McAfee
Together is power.

McAfee Endpoint Security 10.x

Table of Contents

McAfee Endpoint Security 10.x

Introduction

This document serves as a recommended approach to planning and executing an upgrade from McAfee legacy endpoint security products to McAfee® Endpoint Security 10.x. It can also serve as a general guide for planning new deployments of McAfee Endpoint Security 10.x.

This guide is derived from McAfee Professional Services, based on current methodology incorporated into field engagements for endpoint software upgrades from any or all of the following McAfee endpoint legacy products: McAfee® VirusScan® Enterprise 8.8, McAfee® Host Intrusion Prevention 8.0, and McAfee® SiteAdvisor® Enterprise 3.5.

Audience

The intended audience for this outline is administrators who are experienced with McAfee endpoint security products. It is not intended to be a comprehensive solution document, containing detailed supporting information. McAfee recommends that project participants refer to this document as supplemental to their own guidelines and requirements for software deployment within their environment.

Questions or requests for detailed information on steps outlined in this summary should be directed to McAfee subject matter experts within your organization. You can obtain additional information from the McAfee Knowledge Center and McAfee Communities. Contact McAfee Technical Support for further assistance.

Methodology

This software upgrade project follows a methodology that includes the following phases:

Plan: Lay the groundwork for a successful implementation by establishing the teams that will be involved in the upgrade, listing out business and technology goals, and capturing all the information required for a successful upgrade.

Design: Take all the information that was gathered in the **Plan** phase and use it to create a valid design for the new network infrastructure.

Assess: Evaluate your current production environment configuration to provide guidance and recommendations for the upgrade.

Test: Test the newly-designed policies and configuration to ensure that they work as designed.

Implement: After successfully validating your design, roll out the upgrade across all intended endpoints.

This document is structured to follow these five steps, to ensure you have a successful upgrade experience. We also offer a more detailed checklist in the Appendix, where you can view and check off detailed steps within each of the five steps.

Note: You can find the complete Upgrade Project Planning Checklist on page 35 in the Appendix.

Plan

Successful software deployment projects, including upgrades, start with a thorough planning exercise. Upgrade project plans can differ widely, depending on your environment and complexity.

To ensure overall project success, start by identifying key stakeholders who will provide input during the project. Project teams should be made up of members representing various interests across your organization.

Solution validation should be assessed initially in non-production testing environments, and again in production environments using small, manageable pilot groups that are representative of the production environment. This will help ensure that critical business operations are not impacted.

The Planning Checklist identifies a set of initial considerations to assist you with upgrade planning. The decisions you make should be documented for use during the subsequent Design, Assess, Test.

Planning Checklist

Plan	
Prepare for:	By taking these steps:
Project Success	▪ Identify business applications, administrators, and application owners ▪ Determine project and business objectives ▪ Review security requirements ▪ Identify endpoints for the initial pilot deployment ▪ Discuss end user communications ▪ Identify additional planning topics
Technology Implementation	▪ Discus product features ▪ Learn about solution relationships ▪ Review supported platforms ▪ Discuss supported McAfee Agent versions ▪ Consider integration with other McAfee solutions ▪ Review conflicts with existing products ▪ Determine the implementation process
Solution Validation	▪ Establish business application testing procedures ▪ Determine performance testing and baseline metrics ▪ Plan McAfee application validation testing
Ongoing Operations	▪ Identify current security management practices ▪ Review change control processes ▪ Develop back-out and recovery plans ▪ Discuss software updates ▪ Document McAfee ePolicy Orchestrator reporting requirements ▪ Review corporate security policies and supporting documentation

Project Success

Project success can and should be determined by quantifiable metrics, measuring benefits or impediments to the organization. It is critical that initial planning determines and outlines the business objectives and intended security requirements for the organization.

Identify business applications and their owners and administrators

Project planning discussions should include business critical application administrators and application owners to determine how your McAfee security solution might affect these key stakeholders.

The project manager should identify enterprise applications and their owners, and maintain a stakeholder register as necessary. This will help the application owners understand the potential impact of the migration and validate the functionality of their software after McAfee Endpoint Security is deployed.

Note: You can find an Application Owner's tracking sheet on page 38 in the Appendix.

Determine project and business objectives

Project participants should clearly identify the project and business objectives. A common business objective is to improve security by applying technical safeguards that enforce policies. Ensure that your company's information security strategy aligns with its strategic objectives.

You can get the conversation started by asking the project participants these questions:

1. What are our success criteria for the Endpoint Security Upgrade Project?
2. Have we identified any business risks concerning the project?
3. How can the results of this project make our organization more effective?

Review security requirements

Review specific use cases and core product capabilities as needed to ensure policy configurations will meet your organization's defined security requirements.

Review different policy configurations:

- For workstations and servers
- For server role/function
- For functional user groups
- For specific enterprise applications
- For LAN or remote VPN users

Identify endpoints for the initial pilot deployment

Identify a set of endpoints that will be part of the initial pilot deployment. It is recommended that you use a variety of endpoints that are representative of your overall environment.

- Determine the operating system platforms to be managed (such as Windows, Mac, Solaris, etc., as supported by the product).
- Determine groups for type of endpoints: workstations or servers, remote users or VPN, etc. The scope of your project may be limited to only workstations, only servers, or both.
- Verify that McAfee Agent deployment credentials for each platform are available.
- Record the list of hostnames on a pilot endpoint planning sheet.

Note: You can find a Pilot Endpoint Plan tracking sheet on page 37 in the Appendix.

Discuss end user communications

Users, administrators, and internal support personnel (including help desk staff) will need to understand the potential impact of the Endpoint Security modules. It's likely that this upgrade will introduce new security functionality into the organization.

You should determine if:

- The organization has identified end users for testing as part of the pilot deployment.
- End users have been notified about the project and the deployment timeline.
- End users have been informed about how to report any suspected problems.

Identify additional planning topics

Review and identify any additional planning topics that may be unique to the environment, such as the network architecture. These topics should focus on project success and related business outcomes. Implementation, solution validation, and operational topic discussions will happen later in the upgrade process.

Some additional topics to consider include:

- Change control process and lead time to establish change control windows
- Training requirements and kick-off for pilot user group
- Network traffic diagrams for critical applications
- Critical infrastructure servers (such as Active Directory, SQL and DHCP servers)
- List of vendor recommended exclusions

Note: Review technical article McAfee KB66909 in the McAfee Knowledge Center, "Consolidated list of Endpoint Security/VirusScan Enterprise exclusion articles."

Technology Implementation

Before starting the technology implementation, you'll want to confirm you understand the solution's capabilities, know which modules you'll be implementing, and be clear on the features of those modules.

Discuss product features

Review McAfee Endpoint Security features, capabilities, and operational functionality.

Determine which modules or core features you will be implementing for Endpoint Security: Threat Prevention, Adaptive Threat Protection, Firewall, and Web Control or McAfee Client Proxy.

- Review technical article McAfee KB86704 in the McAfee Knowledge Center, "FAQs for Endpoint Security."
- Review Endpoint Security product, installation, and migration guides, plus release notes for further information.

Key Resources

McAfee Endpoint Migration Assistant

McAfee® Endpoint Migration Assistant is a McAfee® ePolicy Orchestrator® (McAfee ePO™) console extension that walks you through the migration process. You can let Endpoint Migration Assistant migrate all your settings and assignments automatically, based on your current settings and new product defaults, or you can select and configure them manually.

Use Endpoint Migration Assistant to migrate product settings where a supported legacy version of a product module is installed.

Endpoint Migration Assistant ensures that the settings in your legacy policies are moved to the correct policies in Endpoint Security. In some cases, they are merged with other Endpoint Security settings, and in others, new default settings are applied to support updated technologies.

Refer to the Endpoint Security 10.x Migration Guide for information on:

- Installing the Endpoint Migration Assistant extension to the McAfee ePO console
- Migrating policies automatically
- Migrating policies manually
- Mapping migrated policies (old solution to Endpoint Security 10.x)

Endpoint Upgrade Assistant

McAfee Endpoint Upgrade Assistant is a McAfee ePO console extension extension that simplifies and automates the tasks required to upgrade the McAfee products on your managed endpoint. Endpoint Upgrade Assistant minimizes the number of upgrade tasks and ensures product interoperability.

Refer to McAfee KB88141 and McAfee Endpoint Upgrade Assistant Product Guide for guidance on installing Endpoint Upgrade Assistant extension to the McAfee ePO console and understanding:

- The Overview tab, to assess current endpoints in the environment
- The Prepare tab, to verify correct prerequisites have been met
- The Deploy & Track tab, to configure, deploy, and track the status of upgrade tasks

Learn about solution relationships

Review the relationship between the McAfee Endpoint Security 10.x modules and legacy endpoint security solutions.

Endpoint Security 10.x Module	Replaces	Description
Threat Prevention	McAfee® VirusScan® Enterprise 8.8, and McAfee® Host Intrusion Prevention IPS security protections	Detects threats in real-time, leveraging McAfee® Global Threat Intelligence (GTI) and AMCore security content files. Layered protection includes anti-malware scanning, script scanning, Access Protection and Exploit Prevention.
Adaptive Threat Protection	McAfee® Threat Intelligence module for VSE	Optional Endpoint Security module that analyzes content from your enterprise and decides what to do based on file reputation, rules, and reputation thresholds. Includes RealProtect and Dynamic Application Containment.
Firewall	McAfee® Host Intrusion Prevention Firewall	Integrated, stateful firewall that dynamically inspects traffic on the network, blocking malicious or undesired traffic. Policy configuration features include: trusted networks, trusted/untrusted executables, Location Aware Groups, connection isolation, and timed firewall groups for end-user VPN connections.
Web Control	McAfee® SiteAdvisor	Updated Web Control browser toolbars improve user experience. Integration of Web Control with Threat Prevention using McAfee® Global Threat Intelligence ensures users have safe, reputable, web browsing, and secure browser file downloads. Web Control notifies users of threats while they search or browse websites.
McAfee Client Proxy		Optional component that integrates with McAfee® Web Gateway

For more information on McAfee Endpoint Security components, refer to the product guide.

