SYNGRESS®

FREE E-BOOK DOWNLOAD

Microsoft Forefront Security Administration Guide

Deploy the Forefront Security Suite for Client, Server, and Edge Security

- Achieve Comprehensive, Integrated, and Simplified Infrastructure Security
- Scan SharePoint Servers for Viruses as well as Inappropriate and Confidential Content
- Conduct Penetration Testing on an Enterprise Using the Microsoft Forefront Security Suite

Jesse Varsalone Technical Editor

Ed Collins
Adam Gent
Chris Hughes
Jan Kanclirz
Mohan Krishnamurthy
Daniel Nerenberg
Matthew Shepherd
Arno Theron
Robert Valentine
Gene Whitley
James Yip

Microsoft Forefront Security Administration Guide

Jesse Varsalone Technical Editor

Ed Collins
Adam Gent
Chris Hughes
Jan Kanclirz
Mohan Krishnamurthy
Daniel Nerenberg
Matthew Shepherd
Arno Theron
Robert Valentine
Gene Whitley
James Yip

This page intentionally left blank

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	BPOQ48722D
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Microsoft Forefront Security Administration Guide

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-244-7

Publisher: Amorette Pedersen
Acquisitions Editor: Andrew Williams
Technical Editor: Jesse Varsalone
Project Manager: Gary Byrne
Page Layout and Art: SPI
Copy Editors: Judy Eby, Michelle Lewis, and Adrienne Rebello,
Indexer: Michael Ferreira
Cover Designer: Michael Kavish

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.

This page intentionally left blank

Technical Editor

Jesse Varsalone (A+, Linux+, Net+, iNet+, Security+, Server+, CTT+, CIW Professional, CWNA, CWSP, MCT, MCSA, MSCE 2000/2003, MCSA/MCSE Security, MCDBA, MCSD, CNA, CCNA, MCDST, Oracle 8i/9i DBA, Certified Ethical Hacker) is a computer forensic senior professional at CSC. For four years, he served as the director of the MCSE and Network Security Program at the Computer Career Institute at Johns Hopkins University. For the 2006 academic year, he served as an assistant professor of computer information systems at Villa Julie College in Baltimore, MD. He taught courses in networking, Active Directory, Exchange, Cisco, and forensics.

Jesse holds a bachelor's degree from George Mason University and a master's degree from the University of South Florida. Jesse was a contributing author for *The Official CHFI Study Guide (Exam 312-49)* and *Penetration Tester's Open Source Toolkit, Second Edition*. He runs several Web sites, including mcsecoach.com, which is dedicated to helping people obtain their MCSE certifications. He currently lives in Columbia, MD, with his wife, Kim, and son, Mason.

Contributing Authors

Edward Collins (CISSP, CEH, Security+, MCSE:Security, MCT) is a senior security analyst for CIAN, Inc., where he is responsible for conducting penetration tests, threat analysis, and security audits. CIAN (www.ciancenter.com) provides commercial businesses and government agencies with all aspects of information security management, including access control, penetration testing, audit procedures, incident response handling, intrusion detection, and risk management. Edward is also a training consultant, specializing in MCSE and Security+ certifications. Edward's background includes positions as information technology manager at Aurora Flight Sciences and senior information technology consultant at Titan Corporation.

Adam Gent (MCSE: Messaging & Security, MCTS: LCS, Security+) is a technical consultant with Datapulse Ltd., a Nortel Developer Partner specializing in attendant consoles, call-billing applications, and value-add applications for Office Communications Server (OCS). Adam works with the company's Product Group to architect and manage products that relate to OCS. He also works with customers consulting on the deployment of OCS within enterprises.

Adam holds a bachelor's degree in computer science from Cardiff University and is a member of the British Computer Society.

Chris Hughes (MCSE 2003 Messaging/Security, MCDBA, MCT, Security+, CISSP, ITIL Service Foundations) is a systems architect at the University of Florida (UF), where he has worked for the past 11 years. He currently works in the College of Medicine, supporting and implementing its budgeting and business intelligence systems with revenue in excess of $500 million.

Chris has a wide variety of experience with nearly the entire Microsoft product portfolio, from performing Active Directory migrations for the 60+ statewide sites at UF's Institute of Food and Agricultural Sciences to supporting the infrastructure behind one of the first Internet MBA programs at UF's Warrington College of Business. He has a special interest in

distributed administration, infrastructure optimization, and IT governance with an emphasis on their implementation in an academic environment.

