BOMGAR™

Bomgar Privileged Access
Appliance Interface (/appliance)

TC:5/3/2017

Table of Contents

Bomgar Privileged Access Appliance Web Interface

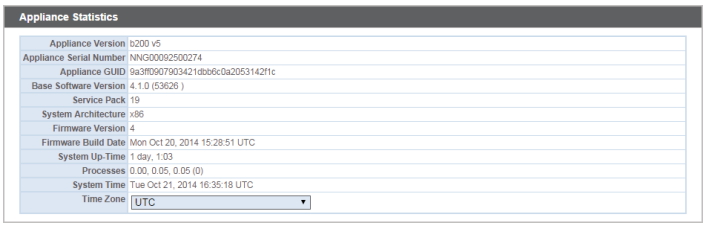
This guide is designed to help you configure and manage the Bomgar Appliance through its **/appliance** web interface. The appliance serves as the central point of administration and management for your Bomgar site.

Use this guide only after an administrator has performed the initial setup and configuration of the Bomgar Appliance as detailed in the Bomgar Appliance Hardware Installation Guide at www.bomgar.com/docs/privileged-access/getting-started/deployment/hardware/. Once Bomgar is properly installed, you can begin accessing your endpoints immediately. Should you need any assistance, please contact Bomgar Technical Support at help.bomgar.com.

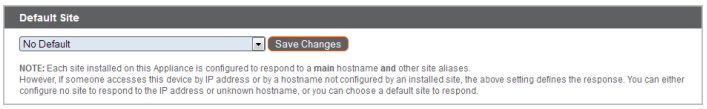
Status

Basics: View Appliance Details

The **Basics** page gives you information about your Bomgar Appliance and allows you to monitor your system.You can also set your local time to any valid global time zone. The system time is always displayed in UTC.

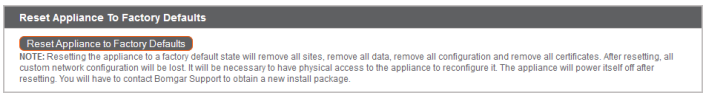


In nearly all scenarios, this setting can be left unchanged. Bomgar discourages multiple sites on one appliance. However, if your setup requires more than one site responding to one IP address, select a default site to respond should someone enter the IP address directly rather than the domain name. If more than one DNS entry directs to this IP address and you select **No Default**, an error message appears if someone tries to access your site by entering the IP address.



From this page, you can also reboot or shut down your Bomgar Appliance. Although rebooting your appliance is not required, you may want to make a monthly reboot part of your regular maintenance. You do not need physical access to the appliance in order to perform this reboot.

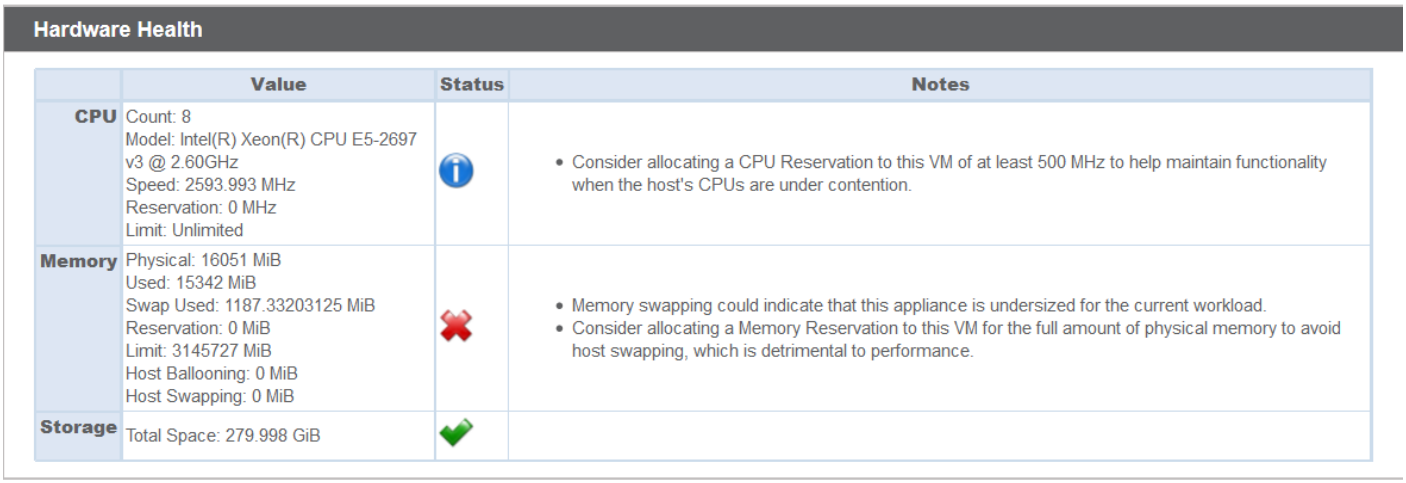
Please do not do the following unless instructed to do so by Bomgar Technical Support: Clicking the **Reset Appliance to Factory Defaults** button reverts your Bomgar Appliance to its factory state. This completely removes all data, configuration settings, sites, and certificates from your appliance. Once the appliance is reset, it also powers itself off.



Health: View Virtual Appliance Health Details

***Note:** The **Health** tab is visible only for sites supported by a virtual appliance or cloud appliance.*

The **Health** page allows you to monitor the state of your virtual or cloud appliance. It displays information pertaining to how many CPUs are in use as well as the amount of memory and storage being used. View the **Status** and **Notes** columns for suggestions on how to improve the health of your appliance.

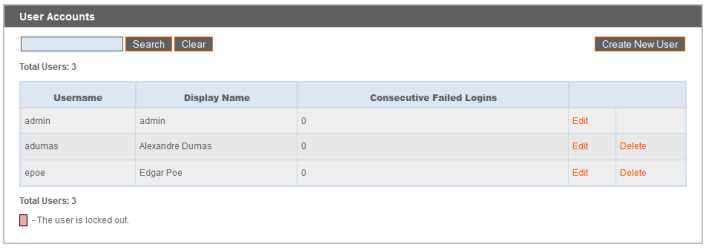


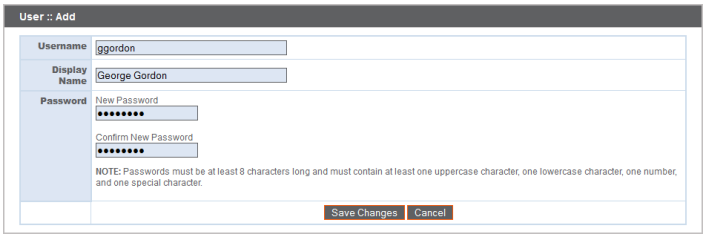
Users

Change Password and Username, Add User

On the **Users** page, you can add, edit, or delete administrative users for the /appliance interface. You can also change an administrator's username, display name, or password. Bomgar recommends changing your password regularly to protect against unauthorized access.

See "Appliance Administration: Restrict Accounts, Networks, and Ports, Enable a STUN Server, Set Up Syslog, Enable Login Agreement, Reset Admin Account" on page 22 to set account restriction rules including password expiration and history.





Note: *You must have at least one user account defined. The Bomgar Appliance comes with one account predefined, which is the admin account. You can keep just the admin account, create additional accounts, or replace the admin account.*

Networking

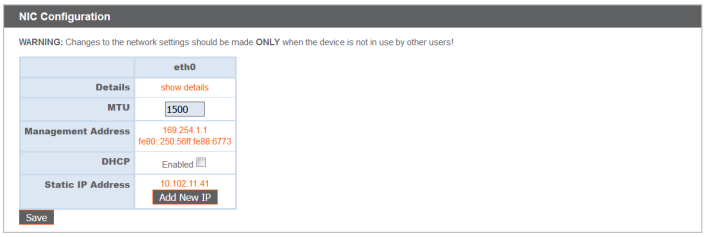
IP Configuration: Configure IP Address and Network Settings

Companies with advanced network configurations can configure multiple IP addresses on the appliance's ethernet ports. Using multiple ports can enhance security or enable connections over non-standard networks. For example, if employees are restricted from accessing the internet but need to provide off-network support, using one port for your internal private network and another for the public internet allows users worldwide to access systems without breaching your network security policies.

NIC teaming combines your system's physical NICs into a single logical interface. NIC teaming operates in active-backup mode. One of the NICs is used to carry all network traffic. If the link on that NIC is lost for any reason, the other NIC becomes active. Before activating NIC teaming, please ensure that both NICs are connected to the same network segment (subnet) and that you have IP addresses configured on only one of the existing NICs.