Discuss supported platforms

Review your existing infrastructure and identify endpoints you're considering for the project.

- Review technical article McAfee KB82761 in the McAfee Knowledge Center, "Supported platforms, environments, and operating systems for Endpoint Security." This article is updated frequently as new operating systems, browsers, and virtualization technologies are released.
- Identify which operating systems, virtualization technologies, and internet browsers are in use within your environment.

Discuss supported McAfee Agent versions

Supported McAfee Agents include McAfee 5.0.5 and later. It's recommended that you deploy the most recent Update (formerly, patch) version, so determine if your version McAfee Agent will need to be upgraded. You can find information on McAfee Agent versions in technical article KB82105 in the McAfee Knowledge Center.

Consider integration with other McAfee solutions

McAfee Endpoint Security integrates with McAfee® Threat Intelligence Exchange (TIE), Data Exchange Layer (DXL), and McAfee® Active Response (MAR) to provide a comprehensive security solution.

- When installed and configured, TIE reputations are leveraged by all McAfee Endpoint Security modules to assist in verifying security threats throughout your entire infrastructure.
- TIE reputations are also leveraged directly by McAfee Endpoint Security Adaptive Threat Protection/Dynamic Application Containment to determine whether containment rules should be triggered.

If McAfee Threat Intelligence Exchange is already deployed for legacy products, the upgraded endpoints will be upgraded when the McAfee Endpoint Security 10.x Adaptive Threat Protection 10.x module is installed.

Review conflicts with existing products

Technical article KB85522 in the McAfee Knowledge Center provides a detailed list of third-party security products that can be removed by the McAfee Endpoint Security installer, when McAfee Endpoint Security is installed. You'll also want to identify other security products within your environment and determine if there are any known uninstall or interoperability issues.

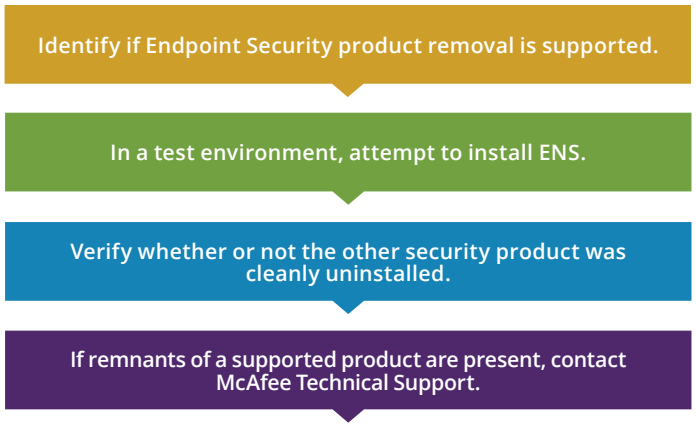


Figure1. Workflow to Identify and Remediate Other Security Products

Note: The Endpoint Security 10.x Installer may not able to successfully remove all security products. Refer back to technical article KB85522.

You'll need to discuss any known operating system incompatibilities and review technical article KB82450 in the McAfee Knowledge Center, "Endpoint Security 10.x Known Issues."

Determine the implementation process

Components within the infrastructure will change during the McAfee Endpoint Security implementation. Review processes to successfully recover or revert components to their prior condition, should any implementation failures occur.

Determine how software will be deployed to managed clients:

- Deployment through McAfee ePO console
- Deployment through a third-party application (such as Microsoft SCCM, KACE, Altiris, etc.)
- Use of Endpoint Security Package Designer (if desired). For information about installing and using Package Designer, see technical article KB86438 in the McAfee Knowledge Center.

McAfee ePolicy Orchestrator repository considerations

Review the McAfee ePolicy Orchestrator Distributed Repositories and methods used to populate repositories.

- Navigate to Menu > Distrubuted Repositories
- Verify that your listed distributed repositories are listed
- Verify that your respositories are providing access with the "Repositories and Percentage Utilization" report in Quries & Reports

Peer-to-Peer (P2P) updating considerations

Review the Peer-to-Peer updating ability of the McAfee Agent. This Peer-to-Peer setting is managed in the McAfee Agent General policy. In nearly all circumstances, Peer-to-Peer updating reduces the load on the distributed rePolicy Orchestrator sitories, and enables software and content to be distributed more quickly.

Endpoints that are **not** good candidates for P2P are:

- Laptops that spend the majority of their time connected via VPN
- Fixed-function machines that have extremely limited spare processing cycles

Endpoints that **may** be good candidates for P2P are:

- Physical or virtual machines in th e datacenter. These machines typically have an extremely high bandwidth connection to a McAfee ePolicy Orchestrator repository, so bandwidth costs are very low.
- Physical or virtual machines at a remote site

Follow these steps for Peer-to-Peer updating:

1. Review performance metrics, both before and after P2P is enabled, to establish a baseline and the actual load of the P2P process. Work with your network admin and monitor traffic via Wireshark or a similar Trace program to complete this task.
2. Enable P2P on a subset of workstations. Document how many nodes are in these specific broadcast domains.
3. Review performance metrics.
4. Continue deploying P2P to additional sites and review their performance.

Solution Validation

Prior to installation, determine the application testing practices for your organization. It's imperative that you understand any existing business application testing that needs to be performed, which may require additional support (such as Exchange, SharePoint, database applications, VPN, etc.)

Establish business application testing procedures

Best Practices

McAfee recommends that:

1. You perform the initial installation or upgrade in a lab, development, or other non-production environment that is representative of your production environment.
2. IT application administrators and business application users perform any existing application tests prior to the full production rollout.
3. During the technical implementation, you use a phased deployment approach. This typically begins with a series of pilot deployments that bring IT and business units together.
4. Your environment's Service Desk personnel should be involved as early as possible to gain valuable experience needed to provide support for your organization.

If your organization hasn't defined functional application testing practices, it's recommended that you create a basic set of practices, based on current industry standards.

A basic functional application testing process should include:

- Organization-specific testing procedures (what testing is done for other applications being rolled out to users?)
- Basic tests that need to be performed (such as Windows updates, enterprise application use, etc.).

- A testing methodology or testing scripts to produce repeatable tests
- Preparation of your test environment
- Installation of the appropriate software
- Testing and analysis of the results
- Resolution of application issues, should any arise

Determine performance testing and baseline metrics

Prior to installing McAfee Endpoint Security, determine whether application performance testing baseline metrics exist for legacy security products within your organization. You must be sure you understand existing performance issues, which should be baselined prior to installing McAfee Endpoint Security. You also must identify the performance testing benchmarks to be measured before and after upgrading to Endpoint Security.

Before and after installing McAfee Endpoint Security consider measuring:

- Average time for endpoint startup
- Average time for user logons
- Average CPU utilization
- Business application-specific performance metrics

The tests and benchmark indicators need to be consistent for both testing environments.

McAfee® Endpoint Security Scan Avoidance is the most efficient way to ensure optimal performance on the endpoint. This feature, which is only available in McAfee Endpoint Security, leverages the AMCore Trust Model to help recognize when a scan is not necessary. This mechanism provides the greatest performance increase because it not only indicates whether a scan is necessary early in the scan workflow, but also has longer term relevance because cached Trusted + Clean results survive an AMCore Content update, whereas Clean results alone will not.

In the new AMCore performance model, the strategy is based around the notion of an "actor." An actor is defined as a running process and its state of trust can be one of three values:

- Suspicious
- Normal
- Trusted

An actor is trusted when it has come from a trusted origin or is directly related to a trusted package.

Note: For more information, please review the white paper, "Understanding Next-Generation Performance Models."

McAfee Endpoint Security includes a policy setting that allows the administrator to trust certain third-party certificates. These certificates are from third-party software that client endpoints have identified and reported back to the McAfee ePolicy Orchestrator software. Once trusted, file access by trusted processes and of trusted files will benefit from the performance optimization provided through Scan Avoidance.

McAfee recommends that you review your legacy policies to decide whether they are relevant to the new McAfee Endpoint Security scan optimization architecture. By default, McAfee Endpoint Security includes an optimized "Let McAfee Decide" option for On-Access Scanning. For more information, see technical article KB88205 in the McAfee Knowledge Center, "How to improve performance with Endpoint Security 10.x."

Plan McAfee application validation testing

Discuss and review the high-level activities that will be performed for your McAfee Endpoint Security deployment and validation testing for your McAfee application. These activities are designed to validate that the solution is working as designed, and **are not** intended to fulfill or replace existing requirements for the validation of your critical business applications.

Endpoint Security validation tests

Validation tests ensure that your McAfee Endpoint Security product is capable of blocking/monitoring activity and producing logs/events that are viewable on your client endpoint and from the McAfee ePolicy Orchestrator console. Validation tests should be created for all McAfee Endpoint Security modules and features you plan to deploy.