Chris would like to thank his wife, Erica, for her love, patience, and encouragement.

Jan Kanclirz Jr. (CCIE #12136 - Security, CCSP, CCNP, CCIP, CCNA, CCDA, INFOSEC Professional, Cisco WLAN Support/Design Specialist) is currently a senior network consulting architect at MSN Communications out of Colorado.

Jan specializes in multivendor designs and post-sale implementations for several technologies such as VPNs, IDS/IPS, LAN/WAN, firewalls, client security, content networking, and wireless. In addition to network design and engineering, Jan's background includes extensive experience with open source applications and operating systems such as Linux and Windows. Jan has contributed to the following Syngress book titles either as a technical editor or author: *Managing and Securing Cisco SWAN*, *Practical VoIP Security*, *How to Cheat at Securing a Wireless Network*, *Microsoft Vista for IT Security Professionals*, and *How to Cheat at Microsoft Vista Administration*.

In addition to his full-time position at MSN Communications, Jan runs a security portal, www.MakeSecure.com, where he dedicates his time to security awareness and consulting. Jan lives in Colorado, where he enjoys outdoor adventures such as hiking Colorado's 14ner peaks.

Mohan Krishnamurthy Madwachar (MCSE, CCSA) is the GM, Network Security, at Almoayed Group, Bahrain. Mohan is a key contributor to Almoayed Group's Projects Division and plays an important role in the organization's network security initiatives. Mohan has a strong networking, security, and training background. His tenure with companies such as Schlumberger Omnes and Secure Network Solutions India adds to his experience and expertise in implementing large and complex network and security projects.

Mohan holds leading IT industry-standard and vendor certifications in systems, networking, and security. He is a member of the IEEE and PMI.

Mohan would like to dedicate his contributions to this book to his friends: Krishnan, Rajmohan, Sankaranarayanan, Vinayagasundaram, Rajagopalan, N.K. Mehta, and Ramesh.

Mohan has coauthored four books published by Syngress: *Designing & Building Enterprise DMZs* (ISBN: 1597491004), *Configuring Juniper Networks NetScreen & SSG Firewalls* (ISBN: 1597491187), *How to Cheat at Securing Linux* (ISBN: 1597492078), and *How to Cheat at Administering Office Communications Server* (ISBN: 1597492126). He also writes in newspaper columns on various subjects and has contributed to leading content companies as a technical writer and a subject matter expert.

Daniel Nerenberg (MCT, MCSE, MCITP, MCTS) is an IT strategy adviser with InfraOp. He delivers training and consulting for companies across North America. He specializes in Microsoft infrastructure technologies, with a particular focus on deploying secure environments.

Daniel is a founding member and current president of the Montreal IT pro user group. He is also a Microsoft MVP and an active member of the Quebec Federation of IT professionals (FiQ). He lives in Montreal, Quebec, with his wife, Emily.

Matt Shepherd (CISSP, MCSE, MCDBA, GCFW, CEH) is a consultant in the Security and Privacy Division at Project Performance Corporation of McLean, VA. Matt uses his experience as a network administrator, IT manager, and security architect to deliver high-quality solutions for Project Performance Corporation's clients in the public and private sector. Matt holds bachelor's degrees from St. Mary's College of Maryland, and he is currently working on his master's of science in information assurance.

Matt would like to thank his wife, Leena, for her wonderful support during this project and throughout their relationship. He thanks his family for a lifetime of love and support and Olive for making every day special.

Arno Theron (MCSA, MCSE, MCITP, MCTS, and MCT) is an independent information security professional with seven years of network/server administration experience and six years of IT training experience as a Microsoft Certified Trainer. He is dedicated to improving training policy and implementation with high-quality technical information. Arno's current interests are focused on SharePoint, Windows Mobile, and ITIL.

Robert Valentine has had a career of more than 20 years in the IT and engineering simulation industry. For most of his career, he has been working as a senior systems engineer. He currently is an IT manager and consults as a trainer.

Over the years, Robert's work has varied with implementing corporate standards for software and hardware, along with coordinating and implementing large corporate deployments while setting corporate migration standards for both client- and server-based platforms for small to enterprise-scaled businesses.

