



BOMGAR™

Bomgar Box™

Secure Deployment Guide



# Bomgar Box™ Secure Deployment Guide

## Contents

<b>Introduction .....</b>	<b>1</b>
<b>Overview of Security Features and Secure options .....</b>	<b>1</b>
<b>Symantec Secure Deployment Recommendations .....</b>	<b>2</b>
<b>Symantec Recommended Security Settings .....</b>	<b>7</b>
<b>About Bomgar™ .....</b>	<b>17</b>

## **Introduction**

The purpose of this paper is to provide an overview of the security features and functionality of the Bomgar Box™ remote support appliance and Symantec's recommendations on the best way to securely deploy this product within your infrastructure.

The Bomgar Box™ provides support professionals the ability to resolve Mac and PC remote support incidents through remote control of the end users' systems. Through the use of an appliance-based solution, Bomgar™ is able to traverse firewalls without the need for port forwarding or any firewall changes. In order to insure privacy, all communications travel through an encrypted SSL connection.

The appliance architecture offers clients the ability to choose how and where it is deployed. Additionally, clients may configure the security features such that it complies with applicable corporate policies or regulations. Security features include role-based access control, secure password requirements, and features to give remote support recipients the ability to resume control of their computers.

## **Overview of Security Features and Secure Options**

The Bomgar Box™ provides multiple features designed to insure the security of remote support sessions. Local security functionality exists to insure proper security controls around support representative accounts. Secure communication is provided through the use of standard encryption protocols. Client security is achieved through controls given to the remote support recipient where he or she can determine the level of access a support representative is granted. Furthermore, the remote support recipient can take control of the support session at any time.

The Bomgar Box™ supports account security, and the notion of Least Privilege access, through the use of account-based access controls. The access controls limit the functionality that a given account may have. For example, support desk representatives can be prevented from accessing the recorded support sessions. Through the use of group policies, permissions can be enforced easily across multiple accounts.

The Bomgar Box™ utilizes SSL (Secure Sockets Layer) encryption for screen sharing sessions. The use of 256-bit AES SSL for encrypted sessions meets industry best practice. It is utilized to protect against eavesdropping and session hijacking. The Bomgar Box™ also supports the ability to utilize SSL to secure LDAP directory access and when accessing the appliance's public web interface.

In addition to the security functionality built into the appliance, the Bomgar Box™ places security in the control of the user. At any time during the screen sharing session, the client can take over control of his or her computer and terminate the session sharing by clicking on the large red "X" icon. Furthermore, the Bomgar Box™ allows the remote user to grant various levels of access to his

## Secure Deployment Guide: Bomgar Box™

or her computer. For example, the remote user may authorize the remote support representative to have “view only” access to his or her computer screen.

More details on the specific security functions and Symantec’s recommended settings are provided in the following sections.

### Symantec Secure Deployment Recommendations

#### Bomgar Box™ Deployment Location

The Bomgar Box™ has a network footprint similar to that of a standard web application; all traffic resides on HTTP (TCP port 80) or HTTPS (TCP port 443), and everything is self-contained in a single appliance. A third port, TCP/8200, is utilized in the event that a remote support recipient cannot establish a connection to port 443 on the Bomgar Box™.

Three common deployment locations exist:

- Inside a DMZ
- External Network (no DMZ)
- Internal Network

#### Inside a DMZ

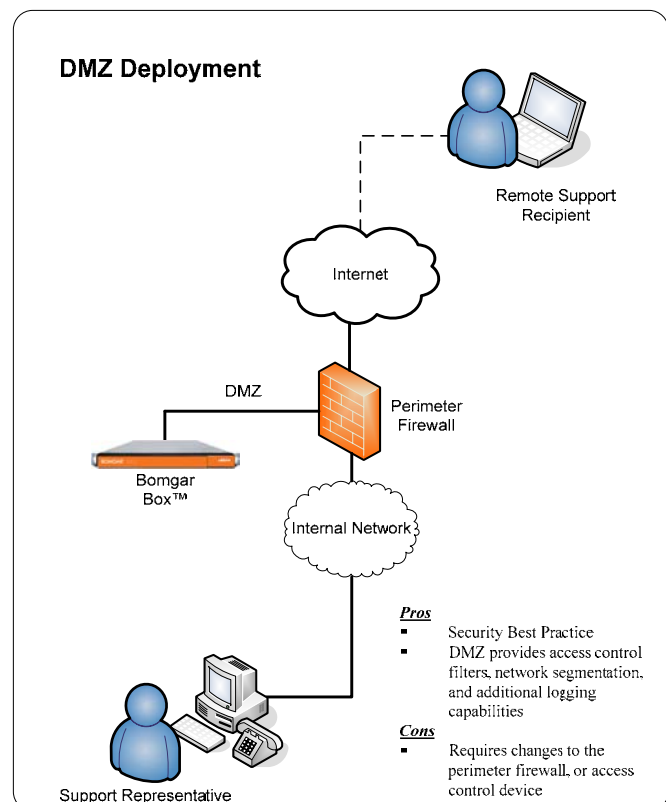
Deploying the Bomgar Box™ appliance into a perimeter-based DMZ segment meets security best practice and is Symantec’s recommended location for the secure deployment of the device. A DMZ, or de-militarized zone, is a network that is protected by access control mechanisms. Access control may be provided by a firewall device, a router or a switch that provides port and address filtering capabilities. The purpose of the DMZ is to limit access to systems that are deployed within it. In the case of the Bomgar Box™, the DMZ will limit connectivity to the device and only allow access to the appropriate ports.

#### Pros

- Security Best Practice
- DMZ provides access control filters, network segmentation, and additional logging capabilities

#### Cons

- Requires changes to the perimeter firewall or access control device



## Secure Deployment Guide: Bomgar Box™

### Firewall Details

When deploying the appliance into a DMZ, the following rules should be opened on the firewall (or other access control device):

Source	Destination	Protocol	Port	Justification
Support Client IP address range -Or- “Any” if clients are Internet-based	Bomgar Box™ IP address	TCP	80	Allow cleartext HTTP access to the device.
Support Client IP address range -Or- “Any” if clients are Internet-based	Bomgar Box™ IP address	TCP	443	Allow encrypted HTTPS access to the device.
Support Client IP address range -Or- “Any” if clients are Internet-based	Bomgar Box™ IP address	TCP	8200	Allow encrypted HTTPS access to the device.

## Secure Deployment Guide: Bomgar Box™

### External Network (No DMZ)

In situations where a DMZ does not exist and is not possible due to technical or business constraints, the Bomgar Box™ may be deployed external to the perimeter firewall. The appliance consists of a hardened operating system and applications that are designed to be directly accessible.

#### Pros

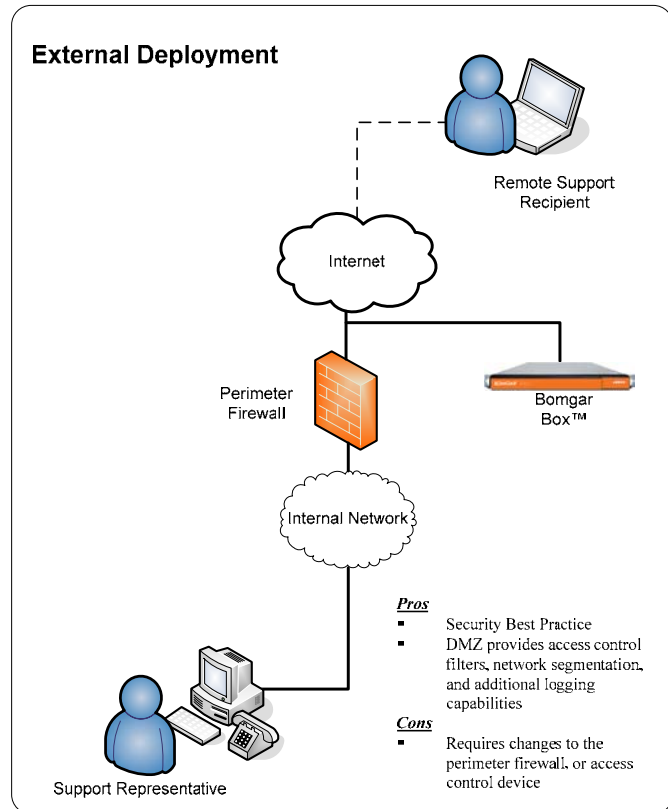
- Does not require any firewall changes

#### Cons

- The ability to implement access controls to block traffic to the appliance is more difficult due to potentially limited access control mechanisms.