Tests may include, but are not limited to:

- On Access Scanning—EICAR Test
- Viewing the Quarantine Folder
- Exploit Prevention—Hidden PowerShell Detected
- Dynamic Application Containment
- Firewall policy block/allow
- Web Control

Note: You can view examples of these tests on page 39 and examples of the McAfee ePolicy Orchestrator reporting formats on page 38 in the Appendix.

Ongoing Operations

To ensure your ongoing operations will function smoothly, you need to first review your existing processes and procedures for performing the migration, as well as for performing future updates.

Identify current security management practices

McAfee recommends that you identify existing processes for:

- Event or change management
- Incident response—What are your procedures for responding to incidents?
- Operations—What portion of your business will be responsible for the day-to-day operations of the McAfee ePolicy Orchestrator application and/or any of the applications that the McAfee ePolicy Orchestrator solution will be managing? This will tie into the users and permissions discussion.
- Maintenance—What are your maintenance windows and how will you coordinate maintenance?
- Governance and compliance—Which groups within your organization are currently addressing compliance within your environment?

Review change control processes

Review and verify the applicable change control procedures. Discuss options and impacts to address existing change control processes and procedures within your environment.

It is assumed that all changes to non-production environments do not need a change control. It is assumed that all changes to the production environment will need a change control.

A list of changes that will need to take place include:

- Installation of McAfee Endpoint Security-related extensions on the McAfee ePolicy Orchestrator server.
- Installation of McAfee Endpoint Security-related packages on the McAfee ePolicy Orchestrator server.
- Creation/modification of policies on the McAfee ePolicy Orchestrator server.
- Deployment of software to nodes in the production environment.

Develop back-out and recovery plans

Be sure to develop a back-out and recovery plan in the event of unforeseen issues or installation failures. This is particularly important when installing on shared file, application, or database servers.

In addition, verify:

- Access to the original installation software for operating system, database, and/or other applications
- VM snapshots or backups of any existing application server and SQL databases

Discuss software updates

You can use the McAfee Support Notification Service (SNS) to provide alerts regarding Hotfixes, Updates, and other notifications relating to Endpoint Security 10.x. The Support Notification Service (SNS) delivers valuable product news, alerts, and best practices to help you increase the functionality and protection capabilities of your McAfee products.

Note: It is recommended that you review the release notes for the current patch for McAfee Endpoint Security 10.x and for the current version of McAfee Agent.

Discuss and review McAfee Endpoint Security content updates to understand the importance of testing updates prior to a full production deployment. Refer to the "How content files work" section of the Endpoint Security 10.x Product Guide to review the types of content McAfee Endpoint Security uses.

AMCore content package

McAfee Labs releases AMCore content packages daily by 7:00 p.m. (GMT/UTC). To receive alerts regarding delays or important notifications, subscribe to the Support Notification Service (SNS). See technical article KB67828 in the McAfee Knowledge Center.

The AMCore content package includes:

AMCore - Engine and content

- Contains updates to the Threat Prevention scan engine and signatures based on results of ongoing threat research

Adaptive Threat Protection- Scanner and rules

- Contains rules to dynamically compute the reputation of files and processes on the endpoints. McAfee releases new Adaptive Threat Protection content files every two months.

Real Protect - Engine and content

- Contains updates to the Real Protect scan engine and signatures based on results of ongoing threat research. Real Protect is a component of the optional Adaptive Threat Protection module.

Exploit Prevention content package

McAfee Labs releases Endpoint Security Exploit Prevention signature content on the second Tuesday of every month. Monthly Exploit Prevention content release notes can be found here.

The Exploit Prevention content package includes:

- Memory protection signatures - Generic Buffer Overflow Protection (GBOP), caller validation, Generic Privilege Escalation Prevention (GPEP), and Targeted API Monitoring
- Application Protection List - Processes that are protected by Exploit Prevention. Exploit Prevention content is similar to the McAfee Host IPS content files. Review corporate security policies and supporting documentation

Document reporting requirements

During this step of the project, you should clearly identify and document the reporting requirements of your business units. Each of your business units should fully document their own reporting requirements. These requirements should identify:

- Purpose of the report
- Permissions to run reports
- Access to related data
- Scheduling requirements (especially what frequency is required for individual reports)
- Report distribution requirements

You'll need to determine if there is an established process for requesting reports. This process should include a review of the requirement, approval, creation of the reports, and acceptance from the requesting party that the reports will satisfy the requirements. You'll want to ensure that the solution is reporting on:

- The status of the security solution within the environment, for example identifying the versions of McAfee Security software that are installed, identifying the latest policy being enforced, etc.
- Compliance of the enterprise with your security standards
- Reporting on risk and risk mitigation within the enterprise
- Incidents, for example, violations of rules, malware, etc.
- Incident response, for example providing information on how the applications reacted to incidents (quarantined, blocked, would have been prevented, etc.)

Corporate security policies and supporting documentation	
Policies, standards, guidelines, and related practices and procedures	These documents communicate management's direction for reducing risk and establishing the control framework. ▪ Acceptable use of assets ▪ Access controls ▪ Malware prevention, detection, and correction ▪ Information and endpoint backup ▪ Security logging and monitoring ▪ Change control ▪ Management of technical vulnerabilities - Endpoint Update management - Update testing procedures ▪ Secure endpoint engineering principles and requirements - Endpoint hardening and configuration standards - Firewall policy documentation ▪ Endpoint acceptance testing ▪ Information security continuity ▪ Data retention and disposal policies
As-built documentation	For the security solutions and platforms related to the implementation: ▪ Endpoint hardening and configuration standards ▪ Network segmentation and configuration standards ▪ Database server hardening and configuration standards ▪ Network diagrams ▪ End-user computing configuration standards, for example, gold disk images

Figure2. Review corporate security policies and supporting documentation

Plan | Design | Assess | Test | Implement

Design

Project participants should discuss the current network and endpoints architecture to facilitate design and implementation of your McAfee security solution.

Design	
Prepare for:	**By taking these steps:**
Solution Integration	- Learn about the McAfee solution architecture - Review the endpoint architecture - Identify required network infrastructure services and McAfee network services - Understand the role of registered servers
Design Principles	- Determine users and groups - Establish roles and responsibilities
Design Validation	- Review known issues - Verify that the installation environment meets specifications - Confirm pilot endpoints configuration - Verify accounts and permissions

Figure3. Design Checklist

Solution Integration

During this phase of the migration process, the main goals are to ensure that all project participants understand the McAfee Endpoint Security Security platform, how it connects to the network infrastructure, and confirm the high-level design of the newly configured network.

Learn about the McAfee solution architecture

Project participants and stakeholders should possess a high-level understanding of the McAfee Endpoint Security Security Platform. Stakeholders should discuss how the total solution addresses their security use cases.

How McAfee Endpoint Threat Protection defenses work together

Use case

Download of a malicious file from the web

A file hash is sent from Web Control to Threat Preventation, triggering an ODS

Malicious files are detected and blocked before they have full access to the system

Forensics data is captured (Source URL, file hash, etc.)

Event data is shared with other modules and McAfee ePO and is visible in the client UI

Project participants can download the Endpoint Threat Protection data sheet located on https://www.mcafee.com/us/resources/data-sheets/ds-endpoint-threat-protection.pdf. This will provide a high-level review of McAfee Endpoint Security and its related components.

Review the endpoint architecture

SecurityManagement			
McAfee ePO Agent Protocol		**Client UI**	
Threat Preventation	**Firewall**	**Web Control**	**Adaptive Threat Protectection**
			
▪ On access scanner ▪ Access protection ▪ ScripScan ▪ Exploit protection ▪ On-demand scanner ▪ Exploit preventation ▪ Right-click scan	▪ Stateful firewall ▪ Adaptive mode ▪ DNS blocking	▪ Site ratings ▪ Site categorization ▪ Browser plugin	▪ File reputation ▪ TIE/DXL intergration ▪ Real protect ▪ Dynamic application containment

Figure4. McAfee Endpoint Security Platform

Identify required network infrastructure services and McAfee network services

Besides standard network infrastructure services, its important to understand the McAfee network services. McAfee Endpoint Security leverages the existing ports that have been configured in your McAfee ePolicy Orchestrator environment.

Default Port	Protocol	Traffic Direction
80	TCP	Outbound connection to the McAfee ePolicy Orchestrator server/Agent Handler.
443	TCP	Outbound connection to the McAfee ePolicy Orchestrator server/Agent Handler.
8081	TCP	Inbound connection from the McAfee ePolicy Orchestrator server/Agent Handler. If the agent is a SuperAgent repository, inbound connection from other McAfee Agents.
8082	UDP	Inbound connection to agents. Inbound/outbound connection from/to SuperAgents.
8083	UDP	Relay server discovery for McAfee Agent.

Figure5. McAfee Agent port reference

Understand the role of registered servers

Registered servers allow for the integration of McAfee ePolicy Orchestrator software with other, external servers. For example, register your LDAP server to connect with the Active Directory server. Registering a server can increase the effectiveness of McAfee Endpoint Security.

Each type of registered server supports or supplements the functionality of McAfee Endpoint Security with other McAfee solutions. For example, if you have TIE/DXL deployed in your environment and McAfee Endpoint Security Adaptive Threat Protection is enabled, you can leverage reputation information from TIE to block applications from executing. McAfee ePolicy Orchestrator users are then able to view TIE server information in McAfee ePolicy Orchestrator reports and dashboards.

Design Principles

In this step, you'll need to determine who your users are, who your admins are, and what responsibilities you'll be assigning for administering McAfee Endpoint Security.