***Note:** If you are using a virtual or cloud appliance environment, the **Enable NIC Teaming** option is not available.*

Although multiple IP addresses can be assigned to each Network Interface Controllers (NIC), do not configure either NIC such that it has an IP address that is in the same subnet as an IP address on the other NIC. In this scenario, packet loss occurs with packets originating from the IP on the NIC that does not have the default gateway. Consider the following example configuration:



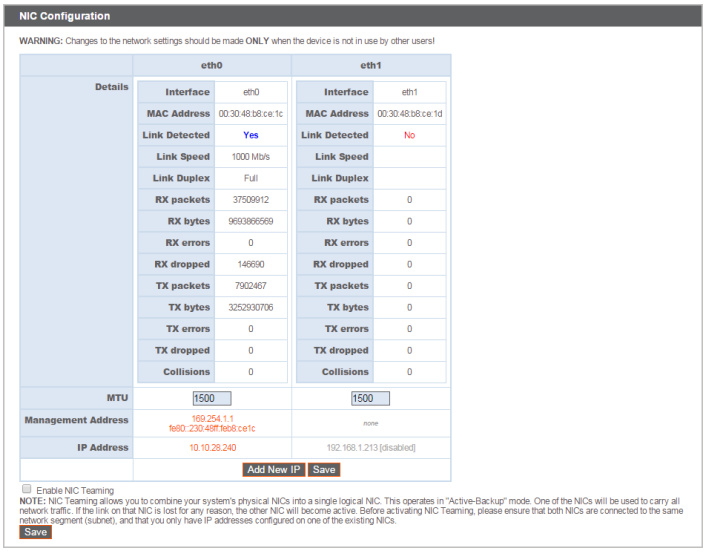
- eth0 is configured with the default gateway of 192.168.1.1
- eth0 is assigned with 192.168.1.5
- eth1 is assigned with 192.168.1.10
- Both eth0 and eth1 are connected to the same subnet switch

Given this configuration, traffic from both NICs is sent to the default gateway (192.168.1.1) regardless of which NIC received traffic. Switches configured with dynamic Address Resolution Protocol (ARP) send packets randomly to either eth0 (192.168.1.5) or eth1 (192.168.1.10), not both. When eth0 receives these packets from the switch destined for eth1, eth0 drops the packets. Some switches are configured with static ARP. These switches drop all packets received from eth1 since this NIC does not have the default gateway and is not present in the static ARP table of the gateway. If you wish to configure redundant NICs on the same subnet, use NIC teaming.

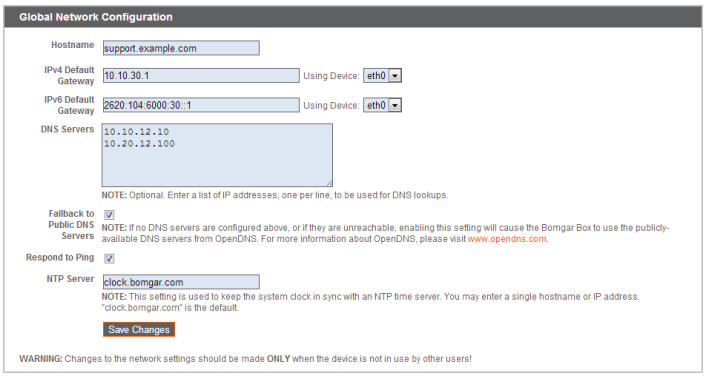
As of Bomgar release 17.1, you can enable Dynamic Host Configuration Protocol (DHCP) for your appliance by checking the **DCHP: Enable** box. DHCP is a network protocol that uses a DHCP server to control the distribution of network parameters, such as IP addresses, allowing systems to automatically request these parameters. This reduces the need to manually configure settings. In this case, when checked, an IP address is obtained from the DHCP server and is removed from the pool of available IP addresses.

Note: *To learn more about DHCP, please see What is DHCP? at https://technet.microsoft.com/en-us/library/.*

Click **Show Details** to view and verify transmission and reception statistics for each ethernet port on the appliance.



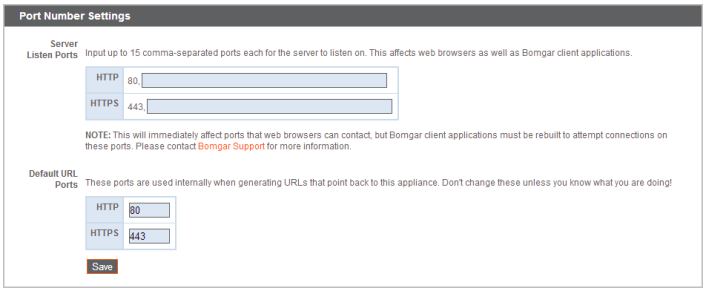
Under the **Global Network Configuration** section, configure the hostname for your Bomgar Appliance.



Note: *The hostname field does not need to meet any technical requirements. It does not affect what hostname client software or remote users connect to. If the hostname attempted by the client software needs to change, notify Bomgar Technical Support of the needed changes so that Support can build a software update. The hostname field exists primarily to help you distinguish between multiple Bomgar Appliances. It is also used as the local server identifier when making SMTP connections to send email alerts. This is useful if the* ***SMTP Relay Server*** *specified at* ***/appliance > Security > Email Configuration*** *is locked down. In this case, the configured hostname might have to match the reverse-DNS lookup of the appliance's IP address.*

Assign a default gateway, selecting which ethernet port to use. Enter an IP address for one or more DNS servers. If DHCP is enabled, the DHCP lease provides you with a default gateway as well as a listing of DNS servers in order of preference. Any statically configured DNS servers listed in the **Custom DNS Servers** field are attempted to be reached first, followed by DNS servers received from DHCP. In the event that these local DNS servers are unavailable, the **Fallback to OpenDNS Servers** option enables the Bomgar Appliance to use publicly available DNS servers from OpenDNS. For more information about OpenDNS, visit www.opendns.com.

Allow your appliance to respond to pings if you wish to be able to test if the host is functioning. Set the hostname or IP address for a Network Time Protocol (NTP) server with which you wish your Bomgar Appliance to synchronize. The default NTP server is **clock.bomgar.com**.

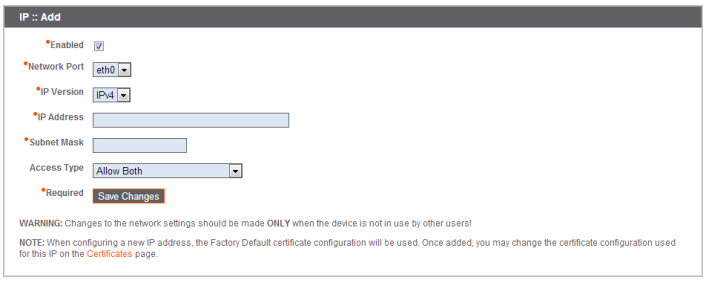


Two settings are available in the **Port Number Settings** area: **Server Listen Ports** and **Default URL Ports**. When configuring these, keep in mind that connections made to valid ports may be rejected by network restrictions set in **/appliance > Security > Appliance Administration** and in **/login > Management > Security**. The opposite is also true: connections made to invalid ports are rejected even if such connections satisfy network restrictions.

The **Server Listen Ports** section allows you to configure ports for the appliance to listen on. You may specify up to 15 comma-separated ports for HTTP and 15 comma-separated ports for HTTPS. Each port may appear only once in any field, and it may appear in only one field, not both. The appliance responds to HTTP connections made to any of the ports listed in the HTTP field, and the appliance responds to HTTPS connections made to any of the ports in the HTTPS field. You cannot change the built-in listen ports (80 and 443) except by contacting Bomgar Support and updating the appliance.

To access the appliance on a given port, use a browser requires that you enter the port in the URL of the browser (e.g., support.example.com:8200). Clients downloaded from the appliance attempt connections to the ports listed on the **/login > Status > Information** page under **Client Software Is Built to Attempt**. These ports are not configurable from /login or /appliance. To change them, you must contact Bomgar Support and have a new update built for your appliance. Once installed, the update sets the **Attempt** ports as specified by Bomgar Support in the parameters of the update.

Default URL Ports are used when generating URLs that point back to the appliance, such as session keys generated from the access console. When the default ports are blocked on the network (or can be expected to fail for any other reason), you can change the default URL ports to have generated URLs spawn with the ports that you specify. Whatever ports you enter should also be listed in the **Server Listen Ports**; otherwise, the default ports do not connect. For example, if you enter **8080** in the **Default URL Port** field, make sure **8080** is also in the **HTTP** or **HTTPS Listen Port** field. Unlike the listen port fields, you cannot enter more than one port in either of the URL port fields. You cannot enter the same port in both fields.



When adding or editing an IP address, choose whether that IP should be enabled or disabled. Select the network port on which you would like this IP to function. The **IP Address** field sets an address to which your appliance can respond, while **Subnet Mask** enables Bomgar to communicate with other devices.

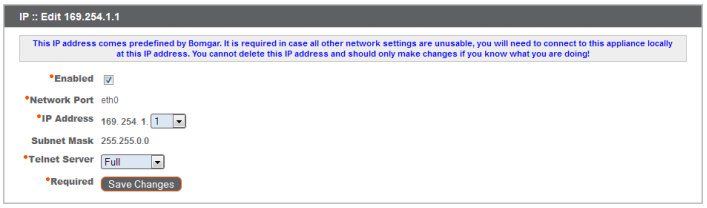
When editing an IP address that is on the same subnet as another IP address for this appliance, choose if this IP address should be **Primary**. When this box is checked, the appliance designates this IP address to be the primary or originating IP address

for the subnet. This helps, for example, to ensure that any network traffic originating from the appliance on that subnet matches and complies with defined firewall rules.