#### Firewall Details

No firewall changes are required with this setup.



## Internal Network

Deploying the Bomgar Box™ on an internal network segment is ideal when the support base is completely internal or accessible through a VPN. No firewall changes are required because the device and all of the supported clients are internal to the firewall.

In environments where the supported users or systems are external to the firewall, Symantec only recommends this deployment location in the event that a DMZ does not exist or when the appliance cannot be deployed externally.

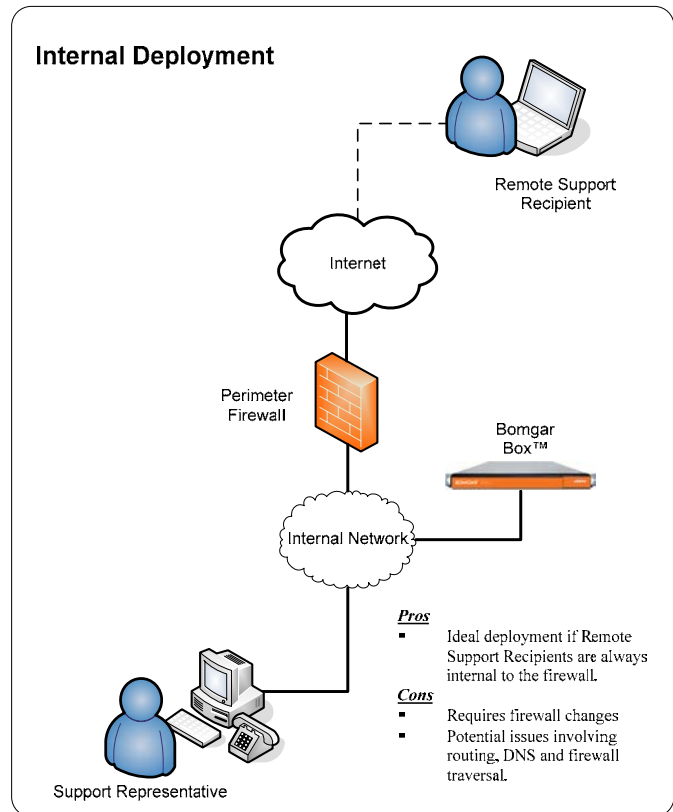
An internal deployment of the Bomgar Box™ requires numerous changes to the environment and a solid understanding of perimeter firewall controls and Network Address Translation.

### Pros

- If the appliance is utilized to support only internal systems, this location is ideal. Firewall changes will not be required, and connectivity to the appliance is limited to only internal systems.

### Cons

- If the appliance is utilized to support systems external to the corporate firewall, the following items must be taken into consideration:
  - Network Address Translation (NAT). If you utilize RFC1918 private IP addresses, such as the 10.0.0.0, 192.168.0.0, or 172.16.0.0 networks, you will have to perform NAT on your perimeter firewall. If you do not use private IP addresses, NAT will not be required.
  - DNS. In NAT environments, you should utilize split-DNS. The external name server must resolve the external IP address of the Bomgar Box™. The internal name server must resolve the internal IP address. Without split-DNS, a situation may occur where internal users will connect to an external IP address to access an internal system. Conversely, if the external DNS resolution resolves the internal IP address, external computers will not be able to connect to the internal IP address because it may be a private address.
  - Firewall Rules. By placing the appliance on an internal network, external Internet-based systems will have the ability to terminate connections on internal systems. This often violates corporate policy and does not adhere to security best practices. Changes to firewall rules will be required in order to



## Secure Deployment Guide: Bomgar Box™

allow external systems to connect to the appliance. Additionally, in the scenario highlighted in the DNS section, firewall rules may have to be made to allow internal systems to connect to the device if a split-DNS environment does not exist.

