Secure Mobile Gateway

2014-03-18 13:37:11 UTC

Contents

Secure Mobile Gateway

XenMobile Secure Mobile Gateway provides fine-grained access control of HTTP ActiveSync requests made by mobile devices against back-end Exchange Client Access Servers (CAS).

Secure Mobile Gateway uses filter-based rules to allow or block access. A particular device client request is evaluated against the organization's rules. The result is a binary state of *allowed*, in which the client is permitted to contact the CAS server, or *blocked*, in which the client request is dropped and access to the CAS is not permitted.

You can also use Secure Mobile Gateway to encrypt email attachments that pass through the Exchange server, to ensure that only users with approved managed devices can view company documents securely and safely on their devices.

About This Release	Contains information about this release, including Secure Mobile Gateway features, components, what's new, and known issues.
System Requirements	Provides system requirements for Secure Mobile Gateway and for the Secure Mobile Gateway Console.
Deploy	Provides deployment information for Secure Mobile Gateway.
Install and Setup	Provides information about how to install Secure Mobile Gateway on either Exchange CAS or a Windows Server 2008 with the Microsoft Forefront Threat Management Gateway (TMG)
Manage	Provides information on choosing a security model for your organization, creating block or allow policies, setting static or dynamic filters, and connecting to Device Manager. This section also provides information about enabling and understanding email attachment encryption.
Monitor	Provides information about enabling Secure Mobile Gateway logging.

About This Release

XenMobile Secure Mobile Gateway 8.5 provides the following capabilities:

- Filter-based rules to allow or block access. XenMobile Secure mobile Gateway evaluates a particular client request against the organization's rules. The end result is a binary state of allowed, in which the client is permitted to contact the Microsoft Exchange 2010 Client Access Server (CAS), or blocked, in which the client request is dropped and access to the Exchange CAS is not permitted. Paired with settings in the Device Manager console, you can prevent Exchange ActiveSync email access to device users based on compliance criteria, such as when a blacklisted app is installed on the device, if the device is jailbroken, and so on.

- A two-tiered filter model. The first tier parses the incoming HTTP requests based on path-specific information. The second tier filters based on user or device specific information. You can configure both tiers.

- Filter rules stored in configuration files. Specific filter rules pertaining to the user accounts and devices in your organization are stored in the gateway's XML configuration files.

- Encryption of email attachments for clients that use the ActiveSync protocol. Attachment encryption is selective based on the properties of the device and file types of attachments.

Key Features

The key features of Secure Mobile Gateway are:

- Access Control of HTTP ActiveSync requests. Secure Mobile Gateway can control the HTTP ActiveSync requests that mobile devices make of Exchange servers. You can build filters in Secure Mobile Gateway that enable you to allow or block user devices based on rules and criteria that you specify. When you set the rules in Secure Mobile Gateway, you can turn on and off the rules in XenMobile Device Manager, which then manages the ability for devices to access email within the organization.

- Attachment encryption. Secure Mobile Gateway supports the encryption of email attachments for user devices that use the ActiveSync protocol. Attachment encryption is selective based on the properties of the device and file types of attachments. You configure Device Manager to control the selection criteria and to dynamically configure Secure Mobile Gateway to perform the encryption.

- Encryption support. The web service interface between Secure Mobile Gateway and Device Manager supports the delivery of encryption keys and criteria.

- Remote configuration. Device Manager controls the baseline and delta intervals used by Secure Mobile Gateway.

- **Logging**. On the Log tab of the Secure Mobile Gateway configuration utility, you can view when the encryption is enabled for a given user device at the request level, in addition to devices that are allowed or blocked.

Known Issues for Secure Mobile Gateway

Known Issues in This Release

- SMG-98: SysLog Redirector doesn't send messages to the SysLog server. The SysLog server must be specified as a DNS address. Dotted IP addresses do not work.

- SWB-63: If you uninstall the Secure Mobile Gateway 8.0.1 or 7.x versions by using the uninstall application, you will see a message prompting you to stop the SysLog service (which does not exist). Click **Retry** or **Ignore** and then proceed with the uninstallation.

- SMG-99: Some Android devices are blocked after a remote wipe. Certain Android devices temporarily send a device ID of "validate" when reestablishing connectivity with ActiveSync after they have been wiped. If you configure Secure Mobile Gateway in Block Mode, you must add the device ID to the Static Allow list to enable the devices to be able to reconnect. By default, this device ID is included in the Static Allow list.

Secure Mobile Gateway System Requirements

Citrix Secure Mobile Gateway is an ISAPI filter that you can deploy on Forefront Threat Management Gateway (Forefront TMG). The product is implemented as a single DLL loaded within the Forefront TMG Server Firewall service or within the Internet Information Services (IIS) service on Microsoft Exchange 2010 Client Access Server (CAS).