Robert holds numerous IT industry certifications, including MCSE, MCSA, MCTS, MCITP, MCT, and Comptia A+. He is also a Dell Certified Systems Engineer and holds two university engineering degrees.

Robert has also coauthored multiple engineering papers that have been published within the engineering community, and he has successfully coauthored multiple information technology books.

Gene Whitley (MBA, MCSE, MCSA) is the president of SiGR Solutions (www.sigrsolutions.com), a systems integrator and value-added reseller in Charlotte, NC. He entered into the systems integration and value-added reseller industry in 1995, and in 2005, he started his own company, SiGR Solutions, which provides services and product procurement for businesses of all sizes, including Fortune 1000 companies.

Gene started his IT career in 1992 with Microsoft, earning his MCP in 1993 and MCSE in 1994. He has been the lead consultant and project manager on numerous Active Directory and Exchange migration projects for companies throughout the U.S. When not working, he spends his time with his wife and best friend, Samantha. Gene holds an MBA from Winthrop University and a BSBA in management information systems from the University of North Carolina at Charlotte.

James Yip (MCT, MCITP, MCPD, MCSE, MCDBA, MCSD, MSF Practitioner, OCP DBA) is a consultant for the Asia region of PerTrac Financial Solutions, a global software vendor that produces software for investment professionals. PerTrac Financial Solutions is headquartered in New York and has offices worldwide. James is stationed in Hong Kong and is responsible for helping customers install and troubleshoot issues related

to the company's software, which is based on Microsoft technologies such as .NET, Microsoft Exchange Server, and SQL Server.

James is also working as a managing consultant at Eventus Limited, a leading system integration solution and consulting services provider for the Asia region. He is involved as an architect or project manager for various technologies, consulting studies, and implementation projects. He also is working as a part-time training consultant for Microsoft technologies at Kenfil Hong Kong Limited, a leading Microsoft Certified Learning Solution Provider in Hong Kong. In this role, he provides official Microsoft training solutions to corporate customers in the region.

Contents

Chapter 1

Introduction to Microsoft Forefront Security Suite

Solutions in this chapter:

- **Components of the Microsoft Forefront Security Suite**
- **Benefits of Using the Microsoft Forefront Suite**

☑ **Solutions Fast Track**

☑ **Frequently Asked Questions**

Introduction

Forefront is a comprehensive suite of security products that will provide companies with multiple layers of defense against threats. Computer and Network Security is a paramount issue for companies in the global marketplace. Businesses can no longer afford for their systems to go down because of viruses, malware, bugs, trojans, or other attacks.

In the past, companies often underestimated the importance of Computer and Network Security. Companies often failed to allocate adequate financial resources toward implementing and maintaining security in the workplace. There are a growing number of companies now using the Internet as part of their day-to-day operations, and there are new federal laws mandating the implementation of adequate network security practices.

Using the Forefront Security Suite from Microsoft makes sense for many companies. A large percentage of these companies already have Microsoft Infrastructures in place, including Domain Controllers, Exchange Servers, and Vista and XP workstations. The Forefront Security Suite will integrate well with existing Microsoft products and infrastructures. Now, computer and network security are top priorities for many companies, and no longer an afterthought. Microsoft Forefront will help companies be at the forefront of dealing with network- and computer-related security threats.

Components of the Microsoft Forefront Security Suite

Forefront Security Suite is developed from multiple components that operate together in an orchestrated way to protect and provide overall end-to-end security for IT environments. Forefront components easily integrate with each other as well as with third-party solutions enabling depth defense, simplified management, deployment, and security analysis.

