Project Rapid Staging

Rapid Staging

Requirements Document

Document Information	
Author	Johnni A Lee
File	Rapid_Staging_Requirements.docx
Last Updated	8/16/2012 3:25 PM
Status	Seeking approval
Completion Target	TBD

Project Team

Role	Responsible Person
Project Sponsor	--
Project Champion	--
Product Manager	Johnni A
Engineering Project Lead	--
IT Project Lead	--
IT	--

This Document

1.1 Summary

Watchguard is known to deliver best in class, easy to use, security appliances. We aim to deliver appliances with world-class manageability, while allowing customers to become secure much more quickly and efficiently than our competition.
With this in mind there are two areas that could be improved to escalate Watchguard to truly best in class for manageability, and ease of use for less experienced users.

The first offering, called the “Rapid Deployment Model”, will allow large partners to ship an appliance to its final destination and upon first power on contact WG.com for a basic configuration file, as part of the “deployment package”. Then upon reboot alert to the associated WSM Management server, which will then push the production configuration file.

In multibox deployments (MSSP or end-user), it costs extra in time and dollars for the customer to have to stage appliances manually—that is, to activate and configure an appliance—before sending them to their final production environments. Every single large customer or prospect we talk to brings up this issue; solving it is a very high priority. The request, heard regularly and with very little variation across customers, is for a way for new, factory-default appliances to automatically connect to “the cloud” (in this case, www.watchguard.com) to receive a running configuration.

The second offering, called the “Easy Configuration Model”, will allow any partner or customer to predefine a configuration for a serial number, so upon boot, the appliance will be all but ready to protect the customer’s network.

An appliance will be tracked through the serial number and associated with a configuration file, and/or a Management Server IP address.
When the device is plugged in with basic connection it will contact Watchguard.com (“phone home”).

The goal for the each device is to be ready to run in a production environment. To accomplish each device must have the following. 1) Be activated with a feature key 2) Have a configuration file in place. (This could be a basic configuration in the case of rapid deployment and enough credentials to connect to the WSM Management Server). 3) Have an IP address to connect to the Management Server. (This would be optional for easy configuration).
A customer notification email should be sent at the completion of the process, and an explanation of what was done and any issues that were encountered.

Rapid deployment model
Customer does rapid or basic activation through WSM (management server). They associate a single or a set of serial numbers with a WSM Management Server IP address or multiple WSM Management Servers IP addresses. There must be a quick way to upload the data such as a csv file. When the appliance boots up for the first time, it will contact WatchGuard.com and the “Deployment package” will be pushed to the device. The deployment package will include A) a feature Key, B) Management Server IP Address and C) Basic configuration (includes credentials for Management Server).
The customer is notified via a “come alive” email that their device is alive and 1) Has been activated. 2) is ready to be managed by Management Server or 3) Ready to be managed by Management Server and has a configuration or 4) There was a problem which will include an in-depth description of what occurred. We will suggest that they upgrade to the last version of the software and provide a link to the location.
Once the device reboots it will notify the associated WSM Management Server that it is ready. The WSM Management Server will push the production configuration to the device.

A Management Server will be required.

Easy configuration model
Customer visits WatchGuard.com. Using their serial number they go through quick activation of their device. They also complete a basic wizard that will suggest and then build a configuration file.
Alternatively we allow the customer to upload a configuration file. Either the built or the provided configuration file are intended for one time, and then deleted (we will store but time bomb it for 30 days). (Factory default the box will require the user to re-run the wizard) time bomb from first fetch for 30 days
When the appliance boots up for the first time, it will contact WatchGuard.com, to get a Feature Key and a configuration file (the Easy configuration "deployment package".
The customer is notified via a "come alive" email that their device is alive, has been activated and the details about the configuration. We will suggest that they upgrade to the last version of the software and provide a link to the location.
When uploading a configuration file, we won't do any validation that the configuration file is good.

1.2 Objectives

Rapid Deployment
Provide a way for certain partners to supply WatchGuard with an appliance (or list of appliances) via their serial numbers and friendly names. Associate them with WSM Management server IP address, and in the process perform mass activation of the appliances. Consequently when the appliance boots up for the first time, it connects to a WG.com to receive a basic configuration, and upon reboot, its associated WSM Management server will push a full configuration.

Easy Configuration
Provide a way for less technical customers to supply WatchGuard with a serial number, and a retrieve pre-made configuration, which can either be defined interactively at WG or uploaded.