Determine users and groups

Users

There are two types of users: Global Administrators and users with limited permissions. You'll need to:

- Decide who Global Admins will be, mapping the Global Admins to AD accounts.
- Identify users requiring access to McAfee ePolicy Orchestrator and other applications.

Groups

To facilitate management of the solution, McAfee recommends that you develop a group structure linked to an existing Active Directory or LDAP directory.

For installation and ongoing operation of the solution, consider creating these Active Directory groups (Global/Universal Groups):

Group	McAfee ePO Permissions
ENS_ Administrators	Users requiring full access to McAfee Endpoint Security policies, queries, and dashboards.
ENS_Reviewers	Users requiring review permissions to McAfee Endpoint Security policies, queries, and dashboards.

Establish roles and responsibilities

With your project participants, discuss roles and responsibilities, segregation of duties, and requirements for access to McAfee ePolicy Orchestrator and other applications. You'll need to identify which types of users require access to the endpoint. Then, spend time understanding their unique roles and responsibilities. This information can then be used to describe and create permission sets that allow users to perform their jobs successfully.

Users should be assigned privileges based upon their operational role for the solution. Operational Roles might include:

- McAfee ePolicy Orchestrator Global Administration
- Product Administration
- Global Reviewer
- Product-level Reviewer

In the production McAfee ePolicy Orchestrator environment, consider providing global administrators with two accounts:

- A Global Administrator account
- A "day-to-day" operations type of account that has more restrictive permissions than the Global Admin account

Typical user permissions include read-acces to:

- Events in McAfee ePolicy Orchestrator
- Policies in McAfee ePolicy Orchestrator
- System tree objects in McAfee ePolicy Orchestrator

Typical "administrative" permissions (only to be used in a change control window) include full access to:

- Policies
- System tree

Design Validation

Validating the design is important in order to confirm that everything is ready for the implementation.

Note: You can view a full list of system requirements on page 43 in the Appendix.

Review known issues

You can find the list of known product incompatibilities in the McAfee Service Portal; be sure to review this list during the course of your project. Please reference technical article KB82450 in the McAfee Knowledge Center, "Endpoint Security 10.x Known Issues."

Verify that the installation environment meets specifications

Compare the endpoints in your environments against technical article KB82761 in the McAfee Knowledge Center, "Supported platforms, environments, and operating systems for Endpoint Security."

Note: This KB article is updated frequently, as new operating systems are released. Your environment will likely have a mix of operating system versions and hardware configurations. Pay special attention to operating systems that are not supported by McAfee Endpoint Security.

Confirm pilot endpoints configuration

Verify that your pilot endpoints have supported versions of the McAfee Agent software installed. Also, ensure that pilot endpoints meet the system requirements as listed in technical article KB82761 in the McAfee Knowledge Center, "Supported platforms, environments, and operating systems for Endpoint Security."

You'll also want to verify that prerequisite software is installed by using McAfee Endpoint Upgrade Assistant, and reviewing the product release notes.

The McAfee Endpoint Upgrade Assistant can provide you with compatibility information that is specific to your McAfee ePolicy Orchestrator environment. McAfee Endpoint Upgrade Assistant examines the software packages in your repository and compares that info against the list of compatible software. The "Overview" and "Prepare" tabs in McAfee Endpoint Upgrade Assistant provide a visual representation of minimum software versions supported by McAfee Endpoint Security.

Verify accounts and permissions

Verify that all your account(s) have the correct permissions. The same account may be used to upgrade software and deploy solution components on endpoints, as needed. You'll want to ensure that you have permissions set for:

- McAfee ePolicy Orchestrator administrative account
- McAfee Agent deployment
- McAfee Endpoint Security deployment (as needed to perform upgrades)

Assess

During this phase, your project participants will perform an assessment of your current production environment configuration to provide guidance and recommendations for the upgrade.

Activities performed during the assessment will result in changes to your production environment; one specific change is checking in the extension for McAfee Endpoint Upgrade Assistant. Prior to checking in the McAfee Endpoint Upgrade Assistant extension, McAfee recommends that you follow your organization's practices for submitting change requests, performing endpoint backups, and developing a back-out plan.

Assess	
Prepare for...	**By performing these activities...**
Technical review	▪ Run Endpoint Upgrade Assistant ▪ Analyze Endpoint Upgrade Assistant results ▪ Review dashboards and queries ▪ Perform McAfee VirusScan Enterprise policy review ▪ Conduct McAfee Host Intrusion policy review ▪ McAfee Site Advisor Enterprise policy review ▪ Export production policies and tasks

Figure6. Assessment Checklist

Technical Review

The technical review is where you'll assess your current production environment by performing a series of activities around the upgrade.

Run the McAfee Endpoint Upgrade Assistant

In this phase, you will be running McAfee Endpoint Upgrade Assistant so that you can get an idea of what machines in your production environment are currently ready for migration to McAfee Endpoint Security 10.x.

Refer to technical article KB88141 on the McAfee Knowledge Center for an explanation of the tool, a video tutorial, and links to product documentation.

Analyze McAfee Endpoint Upgrade Assistant results

Carefully analyze the results from McAfee Endpoint Upgrade Assistant and prepare to implement the recommended upgrade scenarios (after you've completed testing—See Test phase.) The objective of this initial analysis is to understand the upgrade readiness of your environment.

Review dashboards and queries

Next, you'll want to review the McAfee ePolicy Orchestrator dashboards and queries for:

- Mcafee VirusScan
- Mcafee Host IPS
- Mcafee Site Advisor

These dashboards and queries will likely need to be ported into their McAfee Endpoint Security 10.x equivalent. Identify if automated queries and McAfee ePolicy Orchestrator reports are configured for endpoint security products. Then, document this information and create an action plan to ensure operational effectiveness. This review gives you an opportunity to introduce additional monitoring insights into your existing operational processes. Refer to the McAfee ePolicy Orchestrator product guide on the documentation portal for additional information on monitoring and reporting configuration.

Note: You can find an example future state dashboard on page 38 in the Appendix.

Perform McAfee VirusScan Enterprise policy review

The McAfee Endpoint Migration Assistant can be used to migrate McAfee VirusScan policies and tasks to McAfee Endpoint Security 10.x. In order to streamline the migration activities, consider consolidating the number of On-Access Scanning (OAS) VirusScan policies that are present in your environment. To do this, first identify the business purpose for each McAfee VirusScan policy, paying special attention to On-Access Scanning exclusions within the policies.

Identify a policy consolidation workflow that works for your environment. You can use the example workflow shown in this figure as a starting point.

Figure7. OAS – Example Policy Consolidation Workflow

Track policy consolidation decisions , so that you will have a record of why you created new McAfee Endpoint Security OAS policies.

Note: You can find McAfee VirusScan policy and task tracking sheets on page 37 in the Appendix.

Conduct McAfee Host Intrusion Prevention policy review

The McAfee Endpoint Migration Assistant can be used to migrate McAfee Host IPS policies and tasks to McAfee Endpoint Security 10.x.

Project participants and stakeholders should review and consolidate Host IPS policies, exclusions, and firewall rules

Note: McAfee Host Intrusion Prevention, IPS Protection, and Rules policies may contain exceptions and/or changes to the severity of a specific signature. Capture policy settings that deviate from the McAfee default and attempt to consolidate the IPS rules policies.

Exception Rules

Exception Rules from the IPS Rules policy migrate to the Access Protection and Exploit Prevention policies as executables under Exclusions.

Refer to the McAfee Endpoint Security Migration Guide for further information on Exception Rules.

Exception Rules with signatures

IPS Exceptions can include custom signatures. The executables and parameters from exceptions are appended to the McAfee Endpoint Security Access Protection Rule created during signature migration. If all McAfee-defined signatures are added to a subrule exception, the exception migrates as a global exclusion in the Access Protection and Exploit Prevention policies.

You can reduce the complexity of firewall rules by leveraging McAfee Host IPS Catalog, which contains reusable items that you can import into firewall policies.

Consider maintaining a baseline firewall policy that satisfies most of the security requirements of your organization. You can then create additional catalog and policy items for specific types of users and groups.

Review any configured McAfee Host IPS product-specific tasks. Task-consolidation decisions need to take into consideration whether new or additional McAfee Endpoint Security tasks might need to be created to mirror specific task goals.

Note: You can find McAfee HIPS IPS Rules Policies and McAfee Host IPS Firewall Rules Policies tracking sheets on page 37 in the Appendix.

Run McAfee SiteAdvisor Enterprise policy review

McAfee SiteAdvisor Enterprise and Web Control can take action on over 100 categories of web content. You'll need to ensure that your environment has an acceptable internet usage policy and block web categories that violate your usage policy. If numerous McAfee SiteAdvisor Enterprise policies contain similar or identical settings (for example, blocking the same web categories), use the Policy Comparison tool or an Excel spreadsheet to find identical settings that can be consolidated. Identify which web browsers are approved for use in your environment. Both McAfee SiteAdvisor Enterprise and McAfee Endpoint Security Web Control can be configured to block unsupported internet browsers.

Determine if you have an established workflow in place for unblocking websites that are incorrectly categorized. A website's categorization and reputation are linked to

McAfee's TrustedSource.org. Next, review any configured McAfee SiteAdvisor Enterprise product-specific tasks. Consider whether you will need to create McAfee Endpoint Security product tasks to mirror specific task goals.

Export production policies and tasks

Export the recently reviewed and consolidated production policies for McAfee VirusScan, McAfee Host IPS, and McAfee SiteAdvisor Enterprise. These policies will be referenced in the Test phase of this project, when McAfee Endpoint Migration Assistant is used for policy and task conversion to McAfee Endpoint Security 10.x.

