BOMGAR™

Privileged Access Management
Administrative Guide 15.3

TC:5/11/2016

Table of Contents

Bomgar Privileged Access Management Administrative Guide

This guide offers a detailed overview of **/login** and is designed to help you administer Bomgar users and your Bomgar software. The Bomgar Appliance serves as the central point of administration and management for your Bomgar software and enables you to log in from anywhere that has internet access in order to download the access console.

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. 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.

Login to the Administrative Interface

Login

Log into the user administrative interface by going to your appliance's URL followed by **/login**. The user administrative interface enables administrators to create user accounts and configure software settings.

Although your appliance's URL can be any registered DNS, it will most likely be a subdomain of your company's primary domain (e.g. access.example.com/login).

Default Username: **admin**

Default Password: **password**

Note: *For security purposes, the administrative username and password used for the /appliance interface are distinct from those used for the /login interface and must be managed separately.*

Note: *If multifactor authentication has been enabled for your account, enter the email code you have received. If you enter the email code incorrectly three consecutive times, you will have to re-enter your credentials and get a new email code.*

For more information, see Login to the PAM Access Console.

Use Integrated Browser Authentication

If Kerberos has been properly configured for single sign-on, you can click the link to use integrated browser authentication, allowing you to enter directly into the web interface without requiring you to enter your credentials.

Forgot your password?

If password reset has been enabled from the **/login > Management > Security** page, this link will be visible. To reset your password, click the link, enter your username, and then correctly answer your security question. Admins cannot reset their passwords using the security question.

Login Agreement

Administrators may restrict access to the login screen by enabling a prerequisite login agreement that must be confirmed before the login screen is displayed. The login agreement can be enabled and customized from the **/login > Management > Site Configuration** page.

Status

Information: View Bomgar Privileged Access Management Software Details

Site Status

The main page of the Bomgar Privileged Access Management /login interface gives an overview of your Bomgar Appliance statistics. When contacting Bomgar Technical Support for software updates or troubleshooting purposes, you may be asked to email a screenshot of this page.

Time Zone

An administrator can select the appropriate time zone from a dropdown, setting the correct date and time of the appliance for the selected region.

Total Jump Clients Allowed

View the total number of active and passive Jump Clients which are allowed on your system. This number is determined by your Bomgar Appliance hardware capacity.

Maximum Concurrent Users

View the maximum number of users who can be logged into the access console at the same time. This number is determined by your Bomgar Appliance hardware capacity.

Endpoint Licenses

View the number of endpoint licenses available on your Bomgar Appliance. Endpoints include Jump Clients, remote Jump shortcuts, local Jump shortcuts, RDP shortcuts, and Shell Jump shortcuts. If you need more endpoint licenses, contact Bomgar Sales.

Endpoints Configured

View the number of endpoints configured on your Bomgar Appliance. Endpoints include Jump Clients, remote Jump shortcuts, local Jump shortcuts, RDP shortcuts, and Shell Jump shortcuts.

Download License Usage Report

Download a zip file containing detailed information on your Bomgar license usage. This file contains a list of all Jump Items (not counting uninstalled Jump Clients), daily counts for Jump Item operations and license usage, and a summary for the Bomgar Appliance and its endpoint license usage and churn.

Restart

You can restart the Bomgar software remotely. Restart your software only if instructed to do so by Bomgar Technical Support.

Client Software Is Built to Attempt

This is the hostname to which Bomgar client software connects. 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.

Connected Clients

View the number and type of Bomgar software clients that connected to your Bomgar Appliance.

For more information about the Bomgar Appliance, see Privileged Access Management Appliance Overview.

Users: View Logged In Users and Send Messages

Logged In Users

View a list of users logged into the access console, along with their login time and whether they are running any sessions.

Terminate

You can terminate a user's connection to the access console.

Send Message to Users

Send a message to all logged-in users via a pop-up window in the access console.

Extended Availability Users

View users who have extended availability mode enabled.

Disable

You may disable a user's extended availability.

My Account: Change Password and Username, Download the Access Console and Other Software

Bomgar Access Console

Choose Platform

Choose the operating system on which you wish to install this software. This dropdown defaults to the appropriate installer detected for your operating system.

Download Bomgar Access Console

Launch Privileged Web, a web-based access console.

Download the Bomgar access console installer.

For system administrators who need to push out the console installer to a large number of systems, the Microsoft Installer can be used with your systems management tool of choice. In your command prompt, when composing the command to install the console using an MSI, change to the directory where the MSI was downloaded and enter the command included on the **My Account** page.

You can include optional parameters for your MSI installation.

- **INSTALLDIR=** accepts any valid directory path where you want the console to install.
- **RUNATSTARTUP=** accepts **0** (default) or **1**. If you enter 1, the console will run each time the computer starts up.
- **ALLUSERS=** accepts **“”** or **1** (default). If you enter **1**, the console will install for all users on the computer; otherwise, it will install only for the current user.
- **SHOULDAUTOUPDATE=1** If you install for only the current user, you can choose to have the console automatically update each time the site is upgraded by entering a value of 1; a value of **0** (default) will not auto-update, and the console will need to be manually reinstalled when the site is upgraded. If you install the console for all users, it will not auto-update.

Bomgar Virtual Smart Card

To attempt virtual smart card authentication, the Bomgar user must have the Bomgar virtual smart card driver installed. The computer being accessed must be running in elevated mode. Also, either it must have the Bomgar endpoint virtual smart card driver installed, or it must be accessed by the Jump To functionality of the access console. For more details and requirements, see the Smart Cards for Remote Authentication document.

Choose Windows Architecture

Select to download the virtual smart card installer for the Bomgar user system or the endpoint system.

Download Virtual Smart Card Installer

Download the virtual smart card installer selected above. A virtual smart card allows you to authenticate to a remote system using a smart card on your local system.

Bomgar Automatic Elevation Service

Choose Windows Architecture

Choose the operating system on which you wish to install this software. This dropdown defaults to the appropriate installer detected for your operating system.

Download Automatic Elevation Service Installer

In special cases, you may need a session to start with the endpoint client already in elevated mode, or you may need to elevate the endpoint client without providing credentials. To securely elevate the endpoint client without the prompt, download the **Bomgar Automatic Elevation Service** and install it beforehand on the remote Windows systems to which you need credential-less elevation access. You must install the elevation service using an account that has administrative privileges to the local machine.

When the elevation service runs, it adds to the registry a hash unique to your Bomgar site. Then, when the remote system begins a session through that site, the elevation service matches the registry hash against the hash in the client. If they match, the client attempts automatic elevation.

Download Automatic Elevation Service Registry File

After a Bomgar software update, your site hash changes. Download and run the elevation service registry file to update the registry hash on systems which already have the elevation service installed. You must run the elevation service registry file using an account that has administrative privileges to the local machine.

Extended Availability Mode

Enable or Disable

Enable or disable Extended Availability Mode by clicking the **Enable/Disable** button. Extended Availability Mode allows you to receive email invitations from other users requesting to share a session when you are not logged into the console.

Change Your Email Settings

Email Address

Set the email address to which email notifications are sent, such as password resets or extended availability mode alerts.

Preferred Email Language

If more than one language is enabled on this site, set the language in which to send emails.

Change Your Password

Bomgar recommends changing your password regularly.

Username, Current Password, New Password

Verify that you are logged into the account for which you want to change the password, and then enter your current password. Create and confirm a new password for your account. The password may be set to whatever you choose, as long as the string complies with the defined policy set on the **/login > Management > Security** page.

Change Your Security Question/Answer

Security Question and Answer

The security question and answer allow a user to reset a forgotten password after providing the correct answer to the question. Passwords may be reset only if **Enable Password Reset** is checked on the **Management > Security** page. Admins cannot reset their passwords using the security question.

Configuration

Options: Manage Connection Options, Record Sessions

Session Options

Require Closed Sessions on Logout or Quit

If you check **Require Closed Sessions on Logout or Quit**, then users will be unable to log out of the console if they currently have any session tabs open.

Connection Options

Reconnect Timeout

Determine how long a disconnected endpoint client should attempt to reconnect.

Restrict physical access to the endpoint if the endpoint loses its connection or if all of the users in session are disconnected

If the session connection is lost, the remote system's mouse and keyboard input can be temporarily disabled, resuming either when the connection is restored or when the session is terminated.

Session Termination Behavior

If unable to reconnect within the time you set by **Reconnect Timeout**, choose what action to take. To prevent an end-user from accessing unauthorized privileges after an elevated session, set the client to automatically log the end user out of the remote Windows computer at session end, to lock the remote computer, or to do nothing. These rules do not apply to browser sharing sessions.

Allow users to override this setting per session

You can allow a user to override the session termination setting from the **Summary** tab in the console during a session.

Access Session Logging Options

Choose if screen sharing sessions and/or command shell sessions should be automatically recorded as videos. Enabling command shell recordings also enables command shell sessions to be available as text transcripts.

Screen Sharing / Command Shell Recording Resolution

Set the resolution at which to view session recording playback.

Note: *All recordings are saved in raw format; the resolution size affects playback only.*

Enable Automatic Logging of System Information

Choose if system information should be automatically pulled from the remote system at the beginning of the session, to be available later in the session report details.

Enable Session Forensics

Choose if you want the added capability to search across all sessions based on session events, which include chat messages, file transfer, registry editor events, and session foreground window changed events. This feature is enabled by default.

Note*: If Command Shell is enabled, Session Forensics allows you to do an in-depth search of shell recordings. When you search for a key term and a match is made in a stored shell recording, the video will automatically be queued to that point in time in the recording. No command output or passwords are recorded.*

Teams: Group Users into Teams

Teams :: Manage

Grouping users into teams aids efficiency be assigning leadership within groups of users. In the access console, each team appears as a separate queue for sessions.

Add New Team, Edit, Delete

Create a new object, modify an existing object, or remove an existing object. Deleting a team does not delete those user accounts, only the team with which they are associated.

Teams :: Add or Edit

General Settings

Team Name

Create a unique name to help identify this object.

Code Name

Set a code name for integration purposes. If you do not set a code name, one will be created automatically.

Comments

Add comments to help identify the purpose of this object.

Group Policies

Note any group policies which assign members to this team. Click the link to go to the **Group Policies** page to verify or assign policy members.

Team Members

From the list of available users, select one or more users and click the arrow to move them into the team.

You can set each member's role as a **Team Member**, **Team Lead**, or **Team Manager**. These roles play a significant part in the **Dashboard** feature of the access console.

Team members who share membership through one or more group policies are listed, along with a link to the **Group Policies** configuration page.

Jump Client Access

Access Granted By This Team

Select which teams should have access to any Jump Clients pinned to this team's Jump Group. By default, only this team has access to its own Jump Clients. However, you can select multiple other teams to see and Jump to this team's Jump Clients.

Access Granted To This Team

View a list of other teams that share Jump Client access with members of this team.

Teams :: Dashboard Settings

Within a team, a user can administrate only others with roles lower than their own. Note, however, that roles apply strictly on a team-by-team basis, so a user may be able to administrate another user in one team but not be able to administer that same user in another team.

Monitoring Team Members from Dashboard

If enabled, a team lead or manager can monitor team members from the dashboard. Choose a selection to **Disable** the ability to monitor, or choose **Only Access Console** to allow a team lead or manager to monitor a team member's access console. Monitoring affects team leads and managers for all teams on the site.

Enable Session Transfer and Take Over in Dashboard

If this option is checked, a team lead can take over or transfer a team member’s sessions. Similarly, a team manager can administrate both team members and team leads.

Jump

Jump Clients: Manage Settings and Install Jump Clients for Endpoint Access

Jump Client Mass Deployment Wizard

The Mass Deployment Wizard enables administrators and privileged users to deploy Jump Clients to one or more remote computers for later unattended access.