1.3 Audience

This document is intended to provide a centralized set of business and functional requirements. It should be used by involved teams as a starting point for all activities required for this project. The intended audience includes the following WatchGuard teams:

- IT
- Engineering
- Sales
- Marketing
- PT&P

1.4 Project Constraints

Time to deliver is Q412.
Scope is TBD.
Resources are available if needed to deliver full scope by deadline.

1.5 Priorities

Below is a quick summary of the requirement priority definitions.

Priority	Definition
High	Requirement is a "must have" item for the project. At risk high priority items could result in a schedule slide.

Medium	Requirement is a “nice to have” item for the project. At risk medium priority items will be monitored on a case by case basis to determine whether or not the item warrants a slide in the schedule.
Low	Requirement is a “if there is time” item for the project. At risk low priority items would likely be rolled into the next product revision PRD.

1.6 Status

The status property indicates one of four properties.

Status	Definition
Open	Indicates the feature is still under discussion. Implied by a blank status.
Accept	The feature has been accepted as part of the release.
Reject	The feature has been rejected as part of the release and there are no current plans to incorporate it in the future as part of this platform.
Future	The feature will not be included in the release, but may be considered for a future release. A Future feature does not guarantee that it will be accepted in a later release, it only indicates that the feature will be considered for inclusion in future releases or on another platform.

2 Business Rules

2.1 General

These requirements apply to the overall project.

ID	Functions	Priority	Status	Author
2.1.1	Information stored on WG.com private and secure		Open	
2.1.2	All of the transactions in this set of functionality must be secure (https, ssh, etc.)		Open	
2.1.3	An un-activated serial number (appliance with out a feature key) cannot receive any configuration or Management Server address information		Open	
2.1.4	When an appliance is powered on for the first time, it would get a Feature Key first (this will activate the appliance), followed by a configuration file (configuration file could be simple with just a management server, or complex with full settings for proxy, services, etc)			
2.1.5	The feature key, and configuration file as mentioned above are part of a “deployment package”. It’s content will vary depending if it is a Rapid deployment or Easy configuration model. (Management Server address if no configuration is uploaded by the customer)			

2.1.6	The appliance must regularly re-try to fetch a deployment package through the secure portal at WG.com (either via the secure portal or via normal management UI connection to the appliance itself).	???		
2.1.7	When an activated appliance connects to www.watchguard.com, the primary contact on the account that activated the appliance must receive an email from WatchGuard indicating that the appliance has "come alive." This email must indicate whether the appliance 1) It was activated (received a feature key) 2)It has received a configuration and\or Management Server address.		Open	
2.1.8	The "come alive" email will include information about the latest software and provide a link to its location on WG.com			
2.1.9	When the serial number has to be provided at the time of physical delivery of the appliance, this process must be as foolproof as possible. One interesting way to accomplish this would be to use QR codes and smartphone apps, such that the workflow is as follows: 1) Non-technical employee launches the smartphone app; 2) takes photo of QR code with phone; 3) confirms that the data should now be sent to the secure portal at www.watchguard.com		Open	

2.2

2.3

2.4 Rapid Deployment model

These requirements apply to the managed services model for rapid staging

ID	Functions	Priority	Status	Auth or
2.4.1	A WSM Management Server is required. All devices must allow for remote management.			
2.4.2	A serial number is how appliances are tracked and associated to a WSM Management Server. The serial number is also associated to a customer account.			
2.4.3	Rapid activation (mass activation) should be possible in WSM Management Server. A list of appliances and their associated serial numbers are input through WSM Management server, and the system should allow for easy mass input through the interface. The resulting feature key becomes part of the "deployment package".			

2.4.4	In addition the customer may also want to do a smaller quantity of activations, and the system should allow for this also.			
2.4.5	An OS version for the appliance can be associated to a serial number.		Future	
2.4.6	The customer can store multiple WSM Management Server addresses to his account on wg.com (called the "secure portal")			
2.4.7	When the appliance receives its deployment package. It will contain a basic (for security reason) configuration file. The administrator then receives the "come alive" email. Simple instructions should be made available to the customer that describe the basic configuration information and "what happens next".			
2.4.8	When the device reboots it will notify the associated WSM Management server that it is ready for the production configuration file. The WSM Management Server then pushes the configuration to the device.			
2.4.9	When the administrator logs in to his account on www.watchguard.com, he must see the IP addresses from which his appliances have connected. This will help him connect to the devices to manage them (assuming their configurations permit remote management).		Open	