From **Access Type**, you can restrict access over this IP to the public site or customer client. Use **Allow Both** to allow access for both the public site and customer client.

Note: *To restrict access to the* ***/login*** *interface, set network restrictions under* ***/login > Management > Security****. To restrict access to the* ***/appliance*** *interface, set network restrictions under* ***/appliance > Security > Appliance Administration****.*

When viewing the management IP address[1], the **Telnet Server** dropdown provides three settings: **Full**, **Simplified** and **Disabled**, as detailed below. These settings change the menu options of the telnet server that is available only on this private IP and that can be used in emergency recovery situations. Since the telnet feature is specifically tied to the built-in private IP, it does not appear under any other configured IP addresses.



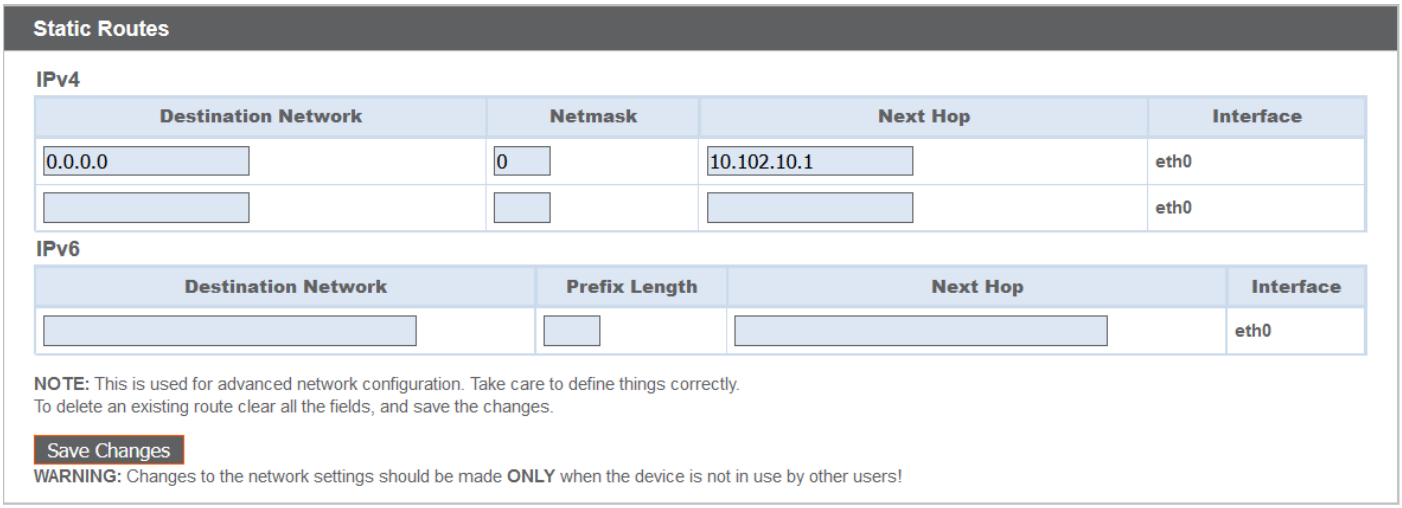
Setting	Function
Full	Enables the telnet server with full functionality
Simplified	Allows four options: **View FIPS Error**, **Reset to Factory Defaults**, **Shutdown**, and **Reboot**
Disabled	Completely disables the telnet server

[1] Do not delete or modify the management IP address.

Static Routes: Set Up Static Routes for Network Communication

Should a situation exist in which two networks are unable to talk to each other, you can establish a static route so that an administrator with a computer on one network can connect through the Bomgar Appliance to a computer on the other network, provided that the appliance is in a place where both networks can communicate with it individually.

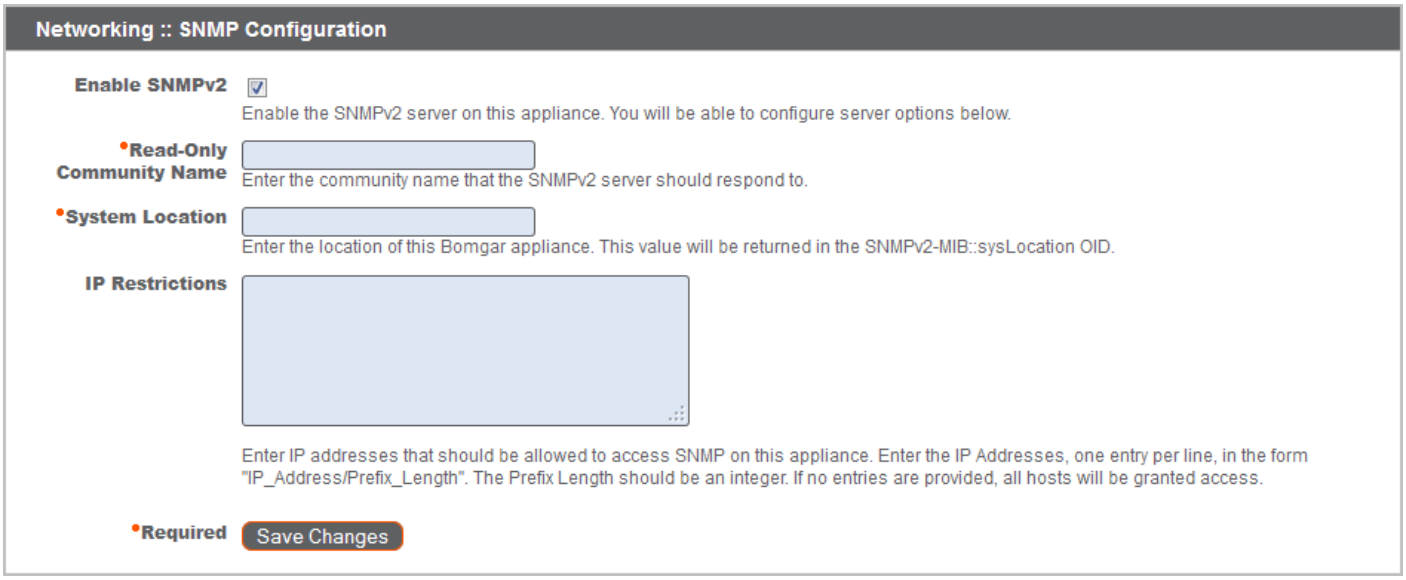
Only advanced administrators should attempt to set up static routes.



SNMP: Enable Simple Network Management Protocol

The Bomgar Appliance supports Simple Network Management Protocol (SNMP)
0Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for monitoring and managing networked devices (see Simple Network Management Protocol at wikipedia.org/wiki/Simple_Network_Management_Protocol).
monitoring for network, hard drive(s), memory, and CPU statistics. This allows tools that collect availability and other statistics via the SNMP protocol to query the Bomgar Appliance for monitoring purposes.

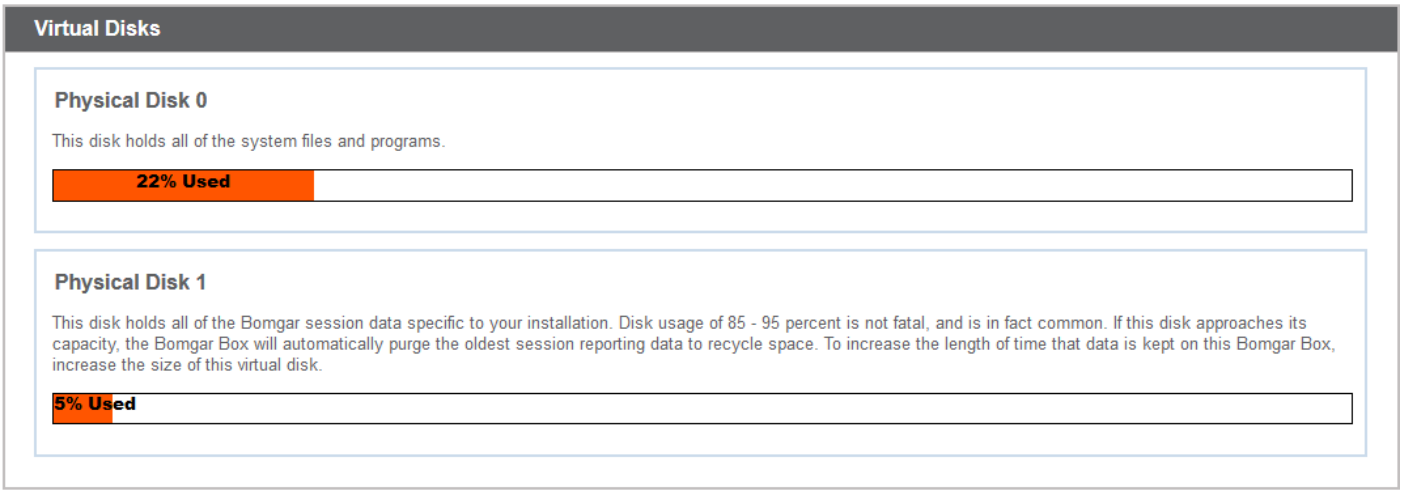
To enable SNMP for this appliance, check **Enable SNMPv2**. This enables a SNMPv2 server to respond to SNMP queries. Enter a value for the **Read-Only Community Name**, the **System Location**, and the **IP Restrictions**, IP addresses that are allowed to query this appliance using SNMP. Note that if no IP addresses are entered, all hosts are granted access.