Allow Override During Installation

Some Mass Deployment Wizard settings allow override, enabling you to use the command line to set parameters that are specific to your deployment, prior to installation.

Jump Group

From the dropdown, select whether to pin the Jump Client to your personal Jump Group or to a team Jump Group. Pinning to your personal Jump Group means that only you can access this remote computer through this Jump Client. Pinning to a team Jump Group makes this Jump Client available to all members of teams which are allowed to access this team's Jump Clients.

Jump Policy

You may apply a **Jump Policy** to this Jump Client. Jump Policies are configured on the **Jump > Jump Policies** page and determine the times during which a user can access this Jump Client. A Jump Policy can also send a notification when it is accessed or can require approval to be accessed. If no Jump Policy is applied, this Jump Client can be accessed without restriction.

Tag

Adding a **Tag** helps to organize your Jump Clients into categories within the access console.

Connection Type

Set the **Connection Type** to **Active** or **Passive** for the Jump Clients being deployed.

Jumpoint Proxy

If you have one or more Jumpoints set up as proxies, you can select a Jumpoint to proxy these Jump Client connections. That way, if these Jump Clients are installed on computers without native internet connections, they can use the Jumpoint to connect back to your Bomgar Appliance. The Jump Clients must be installed on the same network as the Jumpoint selected to proxy the connections.

Comments

Add **Comments**, which can be helpful in searching for and identifying remote computers. Note that all Jump Clients deployed via this installer will have the same comments set initially, unless you check **Allow Override During Installation** and use the available parameters to modify the installer for individual installations.

This Installer Is Valid For

The installer will remain usable only as long as specified by the **This Installer is Valid For** dropdown. Be sure to leave adequate time for installation. If someone should attempt to run the Jump Client installer after this time, installation will fail, and a new Jump Client installer will have to be created. The validity time can be set for anywhere from 10 minutes to 1 year. This time does NOT affect how long the Jump Client remains active.

In addition to expiring after the period given by the **This Installer is Valid For** option, Jump Client mass deployment packages invalidate when their Bomgar Appliance is upgraded. The only exception to this rule is live updates which change the license count or license expiration date. Any other updates, even if they do not change the version number of the appliance, invalidate the Jump Client installers from before the upgrade. If these installers are MSI packages, they can still be used to uninstall Jump Clients if necessary.

Once a Jump Client has been installed, it remains online and active until it is uninstalled from the local system either by a logged-in user, by a Bomgar user from the access console's Jump interface, or by an uninstall script. A Bomgar user cannot remove a Jump Client unless the user is given appropriate permissions by their admin from the /login interface.

Attempt an Elevated Install if the Client Supports It

If **Attempt an Elevated Install if the Client Supports It** is selected, the installer will attempt to run with administrative rights, installing the Jump Client as a system service. If the elevated installation attempt is unsuccessful, or if this option is deselected, the installer will run with user rights, installing the Jump Client as an application. This option applies only to Windows and Mac operating systems.

> ***Note:*** *A Jump Client pinned in user mode is available only when that user is logged in. In contrast, a Jump Client pinned in service mode, with elevated rights, will allow that system to always be available, regardless of which user is logged in.*

Prompt for Elevation Credentials if Needed

If **Prompt for Elevation Credentials if Needed** is selected, the installer will prompt the user to enter administrative credentials if the system requires that these credentials be independently provided; otherwise, it will install the Jump Client with user rights. This applies only if an elevated install is being attempted.

Start Endpoint Client Minimized When Session Is Started

By selecting **Start Endpoint Client Minimized When Session Is Started**, the endpoint client will not take focus and will remain minimized in the taskbar or dock when a session is started through one of these Jump Clients.

Mass Deploy Help

For system administrators who need to push out the Jump Client installer to a large number of systems, the Windows, Mac, or Linux executable or the Windows MSI can be used with your systems management tool of choice. You can include a valid custom install directory path where you want the Jump Client to install. You can also override certain installation parameters specific to your needs. These parameters can be specified for both the MSI and the EXE using a systems administration tool or the command line interface. When you mark specific installation options for override during installation, you can use the following optional parameters to modify the Jump Client installer for individual installations. Note that if a parameter is passed on the command line but not

marked for override in the /login administrative interface, the installation will fail. If the installation fails, view the operating system event log for installation errors.

Command Line Parameter	Value	Description
--install-dir	<directory_path>	Specifies a new writable directory under which to install the Jump Client. This is supported only on Windows and Linux. When defining a custom install directory, ensure that the directory you are creating does not already exist and is in a location that can be written to.
--jc-jump-group	user:<username> team:<team-code-name>	If override is allowed, this command line parameter overrides the Jump Group specified in the Mass Deployment Wizard.
--jc-session-policy	<session-policy-code-name>	If override is allowed, this command line parameter sets the Jump Client's session policy that controls the permission policy during an access session.
--jc-jump-policy	<jump-policy-code-name>	If override is allowed, this command line parameter sets the Jump Policy that controls how users are allowed to Jump to the Jump Client.
--jc-tag	<tag-name>	If override is allowed, this command line parameter sets the Jump Client's tag.
--jc-comments	<comments ... >	If override is allowed, this command line parameter sets the Jump Client's comments.

Note: *When deploying an MSI installer on Windows using an msiexec command, the above parameters can be specified by:*

1. *Removing leading dashes (-)*
2. *Converting remaining dashes to underscores (_)*
3. *Assigning a value using an equal sign (=)*

Example:

```
msiexec /i bomgar-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfefggyezh7c40jc90 jc_jump_
group=team:general jc_tag=servers
```

The only exception to this rule is ***installdir****, which has a dash in the EXE version but no dashes in the MSI version.*

Download or Install the Client Now

Platform

Choose the operating system on which you wish to install this software. This dropdown defaults to the appropriate installer detected for your operating system.

Note that, unlike the access console, Jump Clients installed from an MSI do auto-update.

Download/Install

You can download the installer immediately if you plan to distribute it using a systems management tool or if you are at the computer to which you need later access.

Deploy to Email Recipients

Email

You can also email the installer to one or more remote users. Multiple recipients can install the client from the same link.

Jump Client Statistics

An administrator can choose which statistics to view for all Jump Clients on a site-wide basis. These statistics are displayed in the access console and include operating system, uptime, console user, CPU, disk usage, and a thumbnail of the remote screen. Existing Jump Clients will reflect changes to Jump Client statistics at the next update interval.

Jump Client Settings

Active Jump Client Statistics Update Interval

The **Active Jump Client Statistics Update Interval** determines how often these statistics are updated. Managing which statistics are viewed and how often can help to regulate the amount of bandwidth used. The more active Jump Clients you have deployed, the fewer the statistics and the longer the interval may need to be.

Maximum number of concurrent Jump Client upgrades

Also set the maximum number of Jump Clients to upgrade at the same time. Note that if you have a large number of Jump Clients deployed, you may need to limit this number to regulate the amount of bandwidth consumed.

> ***Note**: This settings does not affect access console upgrades.*

Maximum bandwidth of concurrent Jump Client upgrades

You may further regulate the bandwidth used during upgrades by setting **Maximum bandwidth of concurrent Jump Client upgrades**.

> ***Note**: This settings does not affect access console upgrades.*

Allow simultaneous user access to a single Jump Client

The option **Allow simultaneous user access to a single Jump Client** provides a way for multiple users to gain access to the same Jump Client without having to be invited to join an active session by another user. The first user to access the Jump Client maintains ownership of the session. Users in a shared Jump session will see each other and be able to chat.

Note: *This setting (implemented only in Windows) will prevent a customer from disabling or uninstalling a Jump Client from their local machine using the rightmouse button context menu on the system tray. To remove the Jump Client, users with the appropriate privileges on the client machine can do so using the standard Windows Add/Remove Programs functionality. If this setting is changed, it will be reapplied to a Jump Client the next time a connection with the appliance occurs.*

Allow user to attempt to wake up Jump Clients

Allow users to attempt to wake up Jump Clients provides a way to wake up a selected Jump Client by broadcasting Wake-on-LAN (WOL) packets through another Jump Client on the same network. Once a WOL is attempted, the option becomes unavailable for 30 seconds before a subsequent attempt can be made. WOL must be enabled on the target computer and its network for this function to work. The default gateway information of the Jump Client is used to determine if other Jump Clients reside on the same network. When sending a WOL packet, the user will have an advanced option to provide a password for WOL environments that require a secure WOL password.

Jump Client Default Connection Type

Set whether the default Jump Client connection type should be active or passive.

Passive Jump Client Port

The **Passive Jump Client Port** specifies which port a passive Jump Client will use to listen for a "wake up" command from the appliance. The default port is 5832. Ensure that firewall settings allow inbound traffic on this port for your hosts with passive Jump Clients. Once awake, Jump Clients always connect to the appliance on port 80 or 443 outbound.

Jump Policies: Set Schedules, Notifications, and Approvals for Jump Items

Jump Policies

Jump Policies are used to control when certain Jump Items can be accessed by implementing schedules, sending email notifications when a Jump Item is accessed, or requiring approval or user entry of a ticket system ID before a Jump Item may be accessed.

Add New Jump Policy, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Jump Policies :: Add

Display Name

Create a unique name to help identify this object. This name should help users identify this policy when assigning it to Jump Clients.

Code Name

Set a code name for integration purposes. If you do not set a code name, one will be created automatically.

Description

Add a brief description to summarize the purpose of this object.

Jump Schedule: Enabled

Set a schedule to define when Jump Clients under this policy can be accessed. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.

If, for instance, the time is set to start at 8 am and end at 5 pm, a user can start a session using this Jump Client at any time during this window but may continue to work past the set end time. They will not, however, be allowed to re-access this Jump Client after 5 pm.

Force session to end when schedule does not permit access

If stricter access control is required, check **Force session to end**. This forces the session to disconnect at the scheduled end time. In this case, the user receives recurring notifications beginning 15 minutes prior to being disconnected.

Jump Notification: Notify recipients when a session starts

If this option is checked, a notification email is sent to the designated recipients whenever a session is started with any Jump Client that uses this Jump Policy. When a user attempts to start a session with a Jump Client that uses this policy, a prompt states that a notification email will be sent and asks if the user would like to start the session anyway.

Notify recipients when a session ends

If this option is checked, a notification email is sent to the designated recipients whenever a session ends for any Jump Client that uses this Jump Policy. When a user attempts to start a session with a Jump Client that uses this policy, a prompt states that a notification email will be sent at the end of the session and asks if the user would like to start the session anyway.

Email Address(es)

Enter one or more email addresses to which emails should be sent. Separate addresses with a space. This feature requires valid SMTP configuration for your appliance, set up on the **/login > Management > Email Configuration** page.

Display Name

Enter the name of the email recipient. This name will appear on the prompt the user receives prior to a session with a Jump Client that uses this policy.

Locale

If more than one language is enabled on this site, set the language in which to send emails.

Jump Approval: Require a ticket ID before a session starts

If this option is checked, the user must enter a valid ticket ID before an access session can begin. When a user attempts to access an endpoint with this Jump Policy applied, the user must enter a ticket ID from your existing ITSM or ticket ID approval process before access is granted. Configure the ITSM or ticket system integration from the **Jump Policies :: Ticket System**section.

Require approval before a session starts

If this option is checked, an approval email is sent to the designated recipients whenever a session is attempted with any Jump Client that uses this Jump Policy. When a user attempts to start a session with a Jump Item that uses this policy, a dialog prompts the user to enter a request reason and the time and duration for the request.

Maximum Access Duration

Set the maximum length of time for which a user can request access to a Jump Client that uses this policy. The user can request a shorter length of access but no longer than that set here.

Email Address(es)

Enter one or more email addresses to which emails should be sent. Separate addresses with a space. This feature requires valid SMTP configuration for your appliance, set up on the **/login > Management > Email Configuration** page.