Secure Mobile Gateway requires the following minimum system configuration:

Component	Requirement
Computer and processor	733 MHz Pentium III 733 MHz or higher processor. 2.0 GHz Pentium III or higher processor (recommended)
Server	· Forefront TMG 2010 Service Pack 1, Update 1 (recommended) · Exchange 2007 CAS 2007 with IIS 7.0, Exchange 2010 CAS with IIS 7.5 (recommended)
Memory	1 gigabyte (GB)
Hard disk	NTFS-formatted local partition with 150 MB of available hard-disk space
Operating system	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 SP2 (recommended)
Other devices	· Network adapter compatible with the host operating system for communication with the internal network
Display	VGA or higher-resolution monitor

The host computer for Secure Mobile Gateway requires the following minimum available hard disk space:

- Application. 10 -15 MB (100 MB recommended)
- Logging. 1 GB (20 GB recommended)

Deploying Secure Mobile Gateway

Deploying the Secure Mobile Gateway requires performing the following setup tasks:

- Set up listening addresses for the SMG web service
- Configure communication with the Device Manager server (‘config provider’)
- Define local rules that allow you to override rules set in the Device Manager web console

Choosing a Security Model for Secure Mobile Gateway

Permissive Model (Permit Mode)

Establishing a security model is essential to a successful mobile device deployment for organizations of any size. Although it is not uncommon to allow access to a user, computer, or device by default, using some form of protected or quarantined network control, it is not always a good practice. Every organization that manages IT security may have a slightly different or tailored approach to security for mobile devices.

The same logic applies to mobile device security. The vast numbers of mobile devices and types, quantities of mobile devices per user, and the array of operating system platforms and applications available make the very idea of using a permissive model a weak choice. In most organizations the restrictive model will be the most logical choice. However, it will involve some thinking to successfully roll-out the Secure Mobile Gateway security model. Although it is not uncommon to allow access to a user, computer, or device by default, using some form of protected or quarantined network control, it is not always a good practice

The configuration scenarios that Citrix allows for integrating Secure Mobile Gateway with XenMobile Device Manager is as follows:

The permissive security model operates on the premise that everything is either allowed or granted access by default. Only in the case of rules and filtering will something be blocked and a restriction applied. The permissive security model is good for organizations that have a relatively loose security concern about mobile devices and only applies restrictive controls to deny access where appropriate (when a policy rule is failed).

The Restrictive Model (Block Mode)

The restrictive security model is based on the premise that nothing is allowed or granted access by default. Everything passing through the security check point is filtered and inspected, and is denied access unless the rules allowing access are passed. The restrictive security model is good for organizations that have a relatively tight security criterion about mobile devices. The mode only grants access for use and functionality with the network services when all rules to allow access have passed.

To set up a restrictive mode for Secure Mobile Gateway

The following procedure describes how to set up Secure Mobile Gateway successfully with the restrictive mode (block mode). This configuration for Secure Mobile Gateway and XenMobile Device Manager assumes that both are installed and operational and that mobile devices are enrolled with Device Manager and connecting to ActiveSync services properly. Through and understanding the principles of Secure Mobile Gateway Rules, Filters within Device Manager, Static and Dynamic updates for rules, and the enforcement of an Secure Mobile Gateway restrictive Block mode policy, you can implement a secure device management solution with Device Manager and Secure Mobile Gateway.

Understanding how to set the granularity of security policy and apply it correctly from Device Manager and Secure Mobile Gateway is important with regard to global device management for a large set of users or an entire organization. The following example of a best practice restrictive, or blocked policy, for Secure Mobile Gateway will enable the following results:

- All users and devices noted on the static list need to belong to and pass the Device Manager inventory rule in order to gain access through the ActiveSync connection of Secure Mobile Gateway.
- All users with devices that have apps that match the Blacklisted Apps are denied access until the mobile device user removes them manually from the device and, perhaps, the synchronizing application.
- All unmanaged devices by Device Manager are denied access to ActiveSync connections and services until properly enrolled.
- All Android devices with root account access enable are denied access. With device hardware and operating system encryption not fully up-to-speed with other platforms, this policy can help to ensure that no malicious apps or devices can penetrate the Exchange messaging system and possibly more.
- All other devices that were missed by an in-line static and Device Manager dynamic rule or filter to screen acceptable values for devices, users, and applications is allowed or denied access as the closing rule for Secure Mobile Gateway to process. Because this example chose the Static + ZDM Rules: Block Mode, the final outcome of the linear policy scan is to block devices and drop connections until fixed.

1. Open the SMG Controller Configuration utility and then click Gateway Config tab.
2. Next to Policy click Static + ZDM Rules: Block Mode and then click Save.
3. Click the Static Rules tab and then on the Static Allow and Static Deny tabs, enter values for User, DeviceID, DeviceType, or UserAgents.

   Note:

- Values for Static Allow are available in the Device Manager web console or in the Secure Mobile Gateway Log in the configuration utility. For information, see To configure static rules.

- A single entry for a row will only filter on the single value alone. For example, Username alone will only filter based on the single criteria of User.

- A combination entry for a row will filter based on match for the two values. For example, User and DeviceId combined would restrict access to a user and a specific device.

4. Open the Device Manager web console and then click Options from the console banner.

5. Click Secure Mobile Gateway in the left-hand navigation bar.

6. Choose the desired options for the restrictive environment. In this procedure, the following Secure Mobile Gateway options for Device Manager are enabled:

   - Blacklisted Apps. Enabled with a filter set to Deny devices with any matching applications listed in the Blacklist configuration profile.

