Symantec™ Network Access Control Starter Edition

Simplified endpoint compliance

Overview

Symantec™ Network Access Control Starter Edition makes it easy to begin implementing a network access control solution. It offers a subset of Symantec Network Access Control functionality that can be completely leveraged toward a full Symantec Network Access Control deployment. Like Symantec Network Access Control, it grants access only to endpoints that comply with your defined security policies by evaluating compliance status, providing automatic remediation, and ensuring access is properly provisioned and secured. The result is a network environment in which businesses can realize significant reductions in security incidents, increased levels of compliance with configuration policies, and confidence that endpoint security mechanisms are properly enabled.

Key benefits

Organizations that deploy Symantec Network Access Control Starter Edition can experience multiple measurable benefits, including:

• Reduced propagation of malicious code such as viruses, worms, spyware, and other forms of crimeware

• Lowered risk profile through increased control of unmanaged and managed endpoints accessing the corporate network

• Greater network availability and reduced disruption of services for end users

• Verifiable organizational compliance information through near real-time endpoint compliance data

• Minimized total cost of ownership based on an enterprise-class centralized management architecture

• Verification that endpoint security investments such as Symantec AntiVirus™ and the client firewall are properly enabled

• Seamless integration with Symantec™ Endpoint Protection

Key features
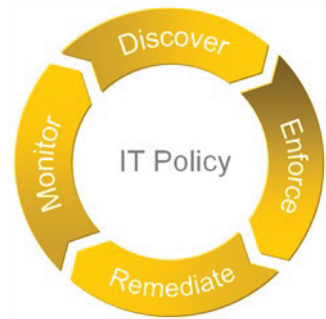
Symantec Network Access Control Starter Edition Process

Network access control process

Network access control is a process—one that mandates coverage for all types of endpoints and all types of networks. It begins prior to connection to the network and continues throughout the duration of the connection. As with all corporate processes, policy serves as the basis for evaluations and actions.

Confidence in a connected world.

symantec™

The network access control process consists of four steps:

1. **Discover and evaluate endpoints**. This occurs as endpoints connect to the network and before they access resources. Through integration with the existing network infrastructure and the use of intelligent agent software, network administrators can be assured that new devices connecting to the network are evaluated according to minimum IT policy requirements.

2. **Provision network access.** Full network access is granted only after systems are evaluated and determined to be in compliance with IT policy. Systems not in compliance, or failing to meet the minimum security requirements for the organization, are quarantined with limited or no access to the network.

3. **Remediate noncompliant endpoints.** Automatic remediation of noncompliant endpoints empowers administrators to quickly bring endpoints into compliance and subsequently alter network access. Administrators can either fully automate the remediation process, resulting in a fully transparent process to the end user, or provide information to the user for manual remediation.

4. **Proactively monitor compliance.** Because adherence to policy is a full-time issue, Symantec Network Access Control actively monitors the compliance posture for all endpoints on an administrator-set interval. If at any time the endpoint's compliance status changes, so will the network access privileges of the endpoint.

Deployable in any network

The typical corporate user connects to the network by multiple access methods; as a result, administrators must have the flexibility to consistently apply evaluation and connection controls regardless of the connection type. As one of the most mature network access control solutions on the market today, Symantec Network Access Control Starter Edition allows network administrators to actively enforce compliance through existing investments in network infrastructure with no required network equipment upgrades.

Whether using one of the Symantec Network Access Control Gateway Enforcers that integrate directly into the network or our host-based Self-Enforcement option requiring no network enforcers, organizations can be assured that end users and endpoints are in compliance at the point of contact to the corporate network.

Symantec Network Access Control architecture

The Symantec Network Access Control architecture includes three core components: policy management, endpoint evaluation, and network enforcement. All three components work together as a single solution without relying on external elements for functionality. If host-based enforcement is desired over network-based enforcement, only the policy management and endpoint evaluation components are necessary.

Centralized policy management and reporting

Paramount to the efficient operation of any solution is an enterprise-class management console. The Symantec Endpoint Protection Manager provides a Java™ technology–based console to centrally create, deploy, manage, and report agent and Enforcer activity. Scalable to fit the most

Confidence in a connected world.   ✹ symantec™

demanding environments, the policy manager provides granular control to all administrative tasks in a high-availability architecture.