Display Name

Enter the name of the email recipient. This name will appear on the prompt the user receives prior to a session with a Jump Client that uses this policy.

Locale

If more than one language is enabled on this site, set the language in which to send emails.

Jump Policies :: Email Notification Template

Subject

Customize the subject of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Jump Policies :: Email Approval Template

Subject

Customize the subject of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Jump Policies :: Ticket System

Ticket System URL

In **Ticket System URL**, enter the URL for your external ticket system. The Bomgar Appliance sends an outbound request to your external ticketing system. The URL must be formatted for either HTTP or HTTPS. If an HTTPS URL is entered, the site certificate must be verified for a valid connection. If a Jump Policy requiring a ticket ID exists, a ticket system URL must be entered or you will receive a warning message.

Current Status

The **Current Status** field is shown only when a valid status value exists to report the connection to the ticket system configured in **Ticket System URL**. Any ticket system configuration change will reset the value.

Upload a certificate for HTTPS connection

Click **Choose File** to upload the certificate for the HTTPS ticket system connection to the appliance. If your certificate is uploaded, the appliance will use it when it contacts the external system. If you do not upload a certificate and the **Ignore SSL certificate**

errors box below this setting is checked, the Bomgar Appliance will optionally fall back to use the built-in certificate store when sending the request.

Ignore SSL certificate errors

If checked, the Bomgar appliance will **not** include the certificate validation information when it is contacting the external ticket system. Leave this box unchecked if you are uploading a certificate for secure HTTPS connection.

User Prompt

In **User Prompt** enter the dialog text you want access console users to see when they are requested to enter the ticket ID required for access.

Jumpoint: Set Up Unattended Access to a Network

Jumpoint Management

Bomgar's Jump Technology enables a user to access computers on a remote network without having to pre-install software on every machine. Simply install a single Jumpoint agent at any network location to gain unattended access to every PC within that network.

Add New Jumpoint, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Redeploy

Uninstall an existing Jumpoint and download an installer to replace the existing Jumpoint with a new one. Jump shortcuts associated with the existing Jumpoint will use the new Jumpoint once it is installed.

Note: *When an existing Jumpoint is replaced, its configuration is not saved. The new Jumpoint must be reconfigured.*

Jumpoint :: Add or Edit

Name

Create a unique name to help identify this object. This name should help users locate this Jumpoint when they need to start a session with a computer on its same network.

Code Name

Set a code name for integration purposes. If you do not set a code name, one will be created automatically.

Disabled

If checked, this Jumpoint is unavailable to make Jump connections.

Clustered

If checked, you will be able to add multiple, redundant nodes of the same Jumpoint on different host systems. This ensures that as long as at least one node remains online, the Jumpoint will be available.

Enable Shell Jump Method

If you want users to be able to connect to SSH-enabled and Telnet-enabled network devices through this Jumpoint, check **Enable Shell Jump Access**.

Add Users

Authorize at least one user to use this Jumpoint. From the Jumpoint edit page, you may authorize users to start sessions through this Jumpoint. After the Jumpoint has been created, you can also grant access to groups of users from **Users & Security > Group Policies**.

Jump Shortcuts Mass Import Wizard

When creating a large number of Jump shortcuts, it may be easier to import them via a spreadsheet than to add them one by one in the access console. From the dropdown in the **Jump Shortcuts Mass Import Wizard section**, select the type of Jump Item you wish to add, and then click **Download Template**. Using the text in the CSV template as column headers, add the information for each Jump shortcut you wish to import. Optional fields can be filled in or left blank.

Once you have completed filling out the template, use **Import Jump Shortcuts** to upload the CSV file containing the Jump Item information. Only one type of Jump Item can be included in each CSV file. The CSV file should use the format described in the tables below. The maximum file sized allowed to be uploaded at one time is 5 MB.

Local Jump Shortcut

Field	Description
Hostname	The hostname of the endpoint to be accessed by this Jump shortcut.
Jump Group	The code name of the team with which this Jump Item should be associated. ***Note:*** *Using the import method, a Jump Item cannot be associated with a personal Jump Group.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Remote Jump Shortcut

Field	Description
Hostname	The hostname of the endpoint to be accessed by this Jump shortcut.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Jump Group	The code name of the team with which this Jump Item should be associated.

Field	Description
	Note: *Using the import method, a Jump Item cannot be associated with a personal Jump Group.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Remote Desktop Protocol Shortcut

Field	Description
Hostname	The hostname of the endpoint to be accessed by this Jump shortcut.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Username (optional)	The username to sign in as.
Domain (optional)	The domain the endpoint is on.
Display Size (optional)	The resolution at which to view the remote system. Can be **primary** (default - the size of your primary monitor), **all** (the size of all of your monitors combined), or **XxY** (where **X** and **Y** are a supported width and height combination - e.g., **640x480**).
Quality (optional)	The quality at which to view the remote system. Can be **low** (2-bit gray scale for the lowest bandwidth consumption), **best_perf** (default - 8-bit color for fast performance), **perf_and_qual** (16-bit for medium quality image and performance), or **best_qual** (32-bit for the highest image resolution). This cannot be changed during the remote desktop protocol (RDP) session.
Console Session (optional)	**1**: Starts a console session. **0**: Starts a new session (default).
Ignore Untrusted Certificate (optional)	**1**: Ignores certificate warnings. **0**: Shows a warning if the server's certificate cannot be verified.
Jump Group	The code name of the team with which this Jump Item should be associated. ***Note:*** *Using the import method, a Jump Item cannot be associated with a personal Jump Group.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Session Policy	The code name of a session policy. You can specify a session policy to manage the permissions

Field	Description
(optional)	available on this Jump Item.

Shell Jump Shortcut

Field	Description
Hostname	The hostname of the endpoint to be accessed by this Jump shortcut.
Jumpoint	The code name of the Jumpoint through which the endpoint is accessed.
Username (optional)	The username to sign in as.
Protocol	Can be either **ssh** or **telnet**.
Port (optional)	A valid port number from **1** to **65535**. Defaults to **22** if the protocol is **ssh** or **23** if the protocol is **telnet**.
Terminal Type (optional)	Can be either **xterm** (default) or **VT100**.
Keep-Alive (optional)	The number of seconds between each packet sent to keep an idle session from ending. Can be any number from **0** to **300**. **0** disables keep-alive (default).
Jump Group	The code name of the team with which this Jump Item should be associated. ***Note:*** *Using the import method, a Jump Item cannot be associated with a personal Jump Group.*
Tag (optional)	You can organize your Jump Items into categories by adding a tag. This string has a maximum of 1024 characters.
Comments (optional)	You can add comments to your Jump Items. This string has a maximum of 1024 characters.
Jump Policy (optional)	The code name of a Jump Policy. You can specify a Jump Policy to manage access to this Jump Item.
Session Policy (optional)	The code name of a session policy. You can specify a session policy to manage the permissions available on this Jump Item.

Endpoint Analyzer: Report on Open Ports on Endpoints

Endpoint Analyzer Configuration

Enable Endpoint Analyzer

If enabled, a scan of open ports is performed once a day on all Jump Items.

TCP Ports

Enter the TCP ports that should be scanned. Enter multiple ports separated by a space or a comma, or enter a port range separated by a hyphen between the minimum port and maximum port.

UDP Ports

Enter the UDP ports that should be scanned. Enter multiple ports separated by a space or a comma, or enter a port range separated by a hyphen between the minimum port and maximum port.

Endpoint Analyzer Report

Jump Item Type

From the dropdown, select the type of Jump Item you wish to report on.

Jumpoint

You may narrow the results by reporting on only Jump Items that connect through a selected Jumpoint.

Include open ports that were already marked as expected

Narrow the results by excluding any ports that have already been marked as expected.

Endpoint Analyzer Results

View open ports found on the endpoints specified on the previous page. You can set ports as expected to allow them to be filtered from future reports. You can also set all ports to unexpected.

Access Console

Access Console Settings: Manage Default Access Console Settings

Manage Access Console Settings

You can configure the default access console settings for your entire user base, applying a consistent access console user experience and increasing team efficiency. You can force settings, allow settings to be overridden by the user, or leave settings unmanaged. If you select **Unmanaged**, the Bomgar default setting will be displayed alongside for your consideration.

Each **Enable** or **Disable** setting provides an administrative checkbox option to become a forced setting. Forced settings take effect on the user's next login and do not allow configuration in the console. Unforced settings may be overridden by a user through the settings window in the access console. A forced setting cannot be overridden unless an administrator deselects the **Forced** checkbox option for that setting in the /login administrative interface.

Choose the settings you want to be the default for your users, and click the **Save** button at the bottom of the page.

Note that saved settings take effect only upon login to the console. Even if you save and apply the changes by clicking the **Apply Now** button at the bottom of the page, detailed later, the user will not use the new settings until login.

If, for instance, you wish to set up default settings for new users but leave existing users' settings unchanged, save your managed settings but do not apply them. This will make it so all new access console logins will begin with your managed default settings. Existing users will have forced settings applied upon next login, but all other settings will remain unchanged.

Global Settings

Spell checking enabled

From the **Global Settings** section, you may choose to enable or disable spell check for chat. Currently, spell check is available for US English only.

Configurable session side bar

Choose if you want the session menu icon to display, if the sidebar can be detached, and if the widgets on the session sidebar can be rearranged and resized.

Alerts :: Chat Messages

Audible alerts - Play a sound when a chat message is received

Choose if a sound should be played when the user receives a chat message. If unmanaged or if enabled and not forced, the user may designate a custom sound in WAV format no larger than 1MB.

Visual alerts - Flash the application icon when a chat message is received

Choose if the application icon should flash when the user receives a chat message.

Show status messages in team chat windows

Choose if the team chat should include status messages, such as users logging in and out, or only chats sent between team members.

pop-up Notifications

Team Queues

Choose if a user should receive a pop-up notification for chat messages received in a team chat.

Access Sessions

Choose if a user should receive a pop-up notification for chat messages received in a access session

Alerts :: Queue Alerts

Audible alerts - Play a sound when a session enters any queue

Choose if a sound should be played when a session enters any of a user's queues.

pop-up Notifications

pop-up notifications appear independent of the access console and on top of other windows. If the pop-up notification is enabled and not forced or left unmanaged, the user will be able to choose how they receive pop-up notifications.

Personal Queue - Shared Sessions

Choose if a user should receive a pop-up notification for shared sessions in this queue.

Team Queues - Shared Sessions

Choose if a user should receive a pop-up notification for shared sessions in this queue.

pop-up Behavior - Location and Duration

Set the default location and duration for pop-up notifications.

Access Sessions :: Automatic Behavior

Automatically request screen sharing

Choose if you want your users' sessions to begin with screen sharing.

Automatically detach

Choose if you want to open sessions as tabs in the access console or to automatically detach sessions into new windows.

Automatically elevate local network Jump attempts

Choose if the endpoint client should automatically elevate to run as a system service when the user executes a local network Jump.

Prompt to elevate if endpoint's secure desktop is enabled

For situations where users may encounter issues due to a customer's having enabled secure desktop, you can allow your users to be prompted to elevate to run with administrative rights when the session begins.

Access Sessions :: Tools

Screen Sharing

Default Quality

Set the default quality for screen sharing sessions.

Default Scaling

Set the default size for screen sharing sessions.

Automatically enter full screen mode when screen sharing starts

When screen sharing starts, the user can automatically enter full screen mode.

Automatically collapse the sidebar when full screen mode is used

When the screen sharing session enters full screen mode, the chat bar can automatically collapse.

Command Shell

Number of lines of available command history

You can set the number of lines to save in the command shell history. The default value is 500 lines.

Save

Click **Save** to save all of the profile settings you have configured. The confirmation message **Settings profile was successfully saved** will appear at the top of the page. All users who log into the access console after you save a new profile will receive the new settings as the default settings.