     Note: To add additional blocking for jailbroken iOS devices later than iOS v4.1, you can add the Cydia application to this list. Jailbroken devices with Cydia components installed are blocked by Secure Mobile Gateway.

   - Unmanaged Devices. Enabled with a filter set to Deny devices that are not enrolled within Device Manager.

   - Rooted Android Devices. Enabled with a filter set to Deny devices that are running in a rooted mode of the Android OS.

7. Click Close to exit the web console settings screen.

Installing Secure Mobile Gateway

You can install Secure Mobile Gateway in one of the following ways. Citrix recommends that you install Secure Mobile Gateway on Windows Server 2008.

- On Microsoft Exchange 2010 Client Access Server (CAS). The installer for the ActiveSync Controller is a Windows Installer .msi file called SmgInstaller.exe. For details, see To install Secure Mobile Gateway on a Microsoft Exchange CAS.

- On Windows Server 2008. To enable the XenMobile Device Manager Exchange email attachment encryption feature, you must configure Microsoft Forefront Threat Management Gateway (TMG) running on Windows Server 2008. You must then install Secure Mobile Gateway on the server running Forefront TMG as an ISAPI plug-in. You use the same SmgInstaller.exe to complete this installation. For details, see Enabling Secure Mobile Gateway Filtering by Configuring Forefront Threat Management Gateway.

To install Secure Mobile Gateway on a Microsoft Exchange CAS

You can install Secure Mobile Gateway on a Microsoft Exchange Client Access Server (CAS). Secure Mobile Gateway is supported on Exchange 2007 CAS and Exchange 2010 CAS. You run the SmgInstaller.exe file to install Secure Mobile Gateway. To do so, double-click SmgInstaller.exe file and then follow the instructions.

Important: To use the Secure Mobile Gateway attachment encryption feature, you must configure Microsoft Forefront Threat Management Gateway (TMG) running on Windows Server 2008. You must then install Secure Mobile Gateway on the server running Forefront TMG as an ISAPI plug-in. For information, see Enabling Secure Mobile Gateway Filtering by Configuring Forefront Threat Management Gateway.

1. Run the 64-bit installation package.
2. A message appears stating that the host is not a TMG server. When prompted to proceed, click Yes.
3. Follow the instructions.
4. When the installation is complete, restart Microsoft Internet Information Server (IIS). Because the Secure Mobile Gateway ISAPI filter runs within the application pool processes of IIS, to ensure than the filter is loaded into these processes, you must restart IIS.

In IIS, do the following:

- Install the ISAPI filter in IIS. In Secure Mobile Gateway, integration of the ISAPI filter is done automatically by the installer, so no manual configuration of IIS is required.
- Configure Secure Mobile Gateway for IIS by running the Secure Mobile Gateway controller configuration. Click the Path Filters tab, click Edit, change the Http Path from Microsoft-Server-ActiveSync to Microsoft-Server-ActiveSync/default.eas and then click Save.

To uninstall Secure Mobile Gateway

Citrix recommends that you use the SmgInstaller.exe file to uninstall or repair Secure Mobile Gateway.

1. Double-click the SmgInstaller.exe file.
2. Select Uninstall and then click OK.
3. If you are uninstalling Secure Mobile Gateway from Windows Server running Microsoft Forefront Threat Management Gateway (TMG), a message appears noting that TMG firewall rule updates don't take effect immediately. Click OK and then click Close.

Managing Secure Mobile Gateway

You can use Secure Mobile Gateway to build access control rules to either allow or block access to ActiveSync connection requests from managed devices based on device status, app blacklists or whitelists and a host of other compliance conditions. Using the Secure Mobile Gateway Controller Configuration utility, you can build dynamic and static rules that enforce corporate email policies, allowing you to block those users in violation of compliance standards. You can also set up email attachment encryption so that all attachments that pass through your Exchange server to managed devices are encrypted and only viewable on managed devices by authorized users.

Configuring Secure Mobile Gateway

You can configure Secure Mobile Gateway to selectively block or allow ActiveSync requests based on the following properties: Active Sync Service ID, Device type, User Agent (device operating system), Authorized user, and ActiveSync Command.

The default configuration supports a combination of static and dynamic groups. You maintain *Static groups* by using the SMG Controller Configuration utility. The static groups may consist of known categories of devices, such as all devices using a given user agent. *Dynamic groups* are maintained by an external source called a Gateway Configuration Provider and collected by Secure Mobile Gateway on a periodic basis. XenMobile Device Manager is Gateway Configuration Provider and can export groups of allowed and blocked devices and users to Secure Mobile Gateway.

A *policy* is an ordered list of groups where each group has an associated action (allow or block) and a list of group members. A policy may have any number of groups. Group ordering within a policy is important because when a match is found the action of the group is taken, and subsequent groups are not evaluated.

A *member* defines a way to match the properties of a request. It can match a single property (such as device ID), or multiple properties (such as device type and user agent).

Configuring the Secure Mobile Gateway XML File

Secure Mobile Gateway uses an XML configuration file to guide its actions. Among other entries, the file specifies the group files and associated actions the filter will take when evaluating HTTP requests. By default, the file is named config.xml and can be found at the following location: ..\Program Files\Citrix\Secure Mobile Gateway\config\.