### *Technical Details*

When deploying the appliance on an internal network, the following rules should be configured to allow external systems to initiate connections to the appliance:

Source	Destination	Protocol	Port	Justification
Support Client IP address range -Or- "Any" if clients are Internet-based	Bomgar Box™ IP address	TCP	80	Allow cleartext HTTP access to the device.
Support Client IP address range -Or- "Any" if clients are Internet-based	Bomgar Box™ IP address	TCP	443	Allow encrypted HTTPS access to the device.
Support Client IP address range -Or- "Any" if clients are Internet-based	Bomgar Box™ IP address	TCP	8200	Allow encrypted HTTPS access to the device.

## Symantec-Recommended Security Settings

The following tables document Symantec’s security recommendations for securely deploying the Bomgar Box™ within your environment. As each environment is unique, Symantec’s recommendations are broad in nature and should be used as a guideline for your environment. Security should map to your business drivers, and as such, some recommendations may not be suitable for your environment.

The recommendations are documented in the following sections:

Source	Destination
<b>Appliance Administration</b>	Functionality that exists within the Appliance Administration Interface accessible through the following URL: <i>https://&lt;Bomgar Box™ IP address&gt;/appliance</i>
<b>Administrative Interface: Management: Security</b>	Functionality that exists within the Administrative Interface accessible through the following URL: <i>https://&lt;Bomgar Box™ IP address&gt;/login</i> and then by clicking the “MANAGEMENT” tab followed by clicking the “SECURITY” sub-tab.
<b>Administrative Interface: User Accounts</b>	Functionality that exists within the Administrative Interface accessible through the following URL: <i>https://&lt;Bomgar Box™ IP address&gt;/login</i> and then by clicking the “USER ACCOUNTS” tab.
<b>Administrative Interface: Public Site: File Store</b>	Functionality that exists within the Administrative Interface accessible through the following URL: <i>https://&lt;Bomgar Box™ IP address&gt;/login</i> and then by clicking the “PUBLIC SITE” tab followed by clicking the “FILE STORE” sub-tab.
<b>Operational Recommendations</b>	Recommendations around secure operational practices with the Bomgar Box™.

Text highlighted in ***Italicized Bold*** in the following tables indicates the name of the configuration or feature in verbatim.

## Appliance Administration

The Appliance Administration Interface is utilized to configure the base attributes for the device.

Symantec recommends that the Bomgar Box™ be configured in a test environment before being transitioned into the production environment.

Recommendation	Rationale
<p>1. <b>Network Restrictions</b></p> <p>Symantec recommends that access to the /appliance functionality be restricted to only a subset of networks by choosing “Allow Only the Following Networks” and then supplying a list of networks. Ideally the list of networks would be composed of networks that house application and network administrators, including any VPN solutions that they may utilize.</p> <p>If your administrators do not live on a separate network segment, Symantec recommends that the list of networks be composed of your internal network ranges.</p>	<p>Security best practice is to limit all access to administrative functionality.</p>
<p>2. <b>Allow SSLv2</b></p> <p>Symantec recommends that support for SSLv2 be disabled.</p>	<p>SSL version 2 is generally considered to be a weak cryptographic protocol with numerous avenues of attack.</p>
<p>3. <b>SSL Certificate Request</b></p> <p>Symantec recommends that a SSL Certificate Request be performed and signed by a trusted authority. At build time of your software package, your Bomgar support representative can configure your representative and support clients to employ the trusted Certificate Authority to authenticate the appliance.</p>	<p>Certificates signed by a trusted authority are considered trusted by commonly installed web browsers. With a certificate signed by a trusted authority, web browsers are able to verify that they are talking to the appliance and not to an attacker.</p> <p>Self-signed certificates do not offer that layer of trust and will prompt a security error in the remote web browsers. Users will not have a way of verifying that they are connecting to the appliance and will have to choose to accept the self-signed certificate.</p>

<b>Recommendation</b>	<b>Rationale</b>
4. <b><i>Appliance Administrator Password</i></b> Symantec recommends that the Appliance Administrator account and password be different from that of the normal Administrator account.	Segmentation of accounts limits the effective access if either of the accounts is compromised.