Apply Managed Access Console Settings

Apply Now

If you wish to push the default settings to your entire user base, click **Apply Now**. The top of the page displays a confirmation message, **Settings profile was successfully applied**.

After applying new settings to your user base, the users will receive an alert dialog for confirmation when they first log into the access console after you apply the settings. The dialog warns them that their settings have changed and prompts them with the option simply to acknowledge the dialog or to open their access console settings window to review the changes.

Custom Links: Add URL Shortcuts to the Access Console

Custom Links

Create links to sites your users can access during sessions. Examples could be a link to a searchable knowledge base, giving users a chance to look for a solution to an issue on the endpoint system, or a customer relationship management (CRM) system.

Links created here become available through the **Links** button on the access console.

Create New Custom Link, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Custom Links :: Add or Edit

Name

Create a unique name to help identify this object.

URL

Add the URL to which this custom link should direct. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Canned Scripts: Create Scripts for Screen Sharing or Command Shell Sessions

Canned Scripts

Create custom scripts to be used in screen sharing and command shell sessions. The script will be displayed in the screen sharing or command shell interface as it is being executed. Executing a script in the screen sharing interface displays the running script on the remote screen.

Filter By

Filter your view by selecting a category or team from the dropdown at the top of the page.

Add New Canned Script, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Canned Script :: Add or Edit

Script Name

Create a unique name to help identify this object. This name should help users locate the script they wish to run.

Description

Add a brief description to summarize the purpose of this object. This description is displayed on the prompt to confirm that the user wants to run the selected script.

Command Sequence

Write the command sequence. Scripts must be written in command line format, similar to writing a batch file or shell script. Note that only the last line of the script may be interactive; you cannot prompt for input in the middle of the script.

Within the script, reference an associated resource file using **"%RESOURCE_FILE%"**, making sure to include the quotation marks. Please note that the command sequence is case sensitive.

You can access the resource file's temporary directory using **%RESOURCE_DIR%**. When you run a script with an associated resource file, that file will be temporarily uploaded to the customer's computer.

Teams

Select which teams should be able to use this item.

Categories

Select the category under which this item should be listed.

Resource File

You may select a resource file to be associated with this script.

Elevation Mode

Select if this script should be available to run in elevated mode only, unelevated mode only, or both.

Categories

Add Category, Delete

Create a new category or remove an existing category.

Resources

Upload

Add any resource files you want to access from within your scripts. You may upload up to 100 MB to your resource file directory.

Delete

Remove an existing resource file.

Special Actions: Create Custom Special Actions

Custom Special Actions

Create custom special actions to speed your processes. Custom special actions can be created for Windows, Mac, and Linux systems.

Add New Custom Special Action, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Add or Edit Special Action

Action Name

Create a unique name to help identify this object. During a session, a user can see this name on the special actions dropdown.

Command

In the **Command** field, enter the full path of the application you wish to run. Do not use quotation marks; they will be added as necessary. Windows systems may make use of the macros provided. If the command cannot be located on the remote system, then this custom special action will not appear in the user's list of special actions.

Arguments

If the provided command will accept command line arguments, you may enter those arguments next. Arguments may use quotation marks if necessary, and arguments for Windows systems may use the provided macros. For help with Windows arguments, search for "command line switches" on msdn.microsoft.com.

Confirm

If you check the **Confirm** box, then users will be prompted to confirm that they want to run this special action before it will execute. Otherwise, selecting the custom special action from the menu during a session will cause that special action to run immediately.

Run Elevated

Checking this option causes this special action to appear only when the endpoint client is running in elevated mode. When you run a custom action in elevated mode, you will be prompted either to run it as the system user or to provide credentials for another valid account on the remote system.

Special Actions Settings

Show Built-In Special Actions

If you want to enable the default special actions provided by Bomgar, check **Show Built-In Special Actions**. Otherwise, to enable only your custom special actions, deselect this option.

Note: *The* ***Windows Security (Ctrl-Alt-Del)*** *special action cannot be disabled.*

Users and Security

Users: Add Account Permissions for a User or Admin

User Accounts

View information about all users who have access to your Bomgar Appliance, including local users and those who have access through security provider integration.

Create New User, Edit, Delete

Create a new object, modify an existing object, or remove an existing object. You cannot delete your own account.

Synchronize

Synchronize the users and groups associated with an external security provider. Synchronization occurs automatically once a day. Clicking this button forces a manual synchronization.

Search

Search user accounts based on username and display name.

Reset

If a user has one or more failed login attempts, click the **Reset** button beside their name to reset the number back to 0.

User :: Add or Edit

User Settings

Username

Unique identifier used to log in.

Display Name

User's name as shown in team chats, in reports, etc.

Email Address

Set the email address to which email notifications are sent, such as password resets or extended availability mode alerts.

Preferred Email Language

If more than one language is enabled on this site, set the language in which to send emails.

Password

Password used with the username to log in. The password may be set to whatever you choose, as long as the string complies with the defined policy set on the **/login > Management > Security** page.

Email Password to User

Send an automatic email to the user containing their new password. If this option is selected, then the user must reset their password at next login. This feature requires valid SMTP configuration for your appliance, set up on the **/login > Management > Email Configuration** page.

Must Reset Password at Next Login

If this option is selected, then the user must reset their password at next login.

Password Expires On

Causes the password to expire after a given date or never to expire.

Security Question and Security Answer

The security question and answer allow a user to reset a forgotten password after providing the correct answer to the question. Passwords may be reset only if **Enable Password Reset** is checked on the **Management > Security** page. Admins cannot reset their passwords using the security question.

Group Policy Memberships

Listing of the group policies to which the user belongs, linking to the **Group Policy** page or the policies themselves.

Team Memberships

Listing of the teams to which the user belongs, linking to the **Teams** page or the teams themselves.

Account Settings

Last Authentication Date

The date and time when this user last logged in.

Email Login Code

Enables multifactor authentication. Users receive an email with a unique authentication code each time they log in to the /login administrative interface, or the access console, both desktop and mobile. If the code is entered incorrectly three consecutive times, users will have to re-enter their credentials and enter a new email code.

Account Expires On

Causes the account to expire after a given date or never to expire.

Account Disabled

Disables the account so the user cannot log in. Disabling does NOT delete the account.

Comments

Add comments to help identify the purpose of this object.

Permissions

Administrator

Grants the user full administrative rights.

Allowed to Set Passwords

Enables the user to set passwords and unlock accounts for non-administrative local users.

Allowed to Edit Jumpoints

Enables the user to create or edit Jumpoints. This option does not affect the user's ability to access remote computers via Jumpoint, which is configured per Jumpoint or group policy.

Access Session Reporting Permissions: Allowed to View Access Session Reports

Enables the user to run reports on access session activity, viewing only sessions for which they were the primary session owner, only sessions in which one of their teams was the primary team or one of their teammates was the primary session owner, or all sessions.

Allowed to view access session recordings

Enables the user to view video recordings of screen sharing sessions and command shell sessions.

Allowed to Use Reporting API

Enables the user's credentials to be used to pull XML reports via the API.

Allowed to Use Command API

Enables the user's credentials to be used to issue commands via the API.

Allowed to Edit Teams

Enables the user to create or edit teams.

Allowed to Edit Canned Scripts

Enables the user to create or edit canned scripts for use in screen sharing or command shell sessions.

Allowed to Edit Custom Links

Enables the user to create or edit custom links.

Access Permissions

Access

Allowed to access endpoints

Enables the user to use the access console in order to run sessions. If endpoint access is enabled, options pertaining to endpoint access will also be available.

Session Management

Allowed to share sessions with teams which they do not belong to

Enables the user to invite a less limited set of user to share sessions, not only their team members. Combined with the extended availability permission, this permission expands session sharing capabilities.

Allowed to invite external users

Enables the user to invite a third-party user to participate in a session one time only.

Allowed to enable extended availability mode

Enables the user to receive email invitations from other users requesting to share a session even when they are not logged into the access console.

Allowed to edit the external key

Enables the user to modify the external key from the session info pane of a session within the access console.

User to User Screen Sharing

Allowed to show screen to other users

Enables the user to share their screen with another user without the receiving user having to join a session. This option is available even if the user is not in a session.

Allowed to give control when showing screen to other users

Enables the user sharing their screen to give keyboard and mouse control to the user viewing their screen.

Jump Technology

Allowed Jump Methods: Allowed to start sessions through Jump Clients which use any of the following Jump methods

Enables the user to Jump to computers using **Jump Clients**, **Local Jump on the local network**, **Remote Jump via a Jumpoint**, **RDP via a Jumpoint**, and/or **Shell Jump via a Jumpoint**.

Jump Item Permissions: Allowed to start sessions from all Jump Items within the system

Enables the user to Jump to remote computers in all team Jump Groups.

Allowed to deploy, remove and modify Jump Items in the following Jump Groups

Enables the user to pin sessions, set groups, and add comments to Jump Items only for their personal Jump Group; for team and team members' Jump Groups; or for all Jump Groups, including those deployed to teams to which the user does not belong as well as to any user's personal Jump Group.

Allowed to change the Session Policies associated with Jump Items

Enables the user to set the session policy a Jump Item should use. Changing the session policy may affect the permissions allowed in the session.

Session Permissions

Set the prompting and permission rules that should apply to this user's sessions. Choose an existing session policy or define custom permissions for this user. If **Not Defined**, the global default policy will be used. These permissions may be overridden by a higher policy.

Description

View the description of a pre-defined session permission policy.

Screen Sharing

Screen Sharing

Enable the user to view or control the remote screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Application Sharing Restrictions

Limit access to specified applications on the remote system with either **Allow only the listed executables** or **Deny only the listed executables**. You may also choose to allow or deny desktop access.

> ***Note:*** *This feature applies only to Windows and Linux operating systems and does not include Remote Desktop Protocol (RDP) sessions.*

Add New Executables

If application sharing restrictions are enforced, an **Add New Executables** button appears. Clicking this button opens a dialog that allows you to specify executables to deny or allow, as appropriate to your objectives.

After you have added executables, one or two tables display the file names or hashes you have selected for restriction. An editable comment field allows administrative notes.

Enter file names or SHA-256 hashes, one per line

When restricting executables, manually enter the executable file names or hashes you wish to allow or deny. Click on **Add Executable(s)** when you are finished to add the chosen files to your configuration.

You may enter up to 25 files per dialog. If you need to add more, click **Add Executable(s)** and then reopen the dialog.

Browse for one or more files

When restricting executables, select this option to browse your system and choose executable files to automatically derive their names or hashes. If you select files from your local platform and system in this manner, use caution to ensure that the files are indeed executable files. No browser level verification is performed.

Choose either **Use file name** or **Use file hash** to have the browser derive the executable file names or hashes automatically. Click **Add Executable(s)** when you are finished to add the chosen files to your configuration.

You may enter up to 25 files per dialog. If you need to add more, click **Add Executable(s)** and then reopen the dialog.

> ***Note:*** *This option is available only in modern browsers, not in legacy browsers.*

Allowed Endpoint Restrictions

Set if the user can suspend the remote system's mouse and keyboard input. The user may also prevent the remote desktop from being displayed.

Allowed to login using credentials from an Endpoint Credential Manager

Enable connection of a user to your Endpoint Credential Manager to use credentials from your existing password stores or vaults.

Use of the Endpoint Credential Manager requires a separate services agreement with Bomgar. Once a services agreement is in place, you may download the required middleware from the Bomgar self-service center.

