
Client Settings
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Antimalware Policies 1 items
Search
Search
Add Criteria
Icon
Name
Type
Order
Deployments
Description
Default Client Antimalware Policy
Default
10000
0
Settings that apply to all clients in the hierarchy, and can be modified by custom client setings
Ready

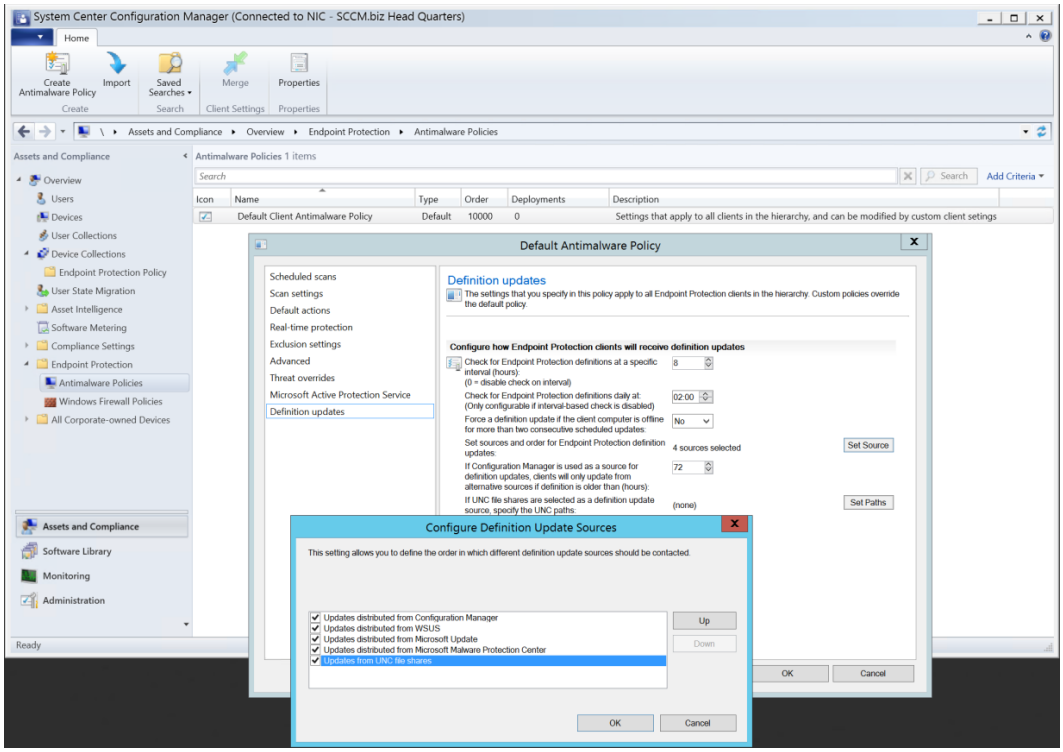

Default Antimalware Policy
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Microsoft Active Protection Service
Definition updates
Definition updates
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Configure how Endpoint Protection clients will receive definition updates
Check for Endpoint Protection definitions at a specific interval (hours):
(0 = disable check on interval)
8
Check for Endpoint Protection definitions daily at:
(Only configurable if interval-based check is disabled)
02:00
Force a definition update if the client computer is offline for more than two consecutive scheduled updates:
No
Set sources and order for Endpoint Protection definition updates:
4 sources selected
Set Source
If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours):
72
If UNC file shares are selected as a definition update source, specify the UNC paths:
(none)
Set Paths
OK
Cancel

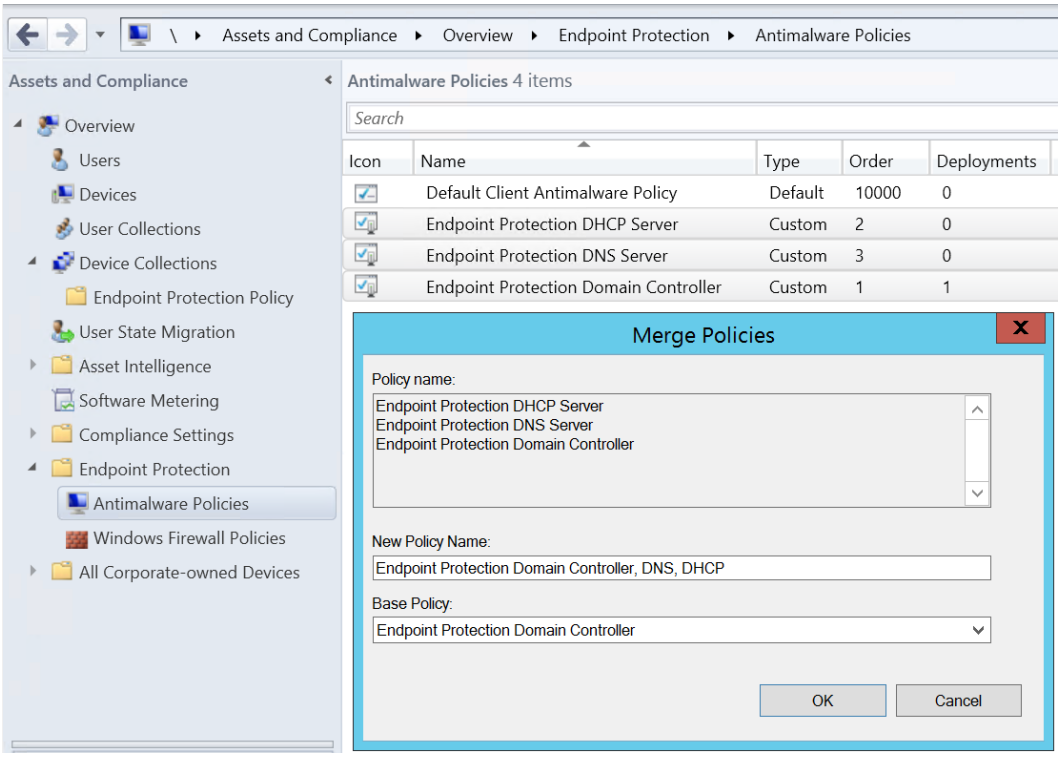

Default Antimalware Policy
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Microsoft Active Protection Service
Definition updates
Definition updates
Configure Definition Update Sources
This setting allows you to define the order in which different definition update sources should be contacted.
Updates distributed from Configuration Manager
Updates distributed from WSUS
Updates distributed from Microsoft Update
Updates distributed from Microsoft Malware Protection Center
Updates from UNC file shares
Up
Down
OK
Cancel
OK
Cancel

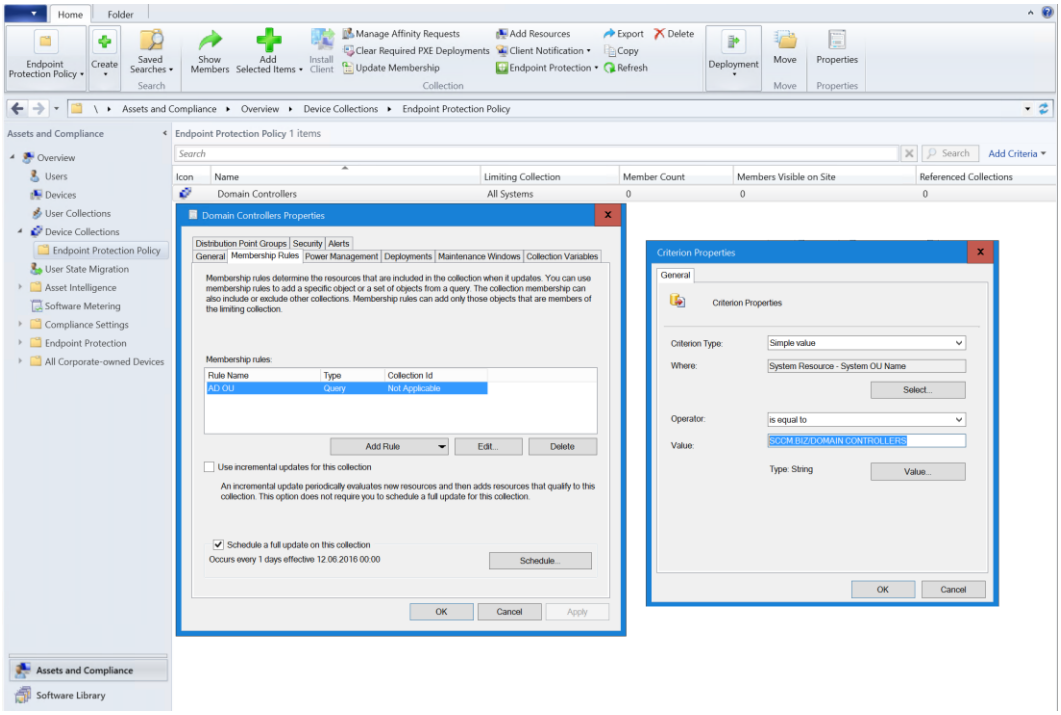

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Antimalware Policy
Import
Saved Searches
Increase Priority
Decrease Priority
Export
Copy
Merge
Refresh
Delete
Deploy
Set Security Scopes
Properties
Create
Search
Client Settings
Deployment
Classify
Properties
Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Antimalware Policies 2 items
Search
Add Criteria
Icon
Name
Type
Order
Deployments
Description
All Workstations
Custom
1
0
Default Client Antimalware Policy
Default
10000
0
Settings that apply to all clients in the hierarchy, and can be modified by custom client setings
All Workstations
Properties
Priority: 1
Deployments: 0
Description
File Properties
Date Created: 25.05.2016 13:14
Created By: SCCM\Administrator
Date Modified: 25.05.2016 13:14
Summary
Deployments
Ready

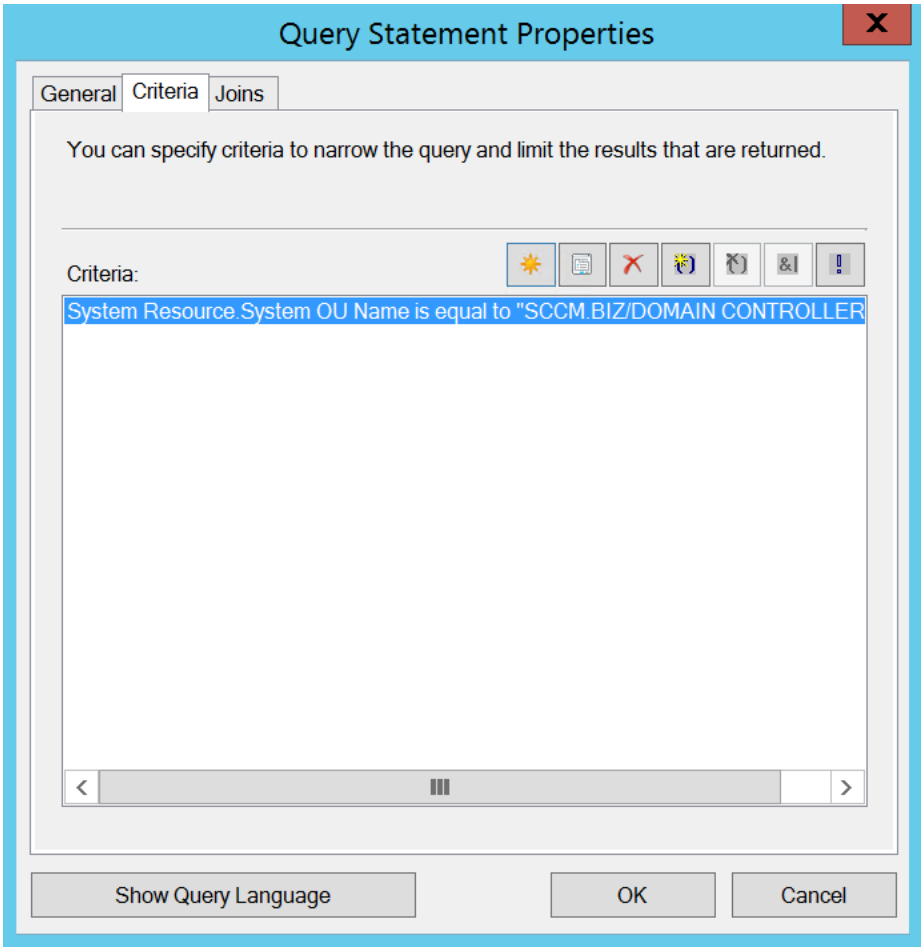
# Chapter 3: Operations and Maintenance for Endpoint Protection in Configuration Manager

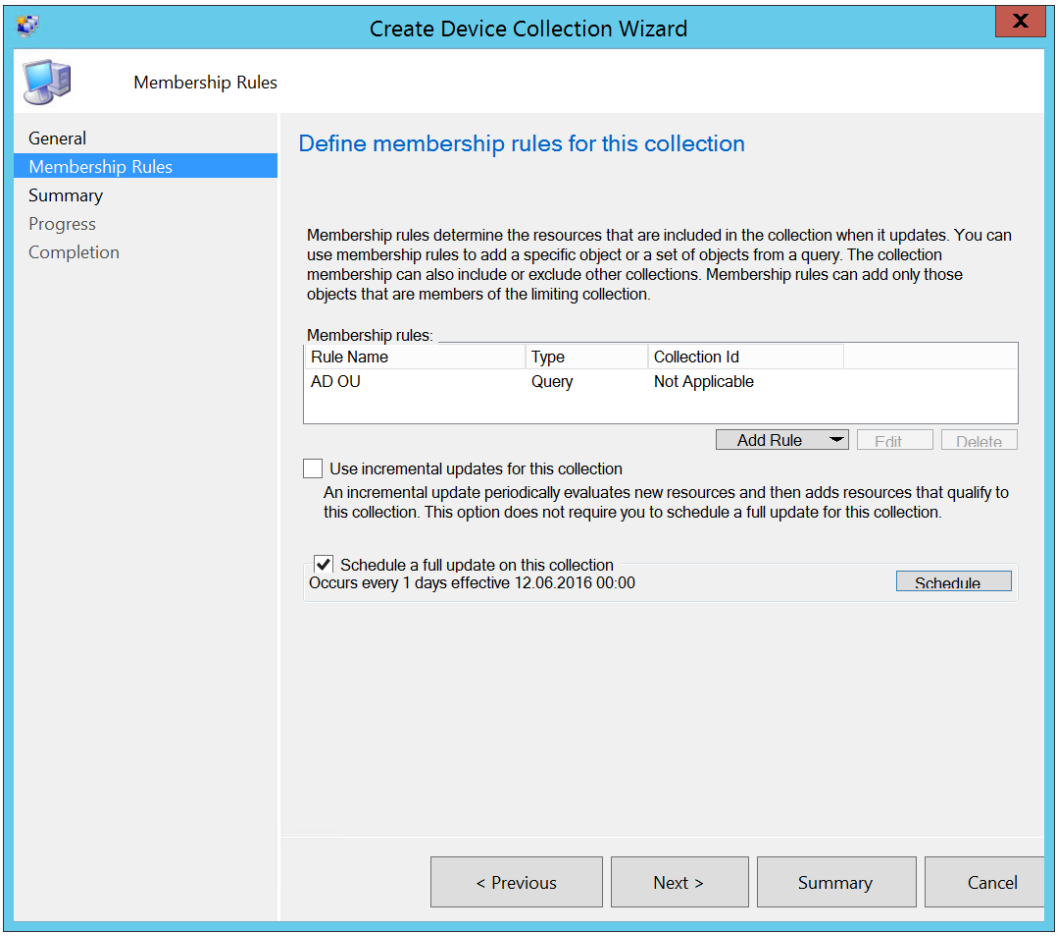


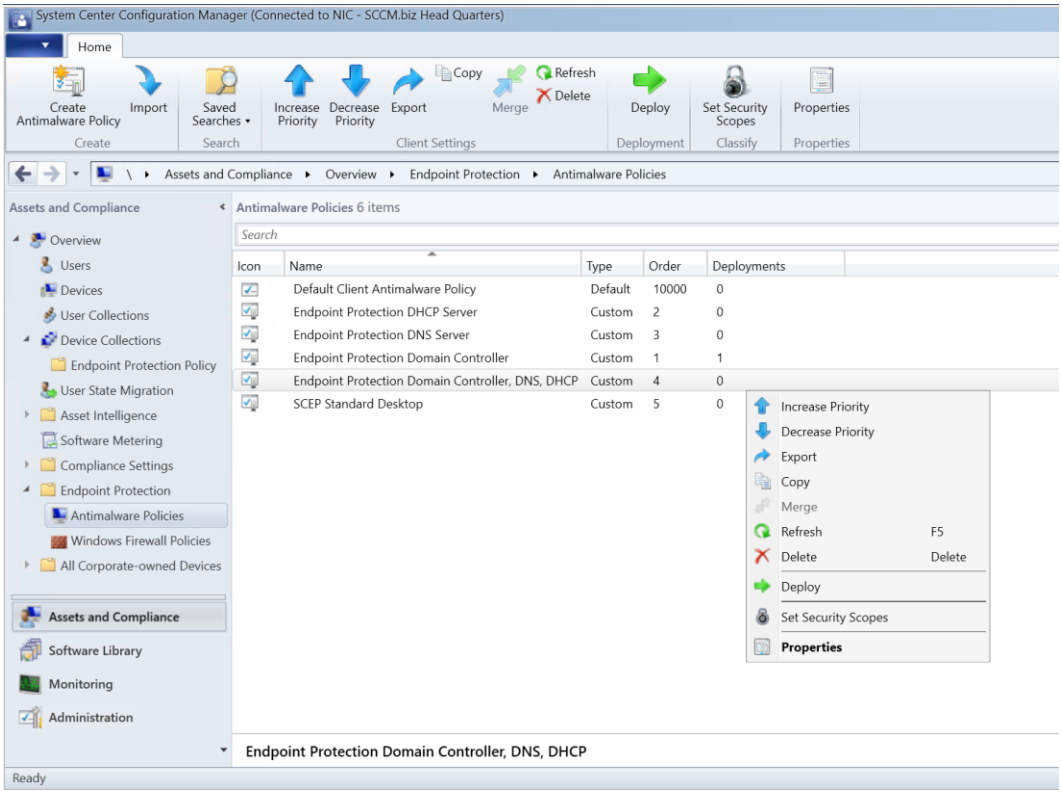

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Antimalware Policy
Import
Saved Searches
Merge
Properties
Create
Search
Client Settings
Properties
Assets and Compliance
Overview
Endpoint Protection
Antimalware Policies
Antimalware Policies 1 items
Search
Add Criteria
Icon
Name
Type
Order
Deployments
Description
Default Client Antimalware Policy
Default
10000
0
Settings that apply to all clients in the hierarchy, and can be modified by custom client setings
Users
Devices
User Collections
Device Collections
Endpoint Protection Policy
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Windows Firewall Policies
All Corporate-owned Devices
Software Library
Monitoring
Administration
Ready
Default Antimalware Policy
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Microsoft Active Protection Service
Definition updates
Definition updates
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Configure how Endpoint Protection clients will receive definition updates
Check for Endpoint Protection definitions at a specific interval (hours):
(0 = disable check on interval)
8
Check for Endpoint Protection definitions daily at:
(Only configurable if interval-based check is disabled)
02:00
Force a definition update if the client computer is offline for more than two consecutive scheduled updates:
No
Set sources and order for Endpoint Protection definition updates:
4 sources selected
Set Source
If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours):
72
If UNC file shares are selected as a definition update source, specify the UNC paths:
(none)
Set Paths
OK
Cancel
Configure Definition Update Sources
This setting allows you to define the order in which different definition update sources should be contacted.
Updates distributed from Configuration Manager
Updates distributed from WSUS
Updates distributed from Microsoft Update
Updates distributed from Microsoft Malware Protection Center
Updates from UNC file shares
Up
Down
OK
Cancel

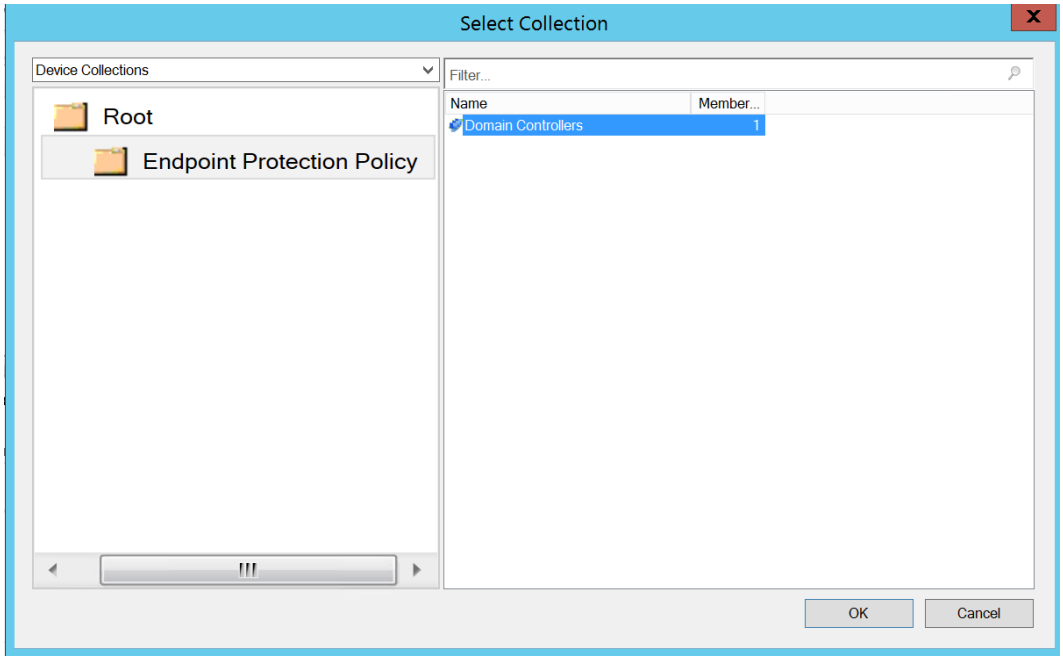

\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Endpoint Protection Policy
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Antimalware Policies 4 items
Search
Icon
Name
Type
Order
Deployments
Default Client Antimalware Policy
Default
10000
0
Endpoint Protection DHCP Server
Custom
2
0
Endpoint Protection DNS Server
Custom
3
0
Endpoint Protection Domain Controller
Custom
1
1
Merge Policies
Policy name:
Endpoint Protection DHCP Server
Endpoint Protection DNS Server
Endpoint Protection Domain Controller
New Policy Name:
Endpoint Protection Domain Controller, DNS, DHCP
Base Policy:
Endpoint Protection Domain Controller
OK
Cancel

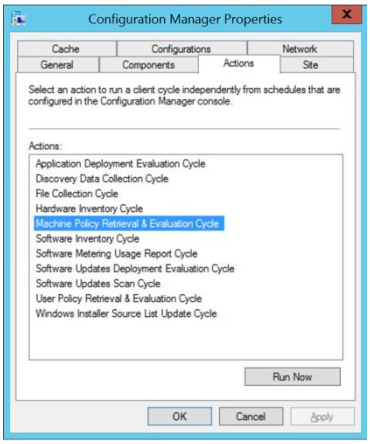

Home
Folder
Endpoint Protection Policy
Create
Saved Searches
Search
Show Members
Add Selected Items
Install Client
Manage Affinity Requests
Clear Required PXE Deployments
Update Membership
Add Resources
Client Notification
Endpoint Protection
Export
Delete
Copy
Refresh
Collection
Deployment
Move
Properties
Assets and Compliance ▸ Overview ▸ Device Collections ▸ Endpoint Protection Policy
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Endpoint Protection Policy
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
All Corporate-owned Devices
Assets and Compliance
Software Library
Endpoint Protection Policy 1 items
Search
Add Criteria
Icon
Name
Limiting Collection
Member Count
Members Visible on Site
Referenced Collections
Domain Controllers
All Systems
0
0
0
Domain Controllers Properties
Distribution Point Groups
Security
Alerts
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.
Membership rules:
Rule Name
Type
Collection Id
AD OU
Query
Not Applicable
Add Rule
Edit...
Delete
Use incremental updates for this collection
An incremental update periodically evaluates new resources and then adds resources that qualify to this collection. This option does not require you to schedule a full update for this collection.
Schedule a full update on this collection
Occurs every 1 days effective 12.06.2016 00:00
Schedule...
OK
Cancel
Apply
Criterion Properties
General
Criterion Properties
Criterion Type:
Simple value
Where:
System Resource - System OU Name
Select...
Operator:
is equal to
Value:
SCCM.BIZ/DOMAIN CONTROLLERS
Type: String
Value...
OK
Cancel

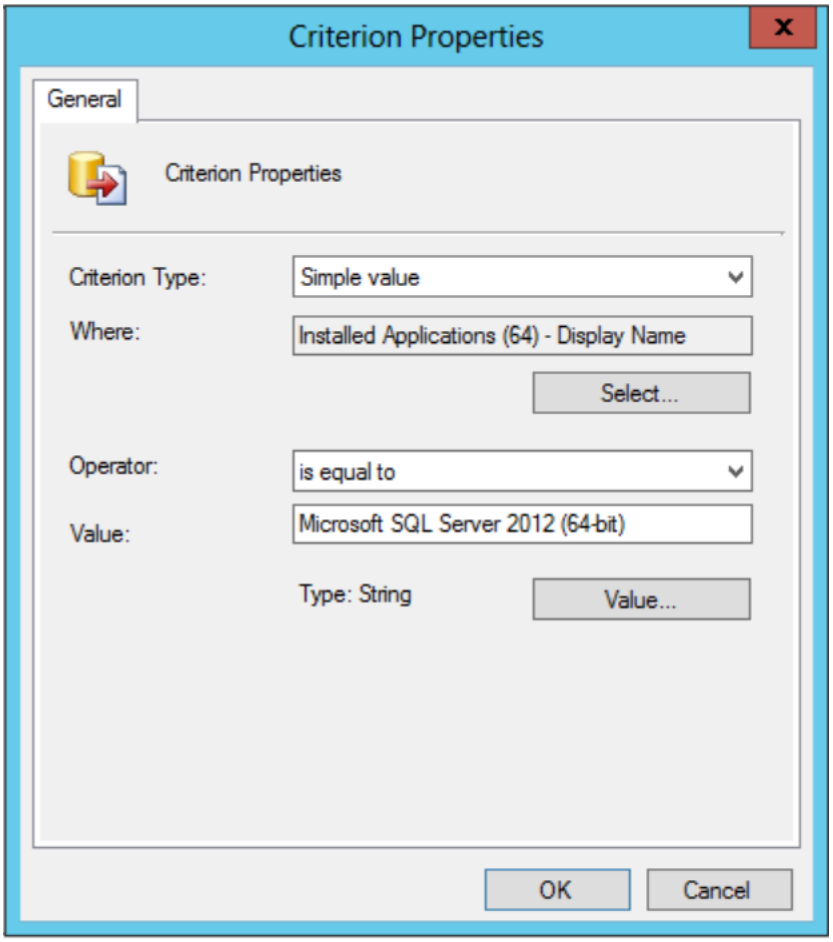

Query Statement Properties
General
Criteria
Joins
You can specify criteria to narrow the query and limit the results that are returned.
Criteria:
System Resource.System OU Name is equal to "SCCM.BIZ/DOMAIN CONTROLLER
Show Query Language
OK
Cancel

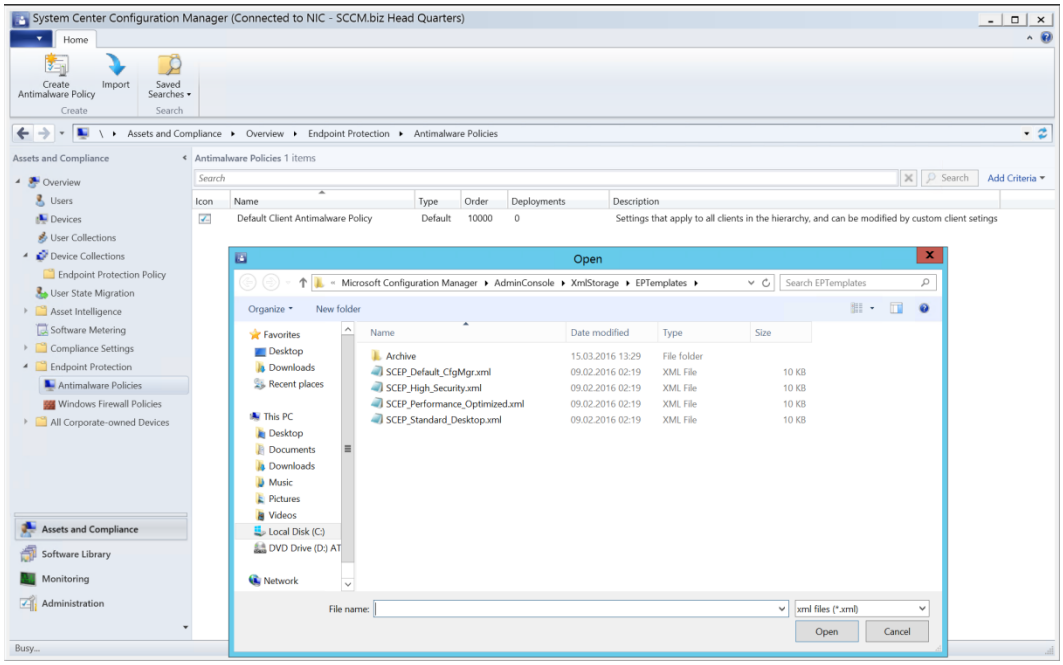

Create Device Collection Wizard
Membership Rules
General
Membership Rules
Summary
Progress
Completion
Define membership rules for this collection
Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.
Membership rules:
Rule Name
Type
Collection Id
AD OU
Query
Not Applicable
Add Rule
Edit
Delete
Use incremental updates for this collection
An incremental update periodically evaluates new resources and then adds resources that qualify to this collection. This option does not require you to schedule a full update for this collection.
Schedule a full update on this collection
Occurs every 1 days effective 12.06.2016 00:00
Schedule
< Previous
Next >
Summary
Cancel

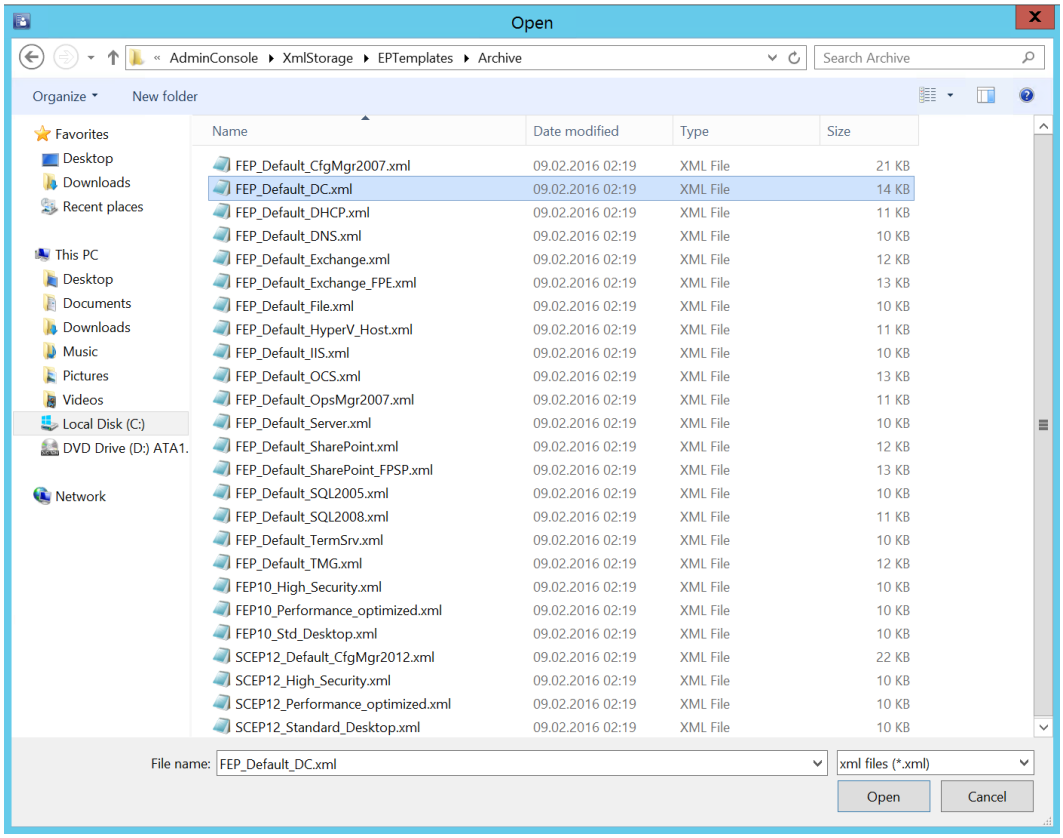

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Antimalware Policy
Import
Saved Searches
Increase Priority
Decrease Priority
Export
Copy
Merge
Refresh
Delete
Deploy
Set Security Scopes
Properties
Create
Search
Client Settings
Deployment
Classify
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Endpoint Protection Policy
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Antimalware Policies 6 items
Search
Icon
Name
Type
Order
Deployments
Default Client Antimalware Policy Default 10000 0
Endpoint Protection DHCP Server Custom 2 0
Endpoint Protection DNS Server Custom 3 0
Endpoint Protection Domain Controller Custom 1 1
Endpoint Protection Domain Controller, DNS, DHCP Custom 4 0
SCEP Standard Desktop Custom 5 0
Increase Priority
Decrease Priority
Export
Copy
Merge
Refresh F5
Delete Delete
Deploy
Set Security Scopes
Properties
Endpoint Protection Domain Controller, DNS, DHCP
Ready

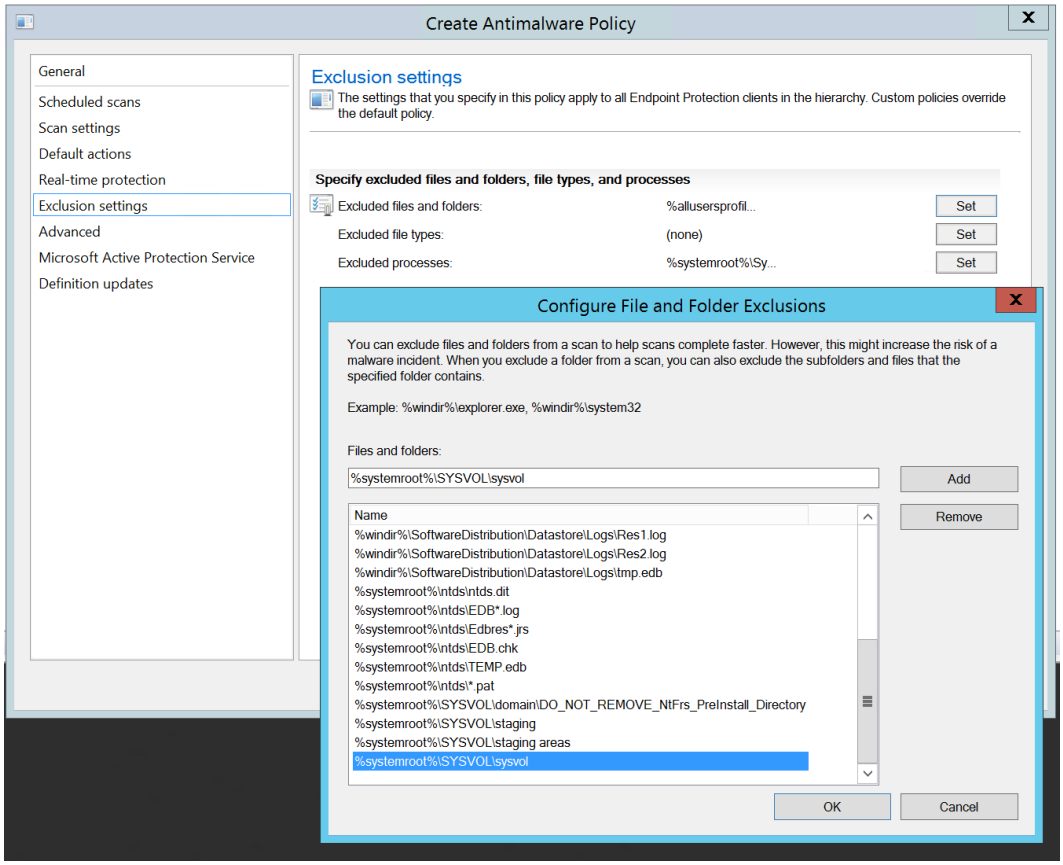

Select Collection
Device Collections
Filter...
Root
Endpoint Protection Policy
Name
Member...
Domain Controllers
1
OK
Cancel

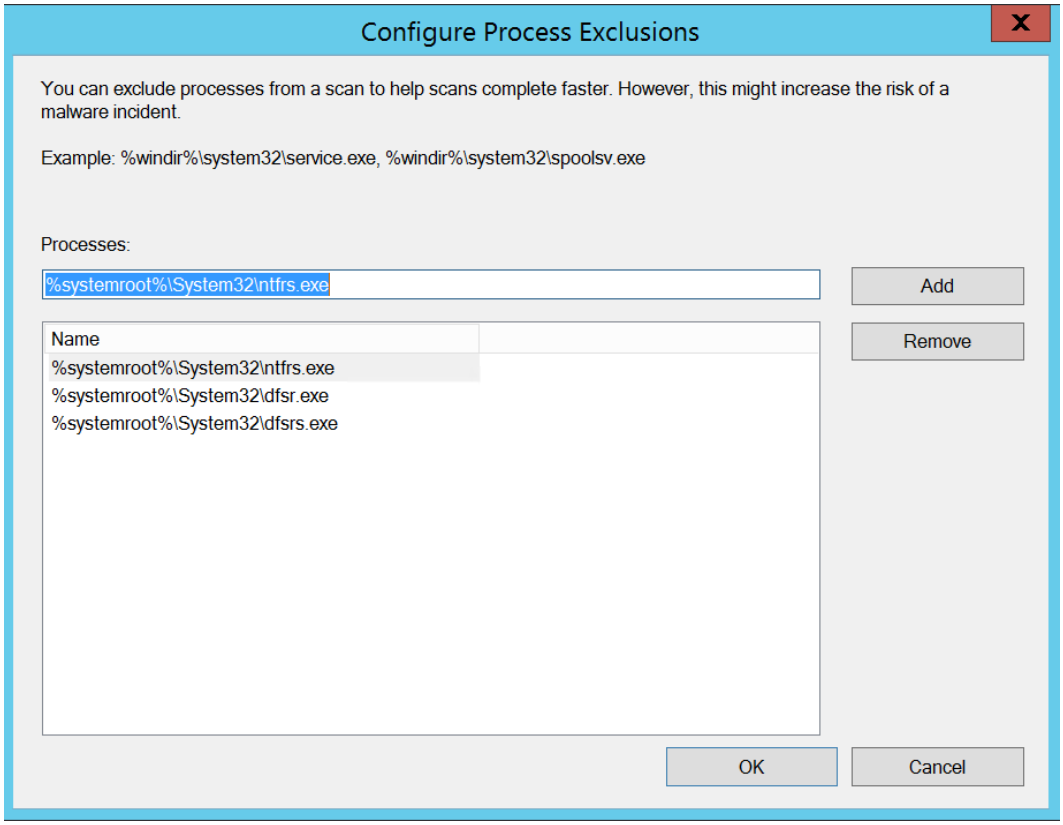

Configuration Manager Properties
Cache
Configurations
Network
General
Components
Actions
Site
Select an action to run a client cycle independently from schedules that are configured in the Configuration Manager console.
Actions:
Application Deployment Evaluation Cycle
Discovery Data Collection Cycle
File Collection Cycle
Hardware Inventory Cycle
Machine Policy Retrieval & Evaluation Cycle
Software Inventory Cycle
Software Metering Usage Report Cycle
Software Updates Deployment Evaluation Cycle
Software Updates Scan Cycle
User Policy Retrieval & Evaluation Cycle
Windows Installer Source List Update Cycle
Run Now
OK
Cancel
Apply

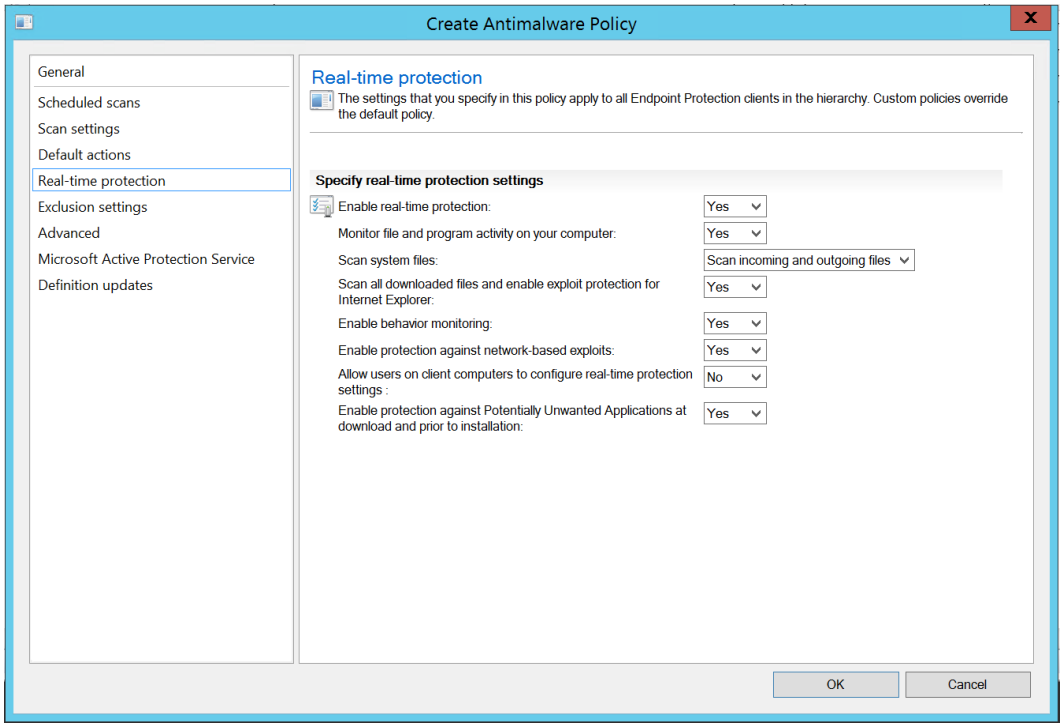

Criterion Properties
General
Criterion Properties
Criterion Type:
Simple value
Where:
Installed Applications (64) - Display Name
Select...
Operator:
is equal to
Value:
Microsoft SQL Server 2012 (64-bit)
Type: String
Value...
OK
Cancel

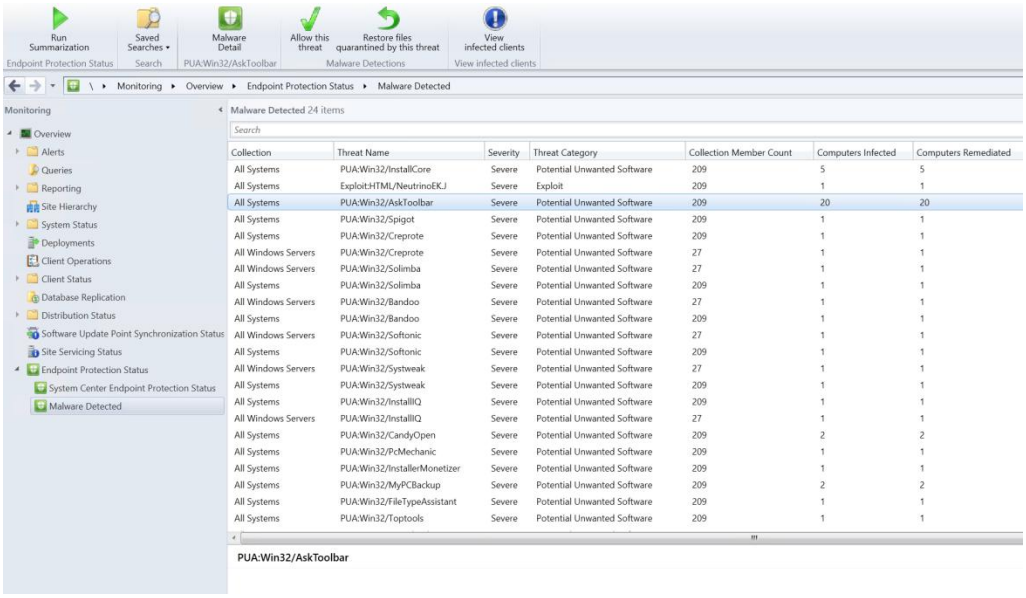

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Antimalware Policy
Import
Saved Searches
Create
Search
Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Endpoint Protection Policy
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Antimalware Policies 1 items
Search
Add Criteria
Icon
Name
Type
Order
Deployments
Description
Default Client Antimalware Policy
Default
10000
0
Settings that apply to all clients in the hierarchy, and can be modified by custom client setings
Busy...
Open
Microsoft Configuration Manager ▸ AdminConsole ▸ XmlStorage ▸ EPTemplates ▸
Search EPTemplates
Organize
New folder
Favorites
Desktop
Downloads
Recent places
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) AT
Network
Name
Date modified
Type
Size
Archive
15.03.2016 13:29
File folder
SCEP_Default_CfgMgr.xml
09.02.2016 02:19
XML File
10 KB
SCEP_High_Security.xml
09.02.2016 02:19
XML File
10 KB
SCEP_Performance_Optimized.xml
09.02.2016 02:19
XML File
10 KB
SCEP_Standard_Desktop.xml
09.02.2016 02:19
XML File
10 KB
File name:
xml files (*.xml)
Open
Cancel