## Administration Interface: Management: Security

The following recommendations exist for functionality that is accessible through the Administration Interface and then by clicking on the “MANAGEMENT” tab followed by clicking the “SECURITY” sub-tab. The Administration Interface allows for changes to the appliance’s password policy, multiple login prevention, idle logouts and the ability to force all traffic to transit an encrypted SSL connection.

	<b>Recommendation</b>	<b>Rationale</b>
5.	<b>Network Restrictions</b> Symantec recommends that access to the /login functionality be restricted to only a subset of networks by choosing “Allow Only the Following Networks” and then supplying a list of networks. Ideally the list of networks would be composed of networks that house application administrators, including any VPN solutions that they may utilize. If your administrators do not live on a separate network segment, Symantec recommends that the list of networks be composed of your internal network ranges. Note: The /login interface contains different functionality than the /appliance interface. If your application administrators reside within a Call Center, that IP address range will need to be included.	Security best practice is to limit all access to administrative functionality.
6.	<b>Minimum Password Length</b> Symantec recommends that the password length be set to comply with your corporate password security policy. If you do not currently have a policy, Symantec recommends a minimum length of 6 characters.	Security best practice, including ISO 17799, specifies passwords to be a minimum length of 6 characters. Depending on the type of support and the systems that will be remotely supported, this number may be increased to 8.

	<b>Recommendation</b>	<b>Rationale</b>
7.	<b>Password Complexity</b> Symantec recommends that the requirement for complex passwords be enabled.	Secure passwords should utilize a combination of upper and lower case characters, numerals, and symbols.
8.	<b>Password Expiration</b> Symantec recommends that the password's expiration be compliant with your corporate password policy. If you do not have a password policy, Symantec recommends that passwords expire every 90 days.	At a minimum, passwords should be set to expire every 90 days. Depending upon the nature of support or supported systems, the expiration date may be decreased to 30 or 60 days.
9.	<b>Account Lockout</b> Symantec recommends that accounts be locked out after 5 consecutive failed login attempts.	Enforcing account lockouts prevents against brute force attacks launched against the appliance and is a common security best practice. Depending on the nature of support, or supported systems, the lockout attempts may be decreased to 3.
10.	<b>Terminate Session If Account Is In Use</b> Symantec recommends that multiple logins should be prevented by enabling the session termination functionality.	Security best practice is to maintain unique accounts on systems and applications. The prevention of multiple logins enforces the use of unique accounts.
11.	<b>Log out Idle Representatives</b> Symantec recommends that idle representatives be logged out of the Bomgar Box™ after 30 minutes of idle time.	Security best practice is to require screen locks and idle timeouts within applications to prevent unauthorized access if a terminal is left unattended. At a minimum, accounts should be logged out within 30 minutes.
12.	<b>Force Public Site to Use SSL (https)</b> Symantec recommends that this feature be enabled such that all communications to the appliance are encrypted.  Note: An SSL certificate must be generated and signed by a trusted authority in order to prevent security warnings from appearing on the appliance's public interface.	Security best practice is to require that all confidential information be encrypted while it transits a network.

## Secure Deployment Guide: Bomgar Box™

The following recommendations exist for functionality that is accessible through the Administration Interface and then by clicking on the “USER ACCOUNTS” tab. The recommendations are split into two subsections; the first involves attributes that can be set on an individual account level. The second subsection details recommendations that can be applied to group policies.

The Bomgar Box™ allows for users to be segmented into teams based on discipline, areas of expertise, or other attributes. Support recipients may then be routed to the team that is most appropriate to address their issue.

In addition to teams, the Bomgar Box™ allows for the use of group policies. Group policies allow administrators to define common attributes and apply them to multiple users. Symantec recommends the use of group policies to segment functionality and to apply the principal of Least Privilege Access. A hypothetical example of group policies would be the segmentation of support representatives into three separate groups: Representative Trainees, Representatives, and Managers.

In this scenario, Representative Trainees could be configured to have the ability to access the appliance, but would not be allowed to initiate remote screen sharing sessions with support recipients. Upon completion of their training, trainees would then be placed into the “Representative” group.

Representatives are full-fledged users that would be able to initiate remote screen sharing sessions to support users. They would be publicly visible on the website and would be allowed to transfer files to the support recipient’s computer. This group would most likely consist of the majority of your support representatives. An additional sub-group may exist that has all the functionality of the Representatives group, but records all screen sharing sessions. This group could be used to monitor representatives that have just completed their training.

The Managers group would be comprised of shift or department managers. These individuals would be allowed to access the Bomgar Box™ reports, add files to the File Store, update the HTML design of the appliance and edit the Canned Messages. In this hypothetical environment, the functionality would not normally be needed by the support desk representatives. In order to comply with the concept of Least Privilege Access, this functionality would be restricted to managers.

Symantec recommends the use of group policies to tailor the level of access granted to support representatives based on business requirements and documented roles and responsibilities within your organization.

## Secure Deployment Guide: Bomgar Box™

The Bomgar Box™ provides the ability to allow the support recipient to determine the level of access granted to his or her computer. Upon enabling this feature, when a support session is initiated, a dialog box will appear on the support recipient's computer. He or she will be prompted to authorize the level of access that the support representative will be given. The client's selection is then saved within a report. In addition, a support recipient may retake control of his or her computer or terminate the support session if required, at any time.

The following recommendations are for functionality accessible upon the editing an individual user account.

<b>Recommendation</b>	<b>Rationale</b>
13. <b>Password Never Expires</b> Symantec recommends that this functionality remain disabled for all accounts.	Password security best practice maintains that all passwords should expire on a periodic basis.
14. <b>Account Expiration</b> Symantec recommends the use of account expiration for temporary or seasonal employees.	Account expiration reduces the risk of unauthorized use via legacy accounts.

The following recommendations are for functionality found upon the editing of a select user or a group policy.

<b>Recommendation</b>	<b>Rationale</b>
15. <b>Group Policies</b> Symantec recommends the use of group policies to segment support desk representatives based on duties and job tasks. Functionality should be provided based on documented roles and responsibilities of the position.	The concept of Least Privilege Access should be upheld when granting functionality to support representative accounts.
16. <b>Administrator Accounts</b> Symantec recommends that a minimal number of administrator accounts be created. Administrator access should be granted to the designated individuals responsible for administering the appliance and user accounts.	A clear separation of duties should exist between the users and administrators. Administrative access should be granted only to designated individuals who are responsible for administrative duties.

<b>Recommendation</b>	<b>Rationale</b>
17. <b>Allowed to Change Display Name</b> Unless a specific business requirement exists for a support desk representative to change his or her display name, Symantec recommends that this feature be disabled.	Preventing users from changing their display name enforces accountability and consistency in customer support sessions.
18. <b>Allowed to View Reports</b> Symantec recommends that this functionality be limited to support desk representatives or managers that have a legitimate requirement for this data.	Separation of duties ensures Least Privilege Access to the configuration or state of a remote client's computer system or server.
19. <b>Allowed to Edit File Store</b> Because files in the File Store can be transferred to a remote client's desktop, Symantec recommends that the ability to alter content within the File Store be limited to dedicated individuals.	In order to maintain integrity of files offered for public download, files should be properly screened and approved prior to being placed online. Limiting access to the upload process ensures that only files from trusted individuals are transferred to remote support recipients.
20. <b>Allowed to Edit Public Site</b> Symantec recommends that this functionality be limited to designated individuals.	Limiting access to alter the public website for the appliance ensures a consistent public image with appropriate content and messaging.
21. <b>Allowed to Edit Canned Messages</b> Symantec recommends that this functionality be provided as needed based on the structure of your support department.	Providing access to edit canned messages to designated individuals ensures a consistent public image and messaging.