> ***Note:*** *Prior to 15.2, this feature is available only in sessions started from an elevated Jump Client on Windows®. Starting with 15.2, you also may use an Endpoint Credential Manager in remote Jump sessions, Microsoft® Remote Desktop Protocol sessions, and Shell Jump sessions. You may also use this feature with the Run As special action in a screen sharing session on a Windows® system.*

Annotations

Enables the user to use annotation tools to draw on the remote system's screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

File Transfer

File Transfer

Enables the user to upload files to the remote system, download files from the remote system, or both. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Accessible paths on the endpoint's filesystem

Allow the user to transfer files to or from any directories on the remote system or only specified directories.

Accessible paths on user's filesystem

Allow the user to transfer files to or from any directories on their local system or only specified directories.

Command Shell

Command Shell

Enables the user to issue commands on the remote computer through a virtual command line interface. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

System Information

System Info

Enables the user to see system information about the remote computer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to use system information actions

Enables the user to interact with processes and programs on the remote system without requiring screen sharing. Kill processes; start, stop, pause, resume, and restart services; and uninstall programs.

Registry Access

Registry Access

Enables the user to interact with the registry on a remote Windows system without requiring screen sharing. View, add, delete and edit keys, search and import/export keys.

Other Tools

Canned Scripts

Enables the user to run canned scripts that have been created for their teams. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Elevation

Enables the user to attempt to elevate the endpoint client to run with administrative rights on the remote system. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Login Schedule

Restrict user login to the following schedule

Set a schedule to define when users can log into the access console. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.

If, for instance, the time is set to start at 8 am and end at 5 pm, a user can log in at any time during this window but may continue to work past the set end time. They will not, however, be allowed to log back in after 5 pm.

Force logout when the schedule does not permit login

If stricter access control is required, check this option. This forces the user to log out at the scheduled end time. In this case, the user receives recurring notifications beginning 15 minutes prior to being disconnected. When the user is logged out, any owned sessions will follow the session fallback rules.

User Account Report

Export detailed information about your users for auditing purposes. Gather detailed information for all users, users from a specific security provider, or just local users. Information collected includes data displayed under the “show details” button, plus group policy and team memberships and permissions.

User Accounts for Password Reset: Allow Users to Administer Passwords

User Accounts

Administrators can delegate, via user permission, the task of resetting local users' passwords and locked user accounts to privileged users, without also granting full administrator permissions. Local users may continue to reset their own passwords.

Note: *Administrators with the* ***Allowed to set passwords*** *permission will see no difference in the user interface.*

When a privileged non-administrative user enters the **Users & Security > Users** page in the administrative /login interface, they will see a limited view **Users** screen containing **Change Password** links for non-administrative users. The privileged user will not be able to edit or delete user accounts. Privileged users are not allowed to reset administrator passwords, nor the passwords of security provider users.

Search

Search user accounts based on username and display name.

Reset

If a user has one or more failed login attempts, click the **Reset** button beside their name to reset the number back to 0.

Change Password

Change the password for a non-administrative user.

User :: Change Password

Username

Unique identifier used to log in. This field is not editable.

Display Names

User's name as shown in team chats, in reports, etc. This field is not editable.

Email Address

The email address to which email notifications are sent, such as password resets or extended availability mode alerts. This field is not editable.

Comments

Comments about the account. This field is not editable.

Password

The new password to assign to this user account. The password may be set to whatever you choose, as long as the string complies with the defined policy set on the **/login > Management > Security** page.

Email Password to User

Send an automatic email to the user containing their new password. If this option is selected, then the user must reset their password at next login. This feature requires valid SMTP configuration for your appliance, set up on the **/login > Management > Email Configuration** page.

Must Reset Password at Next Login

If this option is selected, then the user must reset their password at next login.

Access Invite: Create Profiles to Invite External Users to Sessions

Access Invitation Email

With access invite, a privileged user can invite an external user to join a session one time only. When the user makes the invitation, they will select a security profile to determine what level of privileges the external user should be granted. Access invite security profiles are configured as session policies on the **Users & Security > Session Policies** page and must be enabled for access invite use.

The invitation email is sent to external users when you invite them to join a session.

Subject

Customize the subject of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Security Providers: Enable LDAP, Active Directory, RADIUS, and Kerberos Logins

Security Providers

You can configure your Bomgar Appliance to authenticate users against existing LDAP, RADIUS, or Kerberos servers, as well as to assign privileges based on the pre-existing hierarchy and group settings already specified in your servers. Kerberos enables single sign-on, while RSA and other multifactor authentication mechanisms via RADIUS provide an additional level of security.

Create Provider

Create a new security provider configuration. From the dropdown, select to create an LDAP provider, a RADIUS provider, or a Kerberos provider.

View Log

View the status history for a security provider connection.

Sync

Synchronize the users and groups associated with an external security provider. Synchronization occurs automatically once a day. Clicking this button forces a manual synchronization.

Disable

Disable this security provider connection. This is useful for scheduled maintenance, when you want a server to be offline but not deleted.

Edit, Delete

Modify an exiting object or remove an existing object.

Create Copy

Create a copy of an existing security provider configuration. This will be added as a top-level security provider and not as part of a cluster.

Duplicate Node

Create a copy of an existing clustered security provider configuration. This will be added as a new node in the same cluster.

Upgrade to Cluster

Upgrade a security provider to a security provider cluster. To add more security providers to this cluster, copy an existing node.

Change Order

Click this button to drag and drop security providers to set their priority. You can drag and drop servers within a cluster; clusters can be dragged and dropped as a whole. Click **Save Order** for prioritization changes to take effect.

Security Providers :: Edit - LDAP

General Settings

Name

Create a unique name to help identify this object.

Enabled: This provider is enabled

If checked, your Bomgar Appliance can search this security provider when a user attempts to log in. If unchecked, this provider will not be searched.

User Display Names: Keep display name synchronized with remote system

These values determine which fields should be used as the user's private and public display names.

Synchronization: Enable LDAP object cache

If checked, LDAP objects visible to the appliance are cached and synchronized nightly, or manually, if desired. When using this option, fewer connections are made to the LDAP server for administrative purposes thereby potentially increasing speed and efficiency.

If unchecked, changes to the LDAP server are immediately available without the need to synchronize. However, when you make changes on user policies through the administrative interface, several short-lived LDAP connections may occur as necessary.

For providers that have previously had the synchronization setting enabled, disabling or unchecking the synchronization option will cause all cached records that are currently not in use to be deleted.

Authorization Settings

Lookup Groups

Choose to use this security provider only for user authentication, only for group lookups, or for both.

Default Group Policy *(Visible Only if User Authentication Allowed)*

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your Bomgar Appliance, logging into either the /login interface or the access console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

Note that if a default policy is defined, then any allowed user who authenticates against this server will potentially have access at the level of this default policy. Therefore, it is recommended that you set the default to a policy with minimum privileges to prevent users from gaining permissions that you do not wish them to have.

Note: *If a user is in a default group policy and is then specifically added to another group policy, the settings for the specific policy will always take precedence over the settings for the default, even if the specific policy is a lower priority than the default, and even if the default policy's settings are set to disallow override.*

Connection Settings

Hostname

Enter the hostname of the server that houses your external directory store.

Note: *If you will be using* ***LDAPS*** *or* ***LDAP with TLS****, the hostname must match the hostname used in your LDAP server's public SSL certificate's subject name or the DNS component of its alternate subject name.*

Port

Specify the port for your LDAP server. This is typically port **389** for LDAP or port **636** for LDAPS. Bomgar also supports global catalog over port **3268** for LDAP or **3269** for LDAPS.

Encryption

Select the type of encryption to use when communicating with the LDAP server. For security purposes, **LDAPS** or **LDAP with TLS** is recommended.

Note: *Regular LDAP sends and receives data in clear text from the LDAP server, potentially exposing sensitive user account information to packet sniffing. Both LDAPS and LDAP with TLS encrypt user data as it is transferred, making these methods recommended over regular LDAP. LDAP with TLS uses the StartTLS function to initiate a connection over clear text LDAP but then elevates this to an encrypted connection. LDAPS initiates the connection over an encrypted connection without sending any data in clear text whatsoever.*

If you select **LDAPS** or **LDAP with TLS**, you must upload the Root SSL Certificate used by your LDAP server. This is necessary to ensure the validity of the server and the security of the data. The Root Certificate must be in PEM format.

Note: *If the LDAP server's public SSL certificate's subject name or the DNS component of its alternate subject name does not match the value in the* ***Hostname*** *field, the provider will be treated as unreachable. You can, however, use a wildcard certificate to certify multiple subdomains of the same site. For example, a certificate for* ****.example.com*** *would certify both* ***access.example.com*** *and* ***remote.example.com****.*

Bind Credentials

Specify a username and password with which your Bomgar Appliance can bind to and search the LDAP directory store.

If your server supports anonymous binds, you may choose to bind without specifying a username and password. Anonymous binding is considered insecure and is disabled by default on most LDAP servers.

Connection Method

If you are using an external directory store in the same LAN as your Bomgar Appliance, the two systems may be able to communicate directly, in which case you can leave the option **Proxy from appliance through the Connection Agent** unchecked and move on.

If the two systems are unable to communicate directly, such as if your external directory server is behind a firewall, you must use a connection agent. Downloading the Win32 connection agent enables your directory server and your Bomgar Appliance to communicate via an SSL-encrypted, outbound connection, with no firewall configuration. The connection agent can be downloaded to either the directory server or a separate server on the same network as your directory server (recommended).

In the case above, check **Proxy from appliance through the Connection Agent**. Create a **Connection Agent Password** for use in the connection agent installation process. Then click **Download Connection Agent**, run the installer, and follow the installation wizard. During installation, you will be prompted to enter the security provider name and the connection agent password you created above.

Directory Type

To aid in configuring the network connection between your Bomgar Appliance and your security provider, you can select a directory type as a template. This pre-populates the configuration fields below with standard data but must be modified to match your security provider's specific configuration. Active Directory LDAP is the most common server type, though you can configure Bomgar to communicate with most types of security providers.

Cluster Settings *(Visible Only for Clusters)*

Member Selection Algorithm

Select the method to search the nodes in this cluster.

Top-to-bottom first attempts the server with the highest priority in the cluster. If that server is unavailable or the account is not found, the next highest priority server is attempted. The search moves down through the list of clustered servers until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Round-robin is designed to balance the load between multiple servers. The algorithm choose at random which server to attempt first. If that server is unavailable or the account is not found, another random server is attempted. The search continues at random through the remaining servers in the cluster until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Retry Delay

Set how long to wait after a cluster member becomes unavailable before trying that cluster member again.

User Schema Settings

Override Cluster Values *(Visible Only for Cluster Nodes)*

If this option is unchecked, this cluster node will use the same schema settings as the cluster. If unchecked, you may modify the schema settings below.

Search Base DN

Determine the level in your directory hierarchy, specified by a distinguished name, at which the Bomgar Appliance should begin searching for users. Depending on the size of your directory store and the users who require Bomgar accounts, you may improve performance by designating the specific organizational unit within your directory store that requires access. If you are not sure or if users span multiple organizational units, you may want to specify the root distinguished name of your directory store.

User Query

Specify the query information that the Bomgar Appliance should use to locate an LDAP user when the user attempts to log in. The **User Query** field accepts a standard LDAP query (RFC 2254 – String Representation of LDAP Search Filters). You can modify the query string to customize how your users log in and what methods of usernames are accepted. To specify the value within the string that should act as the username, replace that value with *.

Browse Query

The browse query affects how results are displayed when browsing via group policies. This filters results so that only certain results display in the member selection dropdown when adding members to a group policy.

Object Classes

Specify valid object classes for a user within your directory store. Only users who posses one or more of these object classes will be permitted to authenticate. These object classes are also used with the attribute names below to indicate to your Bomgar Appliance the schema the LDAP server uses to identify users. You can enter multiple object classes, one per line.

Attribute Names

Specify which fields should be used for a user's unique ID and display name.