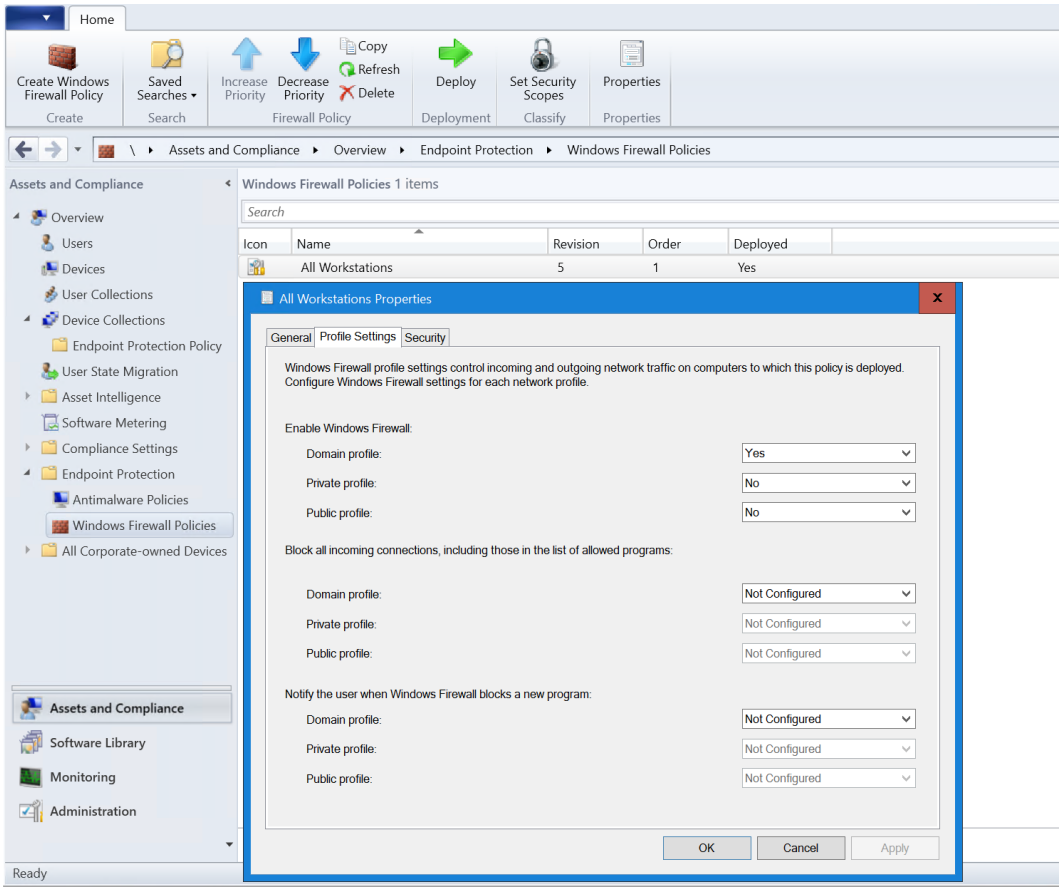

Open
AdminConsole ▸ XmlStorage ▸ EPTemplates ▸ Archive
Search Archive
Organize
New folder
Favorites
Desktop
Downloads
Recent places
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) ATA1.
Network
Name
Date modified
Type
Size
FEP_Default_CfgMgr2007.xml 09.02.2016 02:19 XML File 21 KB
FEP_Default_DC.xml 09.02.2016 02:19 XML File 14 KB
FEP_Default_DHCP.xml 09.02.2016 02:19 XML File 11 KB
FEP_Default_DNS.xml 09.02.2016 02:19 XML File 10 KB
FEP_Default_Exchange.xml 09.02.2016 02:19 XML File 12 KB
FEP_Default_Exchange_FPE.xml 09.02.2016 02:19 XML File 13 KB
FEP_Default_File.xml 09.02.2016 02:19 XML File 10 KB
FEP_Default_HyperV_Host.xml 09.02.2016 02:19 XML File 11 KB
FEP_Default_IIS.xml 09.02.2016 02:19 XML File 10 KB
FEP_Default_OCS.xml 09.02.2016 02:19 XML File 13 KB
FEP_Default_OpsMgr2007.xml 09.02.2016 02:19 XML File 11 KB
FEP_Default_Server.xml 09.02.2016 02:19 XML File 10 KB
FEP_Default_SharePoint.xml 09.02.2016 02:19 XML File 12 KB
FEP_Default_SharePoint_FPSP.xml 09.02.2016 02:19 XML File 13 KB
FEP_Default_SQL2005.xml 09.02.2016 02:19 XML File 10 KB
FEP_Default_SQL2008.xml 09.02.2016 02:19 XML File 11 KB
FEP_Default_TermSrv.xml 09.02.2016 02:19 XML File 10 KB
FEP_Default_TMG.xml 09.02.2016 02:19 XML File 12 KB
FEP10_High_Security.xml 09.02.2016 02:19 XML File 10 KB
FEP10_Performance_optimized.xml 09.02.2016 02:19 XML File 10 KB
FEP10_Std_Desktop.xml 09.02.2016 02:19 XML File 10 KB
SCEP12_Default_CfgMgr2012.xml 09.02.2016 02:19 XML File 22 KB
SCEP12_High_Security.xml 09.02.2016 02:19 XML File 10 KB
SCEP12_Performance_optimized.xml 09.02.2016 02:19 XML File 10 KB
SCEP12_Standard_Desktop.xml 09.02.2016 02:19 XML File 10 KB
File name: FEP_Default_DC.xml
xml files (*.xml)
Open
Cancel

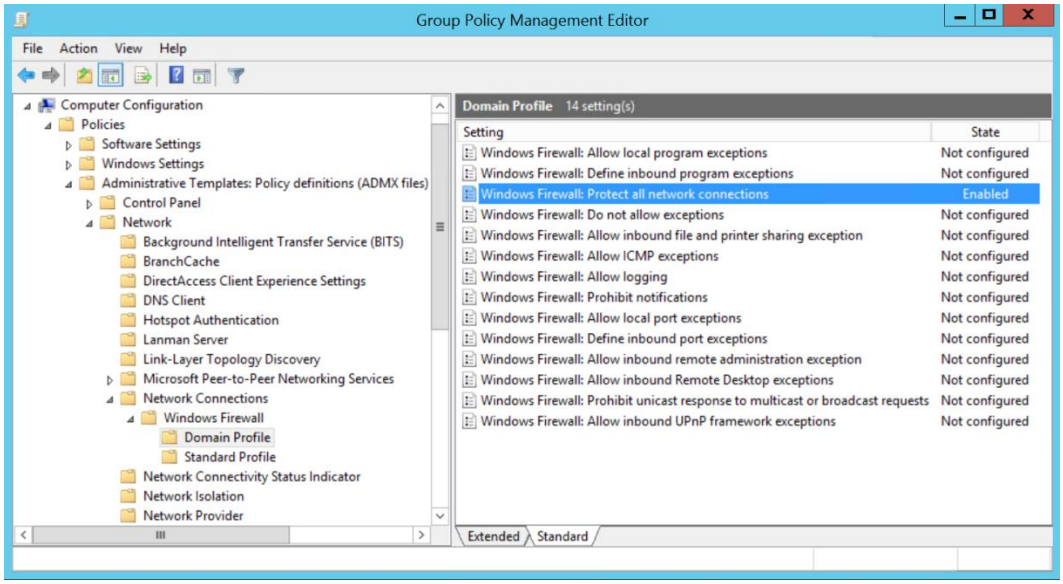

Create Antimalware Policy
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Microsoft Active Protection Service
Definition updates
Exclusion settings
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify excluded files and folders, file types, and processes
Excluded files and folders:
%allusersprofil...
Set
Excluded file types:
(none)
Set
Excluded processes:
%systemroot%\Sy...
Set
Configure File and Folder Exclusions
You can exclude files and folders from a scan to help scans complete faster. However, this might increase the risk of a malware incident. When you exclude a folder from a scan, you can also exclude the subfolders and files that the specified folder contains.
Example: %windir%\explorer.exe, %windir%\system32
Files and folders:
%systemroot%\SYSVOL\sysvol
Add
Remove
Name
%windir%\SoftwareDistribution\Datastore\Logs\Res1.log
%windir%\SoftwareDistribution\Datastore\Logs\Res2.log
%windir%\SoftwareDistribution\Datastore\Logs\tmp.edb
%systemroot%\ntds\ntds.dit
%systemroot%\ntds\EDB*.log
%systemroot%\ntds\Edbres*.jrs
%systemroot%\ntds\EDB.chk
%systemroot%\ntds\TEMP.edb
%systemroot%\ntds*.pat
%systemroot%\SYSVOL\domain\DO_NOT_REMOVE_NtFrs_PreInstall_Directory
%systemroot%\SYSVOL\staging
%systemroot%\SYSVOL\staging areas
%systemroot%\SYSVOL\sysvol
OK
Cancel

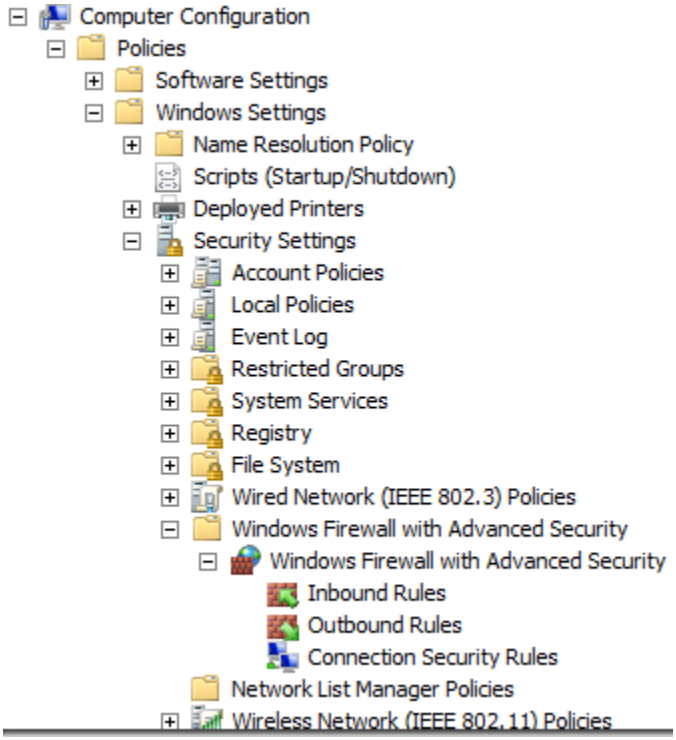

Configure Process Exclusions
You can exclude processes from a scan to help scans complete faster. However, this might increase the risk of a malware incident.
Example: %windir%\system32\service.exe, %windir%\system32\spoolsv.exe
Processes:
%systemroot%\System32\ntfrs.exe
Add
Name
%systemroot%\System32\ntfrs.exe
%systemroot%\System32\dfsr.exe
%systemroot%\System32\dfsrs.exe
Remove
OK
Cancel

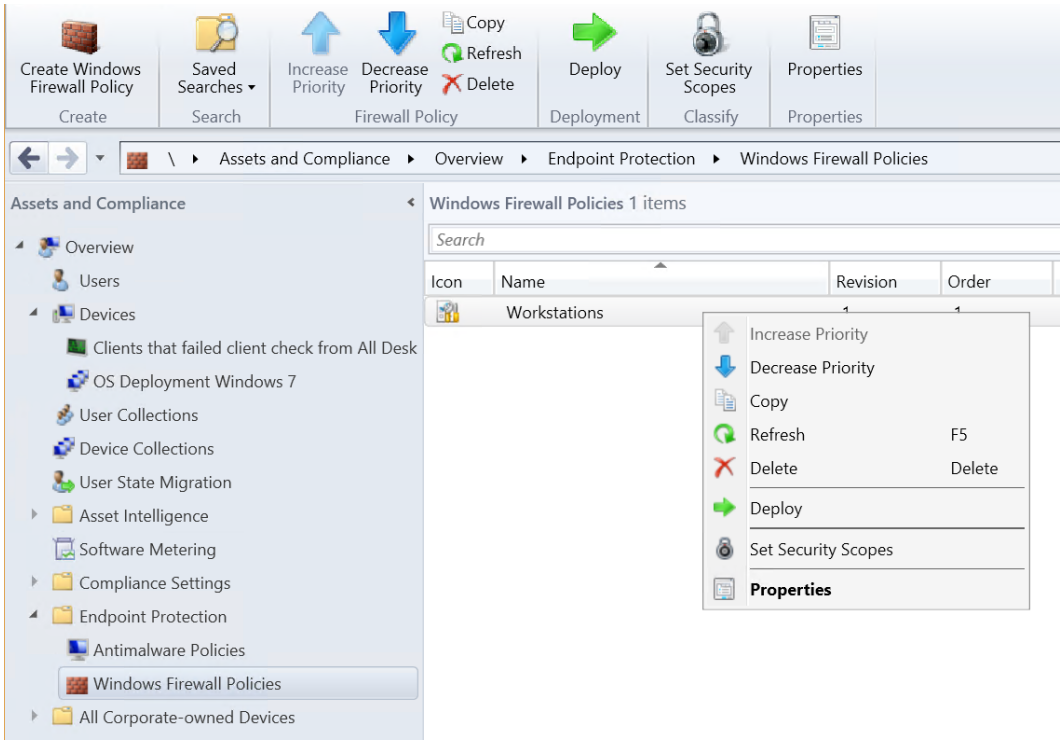

Create Antimalware Policy
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Microsoft Active Protection Service
Definition updates
Real-time protection
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify real-time protection settings
Enable real-time protection: Yes
Monitor file and program activity on your computer: Yes
Scan system files: Scan incoming and outgoing files
Scan all downloaded files and enable exploit protection for Internet Explorer: Yes
Enable behavior monitoring: Yes
Enable protection against network-based exploits: Yes
Allow users on client computers to configure real-time protection settings : No
Enable protection against Potentially Unwanted Applications at download and prior to installation: Yes
OK
Cancel

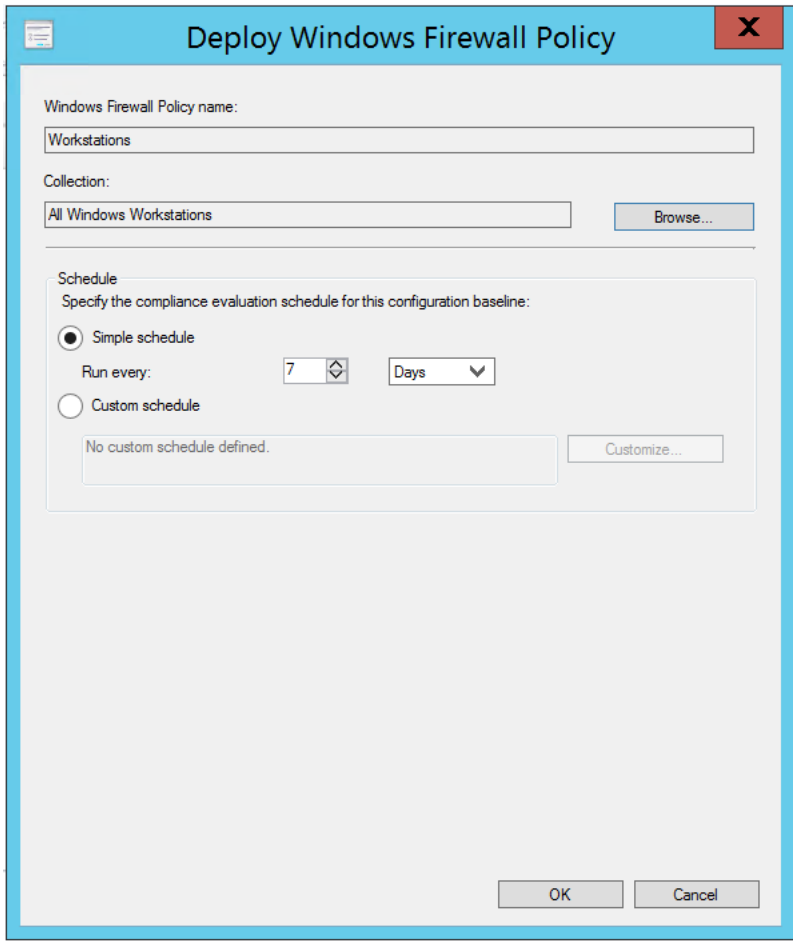

Run Summarization
Saved Searches
Malware Detail
Allow this threat
Restore files quarantined by this threat
View infected clients
Endpoint Protection Status
Search
PUA:Win32/AskToolbar
Malware Detections
View infected clients
Monitoring
Overview
Endpoint Protection Status
Malware Detected
Malware Detected 24 items
Search
Collection
Threat Name
Severity
Threat Category
Collection Member Count
Computers Infected
Computers Remediated
All Systems PUA:Win32/InstallCore Severe Potential Unwanted Software 209 5 5
All Systems Exploit:HTML/NeutrinoEKJ Severe Exploit 209 1 1
All Systems PUA:Win32/AskToolbar Severe Potential Unwanted Software 209 20 20
All Systems PUA:Win32/Spigot Severe Potential Unwanted Software 209 1 1
All Systems PUA:Win32/Creprote Severe Potential Unwanted Software 209 1 1
All Windows Servers PUA:Win32/Creprote Severe Potential Unwanted Software 27 1 1
All Windows Servers PUA:Win32/Solimba Severe Potential Unwanted Software 27 1 1
All Systems PUA:Win32/Solimba Severe Potential Unwanted Software 209 1 1
All Windows Servers PUA:Win32/Bandoo Severe Potential Unwanted Software 27 1 1
All Systems PUA:Win32/Bandoo Severe Potential Unwanted Software 209 1 1
All Windows Servers PUA:Win32/Softonic Severe Potential Unwanted Software 27 1 1
All Systems PUA:Win32/Softonic Severe Potential Unwanted Software 209 1 1
All Windows Servers PUA:Win32/Systweak Severe Potential Unwanted Software 27 1 1
All Systems PUA:Win32/Systweak Severe Potential Unwanted Software 209 1 1
All Systems PUA:Win32/InstallIQ Severe Potential Unwanted Software 209 1 1
All Windows Servers PUA:Win32/InstallIQ Severe Potential Unwanted Software 27 1 1
All Systems PUA:Win32/CandyOpen Severe Potential Unwanted Software 209 2 2
All Systems PUA:Win32/PcMechanic Severe Potential Unwanted Software 209 1 1
All Systems PUA:Win32/InstallerMonetizer Severe Potential Unwanted Software 209 1 1
All Systems PUA:Win32/MyPCBackup Severe Potential Unwanted Software 209 2 2
All Systems PUA:Win32/FileTypeAssistant Severe Potential Unwanted Software 209 1 1
All Systems PUA:Win32/Toptools Severe Potential Unwanted Software 209 1 1
PUA:Win32/AskToolbar

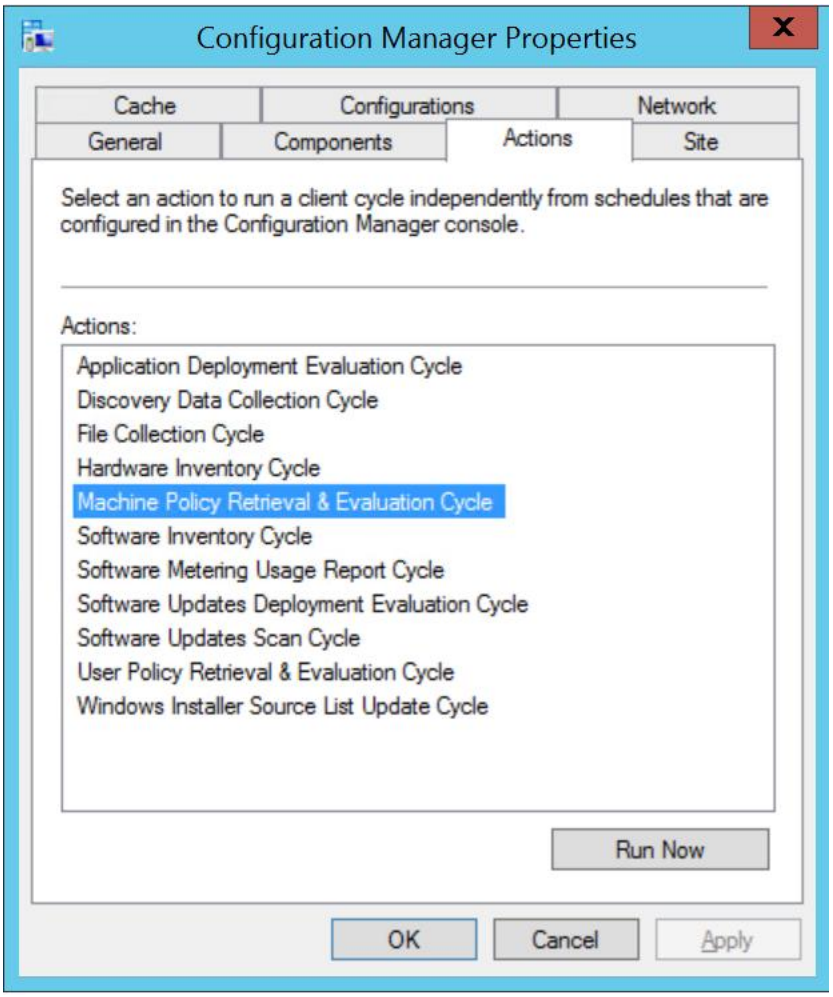

Home
Create Windows Firewall Policy
Create
Saved Searches
Search
Increase Priority
Decrease Priority
Copy
Refresh
Delete
Firewall Policy
Deploy
Deployment
Set Security Scopes
Classify
Properties
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Windows Firewall Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Endpoint Protection Policy
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Windows Firewall Policies 1 items
Search
Icon
Name
Revision
Order
Deployed
All Workstations
5
1
Yes
All Workstations Properties
General
Profile Settings
Security
Windows Firewall profile settings control incoming and outgoing network traffic on computers to which this policy is deployed.
Configure Windows Firewall settings for each network profile.
Enable Windows Firewall:
Domain profile:
Yes
Private profile:
No
Public profile:
No
Block all incoming connections, including those in the list of allowed programs:
Domain profile:
Not Configured
Private profile:
Not Configured
Public profile:
Not Configured
Notify the user when Windows Firewall blocks a new program:
Domain profile:
Not Configured
Private profile:
Not Configured
Public profile:
Not Configured
OK
Cancel
Apply
Ready

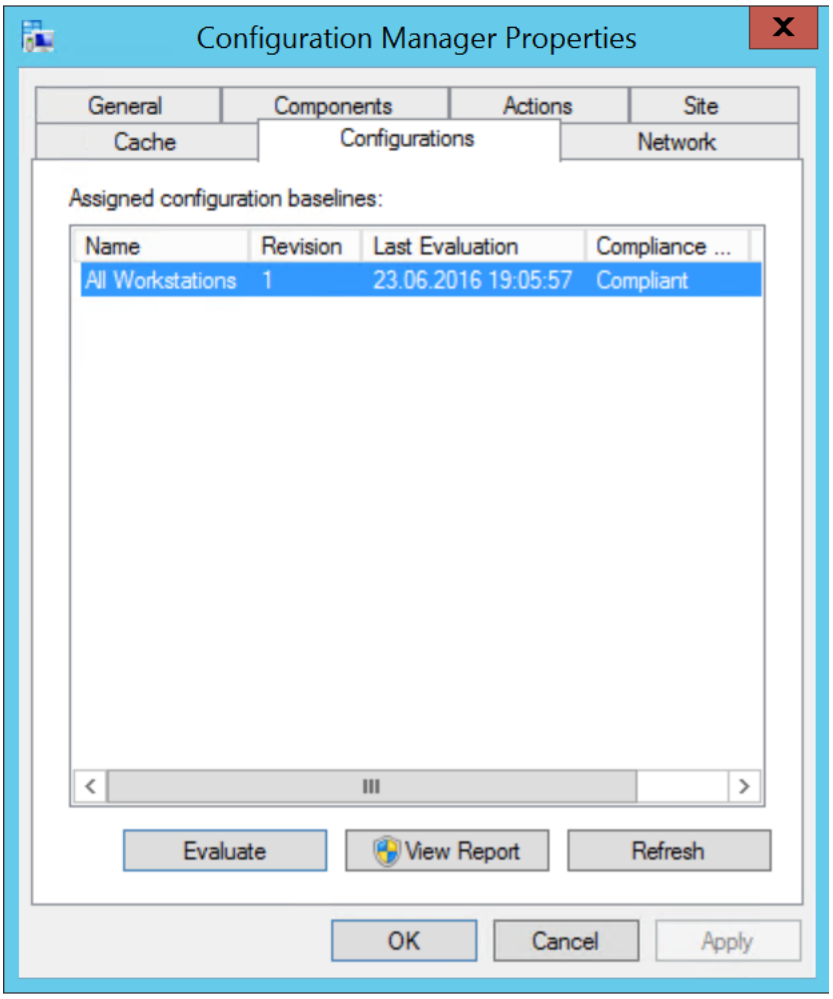

Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files)
Control Panel
Network
Background Intelligent Transfer Service (BITS)
BranchCache
DirectAccess Client Experience Settings
DNS Client
Hotspot Authentication
Lanman Server
Link-Layer Topology Discovery
Microsoft Peer-to-Peer Networking Services
Network Connections
Windows Firewall
Domain Profile
Standard Profile
Network Connectivity Status Indicator
Network Isolation
Network Provider
Domain Profile 14 setting(s)
Setting
State
Windows Firewall: Allow local program exceptions Not configured
Windows Firewall: Define inbound program exceptions Not configured
Windows Firewall: Protect all network connections Enabled
Windows Firewall: Do not allow exceptions Not configured
Windows Firewall: Allow inbound file and printer sharing exception Not configured
Windows Firewall: Allow ICMP exceptions Not configured
Windows Firewall: Allow logging Not configured
Windows Firewall: Prohibit notifications Not configured
Windows Firewall: Allow local port exceptions Not configured
Windows Firewall: Define inbound port exceptions Not configured
Windows Firewall: Allow inbound remote administration exception Not configured
Windows Firewall: Allow inbound Remote Desktop exceptions Not configured
Windows Firewall: Prohibit unicast response to multicast or broadcast requests Not configured
Windows Firewall: Allow inbound UPnP framework exceptions Not configured
Extended
Standard

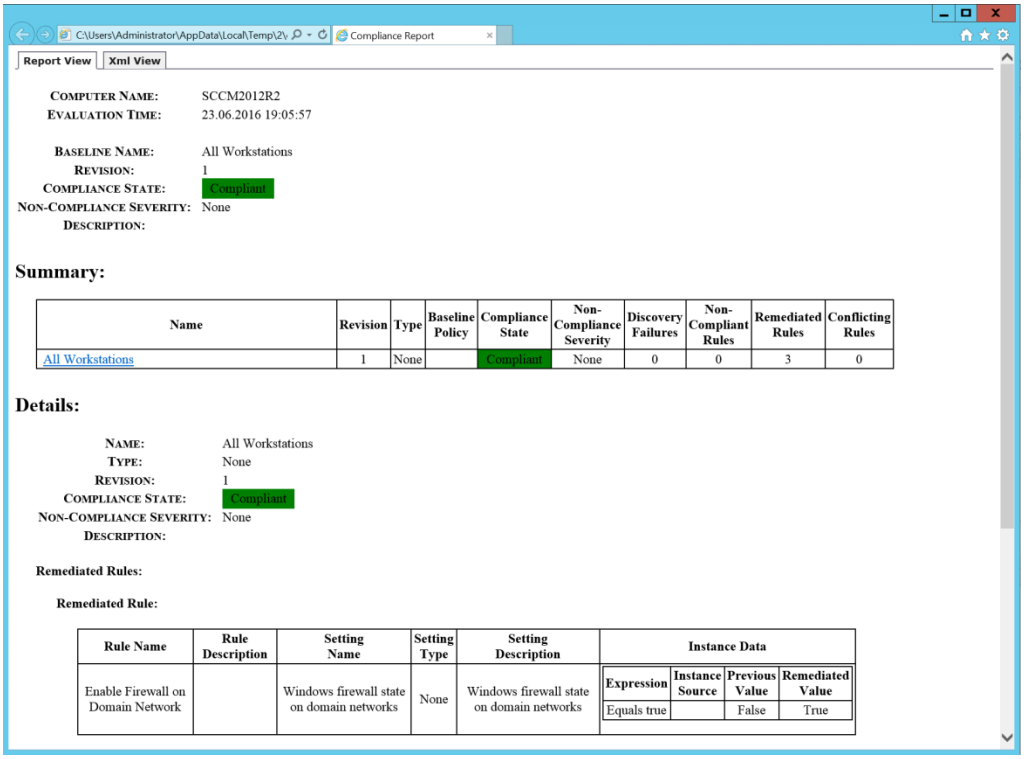

Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies


Create Windows Firewall Policy
Create
Saved Searches
Search
Increase Priority
Decrease Priority
Copy
Refresh
Delete
Firewall Policy
Deploy
Deployment
Set Security Scopes
Classify
Properties
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Windows Firewall Policies
Assets and Compliance
Overview
Users
Devices
Clients that failed client check from All Desk
OS Deployment Windows 7
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Windows Firewall Policies 1 items
Search
Icon
Name
Revision
Order
Workstations
Increase Priority
Decrease Priority
Copy
Refresh F5
Delete Delete
Deploy
Set Security Scopes
Properties


Deploy Windows Firewall Policy
Windows Firewall Policy name:
Workstations
Collection:
All Windows Workstations
Browse...
Schedule
Specify the compliance evaluation schedule for this configuration baseline:
Simple schedule
Run every:
7
Days
Custom schedule
No custom schedule defined.
Customize...
OK
Cancel


Configuration Manager Properties
Cache
Configurations
Network
General
Components
Actions
Site
Select an action to run a client cycle independently from schedules that are configured in the Configuration Manager console.
Actions:
Application Deployment Evaluation Cycle
Discovery Data Collection Cycle
File Collection Cycle
Hardware Inventory Cycle
Machine Policy Retrieval & Evaluation Cycle
Software Inventory Cycle
Software Metering Usage Report Cycle
Software Updates Deployment Evaluation Cycle
Software Updates Scan Cycle
User Policy Retrieval & Evaluation Cycle
Windows Installer Source List Update Cycle
Run Now
OK
Cancel
Apply


Configuration Manager Properties
General
Components
Actions
Site
Cache
Configurations
Network
Assigned configuration baselines:
Name
Revision
Last Evaluation
Compliance ...
All Workstations
1
23.06.2016 19:05:57
Compliant
Evaluate
View Report
Refresh
OK
Cancel
Apply




**COMPUTER NAME:** SCCM2012R2
**EVALUATION TIME:** 23.06.2016 19:05:57

**BASELINE NAME:** All Workstations
**REVISION:** 1
**COMPLIANCE STATE:** Compliant
**NON-COMPLIANCE SEVERITY:** None
**DESCRIPTION:**

## Summary:

| Name | Revision | Type | Baseline Policy | Compliance State | Non-Compliance Severity | Discovery Failures | Non-Compliant Rules | Remediated Rules | Conflicting Rules |
|---|---|---|---|---|---|---|---|---|---|
| All Workstations | 1 | None | | Compliant | None | 0 | 0 | 3 | 0 |

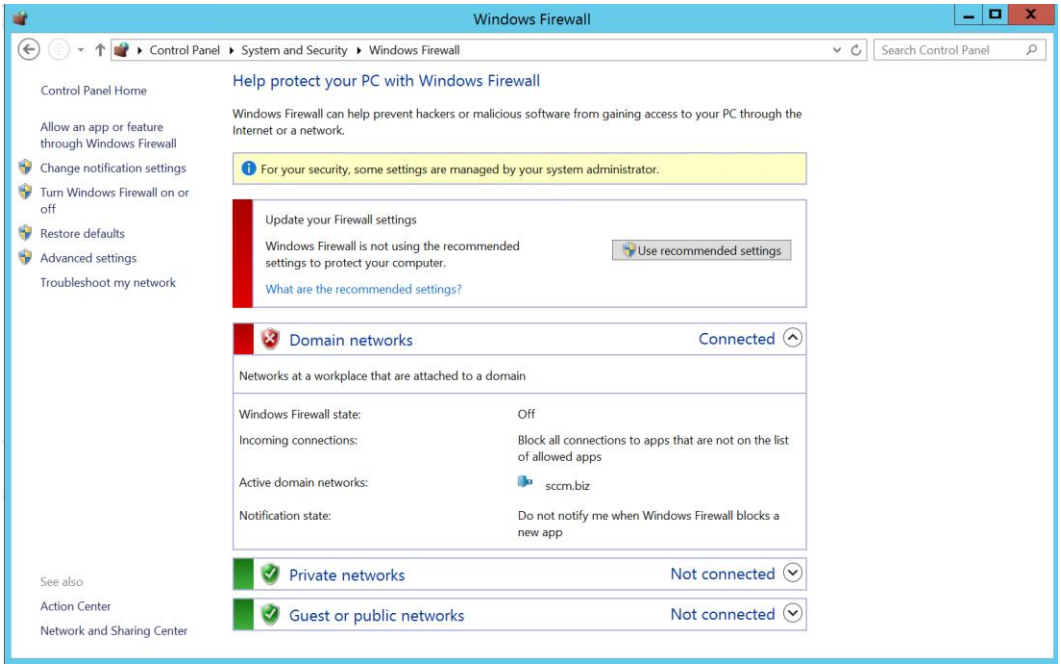
## Details:

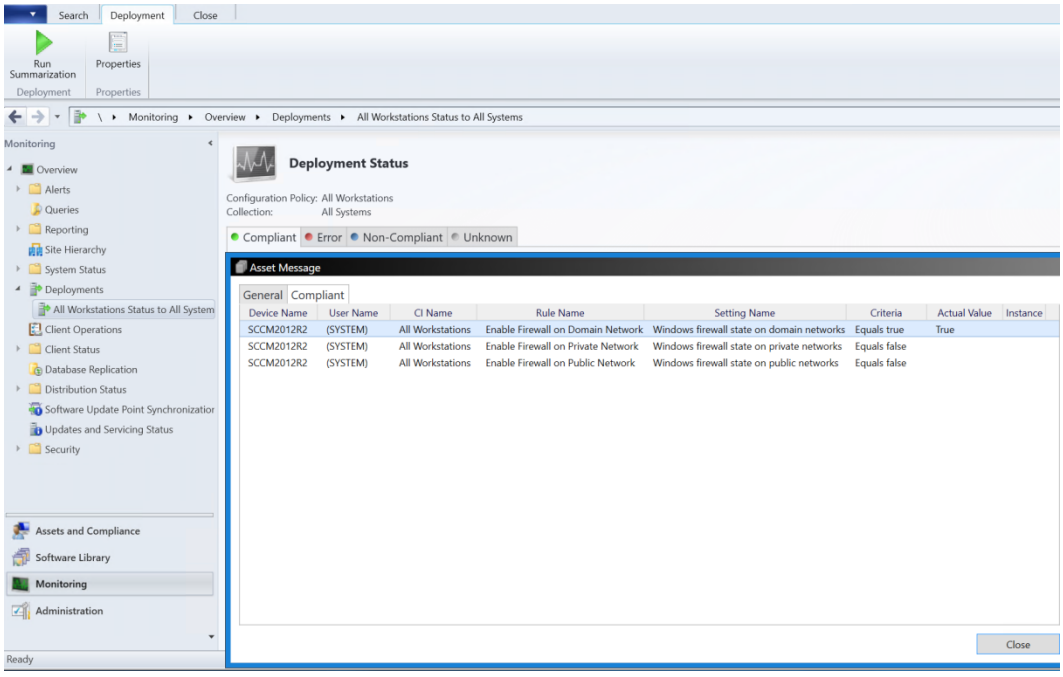
**NAME:** All Workstations
**TYPE:** None
**REVISION:** 1
**COMPLIANCE STATE:** Compliant
**NON-COMPLIANCE SEVERITY:** None
**DESCRIPTION:**

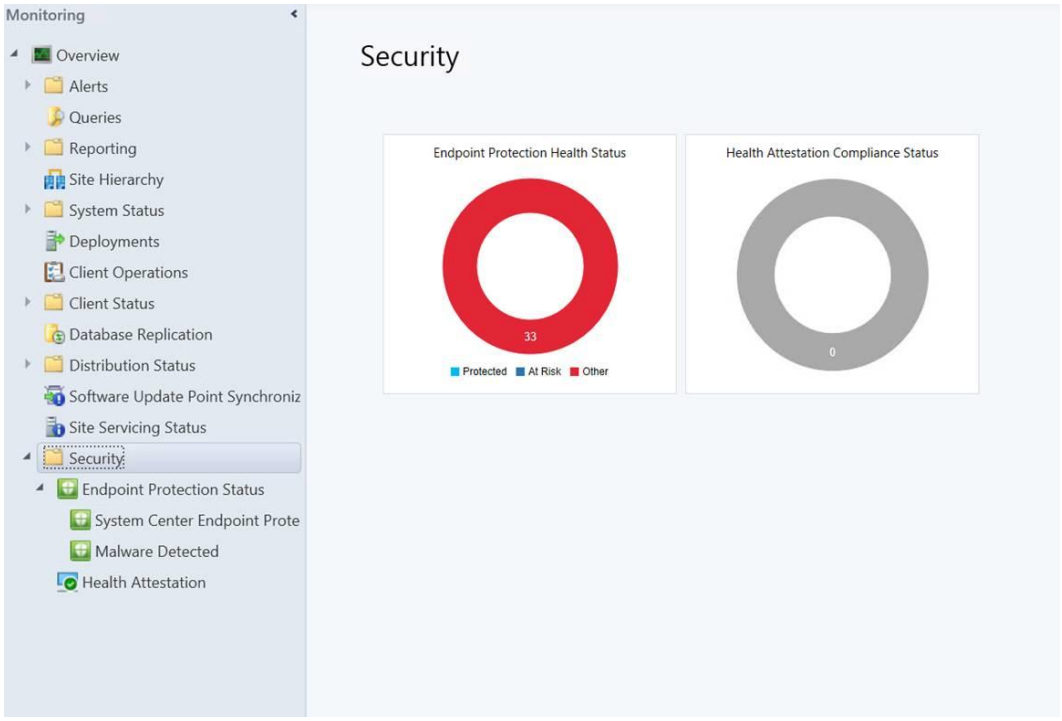
**Remediated Rules:**

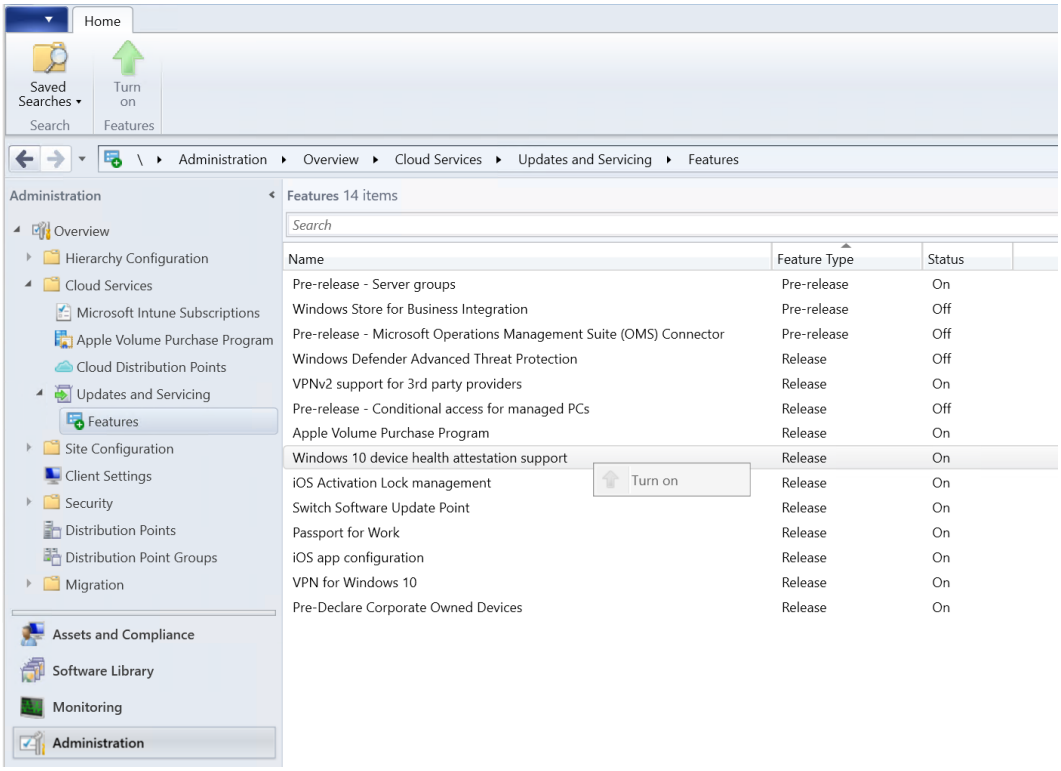
**Remediated Rule:**

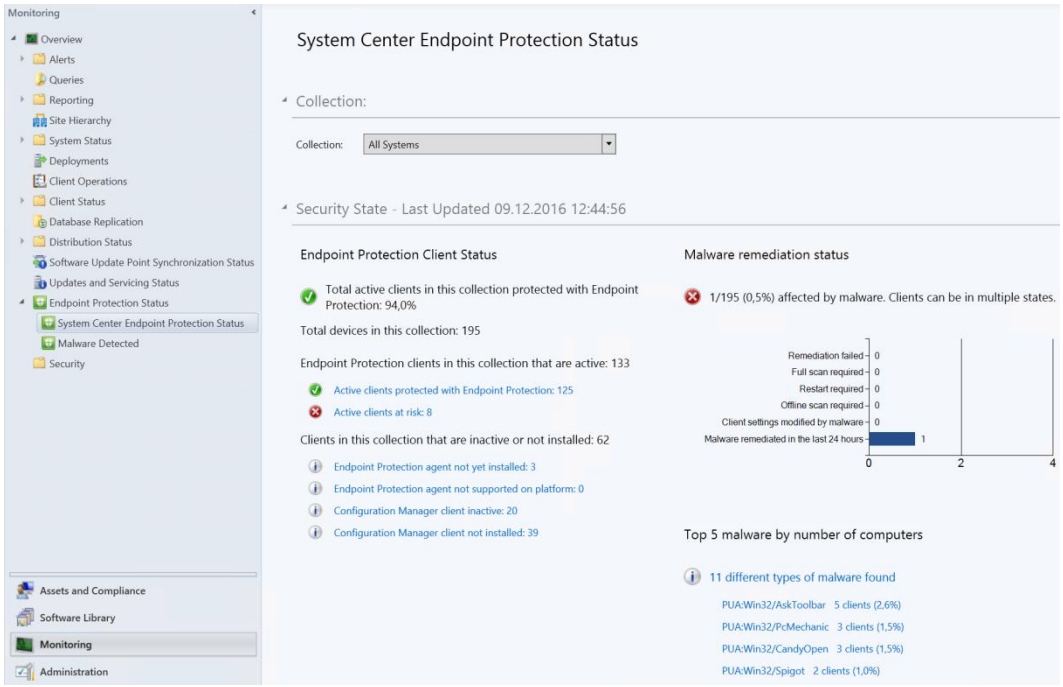
| Rule Name | Rule Description | Setting Name | Setting Type | Setting Description | Instance Data |
|---|---|---|---|---|---|
| Enable Firewall on Domain Network | | Windows firewall state on domain networks | None | Windows firewall state on domain networks | Expression: Equals true; Instance Source: ; Previous Value: False; Remediated Value: True |

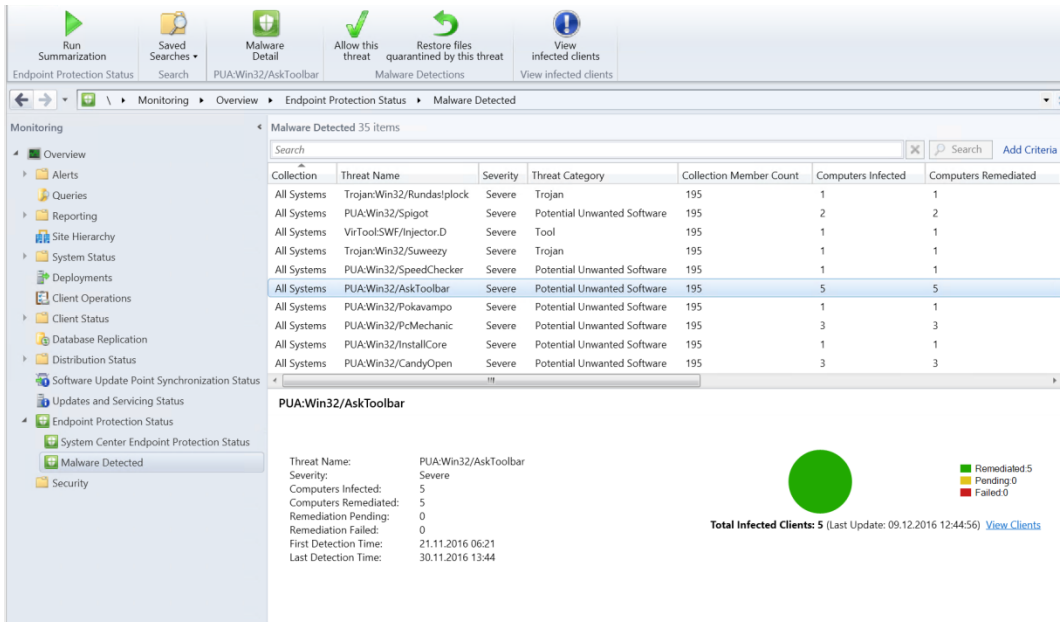

Windows Firewall
Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
For your security, some settings are managed by your system administrator.
Update your Firewall settings
Windows Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Firewall state:
Off
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active domain networks:
sccm.biz
Notification state:
Do not notify me when Windows Firewall blocks a new app
Private networks
Not connected
Guest or public networks
Not connected
See also
Action Center
Network and Sharing Center