2.5 Easy Configuration Model - Jumpstart

These requirements apply to the easy configuration model for rapid staging

ID	Functions	Priority	Status	Auth or
2.5.1	The customer can choose an appropriate configuration from a premade set of configuration files. A decision tree model will be available to allow for a suggested model		Open	
2.5.2	A more advanced wizard will be provided to create a "from scratch" configuration		Future	
2.5.3	The administrator must be able to associate an appliance serial number with a configuration.		Open	
2.5.4	The appliance must connect to www.watchguard.com as soon as it first gains Internet connectivity. If it has been activated, it then downloads Its "deployment package".		Open	

2.5.5	The customer can associate any valid activated serial number with a configuration or Management Server address on the secure portal		Open	

2.6 Easy Configuration Model - Custom

2.6.1	The customer can store multiple configuration files and to his account on wg.com (called the "secure portal")		Future	
2.6.2	The customer will have the option to backup configurations to customer's account in the cloud. Admin can then view and pick a backup configuration to restore, to diff their configuration, etc.		Future	

3 Functional Requirements

3.1 General

ID	Functions	Priority	Status	Author
1.	eth0 must be able to obtain IP address via DHCP		Open	
2.	www.watchguard.com must be reachable via eth0		Open	
3.	eth0 must be configured as WAN interface in the to-be-deployed configuration, so the box can continue to be connect to internet after applying the configuration		Open	
4.	Upon boot, if the appliance is in a "factory default" state, it should attempt to phone home for a Feature Key and configuration information. If the appliance fails to obtain a Feature Key or configuration information, it should continue trying to obtain the Feature Key or configuration information every 5 minutes, or until the appliance is manually configured (e.g. QSW is started). If the appliance successfully obtains a Feature Key, but no configuration information, it should continue trying to obtain configuration information every 5 minutes, or until the appliance is manually configured (e.g. QSW is started).			
5.	Would PPPoE also be doable? Could we add a mechanism by which static IP configuration info could be read from a USB key with			

	a specific file system format from a specific filename in a specific format? Either one of them implies the system is no longer in factory-default configuration when they contact www.watchguard.com. By doing so, we are introducing a new state to the appliance, where the appliance already have a customized configuration, but it still need to contact www.watchguard.com to get configuration. Two issues here: (1) This will probably have non-trivial impact to the whole system. Think about how do we get in and get out of this new state, and what functions should be available and should not be available at this state, what should be done when we transition in and out of this state, etc. This won't fit Wenatchee time frame. (2) Is such state necessary? Why not just put the entire configuration in the USB and the box boot up to the new configuration. This will be easier and quicker than via cloud. This will be a new feature, too, but should be smaller than adding a new state. The problem is that it bypasses the cloud.			
6.	Upon factory defaulting an appliance and rebooting, the appliance should go through the "rapid staging" steps, again. The behavior should be no different than if the device was fresh out of the box.			
7.	After an appliance has a configuration applied, it should no longer call in for a Feature Key or configuration file.			
8.	Will an administrator be able to deactivate/turn off the phone home capabilities for the retrieval?			
9.	On the website, what will be the process of assigning the configuration file to a device? And in the Managed Products/Detailed view will we need to include the configuration file name associated with a device? If yes, for how long?			

4 Appendix

4.1 Use Cases

1. User opens the Rapid Deployment Dashboard (RDD) through Management Server File Menu Item.
   a. Or appliance context menu in Management Server
   b. Or via URL (pasted into browser or saved as a bookmark)
   c. Or by clicking a URL from the Partner Portal

d. Open questions
    i. What's the official name of the RapidDeployment Dashboard?
    ii. Where on the Partner Portal should the link be placed?

2. User logs in with portal credentials

3. Since this is the very first login to the dashboard,
    a. Appliances to Deploy table is empty
    b. Deployed appliances table is empty
    c. Associated Management Server Table

4. Since no activation or deployment can occur without associating at least one Management Server with the Rapid Deployment Dashboard, the user associates a Management Server with this account in the RDD.
    a. Here are the steps
        i. Open Management Server and select "Register Management Server with the cloud"
        ii. Enter portal credentials
        iii. Store Management Server's credentials in the cloud
            1. Management Server IP Address
            2. Public Cert
            3. Shared Secret
            4. Admin password
            5. Status Password
    b. This registration occurs over web services and the user is oblivious to it.
    c. If the user registers the same Management Server twice, no error is thrown and the second call just updates the public certificate in the cloud.