Unique ID

This field requests a unique identifier for the object. While the distinguished name can serve as this ID, a user's distinguished name may change frequently over the life of the user, such as with a name or location change or with the renaming of the LDAP store. Therefore, most LDAP servers incorporate some field that is unique per object and does not change for the lifetime of the user. If you do use the distinguished name as the unique ID and a user's distinguished name changes, that user will be seen as a new user, and any changes made specifically to the individual's Bomgar user account will not be carried over to the new user. If your LDAP server does not incorporate a unique identifier, use a field that is least likely to have an identical entry for another user.

Use the same attribute for public and private display names

If this option is checked, you may specify separate values for the user's private and public display names.

Display Names

These values determines which fields should be used as the user's private and public display names.

Group Schema Settings *(Visible Only if Performing Group Lookups)*

Search Base DN

Determine the level in your directory hierarchy, specified by a distinguished name, at which the Bomgar Appliance should begin searching for groups. Depending on the size of your directory store and the groups that require access to the Bomgar Appliance, you may improve performance by designating the specific organizational unit within your directory store that requires access. If you are not sure or if groups span multiple organizational units, you may want to specify the root distinguished name of your directory store.

Browse Query

The browse query affects how results are displayed when browsing via group policies. This filters results so that only certain results display in the member selection dropdown when adding members to a group policy.

Object Classes

Specify valid object classes for a group within your directory store. Only groups that posses one or more of these object classes will be returned. These object classes are also used with the attribute names below to indicate to your Bomgar Appliance the schema the LDAP server uses to identify groups. You can enter multiple group object classes, one per line.

Attribute Names

Specify which fields should be used for a group's unique ID and display name.

Unique ID

This field requests a unique identifier for the object. While the distinguished name can serve as this ID, a group's distinguished name may change frequently over the life of a group, such as with a location change or with the renaming of the LDAP store. Therefore, most LDAP servers incorporate some field that is unique per object and does not change for the lifetime of the group. If you do use the distinguished name as the unique ID and a group's distinguished name changes, that group will be seen as a new group, and any group policies defined for that group will not be carried over to the new group. If your LDAP server does not incorporate a unique identifier, use a field that is least likely to have an identical entry for another group.

Display Name

This value determines which field should be used as the group's display name.

User to Group Relationships

This field requests a query to determine which users belong to which groups or, conversely, which groups contain which users.

Perform recursive search for groups

You can choose to perform a recursive search for groups. This will run a query for a user, then queries for all of the groups to which that user belongs, then queries for all groups to which those groups belong, and so forth, until all possible groups associated with that user have been found.

Running a recursive search can have a significant impact on performance, as the server will continue to issue queries until it has found information about all groups. If it takes too long, the user may be unable to log in.

A non-recursive search will issue only one query per user. If your LDAP server has a special field containing all of the groups to which the user belongs, recursive search is unnecessary. Recursive search is also unnecessary if your directory design does not handle group members of groups.

Test Settings

Username and Password

Enter a username and password for an account that exists on the server you are testing. This account must match the criteria for login specified in the configuration above.

Try to obtain user attributes and group memberships if the credentials are accepted

If this option is checked, your successful credential test will also attempt to check user attributes and group lookup. Note that for these features to be successfully tested they must be supported and configured in your security provider.

Start Test

If your server is properly configured and you have entered a valid test username and password, you will receive a success message. Otherwise, you will see an error message and a log that will help in debugging the problem.

Security Providers :: Edit - RADIUS

General Settings

Name

Create a unique name to help identify this object.

Enabled: This provider is enabled

If checked, your Bomgar Appliance can search this security provider when a user attempts to log in. If unchecked, this provider will not be searched.

Display Names: Keep display name synchronized with remote system

These values determine which fields should be used as the user's private and public display names.

Authorization Settings

Only allow the following users

You can choose to allow access only to specified users on your RADIUS server. Enter each username separated by a line break. Once entered, these users will be available from the **Add Policy Member** dialog when editing group policies on the **/login > Users & Security > Group Policies** page.

If you leave this field blank, all users who authenticate against your RADIUS server will be allowed; if you allow all, you must also specify a default group policy.

LDAP Group Lookup

If you want users on this security provider to be associated with their groups on a separate LDAP server, choose one or more LDAP group servers to use for group lookup.

Default Group Policy

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your Bomgar Appliance, logging into either the /login interface or the access console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

Connection Settings

Hostname

Enter the hostname of the server that houses your external directory store.

Port

Specify the authentication port for your RADIUS server. This is typically port **1812**.

Connection Method

If you are using an external directory store in the same LAN as your Bomgar Appliance, the two systems may be able to communicate directly, in which case you can leave the option **Proxy from appliance through the Connection Agent** unchecked and move on.

If the two systems are unable to communicate directly, such as if your external directory server is behind a firewall, you must use a connection agent. Downloading the Win32 connection agent enables your directory server and your Bomgar Appliance to communicate via an SSL-encrypted, outbound connection, with no firewall configuration. The connection agent can be downloaded to either the directory server or a separate server on the same network as your directory server (recommended).

In the case above, check **Proxy from appliance through the Connection Agent**. Create a **Connection Agent Password** for use in the connection agent installation process. Then click **Download Connection Agent**, run the installer, and follow the installation wizard. During installation, you will be prompted to enter the security provider name and the connection agent password you created above.

Shared Secret

Provide a new shared secret so that your Bomgar Appliance and your RADIUS server can communicate.

Timeout (seconds)

Set the length of time to wait for a response from the server. Note that if the response is **Response-Accept** or **Response-Challenge**, then RADIUS will wait the entire time specified here before authenticating the account. Therefore, it is encouraged to keep this value as low as reasonably possible given your network settings. An ideal value is 3-5 seconds, with the maximum value at three minutes.

Cluster Settings *(Visible Only for Clusters)*

Member Selection Algorithm

Select the method to search the nodes in this cluster.

Top-to-bottom first attempts the server with the highest priority in the cluster. If that server is unavailable or the account is not found, the next highest priority server is attempted. The search moves down through the list of clustered servers until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Round-robin is designed to balance the load between multiple servers. The algorithm choose at random which server to attempt first. If that server is unavailable or the account is not found, another random server is attempted. The search continues at random through the remaining servers in the cluster until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Retry Delay

Set how long to wait after a cluster member becomes unavailable before trying that cluster member again.

Test Settings

Username and Password

Enter a username and password for an account that exists on the server you are testing. This account must match the criteria for login specified in the configuration above.

Try to obtain user attributes and group memberships if the credentials are accepted

If this option is checked, your successful credential test will also attempt to check user attributes and group lookup. Note that for these features to be successfully tested they must be supported and configured in your security provider.

Start Test

If your server is properly configured and you have entered a valid test username and password, you will receive a success message. Otherwise, you will see an error message and a log that will help in debugging the problem.

Security Providers :: Edit - Kerberos

General Settings

Name

Create a unique name to help identify this object.

Enabled: This provider is enabled

If checked, your Bomgar Appliance can search this security provider when a user attempts to log in. If unchecked, this provider will not be searched.

User and Display Names: Keep display name synchronized with remote system

These values determine which fields should be used as the user's private and public display names.

Strip realm from principal names

Select this option to remove the REALM portion from the User Principal Name when constructing the Bomgar username.

Authorization Settings

User Handling Mode

Select which users can authenticate to your Bomgar Appliance. **Allow all users** allows anyone who currently authenticates via your KDC. **Allow only user principals specified in the list** allows only user principles explicitly designated. **Allow only user principals that match the regex** allows only users principals who match a Perl-compatible regular expression (PCRE).

SPN Handling Mode: Allow only SPNs specified in the list

If unchecked, all configured Service Principal Names (SPNs) for this security provider are allowed. If checked, select specific SPNs from a list of currently configured SPNs.

LDAP Group Lookup

If you want users on this security provider to be associated with their groups on a separate LDAP server, choose one or more LDAP group servers to use for group lookup.

Default Group Policy

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your Bomgar Appliance, logging into either the /login interface or the access console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

Session Policies: Set Session Permission and Prompting Rules

Session Policies

With session policies, you can customize session security permissions to fit specific scenarios. Session policies can be applied to users and Jump Clients.

The **Session Policies** section lists available policies. Click the arrow by a policy name to quickly see where that policy is being used; its availability for users, access invites, and Jump Clients; and the tools configured.

Create New Policy, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Copy

To expedite the creation of similar policies, click **Copy** to create a new policy with identical settings. You can then edit this new policy to meet your specific requirements.

Session Policy :: Add or Edit

Policy Settings

Display Name

Create a unique name to help identify this object. This name helps when assigning a session policy to users and Jump Clients.

Code Name

Set a code name for integration purposes. If you do not set a code name, one will be created automatically.

Description

Add a brief description to summarize the purpose of this object. The description is seen when applying a policy to user accounts, group policies, and access invites.

Availability: Users

Choose if this policy should be available to assign to users (user accounts and group policies).

Availability: Access Invite

Choose if this policy should be available for users to select when inviting an external user to join a session.

Availability: Jump Clients

Choose if this policy should be available to assign to Jump Clients.

Availability: Dependencies

If this session policy is already in use, you will see the number of users and Jump Clients using this policy.

Tools

For all of the permissions that follow, you can choose to enable or disable the permission, or you can choose to set it to **Not Defined**. Session policies are applied to a session in a hierarchical manner, with Jump Clients taking the highest priority, then users, and then the global default. If multiple policies apply to a session, then the policy with the highest priority will take precedence over the others. If, for example, the policy applied to a Jump Client defines a permission, then no other policies may change that permission for the session. To make a permission available for a lower policy to define, leave that permission set to **Not Defined**. For details and examples, see How to Use Session Policies.

Set which tools should be enabled or disabled with this policy.

Screen Sharing

Enable the user to view or control the remote screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Application Sharing Restrictions

Limit access to specified applications on the remote system with either **Allow only the listed executables** or **Deny only the listed executables**. You may also choose to allow or deny desktop access.

> ***Note:*** *This feature applies only to Windows and Linux operating systems and does not include Remote Desktop Protocol (RDP) sessions.*

Add New Executables

If application sharing restrictions are enforced, an **Add New Executables** button appears. Clicking this button opens a dialog that allows you to specify executables to deny or allow, as appropriate to your objectives.

After you have added executables, one or two tables display the file names or hashes you have selected for restriction. An editable comment field allows administrative notes.

Enter file names or SHA-256 hashes, one per line

When restricting executables, manually enter the executable file names or hashes you wish to allow or deny. Click on **Add Executable(s)** when you are finished to add the chosen files to your configuration.

You may enter up to 25 files per dialog. If you need to add more, click **Add Executable(s)** and then reopen the dialog.

Browse for one or more files

When restricting executables, select this option to browse your system and choose executable files to automatically derive their names or hashes. If you select files from your local platform and system in this manner, use caution to ensure that the files are indeed executable files. No browser level verification is performed.

Choose either **Use file name** or **Use file hash** to have the browser derive the executable file names or hashes automatically. Click **Add Executable(s)** when you are finished to add the chosen files to your configuration.

You may enter up to 25 files per dialog. If you need to add more, click **Add Executable(s)** and then reopen the dialog.

> ***Note:*** *This option is available only in modern browsers, not in legacy browsers.*

Allowed Endpoint Restrictions

Set if the user can suspend the remote system's mouse and keyboard input. The user may also prevent the remote desktop from being displayed.

Allowed to login using credentials from an Endpoint Credential Manager

Enable connection of a user to your Endpoint Credential Manager to use credentials from your existing password stores or vaults.

Use of the Endpoint Credential Manager requires a separate services agreement with Bomgar. Once a services agreement is in place, you may download the required middleware from the Bomgar self-service center.