Test

During this phase, project participants will install, configure, upgrade, and validate the McAfee solution in a non-production environment.

Test	
Prepare for: By taking these steps:	
Recovery	- Back up the McAfee ePolicy Orchestrator application server and database
Installation	- Check in required packages - Install required management extensions - Validate distributed repository replication - Run Endpoint Upgrade Assistant and analyze results - Import production policies and tasks
Configuration	- Configure users and permission sets - Perform initial validation testing - Run Endpoint Migration Assistant and analyze the results - Configure the baseline policy - Assign the migrated policies and tasks to endpoints - Configure a deployment dashboard - Configure product deployment tasks
Upgrade	- Deploy McAfee Agents to pilot endpoints - Deploy McAfee Endpoint Security to pilot endpoints
Validation	- Monitor McAfee Agent and McAfee Endpoint Security deployments - Perform post-upgrade validation testing - Export the baseline policy

Figure8. Test Checklist

Recovery

Implementation begins by preparing your test environment for recovery in the unlikely event of an installation or upgrade failure. Verify your back-out and recovery plans with your project participants and stakeholders.

Back up the McAfee ePolicy Orchestrator application server and database

Verify that snapshots or backups of the production McAfee ePolicy Orchestrator server have completed successfully, and that the McAfee ePolicy Orchestrator database was also backed up. If backups of both were taken, you should verify their integrity before installing the management extensions.

Installation

Once you've completed your back ups, it's time to check in and install the McAfee Endpoint Security software and the supporting components.

Check in required packages

You can obtain the installation software from the McAfee ePolicy Orchestrator Software Manager (also called the Software Catalog) or via the McAfee Products download page at https://secure.mcafee.com/apps/downloads/my-products/login.aspx.

- The easiest way to obtain all required extensions and packages for McAfee Endpoint Security 10.x is to download the McAfee Endpoint Security 10.x bundle from the McAfee ePolicy Orchestrator Software Manager. The McAfee Client Proxy package/extension is included in this bundle.
- The McAfee Endpoint Migration Assistant and Endpoint Upgrade Assistant are available for download via the Software Manager. Once these tools have been installed, you can access them through McAfee ePO > Menu > Software > Endpoint Upgrade Assistant or McAfee ePO > Menu > Policy > Migration Assistant.

Note: The Adaptive Threat Protection (ATP) software is optional and not included in the McAfee Endpoint Security bundle. A valid grant number for ATP is required.

The packages for McAfee Endpoint Security 10.x are listed here:

Component
McAfee Endpoint Security Web Control
McAfee Endpoint Security Threat Prevention
McAfee Endpoint Security Platform
McAfee Endpoint Security Firewall
McAfee Client Proxy
McAfee Endpoint Security Adaptive Threat Protection (If licensed)

Figure9. McAfee Endpoint Security 10.x Packages

Install required management extensions

Management extensions allow you to use McAfee ePolicy Orchestrator policies to manage the point products. The Management Extensions are listed here:

Component	Type	Version
McAfee Endpoint Security Web Control	Extension	10.x
McAfee Endpoint Security Threat Prevention	Extension	10.x
McAfee Endpoint Security Platform	Extension	10.x
McAfee Endpoint Security Firewall	Extension	10.x
McAfee Endpoint Security Adaptive Threat Protection (if licensed)	Extension	10.x
McAfee Client Proxy	Extension	2.3.x
McAfee Common Catalog Framework	Extension	2.0.0.190
McAfee Common Catalog	Extension	2.0.0.190

Figure10. Management Extensions

Additional extensions that will aid in the policy migration and upgrade effort are listed here:

Component	Type	Version
Endpoint Migration Assistant	Extension	Latest
Endpoint Upgrade Assistant	Extension	Latest

Figure11. Additional Extensions

Validate distributed McAfee ePolicy Orchestrator repository replication

Prior to deploying the software, ensure that distributed repositories are working as expected. If lazy caching is used, perform a deployment task on a single machine that is pointed to a repository to ensure that the McAfee Endpoint Security packages/content are available. If you've enabled peer-to-peer, ensure that it is operating successfully.

Run McAfee Endpoint Upgrade Assistant and analyze results

The McAfee Endpoint Upgrade Assistant will provide an overview of your environment. This will tell you the number of endpoints that are ready for an upgrade, how many are blocked from the upgrade, and which endpoints require additional changes to complete the upgrade.

Before you continue with the upgrade, you'll need to address the deployment issues identified by McAfee Endpoint Upgrade Assistant.

Note: For more information on McAfee Endpoint Upgrade Assistant, see page 8.

Import production policies and tasks

Next, import the consolidated policies for McAfee VirusScan, McAfee Host IPS, and McAfee SiteAdvisor Enterprise. These policies will be converted to their McAfee Endpoint Security 10.x counterparts by the McAfee Endpoint Migration Assistant tool.

Configuration

You're almost ready to deploy McAfee Endpoint Security to your pilot endpoints. You just need to configure users, permissions, policies, and tasks first.

Configure users and permission sets

Once you check in the McAfee Endpoint Security 10.x extensions, new permissions for McAfee Endpoint Security 10.x will become available. Update your existing permission sets to include these new products and/or create new permission sets that focus on McAfee Endpoint Security 10.x.

You should update the assigned permission sets of existing McAfee ePolicy Orchestrator users who are responsible for McAfee Endpoint Security to reflect the additional McAfee Endpoint Security 10.x products. Existing permission sets will have "no permissions" for McAfee Endpoint Security-specific products until you manually add them.

Perform initial validation testing

Prior to installing McAfee Endpoint Security, collect basic performance information from your test machines. This will give you a simple baseline to measure against.

Note: You can see an example of performance metrics to measure on page 42 in the Appendix.

Run McAfee Endpoint Migration Assistant

Refer to the McAfee Endpoint Security Migration Guide for specific steps required to migrate policies before installing McAfee Endpoint Security.

The McAfee Endpoint Migration Assistant can be accessed from Menu > Policy > Endpoint Migration Assistant.

The McAfee Endpoint Migration Assistant will perform a policy and task conversion of your current VSE/HIPS/SAE settings and migrate them to their corresponding McAfee Endpoint Security counterparts. You can choose from two migration modes:

- Manual Migration—Recommended for environments that have unnecessary policies and tasks that should be consolidated for easier administration. This may need to be run multiple times as different policies are migrated.
- Automatic Migration— Not recommended, since it will migrate unneeded policies.

Note: Remember to configure and assign policies to endpoints and groups prior to deploying McAfee Endpoint Security 10.x.

When you use the manual migration option, you have an opportunity to selectively migrate policies and make policy adjustments on the fly. You'll also want to ensure that you migrate relevant On-Demand Scan Tasks.

Configure the baseline policy

Configure and assign the baseline policy to endpoint groups or to individual endpoints.

Assign the migrated policies and tasks to endpoints

Assign migrated policies and tasks to endpoints in your test environment.

Configure your deployment dashboard

Your deployment dashboard will show endpoints that are in scope for McAfee Endpoint Security 10.x. Consider creating a Boolean pie chart query that contains matching criteria for McAfee Endpoint Security 10.x security modules. Endpoints that lack the matching criteria will appear as "non-compliant."

A default query named "Endpoint Security: Installation Status Report" displays the total number of endpoints that have McAfee Endpoint Security 10.x installed. Consider adding this query to your deployment dashboard.

Configure product deployment tasks

Review and identify the deployment task method(s) you'll be using to control the scope of your software deployments.

You can choose from three methods:

- Method 1: Deploy the Upgrade Automation Task using McAfee Endpoint Upgrade Assistant.
- Method 2: Selectively deploy McAfee Endpoint Security modules via the Client Task Catalog and system tree assignment.
- Method 3: Create a McAfee Endpoint Security package with McAfee Endpoint Upgrade Assistant Package Creator for deployment with a third-party tool.

Method 1: Deploy the Upgrade Automation Task using the McAfee Endpoint Upgrade Assistant

The package named McAfee Endpoint Upgrade Assistant can be used to upgrade devices to McAfee Endpoint Security 10.x. All McAfee Endpoint Security 10.x packages and extensions must be checked into McAfee ePolicy Orchestrator prior to deploying this package.

The McAfee Endpoint Upgrade Assistant package will deploy the McAfee Endpoint Security modules you select. If you do not want to deploy all the modules, you can create a task in the Client Task Catalog that explicitly specifies the modules to be deployed. You also can select the modules to deploy with Endpoint Upgrade Assistant. Refer to the Endpoint Upgrade Assistant Product Guide for further information.

Note: Perform extensive testing prior to using the Deploy Upgrade Automation Task.

The workflow for deploying an Upgrade Automation task is shown here:

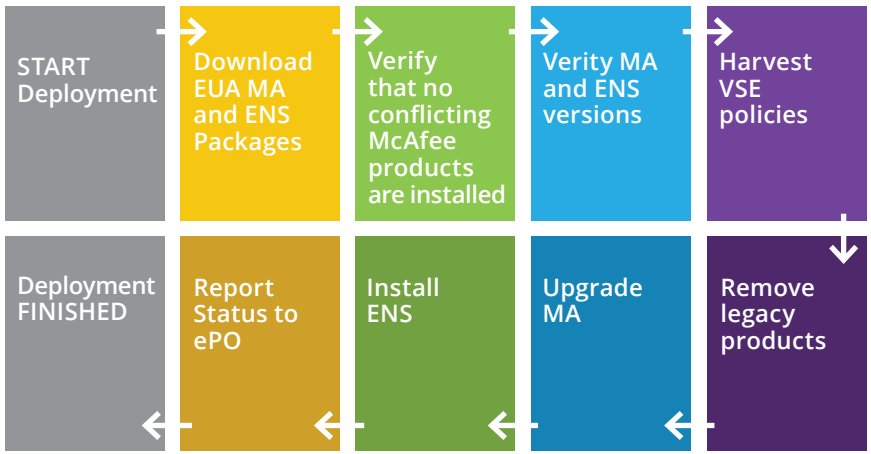


Figure12. Deploying the Endpoint Upgrade Assistant Package

Method 2: Selectively deploy McAfee Endpoint Security modules via the Client Task Catalog and system tree assignment

Create a task in the Client Task Catalog that includes all or some of the McAfee Endpoint Security Modules.