Search
Deployment
Close
Run Summarization
Properties
Deployment
Properties
Monitoring ▸ Overview ▸ Deployments ▸ All Workstations Status to All Systems
Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Deployments
All Workstations Status to All System
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchronizatior
Updates and Servicing Status
Security
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Deployment Status
Configuration Policy: All Workstations
Collection: All Systems
Compliant
Error
Non-Compliant
Unknown
Asset Message
General
Compliant
Device Name
User Name
CI Name
Rule Name
Setting Name
Criteria
Actual Value
Instance
SCCM2012R2 (SYSTEM) All Workstations Enable Firewall on Domain Network Windows firewall state on domain networks Equals true True
SCCM2012R2 (SYSTEM) All Workstations Enable Firewall on Private Network Windows firewall state on private networks Equals false
SCCM2012R2 (SYSTEM) All Workstations Enable Firewall on Public Network Windows firewall state on public networks Equals false
Close


Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Deployments
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchroniz
Site Servicing Status
Security
Endpoint Protection Status
System Center Endpoint Prote
Malware Detected
Health Attestation
Security
Endpoint Protection Health Status
33
Protected
At Risk
Other
Health Attestation Compliance Status
0


Home
Saved Searches
Search
Turn on
Features
\ ▸ Administration ▸ Overview ▸ Cloud Services ▸ Updates and Servicing ▸ Features
Administration
Overview
Hierarchy Configuration
Cloud Services
Microsoft Intune Subscriptions
Apple Volume Purchase Program
Cloud Distribution Points
Updates and Servicing
Features
Site Configuration
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Assets and Compliance
Software Library
Monitoring
Administration
Features 14 items
Search
Name
Feature Type
Status
Pre-release - Server groups Pre-release On
Windows Store for Business Integration Pre-release Off
Pre-release - Microsoft Operations Management Suite (OMS) Connector Pre-release Off
Windows Defender Advanced Threat Protection Release Off
VPNv2 support for 3rd party providers Release On
Pre-release - Conditional access for managed PCs Release Off
Apple Volume Purchase Program Release On
Windows 10 device health attestation support Release On
iOS Activation Lock management Release On
Turn on
Switch Software Update Point Release On
Passport for Work Release On
iOS app configuration Release On
VPN for Windows 10 Release On
Pre-Declare Corporate Owned Devices Release On


Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Deployments
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchronization Status
Updates and Servicing Status
Endpoint Protection Status
System Center Endpoint Protection Status
Malware Detected
Security
Assets and Compliance
Software Library
Monitoring
Administration
System Center Endpoint Protection Status
Collection:
Collection: All Systems
Security State - Last Updated 09.12.2016 12:44:56
Endpoint Protection Client Status
Total active clients in this collection protected with Endpoint Protection: 94,0%
Total devices in this collection: 195
Endpoint Protection clients in this collection that are active: 133
Active clients protected with Endpoint Protection: 125
Active clients at risk: 8
Clients in this collection that are inactive or not installed: 62
Endpoint Protection agent not yet installed: 3
Endpoint Protection agent not supported on platform: 0
Configuration Manager client inactive: 20
Configuration Manager client not installed: 39
Malware remediation status
1/195 (0,5%) affected by malware. Clients can be in multiple states.
Remediation failed 0
Full scan required 0
Restart required 0
Offline scan required 0
Client settings modified by malware 0
Malware remediated in the last 24 hours 1
0
2
4
Top 5 malware by number of computers
11 different types of malware found
PUA:Win32/AskToolbar 5 clients (2,6%)
PUA:Win32/PcMechanic 3 clients (1,5%)
PUA:Win32/CandyOpen 3 clients (1,5%)
PUA:Win32/Spigot 2 clients (1,0%)


Run Summarization
Endpoint Protection Status
Saved Searches
Search
Malware Detail
PUA:Win32/AskToolbar
Allow this threat
Restore files quarantined by this threat
Malware Detections
View infected clients
View infected clients
Monitoring ▸ Overview ▸ Endpoint Protection Status ▸ Malware Detected
Malware Detected 35 items
Search
Add Criteria
Collection | Threat Name | Severity | Threat Category | Collection Member Count | Computers Infected | Computers Remediated
All Systems | Trojan:Win32/Rundas!plock | Severe | Trojan | 195 | 1 | 1
All Systems | PUA:Win32/Spigot | Severe | Potential Unwanted Software | 195 | 2 | 2
All Systems | VirTool:SWF/Injector.D | Severe | Tool | 195 | 1 | 1
All Systems | Trojan:Win32/Suweezy | Severe | Trojan | 195 | 1 | 1
All Systems | PUA:Win32/SpeedChecker | Severe | Potential Unwanted Software | 195 | 1 | 1
All Systems | PUA:Win32/AskToolbar | Severe | Potential Unwanted Software | 195 | 5 | 5
All Systems | PUA:Win32/Pokavampo | Severe | Potential Unwanted Software | 195 | 1 | 1
All Systems | PUA:Win32/PcMechanic | Severe | Potential Unwanted Software | 195 | 3 | 3
All Systems | PUA:Win32/InstallCore | Severe | Potential Unwanted Software | 195 | 1 | 1
All Systems | PUA:Win32/CandyOpen | Severe | Potential Unwanted Software | 195 | 3 | 3
PUA:Win32/AskToolbar
Threat Name: PUA:Win32/AskToolbar
Severity: Severe
Computers Infected: 5
Computers Remediated: 5
Remediation Pending: 0
Remediation Failed: 0
First Detection Time: 21.11.2016 06:21
Last Detection Time: 30.11.2016 13:44
Remediated:5
Pending:0
Failed:0
Total Infected Clients: 5 (Last Update: 09.12.2016 12:44:56) View Clients

SQL Server Reporting Services

# Endpoint Protection

Delete | Move | New Folder | New Data Source | Report Builder | Folder Settings | Upload File

| Type | Name ↓ | Description |
|---|---|---|
| | Endpoint Protection - Hidden | |
| | Antimalware activity report | This report shows an overview of antimalware activity. |
| | Antimalware overall status and history | Antimalware Overall Status and History |
| | Computer malware details | This report shows details about a particular computer and the list of malware found on it. |
| | Infected computers | This report shows a list of computers with a particular threat detected. |
| | Top users by threats | This report shows the list of users with the most number of detected threats. |
| | User threat list | This report shows the list of threats found under a particular user account. |

Microsoft System Center Configuration Manager

# Antimalware activity report

⊞ Description

⊞ Description

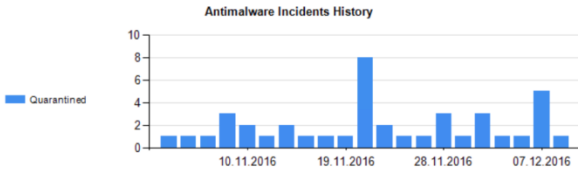
## Computer Infection Status Summary

| Computers with failed remediations | Computers with remediations with pending actions | Computers with successful remediations | Total Remediations |
|---|---|---|---|
| 0 | 0 | 12 | 12 |

⊞ Description

## Antimalware Incidents History

| Cleaning Action | Incidents Count | Computers |
|---|---|---|
| Quarantined | 41 | 12 |



Microsoft System Center Configuration Manager

## Top malware by severity

Description

### Top Malware By Severity

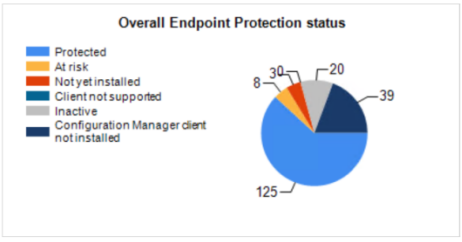
All

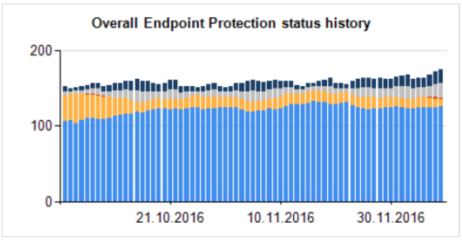
| Threat Name | Category | Severity | Computers | Incidents Count | First Detection (UTC) | Latest Detection (UTC) |
|---|---|---|---|---|---|---|
| PUA:Win32/AskToolbar | Potentially Unwanted Software | Severe | 5 | 6 | 21.11.2016 05:21:16 | 30.11.2016 12:44:49 |
| PUA:Win32/CandyOpen | Potentially Unwanted Software | Severe | 3 | 4 | 08.11.2016 15:22:19 | 22.11.2016 19:43:29 |
| PUA:Win32/PcMechanic | Potentially Unwanted Software | Severe | 3 | 3 | 21.11.2016 06:15:38 | 28.11.2016 08:04:00 |
| PUA:Win32/Spigot | Potentially Unwanted Software | Severe | 2 | 2 | 21.11.2016 09:29:22 | 21.11.2016 22:02:48 |
| Trojan:Win32/Rundas!plock | Trojan | Severe | 1 | 1 | 15.11.2016 08:36:47 | 15.11.2016 08:36:47 |
| Trojan:Win32/Suweezy | Trojan | Severe | 1 | 1 | 10.11.2016 07:48:10 | 10.11.2016 07:48:10 |
| TrojanDownloader:JS/NeutrinoEK.Y | Trojan Downloader | Severe | 1 | 3 | 07.12.2016 07:43:03 | 07.12.2016 07:44:12 |
| VirTool:SWF/Injector.D | Tool | Severe | 1 | 1 | 07.12.2016 07:43:30 | 07.12.2016 07:43:30 |
| PUA:Win32/Pokavampo | Potentially Unwanted Software | Severe | 1 | 1 | 09.11.2016 15:41:22 | 09.11.2016 15:41:22 |
| PUA:Win32/SpeedChecker | Potentially Unwanted Software | Severe | 1 | 1 | 09.11.2016 15:40:51 | 09.11.2016 15:40:51 |
| PUA:Win32/InstallCore | Potentially Unwanted Software | Severe | 1 | 18 | 04.11.2016 08:08:05 | 08.12.2016 13:41:07 |

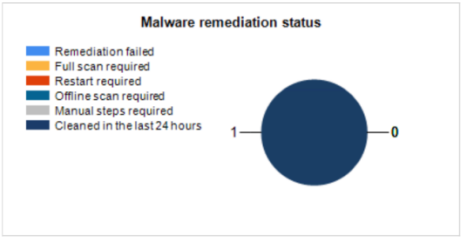
Microsoft System Center Configuration Manager

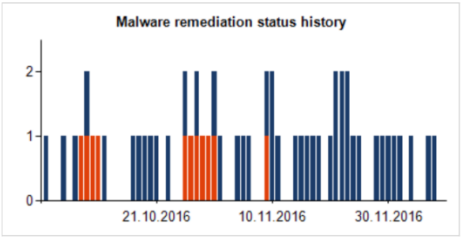
## Antimalware overall status and history

Description

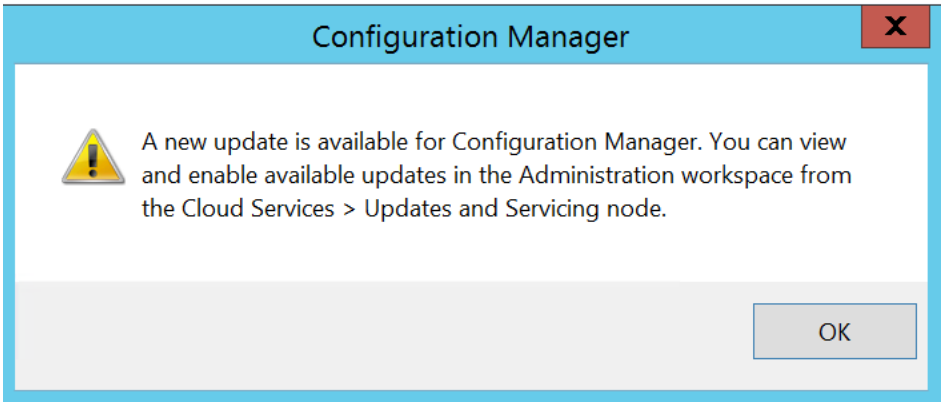


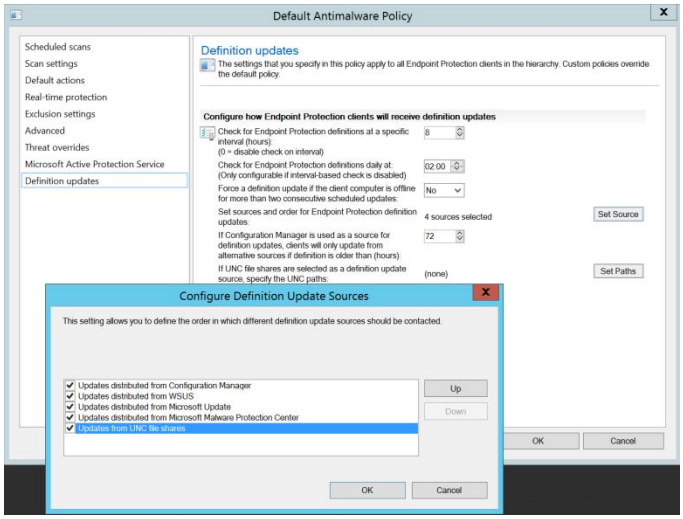



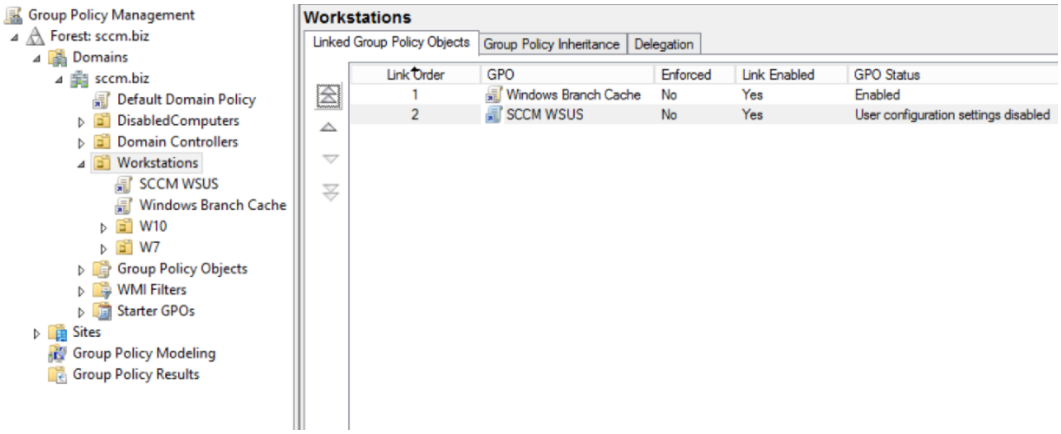



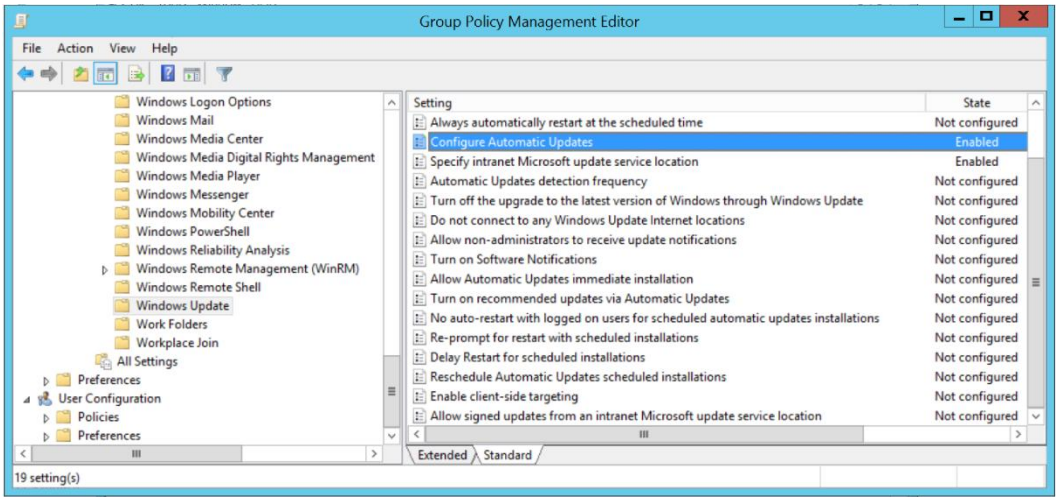



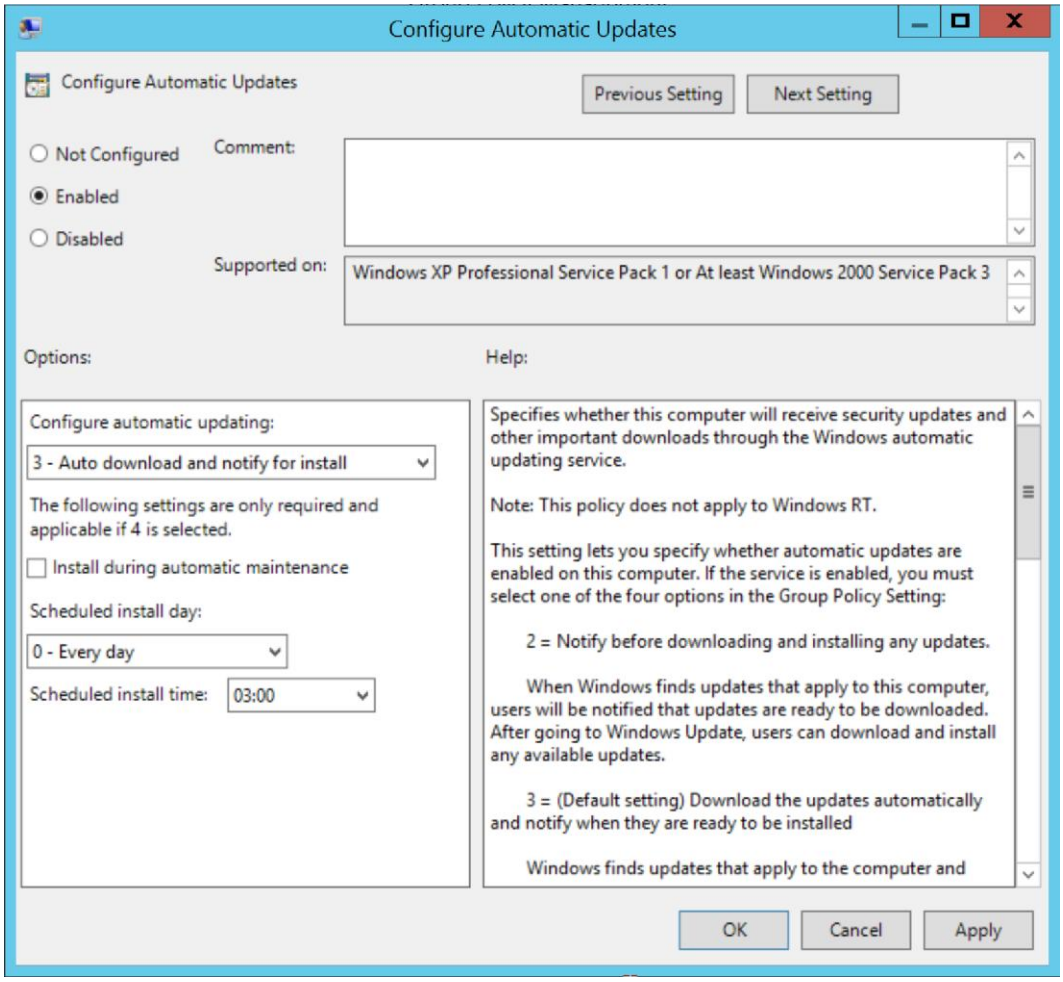
# Chapter 4: Updates

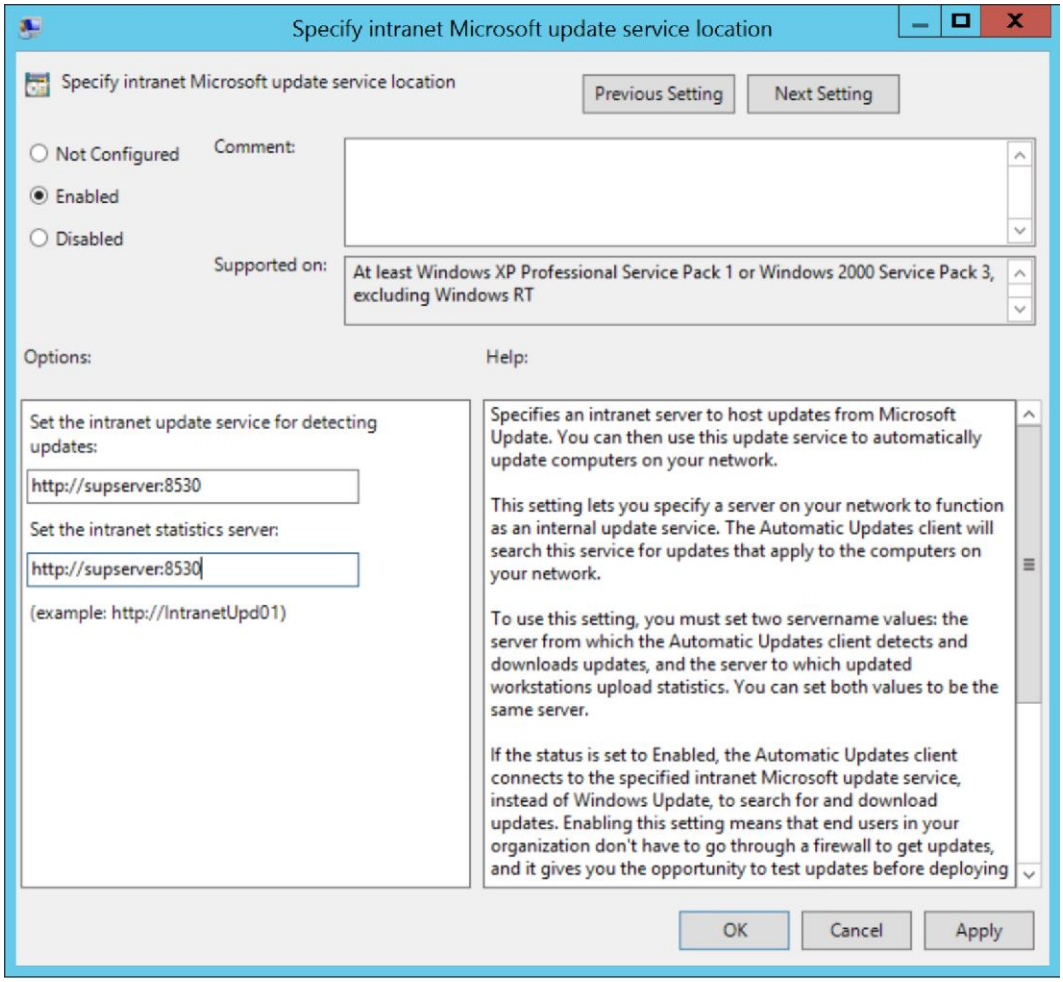


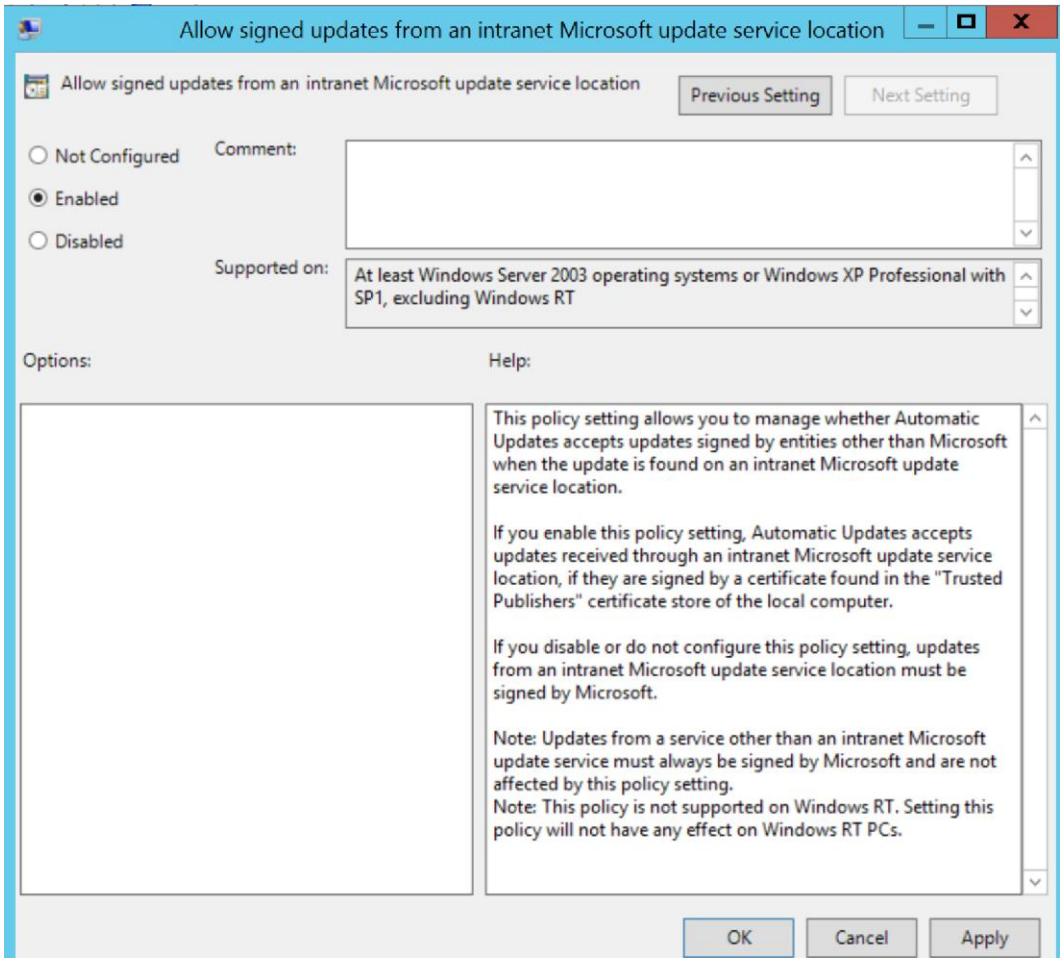




Group Policy Management
Forest: sccm.biz
Domains
sccm.biz
Default Domain Policy
DisabledComputers
Domain Controllers
Workstations
SCCM WSUS
Windows Branch Cache
W10
W7
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Workstations
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
1
Windows Branch Cache
No
Yes
Enabled
2
SCCM WSUS
No
Yes
User configuration settings disabled

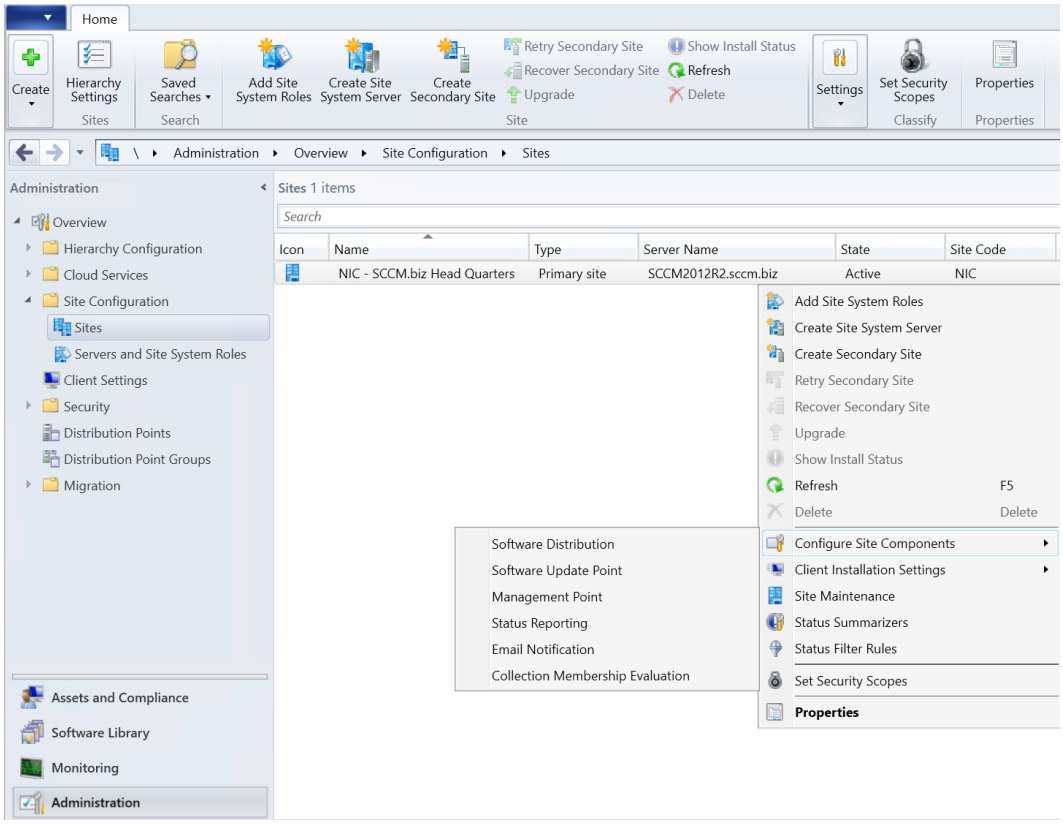

Group Policy Management Editor
File
Action
View
Help
Windows Logon Options
Windows Mail
Windows Media Center
Windows Media Digital Rights Management
Windows Media Player
Windows Messenger
Windows Mobility Center
Windows PowerShell
Windows Reliability Analysis
Windows Remote Management (WinRM)
Windows Remote Shell
Windows Update
Work Folders
Workplace Join
All Settings
Preferences
User Configuration
Policies
Preferences
Setting
State
Always automatically restart at the scheduled time
Not configured
Configure Automatic Updates
Enabled
Specify intranet Microsoft update service location
Enabled
Automatic Updates detection frequency
Not configured
Turn off the upgrade to the latest version of Windows through Windows Update
Not configured
Do not connect to any Windows Update Internet locations
Not configured
Allow non-administrators to receive update notifications
Not configured
Turn on Software Notifications
Not configured
Allow Automatic Updates immediate installation
Not configured
Turn on recommended updates via Automatic Updates
Not configured
No auto-restart with logged on users for scheduled automatic updates installations
Not configured
Re-prompt for restart with scheduled installations
Not configured
Delay Restart for scheduled installations
Not configured
Reschedule Automatic Updates scheduled installations
Not configured
Enable client-side targeting
Not configured
Allow signed updates from an intranet Microsoft update service location
Not configured
Extended
Standard
19 setting(s)

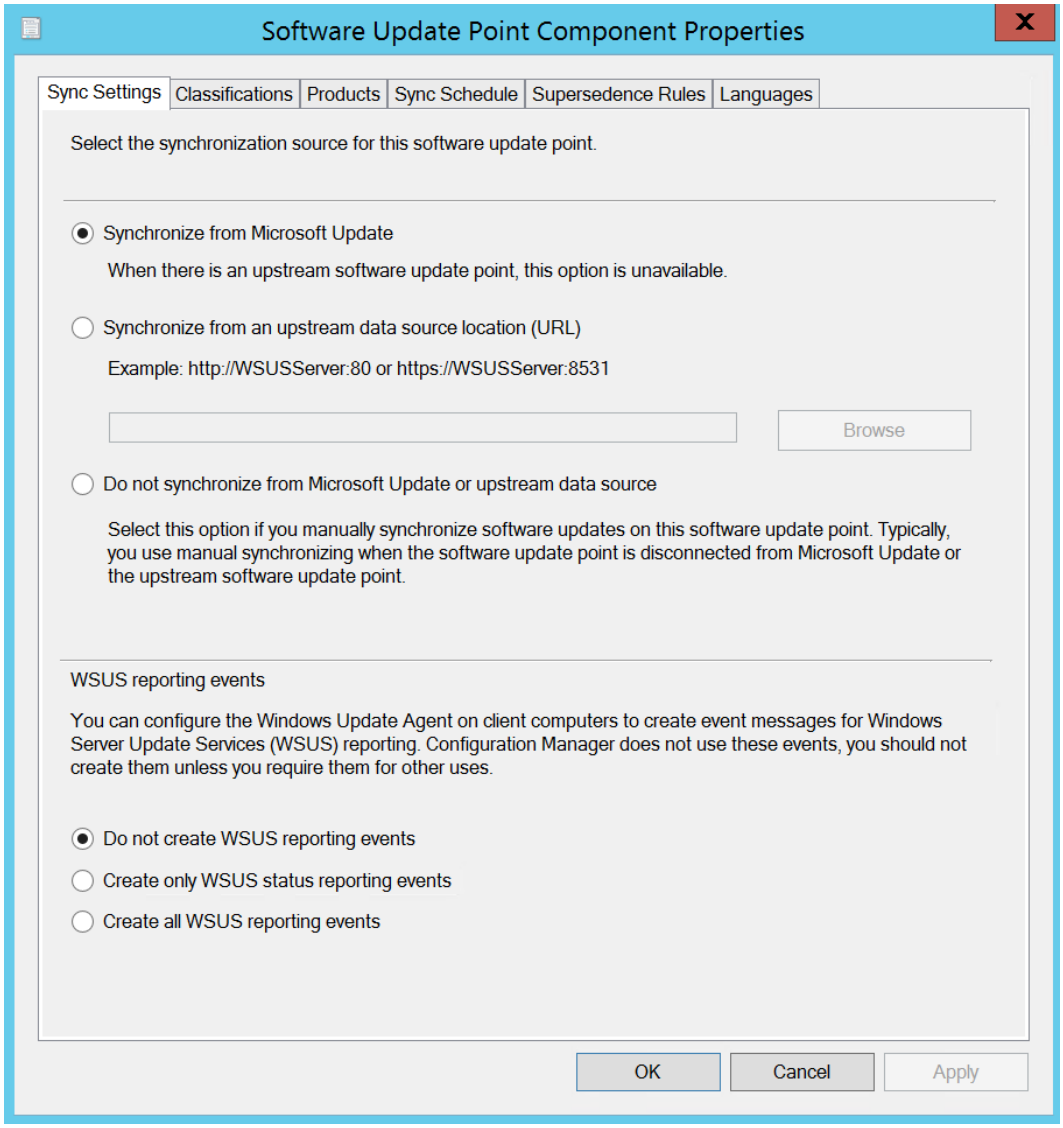

Configure Automatic Updates
Configure Automatic Updates
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3
Options:
Help:
Configure automatic updating:
3 - Auto download and notify for install
The following settings are only required and applicable if 4 is selected.
Install during automatic maintenance
Scheduled install day:
0 - Every day
Scheduled install time:
03:00
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.
Note: This policy does not apply to Windows RT.
This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:
2 = Notify before downloading and installing any updates.
When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.
3 = (Default setting) Download the updates automatically and notify when they are ready to be installed
Windows finds updates that apply to the computer and
OK
Cancel
Apply

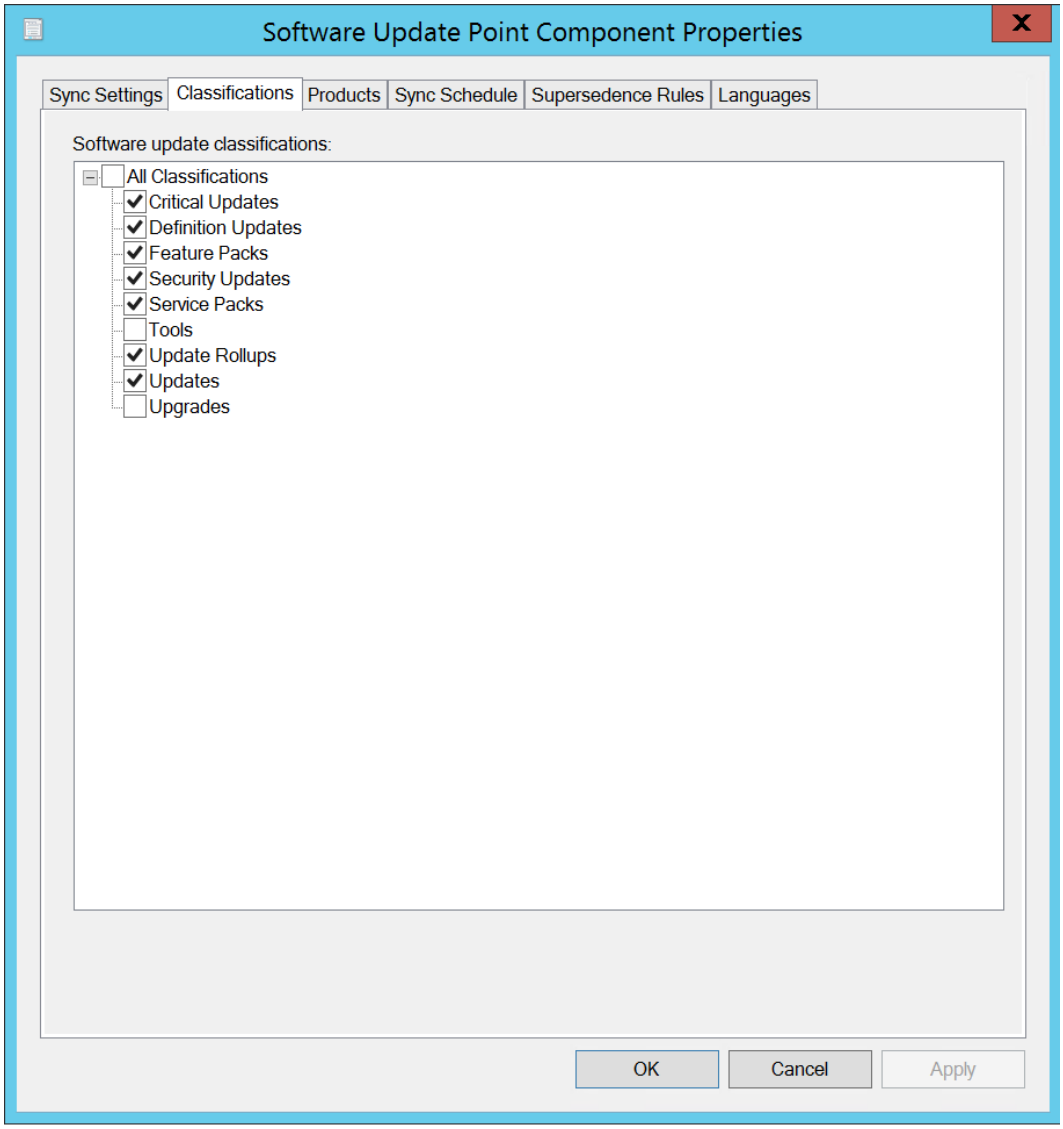

Specify intranet Microsoft update service location
Specify intranet Microsoft update service location
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT
Options:
Help:
Set the intranet update service for detecting updates:
http://supserver:8530
Set the intranet statistics server:
http://supserver:8530
(example: http://IntranetUpd01)
Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.
This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.
To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.
If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying
OK
Cancel
Apply

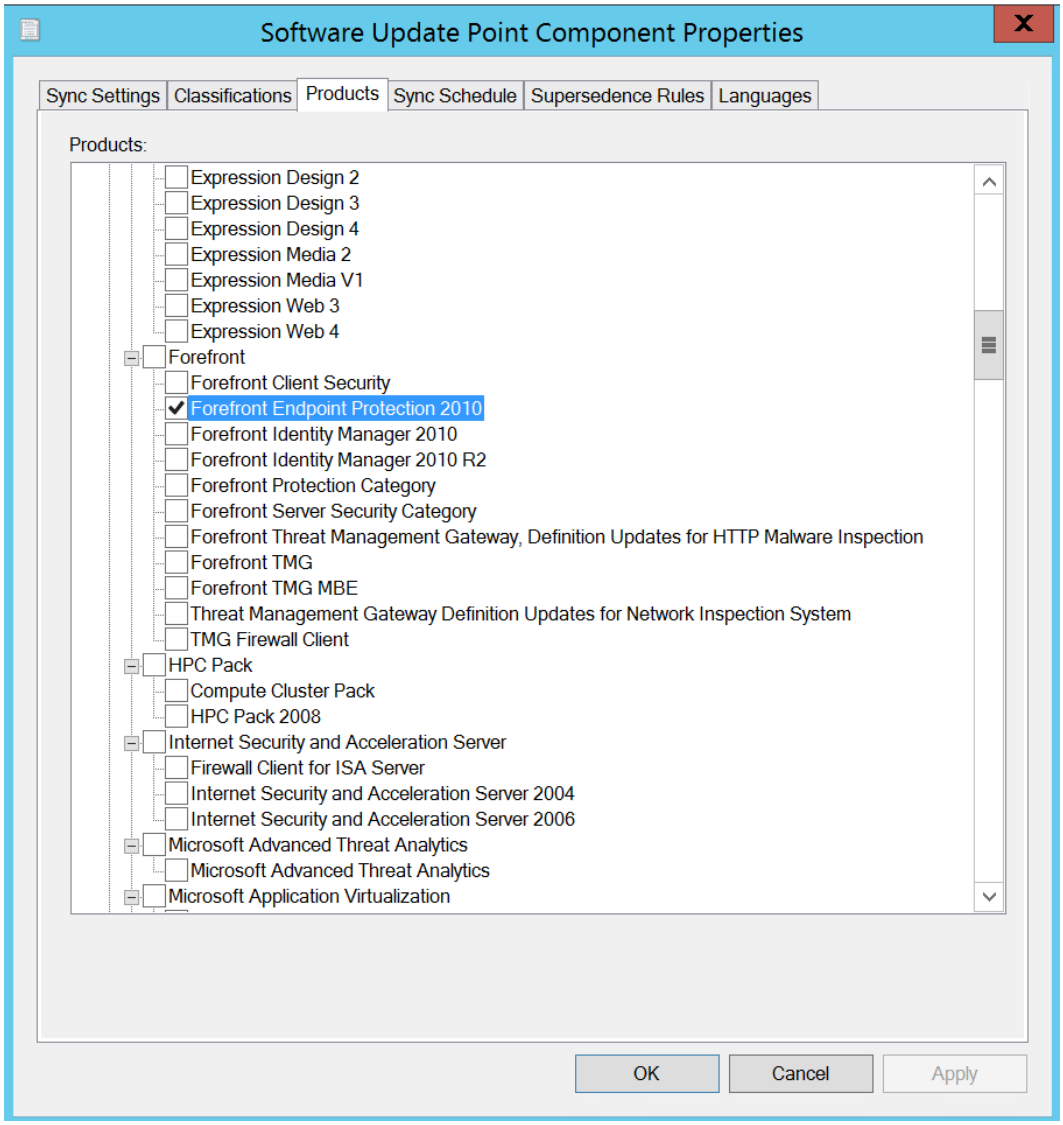


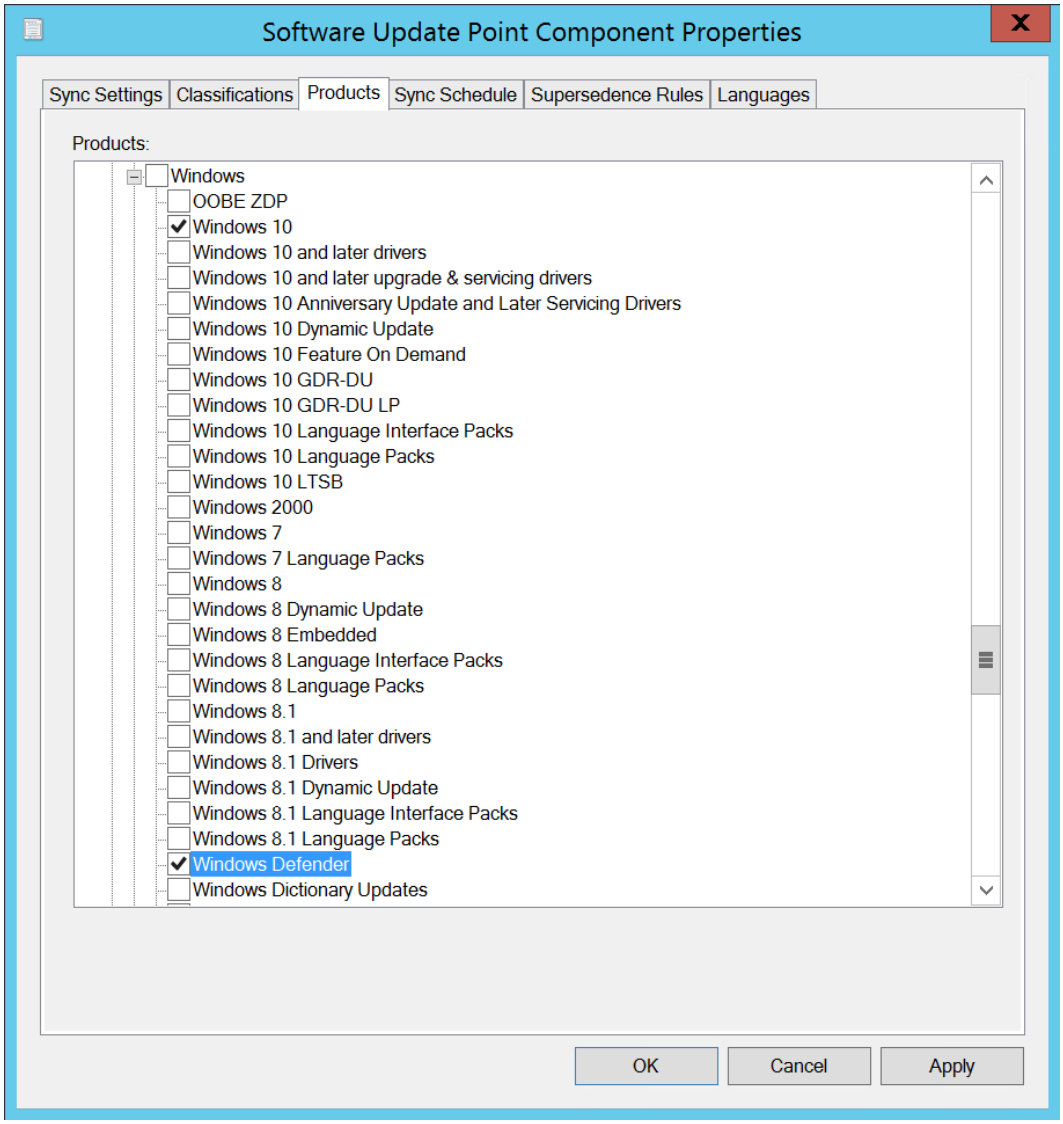

Download http://wsus.ds.download.windowsupdate.com/c/msdownload/update/software/defu/2014/07/am_delta_patch_1.177.1796
Download http://wsus.ds.download.windowsupdate.com/c/msdownload/update/software/defu/2014/07/am_delta_patch_1.177.1796
Download http://wsus.ds.download.windowsupdate.com/c/msdownload/update/software/defu/2014/07/am_delta_patch_1.177.1796
Download http://wsus.ds.download.windowsupdate.com/c/msdownload/update/software/defu/2014/07/am_delta_patch_1.177.1796
ERROR: DownloadContentFiles() failed with hr=0x80072ee2