5. Since the "Appliances to Deploy" table is empty, the user uploads a CSV file.
    a. CSV import is the only way to get new appliances into the RDD.
    b. CSV mandatory fields
        i. Appliance S/N
        ii. Appliance Friendly Name
            1. This will be assigned as both the LiveSecurity "Friendly Name" during activation and as the "WSM Client ID" when associating an appliance to a Management Server
        iii. Management Server IP address
    c. Error Checking
        i. If one row is wrong in the CSV file, no rows will be imported into the RDD and an error message will inform the user what rows need to be corrected.
        ii. These column headers are required
            1. Appliance Serial Number
            2. Appliance Friendly Name
            3. Management Server IP Address
        iii. Only three columns may be present
        iv. Serial Numbers must be in XXXXXXXXX-XXX format. Serial Numbers without hyphens will be rejected.
        v. Appliance Friendly Names
            1. Must be alphanumeric
            2. Can't contain spaces
            3. Must be less than 30 characters

6. Appliances to Deploy Table now has appliances to manage deployment for.
    a. To add new appliances, a new CSV must be imported.
        i. If the Appliance Serial Number isn't present in the RDD, then new CSV rows are added to the RDD.
        ii. If the Serial Number is present in the RDD the new CSV overwrites the existing row in the RDD.
    b. These rows of appliances can be deleted prior to pressing the Activate Appliances Button.
    c. Once an appliance is activated it moves to the Deployed Appliances table and can no longer be edited.
    d. Appliances from previous sessions persist until they've been
        i. Deleted from the list by the user from the Appliances to Deploy table or
        ii. 30 days have passed since the appliance has called for its boot package when all data related to the appliance has been deleted to the cloud

7. User verifies that all appliances have the desired Management Server IP Address.
    a. If the IP Address included in the CSV isn't correct for a given device, another associated management server can be chosen.

8. User selects appliances and presses the Activate button.
    a. The following sequence occurs in the RDD.
        i. Appliances are bulk activated (with the Friendly Names from the CSV)
        ii. A boot package is generated and stored in the database
        iii. The appliance row is moved to the Deployed Appliances Table in the RDD
        iv. The device is powered on
            1. Feature Keys are applied to the device
            2. The device calls
    b. Error Conditions are communicated to the user with dialog boxes
        i. Activation Failure – S/N already activated
        ii. Activation Failure – Prohibited Country or Company
        iii. Activation Failure – Can't contact LSS
        iv. Boot Package Generation Failure -

9. Appliance is powered up and plugged into the network.
    a. Feature Keys are applied to the device

10. Appliance calls the cloud.
    a. Cloud authenticates appliance using S/N, MAC or Cert.

11. Cloud sends down boot package—which is just a partial config containing:
    a. Friendly Name
    b. Management Server IP
    c. Management Server Public Cert
    d. Shared secret password

12. Appliance calls management server and asks to be managed.
    a. Appliance call includes
        i. Management server Public Cert
        ii. Shared Secret password

iii. Admin password
iv. Status password

b. If Management Server doesn't recognize the appliance that is calling it asking to be managed, Management Server calls the cloud with the S/N of the calling appliance to see if the RDD knows about it.

MS contacts LSS with the following
- Live security Account Credentials
- WSM Client ID/Friendly Name
- MS IP address

Return from LSS
- Shared Secret
- Admin PWD for device
- Status PWD for device

i. If the device isn't recognized it shows up in Management Server's "Unknown" file.

13. Management Server Authenticates appliance and starts managing it.

14. Management Server can push a "Full Configuration" directly to the appliance if desired.

4.1.1 Managed Services Model

A delivery person drops off our appliance at a remote location that has minimum, even zero, regular staff. A non-technical (but authorized) person unpacks and physically installs the appliance, plugs in the electricity and network cables, optionally performs a simple administrative task (could be a web site visit or a phone/text message, or a QR code interaction, and in some cases this step won't be necessary), powers on the appliance, and is then finished.

Then, when all goes well: the appliance comes to life, connects to the Internet, receives its proper configuration and feature key, joins the network of managed appliances, and starts securing the network: all without needing a person's onsite intervention.