Storage

Status: Disk space and Hard Drive Status

The **Status** page displays the percentage of your Bomgar Appliance's hard drive space that is in use.



If you enable all recording features on your site (session, protocol tunneling, and remote shell recordings), or if your overall session count is high, it is common to see a higher amount of disk usage. Note that disk usage of 85-95% is NOT a cause for alarm. If the hard drive should become low on disk space, the appliance is configured to automatically purge the oldest session data and recycle that disk space for new session data.

Specific to the Bomgar B300P Appliance

The B300P uses a Redundant Array of Independent Disks to back up your data. RAID 6 is used to allow the appliance to lose up to 2 of its 4 drives without any data loss. In the event of a failure, remove the corrupted drive and contact Bomgar for a return maintenance authorization and repair or replacement drive. When you replace the damaged drive, the appliance automatically rebuilds the RAID using the new drive. You do not need to power off the appliance when replacing drives.

Specific to the Bomgar B400P Appliance

The B400P has two sets of logical Redundant Array of Independent Disks (RAID) disks. This RAID configuration includes eight physical disk drives configured into two logical RAID drives: A RAID 1 configuration that is logical disk 0, and a RAID 6 configuration that is logical disk 1.

If one of the RAID 1 or RAID 6 physical drives fails, no performance impact or data loss occurs. However, second drive failure in the RAID 6 configuration degrades performance, although it does not cause data loss.

Hardware Failure Notification (B300P and B400P Only)

The LEDs on your appliance also indicate your hard drives' status. Normally, the LEDs blinks to indicate disk activity. Should a hard drive fail, the LED turns red, and an audible alarm warns you of the failure. To turn off the alarm before the system is restored, click the **Silence Alarm** button on this web interface.

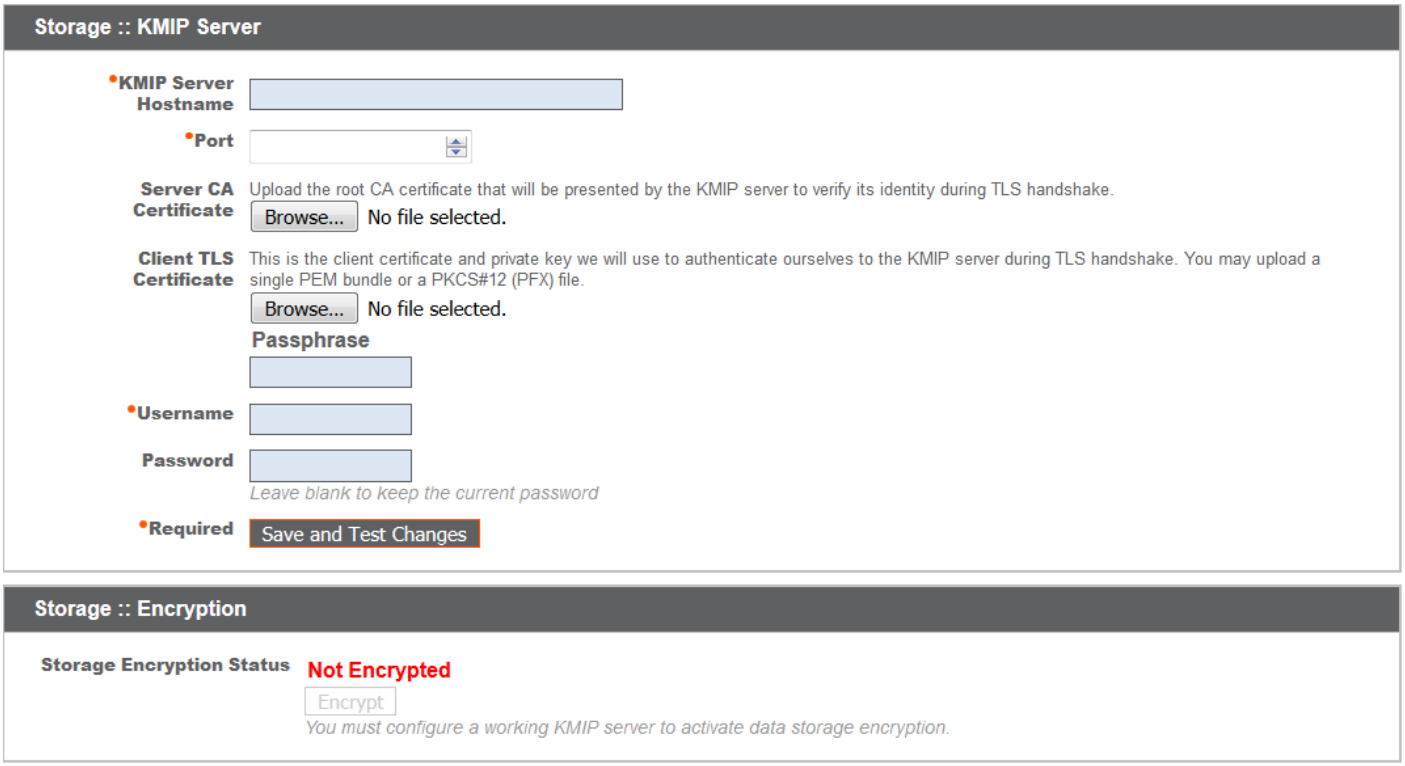
Note: *The* ***Silence Alarm*** *button is available regardless of whether or not an alarm is sounding at the time. The button cannot be used as an indicator of whether or not an alarm is active at any particular moment.*

Note: *To verify whether an alarm is sounding, check the* ***Health Status*** *located immediately above the* ***Silence Alarm*** *button. If there is an alarm sounding in the same room as the Bomgar Appliance and you want to eliminate the appliance as the source, click the* ***Silence Alarm*** *button a few times to cancel any and all possible alarms which might be active.*

Encryption: Configure KMIP Server and Encrypt Session Data

The **Encryption** section allows you to encrypt session data stored on your Bomgar Appliance. To use the data at rest encryption feature to encrypt your session data, a Key Management Interoperability Protocol (KMIP) server must be available within your environment to store the encryption keys needed to encrypt and decrypt the disks on your Bomgar Appliance. When first encrypting your data, you are limited to 4GB or less of data; however, after the initial encryption, this 4GB limit no longer applies.

Note: *If you have more than 4GB of data to initially encrypt, please contact Bomgar Technical Support at help.bomgar.com.*



In the **Storage :: KMIP Server** section, enter the hostname for your external KMIP server and the port through which the server must be accessed. Upload a valid, CA-signed certificate which is presented by the KMIP server to verify its identity to the Bomgar Appliance, as well as a client certificate private key which is used to authenticate the Bomgar Appliance to the KMIP server.

Enter a passphrase, username, and password to assist with authentication to the KMIP server. Click **Save and Test Changes** to save and verify the connection between the Bomgar Appliance and the KMIP server.

If a connection is established between the KMIP server and the appliance, the **Encrypt** button becomes available in the **Storage :: Encryption** section. If the KMIP server is not configured appropriately or if the data has not been previously encrypted, the **Encrypt** option is not available and instead reads as **Not Encrypted**.

When the **Encrypt** button is clicked, the appliance starts the process of backing up the session data and generating an encryption key to store on the KMIP server. Once the encryption key is stored, the data is encrypted and a backup is restored.

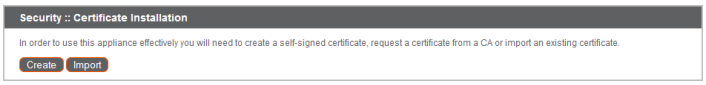
Security

Certificates: Create and Manage SSL Certificates

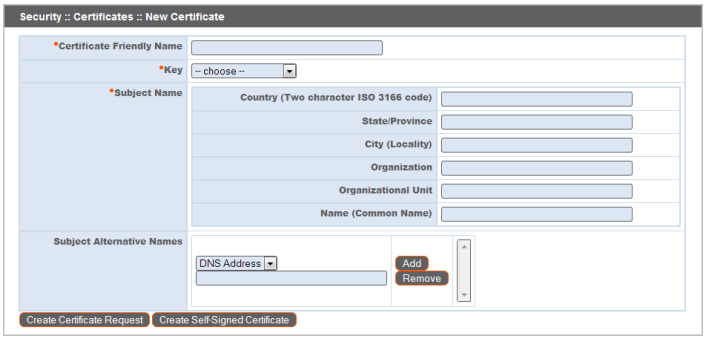
Manage SSL certificates, creating self-signed certificates and certificate requests, importing certificates signed by a certificate authority, and determining which IP addresses should be secured by which certificates.

Certificate Installation

The Bomgar Appliance comes with a self-signed certificate pre-installed. However, to effectively use your Bomgar Appliance, you also need to at minimum create a self-signed certificate, preferably requesting and uploading a certificate signed by a certificate authority.