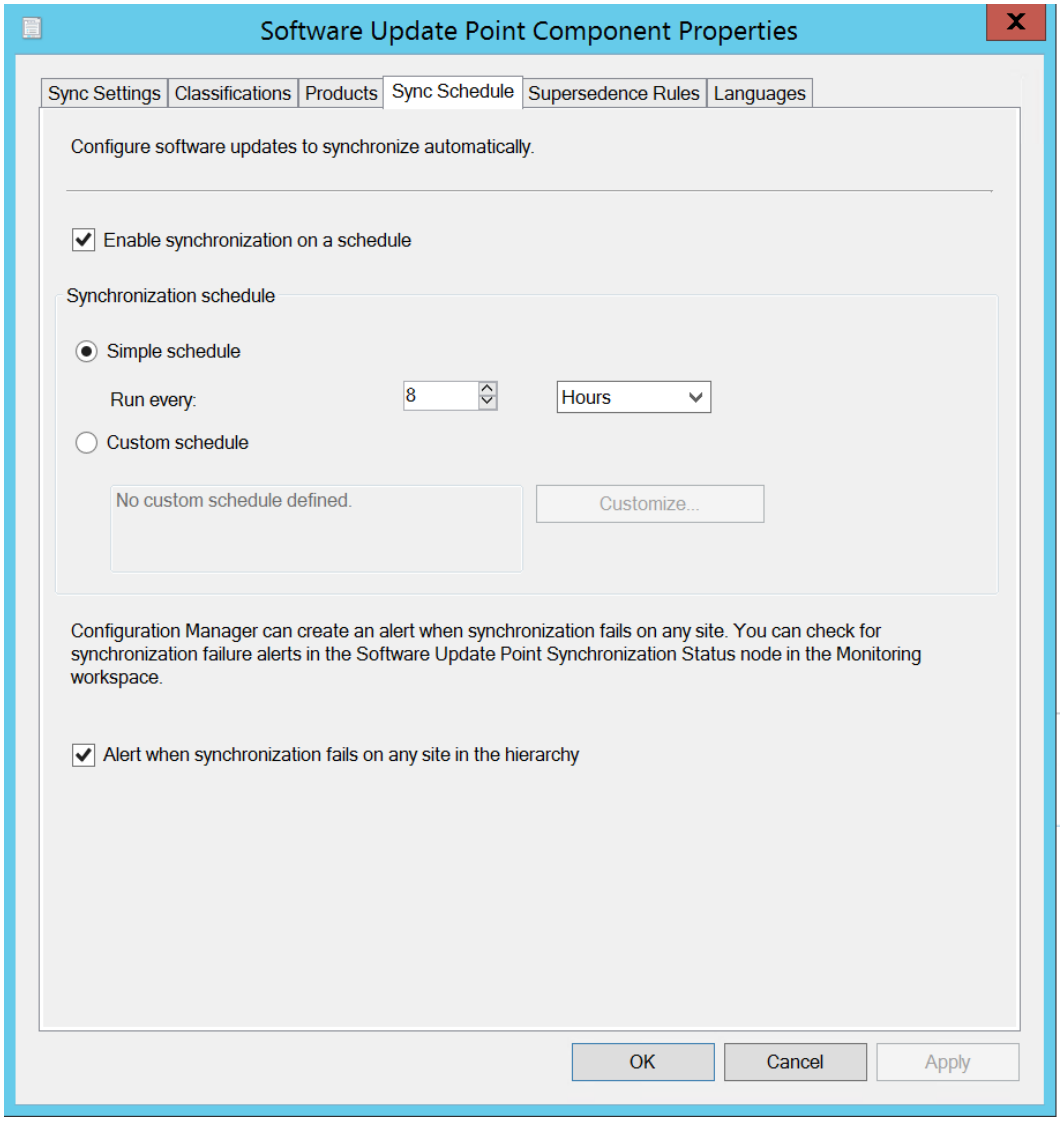

Home
Create
Hierarchy Settings
Sites
Saved Searches
Search
Add Site System Roles
Create Site System Server
Create Secondary Site
Retry Secondary Site
Recover Secondary Site
Upgrade
Show Install Status
Refresh
Delete
Site
Settings
Set Security Scopes
Classify
Properties
Properties
\ ▸ Administration ▸ Overview ▸ Site Configuration ▸ Sites
Administration
Overview
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Assets and Compliance
Software Library
Monitoring
Administration
Sites 1 items
Search
Icon
Name
Type
Server Name
State
Site Code
NIC - SCCM.biz Head Quarters
Primary site
SCCM2012R2.sccm.biz
Active
NIC
Add Site System Roles
Create Site System Server
Create Secondary Site
Retry Secondary Site
Recover Secondary Site
Upgrade
Show Install Status
Refresh F5
Delete Delete
Configure Site Components
Client Installation Settings
Site Maintenance
Status Summarizers
Status Filter Rules
Set Security Scopes
Properties
Software Distribution
Software Update Point
Management Point
Status Reporting
Email Notification
Collection Membership Evaluation

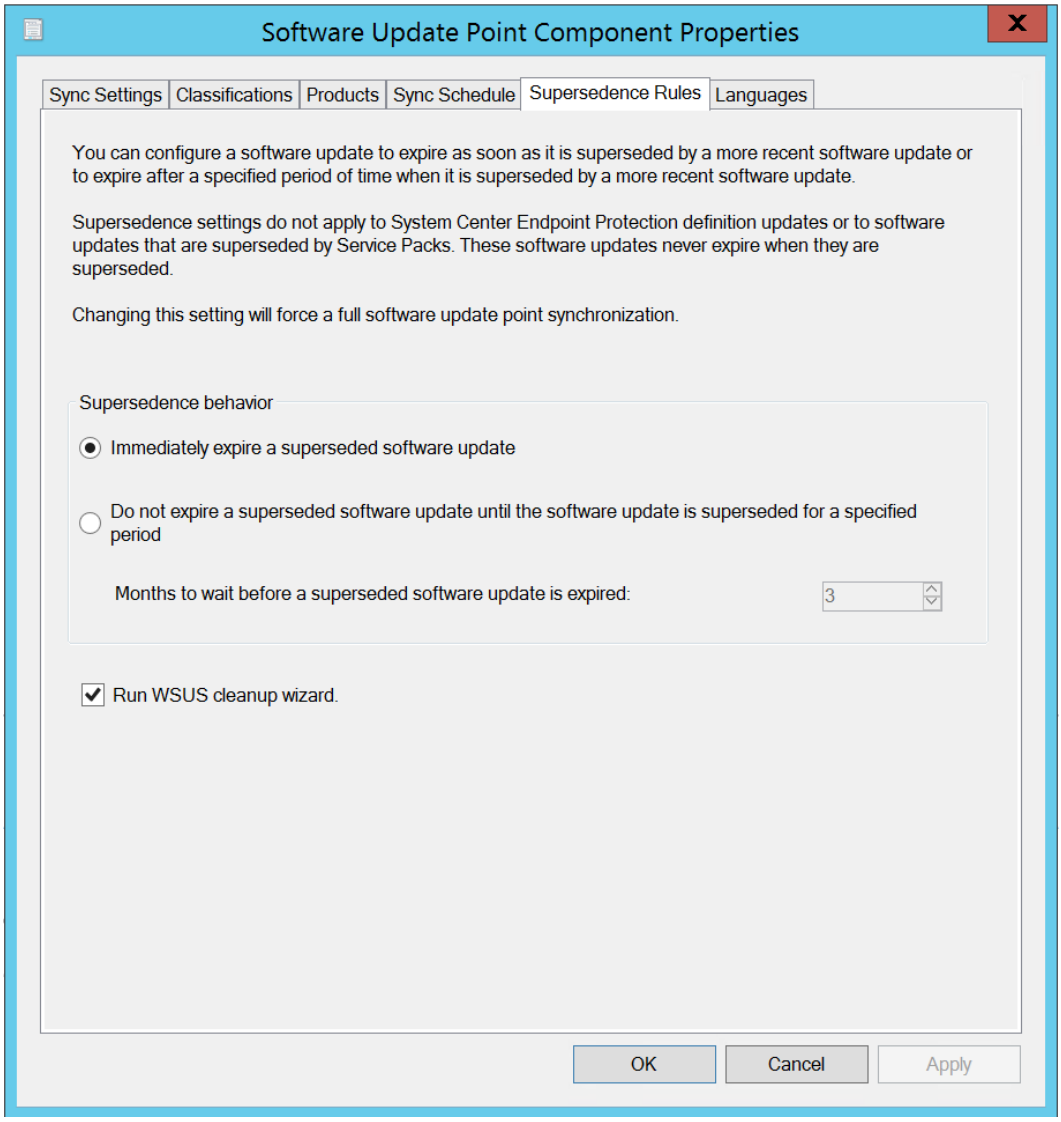

Software Update Point Component Properties
Sync Settings
Classifications
Products
Sync Schedule
Supersedence Rules
Languages
Select the synchronization source for this software update point.
Synchronize from Microsoft Update
When there is an upstream software update point, this option is unavailable.
Synchronize from an upstream data source location (URL)
Example: http://WSUSServer:80 or https://WSUSServer:8531
Browse
Do not synchronize from Microsoft Update or upstream data source
Select this option if you manually synchronize software updates on this software update point. Typically, you use manual synchronizing when the software update point is disconnected from Microsoft Update or the upstream software update point.
WSUS reporting events
You can configure the Windows Update Agent on client computers to create event messages for Windows Server Update Services (WSUS) reporting. Configuration Manager does not use these events, you should not create them unless you require them for other uses.
Do not create WSUS reporting events
Create only WSUS status reporting events
Create all WSUS reporting events
OK
Cancel
Apply

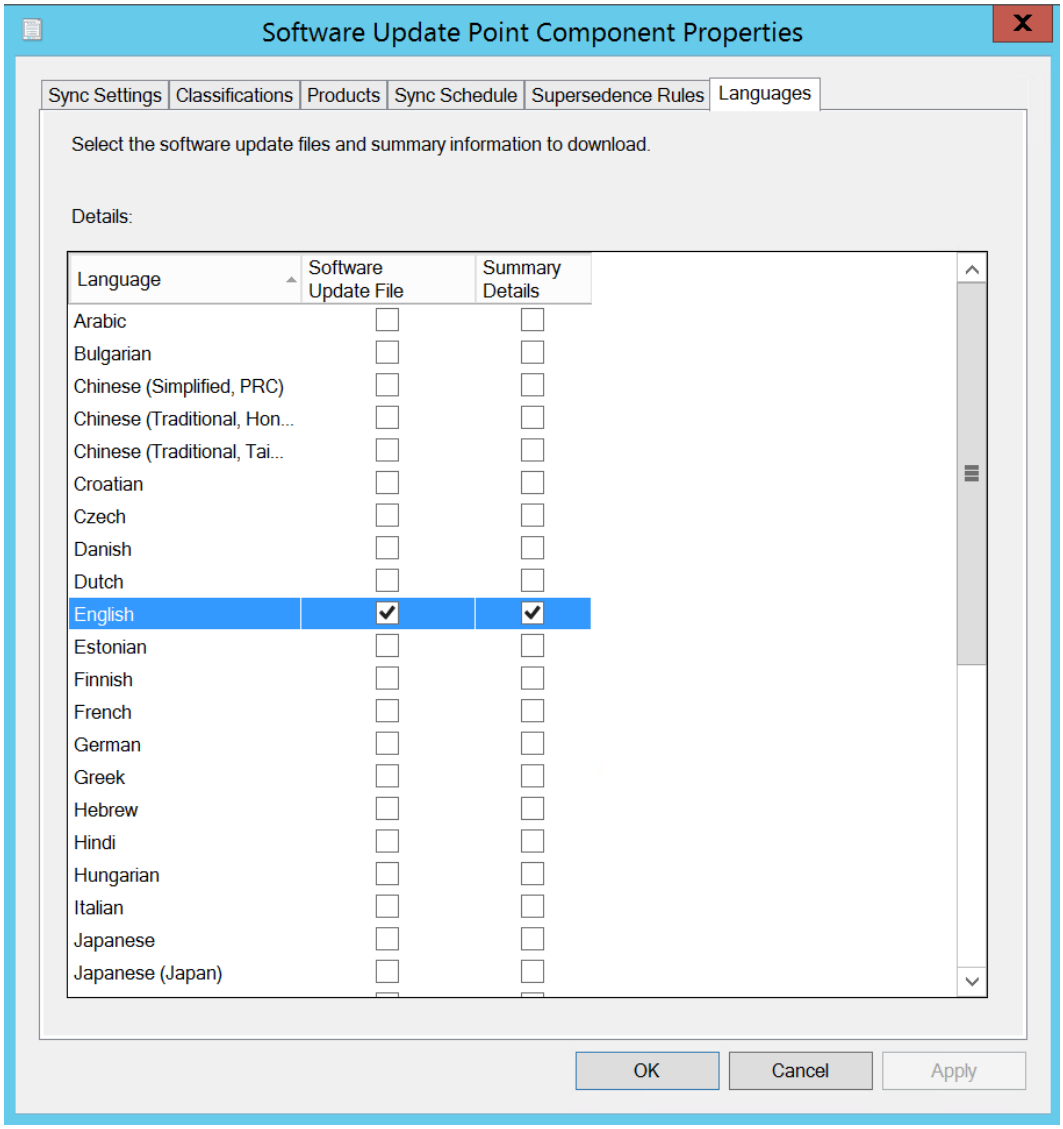

Software Update Point Component Properties
Sync Settings
Classifications
Products
Sync Schedule
Supersedence Rules
Languages
Software update classifications:
All Classifications
Critical Updates
Definition Updates
Feature Packs
Security Updates
Service Packs
Tools
Update Rollups
Updates
Upgrades
OK
Cancel
Apply

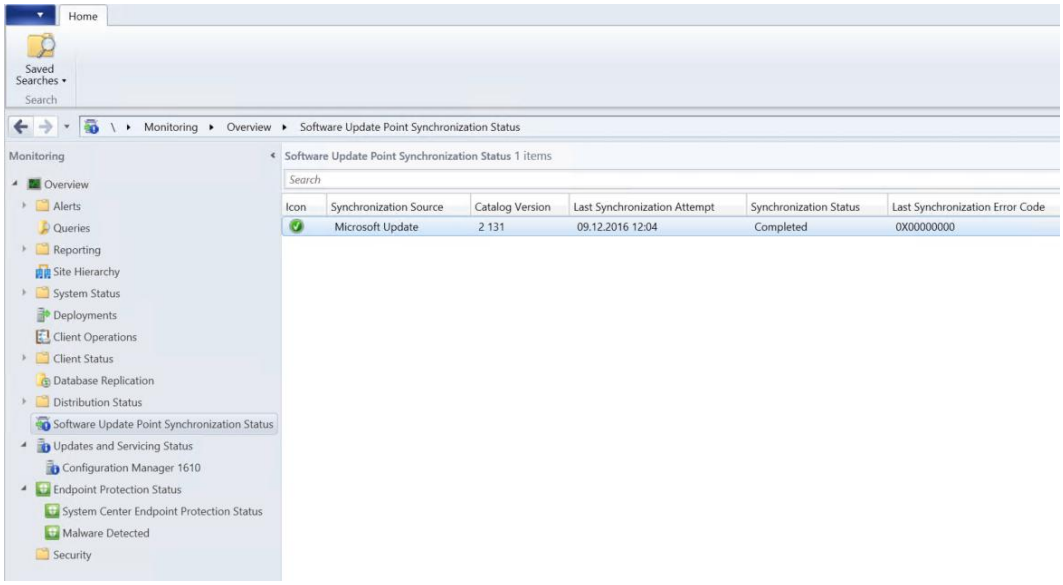

Software Update Point Component Properties
Sync Settings
Classifications
Products
Sync Schedule
Supersedence Rules
Languages
Products:
Expression Design 2
Expression Design 3
Expression Design 4
Expression Media 2
Expression Media V1
Expression Web 3
Expression Web 4
Forefront
Forefront Client Security
Forefront Endpoint Protection 2010
Forefront Identity Manager 2010
Forefront Identity Manager 2010 R2
Forefront Protection Category
Forefront Server Security Category
Forefront Threat Management Gateway, Definition Updates for HTTP Malware Inspection
Forefront TMG
Forefront TMG MBE
Threat Management Gateway Definition Updates for Network Inspection System
TMG Firewall Client
HPC Pack
Compute Cluster Pack
HPC Pack 2008
Internet Security and Acceleration Server
Firewall Client for ISA Server
Internet Security and Acceleration Server 2004
Internet Security and Acceleration Server 2006
Microsoft Advanced Threat Analytics
Microsoft Advanced Threat Analytics
Microsoft Application Virtualization
OK
Cancel
Apply

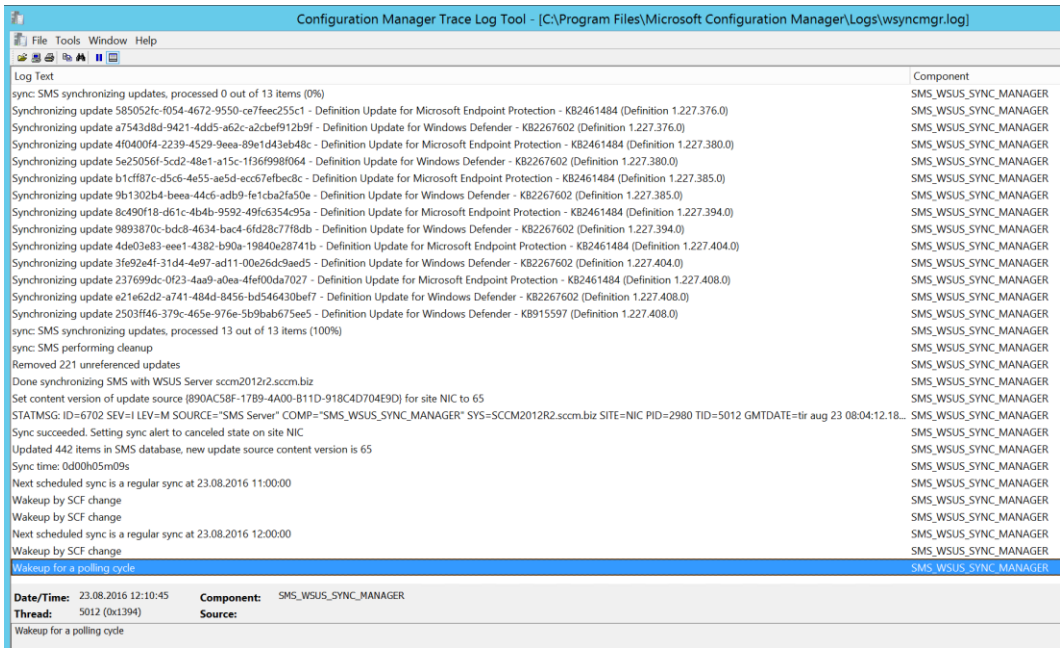

Software Update Point Component Properties
Sync Settings
Classifications
Products
Sync Schedule
Supersedence Rules
Languages
Products:
Windows
OOBE ZDP
Windows 10
Windows 10 and later drivers
Windows 10 and later upgrade & servicing drivers
Windows 10 Anniversary Update and Later Servicing Drivers
Windows 10 Dynamic Update
Windows 10 Feature On Demand
Windows 10 GDR-DU
Windows 10 GDR-DU LP
Windows 10 Language Interface Packs
Windows 10 Language Packs
Windows 10 LTSB
Windows 2000
Windows 7
Windows 7 Language Packs
Windows 8
Windows 8 Dynamic Update
Windows 8 Embedded
Windows 8 Language Interface Packs
Windows 8 Language Packs
Windows 8.1
Windows 8.1 and later drivers
Windows 8.1 Drivers
Windows 8.1 Dynamic Update
Windows 8.1 Language Interface Packs
Windows 8.1 Language Packs
Windows Defender
Windows Dictionary Updates
OK
Cancel
Apply

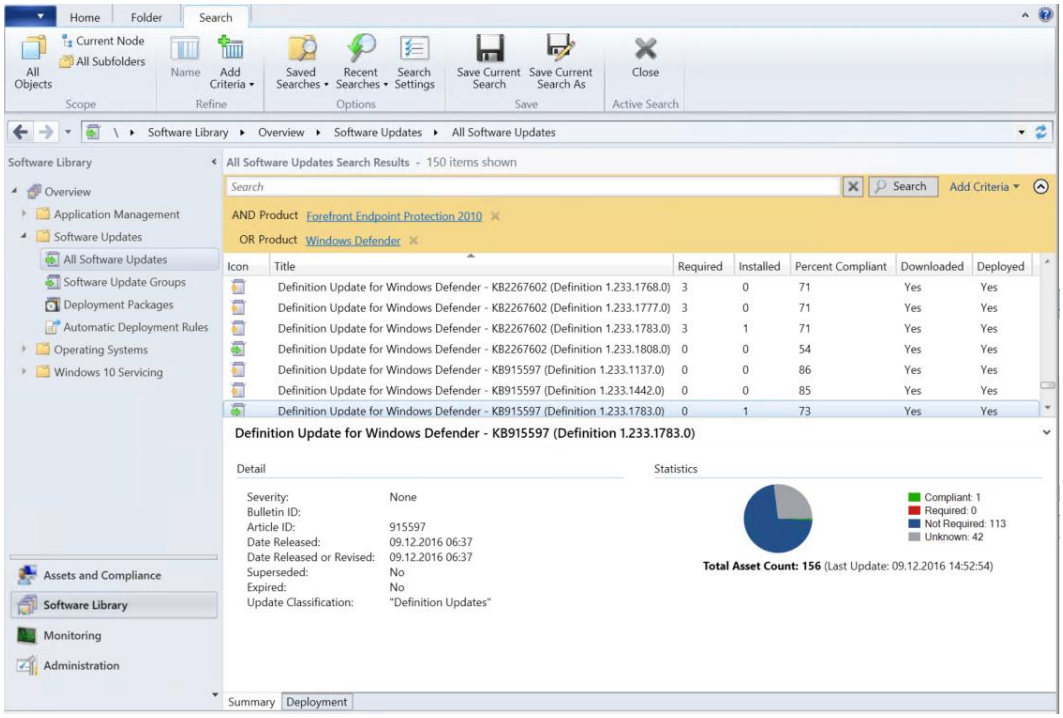

Software Update Point Component Properties
Sync Settings
Classifications
Products
Sync Schedule
Supersedence Rules
Languages
Configure software updates to synchronize automatically.
Enable synchronization on a schedule
Synchronization schedule
Simple schedule
Run every:
8
Hours
Custom schedule
No custom schedule defined.
Customize...
Configuration Manager can create an alert when synchronization fails on any site. You can check for synchronization failure alerts in the Software Update Point Synchronization Status node in the Monitoring workspace.
Alert when synchronization fails on any site in the hierarchy
OK
Cancel
Apply

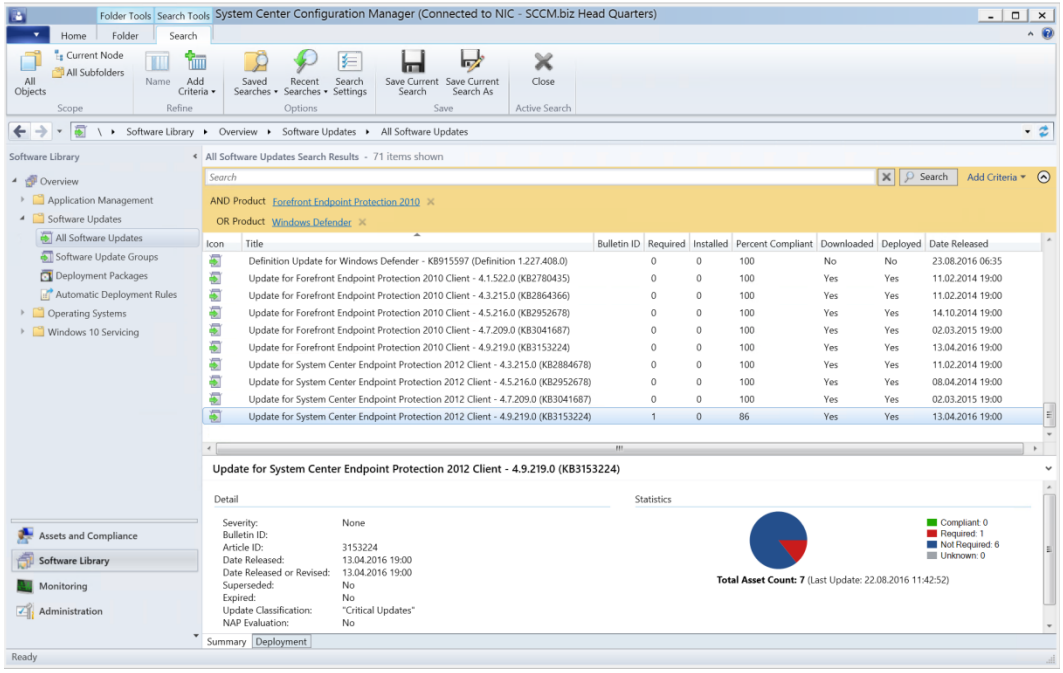

Software Update Point Component Properties
Sync Settings
Classifications
Products
Sync Schedule
Supersedence Rules
Languages
You can configure a software update to expire as soon as it is superseded by a more recent software update or to expire after a specified period of time when it is superseded by a more recent software update.
Supersedence settings do not apply to System Center Endpoint Protection definition updates or to software updates that are superseded by Service Packs. These software updates never expire when they are superseded.
Changing this setting will force a full software update point synchronization.
Supersedence behavior
Immediately expire a superseded software update
Do not expire a superseded software update until the software update is superseded for a specified period
Months to wait before a superseded software update is expired:
3
Run WSUS cleanup wizard.
OK
Cancel
Apply

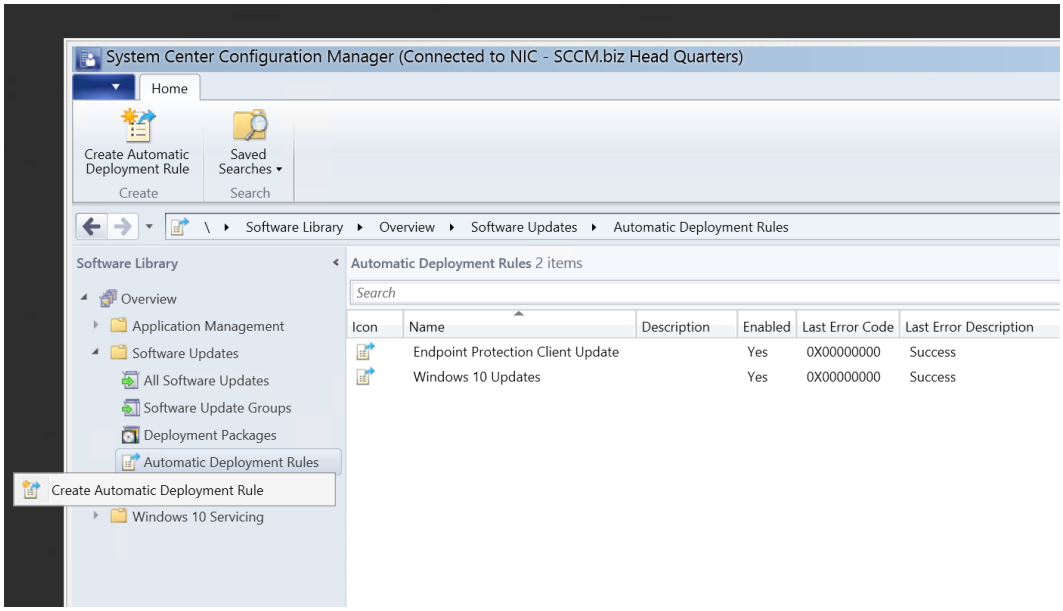

Software Update Point Component Properties
Sync Settings
Classifications
Products
Sync Schedule
Supersedence Rules
Languages
Select the software update files and summary information to download.
Details:
Language
Software Update File
Summary Details
Arabic
Bulgarian
Chinese (Simplified, PRC)
Chinese (Traditional, Hon...
Chinese (Traditional, Tai...
Croatian
Czech
Danish
Dutch
English
Estonian
Finnish
French
German
Greek
Hebrew
Hindi
Hungarian
Italian
Japanese
Japanese (Japan)
OK
Cancel
Apply

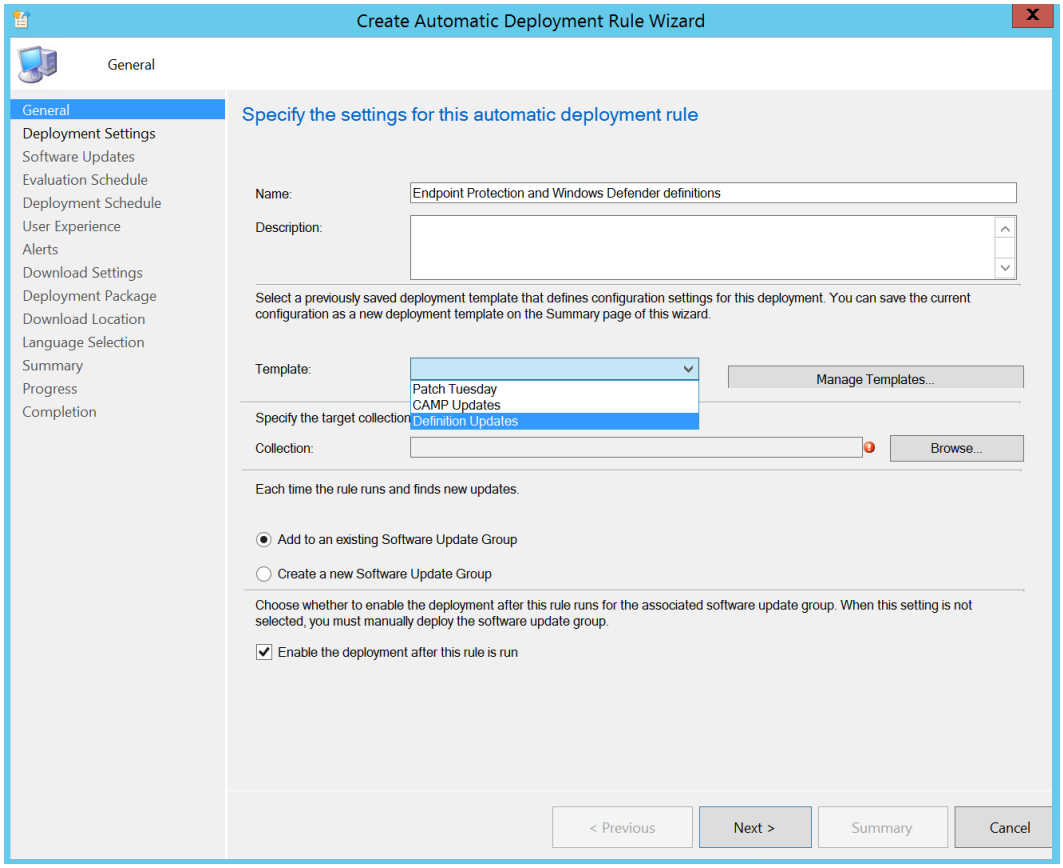

Home
Saved Searches
Search
Monitoring ▸ Overview ▸ Software Update Point Synchronization Status
Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Deployments
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchronization Status
Updates and Servicing Status
Configuration Manager 1610
Endpoint Protection Status
System Center Endpoint Protection Status
Malware Detected
Security
Software Update Point Synchronization Status 1 items
Search
Icon
Synchronization Source
Catalog Version
Last Synchronization Attempt
Synchronization Status
Last Synchronization Error Code
Microsoft Update
2 131
09.12.2016 12:04
Completed
0X00000000

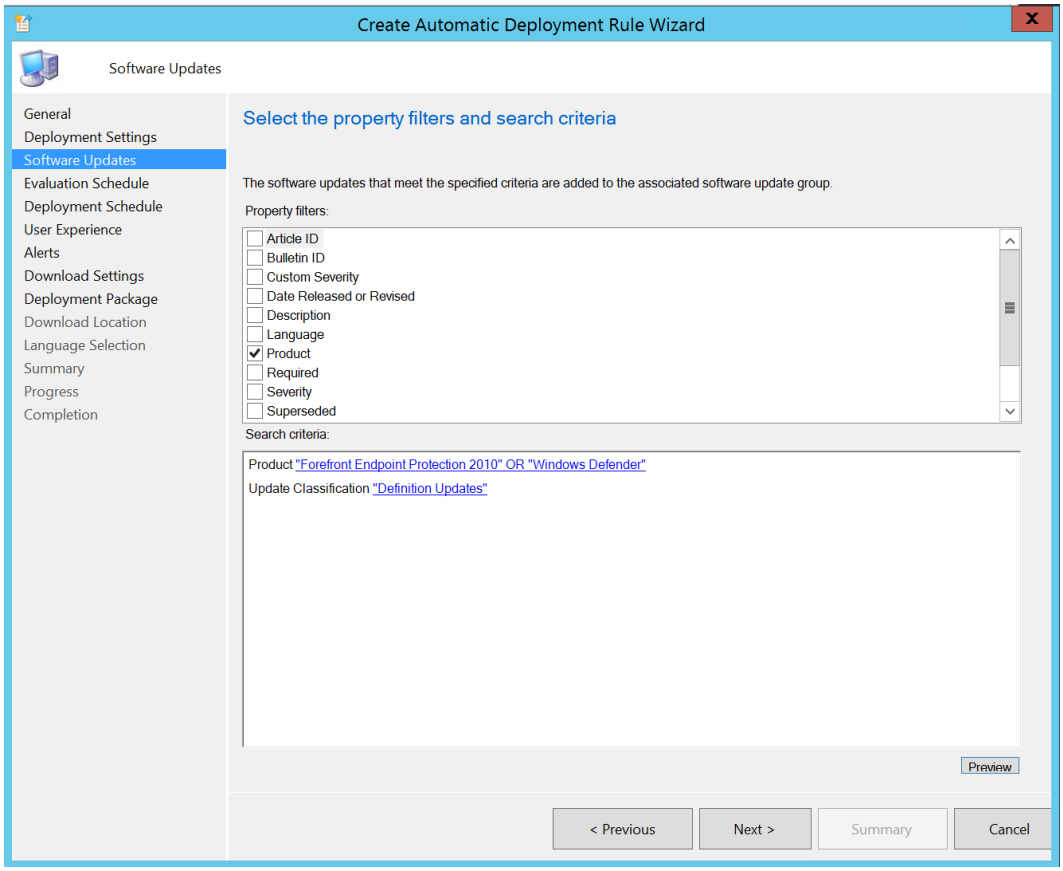

Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\wsyncmgr.log]
File Tools Window Help
Log Text
Component
sync: SMS synchronizing updates, processed 0 out of 13 items (0%) SMS_WSUS_SYNC_MANAGER
Synchronizing update 585052fc-f054-4672-9550-ce7feec255c1 - Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.227.376.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update a7543d8d-9421-4dd5-a62c-a2cbef912b9f - Definition Update for Windows Defender - KB2267602 (Definition 1.227.376.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 4f0400f4-2239-4529-9eea-89e1d43eb48c - Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.227.380.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 5e25056f-5cd2-48e1-a15c-1f36f998f064 - Definition Update for Windows Defender - KB2267602 (Definition 1.227.380.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update b1cff87c-d5c6-4e55-ae5d-ecc67efbec8c - Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.227.385.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 9b1302b4-beea-44c6-adb9-fe1cba2fa50e - Definition Update for Windows Defender - KB2267602 (Definition 1.227.385.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 8c490f18-d61c-4b4b-9592-49fc6354c95a - Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.227.394.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 9893870c-bdc8-4634-bac4-6fd28c77f8db - Definition Update for Windows Defender - KB2267602 (Definition 1.227.394.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 4de03e83-eee1-4382-b90a-19840e28741b - Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.227.404.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 3fe92e4f-31d4-4e97-ad11-00e26dc9aed5 - Definition Update for Windows Defender - KB2267602 (Definition 1.227.404.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 237699dc-0f23-4aa9-a0ea-4fef00da7027 - Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.227.408.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update e21e62d2-a741-484d-8456-bd546430bef7 - Definition Update for Windows Defender - KB2267602 (Definition 1.227.408.0) SMS_WSUS_SYNC_MANAGER
Synchronizing update 2503ff46-379c-465e-976e-5b9bab675ee5 - Definition Update for Windows Defender - KB915597 (Definition 1.227.408.0) SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing updates, processed 13 out of 13 items (100%) SMS_WSUS_SYNC_MANAGER
sync: SMS performing cleanup SMS_WSUS_SYNC_MANAGER
Removed 221 unreferenced updates SMS_WSUS_SYNC_MANAGER
Done synchronizing SMS with WSUS Server sccm2012r2.sccm.biz SMS_WSUS_SYNC_MANAGER
Set content version of update source {890AC58F-17B9-4A00-B11D-918C4D704E9D} for site NIC to 65 SMS_WSUS_SYNC_MANAGER
STATMSG: ID=6702 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=SCCM2012R2.sccm.biz SITE=NIC PID=2980 TID=5012 GMTDATE=tir aug 23 08:04:12.18... SMS_WSUS_SYNC_MANAGER
Sync succeeded. Setting sync alert to canceled state on site NIC SMS_WSUS_SYNC_MANAGER
Updated 442 items in SMS database, new update source content version is 65 SMS_WSUS_SYNC_MANAGER
Sync time: 0d00h05m09s SMS_WSUS_SYNC_MANAGER
Next scheduled sync is a regular sync at 23.08.2016 11:00:00 SMS_WSUS_SYNC_MANAGER
Wakeup by SCF change SMS_WSUS_SYNC_MANAGER
Wakeup by SCF change SMS_WSUS_SYNC_MANAGER
Next scheduled sync is a regular sync at 23.08.2016 12:00:00 SMS_WSUS_SYNC_MANAGER
Wakeup by SCF change SMS_WSUS_SYNC_MANAGER
Wakeup for a polling cycle SMS_WSUS_SYNC_MANAGER
Date/Time: 23.08.2016 12:10:45
Component: SMS_WSUS_SYNC_MANAGER
Thread: 5012 (0x1394)
Source:
Wakeup for a polling cycle

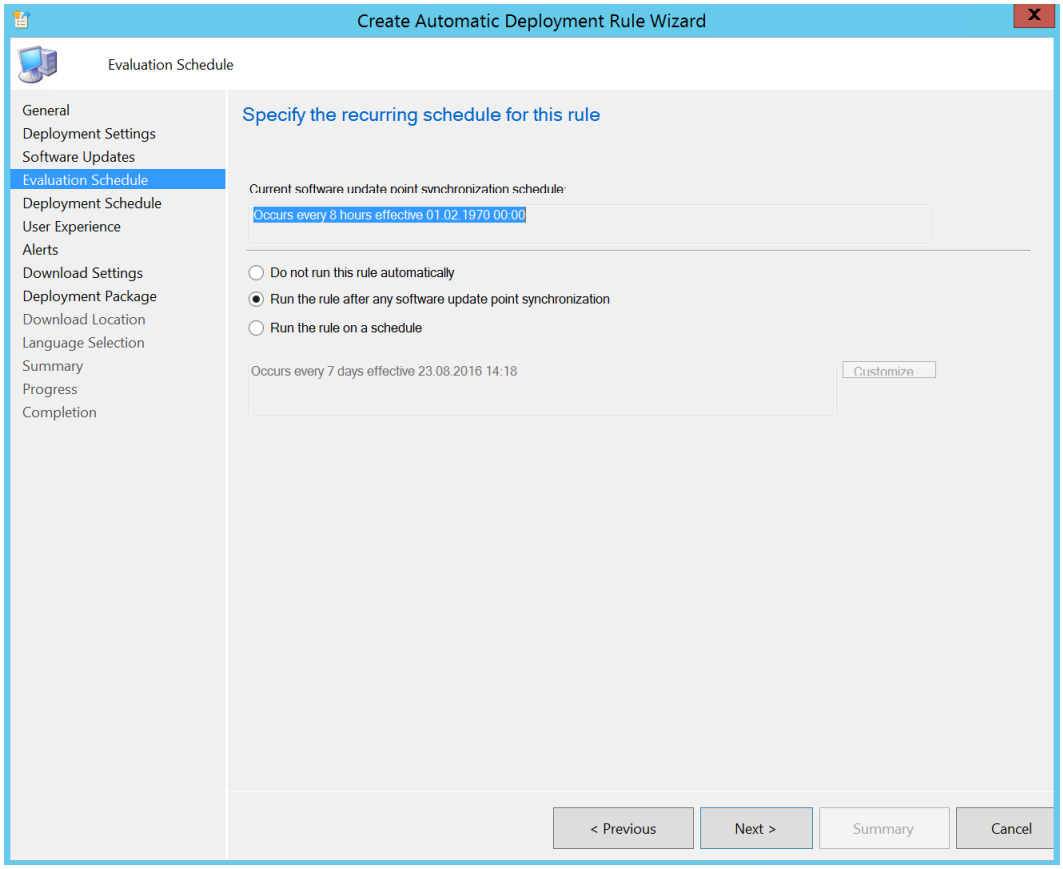

Home
Folder
Search
All Objects
Current Node
All Subfolders
Scope
Name
Add Criteria
Refine
Saved Searches
Recent Searches
Search Settings
Options
Save Current Search
Save Current Search As
Save
Close
Active Search
\ ▸ Software Library ▸ Overview ▸ Software Updates ▸ All Software Updates
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Assets and Compliance
Software Library
Monitoring
Administration
All Software Updates Search Results - 150 items shown
Search
Add Criteria
AND Product Forefront Endpoint Protection 2010
OR Product Windows Defender
Icon
Title
Required
Installed
Percent Compliant
Downloaded
Deployed
Definition Update for Windows Defender - KB2267602 (Definition 1.233.1768.0) 3 0 71 Yes Yes
Definition Update for Windows Defender - KB2267602 (Definition 1.233.1777.0) 3 0 71 Yes Yes
Definition Update for Windows Defender - KB2267602 (Definition 1.233.1783.0) 3 1 71 Yes Yes
Definition Update for Windows Defender - KB2267602 (Definition 1.233.1808.0) 0 0 54 Yes Yes
Definition Update for Windows Defender - KB915597 (Definition 1.233.1137.0) 0 0 86 Yes Yes
Definition Update for Windows Defender - KB915597 (Definition 1.233.1442.0) 0 0 85 Yes Yes
Definition Update for Windows Defender - KB915597 (Definition 1.233.1783.0) 0 1 73 Yes Yes
Definition Update for Windows Defender - KB915597 (Definition 1.233.1783.0)
Detail
Severity: None
Bulletin ID:
Article ID: 915597
Date Released: 09.12.2016 06:37
Date Released or Revised: 09.12.2016 06:37
Superseded: No
Expired: No
Update Classification: "Definition Updates"
Statistics
Compliant: 1
Required: 0
Not Required: 113
Unknown: 42
Total Asset Count: 156 (Last Update: 09.12.2016 14:52:54)
Summary
Deployment