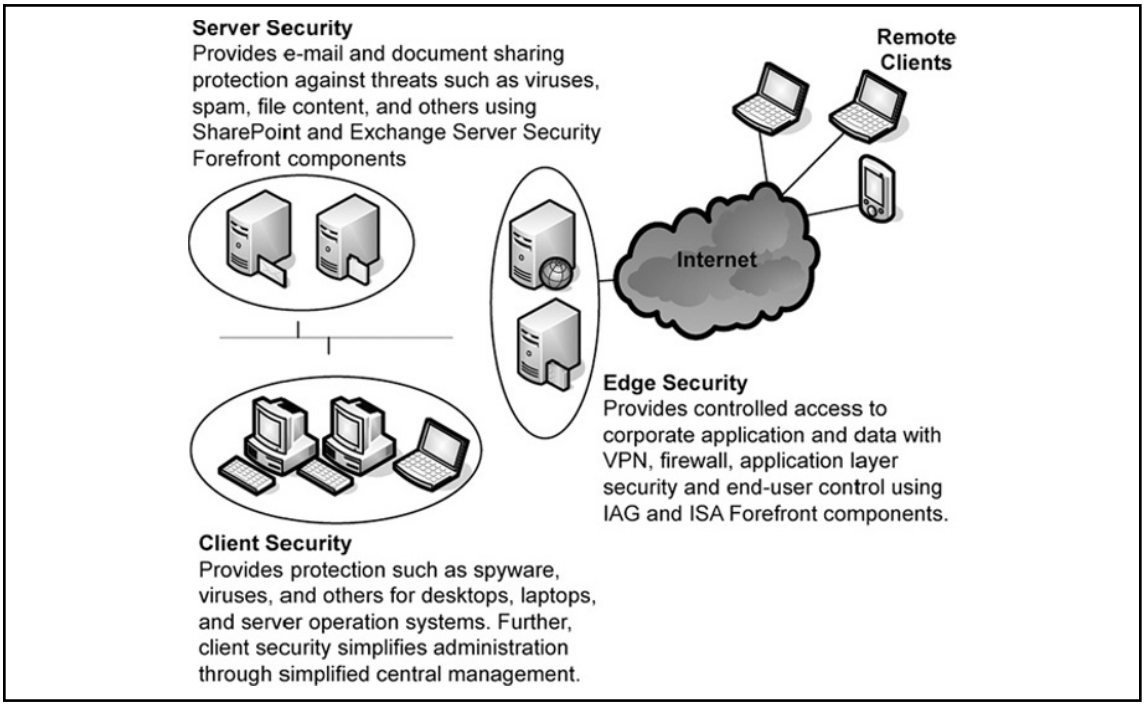
Forefront Security Suite consists of several components, which are separated into three main categories: Client Security, Server Security, and Edge Security. Client Security includes end-user PCs running Microsoft the Business, Enterprise, or Ultimate Editions of Vista, XP Professional, and 2000 Professional. Server Security components include: Security for Exchange Server, Security for SharePoint Server, and Server Security Management Console. Edge Security includes Microsoft ISA Server and Intelligent Application Gateway. Table 1.1 reviews current components and their categories.

Table 1.1 Forefront Client, Server, and Edge Components

Component	Category
Client Security	Microsoft Client Security—Microsoft 2000, Windows XP, Windows Server 2003, Windows Vista—32- and 64-bit OS
Server Security	Security for Exchange Server, Security for SharePoint, Security Management Console
Edge Security	Internet Security and Acceleration Server (ISA), Intelligent Application Gateway (IAG)

A picture tells a thousand words—Figure 1.1 displays the correlation between the three categories for better understanding.

Figure 1.1 The Correlation between Client, Server, and Edge Security



NOTE

For those of you familiar with Antigen products from Microsoft, these products have been rebranded under the new Forefront Security product line. Forefront Security for Exchange Server (formerly Microsoft Antigen for Exchange and Microsoft Antigen for SMTP Gateways), Forefront Security for SharePoint (formerly Antigen for SharePoint), and Forefront Server Security Management Console (formerly Antigen Enterprise Manager) all have been rebranded. Antigen is still used for Instant Messaging security, but it is expected to be rebranded in the near future.

Forefront Security for Clients

Microsoft Forefront for clients enables security for your desktop, laptop, and server operation systems within your environment. It is supported on Windows 2000 Professional and Server, Windows XP Professional, Windows Server 2003, and Windows Vista systems for both 32-bit and 64-bit system environments. Forefront Security for clients helps guard clients against threats such as spyware, rootkits, viruses, worms, and Trojan horses.