> ***Note:*** *Prior to 15.2, this feature is available only in sessions started from an elevated Jump Client on Windows®. Starting with 15.2, you also may use an Endpoint Credential Manager in remote Jump sessions, Microsoft® Remote Desktop Protocol sessions, and Shell Jump sessions. You may also use this feature with the Run As special action in a screen sharing session on a Windows® system.*

Annotations

Enables the user to use annotation tools to draw on the remote system's screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

File Transfer

Enables the user to upload files to the remote system, download files from the remote system, or both. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Accessible paths on the endpoint's filesystem

Allow the user to transfer files to or from any directories on the remote system or only specified directories.

Accessible paths on user's filesystem

Allow the user to transfer files to or from any directories on their local system or only specified directories.

Command Shell

Enables the user to issue commands on the remote computer through a virtual command line interface. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

System Info

Enables the user to see system information about the remote computer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to use system information actions

Enables the user to interact with processes and programs on the remote system without requiring screen sharing. Kill processes; start, stop, pause, resume, and restart services; and uninstall programs.

Registry Access

Enables the user to interact with the registry on a remote Windows system without requiring screen sharing. View, add, delete and edit keys, search and import/export keys.

Canned Scripts

Enables the user to run canned scripts that have been created for their teams. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Elevation

Enables the user to attempt to elevate the endpoint client to run with administrative rights on the remote system. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Save Policy

Click **Save Policy** to make this policy available.

Export Policy

You can export a session policy from one site and import those permissions into a policy on another site. Edit the policy you wish to export and scroll to the bottom of the page. Click **Export Policy** and save the file.

Import Policy

You may import those policy settings to any other Bomgar site that supports session policy import. Create a new session policy and scroll to the bottom of the page. Browse to the policy file and then click **Import Policy**. Once the policy file is uploaded, the page will refresh, allowing you to make modifications. Click **Save Policy** to make the policy available.

Session Policy Simulator

Because layering policies can be complex, you can use the **Session Policy Simulator** to determine what the outcome will be. Additionally, you could use the simulator to troubleshoot why a permission is not available when you expected it to be.

User

Start by selecting the user performing the session. This dropdown includes both user accounts and access invite policies.

Session Start Method

Select the session start method. This can be one of **Jump Client**, **Remote Jump**, or **Local Jump**.

Jump Client / Jump Item

Search for a Jump Item by name, comments, Jump Group, or tag.

Simulate

Click **Simulate**. In the area below, the permissions configurable by session policy are displayed in read-only mode. You can see which permissions are allowed or denied as a result of the stacked policies, as well as which policy set each permission.

Group Policies: Apply User Permissions to Groups of Users

Group Policies

The **Group Policies** page enables you to set up groups of users who will share common privileges.

Create New Policy, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Copy

To expedite the creation of similar policies, click **Copy** to create a new policy with identical settings. You can then edit this new policy to meet your specific requirements.

Change Order

Click this button to drag and drop group policies to set their priority. Click **Save Order** for prioritization changes to take effect. For management purposes, the recommended order of priority is to define policies for more specific user groups as a higher priority (preventing override) and to move your way down from there, setting broader groups as lower priority.

Group Policy :: Add or Edit

Basic Settings

Email Login Code

Enables multifactor authentication. Users receive an email with a unique authentication code each time they log in to the /login administrative interface, or the access console, both desktop and mobile. If the code is entered incorrectly three consecutive times, users will have to re-enter their credentials and enter a new email code.

Policy Name

Create a unique name to help identify this object.

Policy Members

To assign members, click the **Add** button to open a select box. Select users from your local system, or select users or entire groups from configured security providers. To add users or groups from an external directory store such as LDAP, RADIUS, or Kerberos, you must first configure the connection on the **/login > Users & Security > Security Providers** page. If an attempt to add a user from a configured security provider is invalid, the synchronization log error message will appear here as well as in the log.

Account Settings

Defined in this policy

For each setting, select whether it should be defined in this policy or left available for configuration for individual users. If it is defined, you will be unable to modify that privilege for an individual user from their user account page.

If you have a policy that defines a permission and you do not want any policy to be able to replace that permission, then you must select that the permission cannot be overridden, and the policy must be a higher priority than other policies that additionally define that setting.

Account Expires On

Causes the account to expire after a given date or never to expire.

Account Disabled

Disables the account so the user cannot log in. Disabling does NOT delete the account.

Comments

Add comments to help identify the purpose of this object.

Permissions

Administrator

Grants the user full administrative rights.

Allowed to Set Passwords

Enables the user to set passwords and unlock accounts for non-administrative local users.

Allowed to Edit Jumpoints

Enables the user to create or edit Jumpoints. This option does not affect the user's ability to access remote computers via Jumpoint, which is configured per Jumpoint or group policy.

Access Session Reporting Permissions: Allowed to View Access Session Reports

Enables the user to run reports on access session activity, viewing only sessions for which they were the primary session owner, only sessions in which one of their teams was the primary team or one of their teammates was the primary session owner, or all sessions.

Allowed to view access session recordings

Enables the user to view video recordings of screen sharing sessions and command shell sessions.

Allowed to Use Reporting API

Enables the user's credentials to be used to pull XML reports via the API.

Allowed to Use Command API

Enables the user's credentials to be used to issue commands via the API.

Allowed to Edit Teams

Enables the user to create or edit teams.

Allowed to Edit Canned Scripts

Enables the user to create or edit canned scripts for use in screen sharing or command shell sessions.

Allowed to Edit Custom Links

Enables the user to create or edit custom links.

Access Permissions

Access

Allowed to access endpoints

Enables the user to use the access console in order to run sessions. If endpoint access is enabled, options pertaining to endpoint access will also be available.

Session Management

Allowed to share sessions with teams which they do not belong to

Enables the user to invite a less limited set of user to share sessions, not only their team members. Combined with the extended availability permission, this permission expands session sharing capabilities.

Allowed to invite external users

Enables the user to invite a third-party user to participate in a session one time only.

Allowed to enable extended availability mode

Enables the user to receive email invitations from other users requesting to share a session even when they are not logged into the access console.

Allowed to edit the external key

Enables the user to modify the external key from the session info pane of a session within the access console.

User to User Screen Sharing

Allowed to show screen to other users

Enables the user to share their screen with another user without the receiving user having to join a session. This option is available even if the user is not in a session.

Allowed to give control when showing screen to other users

Enables the user sharing their screen to give keyboard and mouse control to the user viewing their screen.

Jump Technology

Allowed Jump Methods: Allowed to start sessions through Jump Clients which use any of the following Jump methods

Enables the user to Jump to computers using **Jump Clients**, **Local Jump on the local network**, **Remote Jump via a Jumpoint**, **RDP via a Jumpoint**, and/or **Shell Jump via a Jumpoint**.

Jump Item Permissions: Allowed to start sessions from all Jump Items within the system

Enables the user to Jump to remote computers in all team Jump Groups.

Allowed to deploy, remove and modify Jump Items in the following Jump Groups

Enables the user to pin sessions, set groups, and add comments to Jump Items only for their personal Jump Group; for team and team members' Jump Groups; or for all Jump Groups, including those deployed to teams to which the user does not belong as well as to any user's personal Jump Group.

Allowed to change the Session Policies associated with Jump Items

Enables the user to set the session policy a Jump Item should use. Changing the session policy may affect the permissions allowed in the session.

Session Permissions

Set the prompting and permission rules that should apply to this user's sessions. Choose an existing session policy or define custom permissions for this user. If **Not Defined**, the global default policy will be used. These permissions may be overridden by a higher policy.

Description

View the description of a pre-defined session permission policy.

Screen Sharing

Screen Sharing

Enable the user to view or control the remote screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Application Sharing Restrictions

Limit access to specified applications on the remote system with either **Allow only the listed executables** or **Deny only the listed executables**. You may also choose to allow or deny desktop access.

> ***Note:*** *This feature applies only to Windows and Linux operating systems and does not include Remote Desktop Protocol (RDP) sessions.*

Add New Executables

If application sharing restrictions are enforced, an **Add New Executables** button appears. Clicking this button opens a dialog that allows you to specify executables to deny or allow, as appropriate to your objectives.

After you have added executables, one or two tables display the file names or hashes you have selected for restriction. An editable comment field allows administrative notes.

Enter file names or SHA-256 hashes, one per line

When restricting executables, manually enter the executable file names or hashes you wish to allow or deny. Click on **Add Executable(s)** when you are finished to add the chosen files to your configuration.

You may enter up to 25 files per dialog. If you need to add more, click **Add Executable(s)** and then reopen the dialog.

Browse for one or more files

When restricting executables, select this option to browse your system and choose executable files to automatically derive their names or hashes. If you select files from your local platform and system in this manner, use caution to ensure that the files are indeed executable files. No browser level verification is performed.

Choose either **Use file name** or **Use file hash** to have the browser derive the executable file names or hashes automatically. Click **Add Executable(s)** when you are finished to add the chosen files to your configuration.

You may enter up to 25 files per dialog. If you need to add more, click **Add Executable(s)** and then reopen the dialog.

> ***Note:*** *This option is available only in modern browsers, not in legacy browsers.*

Allowed Endpoint Restrictions

Set if the user can suspend the remote system's mouse and keyboard input. The user may also prevent the remote desktop from being displayed.

Allowed to login using credentials from an Endpoint Credential Manager

Enable connection of a user to your Endpoint Credential Manager to use credentials from your existing password stores or vaults.

Use of the Endpoint Credential Manager requires a separate services agreement with Bomgar. Once a services agreement is in place, you may download the required middleware from the Bomgar self-service center.

> ***Note:*** *Prior to 15.2, this feature is available only in sessions started from an elevated Jump Client on Windows®. Starting with 15.2, you also may use an Endpoint Credential Manager in remote Jump sessions, Microsoft® Remote Desktop Protocol sessions, and Shell Jump sessions. You may also use this feature with the Run As special action in a screen sharing session on a Windows® system.*

Annotations

Enables the user to use annotation tools to draw on the remote system's screen. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

File Transfer

File Transfer

Enables the user to upload files to the remote system, download files from the remote system, or both. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Accessible paths on the endpoint's filesystem

Allow the user to transfer files to or from any directories on the remote system or only specified directories.

Accessible paths on user's filesystem

Allow the user to transfer files to or from any directories on their local system or only specified directories.

Command Shell

Command Shell

Enables the user to issue commands on the remote computer through a virtual command line interface. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

System Information

System Info

Enables the user to see system information about the remote computer. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Allowed to use system information actions

Enables the user to interact with processes and programs on the remote system without requiring screen sharing. Kill processes; start, stop, pause, resume, and restart services; and uninstall programs.

Registry Access

Registry Access

Enables the user to interact with the registry on a remote Windows system without requiring screen sharing. View, add, delete and edit keys, search and import/export keys.

Other Tools

Canned Scripts

Enables the user to run canned scripts that have been created for their teams. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Elevation

Enables the user to attempt to elevate the endpoint client to run with administrative rights on the remote system. If **Not Defined**, this option will be set by the next lower priority policy. This setting may be overridden by a higher priority policy.

Login Schedule

Restrict user login to the following schedule

Set a schedule to define when users can log into the access console. Set the time zone you want to use for this schedule, and then add one or more schedule entries. For each entry, set the start day and time and the end day and time.

If, for instance, the time is set to start at 8 am and end at 5 pm, a user can log in at any time during this window but may continue to work past the set end time. They will not, however, be allowed to log back in after 5 pm.

Force logout when the schedule does not permit login

If stricter access control is required, check this option. This forces the user to log out at the scheduled end time. In this case, the user receives recurring notifications beginning 15 minutes prior to being disconnected. When the user is logged out, any owned sessions will follow the session fallback rules.

Memberships

Teams

Designates the teams to which users in this group should be added. If a user is in another group that adds users to a team but you do not want users in this group to be on that team, set this policy to remove users from that team. Users added manually to a team cannot be removed via group policy.