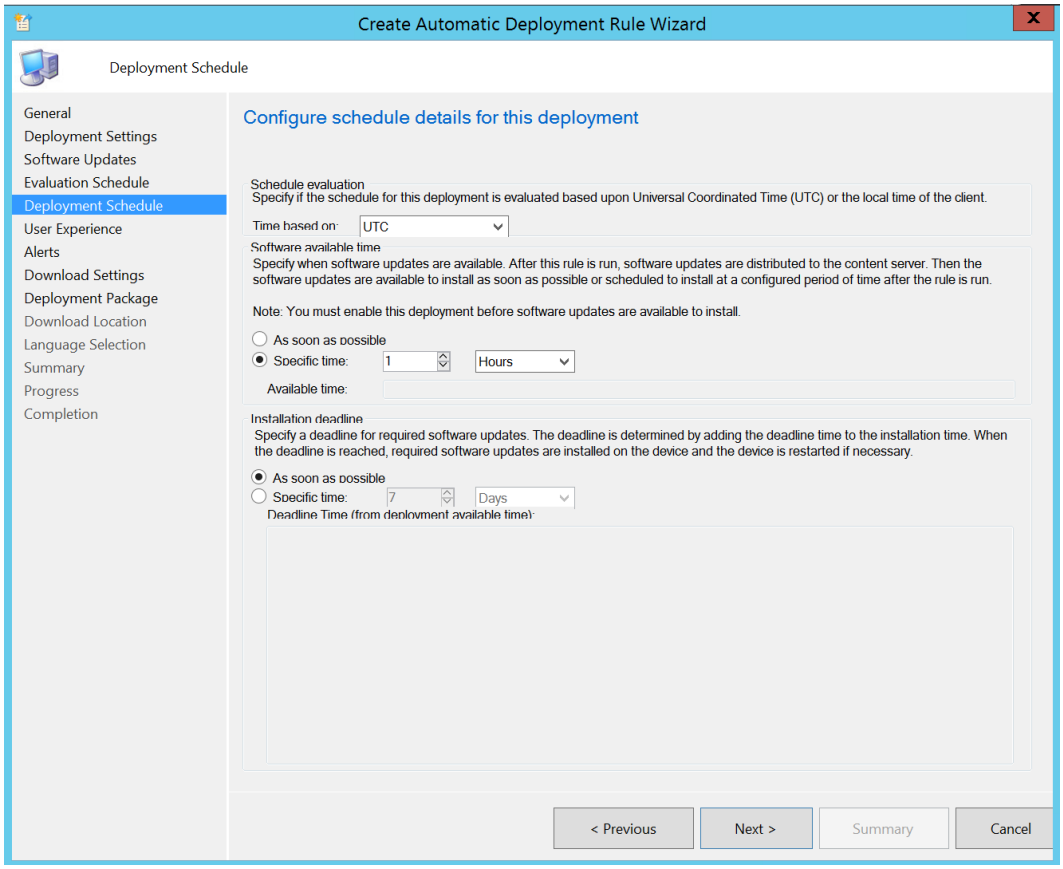

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Folder Tools
Search Tools
Home
Folder
Search
All Objects
Current Node
All Subfolders
Name
Add Criteria
Saved Searches
Recent Searches
Search Settings
Save Current Search
Save Current Search As
Close
Scope
Refine
Options
Save
Active Search
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
All Software Updates Search Results - 71 items shown
AND Product Forefront Endpoint Protection 2010
OR Product Windows Defender
Icon
Title
Bulletin ID
Required
Installed
Percent Compliant
Downloaded
Deployed
Date Released
Definition Update for Windows Defender - KB915597 (Definition 1.227.408.0)
Update for Forefront Endpoint Protection 2010 Client - 4.1.522.0 (KB2780435)
Update for Forefront Endpoint Protection 2010 Client - 4.3.215.0 (KB2864366)
Update for Forefront Endpoint Protection 2010 Client - 4.5.216.0 (KB2952678)
Update for Forefront Endpoint Protection 2010 Client - 4.7.209.0 (KB3041687)
Update for Forefront Endpoint Protection 2010 Client - 4.9.219.0 (KB3153224)
Update for System Center Endpoint Protection 2012 Client - 4.3.215.0 (KB2884678)
Update for System Center Endpoint Protection 2012 Client - 4.5.216.0 (KB2952678)
Update for System Center Endpoint Protection 2012 Client - 4.7.209.0 (KB3041687)
Update for System Center Endpoint Protection 2012 Client - 4.9.219.0 (KB3153224)
Update for System Center Endpoint Protection 2012 Client - 4.9.219.0 (KB3153224)
Detail
Severity: None
Bulletin ID:
Article ID: 3153224
Date Released: 13.04.2016 19:00
Date Released or Revised: 13.04.2016 19:00
Superseded: No
Expired: No
Update Classification: "Critical Updates"
NAP Evaluation: No
Statistics
Compliant: 0
Required: 1
Not Required: 6
Unknown: 0
Total Asset Count: 7 (Last Update: 22.08.2016 11:42:52)
Assets and Compliance
Software Library
Monitoring
Administration
Summary
Deployment
Ready

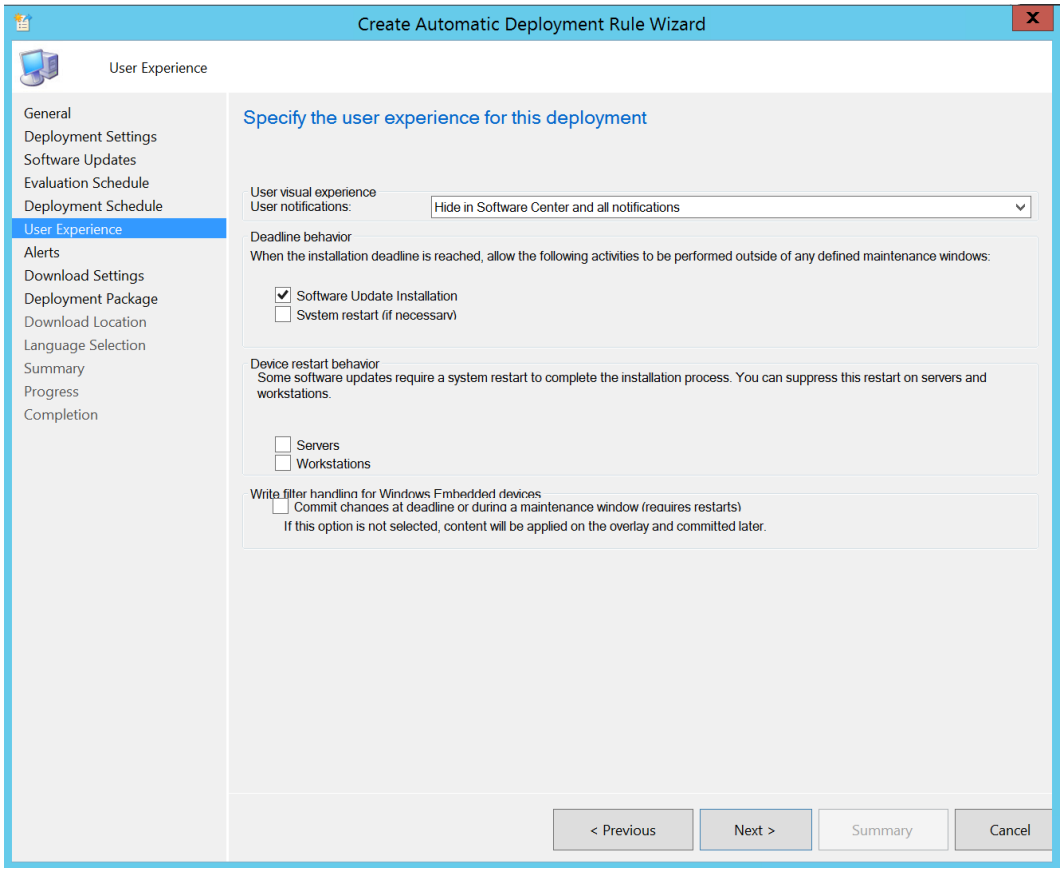

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Automatic Deployment Rule
Create
Saved Searches
Search
Software Library
Overview
Software Updates
Automatic Deployment Rules
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Create Automatic Deployment Rule
Windows 10 Servicing
Automatic Deployment Rules 2 items
Search
Icon
Name
Description
Enabled
Last Error Code
Last Error Description
Endpoint Protection Client Update
Yes
0X00000000
Success
Windows 10 Updates
Yes
0X00000000
Success

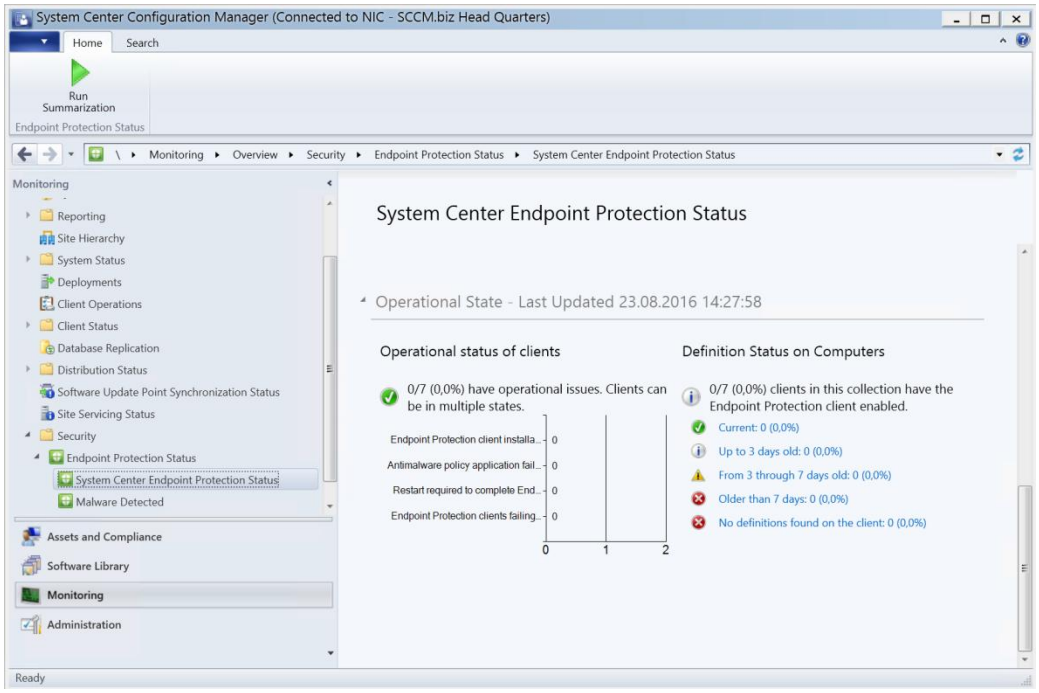

Create Automatic Deployment Rule Wizard
General
General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Download Location
Language Selection
Summary
Progress
Completion
Specify the settings for this automatic deployment rule
Name:
Endpoint Protection and Windows Defender definitions
Description:
Select a previously saved deployment template that defines configuration settings for this deployment. You can save the current configuration as a new deployment template on the Summary page of this wizard.
Template:
Patch Tuesday
CAMP Updates
Definition Updates
Manage Templates...
Specify the target collection
Collection:
Browse...
Each time the rule runs and finds new updates.
Add to an existing Software Update Group
Create a new Software Update Group
Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.
Enable the deployment after this rule is run
< Previous
Next >
Summary
Cancel

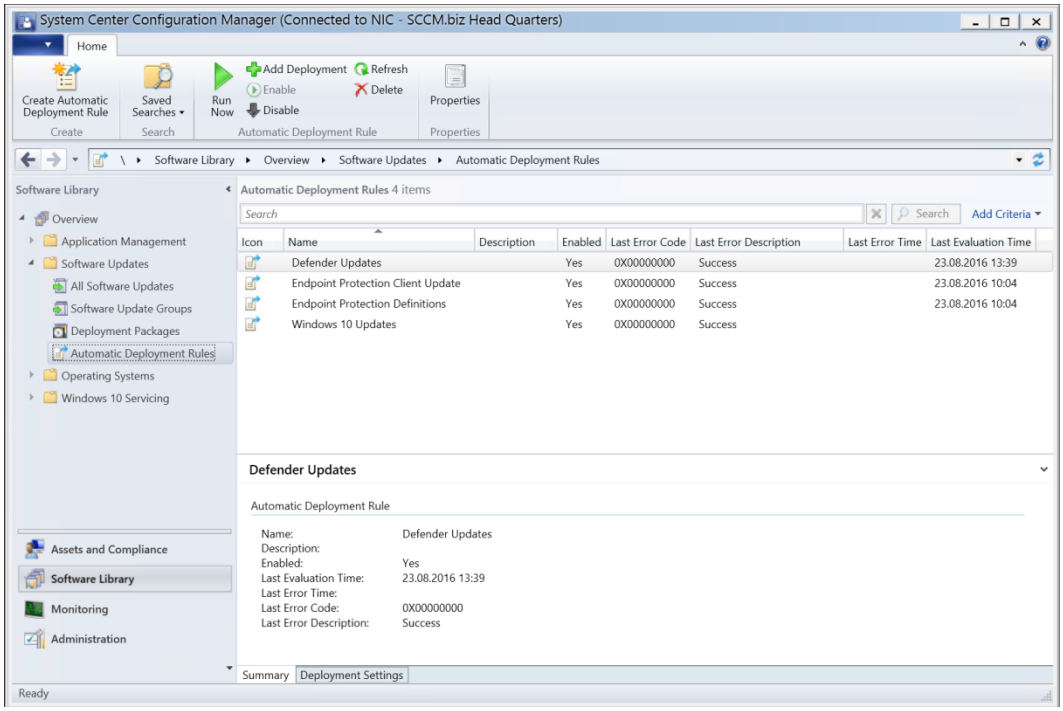

Create Automatic Deployment Rule Wizard
Software Updates
General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Download Location
Language Selection
Summary
Progress
Completion
Select the property filters and search criteria
The software updates that meet the specified criteria are added to the associated software update group.
Property filters:
Article ID
Bulletin ID
Custom Severity
Date Released or Revised
Description
Language
Product
Required
Severity
Superseded
Search criteria:
Product "Forefront Endpoint Protection 2010" OR "Windows Defender"
Update Classification "Definition Updates"
Preview
< Previous
Next >
Summary
Cancel

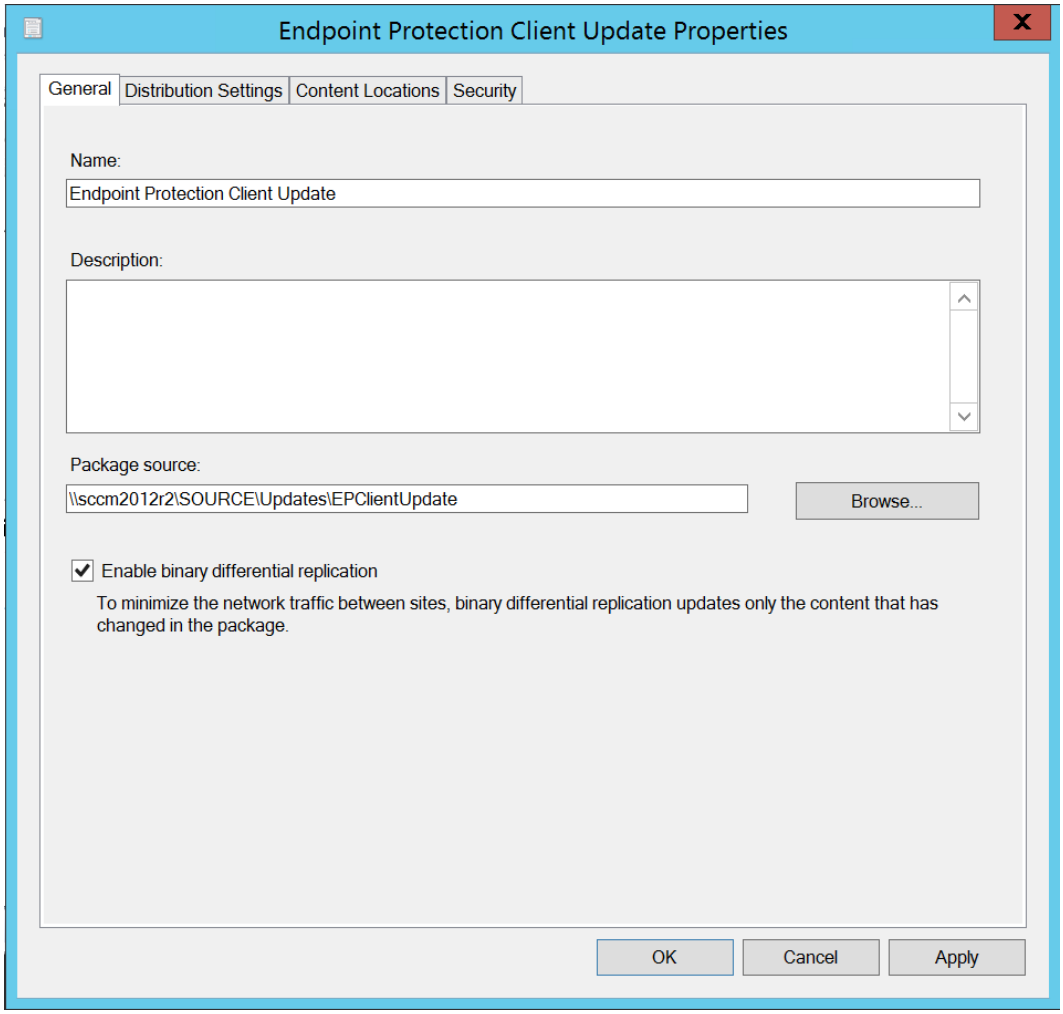

Create Automatic Deployment Rule Wizard
Evaluation Schedule
General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Download Location
Language Selection
Summary
Progress
Completion
Specify the recurring schedule for this rule
Current software update point synchronization schedule:
Occurs every 8 hours effective 01.02.1970 00:00
Do not run this rule automatically
Run the rule after any software update point synchronization
Run the rule on a schedule
Occurs every 7 days effective 23.08.2016 14:18
Customize...
< Previous
Next >
Summary
Cancel

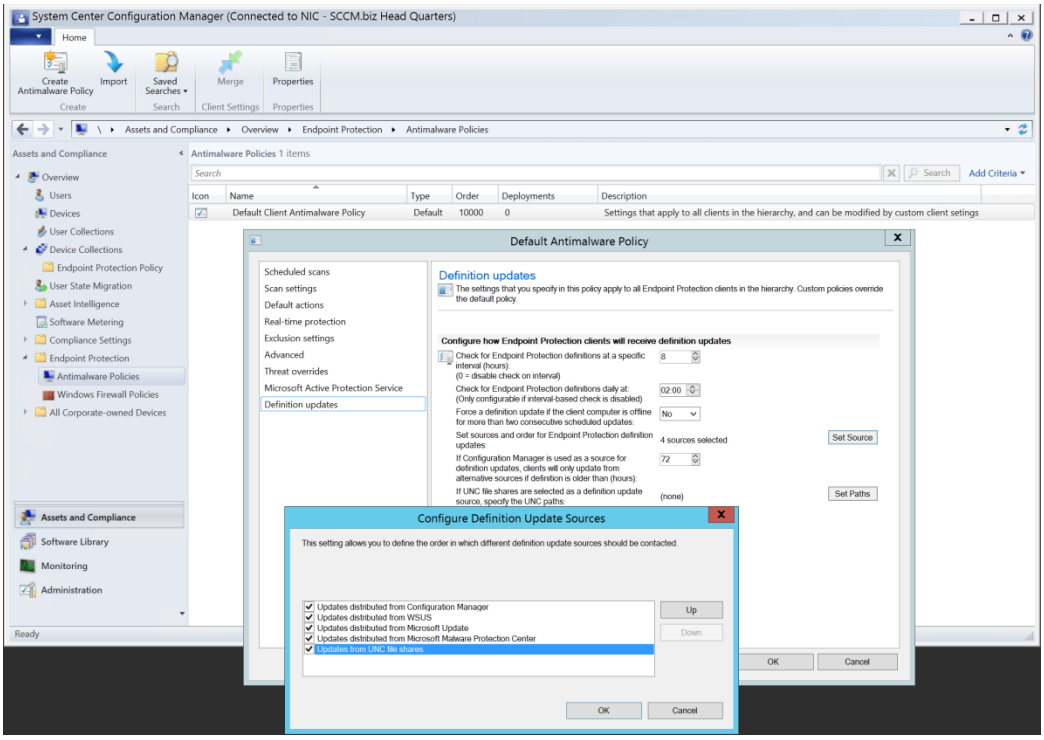

Create Automatic Deployment Rule Wizard
Deployment Schedule
General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Download Location
Language Selection
Summary
Progress
Completion
Configure schedule details for this deployment
Schedule evaluation
Specify if the schedule for this deployment is evaluated based upon Universal Coordinated Time (UTC) or the local time of the client.
Time based on:
UTC
Software available time
Specify when software updates are available. After this rule is run, software updates are distributed to the content server. Then the software updates are available to install as soon as possible or scheduled to install at a configured period of time after the rule is run.
Note: You must enable this deployment before software updates are available to install.
As soon as possible
Specific time:
1
Hours
Available time:
Installation deadline
Specify a deadline for required software updates. The deadline is determined by adding the deadline time to the installation time. When the deadline is reached, required software updates are installed on the device and the device is restarted if necessary.
As soon as possible
Specific time:
7
Days
Deadline Time (from deployment available time):
< Previous
Next >
Summary
Cancel

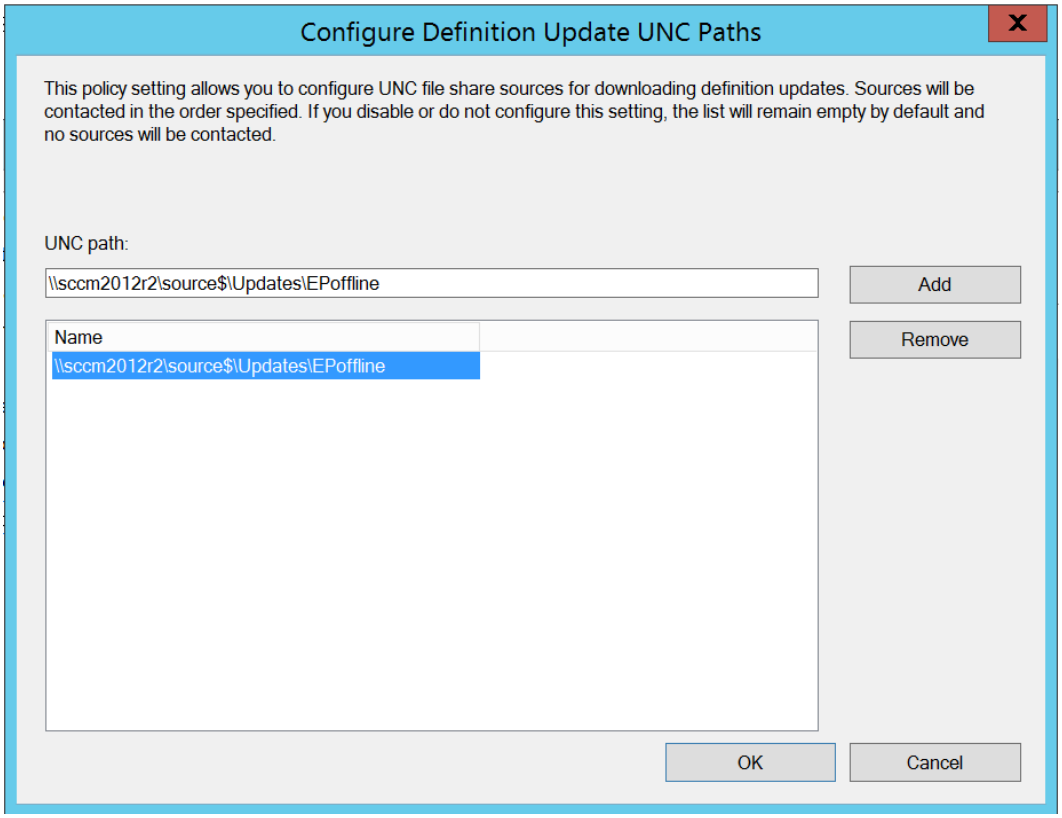

Create Automatic Deployment Rule Wizard
User Experience
General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Download Location
Language Selection
Summary
Progress
Completion
Specify the user experience for this deployment
User visual experience
User notifications:
Hide in Software Center and all notifications
Deadline behavior
When the installation deadline is reached, allow the following activities to be performed outside of any defined maintenance windows:
Software Update Installation
System restart (if necessary)
Device restart behavior
Some software updates require a system restart to complete the installation process. You can suppress this restart on servers and workstations.
Servers
Workstations
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel

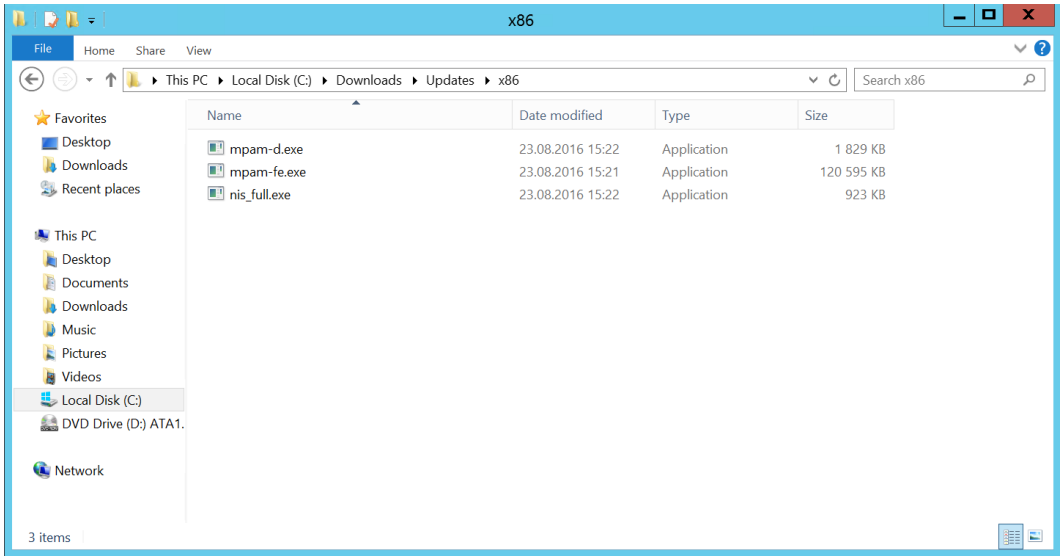

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Search
Run Summarization
Endpoint Protection Status
\ ▸ Monitoring ▸ Overview ▸ Security ▸ Endpoint Protection Status ▸ System Center Endpoint Protection Status
Monitoring
Reporting
Site Hierarchy
System Status
Deployments
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchronization Status
Site Servicing Status
Security
Endpoint Protection Status
System Center Endpoint Protection Status
Malware Detected
Assets and Compliance
Software Library
Monitoring
Administration
System Center Endpoint Protection Status
Operational State - Last Updated 23.08.2016 14:27:58
Operational status of clients
0/7 (0,0%) have operational issues. Clients can be in multiple states.
Endpoint Protection client installa... 0
Antimalware policy application fail... 0
Restart required to complete End... 0
Endpoint Protection clients failing... 0
0
1
2
Definition Status on Computers
0/7 (0,0%) clients in this collection have the Endpoint Protection client enabled.
Current: 0 (0,0%)
Up to 3 days old: 0 (0,0%)
From 3 through 7 days old: 0 (0,0%)
Older than 7 days: 0 (0,0%)
No definitions found on the client: 0 (0,0%)
Ready

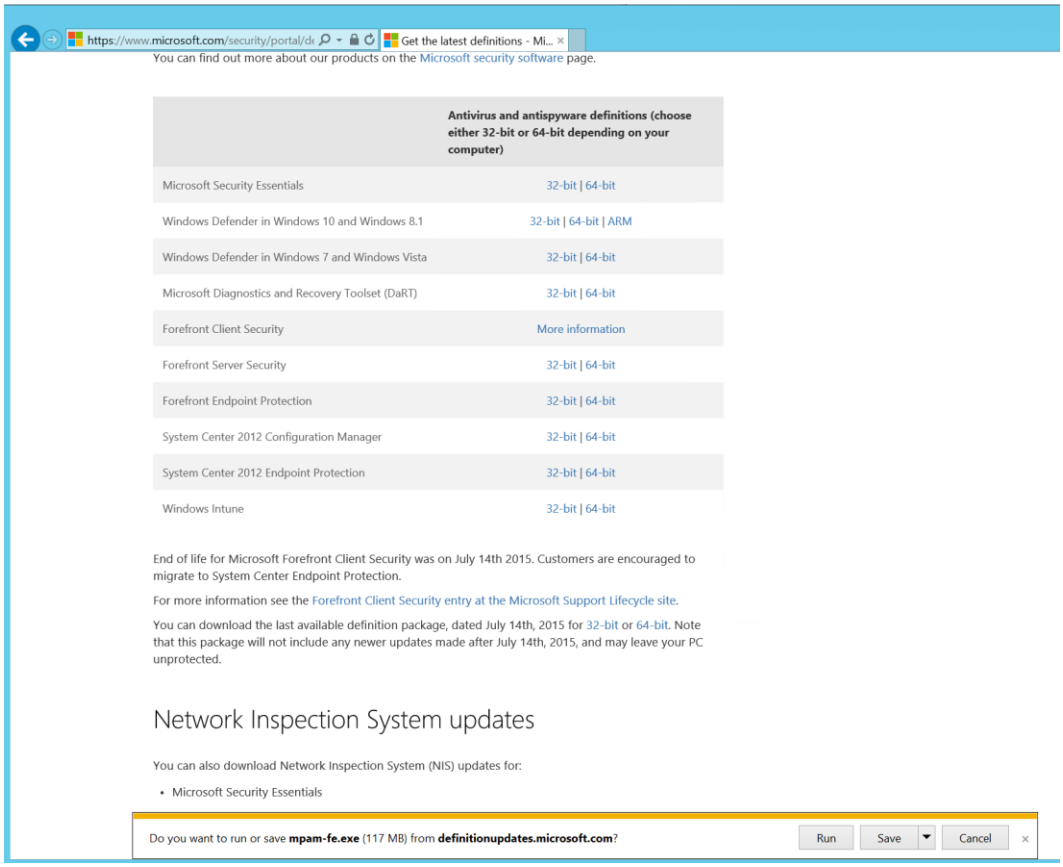

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Automatic Deployment Rule
Saved Searches
Run Now
Add Deployment
Enable
Disable
Refresh
Delete
Properties
Create
Search
Automatic Deployment Rule
Properties
\ ▸ Software Library ▸ Overview ▸ Software Updates ▸ Automatic Deployment Rules
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Assets and Compliance
Software Library
Monitoring
Administration
Automatic Deployment Rules 4 items
Search
Add Criteria
Icon
Name
Description
Enabled
Last Error Code
Last Error Description
Last Error Time
Last Evaluation Time
Defender Updates
Yes
0X00000000
Success
23.08.2016 13:39
Endpoint Protection Client Update
Yes
0X00000000
Success
23.08.2016 10:04
Endpoint Protection Definitions
Yes
0X00000000
Success
23.08.2016 10:04
Windows 10 Updates
Yes
0X00000000
Success
Defender Updates
Automatic Deployment Rule
Name: Defender Updates
Description:
Enabled: Yes
Last Evaluation Time: 23.08.2016 13:39
Last Error Time:
Last Error Code: 0X00000000
Last Error Description: Success
Summary
Deployment Settings
Ready


Endpoint Protection Client Update Properties
General
Distribution Settings
Content Locations
Security
Name:
Endpoint Protection Client Update
Description:
Package source:
\\sccm2012r2\SOURCE\Updates\EPClientUpdate
Browse...
Enable binary differential replication
To minimize the network traffic between sites, binary differential replication updates only the content that has changed in the package.
OK
Cancel
Apply

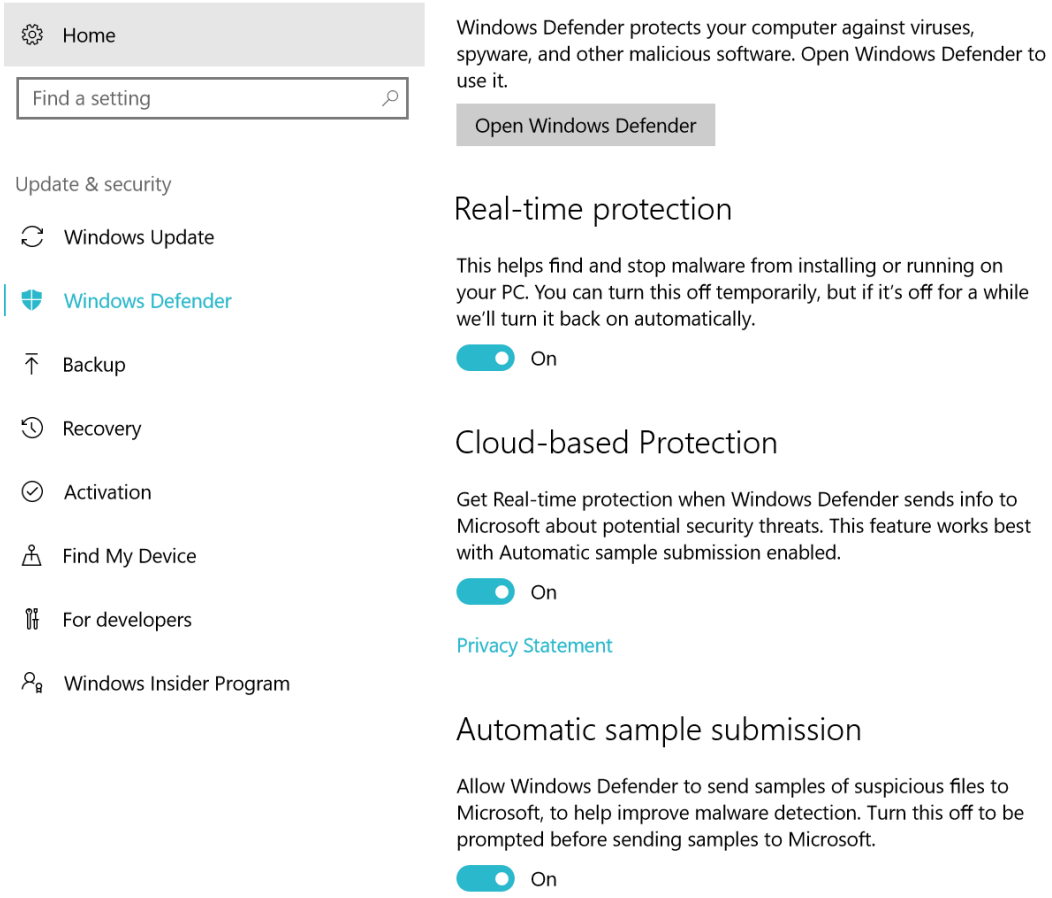

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Antimalware Policy
Import
Saved Searches
Merge
Properties
Create
Search
Client Settings
Properties
Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Endpoint Protection Policy
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Antimalware Policies 1 items
Search
Add Criteria
Icon
Name
Type
Order
Deployments
Description
Default Client Antimalware Policy
Default
10000
0
Settings that apply to all clients in the hierarchy, and can be modified by custom client setings
Default Antimalware Policy
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Microsoft Active Protection Service
Definition updates
Definition updates
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Configure how Endpoint Protection clients will receive definition updates
Check for Endpoint Protection definitions at a specific interval (hours):
(0 = disable check on interval)
8
Check for Endpoint Protection definitions daily at:
(Only configurable if interval-based check is disabled)
02:00
Force a definition update if the client computer is offline for more than two consecutive scheduled updates:
No
Set sources and order for Endpoint Protection definition updates:
4 sources selected
Set Source
If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours):
72
If UNC file shares are selected as a definition update source, specify the UNC paths:
(none)
Set Paths
OK
Cancel
Configure Definition Update Sources
This setting allows you to define the order in which different definition update sources should be contacted.
Updates distributed from Configuration Manager
Updates distributed from WSUS
Updates distributed from Microsoft Update
Updates distributed from Microsoft Malware Protection Center
Updates from UNC file shares
Up
Down
OK
Cancel

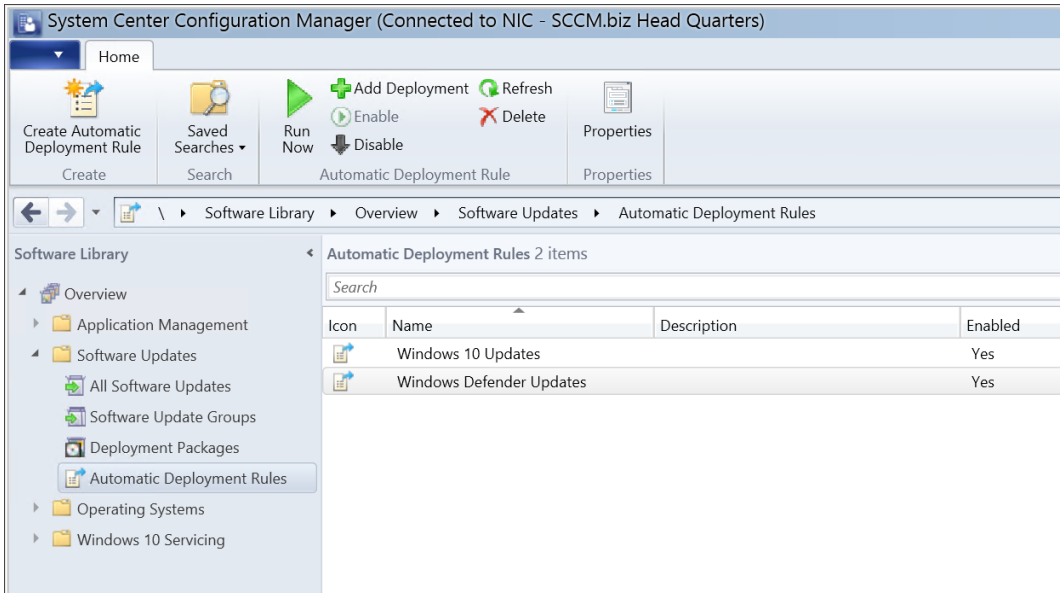

Configure Definition Update UNC Paths
This policy setting allows you to configure UNC file share sources for downloading definition updates. Sources will be contacted in the order specified. If you disable or do not configure this setting, the list will remain empty by default and no sources will be contacted.
UNC path:
\\sccm2012r2\source$\Updates\EPoffline
Add
Name
\\sccm2012r2\source$\Updates\EPoffline
Remove
OK
Cancel

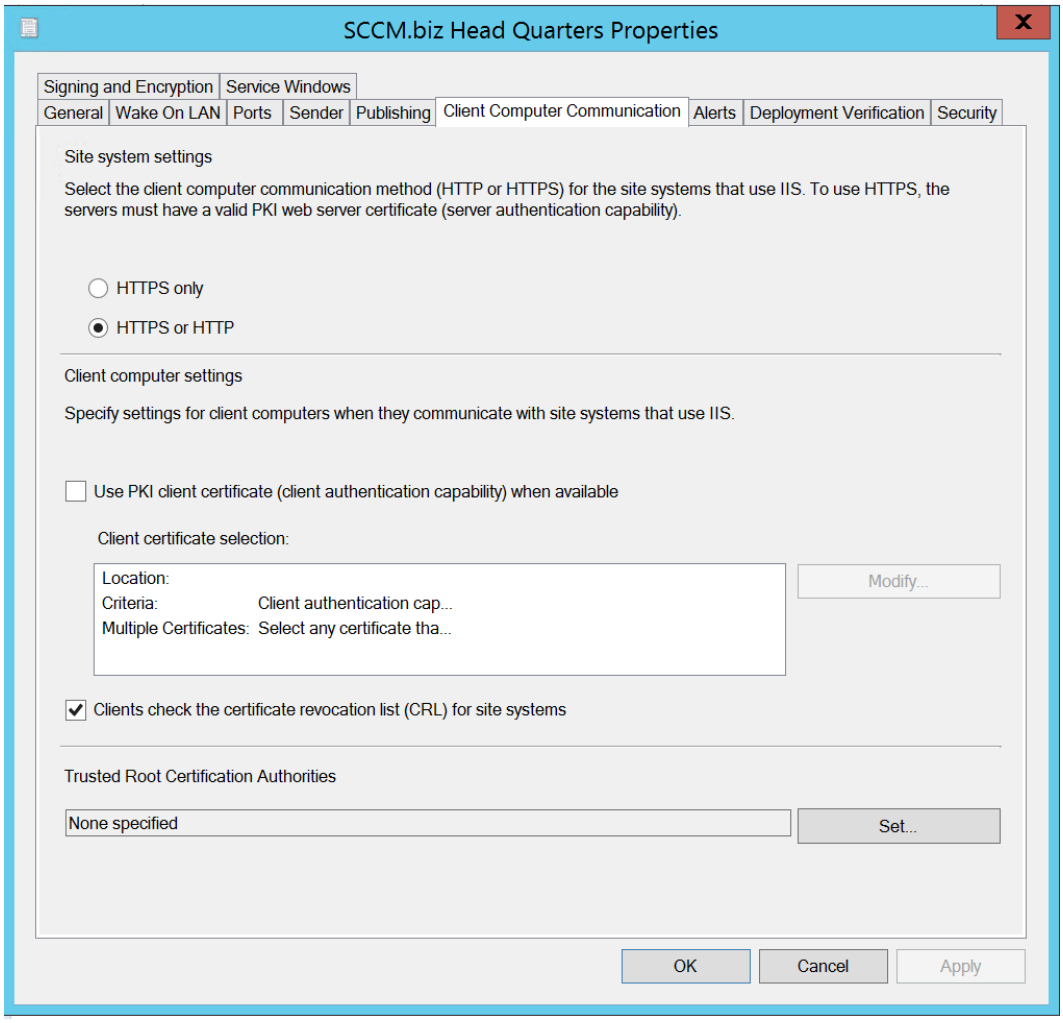

x86
File
Home
Share
View
This PC ▸ Local Disk (C:) ▸ Downloads ▸ Updates ▸ x86
Search x86
Favorites
Desktop
Downloads
Recent places
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) ATA1.
Network
Name
Date modified
Type
Size
mpam-d.exe
23.08.2016 15:22
Application
1 829 KB
mpam-fe.exe
23.08.2016 15:21
Application
120 595 KB
nis_full.exe
23.08.2016 15:22
Application
923 KB
3 items

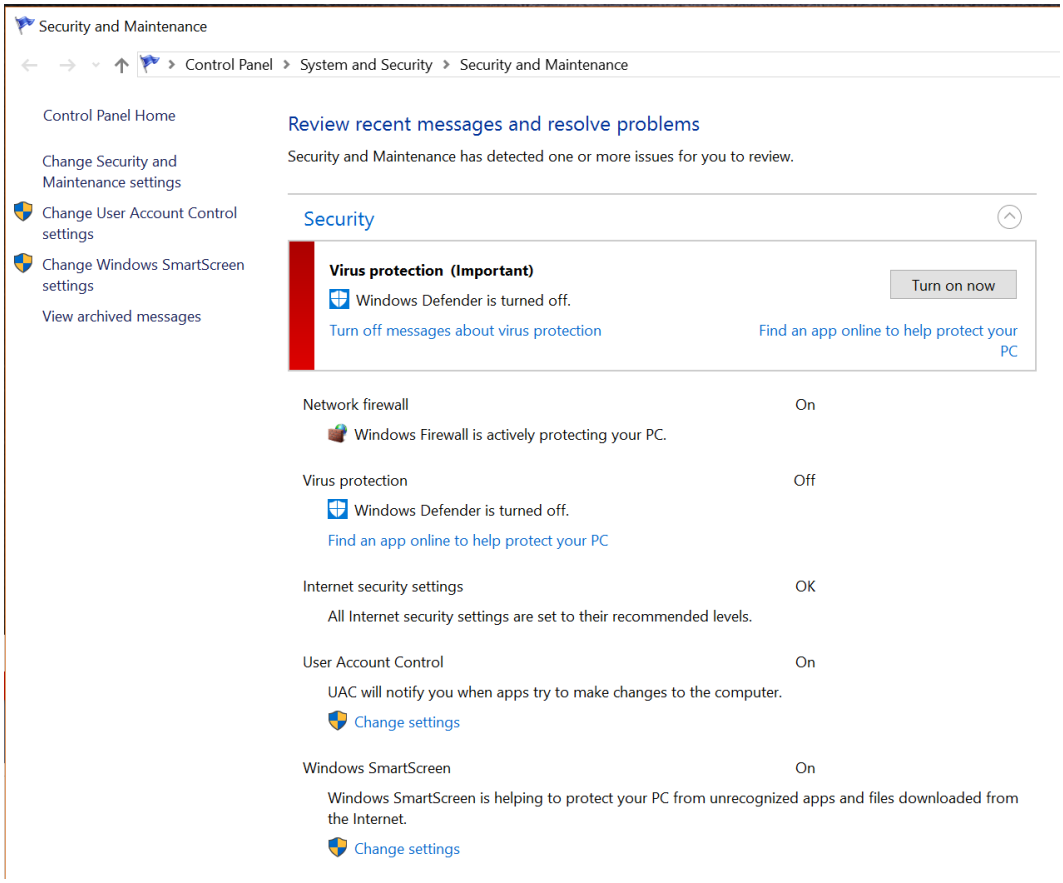

https://www.microsoft.com/security/portal/d
Get the latest definitions - Mi...
You can find out more about our products on the Microsoft security software page.
Antivirus and antispyware definitions (choose either 32-bit or 64-bit depending on your computer)
Microsoft Security Essentials
32-bit | 64-bit
Windows Defender in Windows 10 and Windows 8.1
32-bit | 64-bit | ARM
Windows Defender in Windows 7 and Windows Vista
32-bit | 64-bit
Microsoft Diagnostics and Recovery Toolset (DaRT)
32-bit | 64-bit
Forefront Client Security
More information
Forefront Server Security
32-bit | 64-bit
Forefront Endpoint Protection
32-bit | 64-bit
System Center 2012 Configuration Manager
32-bit | 64-bit
System Center 2012 Endpoint Protection
32-bit | 64-bit
Windows Intune
32-bit | 64-bit
End of life for Microsoft Forefront Client Security was on July 14th 2015. Customers are encouraged to migrate to System Center Endpoint Protection.
For more information see the Forefront Client Security entry at the Microsoft Support Lifecycle site.
You can download the last available definition package, dated July 14th, 2015 for 32-bit or 64-bit. Note that this package will not include any newer updates made after July 14th, 2015, and may leave your PC unprotected.
Network Inspection System updates
You can also download Network Inspection System (NIS) updates for:
• Microsoft Security Essentials
Do you want to run or save mpam-fe.exe (117 MB) from definitionupdates.microsoft.com?
Run
Save
Cancel