Endpoint evaluation

Symantec Network Access Control Starter Edition protects the network from malicious code and also verifies that endpoints connecting to the network are configured properly so they are protected from online attacks. Regardless of the goal, the process begins with evaluating the endpoint. While the common minimum requirements for allowing network access include checking for antivirus, antispyware, and installed patches, most organizations quickly expand well beyond these minimums after the initial network access control deployment.

Symantec Network Access Control Starter Edition offers persistent agent–based evaluation technology when determining endpoint compliance. Corporate-owned and other managed systems use an administrator-installed agent to determine compliance status. It checks antivirus, antispyware, and installed patches as well as complex system status characteristics such as registry entries, running processes, and file attributes. Persistent agents provide the most in-depth, accurate, and reliable system compliance information while offering the most flexible remediation and repair functionality of assessment options.

Enforcement

Symantec Network Access Control Starter Edition allows you to select between gateway-based enforcement and host-based enforcement:

• **Gateway Enforcer** is an in-line enforcement device used at network choke points. It controls the flow of traffic through the device based upon policy compliance of remote endpoints. Whether the choke point is at perimeter network connection points, such as WAN links or VPNs, or on internal segments accessing critical business systems, Gateway Enforcer efficiently provides controlled access to resources and remediation services.

• **Self-Enforcement** leverages the host-based firewall capabilities within the Symantec Protection Agent to adjust local agent policies according to endpoint compliance status. This allows administrators to control access to any network, on or off the corporate network, for devices such as laptops that routinely move between multiple networks.

Support services

Symantec provides a range of consulting, technical education, and support services that guide you through the migration, deployment, and management of Symantec Network Access Control Starter Edition and help you realize the full value of your investment. For organizations that want to outsource security monitoring and management, Symantec also offers Managed Security Services to deliver real-time security protection.

Confidence in a connected world. symantec™

Symantec Network Access Control Starter Edition product family

	Symantec Network Access Control	Symantec Network Access Control Starter Edition
Enforcement		
LAN 802.1X	X	
DHCP	X	
Gateway	X	X
Self-enforcement	X	X
Endpoint evaluation		
Persistent agent	X	X
Dissolvable agent*	X	X
Remote vulnerability scanning*	X	X

* = purchased separately

Minimum system requirements

Platform support

Symantec Endpoint Protection Manager

Central administration server

Component	32-bit	64-bit
Microsoft® Windows® 2003	X	X
Microsoft Windows XP	X	
Microsoft Windows 2000 (SP3 and later)	X	
Processor	600 MHz	1 GHz
Memory	512 MB of RAM	512 MB of RAM
Hard disk	500 MB	500 MB

Symantec Endpoint Protection Console

Remote administration console (optional)

Component	32-bit	64-bit
Microsoft Windows Vista®	X	X
Microsoft Windows 2003	X	X
Microsoft Windows XP	X	X
Microsoft Windows 2000 (SP3 and later)	X	
Processor	600 MHz	1 GHz
Memory	256 MB of RAM	256 MB of RAM
Hard disk	40 MB	40 MB

Symantec Network Access Control Client

Component	32-bit	64-bit
Microsoft Windows Vista	X	X
Microsoft Windows 2003	X	X
Microsoft Windows XP	X	X
Microsoft Windows 2000 Professional	X	
Memory	128 MB of RAM	128 MB of RAM
Hard disk	600 MB	600 MB

Symantec Network Access Control Enforcer 6100 Series (optional)

Base Appliance Option (Gateway)

Rack units	1
Dimensions	1.68" x 17.60" x 21.5"
Processor	One 2.8-GHz Intel® Pentium® 4 processor
Memory	1 GB
Storage	One 160-GB (SATA)

Fail Open Appliance Option (Gateway)

Rack units	1
Dimensions	1.68" x 17.60" x 21.5"
Processor	One 2.8-GHz Intel Pentium 4 processor
Memory	1 GB
Storage	One 160-GB (SATA)

Symantec Network Access Control Scanner (optional)

Operating system:

• Microsoft Windows 2000 Server (SP4)

• Microsoft Windows 2003 Server (SP1)

Minimum processor:

• Intel® Pentium® 4 1.8 GHz

• 1 GB of RAM minimum

• 1 GB free hard disk space

• Internet Explorer® 5.5 or later

• Microsoft Windows 2000 Professional

Confidence in a connected world.

symantec™

More information

Visit our Web site

www.symantec.com/endpoint

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our Web site.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

Confidence in a connected world.   symantec.