If the device fails to connect to the Internet, the on-site person needs a simple diagnostic UI to help understand and remedy the problem.

4.1.2 Easy Configuration Model

Joe wants to add a better security set-up to his small business. He does not know that much about networking, but knows he would like to set a firewall with a UTM bundle. He also know he would like to set up some application filtering to dis-allow the use of Facebook, and other websites that might slow down the network such as YouTube. He orders a WG appliance from CDW.

It will take several days for the appliance to arrive, but he has he serial number and he is anxious to take advantage of WG's easy configuration so that when the appliance arrives all he has to do to be protected is to plug in the device.

He logs into WG.com. He activates the appliance with the serial number, and answers a few questions and to select his configuration file. He is then prompted to enter some specifics about his network, ip addresses and user name and password and then saves the file to his account and its associated serial number.

Friday afternoon Joe is anxious for the weekend. UPS arrives at about 4:30. Joe unpacks his new appliance, plugs it in and connects it to the network. The appliances powers on and in a few minutes re-boots. Joe's network is set-up and he is ready to enjoy his weekend.

RMA—when a device is RMA'd, the serial numbers are changed out in the WatchGuard back-end systems so that the replacement device inherits the same services, features, etc. as the original device. With Unattended Activation in place, the RMA device should phone home and receive its information just as a new device would, the difference being that there is no activation requirement since an RMA device is already "active."
Decommissioned and Recommissioned device—TBD (not a showstopper for initial release). Customer receives new device in box.
They unpack box, turn on power and provide box with external internet access
Device calls home to www.watchguard.com
The www.watchguard.com site recognizes the device as being activated to an account (meaning someone has activated it already.)
When the devices established connection with www.watchguard.com it will:

- Request a feature key
- Check to see if there is an assigned config.xml assigned to it
- Retrieve the IP of the management server, if available

The feature key will be sent to the device
The configuration file will be sent to the device

- If the device does not have the default configuration on it for some reason, does the one assigned to it on the website take precedence?
- Will there be any prompting re: the placement of this configuration file?

The IP of the Management Server will be sent to the device
Everyone is happy and moves on their merry way.

4.2 Appliance States

This functionality imagines the following possible states for the appliance:

ID	Condition	Description	Error State
4.2.1	Unactivated default state	In this state, the appliance has never been activated. The appliance in this state must attempt to receive a DHCP address on eth0; if it succeeds, it then tries to connect to the secure portal to retrieve feature key and configuration or Management Server address. If the device still has not been activated by the customer by the time it achieves Internet connectivity, it continues to re-try at regular intervals (but since it is unactivated, the secure portal does not return anything to it). WatchGuard technical support/customer care and engineering personnel must be able to see evidence of	Non error state

DATE	AUTHOR	REMARKS
August 7, 2012	Lee B	draft
August 15, 2012	Johnni A	Updated with functional section
August 15. 2012	Johnni A	Updated from review, added use cases

		appliances connecting in this state, but no one else should be able to see this information.	
4.2.2	Activated default state	In this state, the appliance has been activated but no configuration or Management Server address has been associated with it. The appliance has a feature key but no configuration file. It continues to connect regularly to the secure portal to check if the customer has associated a configuration or server address with it. The secure portal should send the administrator a one-time notification that the appliance is in this state.	Non error state
4.2.3	Activated configured state	In this state, the appliance is running a customer-generated configuration. This would be the same as the appliance's normal runtime state in production. The secure portal should send the administrator an email notification that the device is in this state (since, if all goes well, this could happen without the administrator lifting a finger after activation).	Non error state
4.2.4	Unactivated default state, no connectivity	In this state, the appliance cannot connect to the Internet. It must display a non-technical error code on the LCD (for appliances with LCDs) indicating that it cannot connect to the Internet. The administrator may have activated the serial number online, but for the appliance, since it has no connectivity, there is no activation.	Error state
4.2.5	Activated default state, bad configuration or Management Server IP	In this state, the appliance was successfully activated and there was a configuration or server address associated with it, but the appliance has not successfully transitioned to the activated configured state. Reasons could be an invalid configuration, a bad Management Server address, failure to properly load the configuration, etc. The appliance should display a non-technical error code on the LCD (for appliances with LCDs) indicating that it could not load a configuration; the secure portal must send a notification to the administrator and must display the error state on the portal when the customer visits the "Manage Products" page	Error state

5 Document Version History