# Chapter 5: Security and Privacy for Endpoint Protection in Configuration Manager

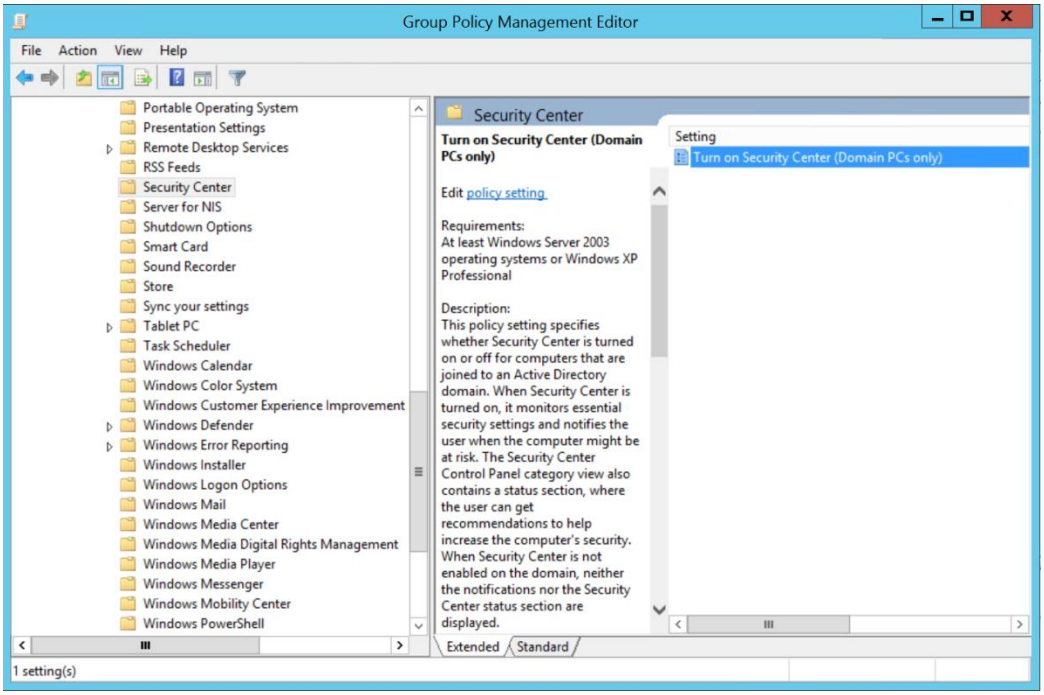


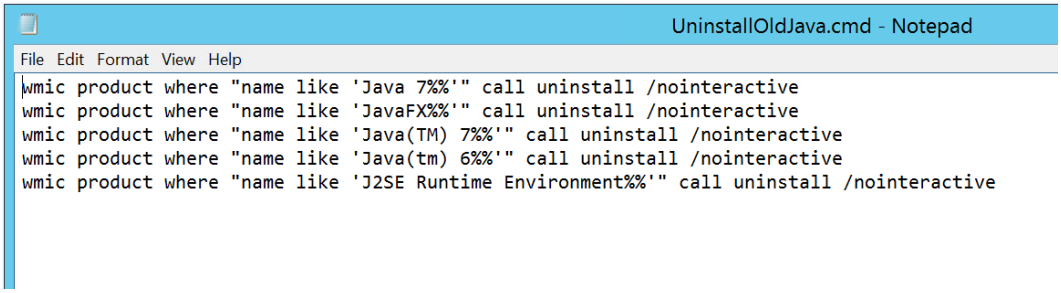

System Center Configuration Manager (Connected to NIC - SCCM.biz Head Quarters)
Home
Create Automatic Deployment Rule
Saved Searches
Run Now
Add Deployment
Enable
Disable
Refresh
Delete
Properties
Create
Search
Automatic Deployment Rule
Properties
\ ▸ Software Library ▸ Overview ▸ Software Updates ▸ Automatic Deployment Rules
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Automatic Deployment Rules 2 items
Search
Icon
Name
Description
Enabled
Windows 10 Updates
Yes
Windows Defender Updates
Yes

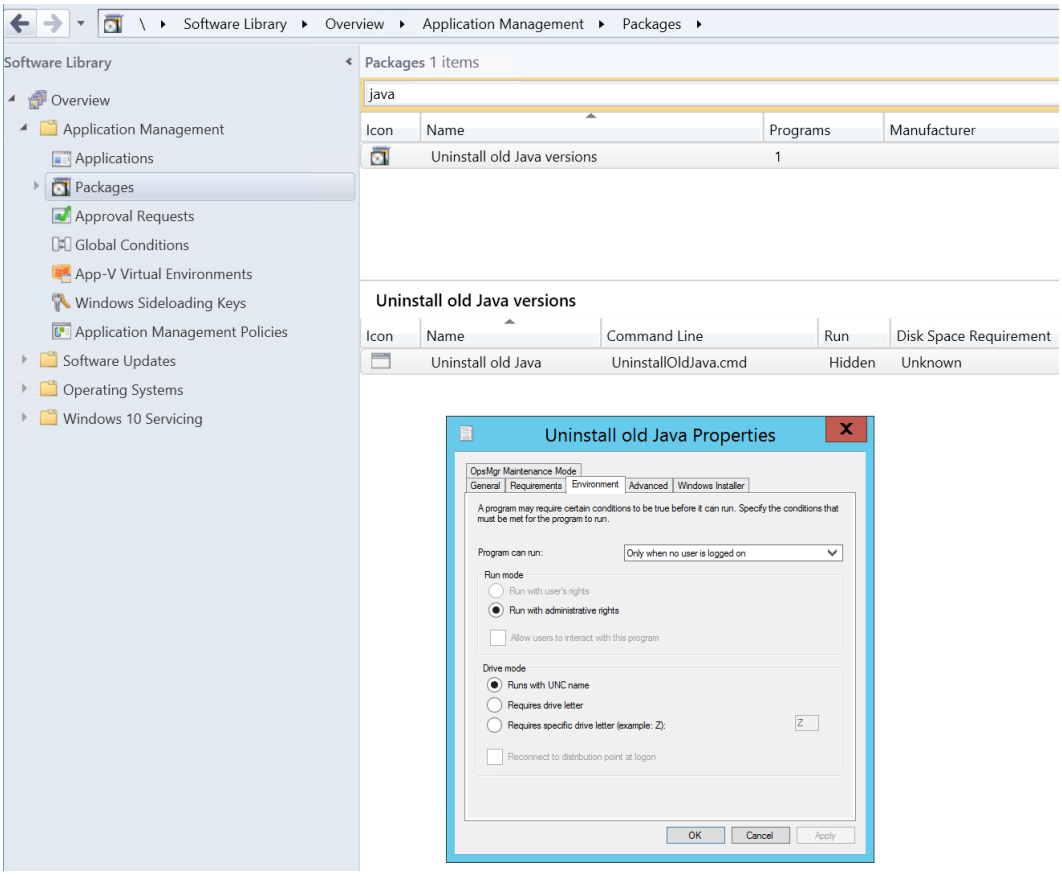

SCCM.biz Head Quarters Properties
Signing and Encryption
Service Windows
General
Wake On LAN
Ports
Sender
Publishing
Client Computer Communication
Alerts
Deployment Verification
Security
Site system settings
Select the client computer communication method (HTTP or HTTPS) for the site systems that use IIS. To use HTTPS, the servers must have a valid PKI web server certificate (server authentication capability).
HTTPS only
HTTPS or HTTP
Client computer settings
Specify settings for client computers when they communicate with site systems that use IIS.
Use PKI client certificate (client authentication capability) when available
Client certificate selection:
Location:
Criteria: Client authentication cap...
Multiple Certificates: Select any certificate tha...
Modify...
Clients check the certificate revocation list (CRL) for site systems
Trusted Root Certification Authorities
None specified
Set...
OK
Cancel
Apply

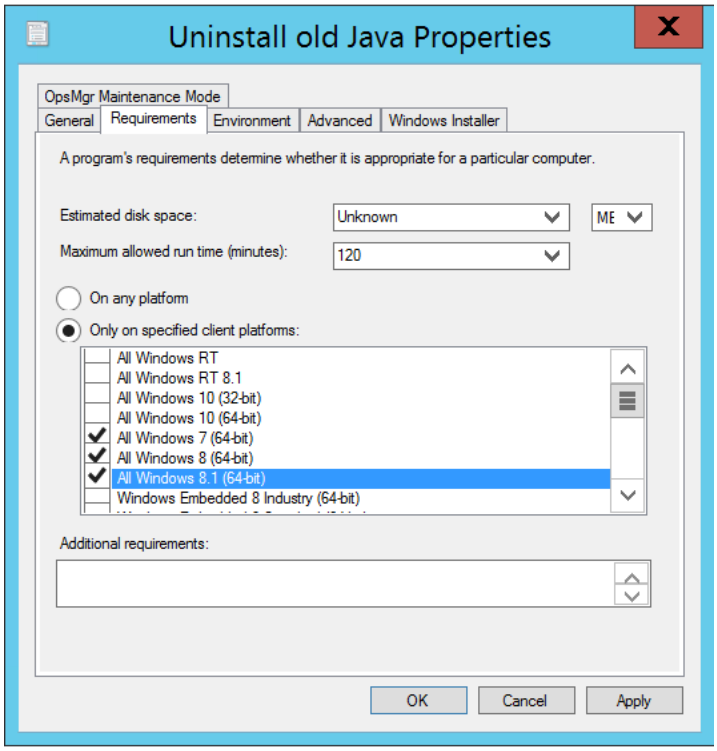

Security and Maintenance
Control Panel › System and Security › Security and Maintenance
Control Panel Home
Change Security and Maintenance settings
Change User Account Control settings
Change Windows SmartScreen settings
View archived messages
Review recent messages and resolve problems
Security and Maintenance has detected one or more issues for you to review.
Security
Virus protection (Important)
Windows Defender is turned off.
Turn off messages about virus protection
Turn on now
Find an app online to help protect your PC
Network firewall
On
Windows Firewall is actively protecting your PC.
Virus protection
Off
Windows Defender is turned off.
Find an app online to help protect your PC
Internet security settings
OK
All Internet security settings are set to their recommended levels.
User Account Control
On
UAC will notify you when apps try to make changes to the computer.
Change settings
Windows SmartScreen
On
Windows SmartScreen is helping to protect your PC from unrecognized apps and files downloaded from the Internet.
Change settings

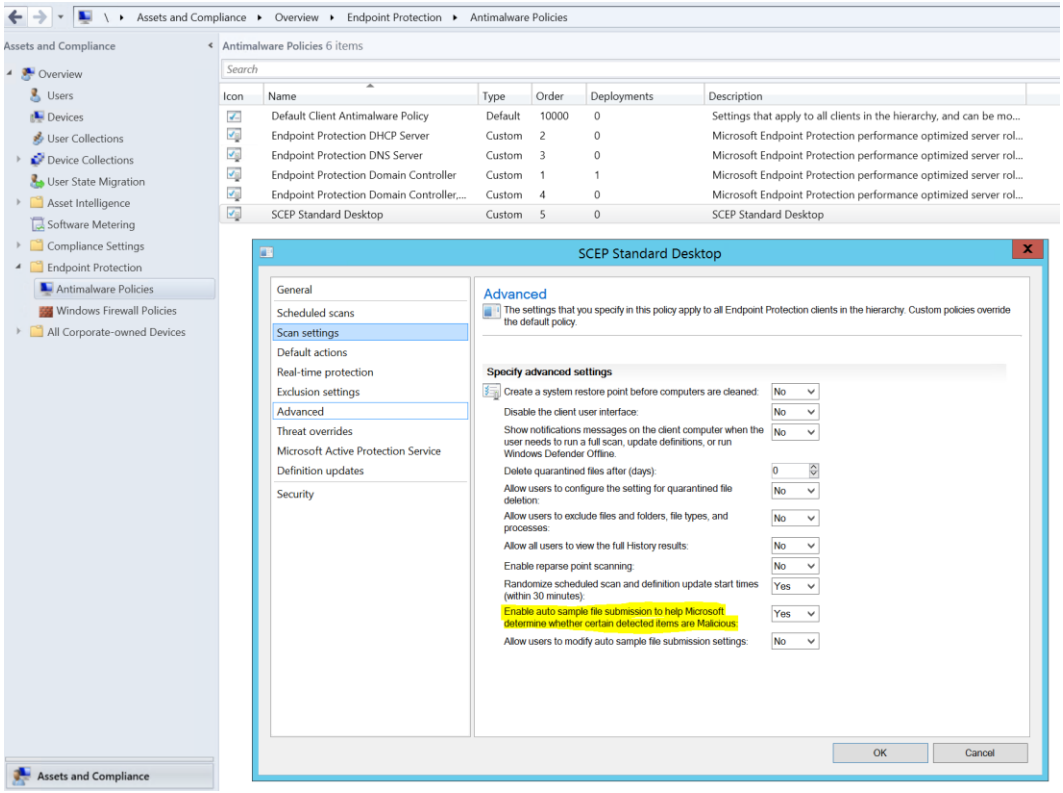

Turn on virus protection
Virus protection is turned off. Tap or click to turn on Windows Defender.
Security and Maintenance
Evaluation copy. Build 14951.rs_prerelease.161014-1700
NICWIN1...
Security and Mainte...
Windows Defender
Settings
NOB
13.10
24.10.2016

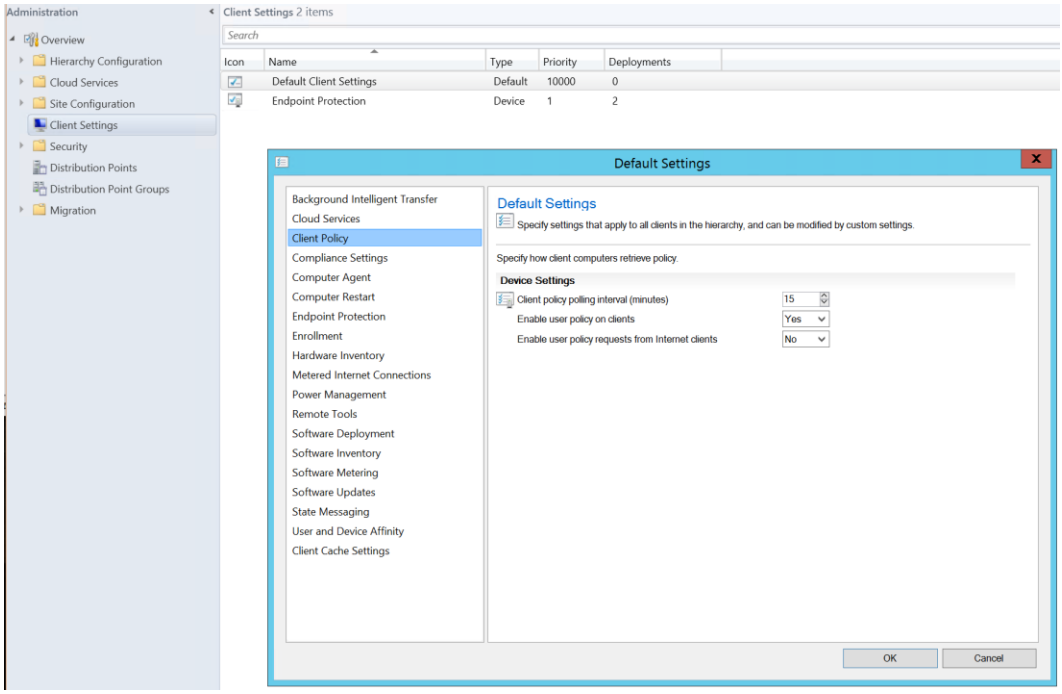

Group Policy Management Editor
File Action View Help
Portable Operating System
Presentation Settings
Remote Desktop Services
RSS Feeds
Security Center
Server for NIS
Shutdown Options
Smart Card
Sound Recorder
Store
Sync your settings
Tablet PC
Task Scheduler
Windows Calendar
Windows Color System
Windows Customer Experience Improvement
Windows Defender
Windows Error Reporting
Windows Installer
Windows Logon Options
Windows Mail
Windows Media Center
Windows Media Digital Rights Management
Windows Media Player
Windows Messenger
Windows Mobility Center
Windows PowerShell
Security Center
Turn on Security Center (Domain PCs only)
Edit policy setting
Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional
Description:
This policy setting specifies whether Security Center is turned on or off for computers that are joined to an Active Directory domain. When Security Center is turned on, it monitors essential security settings and notifies the user when the computer might be at risk. The Security Center Control Panel category view also contains a status section, where the user can get recommendations to help increase the computer's security. When Security Center is not enabled on the domain, neither the notifications nor the Security Center status section are displayed.
Setting
Turn on Security Center (Domain PCs only)
Extended
Standard
1 setting(s)

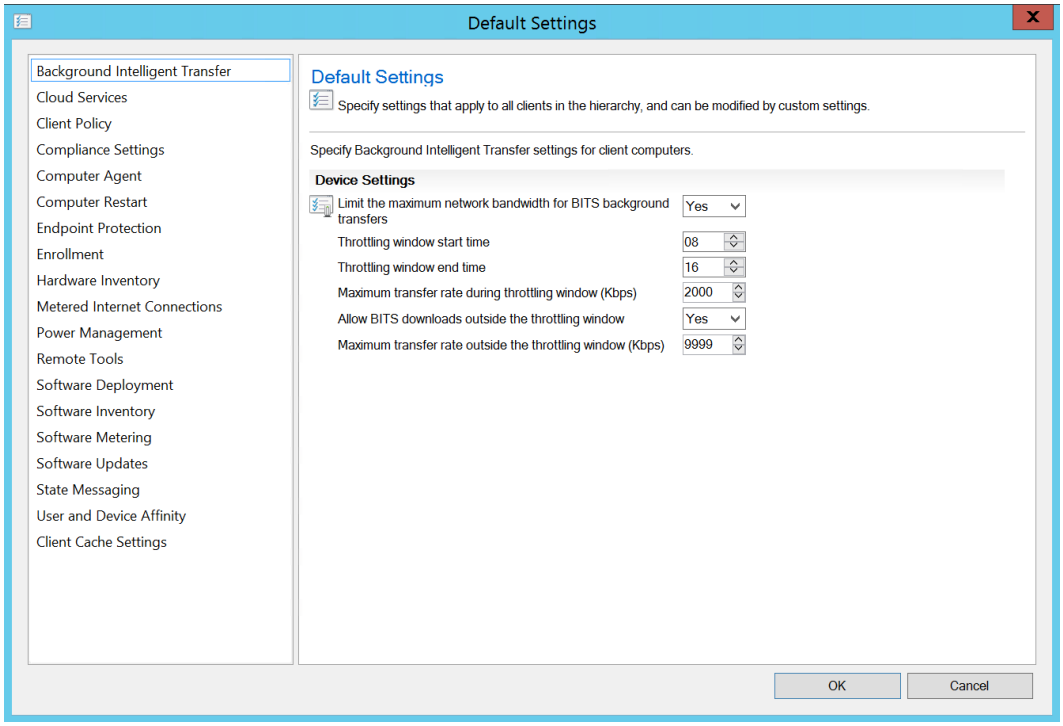

UninstallOldJava.cmd - Notepad
File Edit Format View Help
wmic product where "name like 'Java 7%%'" call uninstall /nointeractive
wmic product where "name like 'JavaFX%%'" call uninstall /nointeractive
wmic product where "name like 'Java(TM) 7%%'" call uninstall /nointeractive
wmic product where "name like 'Java(tm) 6%%'" call uninstall /nointeractive
wmic product where "name like 'J2SE Runtime Environment%%'" call uninstall /nointeractive

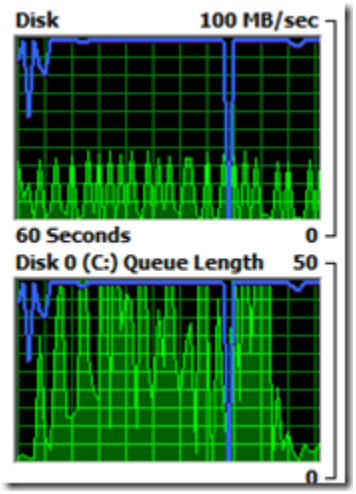

Software Library
Overview
Application Management
Packages
Packages 1 items
java
Icon
Name
Programs
Manufacturer
Uninstall old Java versions
1
Applications
Packages
Approval Requests
Global Conditions
App-V Virtual Environments
Windows Sideloading Keys
Application Management Policies
Software Updates
Operating Systems
Windows 10 Servicing
Uninstall old Java versions
Icon
Name
Command Line
Run
Disk Space Requirement
Uninstall old Java
UninstallOldJava.cmd
Hidden
Unknown
Uninstall old Java Properties
OpsMgr Maintenance Mode
General
Requirements
Environment
Advanced
Windows Installer
A program may require certain conditions to be true before it can run. Specify the conditions that must be met for the program to run.
Program can run:
Only when no user is logged on
Run mode
Run with user's rights
Run with administrative rights
Allow users to interact with this program
Drive mode
Runs with UNC name
Requires drive letter
Requires specific drive letter (example: Z):
Z
Reconnect to distribution point at logon
OK
Cancel
Apply


Uninstall old Java Properties
OpsMgr Maintenance Mode
General
Requirements
Environment
Advanced
Windows Installer
A program's requirements determine whether it is appropriate for a particular computer.
Estimated disk space:
Unknown
MB
Maximum allowed run time (minutes):
120
On any platform
Only on specified client platforms:
All Windows RT
All Windows RT 8.1
All Windows 10 (32-bit)
All Windows 10 (64-bit)
All Windows 7 (64-bit)
All Windows 8 (64-bit)
All Windows 8.1 (64-bit)
Windows Embedded 8 Industry (64-bit)
Additional requirements:
OK
Cancel
Apply

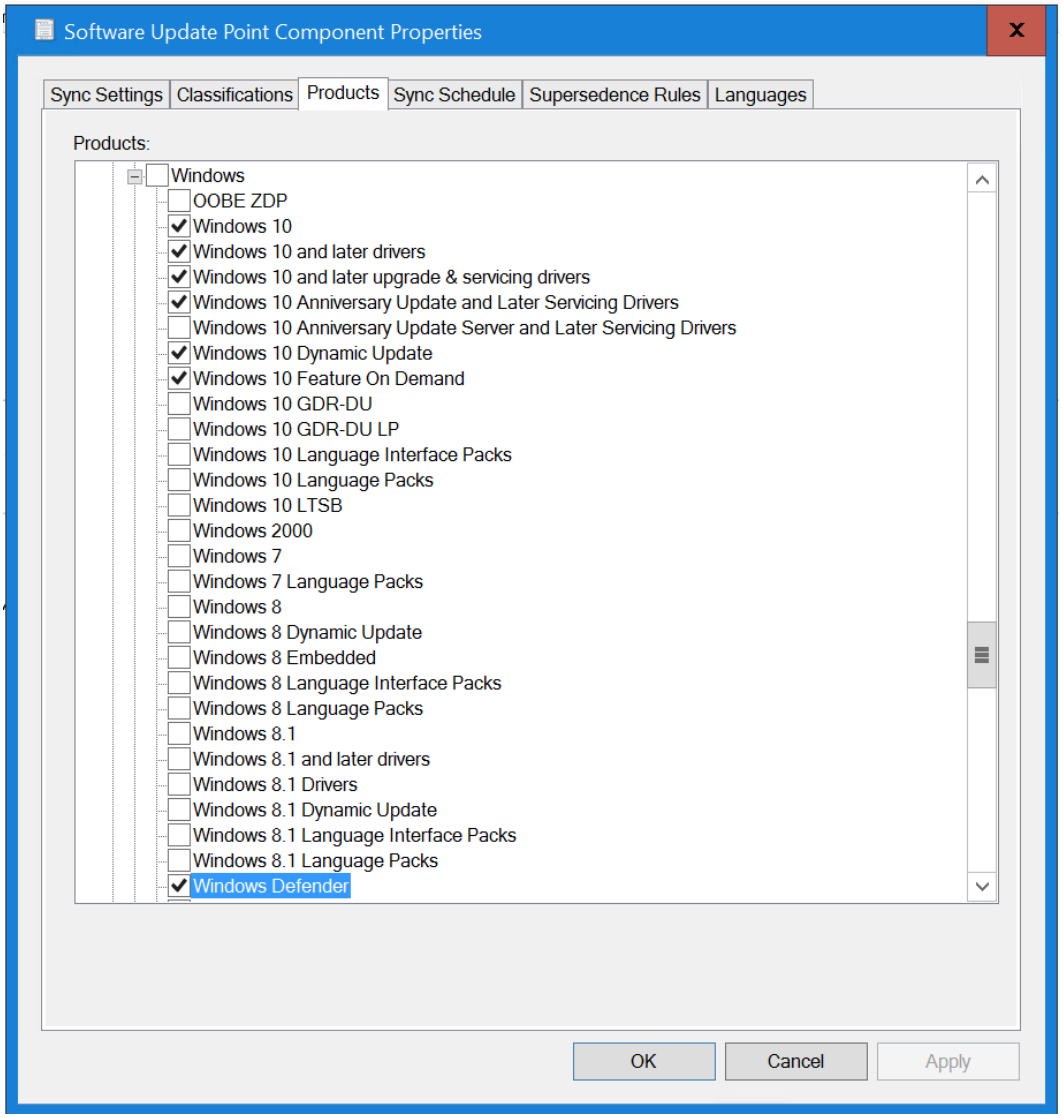

Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Firewall Policies
All Corporate-owned Devices
Assets and Compliance
Antimalware Policies 6 items
Search
Icon
Name
Type
Order
Deployments
Description
Default Client Antimalware Policy
Default
10000
0
Settings that apply to all clients in the hierarchy, and can be mo...
Endpoint Protection DHCP Server
Custom
2
0
Microsoft Endpoint Protection performance optimized server rol...
Endpoint Protection DNS Server
Custom
3
0
Microsoft Endpoint Protection performance optimized server rol...
Endpoint Protection Domain Controller
Custom
1
1
Microsoft Endpoint Protection performance optimized server rol...
Endpoint Protection Domain Controller,...
Custom
4
0
Microsoft Endpoint Protection performance optimized server rol...
SCEP Standard Desktop
Custom
5
0
SCEP Standard Desktop
SCEP Standard Desktop
General
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Microsoft Active Protection Service
Definition updates
Security
Advanced
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify advanced settings
Create a system restore point before computers are cleaned:
No
Disable the client user interface:
No
Show notifications messages on the client computer when the user needs to run a full scan, update definitions, or run Windows Defender Offline.
No
Delete quarantined files after (days):
0
Allow users to configure the setting for quarantined file deletion:
No
Allow users to exclude files and folders, file types, and processes:
No
Allow all users to view the full History results:
No
Enable reparse point scanning:
No
Randomize scheduled scan and definition update start times (within 30 minutes):
Yes
Enable auto sample file submission to help Microsoft determine whether certain detected items are Malicious:
Yes
Allow users to modify auto sample file submission settings:
No
OK
Cancel

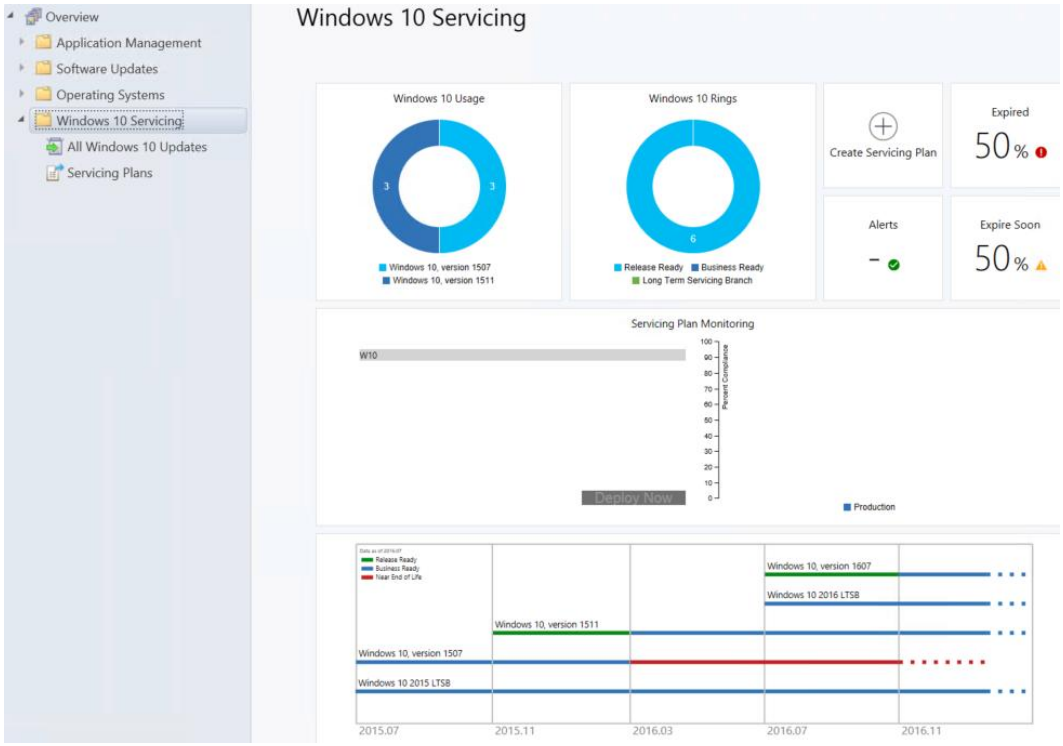

Administration
Overview
Hierarchy Configuration
Cloud Services
Site Configuration
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Client Settings 2 items
Search
Icon
Name
Type
Priority
Deployments
Default Client Settings
Default
10000
0
Endpoint Protection
Device
1
2
Default Settings
Background Intelligent Transfer
Cloud Services
Client Policy
Compliance Settings
Computer Agent
Computer Restart
Endpoint Protection
Enrollment
Hardware Inventory
Metered Internet Connections
Power Management
Remote Tools
Software Deployment
Software Inventory
Software Metering
Software Updates
State Messaging
User and Device Affinity
Client Cache Settings
Default Settings
Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.
Specify how client computers retrieve policy.
Device Settings
Client policy polling interval (minutes)
15
Enable user policy on clients
Yes
Enable user policy requests from Internet clients
No
OK
Cancel

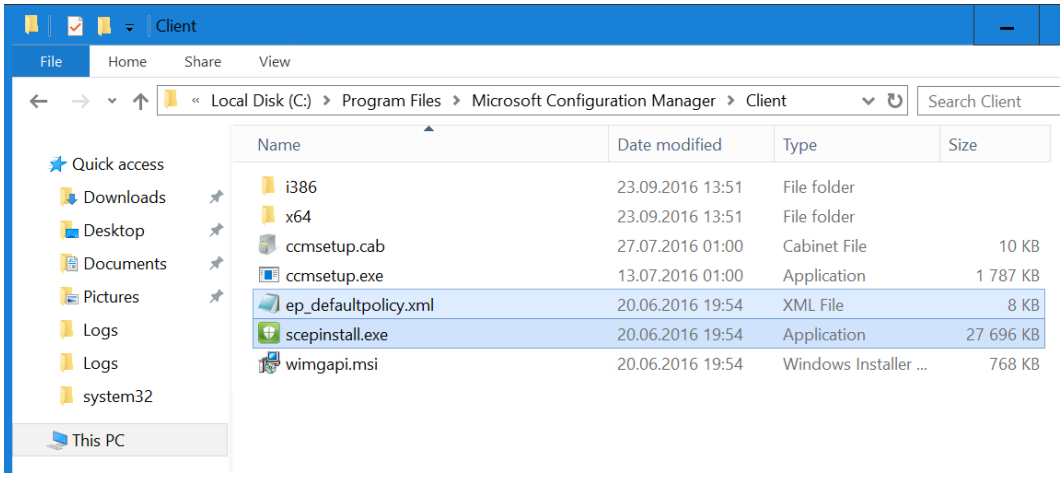

Default Settings
Background Intelligent Transfer
Cloud Services
Client Policy
Compliance Settings
Computer Agent
Computer Restart
Endpoint Protection
Enrollment
Hardware Inventory
Metered Internet Connections
Power Management
Remote Tools
Software Deployment
Software Inventory
Software Metering
Software Updates
State Messaging
User and Device Affinity
Client Cache Settings
Default Settings
Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.
Specify Background Intelligent Transfer settings for client computers.
Device Settings
Limit the maximum network bandwidth for BITS background transfers
Yes
Throttling window start time
08
Throttling window end time
16
Maximum transfer rate during throttling window (Kbps)
2000
Allow BITS downloads outside the throttling window
Yes
Maximum transfer rate outside the throttling window (Kbps)
9999
OK
Cancel

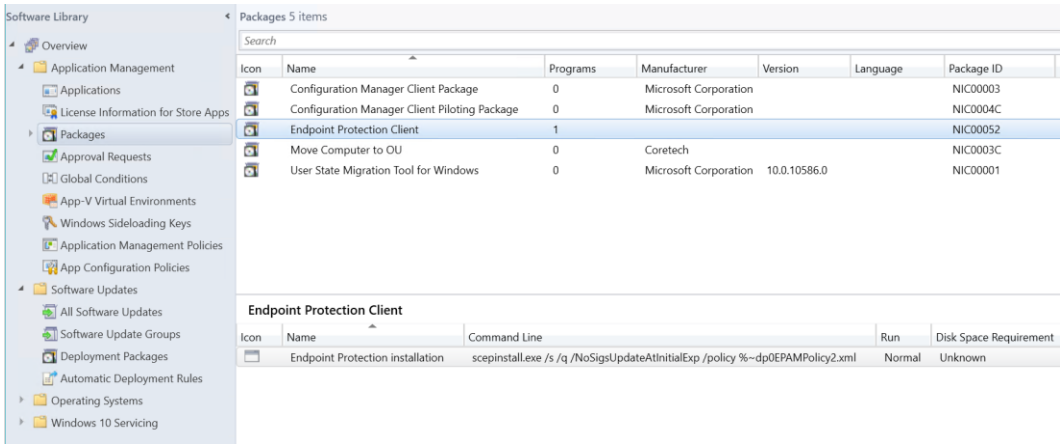

Disk
100 MB/sec
60 Seconds
0
Disk 0 (C:) Queue Length
50
0

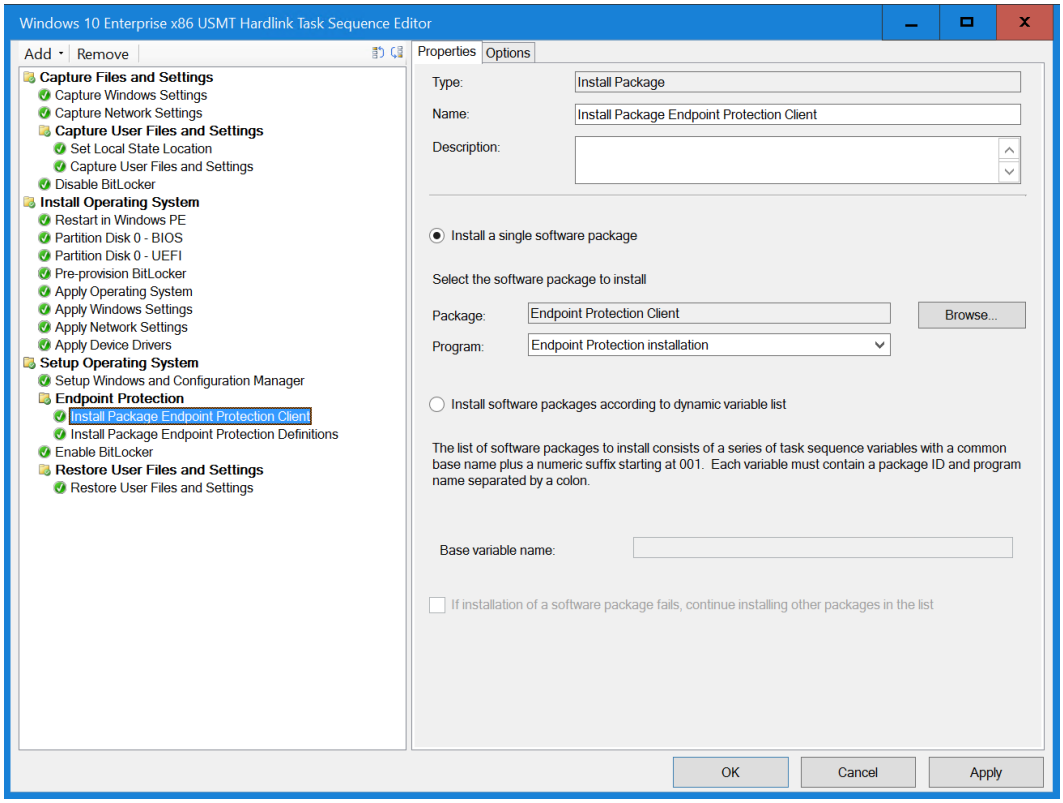
# Chapter 6: Configuring and Troubleshooting Performance and Advanced Protection

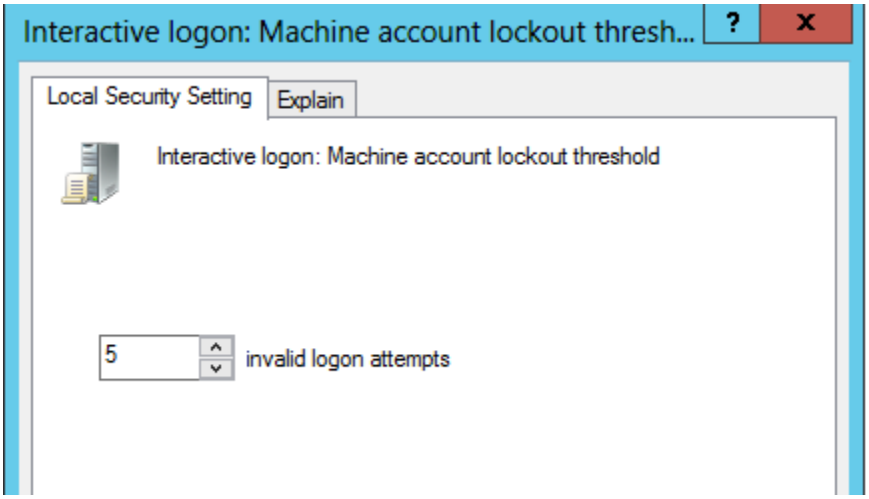


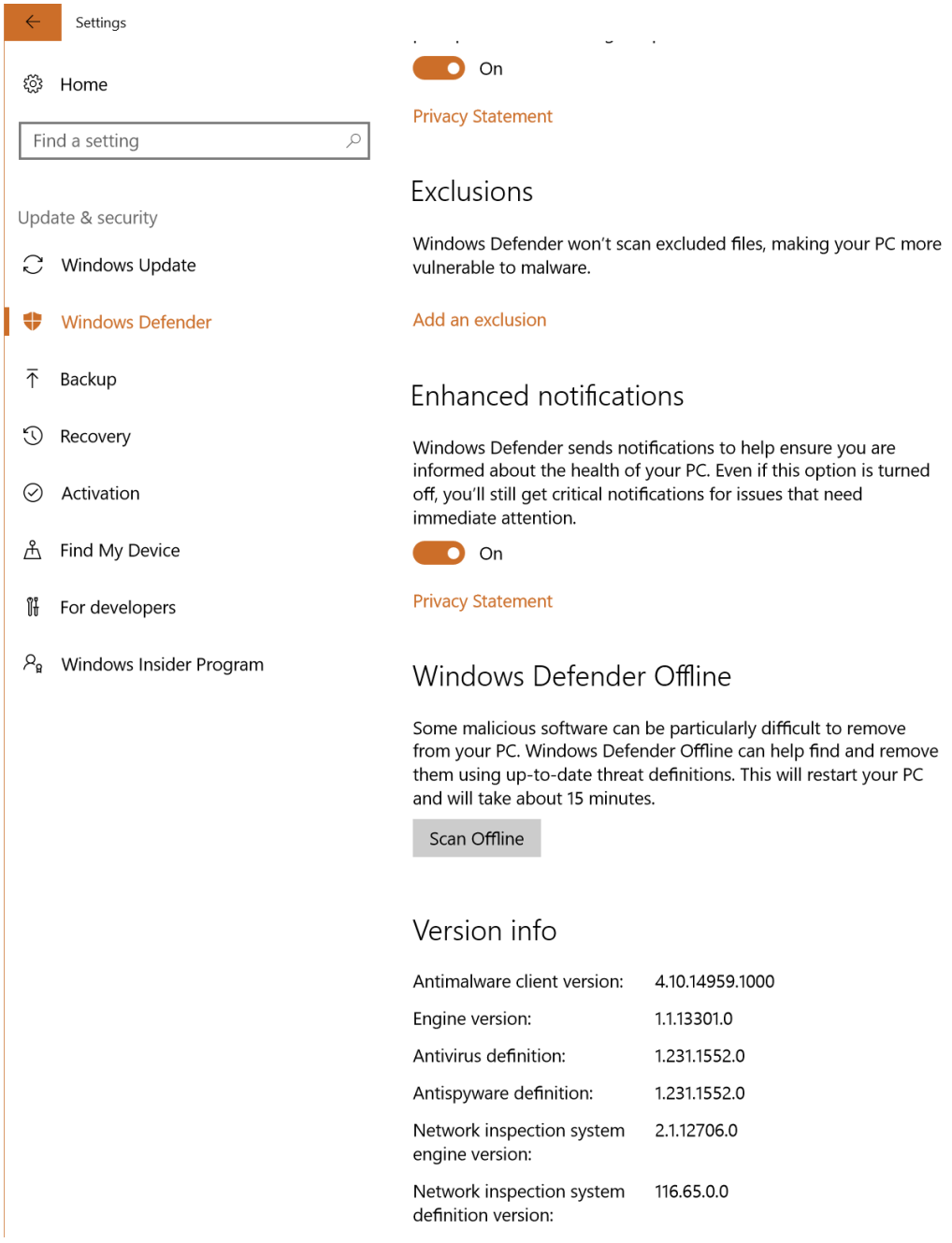

Overview
Application Management
Software Updates
Operating Systems
Windows 10 Servicing
All Windows 10 Updates
Servicing Plans
Windows 10 Servicing
Windows 10 Usage
Windows 10, version 1507
Windows 10, version 1511
Windows 10 Rings
Release Ready
Business Ready
Long Term Servicing Branch
Create Servicing Plan
Expired
50 %
Alerts
Expire Soon
50 %
Servicing Plan Monitoring
W10
Deploy Now
Production
Windows 10, version 1607
Windows 10 2016 LTSB
Windows 10, version 1511
Windows 10, version 1507
Windows 10 2015 LTSB
2015.07
2015.11
2016.03
2016.07
2016.11


Client
File
Home
Share
View
Local Disk (C:) › Program Files › Microsoft Configuration Manager › Client
Search Client
Quick access
Downloads
Desktop
Documents
Pictures
Logs
Logs
system32
This PC
Name
Date modified
Type
Size
i386 23.09.2016 13:51 File folder
x64 23.09.2016 13:51 File folder
ccmsetup.cab 27.07.2016 01:00 Cabinet File 10 KB
ccmsetup.exe 13.07.2016 01:00 Application 1 787 KB
ep_defaultpolicy.xml 20.06.2016 19:54 XML File 8 KB
scepinstall.exe 20.06.2016 19:54 Application 27 696 KB
wimgapi.msi 20.06.2016 19:54 Windows Installer ... 768 KB

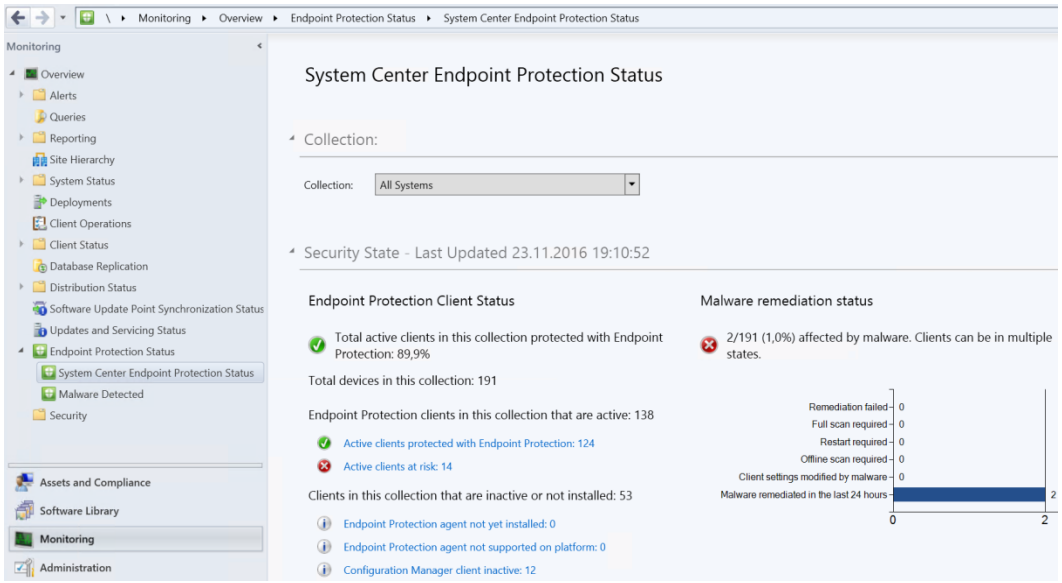

Software Library
Overview
Application Management
Applications
License Information for Store Apps
Packages
Approval Requests
Global Conditions
App-V Virtual Environments
Windows Sideloading Keys
Application Management Policies
App Configuration Policies
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Packages 5 items
Search
Icon
Name
Programs
Manufacturer
Version
Language
Package ID
Configuration Manager Client Package 0 Microsoft Corporation NIC00003
Configuration Manager Client Piloting Package 0 Microsoft Corporation NIC0004C
Endpoint Protection Client 1 NIC00052
Move Computer to OU 0 Coretech NIC0003C
User State Migration Tool for Windows 0 Microsoft Corporation 10.0.10586.0 NIC00001
Endpoint Protection Client
Icon
Name
Command Line
Run
Disk Space Requirement
Endpoint Protection installation scepinstall.exe /s /q /NoSigsUpdateAtInitialExp /policy %~dp0EPAMPolicy2.xml Normal Unknown