GroupRef Nodes

The GroupRef nodes define the logical group names - by default, the AllowGroup and the DenyGroup.

Note: The order of the GroupRef nodes as they appear in the GroupRefList node is significant.

The id value of a GroupRef node identifies a logical container or collection of members that are used for matching specific user accounts or devices. The action attributes specifies how the filter will treat a member that matches a rule in the collection. For example, a user account or device that matches a rule in the AllowGroup set will "pass" (be allowed to access the Exchange CAS), while a user account or device that matches a rule in the DenyGroup set will be "rejected" (not allowed to access the Exchange CAS).

When a particular user account/device or combination meets rules in both groups, a precedence convention is used to direct the request's outcome. Precedence is embodied in the order of the GroupRef nodes in the config.xml file from top to bottom. The GroupRef nodes are ranked in priority order. Thus, the nodes shown in the figure above (which depicts the default order) are such that rules for a given condition in the Allow group will always take precedence over rules for the same condition in the Deny group.

Group Nodes

Additionally, the config.xml defines Group nodes. These nodes link the logical containers AllowGroup and DenyGroup to external XML files. Entries stored in the external files form the basis of the filter rules.

Note: In this release, only external XML files are supported.

The default installation implements two XML file in the configuration - allow.xml and deny.xml.

Secure Mobile Gateway Policy Modes

Secure Mobile Gateway can run in the following six modes:

- Allow All. This policy mode will grant access for all traffic passing through Secure Mobile Gateway. No other filtering rules are used.
- Deny All. This policy mode will block access for all traffic passing through Secure Mobile Gateway. No other filtering rules are used.
- Static Rules: Block Mode. This policy mode will execute static rules with an implicit deny or block statement at the end. Devices that are not allowed or permitted via other filter rules will be blocked by Secure Mobile Gateway.
- Static Rules: Permit Mode. This policy mode will execute static rules with an implicit permit or allow statement at the end. Devices that are not blocked or denied via other filter rules will be allowed through Secure Mobile Gateway.
- Static + ZDM Rules: Block Mode. This policy mode will execute static rules first, followed by dynamic rules from Device Manager with an implicit deny or block statement at the end. Devices are permitted or denied based on defined filters and Device Manager rules. Any devices that do not match on defined filters and rules are blocked.
- Static + ZDM Rules: Permit Mode. This policy mode will execute static rules first, followed by dynamic rules from XenMobile Device Manager with an implicit permit or allow statement at the end. Devices are permitted or denied based on defined filters and Device Manager rules. Any devices that do not match on defined filters and rules are allowed.

The Secure Mobile Gateway process permits or blocks for dynamic rules based on unique ActiveSync IDs for iOS and Windows-based mobile devices received from Device Manager. Android devices differ in their behavior based on the manufacturer and some do not readily expose a unique ActiveSync ID. To compensate, Device Manager sends user ID information for Android devices to make a permit or block decision. As a result, if a user has only one Android device, permits and blocks function normally. If the user has multiple Android devices, all the devices are allowed since Android devices cannot be definitively differentiated. The gateway can still be configured to statically block these devices by ActiveSyncID, if they are known, and can also be configured to block based on device type or user agent.

To specify the policy mode, in the SMG Controller Configuration utility, do the following:

1. Click the Path Filters tab and then click Add.
2. In the Path Properties dialog box, select a policy mode from the Policy drop-down list and then click Save.

You can review rules on the Policies tab of the configuration utility. The rules are processed on Secure Mobile Gateway from top to bottom. The active policy is displayed with green checkmark, while the rules that are not active show a red circle with a line through it. To

refresh the screen and see the most updated rules, click Refresh. The ordering of rules can be modified in the config.xml file.

To test rules, click the Simulator tab. Specify values in the fields. These can also be obtained from the logs. Click Simulate. A result message will appear specifying Allow or Block.

To configure a connection to XenMobile Device Manager

Secure Mobile Gateway communicates with XenMobile Device Manager and other remote configuration providers through secure web services.

1. In the SMG Controller Configuration utility, click the Config Providers tab and then click Add.

2. In the Config Providers dialog box, in Name, enter a user name that will be used for basic HTTP authorization with the Device Manager web server and has administrative privileges.

3. In Url, enter the Web address of the Device Manager GCP, typically in the format https://ZdmHost/zdm/services/MagConfigService. The MagConfigService name is case sensitive.

4. In Password, enter the password that will be used for basic HTTP authorization with the Device Manager web server.

5. In Managing Host, enter the Secure Mobile Gateway server name.

6. In Baseline Interval, specify a time period for when a new refreshed dynamic ruleset is pulled from Device Manager.

7. In Delta interval, specify a time period for when an update of dynamic rules is pulled.

8. In Request Timeout, specify the server request timeout interval.

9. In Config Provider, select if the config provider server instance is providing the policy configuration.

10. In Events Enabled, enable this option if you want Secure Mobile Gateway to notify Device Manager when a device is blocked. This option is required if you are using Secure Mobile Gateway rules in any of your Device Manager Automated Actions.