To create a self-signed certificate or a certificate request, click **Create**. In **Certificate Friendly Name**, enter a name you can use to identify this certificate. From the **Key** dropdown, choose to create a new key or select an existing key. Enter the remaining information pertaining to your organization.



***Note**: If the certificate being requested is a replacement, you should select the existing key of the certificate being replaced.*

*If the certificate being requested is a re-key, you should select **New Key** for the certificate.*

*For a re-key, all information on the **Security :: Certificates :: New Certificate** section should be the same as the certificate for which re-key is being requested. A new certificate friendly name should be used so that it is easy to identify the certificate in the **Security :: Certificates** section.*

*Required information for the re-key can be obtained by clicking on the earlier certificate from the list displayed in the **Security :: Certificates** section.*

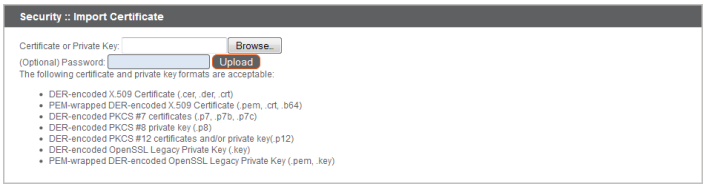
For a new key or re-key certificate, the steps to import and apply the IP addresses are the same.

In the **Name (Common Name)** field, enter a descriptive title for your Bomgar site.

In the **Subject Alternative Names** section, enter your Bomgar site hostname and click **Add**. Add a SAN for each DNS name or IP address to be protected by this SSL certificate.

Note: *DNS addresses can be entered as fully qualified domain names, such as access.example.com, or as wildcard domain names, such as *.example.com. A wildcard domain name covers multiple subdomains, such as access.example.com, remote.example.com, and so forth.*

To use a CA-signed certificate, contact a certificate authority of your choice and purchase a new certificate from them using the CSR you created in Bomgar. Once the purchase is complete, the CA sends you one or more new certificate files, each of which you must install on the Bomgar Appliance.



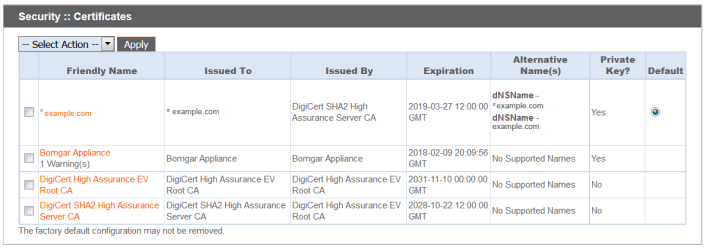
Browse to the first file and upload it. Repeat this for each certificate sent by your CA. Often, a CA does not send their root certificate, which must be installed on your Bomgar Appliance. If the root is missing, a warning appears beneath your new certificate: "The certificate chain appears to be missing one or more certificate authorities and does not appear to terminate in a self-signed certificate."

To download the root certificate for your appliance certificate, check the information sent from your CA for a link to the appropriate root. If there is none, contact the CA to obtain it. If this is impractical, search their website for their root certificate store. This contains all the root certificates of the CA, and all major CAs publish their root store online.

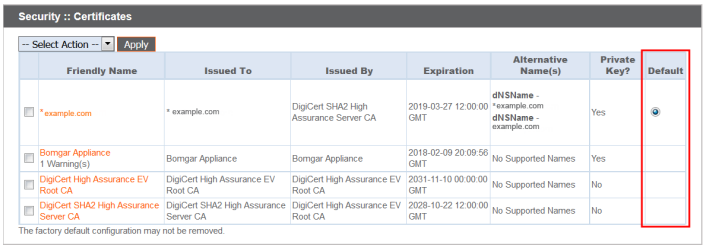
Usually, the easiest way to find the correct root for your certificate is to open the certificate file on your local machine and inspect its "Certification Path" or "Certificate Hierarchy". The root of this hierarchy or path is typically shown at the top of the tree. Locate this root certificate. Once done, download it from the CA's root store and import it to your Bomgar Appliance as described above.

Certificates

View a table of SSL certificates available on your appliance.

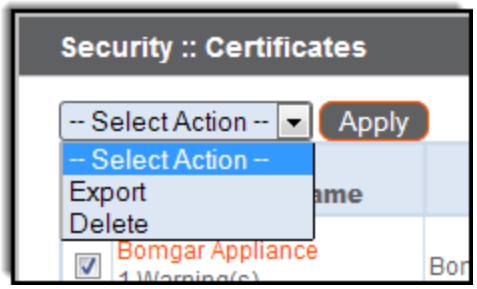


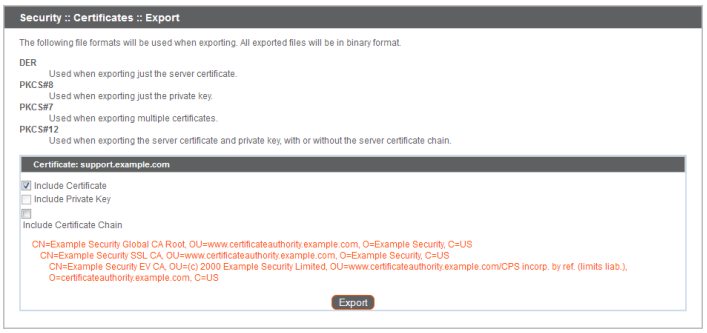
For connections that do not supply a Server Name Indication (SNI) or supply an incorrect SNI, select a default SSL certificate from the list to provide for these connections by clicking the button under the **Default** column. The default SSL certificate cannot be a self-signed certificate nor the default Bomgar Appliance certificate provided for initial installation.



Note: *To learn more about SNI, please see Server Name Indication at https://cio.gov/sni/.*

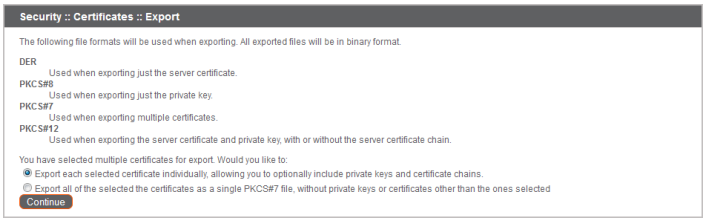
To export one or more certificates, check the box for each desired certificate, select **Export** from the dropdown at the top of the table, and then click **Apply**.





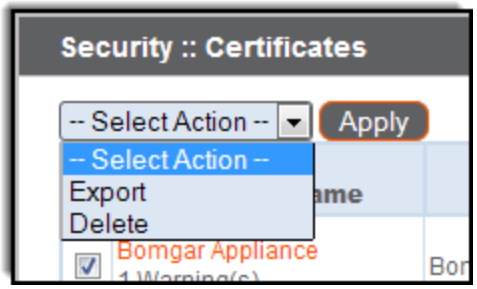
If you are exporting multiple certificates, you have the option to export each certificate individually or in a single PKCS#7 file.

When selecting to export multiple certificates as one file, click **Continue** to start the download.



To delete one or more certificates, check the box for each desired certificate, select **Delete** from the dropdown at the top of the table, and then click **Apply**.

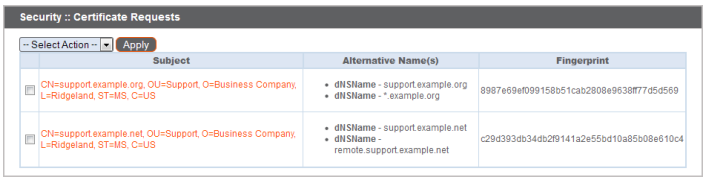
> ***Note**: Under normal circumstances, a certificate should never be deleted unless it has already been successfully replaced by a working substitute.*



To confirm accuracy, review the certificates you wish to delete, and then click **Delete.**

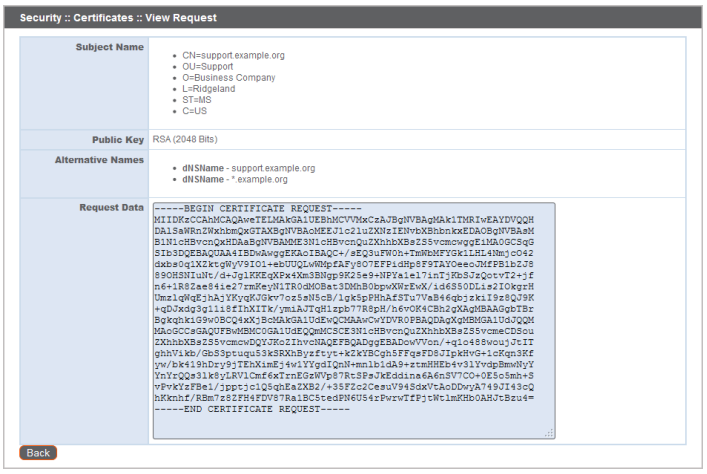
Certificate Requests

View a table of pending requests for third-party-signed certificates. Click a certificate request name to view details.