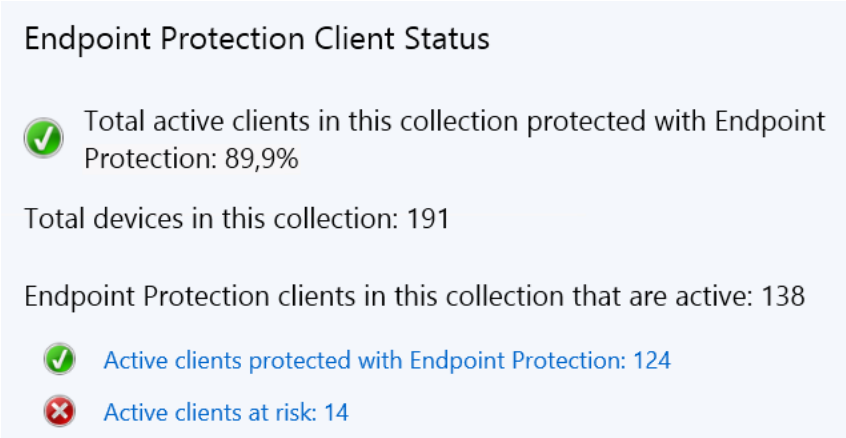

Windows 10 Enterprise x86 USMT Hardlink Task Sequence Editor
Add
Remove
Capture Files and Settings
Capture Windows Settings
Capture Network Settings
Capture User Files and Settings
Set Local State Location
Capture User Files and Settings
Disable BitLocker
Install Operating System
Restart in Windows PE
Partition Disk 0 - BIOS
Partition Disk 0 - UEFI
Pre-provision BitLocker
Apply Operating System
Apply Windows Settings
Apply Network Settings
Apply Device Drivers
Setup Operating System
Setup Windows and Configuration Manager
Endpoint Protection
Install Package Endpoint Protection Client
Install Package Endpoint Protection Definitions
Enable BitLocker
Restore User Files and Settings
Restore User Files and Settings
Properties
Options
Type:
Install Package
Name:
Install Package Endpoint Protection Client
Description:
Install a single software package
Select the software package to install
Package:
Endpoint Protection Client
Browse...
Program:
Endpoint Protection installation
Install software packages according to dynamic variable list
The list of software packages to install consists of a series of task sequence variables with a common base name plus a numeric suffix starting at 001. Each variable must contain a package ID and program name separated by a colon.
Base variable name:
If installation of a software package fails, continue installing other packages in the list
OK
Cancel
Apply

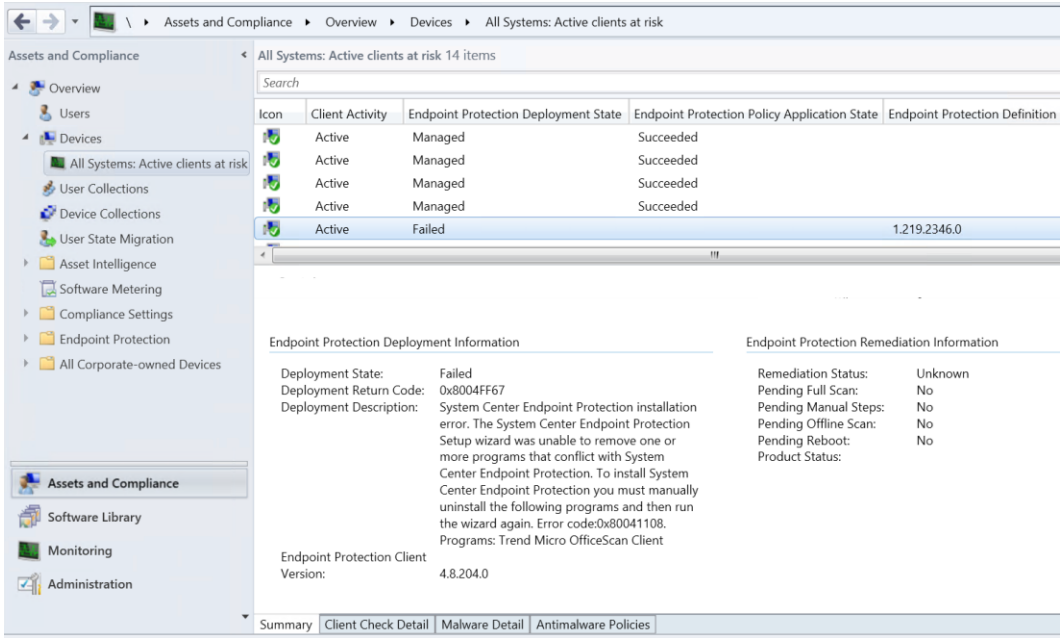

Interactive logon: Machine account lockout thresh...
?
Local Security Setting
Explain
Interactive logon: Machine account lockout threshold
5
invalid logon attempts


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Recovery
Activation
Find My Device
For developers
Windows Insider Program
On
Privacy Statement
Exclusions
Windows Defender won't scan excluded files, making your PC more vulnerable to malware.
Add an exclusion
Enhanced notifications
Windows Defender sends notifications to help ensure you are informed about the health of your PC. Even if this option is turned off, you'll still get critical notifications for issues that need immediate attention.
On
Privacy Statement
Windows Defender Offline
Some malicious software can be particularly difficult to remove from your PC. Windows Defender Offline can help find and remove them using up-to-date threat definitions. This will restart your PC and will take about 15 minutes.
Scan Offline
Version info
Antimalware client version: 4.10.14959.1000
Engine version: 1.1.13301.0
Antivirus definition: 1.231.1552.0
Antispyware definition: 1.231.1552.0
Network inspection system engine version: 2.1.12706.0
Network inspection system definition version: 116.65.0.0

# Chapter 7: Troubleshooting and Fixing Issues



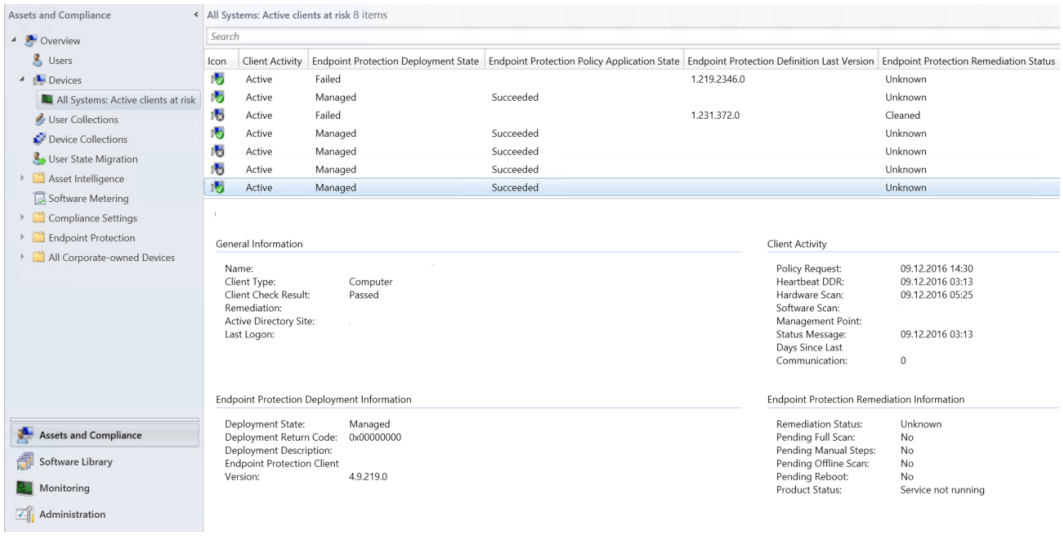


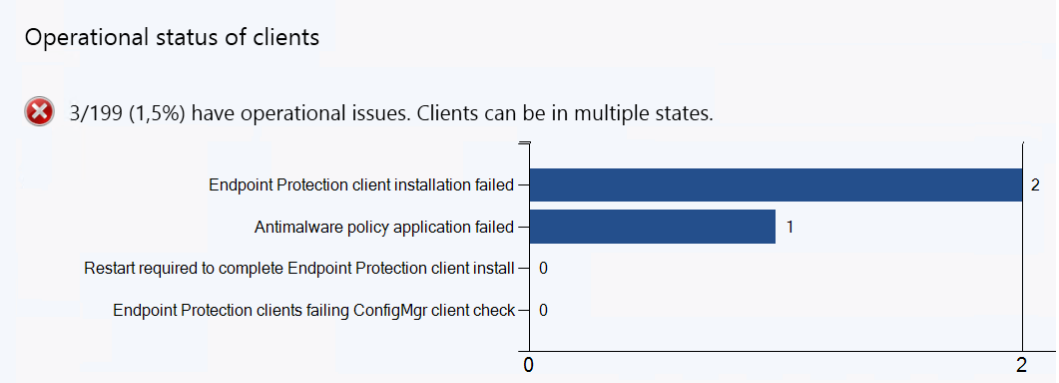

Endpoint Protection Deployment Information

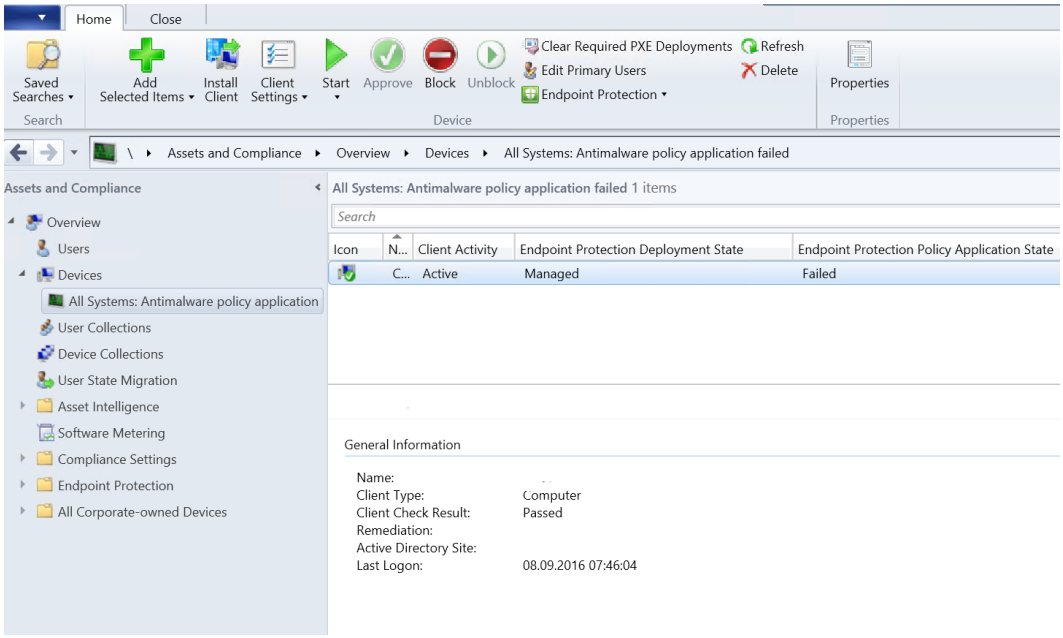
| | |
|---|---|
| Deployment State: | Failed |
| Deployment Return Code: | 0x8004FF83 |
| Deployment Description: | Cannot complete the System Center Endpoint Protection installation. An error has prevented the System Center Endpoint Protection setup wizard from completing successfully. Please restart your computer and try again. Error code:0x8004FF83. |
| Endpoint Protection Client Version: | 4.7.214.0 |

Endpoint Protection Remediation Information

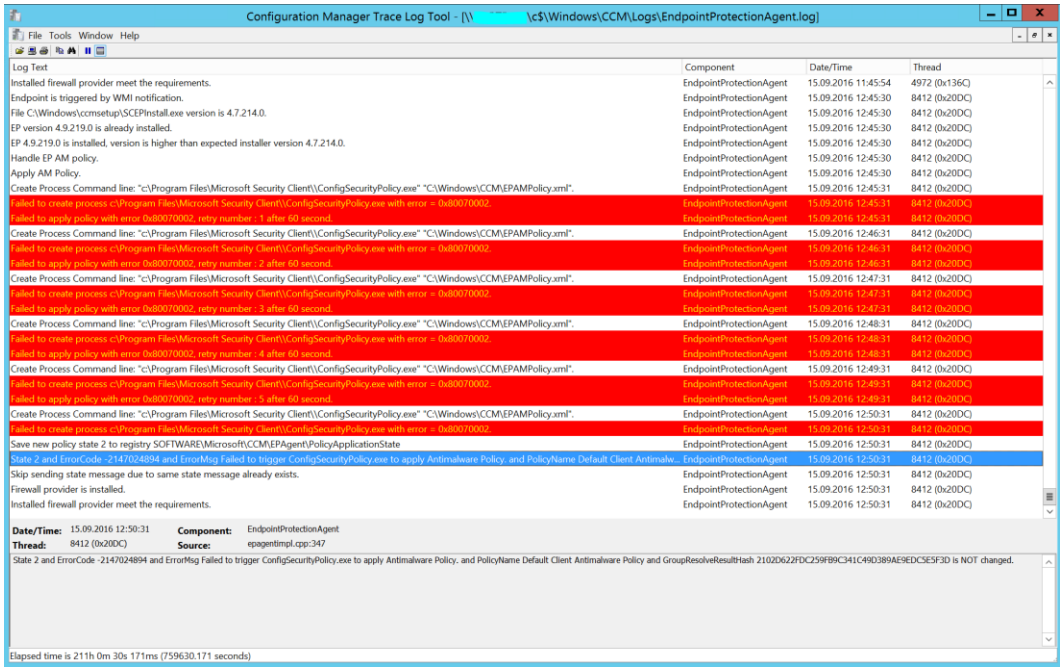
| | |
|---|---|
| Remediation Status: | None |
| Pending Full Scan: | No |
| Pending Manual Steps: | No |
| Pending Offline Scan: | No |
| Pending Reboot: | No |
| Product Status: | Service started without any malware protection engine; AV signatures out of date; AS signatures out of date |


Assets and Compliance
Overview
Users
Devices
All Systems: Active clients at risk
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
All Systems: Active clients at risk 8 items
Search
Icon
Client Activity
Endpoint Protection Deployment State
Endpoint Protection Policy Application State
Endpoint Protection Definition Last Version
Endpoint Protection Remediation Status
Active Failed 1.219.2346.0 Unknown
Active Managed Succeeded Unknown
Active Failed 1.231.372.0 Cleaned
Active Managed Succeeded Unknown
Active Managed Succeeded Unknown
Active Managed Succeeded Unknown
Active Managed Succeeded Unknown
General Information
Name:
Client Type: Computer
Client Check Result: Passed
Remediation:
Active Directory Site:
Last Logon:
Client Activity
Policy Request: 09.12.2016 14:30
Heartbeat DDR: 09.12.2016 03:13
Hardware Scan: 09.12.2016 05:25
Software Scan:
Management Point:
Status Message: 09.12.2016 03:13
Days Since Last Communication: 0
Endpoint Protection Deployment Information
Deployment State: Managed
Deployment Return Code: 0x00000000
Deployment Description:
Endpoint Protection Client Version: 4.9.219.0
Endpoint Protection Remediation Information
Remediation Status: Unknown
Pending Full Scan: No
Pending Manual Steps: No
Pending Offline Scan: No
Pending Reboot: No
Product Status: Service not running


Operational status of clients
3/199 (1,5%) have operational issues. Clients can be in multiple states.
Endpoint Protection client installation failed
2
Antimalware policy application failed
1
Restart required to complete Endpoint Protection client install
0
Endpoint Protection clients failing ConfigMgr client check
0
0
2

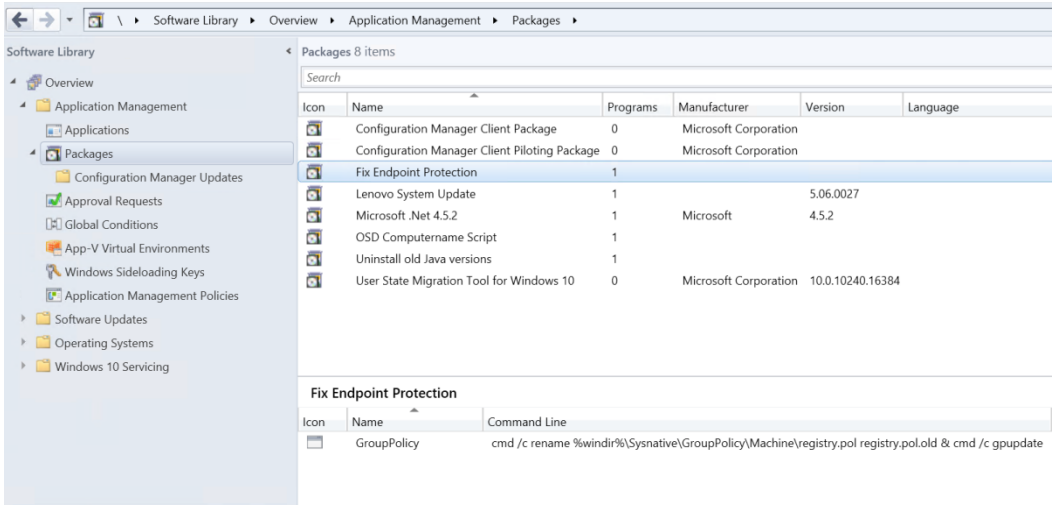


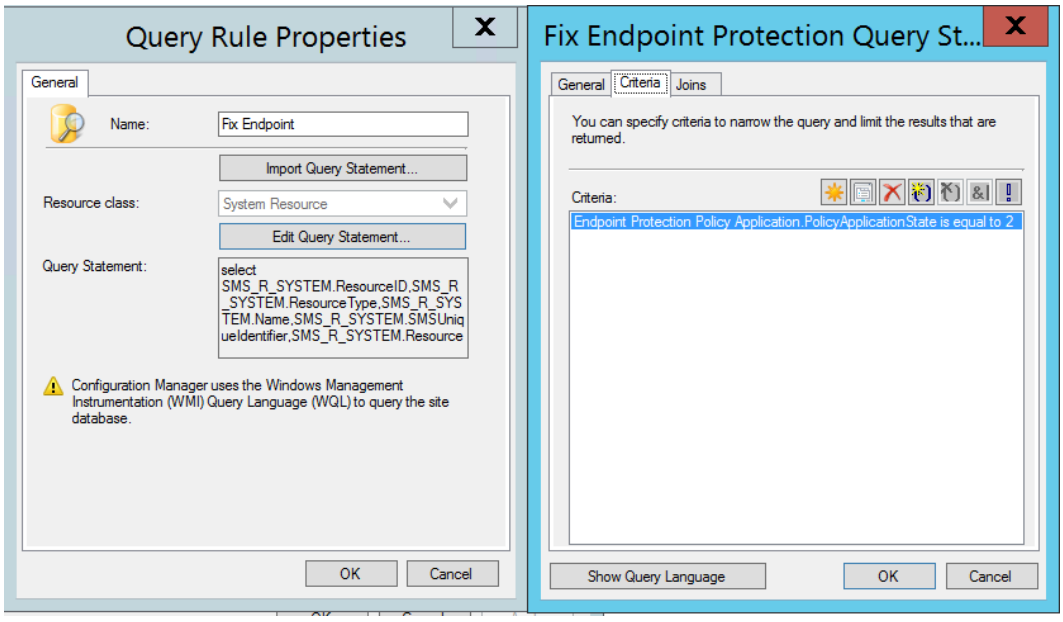

| Policy Application State | Last Update Time | Policy Application Return Code | Policy Application Description |
|---|---|---|---|
| Failed | 31.05.2016 08:50 | 0x80070002 | Failed to trigger ConfigSecurityPolicy.exe to apply Antimalware Policy. |

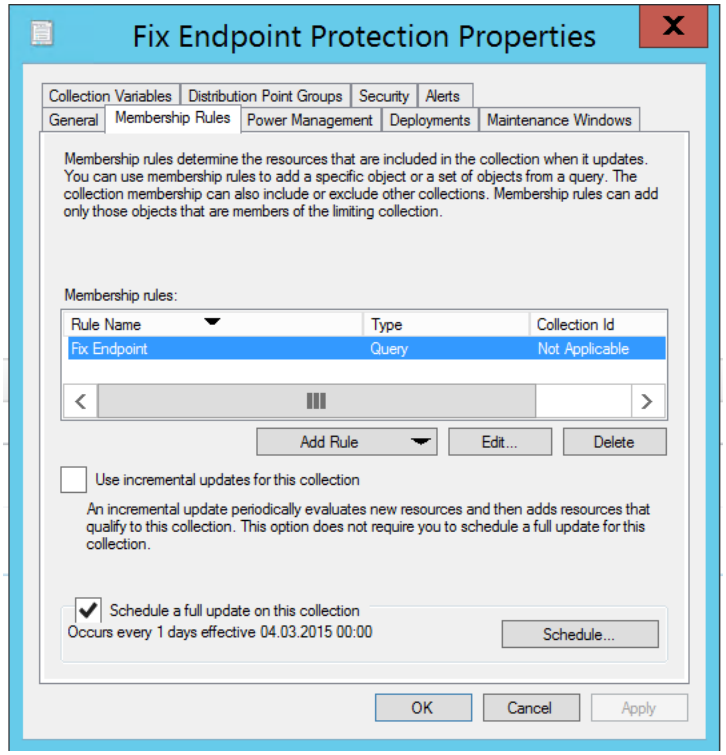


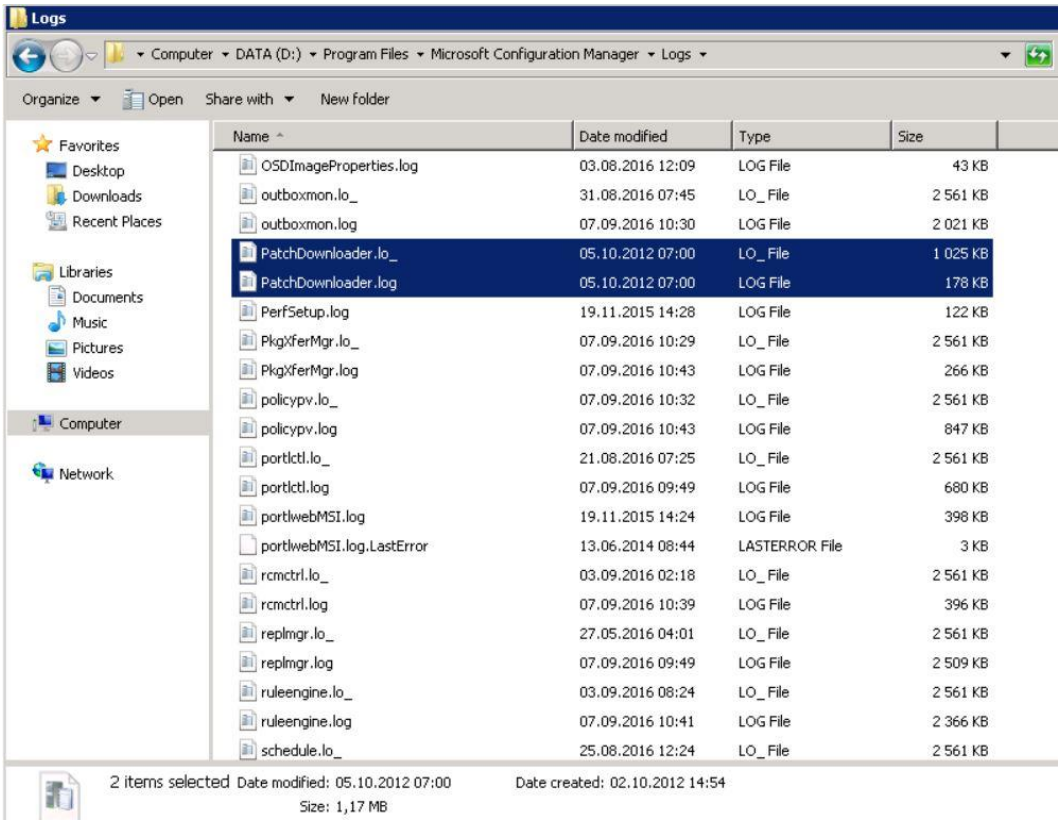

Apply AM Policy.
Create Process Command line: "C:\Program Files\Microsoft Security Client\ConfigSecurityPolicy.exe" "C:\Windows\CCM\EPAMPolicy.xml".
Applied the C:\Windows\CCM\EPAMPolicy.xml with ConfigSecurityPolicy.exe successfully.
Send State Message with topic type = 2002, state id = 1, error code = 0x00000000, and message = <PolicyName>SCEP2012 Standard Desktop
Save new policy state 1 to registry SOFTWARE\Microsoft\CCM\EPAgent\PolicyApplicationState

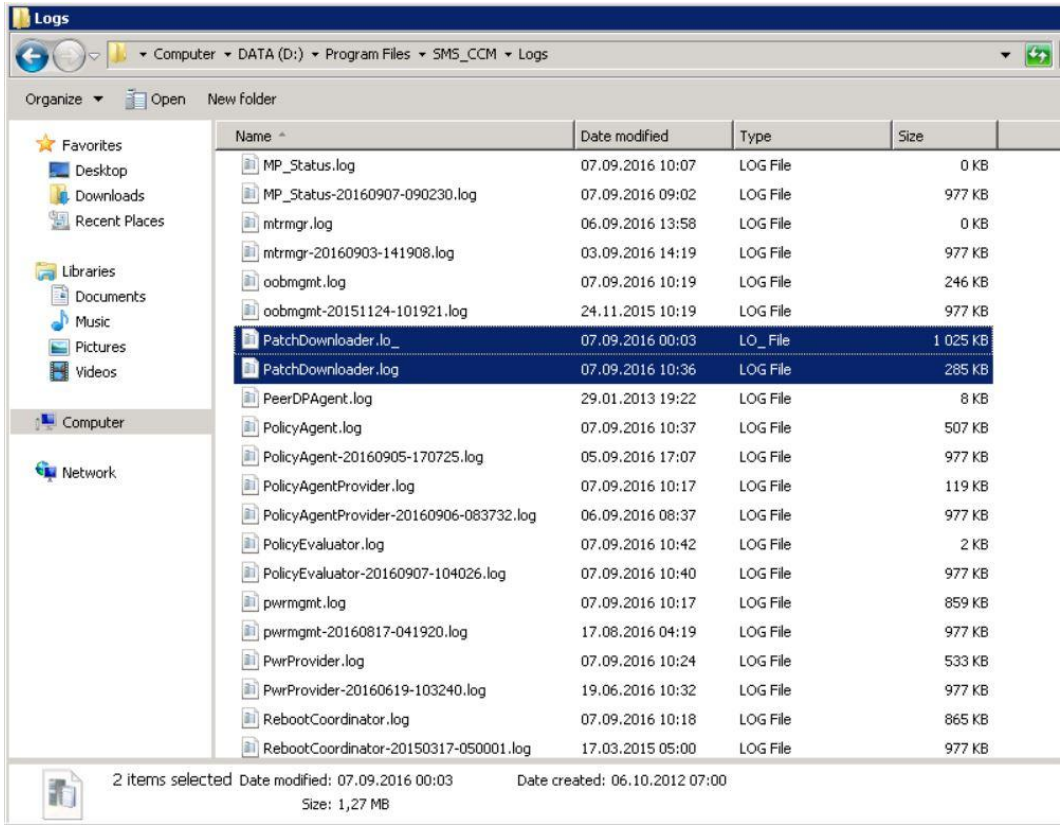
| Client Activity | EP Deployment State | EP Policy Name | EP Policy Application State |
|---|---|---|---|
| Active | Managed | Default Client Antimalware Policy | Succeeded |

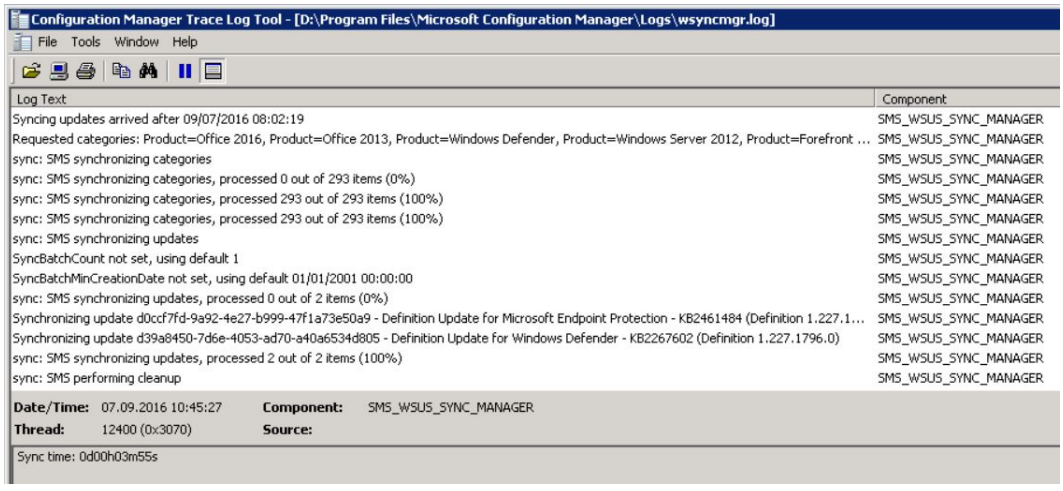

Software Library ▸ Overview ▸ Application Management ▸ Packages ▸
Software Library
Overview
Application Management
Applications
Packages
Configuration Manager Updates
Approval Requests
Global Conditions
App-V Virtual Environments
Windows Sideloading Keys
Application Management Policies
Software Updates
Operating Systems
Windows 10 Servicing
Packages 8 items
Search
Icon
Name
Programs
Manufacturer
Version
Language
Configuration Manager Client Package 0 Microsoft Corporation
Configuration Manager Client Piloting Package 0 Microsoft Corporation
Fix Endpoint Protection 1
Lenovo System Update 1 5.06.0027
Microsoft .Net 4.5.2 1 Microsoft 4.5.2
OSD Computername Script 1
Uninstall old Java versions 1
User State Migration Tool for Windows 10 0 Microsoft Corporation 10.0.10240.16384
Fix Endpoint Protection
Icon
Name
Command Line
GroupPolicy
cmd /c rename %windir%\Sysnative\GroupPolicy\Machine\registry.pol registry.pol.old & cmd /c gpupdate

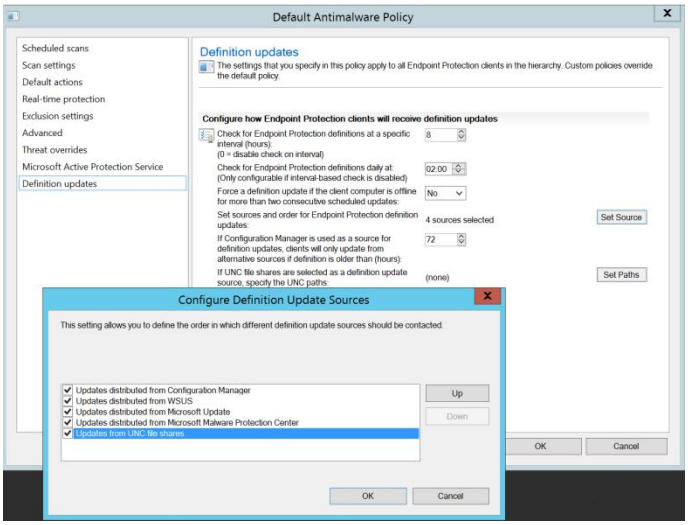

Query Rule Properties
General
Name:
Fix Endpoint
Import Query Statement...
Resource class:
System Resource
Edit Query Statement...
Query Statement:
select SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SMSUniqueIdentifier,SMS_R_SYSTEM.Resource
Configuration Manager uses the Windows Management Instrumentation (WMI) Query Language (WQL) to query the site database.
OK
Cancel
Fix Endpoint Protection Query St...
General
Criteria
Joins
You can specify criteria to narrow the query and limit the results that are returned.
Criteria:
Endpoint Protection Policy Application.PolicyApplicationState is equal to 2
Show Query Language
OK
Cancel

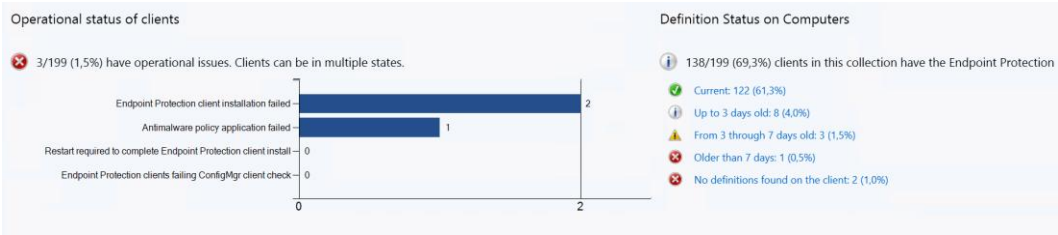

Fix Endpoint Protection Properties
Collection Variables
Distribution Point Groups
Security
Alerts
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.
Membership rules:
Rule Name
Type
Collection Id
Fix Endpoint
Query
Not Applicable
Add Rule
Edit...
Delete
Use incremental updates for this collection
An incremental update periodically evaluates new resources and then adds resources that qualify to this collection. This option does not require you to schedule a full update for this collection.
Schedule a full update on this collection
Occurs every 1 days effective 04.03.2015 00:00
Schedule...
OK
Cancel
Apply

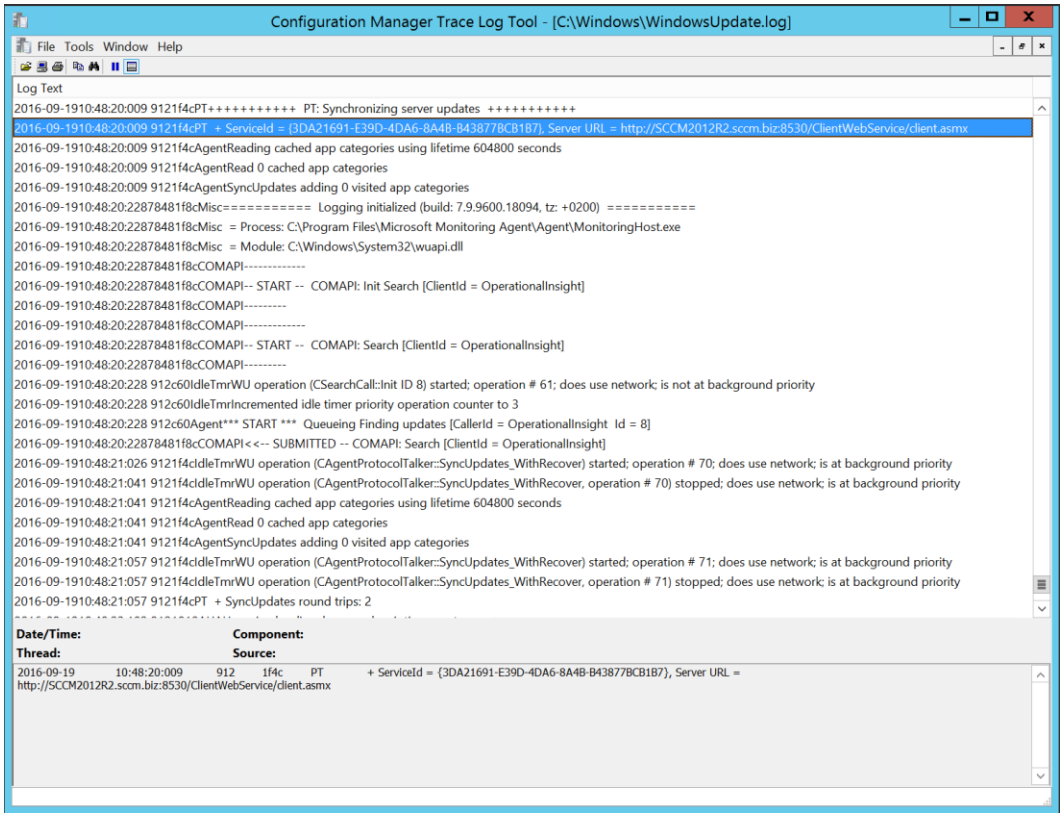

Logs
Computer ▸ DATA (D:) ▸ Program Files ▸ Microsoft Configuration Manager ▸ Logs ▸
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
OSDImageProperties.log 03.08.2016 12:09 LOG File 43 KB
outboxmon.lo_ 31.08.2016 07:45 LO_File 2 561 KB
outboxmon.log 07.09.2016 10:30 LOG File 2 021 KB
PatchDownloader.lo_ 05.10.2012 07:00 LO_File 1 025 KB
PatchDownloader.log 05.10.2012 07:00 LOG File 178 KB
PerfSetup.log 19.11.2015 14:28 LOG File 122 KB
PkgXferMgr.lo_ 07.09.2016 10:29 LO_File 2 561 KB
PkgXferMgr.log 07.09.2016 10:43 LOG File 266 KB
policypv.lo_ 07.09.2016 10:32 LO_File 2 561 KB
policypv.log 07.09.2016 10:43 LOG File 847 KB
portlctl.lo_ 21.08.2016 07:25 LO_File 2 561 KB
portlctl.log 07.09.2016 09:49 LOG File 680 KB
portlwebMSI.log 19.11.2015 14:24 LOG File 398 KB
portlwebMSI.log.LastError 13.06.2014 08:44 LASTERROR File 3 KB
rcmctrl.lo_ 03.09.2016 02:18 LO_File 2 561 KB
rcmctrl.log 07.09.2016 10:39 LOG File 396 KB
replmgr.lo_ 27.05.2016 04:01 LO_File 2 561 KB
replmgr.log 07.09.2016 09:49 LOG File 2 509 KB
ruleengine.lo_ 03.09.2016 08:24 LO_File 2 561 KB
ruleengine.log 07.09.2016 10:41 LOG File 2 366 KB
schedule.lo_ 25.08.2016 12:24 LO_File 2 561 KB
2 items selected Date modified: 05.10.2012 07:00 Date created: 02.10.2012 14:54
Size: 1,17 MB

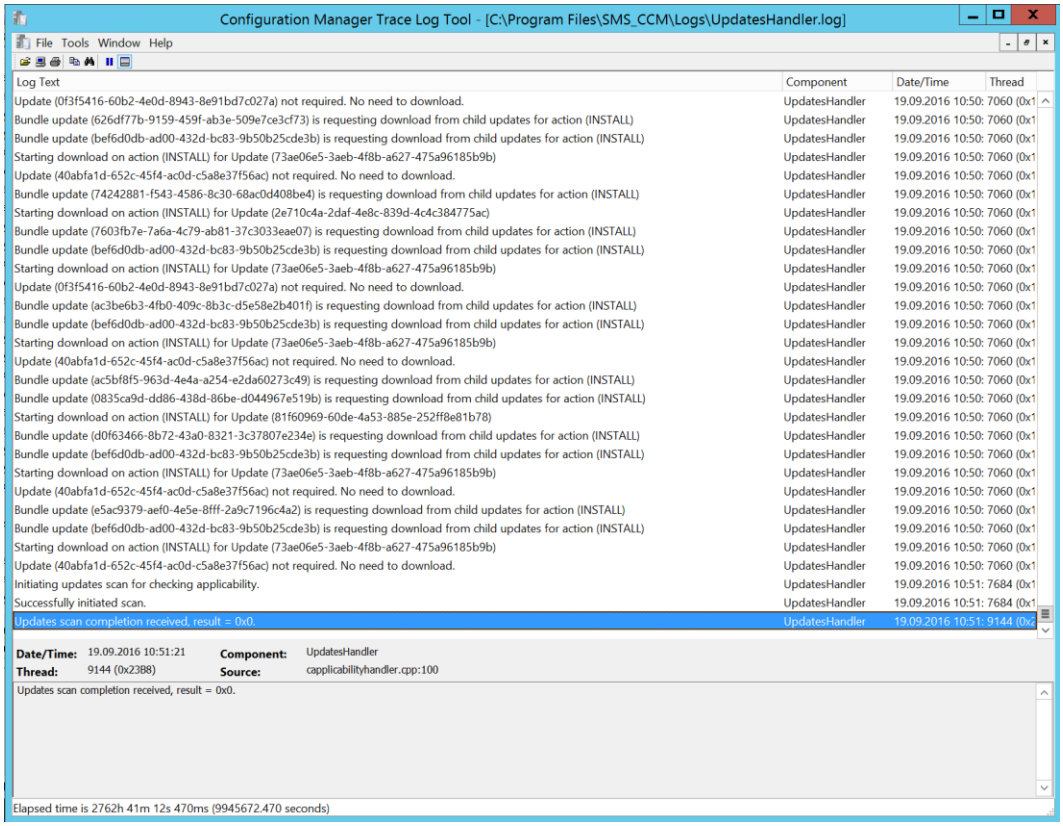

Logs
Computer ▸ DATA (D:) ▸ Program Files ▸ SMS_CCM ▸ Logs
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
MP_Status.log 07.09.2016 10:07 LOG File 0 KB
MP_Status-20160907-090230.log 07.09.2016 09:02 LOG File 977 KB
mtrmgr.log 06.09.2016 13:58 LOG File 0 KB
mtrmgr-20160903-141908.log 03.09.2016 14:19 LOG File 977 KB
oobmgmt.log 07.09.2016 10:19 LOG File 246 KB
oobmgmt-20151124-101921.log 24.11.2015 10:19 LOG File 977 KB
PatchDownloader.lo_ 07.09.2016 00:03 LO_ File 1 025 KB
PatchDownloader.log 07.09.2016 10:36 LOG File 285 KB
PeerDPAgent.log 29.01.2013 19:22 LOG File 8 KB
PolicyAgent.log 07.09.2016 10:37 LOG File 507 KB
PolicyAgent-20160905-170725.log 05.09.2016 17:07 LOG File 977 KB
PolicyAgentProvider.log 07.09.2016 10:17 LOG File 119 KB
PolicyAgentProvider-20160906-083732.log 06.09.2016 08:37 LOG File 977 KB
PolicyEvaluator.log 07.09.2016 10:42 LOG File 2 KB
PolicyEvaluator-20160907-104026.log 07.09.2016 10:40 LOG File 977 KB
pwrmgmt.log 07.09.2016 10:17 LOG File 859 KB
pwrmgmt-20160817-041920.log 17.08.2016 04:19 LOG File 977 KB
PwrProvider.log 07.09.2016 10:24 LOG File 533 KB
PwrProvider-20160619-103240.log 19.06.2016 10:32 LOG File 977 KB
RebootCoordinator.log 07.09.2016 10:18 LOG File 865 KB
RebootCoordinator-20150317-050001.log 17.03.2015 05:00 LOG File 977 KB
2 items selected Date modified: 07.09.2016 00:03 Date created: 06.10.2012 07:00
Size: 1,27 MB


Configuration Manager Trace Log Tool - [D:\Program Files\Microsoft Configuration Manager\Logs\wsyncmgr.log]
File Tools Window Help
Log Text
Component
Syncing updates arrived after 09/07/2016 08:02:19 SMS_WSUS_SYNC_MANAGER
Requested categories: Product=Office 2016, Product=Office 2013, Product=Windows Defender, Product=Windows Server 2012, Product=Forefront ... SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing categories SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing categories, processed 0 out of 293 items (0%) SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing categories, processed 293 out of 293 items (100%) SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing categories, processed 293 out of 293 items (100%) SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing updates SMS_WSUS_SYNC_MANAGER
SyncBatchCount not set, using default 1 SMS_WSUS_SYNC_MANAGER
SyncBatchMinCreationDate not set, using default 01/01/2001 00:00:00 SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing updates, processed 0 out of 2 items (0%) SMS_WSUS_SYNC_MANAGER
Synchronizing update d0ccf7fd-9a92-4e27-b999-47f1a73e50a9 - Definition Update for Microsoft Endpoint Protection - KB2461484 (Definition 1.227.1... SMS_WSUS_SYNC_MANAGER
Synchronizing update d39a8450-7d6e-4053-ad70-a40a6534d805 - Definition Update for Windows Defender - KB2267602 (Definition 1.227.1796.0) SMS_WSUS_SYNC_MANAGER
sync: SMS synchronizing updates, processed 2 out of 2 items (100%) SMS_WSUS_SYNC_MANAGER
sync: SMS performing cleanup SMS_WSUS_SYNC_MANAGER
Date/Time: 07.09.2016 10:45:27 Component: SMS_WSUS_SYNC_MANAGER
Thread: 12400 (0x3070) Source:
Sync time: 0d00h03m55s