Note: You might be more familiar with leveraging Method 2 as it is the legacy method.

Method 3: Use the McAfee Endpoint Upgrade Assistant Package Creator to create an Endpoint Security package

The McAfee Endpoint Upgrade Assistant Package Creator will walk you through the creation of a package to be deployed with a third-party deployment tool, and will provide options for tailoring the deployment package to various environments.

After the package is created, you can use a third-party deployment tool, such as SCCM or Bigfix, to perform the deployment.

Upgrade

Now you're ready to deploy McAfee Endpoint Security to your pilot endpoints and validate the success of that deployment.

Deploy McAfee Agents to pilot endpoints

If the required version of McAfee Agent is not currently installed, deploy the required McAfee Agent version for your test environment to your pilot endpoints before you move on to deploying McAfee Endpoint Security 10.x.

Deploy McAfee Endpoint Security to pilot endpoints

Deploy McAfee Endpoint Security 10.x using your planned deployment method.

Validation

During this step, you'll verify that your technical implementation meets the security objectives that you previously established and perform tests to ensure that everything is operating properly.

Monitor McAfee Agent and McAfee Endpoint Security deployments

The overwhelming majority of your McAfee Endpoint Security deployments should be successful. Capture any reported issues and document the solutions for those issues. Engage the McAfee Support team when necessary.

Perform post-upgrade validation testing

Verify that your technical implementation meets the security objectives discussed in the Plan and Design phases.

These activities will validate the newly created McAfee Endpoint Security 10.x policies configured for your environment. Validate any additional testing criteria that may have been defined in the Plan and Design phases, for specific use cases.

Note: Verify any additional performance and functional testing requirements planned for your critical enterprise applications. Ensure all applications perform the required business tasks that business owners specified as requirements in the Plan phase.

Validation tests verify that your McAfee products are blocking and monitoring activity and producing logs and events that are viewable on client endpoints and from the McAfee ePolicy Orchestrator console.

Note: You can find example validation tests for features specific to McAfee Endpoint Security on pages 39-41 in the Appendix.

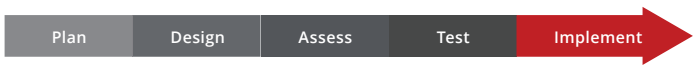
The results of the Application Validation testing should be captured and shared with project participants.

Note: You can find an example of validation testing results on page 38 in the Appendix.

Export the baseline policy

If the McAfee Migration Assistant was used to convert policies to their McAfee Endpoint Security 10.x equivalents, these newly converted policies are now ready to be exported from your test environment and imported into your production environment.

Note: Ensure you are exporting all of the policies that were validated in your test environment.



Implement

During this phase, project participants will install, configure, upgrade, and validate your McAfee solution in a production environment.

The activities listed in this phase will closely mirror the activities completed in the Test phase.

Activities performed during this phase will result in changes to your production environment. McAfee recommends following your organization's practices for submitting change requests, performing endpoint backups, and developing a recovery plan.

Implement	
Prepare for:	**By taking these steps:**
Recovery	▪ Prepare for installation ▪ Back up the McAfee ePolicy Orchestrator application server and database
Installation	▪ Check in the required client packages ▪ Install required management extensions ▪ Validate distributed repository replication ▪ Import the baseline policies and tasks ▪ Configure users and permission sets ▪ Configure a deployment dashboard
Deployment	▪ Run Endpoint Upgrade Assistant ▪ Analyze Endpoint Upgrade Assistant results ▪ Configure the baseline policy ▪ Assign the migrated policies and tasks to endpoints ▪ Configure product deployment tasks ▪ Deploy McAfee Agents to endpoints, as needed ▪ Deploy McAfee Endpoint Security to endpoints
Validation	▪ Monitor McAfee Agent and McAfee Endpoint Security deployments ▪ Perform validation testing

Recovery

Production implementation begins by preparing the environment for recovery in the unlikely event of an installation or upgrade failure. Discuss your back-out and recovery plans with your project participants.

Note: For more on installing and backing up the McAfee ePolicy Orchestrator application server and database, please see page 25.

Installation

Check in required packages

Ensure that software versions in your production environment are the same as those in your test environment.

You can obtain the installation software directly from the McAfee ePolicy Orchestrator Software Manager or via the McAfee Products download page https://secure.mcafee.com/apps/downloads/my-products/login.aspx.

Note: For more on Installation, please see page 38.

Install required management extensions

Management extensions allow the point products to be managed via McAfee ePolicy Orchestrator using policies. Ensure that the same extensions that were checked in to your test environment are also checked in to your production environment.

Note: For more on installing management extensions, please see page 27.

Validate distributed McAfee ePolicy Orchestrator repository replication

Prior to deploying the software, ensure that distributed repositories are working as expected. If lazy caching is used, perform a deployment task on a single endpoint that is pointed to a repository to ensure that the McAfee Endpoint Security packages and content are available. Refer to the McAfee ePolicy Orchestrator Best Practices Guide for additional information.

Import the baseline policies and tasks

Import the polices that you worked with in the test environment. These policies were from the production environment and have undergone a migration to McAfee Endpoint Security 10.x via the Endpoint Migration Assistant.

Ensure that policies have been tested and tailored for critical applications. Next, import the baseline tasks, so that your devices can run the necessary tasks to stay protected.

Configure users and permission sets

Note: For more on this topic, please see page 28.

Configure a deployment dashboard

Ensure that the dashboard is viewable by those tracking the deployment.

Note: For more on this topic, please see page 29.

Deployment

To ensure success, deploy McAfee Endpoint Security to your environment in a phased approach.

Run Endpoint Upgrade Assistant

Ensure that you have set Endpoint Upgrade Assistant to focus on a McAfee Endpoint Security 10.x upgrade.

Analyze Endpoint Upgrade Assistant results

The upgrade scenarios that are displayed in your production environment might be different than those in your test environment. Perform additional testing where necessary to ensure a smooth McAfee Endpoint Security upgrade.

Configure the baseline policy

Configure and assign the baseline policy to endpoint groups or individual endpoints.

Assign the migrated policies and tasks to endpoints

Assign migrated policies and tasks to endpoints in your production environment.

Configure product deployment tasks

Ensure that the tasks are set to execute in accordance with the information listed in the change request.

Note: For more on this topic, please see page 29.

Deploy McAfee Agents to endpoints, as needed

Machines that have a broken McAfee Agent will need to be remediated prior to deploying McAfee Endpoint Security 10.x through McAfee ePolicy Orchestrator.

Deploy McAfee Endpoint Security to endpoints

Use a phased implementation approach and tightly control the number of endpoints that receive McAfee Endpoint Security 10.x.

Validation

In this phase, you'll verify that the technical implementation meets the security objectives laid out in the Plan and Design phases.

Monitor McAfee Agent and McAfee Endpoint Security deployments

The overwhelming majority of McAfee Endpoint Security deployments should be successful. Closely monitor any failed deployments and identify common scenarios that result in failure. Engage McAfee Support when necessary.

Perform validation testing

Ensure that your stakeholders (especially your application owners) are aware of the implementation timeline. Encourage stakeholders to validate endpoint performance once McAfee Endpoint Security 10.x modules are installed on critical servers. Application owners should perform a regression test against their applications to ensure that McAfee Endpoint Security 10.x has not introduced a new issue into the environment.

In the event that your stakeholders discover performance issues, refer to the technical article KB86691 in the McAfee Knowledge Center, "Data collection steps for troubleshooting McAfee Endpoint Security issues." This article provides guidance on collecting data using:

- Process Monitor—An advanced monitoring tool for Windows that shows real-time file endpoint, Registry and process/thread activity.
- Windows Performance Recorder—A performance-recording tool that is based on Event Tracing for Windows (ETW). It records endpoint events that you can then analyze by using Windows Performance Analyzer (WPA).
- AMTrace—An internal tool to collect logging data from McAfee AMCore.

Note: For more on this topic, please see page 30.