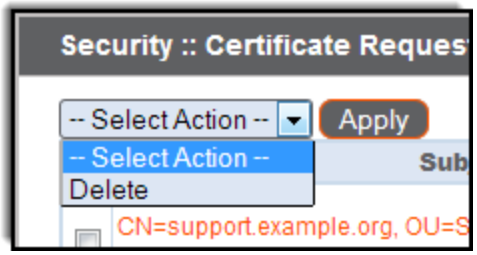


The detail view also provides the request data you give your preferred certificate authority when requesting a signed certificate.

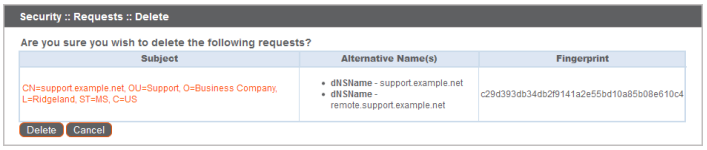
***Note**: If you are renewing a certificate, use the same certificate Request Data that was used for the original certificate.*



To delete one or more certificate requests, check the box for each desired request, select **Delete** from the dropdown at the top of the table, and then click **Apply**.



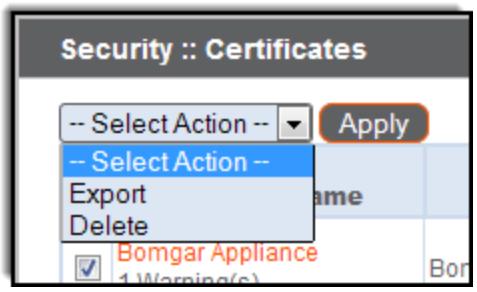
To confirm accuracy, review the certificate requests you wish to delete, and then click **Delete**.



Keys

View a table of private keys associated with certificates and certificate requests on your appliance. Click a linked certificate name or request name to view details about that associated item.

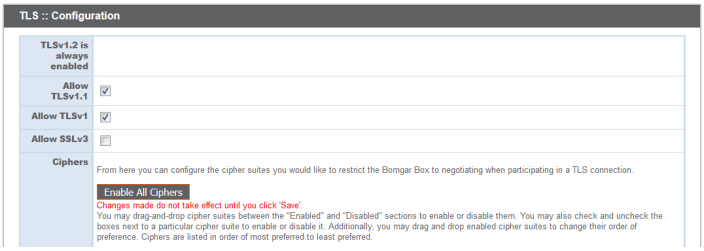
To delete one or more private keys, check the box for each desired key, select **Delete** from the dropdown at the top of the table, and then click **Apply**.



To confirm accuracy, review the private keys you wish to delete, and then click **Delete**.

> ***Note:*** *Keys associated with certificates in use (those with assigned IP addresses) cannot be deleted.*

SSL/TLS Configuration: Choose SSL Ciphers and Versions



Be aware, some older browsers may not support TLSv1.2. If you disable one or more of the older security protocols and intend to access your administrative interface from an older browser which does not support the security protocols you have enabled, Bomgar does not allow you to log in.

Note that this setting primarily affects connections to the web interface of your Bomgar Appliance. The support tunnel between your computer and your customer's computer defaults to using TLSv1.2 regardless of any other security protocols you have enabled.

Select which Ciphersuites should be enabled or disabled on your appliance. Drag and drop Ciphersuites to change the order of preference. Note that changes to Ciphersuites do not take effect until the **Save** button is clicked.

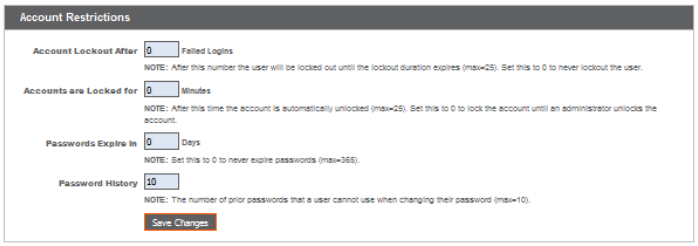
Appliance Administration: Restrict Accounts, Networks, and Ports, Enable a STUN Server, Set Up Syslog, Enable Login Agreement, Reset Admin Account

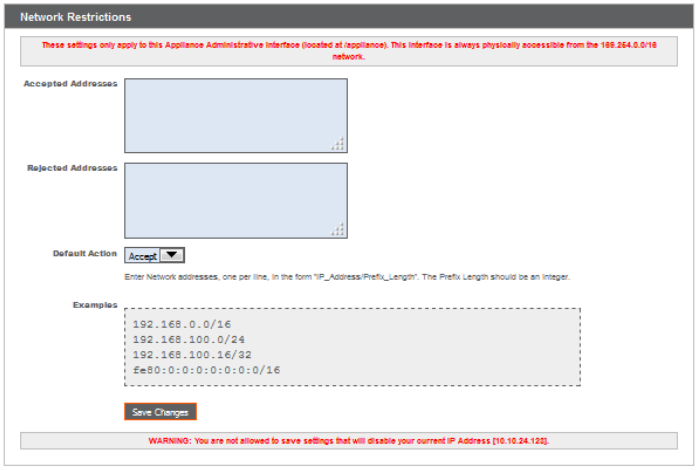
Manage access to /appliance administrative interface accounts by setting how many failed logins are allowed. Set how long an account is locked out after passing the failed login limit. Also, set the number of days a password may be used before expiration, and restrict the reuse of previous passwords.

You can restrict access to your appliance's administrative interface by setting network addresses that are or are not allowed, and you can select the ports through which this interface is be accessible.

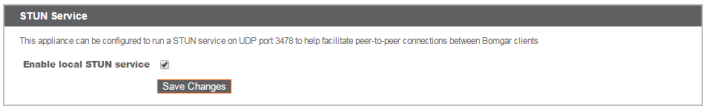
In the **Accepted Addresses** field, define IP addresses or networks that are always granted access to /appliance. In **Rejected Addresses**, define IP addresses or networks that are always denied access to /appliance. Use the **Default Action** dropdown to determine whether to accept or to reject IP addresses and networks not listed in either of the above fields. In the case of overlap, the most specific match takes precedence.

If, for example, you want to allow access to 10.10.0.0/16 but reject access to 10.10.16.0/24 and reject access from anywhere else, you would enter 10.10.0.0/16 in the **Accepted Addresses** field, enter 10.10.16.0/24 in the **Rejected Addresses** field, and set the **Default Action** to **Reject**.

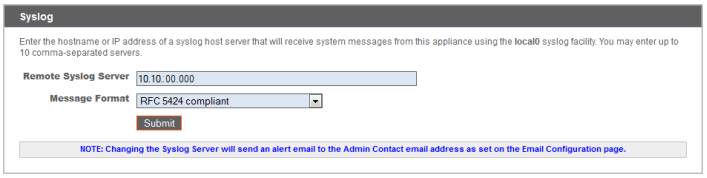




The Bomgar Appliance can be configured to run a STUN service on UDP port 3478 to help facilitate peer-to-peer connections between Bomgar clients. Check the **Enable local STUN Service** box to use this functionality.



You can configure your appliance to send log messages to up to ten syslog servers, separating entries by commas. Select the data format for the event notification messages. Choose from the standards specification RFC 5424, one of the legacy BSD

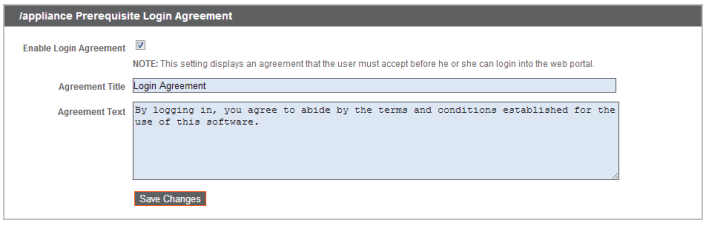


formats, or Syslog over TLS. Bomgar Appliance logs are sent using the **local0** facility.

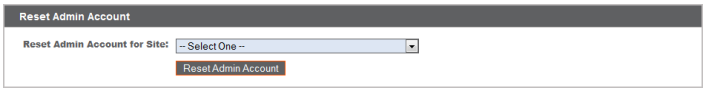
> ***Note:*** *Syslog over TLS always uses TCP port 6514*

For a detailed syslog message reference, see the Syslog Message Reference at www.bomgar.com/docs/privileged-access/how-to/integrations/syslog/.

You can enable a login agreement that users must accept before accessing the /appliance administrative interface. The configurable agreement allows you to specify restrictions and internal policy rules before users are allowed to log in.