Jumpoints

Designates Jumpoints to which users in this group have access.

For group policies only, if a user is in another group that gives access to a Jumpoint but you do not want users in this group to have access to that Jumpoint, set this policy to remove users from that Jumpoint. Users added manually to a Jumpoint cannot be removed via group policy.

Save Policy

Click **Save Policy** to put the policy into effect.

Export Policy

You can export a group policy from one site and import those permissions into a policy on another site. Edit the policy you wish to export and scroll to the bottom of the page. Click **Export Policy** and save the file.

Note: *When exporting a group policy, only the policy name, account settings, and permissions are exported. Policy members, team memberships, and Jumpoint memberships are not included in the export.*

Import Policy

You may import exported group policy settings to any other Bomgar site that supports group policy import. Create a new group policy or edit an exiting policy whose permissions you wish to overwrite, and scroll to the bottom of the page. Browse to the policy file and then click **Import Policy**. Once the policy file is uploaded, the page will refresh, allowing you to make modifications; click **Save Policy** to put the group policy into effect.

Note: *Importing a policy file to an existing group policy will overwrite any previously defined permissions, with the exception of policy members, team memberships, and Jumpoint memberships.*

Kerberos Keytab: Manage the Kerberos Keytab

Kerberos Keytab Management

Bomgar supports single sign-on functionality using the Kerberos authentication protocol. This enables users to authenticate to the Bomgar Appliance without having to enter their credentials. Kerberos authentication applies both to the /login web interface and to the access console.

To integrate Kerberos with your Bomgar Appliance, you must have a Kerberos implementation either currently deployed or in the process of being deployed. Specific requirements are as follows:

- You must have a working Key Distribution Center (KDC) in place.
- Clocks must be synchronized across all clients, the KDC, and the Bomgar Appliance. Using a Network Time Protocol server (NTP) is an easy way to ensure this.
- You must have a Service Principal Name (SPN) created on the KDC for your Bomgar Appliance.

Configured Principles

The **Configured Principals** section lists all of the available SPNs for each uploaded keytab.

Once you have available SPNs, you can configure a Kerberos security provider from the **Security Providers** page and define which user principals may authenticate to the Bomgar Appliance via Kerberos.

Import Keytab

Upload

Export the keytab for the SPN from your KDC and upload it to the Bomgar Appliance via the **Import Keytab** section of this page.

Reports: Report on Session Activity

Reports :: Access

Administrators and privileged users can generate broad, comprehensive reports and also apply specific filtering to customize reported information based on clear-cut needs.

Report Type

Generate activity reports according to three separate report types: **Session**, **Summary**, and **Session Forensics** (if enabled).

Filters

Apply filtering options as needed to derive more customized reports from the basic report types. Enable one or more filters as you wish, but only sessions that match all filters selected will be shown.

Session ID or Sequence Number

This unique identifier requires that you specify the ID (LSID) or sequence number for the single session you seek. This is often helpful if you have an external ticketing system or CRM integration. You cannot combine this filter with others.

Date Range

Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.

Endpoint

Filter sessions by computer name, public IP, or private IP.

User

Use the dropdown to choose the type of user participation you want to include. Choose sessions where a specific user participated or where any user within a team participated, including sessions that were never associated with the specified team.

External Key

Filter to report sessions that used the same specific external key.

Include only completed sessions

Filter to include only sessions that have been completed. This excludes sessions that are still running.

Access Session Report

View all sessions that match the criteria specified on the previous page. Session reports include basic session information along with links to session details, chat transcripts, and video recordings of screen sharing and command shells.

Access Session Detail

Session reports detail a record of the full chat transcript, the number of files tranferred, and specific actions that took place during

the session. Windows events that present obvious visual changes within a session are captured as events in the session details. This primarily includes changes to the foreground window, with the executable name and its window title.

Other session information includes the session duration, local and remote IP addresses, and remote system information (if enabled). Reports can be viewed online or downloaded to your local system.

If session recording is enabled, view a video playback of individual sessions, including captions of who was in control of the mouse and keyboard at any given point during the session. If command prompt recording is enabled, you can also view recordings and/or text transcripts of all command shells run during the session. All recordings are stored on the Bomgar Appliance in raw format and are converted to compressed format when viewed or downloaded.

Access Summary Report

Summary reports provide an overview of activity over time, categorized by user. Statistics include the total number of sessions run, the average number of sessions per weekday, and the average duration of sessions.

Reports :: Team Activity

Range Start, Duration, Range End

Select a start date for which to pull reporting data. Then select either the number of days for which to pull your report or an end date.

Limit To

Choose the team for which you want to view activity logs.

Team Activity Report

View all team activity that matches the criteria specified on the previous page. Team activity reports include information about users as they log in or out of the access console, chat messages sent between team members, user-to-user screen sharing actions as logged in chat, and files shared and downloaded.

Management

Software Management: Download a Backup, Upgrade Software

Software :: Backup Settings

It is an important disaster recovery best practice to save a backup copy of your software settings regularly. Bomgar recommends backing up your Bomgar Appliance configuration each time you change its settings. In the event of a hardware failure, a backup file will speed time-to-recovery and, if necessary, allow Bomgar to provide you access to temporary hosted services while retaining the settings from your most recent backup.

Backup Password

To password protect your software backup file, create a password. If you do choose to set a password, you will be unable to revert to the backup without providing the password.

Include logged history

If this option is checked, your backup file will include session logs. If unchecked, session reporting data will be excluded from the backup.

Download Backup

Save a secure copy of your software configuration. Save this file in a secure location.

Software :: Restore Settings

Backup File

Should you need to revert to a backup, browse to the latest backup file that you saved.

Backup Password

If you created a password for your backup file, enter it here.

Upload Backup

Upload the backup file to your Bomgar Appliance and restore your site's settings to those saved on the backup.

Software :: Upload Update

Use **Upload Software Update** to manually upload new software packages from Bomgar. You will be asked to confirm that you wish to upload the software package. The **Uploaded Update** section displays additional information to verify your uploaded package. Click **Install** if you wish to complete the installation process, or **Delete Update** if you wish to clear the update staging area. If your update package only contains additional licenses, you can install the update without restarting the appliance. After confirmation that you wish to install, the page will display a progress bar to notify you of the overall installation progress. Updates made here will automatically update all sites and licenses on your Bomgar Appliance.

Note: *Your Bomgar Appliance administrative can also use the* ***Check for Updates*** *feature of the appliance interface to automatically search for and install new software packages.*

Security: Manage Security Settings

Security :: Options

Minimum Password Length

Set rules for local user accounts regarding the length of passwords.

Require Complex Passwords

Set rules for local user accounts regarding the complexity of passwords.

Default Password Expiration

Set rules for local user accounts regarding how often passwords expire.

Enable Password Reset

Set rules for local user accounts regarding if a forgotten password can be reset after correctly answering a security question.

Enable Saved Logins

Allow or disallow the access console to remember a user's credentials.

Account Lockout After

Set the number of times an incorrect password can be entered before the account is locked out.

Terminate Session If Account Is In Use

If a user tries to log into the access console with an account already in use, a checked **Terminate Session** box will disconnect the previous connection in order to allow the new login.

Log Out Idle User After

Set the length of time after which an inactive user will be logged out of the access console.

Remove User from Session After Inactivity

The option **Remove User from Session After Inactivity** effectively pushes a user out of a session after the period of inactivity you select. This helps Bomgar customers meet compliance initiatives with inactivity requirements. The user will be notified 1 minute prior to removal and may reset the timeout.

A user is considered active in a session if any files are being transferred, whether through the file transfer tab or the chat interface, or if they click the mouse or presses a key in the session tab. Mouse movement by itself does not count as activity. As soon as activity stops, the inactivity timer begins.

Allow Mobile Bomgar Access Consoles to Connect

Allow Mobile Bomgar Access Consoles to Connect gives users the option of accessing remote systems through the Bomgar access console app for iOS and Android.

Enable Privileged Web

Enable Privileged Web gives users the option of accessing remote systems through the Privileged Web console, a web browser-based access console.

Clipboard Synchronization Mode

Clipboard Synchronization Mode determines how users are allowed to synchronize clipboards within a screen sharing session. The available settings are as follows:

- **Not Allowed** – The user cannot access or modify the remote computer's clipboard.
- **Allowed to Manually Send Clipboard from User to Endpoint** – The user can click a button to copy the contents of the local clipboard to the remote computer's clipboard.
- **Allowed to Manually Send Clipboard in Either Direction** – The user can click a button to copy the contents of the local clipboard to the remote computer's clipboard or can copy the contents of the remote clipboard to their local clipboard.
- **Automatically Send Clipboard Changes in Both Directions** – The contents of both the local and remote clipboards automatically remain the same.

You MUST restart the software on the status page for this setting to take effect.

SSL Certificate Validation

You can require **SSL Certificate Validation** to force Bomgar software – including access consoles, endpoint clients, and Jump Clients – to verify that the certificate chain is trusted, that the certificate has not expired, and that the certificate name matches the Bomgar Appliance hostname. If the certificate chain cannot be properly validated, the connection will not be allowed.

If certificate verification has been disabled and is then enabled, all consoles and clients will automatically upgrade the next time they connect. Note that LDAP connection agents are not automatically upgraded but must be reinstalled for this setting to take effect.

When **SSL Certificate Validation** is enabled, security checks in addition to Bomgar's built-in security are performed to validate the SSL certificate chain being used to secure communications. It is highly recommended that you do enable SSL validation. If certificate validation is disabled, a warning message will appear on your administrative interface. You can hide this message for thirty days.

> ***Note:*** *To enable SSL certificate validation, you must provide your SSL certificate to Bomgar so that the certificate can be embedded within your Bomgar software.*

Allow Endpoint Credential Manager Connections

Enable connection of a user to your Endpoint Credential Manager to use credentials from your existing password stores or vaults.

Use of the Endpoint Credential Manager requires a separate services agreement with Bomgar. Once a services agreement is in place, you may download the required middleware from the Bomgar self-service center.

> ***Note:*** *Prior to 15.2, this feature is available only in sessions started from an elevated Jump Client on Windows®. Starting with 15.2, you also may use an Endpoint Credential Manager in remote Jump sessions, Microsoft® Remote Desktop Protocol sessions, and Shell Jump sessions. You may also use this feature with the Run As special action in a screen sharing session on a Windows® system.*

Days to Keep Logging Information

In **Days to Keep Logging Information**, you can set how long logging information should be stored on the appliance. This information includes the session reporting data and recordings.

Inter-appliance Communication Pre-shared Key

Enter a password in the **Inter-appliance Communication Pre-shared Key** field to establish a trusted relationship between two appliances. Matching keys are required for two or more appliances to be configured for features such as failover or clustering. The key must contain at least 6 characters and contain at least one uppercase letter, one lowercase letter, one number, and one special character.

Security :: Network Restrictions

Determine which IP networks should be able to access /login and /api on your Bomgar Appliance. If you enable network restrictions, you can also enforce the networks on which access consoles may be used.

Allow From Any Network

No network restrictions are enforced.

Allow Only the Following Networks

Only the listed IP addresses can access your Bomgar Appliance on /login or /api.

Deny Only the Following Networks

All but the listed IP addresses can access your Bomgar Appliance on /login or /api.

Restrict Bomgar Access Console access to the above networks

If you select **Only on user's first authentication**, then a user must be on an allowed network the first time they log into the access console. At that time, a token is issued to the device so that subsequent logins to the access console can occur from any network location.

If you select **Always**, then a user must be on an allowed network every time they log into the access console.

If you select **Never**, then a user can access the access console from any network location.

Security :: Port Restrictions for Administrative Web Interface

Set the ports through which your /login interface can be accessed.

Site Configuration: Set HTTP Ports, