# **Release Notes for Forefront Threat Management Gateway Beta 2**

## **Introduction**

These release notes address late-breaking issues and information about the installation, deployment, configuration, and monitoring of Forefront Threat Management Gateway (Forefront TMG). It is very important that you review the information contained in this document before installing Forefront TMG.

## **Installation and deployment issues**

The following sections describe issues that relate to the installation and deployment of Forefront TMG:

* Exchange Edge Installation for E-mail Protection
* Migration
* Workgroup support
* Replication of an Enterprise Management Server
* Disconnected network adapter during installation
* Forefront TMG Management console
* Uninstall
* Getting Started wizard
* Importing arrays

### **Exchange Edge Installation for E-Mail Protection**

In order to use the Forefront TMG E-Mail Protection feature, you must install the Exchange Edge Transport Role of Exchange Server 2007 with Service Pack 1 on the Forefront TMG server, prior to installing Forefront TMG. You can download the evaluation version of Service Pack 1 from the [Microsoft Download Center](http://go.microsoft.com/fwlink/?LinkId=140026).

For installation instructions, see [How to Perform a Custom Installation Using Exchange Server 2007 Setup](http://go.microsoft.com/fwlink/?LinkId=140024) and [How to Install Exchange 2007 in Unattended Mode](http://go.microsoft.com/fwlink/?LinkId=140025).

Following is the syntax you would use for an unattended setup:

<Exchange Edge Drop>\Exchange\setup.com" /mode:Install /role:EdgeTransport /TargetDir:"%ProgramFiles%\Microsoft\Exchange Server"

### **Migration**

Configuration import for migration is supported only from ISA Server 2006 Standard Edition and from the Beta 1 release of Forefront TMG. Do not import a configuration that includes any rules that use the Microsoft Firewall client (UDP) protocol, as this will result in unexpected behavior that cannot be corrected.

When you migrate your configuration from ISA Server 2006, the features provided by ISA Server 2006 Service Pack 1 will not be available.

Migration from ISA Server 2000, ISA Server 2004 Standard Edition, ISA Server 2004 Enterprise Edition, and ISA Server 2006 Enterprise Edition are not supported.

### **Workgroup support**

The installation of Forefront TMG in a workgroup configuration is not supported. Forefront TMG must be a member of a domain.

Ensure that the server is joined to a domain prior to installing Forefront TMG. Joining the server to a domain after installing Forefront TMG will result in unexpected behavior.

### **Replication of an Enterprise Management Server**

You cannot replicate a Forefront TMG Enterprise Management Server to an ISA Server Configuration Storage server, even though this option appears to be supported by the Setup wizard.

### **Disconnected network adapter during installation**

If any network adapter on the server is not connected during the Forefront TMG installation, the intra array IP Address is set to 0.0.0.0. This invalid address disables reporting functionality and interferes with other functionality. To prevent this, all network adapters must be either connected or disabled during the Forefront TMG installation.

To resolve the problem, in Forefront TMG Management open the Server's properties page from the Forefront TMG System node, select the Communication tab and change the Intra Array Communication address to a valid value.

### **Forefront TMG Management console**

Installation of the Forefront TMG Management console is supported only on Windows Vista® and Windows Server® 2008 operating systems.

### **Uninstall**

When you uninstall Forefront TMG, Routing and Remote Access (RRAS) Dynamic Host Configuration Protocol (DHCP) relay agents are removed from the server. If you require RRAS DHCP agents on the server, reconfigure them after you uninstall Forefront TMG.

### **Getting Started wizard**

When you run the Network Setup wizard in the Getting Started wizard, and select to use DHCP for the external network adapter, follow the instructions in <http://support.microsoft.com/kb/841141> to enable access to the DHCP server.

After joining a server to an array managed by a Forefront TMG Enterprise Management Server (EMS), do not run the Getting Started wizard as this will result in unexpected behavior. Run the Getting Started wizard prior to joining the server to the EMS array.

### **Importing arrays**

If you import a configuration that includes an array, the import fails and you receive an error message "Cannot get/set new property/child in mixed enterprise". To avoid this, first create the array in Forefront TMG, and then import the configuration into the array.

## **Configuration and monitoring issues**

The following sections describe issues that relate to the configuration and monitoring of Forefront TMG:

* Network Inspection System
* E-mail
* Internet service provider (ISP) redundancy
* HTTPS Inspection
* Malware Inspection
* Forefront Stirling Integration
* Voice Over IP - Session Initiation Protocol
* VPN Site to Site and Networks with a NAT Relationship
* SQL Server Hotfix

### **Network Inspection System**

#### **Default Response Policy**

In this release, the response policy for new signatures in the Network Inspection System (NIS) is set at deployment to Detect Only, rather than to Microsoft default policy.

To change the response policy:

1. In the Intrusion Prevention System node, on the Tasks pane, select the task Configure Settings.
2. On the Update Configuration tab of the Network Inspection System Properties, in Select the response policy for new signatures, select a different response policy.

Note: You can also change the response policy for a specific signature by double-clicking the signature in the details pane and selecting a response from the drop-down menu.

#### **Signature sets in arrays**

In an array containing more than one server, the NIS signature sets on the array members should be identical. If they are not, and you attempt to use the Version Control user interface, Forefront TMG Management will crash. Note that updated signature sets are stored on the array member’s local file system.

### **E-mail**

#### **E-mail Policy**

This release of Forefront TMG features mail protection functionality that allows you to inspect email traffic for spam, malware and content policy compliance.

In the E-mail Policy node you can configure Forefront TMG to inspect inbound and outbound email traffic using the E-mail Protection wizard. You can also configure the advanced Antispam and Antimalware settings and Content Filtering rules. Mail inspection functionality is implemented by Exchange Edge and Forefront Security for Exchange components, integrated into and managed by Forefront TMG.

##### **Limitations**

* You cannot configure IP Block List Providers or IP Allow List Providers in Forefront TMG Management.
* Setting authentication for Server-To-Server connections and subscribing the Exchange Edge servers to internal Exchange Hub servers do not function in this version.
* Forefront Security for Exchange (FSE) Antispam and Malware updates are not configurable through Forefront TMG, but you can configure them in the FSE administration console or in the Exchange management console.

Warning: Do not subscribe Exchange Edge to internal hub servers manually, as this will cause your configuration to fail.

#### **Existing accepted domain**

In some cases, E-mail Policy may cause your Forefront TMG configuration to fail with the following description:

Description: The accepted domain <name of accepted domain> already exists. The list of executed commands includes: New-AcceptedDomain

To resolve this issue, do the following:

1. Open Microsoft Exchange Server 2007 management shell.
2. Run the following cmdlet:

 Get-AcceptedDomain

You will be presented with a table of domains.

1. Locate the accepted domain name in the first column of the list. Confirm that it is the default domain (labeled True in the Default column).
2. If the domain is the default domain, create another default domain (Forefront TMG will remove it automatically at the end of the procedure, when you apply changes). Use these cmdlets:

 New-AcceptedDomain -DomainName temporary.com -Name temporary.com

 Set-AcceptedDomain -Identity temporary.com -MakeDefault:$true

1. Remove the existing accepted domain with the following cmdlet:

 Remove-AcceptedDomain <name of domain>

 You will be asked to confirm the process.

1. In the Forefront TMG Management console, apply the changes.

#### **SMTP Routes**

##### **Using the New SMTP Route wizard**

Create SMTP routes using the E-mail Protection wizard. The wizard adds two routes, one for internal servers and another for Internet servers. Add additional routes for external mail servers (such as partner companies' servers) using the New SMTP Route wizard.

Do not use the New SMTP Route wizard to create internal SMTP routes. These routes will not be able to route mail to the Internet, and outgoing mail will be rejected with error 5.7.1.

##### **IP address duplication**

When configuring SMTP routes, do not to use the same IP addresses for listeners for different routes. Doing so will cause the configuration to fail with the following error message:

Description: The values that you specified for the Bindings and RemoteIPRanges parameters conflict with the settings on Receive connector "<machine name>\<smtp route name>". A Receive connector must have a unique combination of a local IP address, port bindings, and remote IP address ranges. Change at least one of these values. The list if executed commands includes: New-ReceiveConnector

To resolve the issue, open the SMTP route mentioned in the error message and change the IP address to one that is not used by other SMTP routes.

#### **TLS**

In the E-mail Protection wizard, the External Mail Routing Configuration page includes a TLS Enabled checkbox. This feature is not available in this release. If TLS Enabled is checked, when the changes are applied you will receive this error:

Alert: Configuration of SMTP Protection Failed

If you receive this error, run the E-mail Protection wizard again and leave TLS Enabled unchecked, and then apply the changes.

### **Internet service provider (ISP) redundancy**

Do not use ISP redundancy in a production environment.

### **HTTPS Inspection**

When deploying the HTTPS inspection certificate via Active Directory, use the domain controller's NetBios name rather than the fully qualified domain name (FQDN). For example, if the FQDN is cleveland.contoso.com, the NetBios name is cleveland.

### **Malware Inspection**

Outbound traffic from clients is not inspected for malware in this release.

### **Forefront Stirling Integration**

#### **Forefront Stirling Beta 2 requirement**

Connecting Forefront TMG to a Forefront Stirling server is supported only with the public Beta 2 of Forefront Stirling.

#### **Forefront Stirling response failure**

To support Forefront Stirling responses blocking or limiting client access, Forefront TMG includes two system policy rules. One rule blocks all URLs for any client in the Forefront codename Stirling Blocked Access Computers (Dynamic) computer set. The other rule limits access for any client in the Forefront codename Stirling Limited Access Computers (Dynamic) computer set.

The computer set information is stored on the local server. In an array scenario, the information is also stored on the Enterprise Management Server (EMS). However, array members do not by default have permission to save this information on the EMS. When the attempt to store the information on the EMS fails, the client will be blocked or limited, and there will be no means of changing that client's status.

To avoid this problem, perform this procedure:

1. In Forefront TMG Management, right-click the array node and select Properties.
2. On the Assign Roles tab, click Add, and add each array member as a Forefront TMG Array Administrator, using this syntax for the server name:

 domain\TMGServerName$

Note: If the connection to the EMS fails, or if the EMS server itself fails, the same issue of client categorization can occur. In this scenario, there is no workaround.

#### **Configuring Forefront TMG report availability in Forefront Stirling**

In this release of Forefront TMG the following steps should be performed to enable report availability in Forefront Stirling.

1. Allow Microsoft Operation Manager traffic from Forefront TMG Server to the Stirling Operations Manager Server, which should be deployed in the Internal network. To allow access to the Stirling Operations Manager server:
2. Enable the Forefront TMG System Policy Rule Allow remote monitoring from Forefront TMG to trusted servers, using Microsoft Operations Manager (MOM) Agent.
3. Create a protocol called Microsoft Operation Manager Agent - Installation with the port Range: 5724-5724, TCP, Outbound.
4. Create an access rule allowing traffic on the new protocol from the Local Host to the Internal network.
5. Apply the changes.
6. Allow manual agent installations on the Stirling Operations Manager Server:
7. On the Stirling Operations Manager Server, open the System Center Operations Manager Console.
8. Select Administration=>Settings.
9. In the middle pane, select and open Type:Server Security.
10. Select Review new manual agent installations in pending management view.
11. Install the Forefront Agent package:
12. On the Forefront TMG Server, open a command box with Administrator privilege and run: <Stirling\_CD>:\Client\FSysAgentPackage.exe /mg <StirlingMngGroup> /ms <SOMS\_COMPUTER\_NAME> /l <install\_log\_directory>
* <StirlingMngGroup> is the name of the System Operations Management Group that was configured when installing System Operations Management on the Stirling Operations Manager Server. To find the actual name, open the System Center Operations Manager Console on the Stirling Operations Manager Server and read the management group name in the title bar.
* <SOMS\_COMPUTER\_NAME> is the name of the Stirling Operations Manager Server computer.
* <install\_log\_directory> is the directory for the setup log files.
1. Approve the agent management request on the Stirling Operations Manager Server computer.
2. On the Stirling Operations Manager Server, from the Start menu, open the System Center Operations Manager Console.
3. In the right pane, expand the Administration node, and expand the Device Management node. Select Pending Management.
4. Wait for the management request to appear in the central pane and then right-click Approve.
5. After completing this step, disable the Forefront TMG access rule created in step 1.
6. On the Forefront TMG Server, run the following commands at a command prompt with Administrator privilege:

gacutil /i "%ProgramFiles%\Microsoft ISA Server\Microsoft.Forefront.SecuritySuite.APTAdapter.dll"

%windir%\Microsoft.NET\Framework64\v2.0.50727\RegAsm.exe /codebase "%ProgramFiles%\Microsoft ISA Server\SASRepAdapter.dll"

1. Copy the following text into a text file named TMGAPTA.REG

Windows Registry Editor Version 5.00

 [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Forefront\Forefront System\Client\Agent\Adapters\TMG]

"LoadAdapter"=dword:00000001

"ProgId"="Microsoft.ISA.Reporting.SAS.APTAdapter"

"Namespace"=hex(7):46,00,53,00,79,00,73,00,2e,00,54,00,4d,00,47,00,00,00,00,00

1. On the Forefront TMG Server, open a command line prompt with Administrator privilege and run:

regedit /s TMGAPTA.REG

1. View the Forefront TMG reports.

Forefront TMG reports can be viewed approximately two hours after you complete these procedures. To view the Forefront TMG reports, run Internet Explorer and navigate to http://<StirlingCoreServerName>/reports. On the Web page, click Stirling and then click Threat Management Gateway.

Note: Forefront TMG uninstallation does not unregister the components installed in these procedures. To uninstall these components, run the following commands (before uninstalling Forefront TMG) in a command prompt with administrator privilege:

%windir%\Microsoft.NET\Framework64\v2.0.50727\RegAsm.exe /unregister "%ProgramFiles%\Microsoft ISA Server\SASRepAdapter.dll"

gacutil /u "%ProgramFiles%\Microsoft ISA Server\Microsoft.Forefront.SecuritySuite.APTAdapter.dll"

For information on the Global Assembly Cache Tool (GacUtil), see [MSDN](http://go.microsoft.com/fwlink/?LinkId=140028).

### **Voice Over IP - Session Initiation Protocol**

The following are not supported:

* [iConnectHere](http://www.iconnecthere.com/) Soft phone
* Polycom Sound Point 501 phone
* Microsoft Response Point
* Packet8 interoperation
* Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption Session Initiation Protocol (SIP) messages
* A deployment where the Internal PBX and the internal phones are in separate networks, and the Internal PBX is not a media relay.
* Publishing a PBX on the Internal network and concurrently hosting a PBX on the External network

Other limitations

* Only one registration socket is supported.
* In an array of Forefront TMG servers, registration fault tolerance is not provided. If an array member fails, all of the phones that registered through that member will not receive incoming calls until the phones register again.
* When employing redundant ISP links, registration fault tolerance is not provided. If the Internet connection fails on one of the links, phones that registered through that link will not receive incoming calls until they register again.
* Keep Alive SIP messages that cannot be parsed are blocked.
* The SIP Configuration wizard does not create all of the needed rules when there is a route relationship between the phones and the PBX.
* In a publishing scenario, external clients must receive SIP messages on port 5060.
* In a hold scenario, Forefront TMG closes idle inbound media connections after one minute.
* When a call is initiated from the external network, outgoing media is not received by SIPGate.

### **VPN Site to Site and Networks with a NAT Relationship**

#### **NAT Relationship**

In a VPN site-to-site scenario where the networks have a NAT relationship, traffic will not pass between the sites. The workaround is to create a route relationship between the local and remote sites.

#### **Web traffic**

In a VPN site-to-site scenario, Web traffic will not pass between the sites or networks. To enable traffic in this scenario:

1. Create a new HTTP protocol:
2. In Forefront TMG Management, in the Firewall Policy node, select the Toolbox tab.
3. Click Protocols.
4. Click New, and select Protocol, to start the New Protocol wizard. Follow the wizard instructions to create a new HTTP protocol with these properties:
* Port range = 80
* Protocol type = TCP
* Direction = Outbound
* Web Proxy Filter is not attached to the new protocol.
1. Make sure all Allow rules between the 2 sites use the new HTTP protocol, not the built-in HTTP protocol. For example, you can add a rule that allows all traffic from local site to a remote site for all protocols except the built-in HTTP protocol.

### **SQL Server Hotfix**

This issue concerns Microsoft SQL Server 2005, required for Forefront TMG reporting. To install the SQL hotfix described in KB 954606 follow these steps:

1. Open IIS Manager. From the Start menu, select Run, type InetMgr.exe, and click OK.
2. On the Sites node, if site\_2 is listed, right-click site\_2 and select Remove.
3. On the Default web site node, in the Action click the bindings action. Edit the existing port 8008 binding to listen on port 80, and close the bindings dialog.
4. Run Windows update to install the SQL hotfix. You might need to restart the server.
5. After the hotfix is installed, reconfigure the DefaultWebSite binding to port 8008.
6. Ensure that the service ReportServer$ISARS is running.

## **Copyright information**

Information in this document, including URL and other Internet Web site references, is subject to change without notice and is provided for informational purposes only. The entire risk of the use or results from the use of this document remains with the user, and Microsoft Corporation makes no warranties, either express or implied. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Forefront, SQL Server, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.