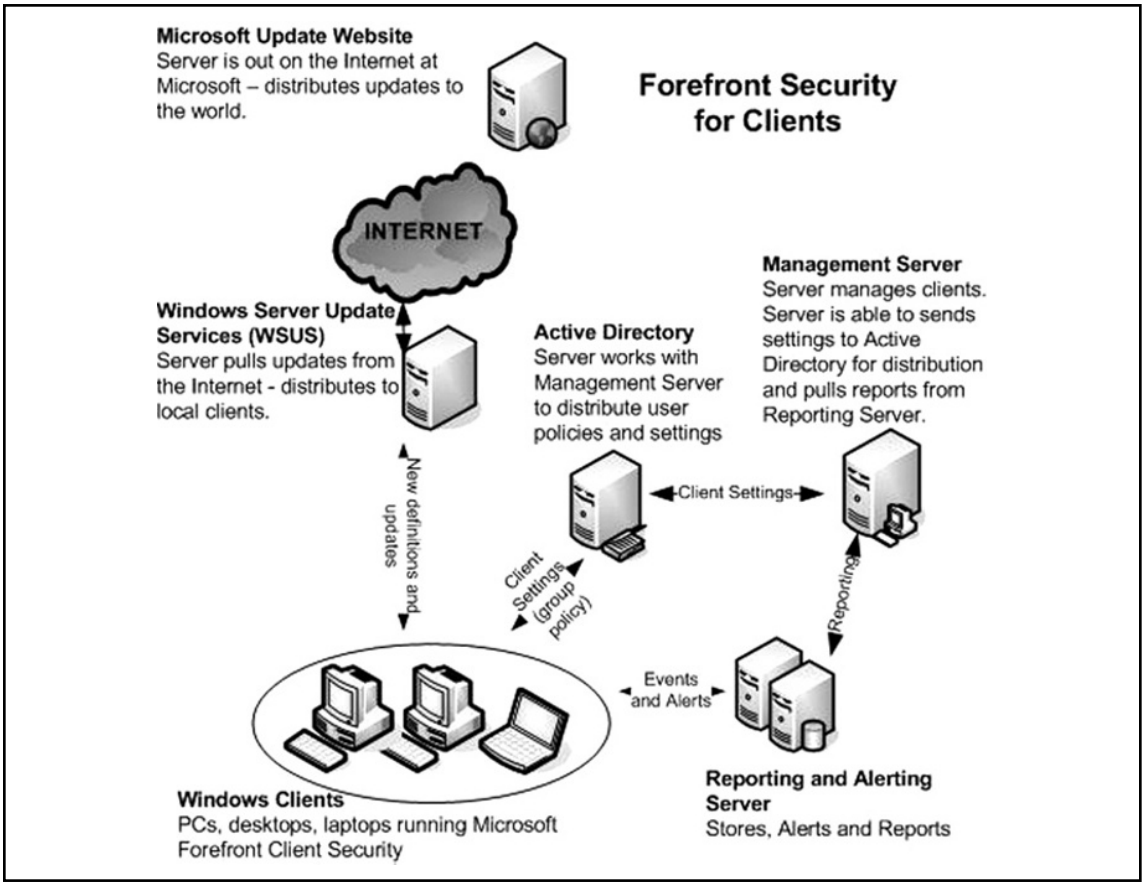
Forefront Security for clients includes several components such as the management server, reporting and alerting servers, and the actual client that is installed on the PC. The management server runs on a central console and all clients can be controlled via this central console. From the central console you can select preconfigured client settings or change specific client settings to best fit your environment as a whole. To simplify the environment and distribution of client policy settings from the management server, Forefront security for clients can use Active Directory Group Policy to propagate policies to clients. The reporting and alerting server accepts alerts from events that happen on the client. The alerting server will then store the alert and alarm you if needed, depending on the severity of the alert. Alerts will be generated by events such as a malware outbreak or a failure to remove a threat. Further, the reporting server has the ability to generate overall or specific reports; these reports can be pulled from your management central console server.

TIP

Forefront Client Security uses database and reporting systems from Microsoft SQL Server, which is included in the purchase of Forefront Client Security. (Customers also have the option of purchasing Forefront Client Security without SQL Server if they have an existing installation.)

Malware definitions and updates for clients can be updated either directly from the Microsoft Update Web site or from your Microsoft Windows Server Update Services (WSUS). WSUS has many benefits; for one, it saves your Internet bandwidth because it has to download updates only once from the Internet and then locally distribute to clients. WSUS enables you to auto-approve the latest updates and signatures or first test and then approve the updates. Figure 1.2 shows how the Forefront security components for clients work together.

Figure 1.2 Forefront Security for Clients



Client Security Features

Forefront Security for clients introduces many new features and benefits. Some of the core features include the integrated anti-virus and anti-spyware that work in real time or on scheduled times to protect individuals from new threats. Filter Manager, which is part of the client security feature, is able to run virus and malware scans before a file is executed, thus giving better protection capability against threats. According to the Microsoft Web site, the Forefront client suite contains the features displayed in Table 1.2. For further features and a detailed updated description visit www.microsoft.com/forefront/clientsecurity/prodinfo/features.mspx.