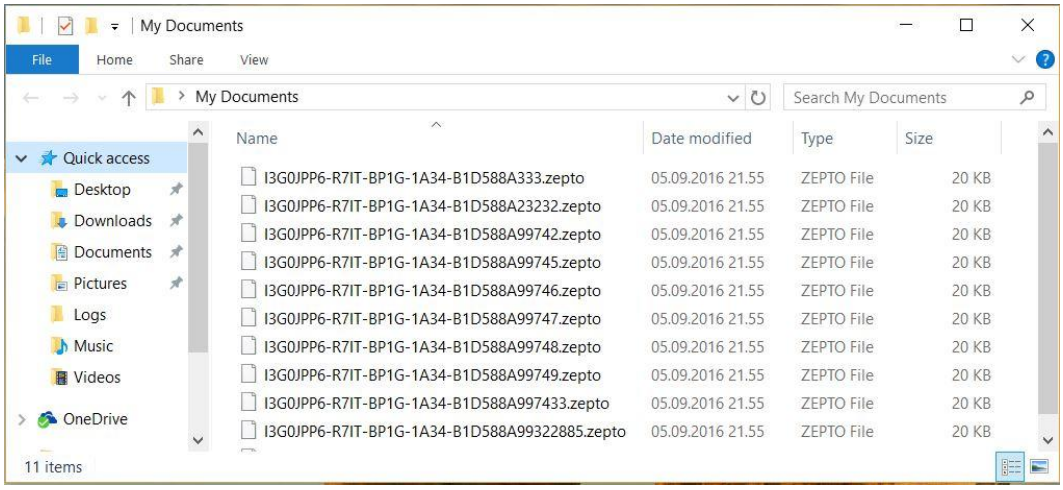

Default Antimalware Policy
Scheduled scans
Scan settings
Default actions
Real-time protection
Exclusion settings
Advanced
Threat overrides
Microsoft Active Protection Service
Definition updates
Definition updates
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Configure how Endpoint Protection clients will receive definition updates
Check for Endpoint Protection definitions at a specific interval (hours):
(0 = disable check on interval)
8
Check for Endpoint Protection definitions daily at:
(Only configurable if interval-based check is disabled)
02:00
Force a definition update if the client computer is offline for more than two consecutive scheduled updates:
No
Set sources and order for Endpoint Protection definition updates:
4 sources selected
Set Source
If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours):
72
If UNC file shares are selected as a definition update source, specify the UNC paths:
(none)
Set Paths
OK
Cancel
Configure Definition Update Sources
This setting allows you to define the order in which different definition update sources should be contacted.
Updates distributed from Configuration Manager
Updates distributed from WSUS
Updates distributed from Microsoft Update
Updates distributed from Microsoft Malware Protection Center
Updates from UNC file shares
Up
Down
OK
Cancel

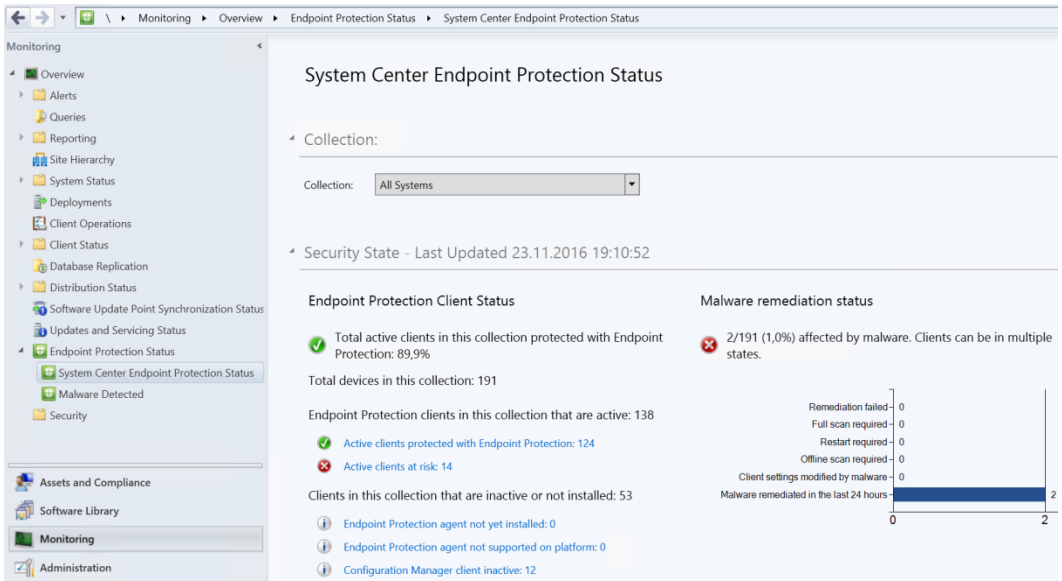

Operational status of clients
3/199 (1,5%) have operational issues. Clients can be in multiple states.
Endpoint Protection client installation failed
2
Antimalware policy application failed
1
Restart required to complete Endpoint Protection client install
0
Endpoint Protection clients failing ConfigMgr client check
0
0
2
Definition Status on Computers
138/199 (69,3%) clients in this collection have the Endpoint Protection
Current: 122 (61,3%)
Up to 3 days old: 8 (4,0%)
From 3 through 7 days old: 3 (1,5%)
Older than 7 days: 1 (0,5%)
No definitions found on the client: 2 (1,0%)


Configuration Manager Trace Log Tool - [C:\Windows\WindowsUpdate.log]
File Tools Window Help
Log Text
2016-09-1910:48:20:009 9121f4cPT++++++++++ PT: Synchronizing server updates ++++++++++
2016-09-1910:48:20:009 9121f4cPT + ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7}, Server URL = http://SCCM2012R2.sccm.biz:8530/ClientWebService/client.asmx
2016-09-1910:48:20:009 9121f4cAgentReading cached app categories using lifetime 604800 seconds
2016-09-1910:48:20:009 9121f4cAgentRead 0 cached app categories
2016-09-1910:48:20:009 9121f4cAgentSyncUpdates adding 0 visited app categories
2016-09-1910:48:20:22878481f8cMisc========== Logging initialized (build: 7.9.9600.18094, tz: +0200) ==========
2016-09-1910:48:20:22878481f8cMisc = Process: C:\Program Files\Microsoft Monitoring Agent\Agent\MonitoringHost.exe
2016-09-1910:48:20:22878481f8cMisc = Module: C:\Windows\System32\wuapi.dll
2016-09-1910:48:20:22878481f8cCOMAPI----------
2016-09-1910:48:20:22878481f8cCOMAPI-- START -- COMAPI: Init Search [ClientId = OperationalInsight]
2016-09-1910:48:20:22878481f8cCOMAPI---------
2016-09-1910:48:20:22878481f8cCOMAPI----------
2016-09-1910:48:20:22878481f8cCOMAPI-- START -- COMAPI: Search [ClientId = OperationalInsight]
2016-09-1910:48:20:22878481f8cCOMAPI---------
2016-09-1910:48:20:228 912c60IdleTmrWU operation (CSearchCall::Init ID 8) started; operation # 61; does use network; is not at background priority
2016-09-1910:48:20:228 912c60IdleTmrIncremented idle timer priority operation counter to 3
2016-09-1910:48:20:228 912c60Agent*** START *** Queueing Finding updates [CallerId = OperationalInsight Id = 8]
2016-09-1910:48:20:22878481f8cCOMAPI<-- SUBMITTED -- COMAPI: Search [ClientId = OperationalInsight]
2016-09-1910:48:21:026 9121f4cIdleTmrWU operation (CAgentProtocolTalker::SyncUpdates_WithRecover) started; operation # 70; does use network; is at background priority
2016-09-1910:48:21:041 9121f4cIdleTmrWU operation (CAgentProtocolTalker::SyncUpdates_WithRecover, operation # 70) stopped; does use network; is at background priority
2016-09-1910:48:21:041 9121f4cAgentReading cached app categories using lifetime 604800 seconds
2016-09-1910:48:21:041 9121f4cAgentRead 0 cached app categories
2016-09-1910:48:21:041 9121f4cAgentSyncUpdates adding 0 visited app categories
2016-09-1910:48:21:057 9121f4cIdleTmrWU operation (CAgentProtocolTalker::SyncUpdates_WithRecover) started; operation # 71; does use network; is at background priority
2016-09-1910:48:21:057 9121f4cIdleTmrWU operation (CAgentProtocolTalker::SyncUpdates_WithRecover, operation # 71) stopped; does use network; is at background priority
2016-09-1910:48:21:057 9121f4cPT + SyncUpdates round trips: 2
Date/Time:
Component:
Thread:
Source:
2016-09-19 10:48:20:009 912 1f4c PT + ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7}, Server URL = http://SCCM2012R2.sccm.biz:8530/ClientWebService/client.asmx


Configuration Manager Trace Log Tool - [C:\Program Files\SMS_CCM\Logs\UpdatesHandler.log]
File Tools Window Help
Log Text Component Date/Time Thread
Update (0f3f5416-60b2-4e0d-8943-8e91bd7c027a) not required. No need to download. UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (626df77b-9159-459f-ab3e-509e7ce3cf73) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (bef6d0db-ad00-432d-bc83-9b50b25cde3b) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Starting download on action (INSTALL) for Update (73ae06e5-3aeb-4f8b-a627-475a96185b9b) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Update (40abfa1d-652c-45f4-ac0d-c5a8e37f56ac) not required. No need to download. UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (74242881-f543-4586-8c30-68ac0d408be4) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Starting download on action (INSTALL) for Update (2e710c4a-2daf-4e8c-839d-4c4c384775ac) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (7603fb7e-7a6a-4c79-ab81-37c3033eae07) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (bef6d0db-ad00-432d-bc83-9b50b25cde3b) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Starting download on action (INSTALL) for Update (73ae06e5-3aeb-4f8b-a627-475a96185b9b) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Update (0f3f5416-60b2-4e0d-8943-8e91bd7c027a) not required. No need to download. UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (ac3be6b3-4fb0-409c-8b3c-d5e58e2b401f) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (bef6d0db-ad00-432d-bc83-9b50b25cde3b) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Starting download on action (INSTALL) for Update (73ae06e5-3aeb-4f8b-a627-475a96185b9b) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Update (40abfa1d-652c-45f4-ac0d-c5a8e37f56ac) not required. No need to download. UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (ac5bf8f5-963d-4e4a-a254-e2da60273c49) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (0835ca9d-dd86-438d-86be-d044967e519b) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Starting download on action (INSTALL) for Update (81f60969-60de-4a53-885e-252ff8e81b78) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (d0f63466-8b72-43a0-8321-3c37807e234e) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (bef6d0db-ad00-432d-bc83-9b50b25cde3b) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Starting download on action (INSTALL) for Update (73ae06e5-3aeb-4f8b-a627-475a96185b9b) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Update (40abfa1d-652c-45f4-ac0d-c5a8e37f56ac) not required. No need to download. UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (e5ac9379-aef0-4e5e-8fff-2a9c7196c4a2) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Bundle update (bef6d0db-ad00-432d-bc83-9b50b25cde3b) is requesting download from child updates for action (INSTALL) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Starting download on action (INSTALL) for Update (73ae06e5-3aeb-4f8b-a627-475a96185b9b) UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Update (40abfa1d-652c-45f4-ac0d-c5a8e37f56ac) not required. No need to download. UpdatesHandler 19.09.2016 10:50: 7060 (0x1
Initiating updates scan for checking applicability. UpdatesHandler 19.09.2016 10:51: 7684 (0x1
Successfully initiated scan. UpdatesHandler 19.09.2016 10:51: 7684 (0x1
Updates scan completion received, result = 0x0. UpdatesHandler 19.09.2016 10:51: 9144 (0x2
Date/Time: 19.09.2016 10:51:21 Component: UpdatesHandler
Thread: 9144 (0x23B8) Source: capplicabilityhandler.cpp:100
Updates scan completion received, result = 0x0.
Elapsed time is 2762h 41m 12s 470ms (9945672.470 seconds)

# Chapter 8: Malware Handling



## Top 5 malware by number of computers

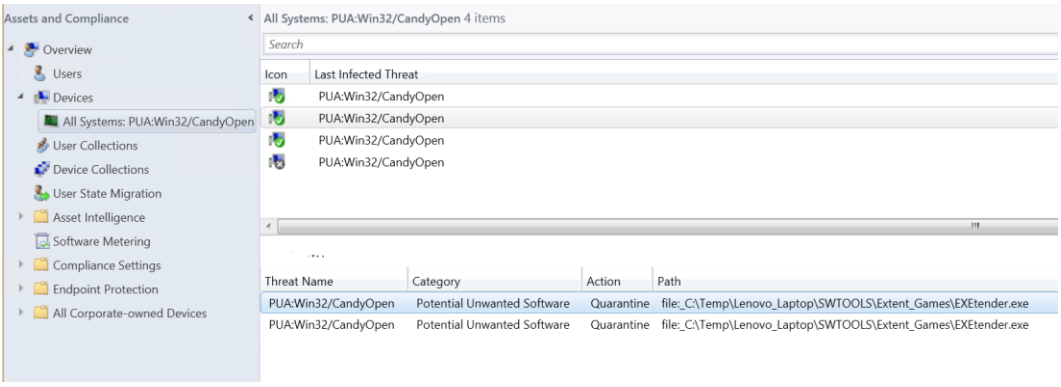
11 different types of malware found

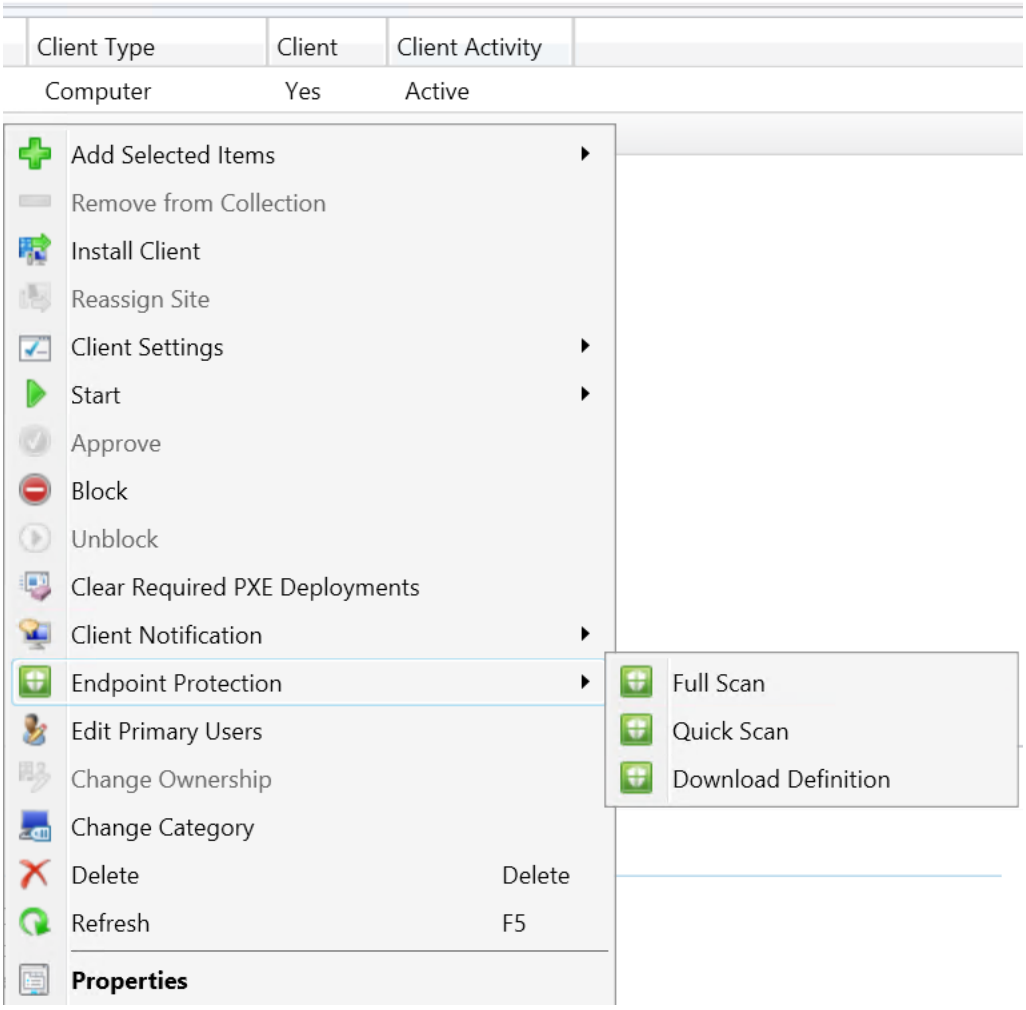
PUA:Win32/AskToolbar 5 clients (2,6%)

PUA:Win32/PcMechanic 3 clients (1,5%)

PUA:Win32/CandyOpen 3 clients (1,5%)

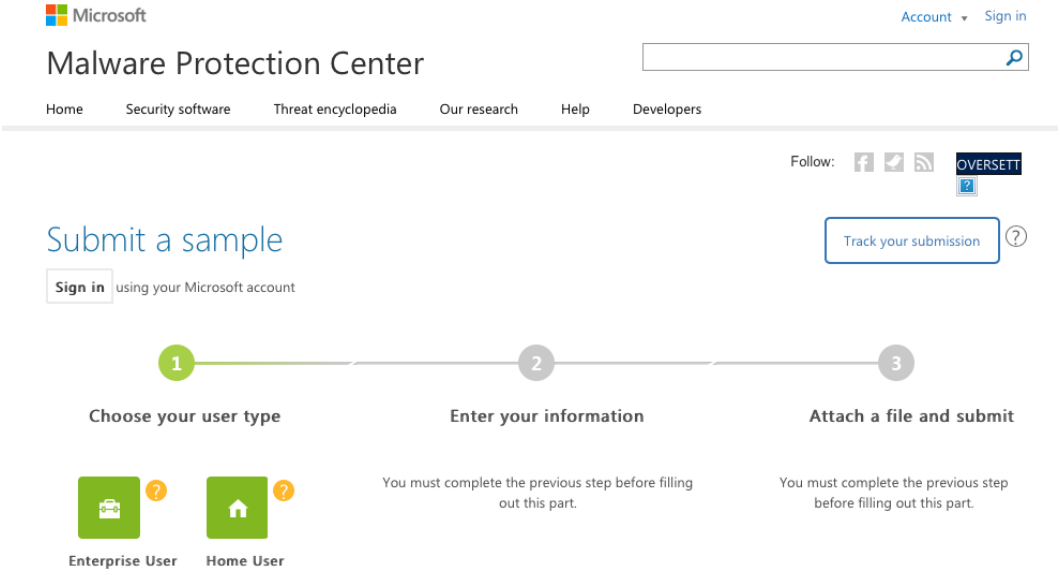
PUA:Win32/Spigot 2 clients (1,0%)

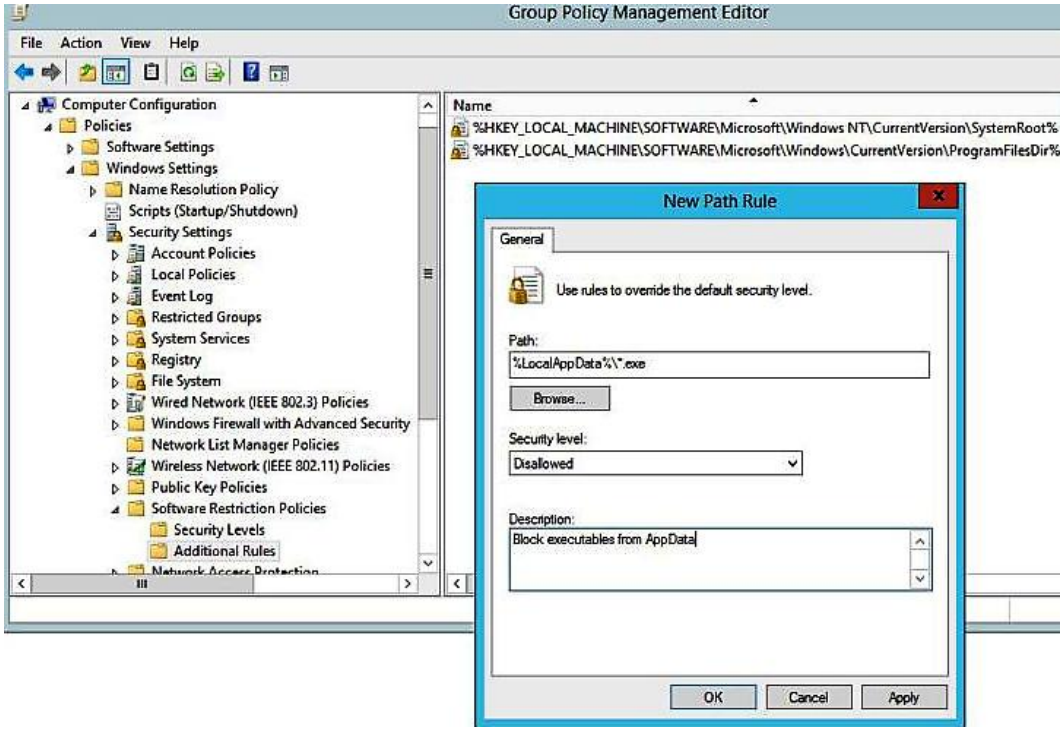


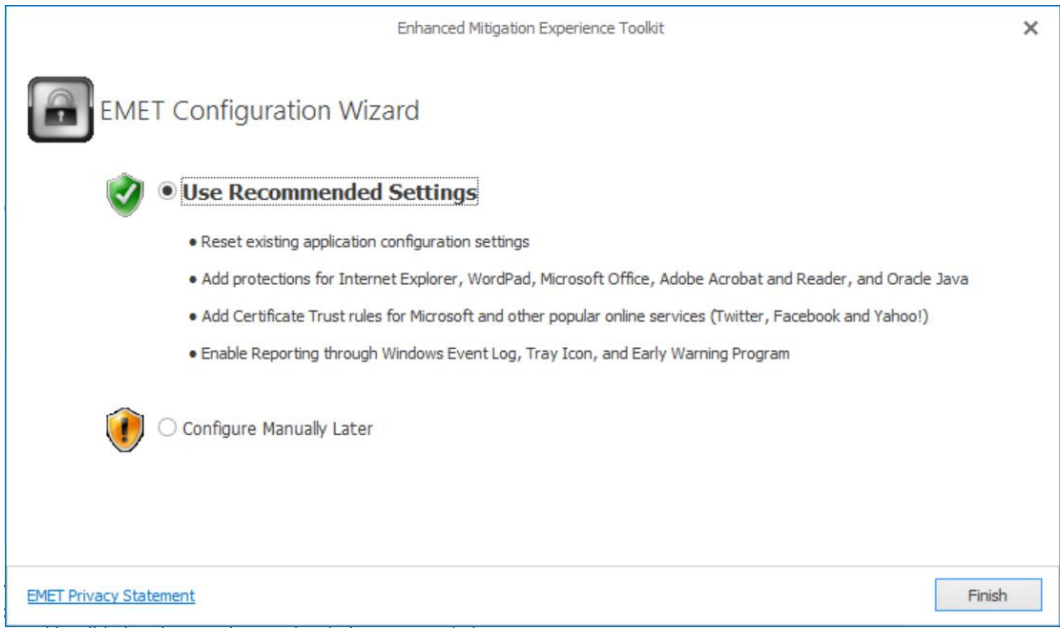

Client Type
Client
Client Activity
Computer
Yes
Active
Add Selected Items
Remove from Collection
Install Client
Reassign Site
Client Settings
Start
Approve
Block
Unblock
Clear Required PXE Deployments
Client Notification
Endpoint Protection
Edit Primary Users
Change Ownership
Change Category
Delete
Delete
Refresh
F5
Properties
Full Scan
Quick Scan
Download Definition

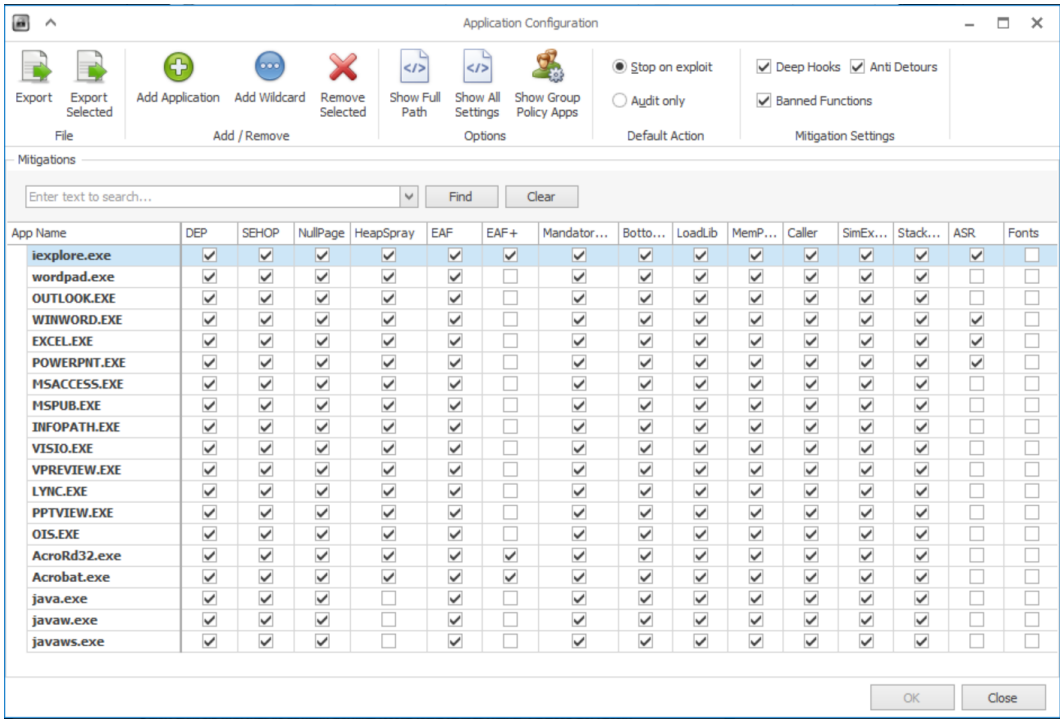

Home
Run Summarization
Saved Searches
Malware Detail
Allow this threat
Restore files quarantined by this threat
View infected clients
Endpoint Protection Status
Search
PUA:Win32/CandyOpen
Malware Detections
View infected clients

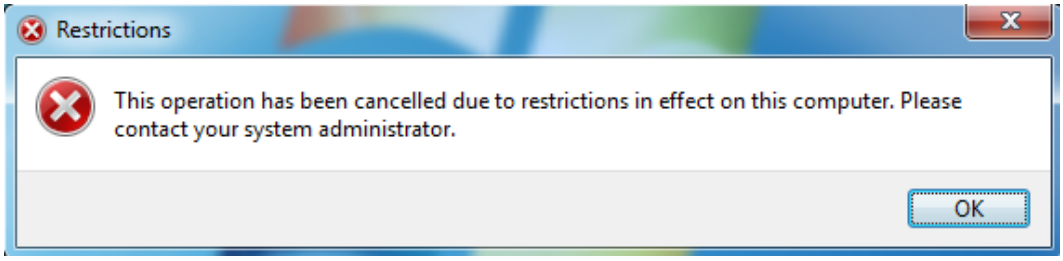

Microsoft
Malware Protection Center
Home
Security software
Threat encyclopedia
Our research
Help
Developers
PUA: Win32/CandyOpen
Also detected as: not-a-virus:AdWare.Win32.OpenCandy.aa (Kaspersky), Adware-OpenCandy (McAfee), a variant of Win32/OpenCandy.A potentially unsafe application (ESET), OpenCandy (Sophos), ADW_OPENCANDY (Trend Micro), Trojan.Win32.Generic.13F2CA41 (Rising AV), Adware.OpenCandy.I (BitDefender), PUA.OpenCandy (Symantec),
PUA:Win32/CandyOpen
Alert level: Low
First published: Mar 11, 2015
Latest published: Jun 29, 2016
Summary
What to do now
Technical information
Symptoms

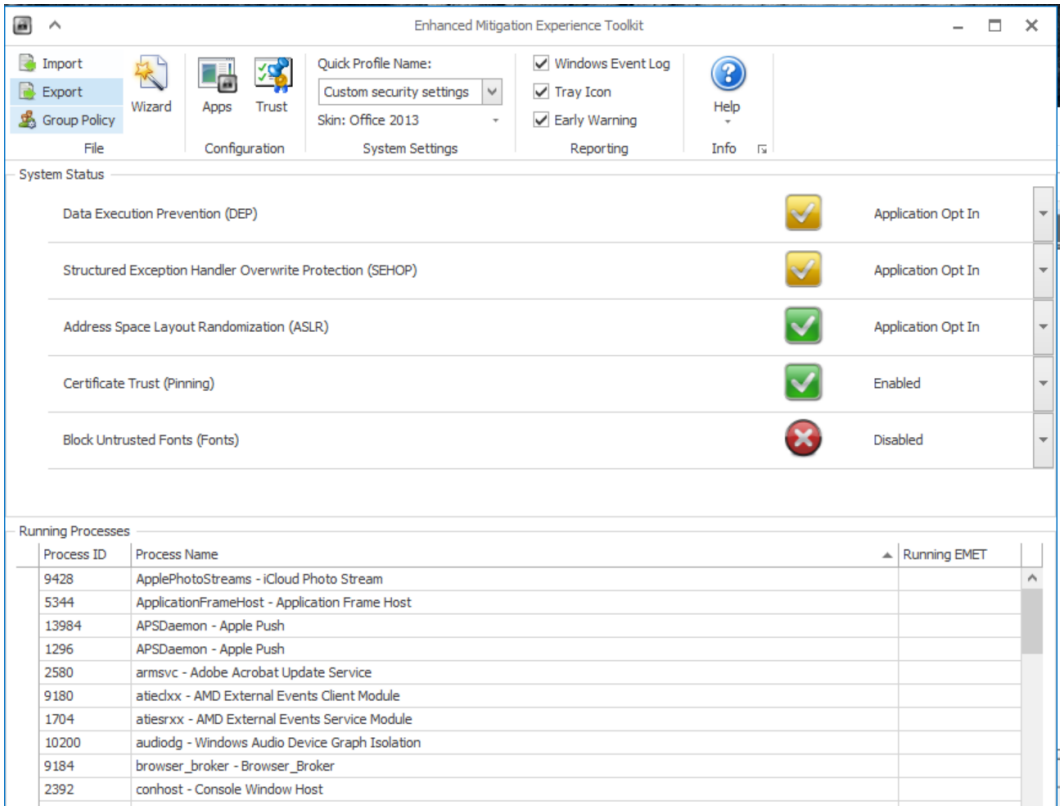

Microsoft
Account
Sign in
Malware Protection Center
Home
Security software
Threat encyclopedia
Our research
Help
Developers
Follow:
OVERSETT
Submit a sample
Track your submission
Sign in using your Microsoft account
1
2
3
Choose your user type
Enter your information
Attach a file and submit
You must complete the previous step before filling out this part.
You must complete the previous step before filling out this part.
Enterprise User
Home User

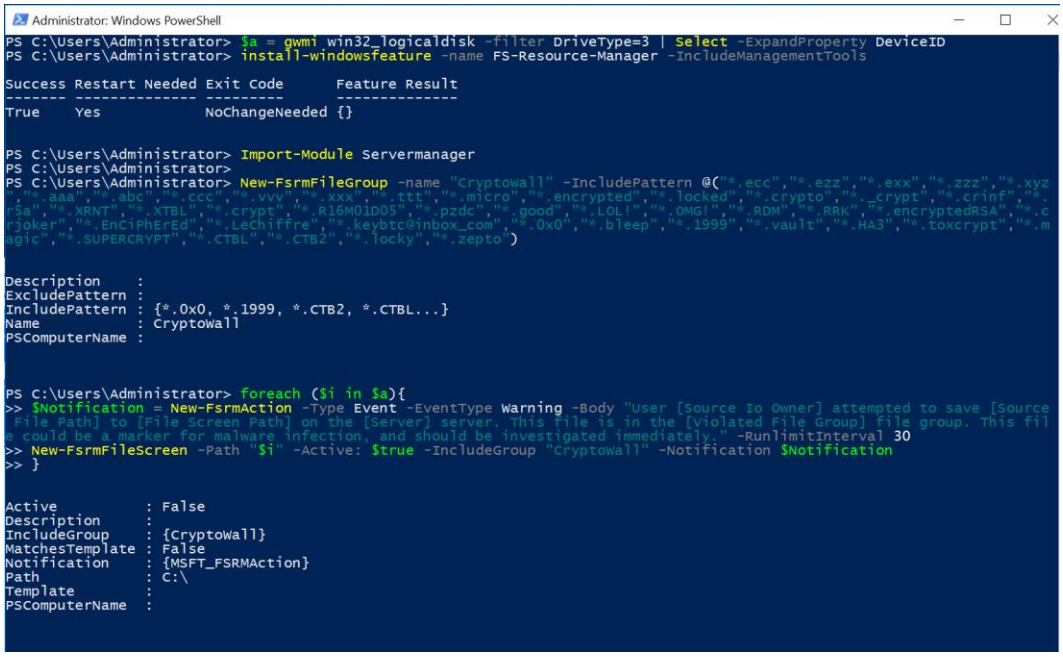

Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Name
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%
New Path Rule
General
Use rules to override the default security level.
Path:
%LocalAppData%*.exe
Browse...
Security level:
Disallowed
Description:
Block executables from AppData
OK
Cancel
Apply

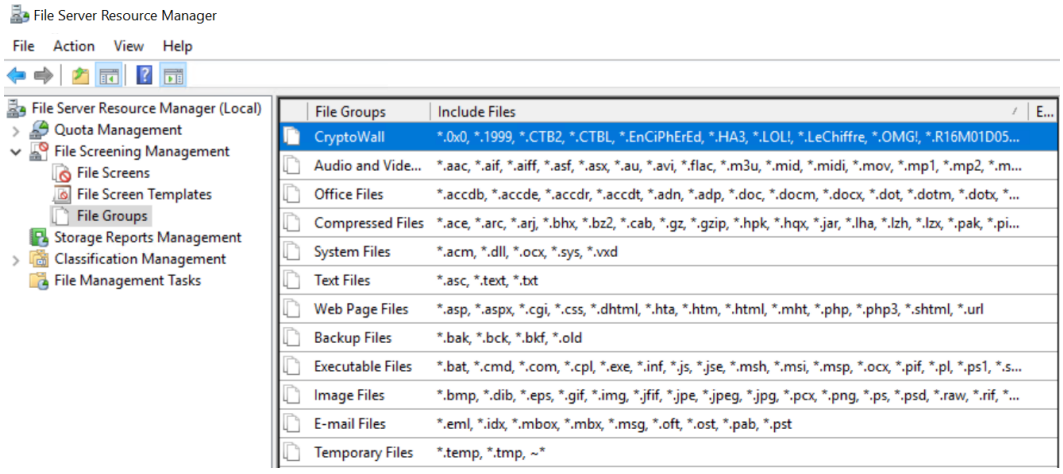

Enhanced Mitigation Experience Toolkit
EMET Configuration Wizard
Use Recommended Settings
• Reset existing application configuration settings
• Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java
• Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!)
• Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program
Configure Manually Later
EMET Privacy Statement
Finish

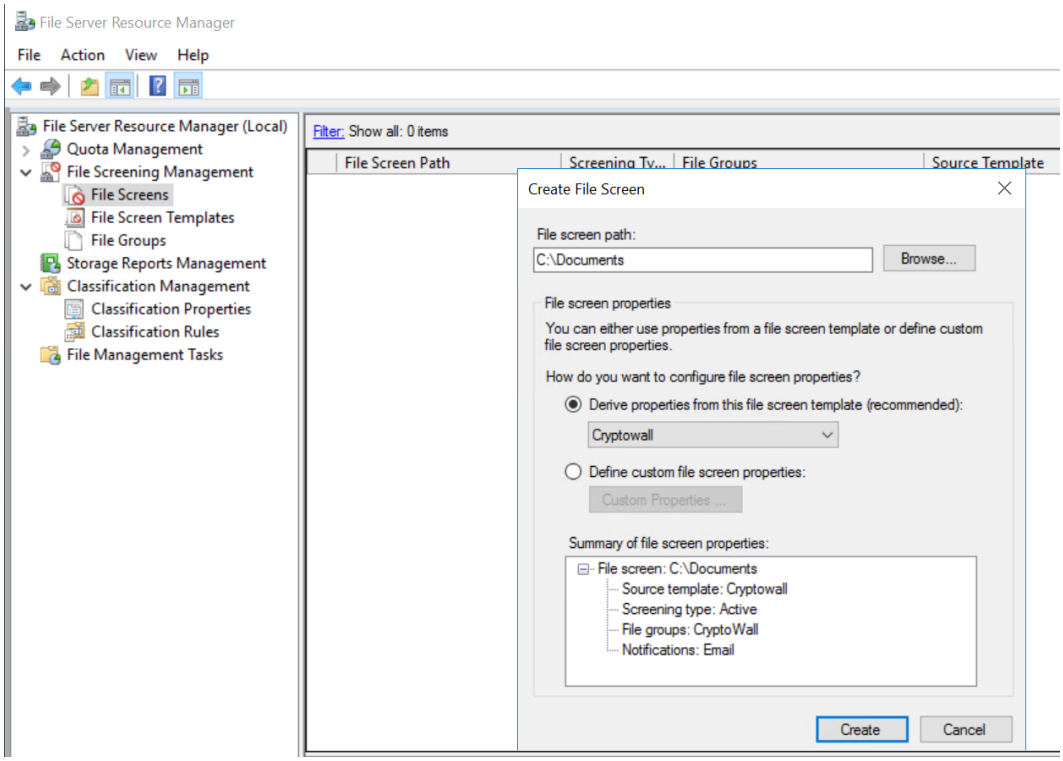

Application Configuration
Export
Export Selected
File
Add Application
Add Wildcard
Remove Selected
Add / Remove
Show Full Path
Show All Settings
Show Group Policy Apps
Options
Stop on exploit
Audit only
Default Action
Deep Hooks
Anti Detours
Banned Functions
Mitigation Settings
Mitigations
Enter text to search...
Find
Clear
App Name
DEP
SEHOP
NullPage
HeapSpray
EAF
EAF+
Mandator...
Botto...
LoadLib
MemP...
Caller
SimEx...
Stack...
ASR
Fonts
iexplore.exe
wordpad.exe
OUTLOOK.EXE
WINWORD.EXE
EXCEL.EXE
POWERPNT.EXE
MSACCESS.EXE
MSPUB.EXE
INFOPATH.EXE
VISIO.EXE
VPREVIEW.EXE
LYNC.EXE
PPTVIEW.EXE
OIS.EXE
AcroRd32.exe
Acrobat.exe
java.exe
javaw.exe
javaws.exe
OK
Close

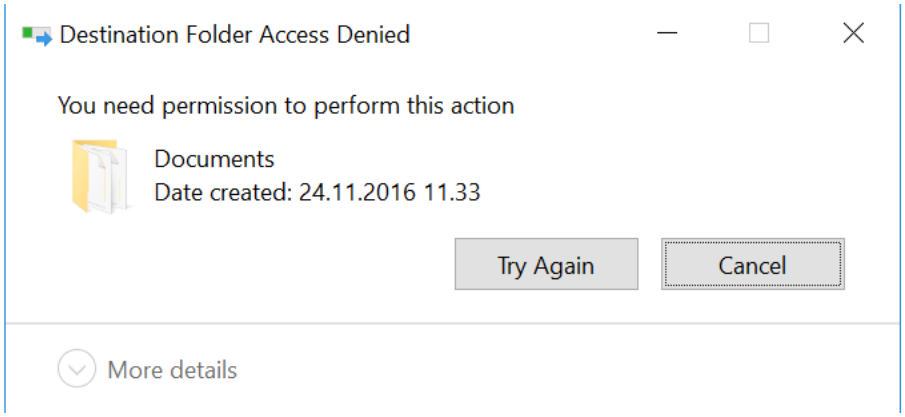

Restrictions
This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.
OK


Enhanced Mitigation Experience Toolkit
Import
Export
Group Policy
File
Wizard
Apps
Trust
Configuration
Quick Profile Name:
Custom security settings
Skin: Office 2013
System Settings
Windows Event Log
Tray Icon
Early Warning
Reporting
Help
Info
System Status
Data Execution Prevention (DEP)
Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)
Application Opt In
Address Space Layout Randomization (ASLR)
Application Opt In
Certificate Trust (Pinning)
Enabled
Block Untrusted Fonts (Fonts)
Disabled
Running Processes
Process ID
Process Name
Running EMET
9428 ApplePhotoStreams - iCloud Photo Stream
5344 ApplicationFrameHost - Application Frame Host
13984 APSDaemon - Apple Push
1296 APSDaemon - Apple Push
2580 armsvc - Adobe Acrobat Update Service
9180 atiedxx - AMD External Events Client Module
1704 atiesrxx - AMD External Events Service Module
10200 audiodg - Windows Audio Device Graph Isolation
9184 browser_broker - Browser_Broker
2392 conhost - Console Window Host


Administrator: Windows PowerShell
PS C:\Users\Administrator> $a = gwmi win32_logicaldisk -filter DriveType=3 | Select -ExpandProperty DeviceID
PS C:\Users\Administrator> install-windowsfeature -name FS-Resource-Manager -IncludeManagementTools
Success Restart Needed Exit Code Feature Result
True Yes NoChangeNeeded {}
PS C:\Users\Administrator> Import-Module Servermanager
PS C:\Users\Administrator>
PS C:\Users\Administrator> New-FsrmFileGroup -name "CryptoWall" -IncludePattern @("*.ecc","*.ezz","*.exx","*.zzz","*.xyz","*.aaa","*.abc","*.ccc","*.vvv","*.xxx","*.ttt","*.micro","*.encrypted","*.locked","*.crypto","*._crypt","*.crinf","*.r5a","*.XRNT","*.XTBL","*.crypt","*.R16M01D05","*.pzdc","*.good","*.LOL!","*.OMG!","*.RDM","*.RRK","*.encryptedRSA","*.crjoker","*.EnCiPhErEd","*.LeChiffre","*.keybtc@inbox_com","*.0x0","*.bleep","*.1999","*.vault","*.HA3","*.toxcrypt","*.magic","*.SUPERCRYPT","*.CTBL","*.CTB2","*.locky","*.zepto")
Description :
ExcludePattern :
IncludePattern : {*.0x0, *.1999, *.CTB2, *.CTBL...}
Name : CryptoWall
PSComputerName :
PS C:\Users\Administrator> foreach ($i in $a){
>> $Notification = New-FsrmAction -Type Event -EventType Warning -Body "User [Source Io Owner] attempted to save [Source File Path] to [File Screen Path] on the [Server] server. This file is in the [Violated File Group] file group. This file could be a marker for malware infection, and should be investigated immediately." -RunLimitInterval 30
>> New-FsrmFileScreen -Path "$i" -Active: $true -IncludeGroup "CryptoWall" -Notification $Notification
>> }
Active : False
Description :
IncludeGroup : {CryptoWall}
MatchesTemplate : False
Notification : {MSFT_FSRMAction}
Path : C:\
Template :
PSComputerName :


File Server Resource Manager
File Action View Help
File Server Resource Manager (Local)
Quota Management
File Screening Management
File Screens
File Screen Templates
File Groups
Storage Reports Management
Classification Management
File Management Tasks
File Groups
Include Files
E...
CryptoWall *.0x0, *.1999, *.CTB2, *.CTBL, *.EnCiPhErEd, *.HA3, *.LOL!, *.LeChiffre, *.OMG!, *.R16M01D05...
Audio and Vide... *.aac, *.aif, *.aiff, *.asf, *.asx, *.au, *.avi, *.flac, *.m3u, *.mid, *.midi, *.mov, *.mp1, *.mp2, *.m...
Office Files *.accdb, *.accde, *.accdr, *.accdt, *.adn, *.adp, *.doc, *.docm, *.docx, *.dot, *.dotm, *.dotx, *...
Compressed Files *.ace, *.arc, *.arj, *.bhx, *.bz2, *.cab, *.gz, *.gzip, *.hpk, *.hqx, *.jar, *.lha, *.lzh, *.lzx, *.pak, *.pi...
System Files *.acm, *.dll, *.ocx, *.sys, *.vxd
Text Files *.asc, *.text, *.txt
Web Page Files *.asp, *.aspx, *.cgi, *.css, *.dhtml, *.hta, *.htm, *.html, *.mht, *.php, *.php3, *.shtml, *.url
Backup Files *.bak, *.bck, *.bkf, *.old
Executable Files *.bat, *.cmd, *.com, *.cpl, *.exe, *.inf, *.js, *.jse, *.msh, *.msi, *.msp, *.ocx, *.pif, *.pl, *.ps1, *.s...
Image Files *.bmp, *.dib, *.eps, *.gif, *.img, *.jfif, *.jpe, *.jpeg, *.jpg, *.pcx, *.png, *.ps, *.psd, *.raw, *.rif, *...
E-mail Files *.eml, *.idx, *.mbox, *.mbx, *.msg, *.oft, *.ost, *.pab, *.pst
Temporary Files *.temp, *.tmp, ~*


File Server Resource Manager
File Action View Help
File Server Resource Manager (Local)
Quota Management
File Screening Management
File Screens
File Screen Templates
File Groups
Storage Reports Management
Classification Management
Classification Properties
Classification Rules
File Management Tasks
Filter: Show all: 0 items
File Screen Path
Screening Ty...
File Groups
Source Template
Create File Screen
File screen path:
C:\Documents
Browse...
File screen properties
You can either use properties from a file screen template or define custom file screen properties.
How do you want to configure file screen properties?
Derive properties from this file screen template (recommended):
Cryptowall
Define custom file screen properties:
Custom Properties ...
Summary of file screen properties:
File screen: C:\Documents
Source template: Cryptowall
Screening type: Active
File groups: CryptoWall
Notifications: Email
Create
Cancel


Destination Folder Access Denied
You need permission to perform this action
Documents
Date created: 24.11.2016 11.33
Try Again
Cancel
More details