11. Click Save and then click Test Connectivity to test gateway to configuration provider connectivity . If the connection fails, check that the local firewall settings allow the connection or contact the Device Manager administrator.

12. When the connection succeeds, clear the Disabled check box and then click Save.

When you add a new configuration provider, Secure Mobile Gateway automatically creates one or more policies associated with the provider. These policies are defined by a template definition contained in config\policyTemplates.xml in the NewPolicyTemplate> section. For each Policy element defined within this section, a new policy is created. The operator may add, remove, or modify policy elements provided that the policy element conforms to the schema definition, and that the standard substitution strings (enclosed in braces) are mot modified. Next, add new groups for the provider and update the policy to include the new groups.

To import a policy from Device Manager

1. In the SMG Controller Configuration utility, click the Config Providers tab and then click Add.

2. In the Config Providers dialog box, in Name, enter a user name that will be used for basic HTTP authorization with the Device Manager web server and that has administrative privileges.

3. In Url, enter the Web address of the XenMobile Device Manager Gateway Configuration Service (GCP), typically in the format https://xdmHost/xdm/services/MagConfigService. The MagConfigService name is case sensitive.

4. In Password, enter the password that will be used for basic HTTP authorization with the Device Manager web server.

5. Click Test Connectivity to test gateway to configuration provider connectivity . If the connection fails, check that your local firewall settings allow the connection, or check with your administrator.

6. When a connection is successfully made, clear the Disabled check box and then click Save.

7. In Managing Host, leave the default DNS name of the local host computer. This setting used to coordinate communication with Device Manager when multiple Forefront Threat Management Gateway (TMG) servers are configured in an array. For details, see Configuring Multiple Instances of Secure Mobile Gateway in a Threat Management Gateway Array.

After you save the settings, open the GCS.

To configure static rules

You configure static rules on Secure Mobile Gateway by using the SMG Controller Configuration utility. You must enter static rules with values that are read by the ISAPI filtering of the ActiveSync connection HTTP request. Static rules enable Secure Mobile Gateway to permit or block traffic by the following criteria:

- User. Secure Mobile Gateway uses the authorized user value and name structure that was captured during device enrollment. This is commonly found as domain\username as referenced by the server running XenMobile Device Manager connected to Active Directory via LDAP. The Log tab within the Secure Mobile Gateway configuration utility will show the values that are passed through Secure Mobile Gateway if the value structure needs to be determined or is different.

- Deviceid (ActiveSyncID). Also known as the ActiveSyncID of the connected device. This value is commonly found within the specific device properties page in the Device Manager web console. This value can also be screened from the Log tab in the Secure Mobile Gateway configuration utility.

- DeviceType. Secure Mobile Gateway can determine if a device is an iPhone, iPad or other device type and permit or block based on that criteria. As with other values, the SMG Controller Configuration utility can reveal all connected device types being processed for the ActiveSync connection.

- UserAgent. Contains information on the ActiveSync client that is utilized. In most cases, the value specified corresponds to a specific operating system build and version for the mobile device platform.

The SMG Controller Configuration utility running on the server always manages the static rules.

To add a static rule

1. In the SMG Controller Configuration utility, click the Static Rules tab and then click Add.

2. In the Static Rule Properties dialog box, specify the values that you want to use as criteria. For example, you can enter a user to allow access by entering the user name (for example, `AllowedUser`, and clearing the Disabled check box.

3. Click Save. The static rule is now in effect. Additionally, you can use regular expressions to define values, but you must enable the rule processing mode in the config.xml file.

To configure dynamic rules

Dynamic rules are defined by device policies and properties in XenMobile Device Manager and can trigger a dynamic Secure Mobile Gateway filter based on the presence of a policy violation or property setting. The Secure Mobile Gateway filters work by analyzing a device for a given policy violation or property setting and if the device meets the criteria, the device is placed in a Device List. This Device List is neither an allow list or a block list. It is a list of devices that meet the criteria defined. The following configuration options enable you to define whether you want to allow or deny the devices in the Device List by using Secure Mobile Gateway.

Note: These dynamic rules must be configured on the Device Manager web console.

1. Open the Device Manager web console and then click Options from the console banner.
2. In the left-hand navigation, click Mobile Configuration and then click Secure Mobile Gateway.
3. In the Enable column, select the check boxes for the filters that you want to enable and then select either the Allow or Deny check box. For more information, see To configure static rules.

Choosing Secure Mobile Gateway Filters

Secure Mobile Gateway filters work by analyzing a device for a given policy violation or property setting. If the device meets the criteria, the device is placed in a Device List. This Device List is neither an allow list or a block list. It is a list of devices that meet the criteria defined. The following filters are available for Secure Mobile Gateway within XenMobile Device Manager.