Table 1.2 Client Features (from Microsoft)

Feature	Description
Integrated anti-virus and anti-spyware engine	Single engine enhances client machines performance and detection capabilities by minimizing end user disruptions.
Real-time protection with the Windows Filter Manager	By using "mini-filter" technology with the Windows Filter Manager, Forefront Client Security is able to scan both virus and spyware files before they run, thus providing better security against spyware and blended threats (for example, spyware that gets on a PC through backdoor Trojans or other means). The other benefit to using the Windows Filter Manager is that end user disruption (system slow-downs) is minimized during real-time scans for both viruses and spyware.
Scheduled and on-demand scans	Quickly scan in-memory processes, targeted directories, and common malware extensibility points to ensure that the client machine is malware-free at all times.
Malware removal and system recovery	The Microsoft anti-malware engine removes malware and runs cleaning scripts to help ensure that the machine is still in a usable state.
Archives and packers scans	Archives and packers are a common way for malware authors to try to hide from anti-malware technologies, but the engine is able to look inside archives and packers and remove infected files.

Continued

Table 1.2 Continued. Client Features (from Microsoft)

Feature	Description
Advanced protection mechanisms	The engine includes advanced protection mechanisms to find user-mode rootkits, polymorphic viruses based on behavior analysis, tunneling signatures, and heuristic detection mechanisms that find new malware and variants.
Compatible with Windows Security Center and Vista Network Access Protection (NAP)	Forefront Client Security provides customers with the ability to see whether Forefront Client Security is running and up to date. IT administrators are able to configure Network Access Protection (NAP) on Windows Server 2008 so that Forefront Client Security-managed machines attempting to connect to the network are checked to ensure that the security agent is up to date and actively protecting clients. If the client machine does not have the Forefront Client Security agent or it is not up to date, the user is not allowed to connect to the network and gets notified within Windows Security Center. If the user installs the security agent for Forefront Client Security with updated signatures, they can then connect to the network.
Central Management System	With one console for simplified client security administration, Microsoft Forefront Client Security saves time and reduces complexity.
Single policy to manage client protection settings	Forefront Client Security helps increase your efficiency through a single policy that configures the anti-spyware, anti-virus, and state assessment technologies for one or more protected computers. New policies are created with preconfigured settings that can be easily tailored to the needs of your environment. Policies also include alert level settings that can be easily configured to specify the type and volume of alerts and events generated by different groups of protected machines.
Integration with Active Directory for policy deployment	Integrating with familiar Microsoft infrastructure saves administrative time and reduced "learning curve." Target policy based on Active Directory organizational units (OUs) and security groups.

Continued

Table 1.2 Continued. Client Features (from Microsoft)

Feature	Description
Integration with WSUS/MU for client deployment	Installing client agents throughout the organization can be a time consuming process for administrators. Deploying client agents using Microsoft Windows Server Update Services (WSUS) reduces administrative workload as these agents get installed automatically through WSUS sync. Administrators do not require additional software or technology, but can leverage their WSUS distribution infrastructure that provides deployment, status, and reporting. Furthermore, as this is an administrative controlled policy, even rogue machines (that is, machines that have removed client agents accidentally or intentionally) receive the client agent automatically when they sync with the WSUS server.
Signature updates for roaming users `	Forefront Client Security provides a failover system for mobile users that allows them to connect to Microsoft Update (MU) to download the latest definition updates if they cannot get access to the corporate network. The administrator will have the ability to centrally manage the opt-in process for managed clients using the Forefront Client Security policy.
Security state assessment checks	The security state assessment (SSA) checks to examine data from the registry, the file system, WMI, IIS metabase, SQL, and more. Those checks allow a security administrator to detect common vulnerabilities in their environment as well as configuration issues that increase their exposure. These checks are a set of risk criteria defining industry best practices and known vulnerabilities. The reporting functionality that includes the security state assessment capabilities in Forefront Client Security enables customers to measure their security risk profile based on security best practices. As a result, customers can focus critical IT resources on the right security issues, and spend less time trying to find and then analyze information from disparate sources.

Continued