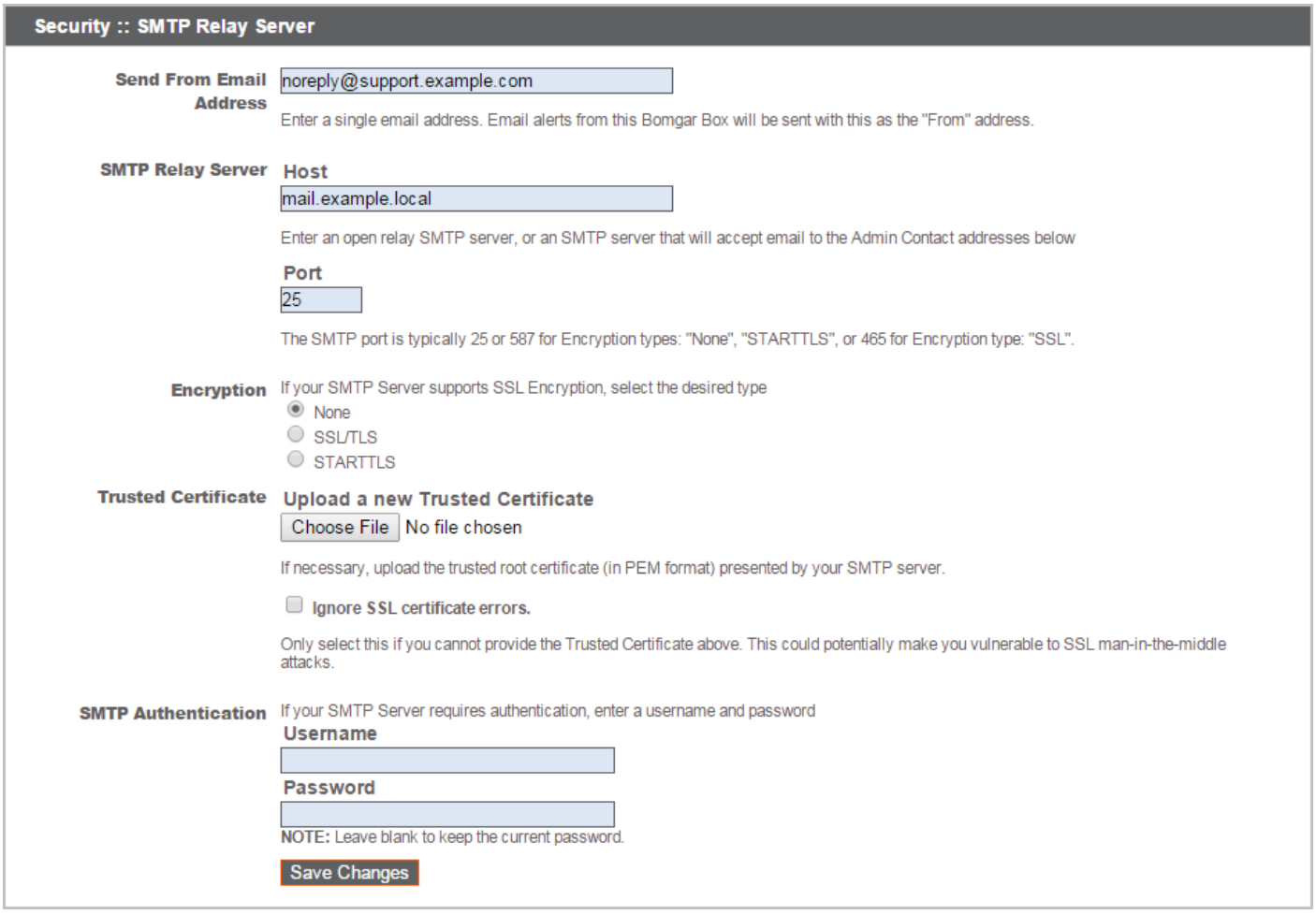
You can choose to select **Reset Admin Account**, which restores a site's administrative username and password to the default should the login be forgotten or need to be replaced.



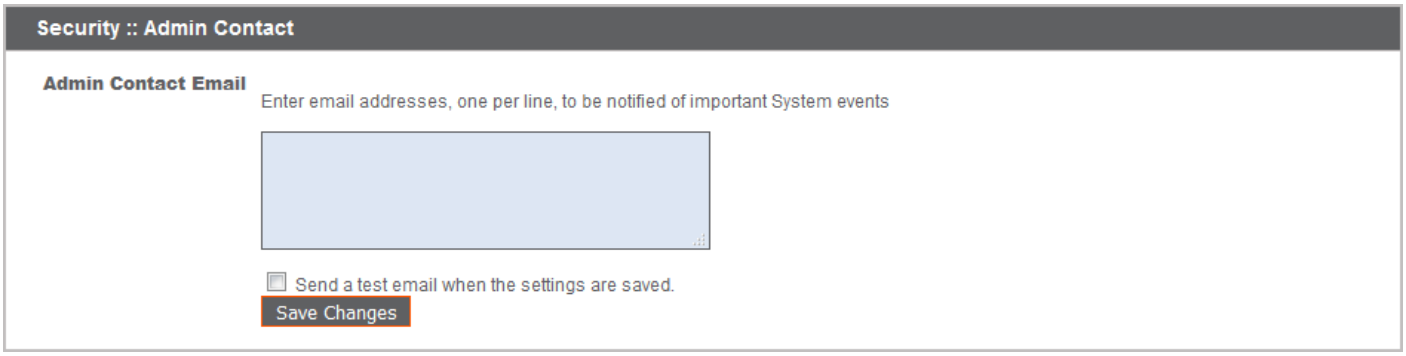
Email Configuration: Configure Appliance to Send Email Alerts

STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT
CERTIFICATES | SSL/TLS CONFIGURATION | APPLIANCE ADMINISTRATION | EMAIL CONFIGURATION

Configure your SMTP relay server and set one or more administrative contacts so that your Bomgar Appliance can send you automatic email notifications.



After entering the email addresses for the administrator contacts, save your settings and send a test email to ensure everything works correctly.



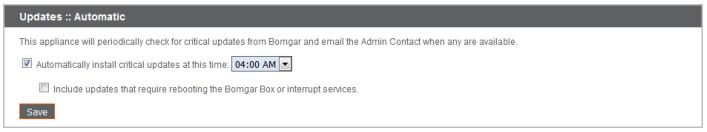
Emails are sent for the following events:

- **Syslog Server has been Changed** – A user on /appliance has changed the syslog server parameter.
- **RAID Event** – One or more RAID logical drives is not in Optimum state (Degraded or Partially Degraded).
- **SSL Certificate Expiration Notice** – An in-use SSL certificate (include either end-entity certificates or any CA certificate in the chain) expires in 90 days or less.

Updates

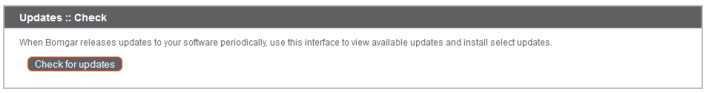
Check for Update Availability and Install Software

The appliance periodically checks for critical updates and emails the admin contact person when updates are available. You can select if you want the updates to install automatically and use the dropdown menu to select a time for the installation.

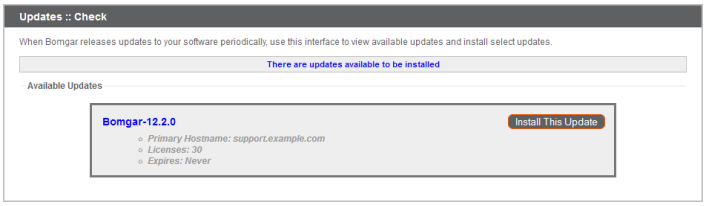


Updates requiring an appliance reboot or the interruption of services are excluded from the automatic update process unless you check the box to include them.

Bomgar continues to notify you of the latest builds as they become available. Whenever you receive notification that new update packages have been built for your appliance, clicking the **Check for Updates** button locates the packages and makes them available for you to install.



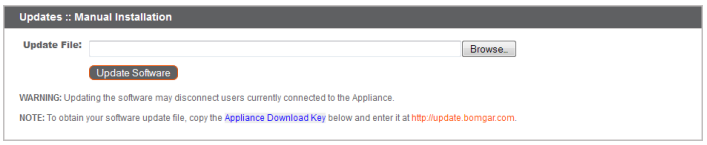
If multiple software packages have been built for your appliance, each one is listed separately in the list of available updates. Your new software is automatically downloaded and installed when you click the appropriate **Install This Update** button.

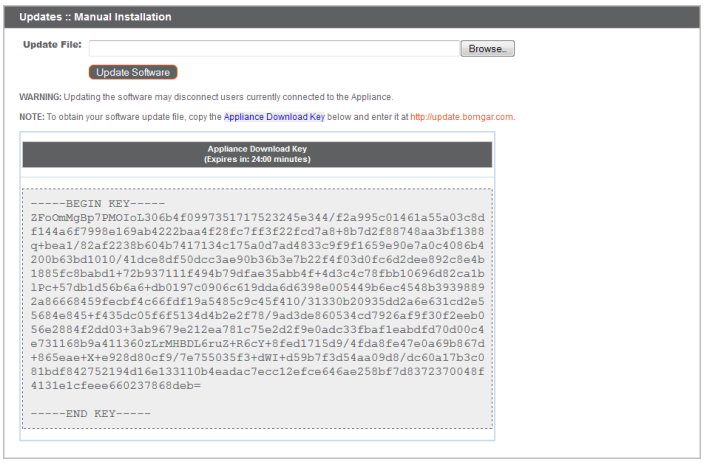


If no update packages or patches are available for your Bomgar Appliance, a message stating "No updates available" is displayed. If an update is available but an error occurred when distributing the update to your appliance, an additional message is displayed, such as, "An error occurred building your update. Please visit help.bomgar.com for more information."