Appendix

Plans and Tracking Sheets

Upgrade Project Planning Checklist

Plan	
[ ]	Identify business applications, administrators and application owners
[ ]	Discuss project and business objectives
[ ]	Discuss security requirements
[ ]	Discuss end user communications
[ ]	Discuss additional planning topics
[ ]	Discuss product features
[ ]	Discuss product feature parity
[ ]	Discuss supported platforms
[ ]	Discuss supported McAfee agents
[ ]	Discuss integration with other McAfee solutions
[ ]	Discuss conflicts with existing products
[ ]	Discuss the implementation process
[ ]	Identify endpoints for the initial pilot deployment
[ ]	Discuss McAfee application validation testing
[ ]	Discuss performance testing and baseline metrics
[ ]	Discuss business application testing procedures
[ ]	Discuss current security management practices
[ ]	Discuss change control processes
[ ]	Discuss back out and recovery plans
[ ]	Discuss software updates
[ ]	Discuss signature content testing
[ ]	Discuss McAfee GetClean
[ ]	Discuss reporting requirements
[ ]	Review corporate security policies and supporting documentation

Design	
[ ]	Discuss the McAfee solution architecture overview
[ ]	Discuss the endpoint architecture
[ ]	Discuss the network infrastructure services
[ ]	Discuss McAfee network services
[ ]	Discuss registered servers
[ ]	Discuss roles and responsibilities
[ ]	Discuss users and groups
[ ]	Review release notes
[ ]	Review known issues Knowledge Base articles
[ ]	Review the product compatibility matrix
[ ]	Verify that the installation environment meets specifications
[ ]	Verify accounts and permissions
[ ]	Verify prerequisite software is installed
[ ]	Verify pilot endpoints configuration
Assess	
[ ]	Prepare for installation
[ ]	Backup the McAfee ePO application server and database
[ ]	Obtain the installation software
[ ]	Install required management extensions
[ ]	Run Endpoint Upgrade Assistant
[ ]	Analyze Endpoint Upgrade Assistant results
[ ]	Review dashboards and queries
[ ]	Perform McAfee VirusScan Enterprise policy review(s)
[ ]	Perform McAfee Host Intrusion Prevention policy review(s)
[ ]	Perform SiteAdvisor Enterprise policy review(s)
[ ]	Export production policies
[ ]	Export production tasks

Test	
[ ]	Prepare for installation
[ ]	Backup the McAfee ePO application server and database
[ ]	Check in required packages
[ ]	Install required management extensions
[ ]	Validate distributed repository replication
[ ]	Run Endpoint Upgrade Assistant
[ ]	Analyze Endpoint Upgrade Assistant results
[ ]	Import production policies
[ ]	Import production tasks
[ ]	Configure users and permission sets
[ ]	Perform initial validation testing
[ ]	Run the Endpoint Migration Assistant
[ ]	Migrate policies
[ ]	Migrate tasks
[ ]	Configure the baseline policy
[ ]	Assign the migrated policies to endpoints
[ ]	Assign the migrated tasks to endpoints
[ ]	Configure a deployment dashboard
[ ]	Configure product deployment tasks
[ ]	Deploy McAfee Agents to pilot endpoints, as needed
[ ]	Deploy McAfee Endpoint Security to pilot endpoints
[ ]	Monitor McAfee Agent and Endpoint Security deployments
[ ]	Perform post-upgrade validation testing
[ ]	Export the baseline policy

Implement	
[ ]	Prepare for installation
[ ]	Backup the McAfee ePO application server and database
[ ]	Check in required packages
[ ]	Install required management extensions
[ ]	Validate distributed repository replication
[ ]	Import the baseline policies
[ ]	Import the baseline tasks
[ ]	Configure users and permission sets
[ ]	Configure a deployment dashboard
[ ]	Run the Endpoint Upgrade Assistant
[ ]	Analyze Endpoint Upgrade Assistant results
[ ]	Configure the baseline policy
[ ]	Assign the migrated policies to endpoints
[ ]	Assign the migrated tasks to endpoints
[ ]	Configure product deployment tasks
[ ]	Deploy McAfee Agents to endpoints, as needed
[ ]	Deploy McAfee Endpoint Security to endpoints
[ ]	Monitor McAfee Agent and Endpoint Security deployments
[ ]	Perform validation testing

Pilot Endpoint Plan Tracking Sheet

Application(s)	OS	App Owner Contact	# Pilot Devices
EMC Backup Server	Win Server 2012	John.doe@contoso.com	2
DHCP Server	Win Server 2016	kyle.doe@contoso.com	2
Common Desktop Applications	Win 7 and 10 (x86 and 64bit)	Desktop_infra@contoso.com	4
[Critical App 1]	Win Server 2016	DL-DatabaseTeam@contoso.com	3
Mac Desktop	MacOS 10.12	macs@contoso.com	1

VirusScan Policies - Consolidation Tracking Sheet

VirusScan Policies - Consolidation Tracking Sheet		
VSE Policy Name	**Description**	**Action Plan**
Finance.Corp-OAS Policy	This policy includes exclusions Legacy financial applications that have known performance issues. The exclusions are recommended by the vendor.	The list of exclusions for these applications will be placed into a new policy named "Finance-OAS-G1".
Revenue Cycle-OAS Policy	This policy includes exclusions for the app named Revenue Cycle. The exclusions are recommended by the vendor.	

Note: Repeat the above methodology for all configured McAfee VirusScan tasks. Task consolidation decisions need to ensure whether new or additional Endpoint Security product tasks might need to be created.

McAfee VirusScan Tasks - Consolidation Tracking Sheet

McAfee VirusScan Tasks - Consolidation Tracking Sheet		
VSE Task Name	**Description**	**Action Plan**
Update All	Updates DAT files for VSE	None – This task will be used for Endpoint Security content updates
Weekly ODS	Performs full endpoint scan a weekly basis	Schedule a new Scan task for Endpoint Security 10.x

McAfee HIPS IPS Rules Policies - Consolidation Tracking Sheet

McAfee IPS IPS Rules Policies - Consolidation Tracking Sheet		
HIPS IPS Rules Policy	**Description**	**Action Plan**
IPS Rules-Marketing	Contains exceptions for an app used by Marketing.	The list of exclusions pertaining to these applications will be consolidated into a new policy named IPS Rules-General-Apps
IPS Rules Publishing	Contains exceptions for an app used by Marketing.	

Note: The environment may have many firewall policies with rules in them that are not currently linked to the Host IPS Firewall Catalog.

McAfee Host IPS Firewall Rules Policies - Consolidation Tracking Sheet

McAfee HIPS Firewall Rules Policies - Consolidation Tracking Sheet		
HIPS Firewall Rules Policy	**Description**	**Action Plan**
FW Rules-Coders	Firewall rules used by software coders.	The firewall rules for these applications will be placed into a new firewall policy named FW-Rules-Developers.
FW Rules-Programmers	Firewall rules used by Python Programmers.	

Examples

Example Application Owners Sheet

Application Owners		
Application Name	**Purpose**	**Owner/Administrator**
Example: Meditech	Pharmacy Workflow, Laboratory Diagnostics	John.doe@company.com
Example: Invoice Supreme	Accounts Receivable, Recurring Billing	John.doe@company.com

Note: The Application Owners Sheet is important for Endpoint Security-based exclusions, exceptions, and other policies. Business owners may require a new or different policy based on the application vendor's list of recommended exclusions or other configurations.

Example Format for a Validation Test

Test Name	Test ID#
Validation Steps	Step 1) Step 2) Step 3)
Expected Results	
Actual Results	

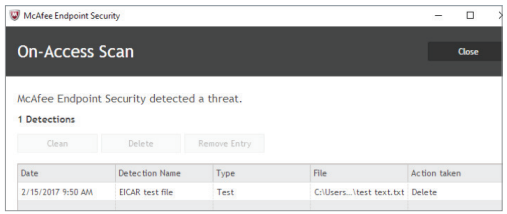
Note: The results of validation testing should provide discussion points for additional policy configurations as required.

Example Future State Dashboard for Endpoint Security Products

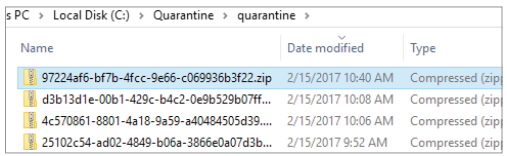
Operational Dashboard		
Monitor Name	Description	Action Plan
Antivirus Installed/ Missing	This Boolean chart shows machines that have AV installed as well as machines that are missing AV. The approved antivirus software is McAfee VirusScan .	Update the query to include criteria for McAfee Endpoint Security 10.x Threat Prevention.
HIPS Content Compliance	Shows devices running up to date HIPS content (Signatures).	Add a new monitor that also shows content compliance for Exploit Prevention.
McAfee VirusScan Current DAT Adoption	Displays the number of workstations which have recent McAfee VirusScan DATs (Within 2 versions of the master repository).	Add a new monitor that shows AMCore Content (Threat Prevention) within 2 version versions of the Master Repository.