- Blacklisted Apps. Allows or denies devices based on the Device List defined by Blacklist policies and the presence of blacklisted apps.
- Whitelisted Apps only. Allows or denies devices based on the Device List defined by Whitelist policies and the presence of non-whitelisted apps.
- Unmanaged Devices. Creates a Device List of all devices in the Device Manager database. The Mobile Application Gateway needs to be deployed in a Block Mode.
- Rooted Android /Jailbroken iOS Devices. Creates a Device List of all devices flagged as rooted and allows or denies based on rooted status.
- Out of Compliance Devices. Allows you to deny or allow devices that meet your own internal IT compliance criteria. Compliance is an arbitrary setting defined by the device property named Out of Compliance, which is a Boolean flag that can be either True or False. (You can create this property manually and set the value, or you can use Automated Actions to create this property on a device if the device does or does not meet specific criteria.)
    - Out of Compliance = True. If a device does not meet the compliance standards and policy definitions set by your IT department, the device is out of compliance.
    - Out of Compliance = False. If a device does meet the compliance standards and policy definitions set by your IT department, the device is compliant.
- Noncompliant password. Creates a Device List of all devices that do not have a passcode on the device.
- Revoked Status. Creates a Device List of all revoked devices and allows or denies based on revoked status.
- Inactive devices. Creates a Device List of devices that have not communicated with Device Manager within a specified period of time and are thus considered inactive and allows or denies the devices accordingly.
- Anonymous Devices. Allows or denies those devices that are enrolled in Device Manager but the user's identity is unknown. For example, this could be a user who was enrolled but their Active Directory password is expired, or a user who enrolled with unknown credentials.
- Implicit Allow / Deny. Creates a Device List of all devices that do not meet any of the other filter rule criteria and allows or denies based on that list. The Implicit Allow/Deny option ensures that the Secure Mobile Gateway status in the Devices tab is enabled and shows Secure Mobile Gateway status for your devices. The Implicit

Allow/Deny option also controls all of the other Secure Mobile Gateway filters that have not been selected. For example, Blacklists Apps will be denied (blocked) by Secure Mobile Gateway, whereas all other filters will be allowed because the Implicit Allow/Deny option is selected to Allow.

Secure Mobile Gateway Policies and Rules

You configure ActiveSync policies and rules to allow or deny access to all users, user groups, individual users, all devices, device types, individual devices, or device user agent strings. The default Secure Mobile Gateway configuration includes a number of basic policies that you can view on the Policies tab of the configuration utility.

Secure Mobile Gateway uses filter-based rules to allow or block access. A particular client request is evaluated against the organization's rules with the end result being a binary state of allowed (the client is permitted to contact the CAS server) or blocked (the client request is dropped and access to the CAS is not permitted).

Secure Mobile Gateway uses a two-tiered filter model. The first tier parses the incoming HTTP requests based on path-specific information, and the second tier filters based on user and/or device specific information. You configure filters in XenMobile Device Manager. Specific filter rules pertaining to the user accounts and devices in your organization are stored in the Secure Mobile Gateway XML configuration files.

To configure custom policies by editing the Secure Mobile Gateway XML file

You can view the basic policies in the default configuration on the Policies tab of the configuration tool. If you want to create custom policies, you can edit the XML configuration file (config\config.xml).

1. Find the PolicyList section in the file and add a new Policy element.
2. If a new Group is also required, such as an additional static group or to support an additional GCP, add the new Group element to the GroupList section.
3. Optionally, you can change the ordering of Groups within an existing Policy by rearranging the GroupRef elements.

Enabling Secure Mobile Gateway Filtering by Configuring Forefront Threat Management Gateway

To enable Secure Mobile Gateway to perform the XenMobile Device Manager Exchange email filtering and blocking features, you configure Microsoft Forefront Threat Management Gateway (TMG) running on Windows Server 2008. You then install Secure Mobile Gateway on the server running Forefront TMG as an ISAPI plug-in. The installer for the Secure Mobile Gateway is a Windows Installer .msi file that will place all the necessary components on the server.

After installation, you create a firewall policy access rule on Forefront TMG to allow Secure Mobile Gateway to connect to Device Manager and then request and retrieve the dynamic rules, restrictions, and device information managed Device Manager. You configure a new access rule by using a wizard in the management console for Forefront TMG.

When you configure the access rule, in Forefront TMG, be sure to configure the following settings:

- Give the rule a name that references the purpose of the rule, such as XenMobile Device Manager.
- Select Allow as the action to take when the rule conditions are met.
- Add the HTTPS protocol.
- Add the Local Host network as the access rule source.
- Create a destination for the rule by creating a computer set with a recognizable name, such as XenMobile computers.
- Make sure the All Users object is included in the user sets.

After you configure and apply the rule, do the following to connect the Secure Mobile Gateway with the Device Manager server.

1. From the Start menu, click All Programs and then click SMG Controller Configuration.
2. On the Config Providers tab, click Add and then enter the Web address for the Device Manager in the following format: https://zdmserver.domain.com/zdm/services/MagConfigService and the administrator account credentials for Device Manager.

   Note: Be sure to enter the fully qualified domain name (FQDN) or DNS name of the server used by the devices and web console connections. For SSL connections, you must use the DNS name of the server (and not the IP address).

3. Select the Events Enabled check box if you want to able Device Manager Automated Actions, which sends a notification when Secure Mobile Gateway blocks a user device.

4. Click Test Connectivity to validate that the connection works through the new access rule.

Configuring Multiple Instances of Secure Mobile Gateway in a Threat Management Gateway Array

To configure multiple instances of Secure Mobile Gateway in a Microsoft Forefront Threat Management Gateway (TMG) array, you must install TMG on each server of the array. Configure the instances of the Secure Mobile Gateway to share a common Secure Mobile Gateway configuration.

Configuration Replication

To configure multiple instances, you replicate the config folder across members of the array or share a common config folder. The ISAPI filter itself responds automatically to changes in the contents of the config folder, so it will dynamically reconfigure itself whether the configuration files are changed by replication, or by an update from the Gateway Configuration Service (GCS) in a shared folder.

In either model, one of the servers running Secure Mobile Gateway is designated as the Managing Host of the Device Manager. This server will perform the communication with the server running Device Manager to retrieve policy updates and then commit them to the config folder. The Managing Host property is set in the SMG Controller Configuration utility on the Config Provider tab. When the resulting configuration is replicated or shared, only the GCS of the Managing Host will communicate with the server running Device Manager.

To deploy configuration replication, you must configure a third-party replication product to replicate the config folder from the Managing Host server to all other servers.

Configuration Sharing

Shared configuration is a model for automatically sharing Secure Mobile Gateway state across all members in a TMG array (or IIS cluster). To set up Shared Configuration, a filesystem share must be created that is accessible from all members of the array. Then each array member must be configured to use the share by using the Shared Configuration tab in the SMG Controller Configuration. To deploy configuration sharing, create a network shared folder that accessible by each server. This folder must have permissions that allow read access by the TMG firewall process or IIS service process (typically NT AUTHORITY\NetworkService) read access, and read/write access by the GCS user, and read/write access by any users that will be using the SMG Controller Configuration. Once the shared folder is created, run the SMG Controller Configuration utility on each member of the array, select the Configuration Store tab, and change the configuration folder. Secure Mobile Gateway automatically detects changes in configuration or configuration location, so no restart of services is required.

The share must have the following permissions:

- ReadWrite access from any user that runs the SMG Controller Configuration utility
- ReadWrite access from the user of the XenMobile Gateway Configuration service (default user is LocalService)
- Read access from the user of the XenMobile Gateway Log Redirector service (default user is LocalService)
- Read access from the Secure Mobile Gateway ISAPI filter. This filter is the TMG Firewall Service on TMG (user defaults to NETWORK_SERVICE) or Wpw3.exe on IIS (user defaults to an IIS AppPool user)

An alternative to shared configuration is to automate replicate the Secure Mobile Gateway config folder to the other members of the array. Replication is the responsibility of the administrator. Secure Mobile Gateway automatically detects and responds to any changes to .xml files in the config folder.

How Attachment Encryption Works

Secure Mobile Gateway supports the encryption of email attachments for user devices that use the ActiveSync protocol. Attachment encryption is selective based on the properties of the device and file types of attachments. You configure XenMobile Device Manager to control the selection criteria and to dynamically configure Secure Mobile Gateway to perform the encryption.

Important: Due to limitations of Microsoft IIS, attachment encryption is only supported on Forefront Threat Management Gateway (TMG) platforms.

Attachment encryption is a system, not an isolated feature of Secure Mobile Gateway. Attachment encryption is designed to work with a large number of native and third-party email clients. To work, it requires the participation together of Device Manager, Secure Mobile Gateway, and Device Agents, as follows:

- Device Manager provides *Key Management*, in which Device Manager creates and distributes the key components to both the users devices and to Secure Mobile Gateway.
- Secure Mobile Gateway is responsible for encrypting attachments by monitoring the ActiveSync traffic between user devices and mail servers.
- The Device Agents are responsible for decrypting and providing access to the attachments.

Security Standards

Encrypted attachments are protected by using an industry standard secure container known as PKCS #7. The container provides a cryptographically secure envelope around the attachment data. Such containers can only be decrypted by the mobile device to which the attachment is delivered, and by Secure Mobile Gateway. When attachments are encrypted by Secure Mobile Gateway, the suffix .zsa is appended to the original attachment name, creating a *ZSA container*. The suffix allows the Device Agent, which associates itself with .zsa files, to be automatically invoked when a .zsa file is opened in any email client.

How Attachments Are Enrcrypted

ZSA containers are constructed by Secure Mobile Gateway when email attachments are delivered to the device via ActiveSync. The Device Agent reads the container when the attachment is accessed from within the email client. The content of container is encrypted with a symmetric key generated uniquely for each attachment. The symmetric content key in then encrypted with the public key of each recipient of the ZSA. Any recipient that holds the associated private key can then open and decrypt a ZSA container.

In the XenMobile system, there are two recipients for each ZSA: the targeted device and Secure Mobile Gateway. Secure Mobile Gateway is a recipient because it must be able to decrypt ZSA containers that are forwarded or sent from the devices. To process ZSA containers, Secure Mobile Gateway requires the public key of the device, and the public and private key for itself.

Attachment encryption occurs through the interception and modification of ActiveSync request and response data. As a plug-in within TMG, the Secure Mobile Gateway ISAPI filter intercepts packets and re-aggregates packets into ActiveSync messages in binary xml form (WbXml). The messages are then parsed to determine if encryption is enabled by the configuration. This includes checking that the file criteria defined by Device Manager applies to any attachments referenced by the message. If encryption is selected, the messages are modified. Due to encryption and message aggregation, there is a additional performance cost in terms of CPU and memory use for the TMG server.