It is not mandatory to use this **Check for Updates** feature. Click the **Appliance Download Key** link to generate a unique appliance key, and then, from a non-restricted system, submit that key to Bomgar's update server at update.bomgar.com. Download any available updates to a removable storage device and then transfer those updates to a system from which you can manage your appliance.

After downloading a software package, browse to the file from the **Manual Installation** section, and then click the **Update Software** button to complete the installation.





IMPORTANT

Please be prepared to install software updates directly after download. Once an update has been downloaded, it no longer appears in your list of available updates. Should you need to redownload a software update, contact Bomgar Technical Support.

When the Bomgar End User License Agreement (EULA) screen appears, fill out the required contact information and click the **Agree-Begin Download** button to accept the EULA and continue the installation.

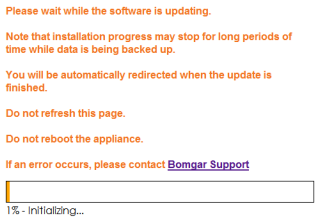
Note that if you chose to decline the EULA, an error message displays and you are not able to update your Bomgar software.

If you have any issues updating after accepting the EULA, please contact Bomgar Technical Support at help.bomgar.com.

During the installation process, the **Updates** page displays a progress bar to notify you of the overall update progress. Updates made here automatically update all sites and licenses on your Bomgar Appliance.

If you are installing a software update, logged-in users temporarily lose connection to any access sessions and the access console; therefore, schedule software updates for non-peak hours. However, if your update package contains only additional licenses, you can install the update without interrupting user connections.

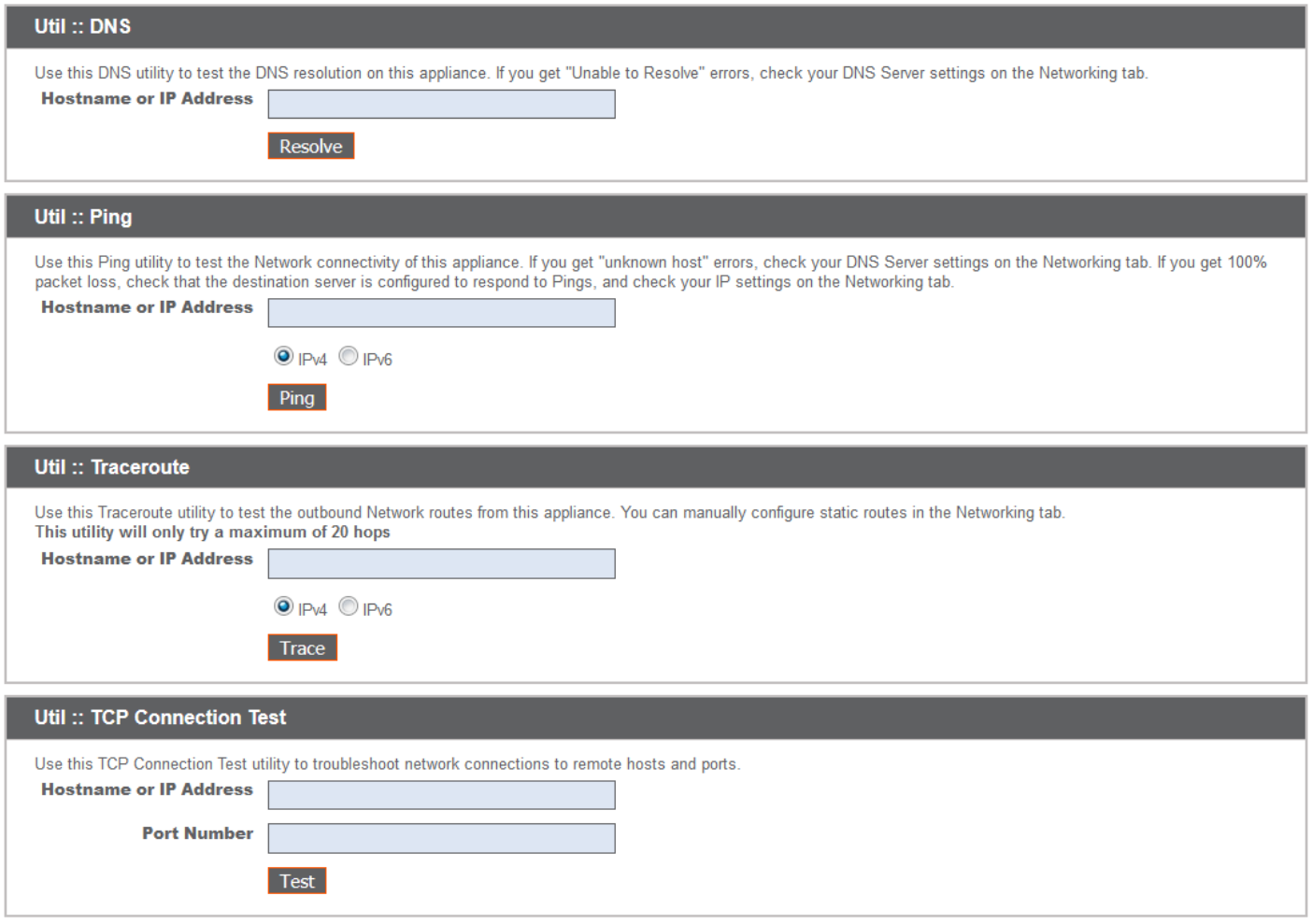
Find current information about the latest Bomgar updates at www.bomgar.com/support/changelog.



Support

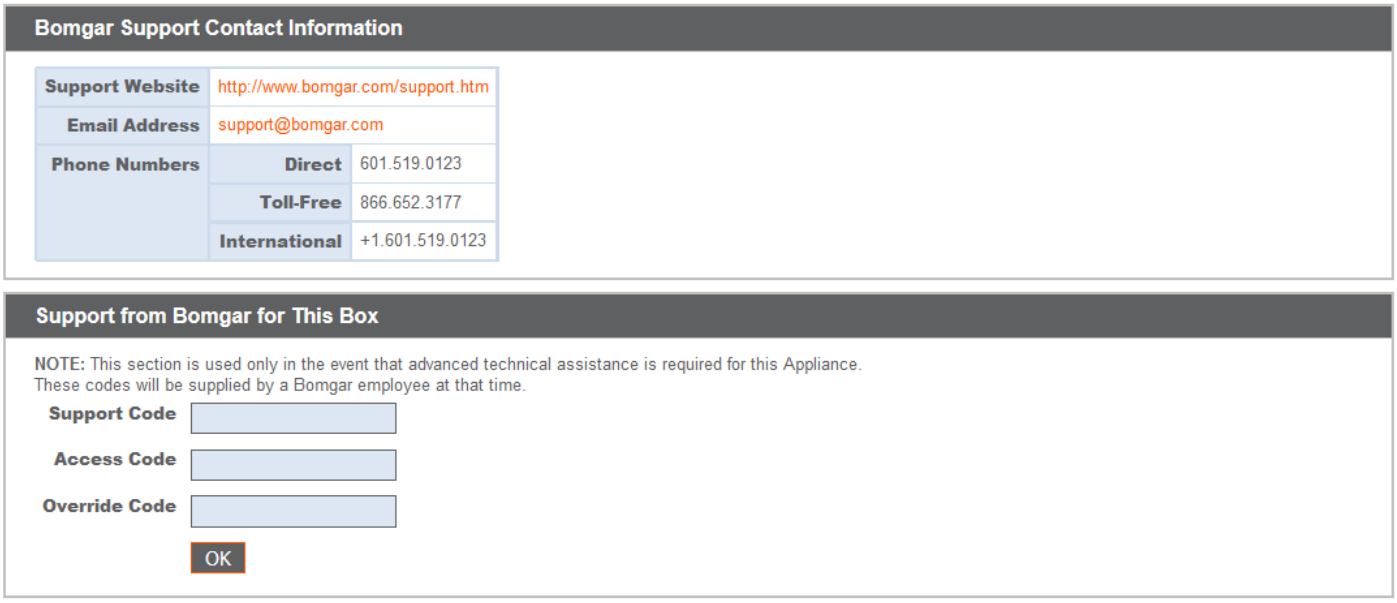
Utilities: Debug Network Problems

The **Utilities** section can be used for debugging network problems. If you are unable to establish a connection, these utilities may help to determine the reason. Test the appliance's DNS server to check that the hostname or IP address is resolving correctly. Ping your Bomgar Appliance to test its network connectivity. Use the traceroute to view the path that packets take on their journey from the appliance to any external system. You can also use the TCP connection test to check connectivity of a specific port on a target IP address or hostname.



Advanced Support: Contact Bomgar Technical Support

The **Advanced Support** section gives you contact information for your Bomgar Technical Support team and allows an appliance-initiated support tunnel back to Bomgar Technical Support, enabling quick resolution of complex issues.



If the **A Support Session with Bomgar Corporation in progress** section is visible, Bomgar Technical Support has an active session taking place with your Bomgar Appliance. The **Duration** column indicates how long Bomgar Technical Support has been in session with your appliance. To stop the session, click **Terminate**, and the tunnel between your appliance and Bomgar Technical Support closes.