Example Validation Tests for Endpoint Security-specific Features

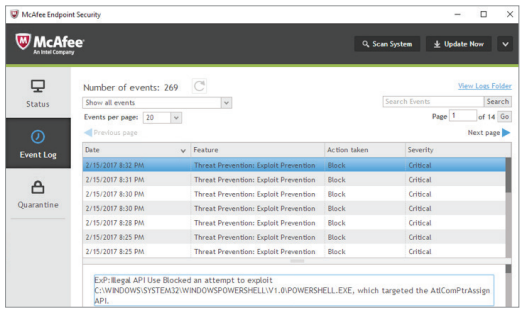
On Access Scanning - EICAR Test

On Access Scanning – EICAR Test	
Validation Steps	▪ Create a new text file ▪ Within the text file, enter the following string: **X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*** ▪ Save and close the text file ▪ Attempt to copy the text file
Expected Results	The test file will be deleted and a popup message similar to the one shown below will be produced. 
Actual Results	

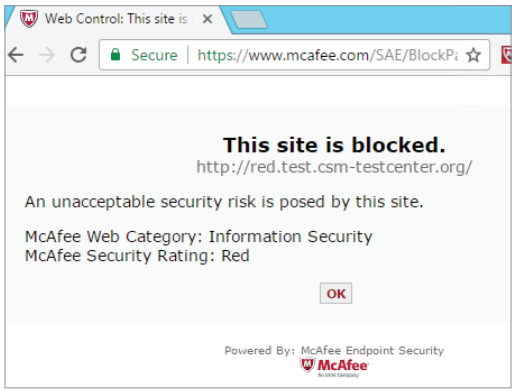
Viewing the Quarantine Folder

Options – Viewing the Quarantine Folder	
Validation Steps	▪ Navigate to C:\quarantine ▪ Verify that files appear in the quarantine folder
Expected Results	Files that have been quaratined will be in compresed zip format. 
Actual Results	

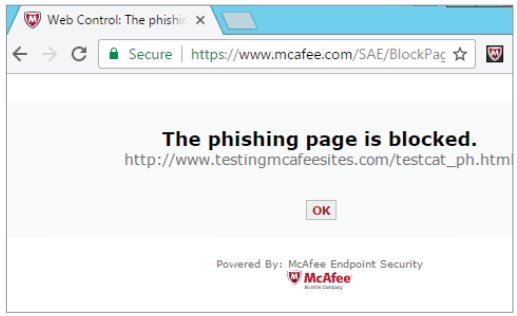
Exploit Prevention - Blocking Hidden PowerShell

Exploit Prevention - Hidden PowerShell Detected	TC-ENS-003
Test Setup	Ensure that the browser plugin for McAfee Endpoint Security Web Control is running
Validation Steps	▪ Open the Google Chrome Browser ▪ Navigate to http://www.testingmcafeesites.com/testcat_ph.html
Expected Results	The site is blocked because it is has a “red rating” (See screen shot) 
Actual Results	

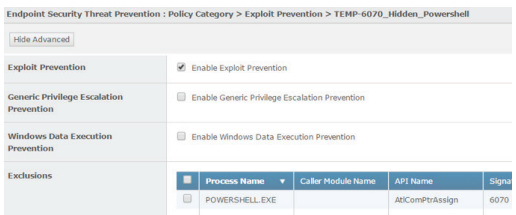
Web Control - Blocking Navigation to a Malicious Website

Web Control – Blocking Navigation to a Phishing Page	TC-ENS-004
Test Setup	Ensure that the browser plugin for McAfee Endpoint Security Web Control is running
Validation Steps	▪ Open the Google Chrome Browser ▪ Navigate to http://red.test.csm-testcenter.org/
Expected Results	The site is blocked because it is has a "red rating" (See screen shot) 
Actual Results	
Attachments	How to test SiteAdvisor Enterprise 3.x category ratings https://kc.mcafee.com/corporate/index?page=content&id=KB72563

Web Control – Blocking Navigation to a Phishing Page

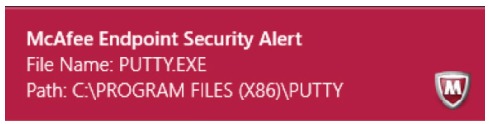
Web Control – Blocking Navigation to a Phishing Page	TC-ENS-005
Test Setup	Ensure that the browser plugin for McAfee Endpoint Security Web Control is running
Validation Steps	▪ Open the Google Chrome Browser ▪ Navigate to http://www.testingmcafeesites.com/testcat_ph.html
Expected Results	The phishing webpage is blocked because phishing is a category on the block list" (See screen shot) 
Actual Results	
Attachments	How to test SiteAdvisor Enterprise 3.x category ratings https://kc.mcafee.com/corporate/index?page=content&id=KB72563

Exploit Prevention – Viewing Aggregated Events

Exploit Prevention – Viewing Aggregated Events	TC-ENS-006
Validation Steps	▪ Open the McAfee ePO console ▪ Navigate to Reporting > Exploit Prevention Events ▪ Aggregate on "Analyzer Rule ID + Threat Target File Path + Action Taken ▪ Drill into an event with Analyzer ID 6070 ▪ On the page named "Aggregated Exploit Prevention Events Details", click Actions > Add Exclusion" ▪ In the "Select a destination policy" page, click the policy named "TEMP-6070_Hidden_Powershell" and select ok ▪ Navigate to the policy named "TEMP-6070_Hidden_Powershell" (it can be found at "Endpoint Security Threat Prevention : Policy Category > Exploit Prevention > TEMP-6070_Hidden_Powershell") ▪ Select "Show Advanced"
Expected Results	An exclusion for the process "POWERSHELL.EXE" was created in the policy (See screen shot) 
Actual Results	

Optional TIE/DXL Validation Tests

McAfee Threat Intelligence Exchange – Manually Changing a File's Reputation to "Most Likely Malicious"

McAfee Threat Intelligence Exchange – Manually Changing a File's Reputation to "Most Likely Malicious"	TC-ENS-007
Test Setup	▪ The TIE and DXL Infrastructure must be up and running in your environment. ▪ ATP must be enabled ▪ The action enforcement setting to Block when reputation threshold reaches "Most Likely Malicious" must be enabled. ▪ Download and install the software named "Putty". It can be downloaded from https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html ▪ Note: If you are currently using Putty for business purposes please select a different .exe to test.
Validation Steps	▪ Navigate to Menu > Systems > Reputation > Tie Reputations ▪ Using the Quick Find, search for "putty" ▪ Select Putty.exe and click Actions > Most Likely Malicious ▪ Attempt to launch putty from your test computer
Expected Results	A McAfee Endpoint Security Alert is produced on your test computer (see screen shot)  The file is blocked on execute. Note: Revert Putty's reputation by setting the Reputation for Putty to "known trusted"
Actual Results	

Example Performance Metrics

Performance Metric	Value
Average time for endpoint startup	
Average time for user login	
Average CPU utilization (over 24 hr period)	
[example] application specific performance metrics	

Example Endpoint Security Validation Results

Test ID	Test Name	Results
TC-ENS-001	On Access Scanning – EICAR Test	Pass
TC-ENS-002	Options – Viewing the Quarantine Folder	Pass
TC-ENS-003	Exploit Prevention - Hidden PowerShell Detected	Pass
TC-ENS-004	Web Control – Blocking Navigation to a Malicious Site	Pass
TC-ENS-005	Web Control – Blocking Navigation to a Phishing page	Pass
TC-ENS-006	Exploit Prevention – Viewing Aggregated events	Pass
TC-ENS-007	Threat Intelligence Exchange – Manually changing a file's reputation to "most likely malicious"	Pass

Technical Information

Endpoint Requirements

Operating System	Service Pack	32bit	64bit	Processor	RAM	Minimum Hard Disk Space Free
Windows 10		X	X	2 GHz or higher	3 GB	1 GB
Windows 10 with November update		X	X	2 GHz or higher	3 GB	1 GB
Windows 8.1 Update 1		X	X	2 GHz or higher	3 GB	1 GB
Windows 8.1		X	X	2 GHz or higher	3 GB	1 GB
Windows 8 (Except RT)		X	X	2 GHz or higher	3 GB	1 GB
Windows 7	SP1	X	X	1.4 GHz or higher	2 GB	1 GB
Windows Embedded Standard 7		X		1 GHz or higher	1 GB	1 GB
Windows Vista (not supported with Endpoint Security 10.5)	SP2	X	X	1.4 GHz or higher	2 GB	1 GB
Windows XP Pro (No longer supported by Microsoft.) (not supported with Endpoint Security 10.5)	SP3	X		1 GHz or higher	1 GB	1 GB
Windows Embedded for POS (WEPOS)		X		1 GHz or higher	1 GB	1 GB
Windows Embedded 8 (Pro, Standard, and Industry)		X		1 GHz or higher	1 GB	1 GB
Windows Server 2016			X	2 GHz or higher	3 GB	1 GB
Windows Server 2012 R2 Update 1			X	2 GHz or higher	3 GB	1 GB

Operating System	Service Pack	32bit	64bit	Processor	RAM	Minimum Hard Disk Space Free
Windows Server 2012 R2 Essentials, Standard, and Datacenter (including Server Core Mode)			X	2 GHz or higher	3 GB	1 GB
Windows Server 2012 Essentials, Standard, and Datacenter (including Server Core Mode)			X	2 GHz or higher	3 GB	1 GB
Windows Server 2008 Essentials, Standard, Datacenter, and Enterprise Web (including Server Core Mode) (not supported with Endpoint Security 10.5)	SP2	X	X	1.4 GHz or greater	2 GB	1 GB
Windows Server 2008 R2 Essentials, Standard, Datacenter, and Enterprise Web (including Server Core Mode)	SP2	X	X	1.4 GHz or greater	2 GB	1 GB
Windows Storage Server 2008 (not supported with Endpoint Security 10.5)		X	X	1.4 GHz or higher	2 GB	1 GB
Windows Storage Server 2008 R2		X	X	1.4 GHz or higher	2 GB	1 GB
Windows Server 2003, 2003 R2 – All No longer supported by Microsoft.		X		1.4 GHz or higher	2 GB	1 GB
Windows Small Business Server 2008 (not supported with Endpoint Security 10.5)		X		1.4 GHz or higher	2 GB	1 GB

Operating System	Service Pack	32bit	64bit	Processor	RAM	Minimum Hard Disk Space Free
Windows Small Business Server 2011		X		1.4 GHz or higher	2 GB	1 GB
Windows Embedded Standard 2009		X		1 GHz or higher	1 GB	1 GB
Windows Point of Service 1.1		X		1 GHz or higher	1 GB	1 GB
Windows Point of Service Ready 2009		X		1 GHz or higher	1 GB	1 GB

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com