Communication Between Secure Mobile Gateway and Device Manager

Secure Mobile Gateway dynamically retrieves configuration updates from Device Manager, including whitelist/blacklist information and encryption keys. Secure Mobile Gateway initiates the protocol by initially requesting a baseline, or a complete set of information about all devices known to Device Manager. Subsequent communication requests a delta, or the set of information that has changed since the last request. In each response, Device Manager alerts Secure Mobile Gateway as to when to send a request for the subsequent delta or baseline (the intervals are configurable within Device Manager). At any point in the protocol, each side may request or force a baseline (for example, if Device Manager or Secure Mobile Gateway restarts).

Encryption File Type Selection Criteria

The criteria for selecting the types of files to be encrypted is configurable within Device Manager, and delivered to Secure Mobile Gateway as to when to send a request for the subsequent delta or baseline (the intervals are configurable within Device Manager). At any point in the protocol, each side may request or force a base. The interface between Device Manager and Secure Mobile Gateway supports defining the selection criteria as a set of rules in which each rule defines a method of matching (for example, all files that end with .doc or .docx) and an outcome (either encrypt or not). The rules are evaluated in order until a match is found. Rules can therefore be created to define general rules and exception rules (for example, all .doc files except my.doc). The selection criteria employed for a given device is viewable in the Policy tab of the SMG Controller Configuration utility.

Note: Device Manager supports a single selection criteria for all devices.

To configure attachment encryption

To configure attachment encryption, you must install Secure Mobile Gateway as an ISAPI plug-in on a Windows Server 2008 that is running Forefront Threat Management Gateway (TMG). For details, see Enabling Secure Mobile Gateway Filtering by Configuring Forefront Threat Management Gateway.

1. In the SMG Controller Configuration, click the Encryption tab.

2. Select Enable Encryption and then click Save.

3. Click the Config Providers tab, add an entry for Device Manager and then select the Enable Encryption check box. Device Manager remotely configures the required rules and encryption keys. You can view the rules on the Policies tab.

   Note: On the Log tab, in the Secure column, devices that enabled for encryption appear with a check mark.

How Key Management Works

There are two components that make up key management in XenMobile:

- Device key management within the XenMobile Device Manager. Device Manager is responsible for management of device keys. This includes the generation and revocation of a key pair unique to each device and the distribution of the key pair to the device, as well as distribution of the associated public key to Secure Mobile Gateway. When a device is successfully enrolled, a key pair is generated and delivered to the device. The device's public key and its associated ActiveSync Device ID is then delivered to Secure Mobile Gateway, along with whitelist and blacklist rules governing email access. The serial number of the device public key is viewable by using the Policy tab in the Secure Mobile Gateway configuration utility. You can configure Device Manager so that email access is not enabled until the device is enrolled.

- Secure Mobile Gateway key management. Secure Mobile Gateway is responsible for periodically initiating communication with Device Manager to retrieve configuration information pertaining to attachment encryption, including device public keys and their associated ActiveSync Device IDs. The device public keys are stored in the Secure Mobile Gateway config folder in an .xml file associated with the Device Manager.

  Secure Mobile Gateway is also responsible for generating its own set of assymetric keys so that it can be a recipient of ZSA containers. These keys are cryptographically protected and stored in the Secure Mobile Gateway KeyStore (ArraySharedData.xml). An initial key is automatically created when attachment encryption is first enabled on the Encryption tab of the configuration utility. Secure Mobile Gateway uses the most recent key in its KeyStore to create ZSA containers, and may use any of the keys in the KeyStore for decrypting (because attachment containers may have been created with earlier keys). A single key is sufficient for normal operation. If you want to create a new key, you use the GenerateKey.bat script in the product install directory.

Note: In Forefront Threat Management Gateway (TMG) array configurations, the Secure Mobile Gateway KeyStore must be shared by all members of the array. The recommended way to enable this functionality is to configure Secure Mobile Gateway to use the Shared Configuration model, in which the config folder is shared by all array members. If you do not use Shared Configuration, the ArraySharedData.xml file must be replicated to the config folder of each member of the cluster whenever it is modified.

Monitoring Secure Mobile Gateway

The Secure Mobile Gateway SMG Controller configuration utility provides detailed logging that you can use to view all traffic passing through your Exchange sever that is either allowed or blocked by Secure mobile Gateway.

Enabling Secure Mobile Gateway Logging

Secure Mobile Gateway logs the following information:

- Incoming ActiveSync traffic. Under the Secure column, all devices that are enabled for encryption are selected.
- Firewall results of incoming requests. You can sort entries by time, action (allow or deny), or URL match by using a regular expression.

To review logs for Secure Mobile Gateway, in the SMG Controller Configuration utility, click the Logs tab. Specify a data range and actions that you want to query and then click Go.

You can configure the total disk space available for use by log files in Logging.MaxTotalDiskSpaceMB by changing Logging.MaxTotalDiskSpaceMB>.