<b>Recommendation</b>	<b>Rationale</b>
<p>22. <b>Allowed to control customer's computer and use file transfer interface</b> Symantec recommends that only trained and approved support representatives have access to initiate screen sharing functionality.</p>	<p>Limiting remote control functionality to trained support representatives ensures a consistent level of response and support and complies with the best practice of only granting access to features/functionality to trained individuals.</p>
<p>23. <b>Prompt customer for approval when screen sharing and file transfer are requested</b> Symantec recommends that clients be provided the choice between Full Control, View Only, or be able to Cancel the support session.</p>	<p>Requiring client approval provides an additional auditable layer of authorization between the remote client and the support representative.</p>
<p>24. <b>Allowed to use Push and Start</b> Symantec recommends that this functionality be limited to the designated support representatives that have the appropriate access on the remote computer.</p>	<p>Because the Push and Start functionality requires credentials to access the remote computer, this functionality should be limited to the appropriate support individuals to ensure adequate separation of duties and adheres to the concept of Least Privilege Access.</p>
<p>25. <b>LDAP Support</b> If LDAP is utilized, Symantec recommends that support for encrypted LDAP sessions be enabled by configuring the appliance to use LDAPS or LDAP with TLS (RFC 2830).</p>	<p>Security best practice is to encrypt authentication credentials if they transit a network.</p>

## Administration Interface: Public Site: File Store

The following recommendations exist for functionality that is accessible through the Administration Interface and then by clicking on the “PUBLIC SITE” tab followed by clicking the “FILE STORE” sub-tab.

<b>Recommendation</b>	<b>Rationale</b>
26. <b>Show File Listing for File Store at /files</b> Symantec recommends that this feature be disabled if the File Store contains files that are not currently publicly available or files that may contain information which may be leveraged by an attacker.	Information gathering style attacks allow an attacker to obtain information about an application, product, or company which may be leveraged in other attacks to successfully gain unauthorized access.

## Operational Practices Recommendations

The following recommendations pertain to common operational security practices.

<b>Recommendation</b>	<b>Rationale</b>
27. <b>Logging &amp; Reporting</b> Symantec recommends that reports be downloaded and archived. A future Bomgar Box™ software update will add the ability to send logs to a centralized log sever. Symantec recommends that this functionality be enabled when available.	Collection and reviewing of logs aids in identifying anomalous activities and is of benefit when investigating security or misconduct related events.
28. <b>Least Privilege Access</b> Symantec recommends that group policies be utilized to apply appropriate segmentation and delegation of functionality to your support representative team.	The security best practice of providing Least Privilege Access ensures that adequate separation of duties and the ability to grant functionality based on the business requirement for the individual roles and responsibilities is maintained.

### **About Bomgar™ Corporation**

Bomgar™ specializes in appliance-based solutions for remote control support. Bomgar™ enables remote desktop control of PCs or Macs. It works through corporate firewalls and requires no pre-installed software or configuration on the end-user's computer. Bomgar™'s remote support solutions enable its clients to streamline business and keep unnecessary travel to a minimum. Bomgar™ Corporation began in 2003 with the vision of simplifying remote support for all types of organizations. The company has since grown steadily, obtaining over 2,500 customers in all 50 states and over 30 countries.

To learn more about Bomgar™'s remote support solutions, visit them online at:  
<http://www.bomgar.com>

## About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, California, Symantec has operations in more than 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

Symantec has worldwide operations in more than 40 countries. For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
1 408 517 8000  
1 800 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec makes this document available for informational purposes only. It may not reflect the most current legal developments, and Symantec does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Symantec offer any certification or guarantee with respect to the opinions expressed herein. Changing circumstances may change the accuracy of the content herein. The information contained herein is not intended to constitute legal advice nor should it be used as a substitute for specific legal advice from a licensed attorney. This report makes no representations or warranties of any kind regarding the security of Bomgar Corporation or forward-looking statements regarding the effects of future events. You should not act (or refrain from acting) based upon information herein without obtaining professional advice regarding your particular facts and circumstances. Opinions presented in this document reflect judgment at the time of publication and are subject to change. While every precaution has been taken in the preparation of this document, Symantec assumes no responsibility for errors, omissions, or damages resulting from the use of the information herein."

Reproduction guidelines: You may make copies of this document unless otherwise noted. If you quote or reference this document, you must appropriately attribute the contents and authorship to Symantec. Symantec and the Symantec logo are trademarks or registered trademarks, in the United States and certain other countries, of Symantec Corporation. Additional company and product names may be trademarks or registered trademarks of the individual companies and are respectfully acknowledged."

Symantec and the Symantec logo are U.S registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Copyright ©2005 Symantec Corporation. All rights reserved. Printed in the U.S.A. 07/05 10434083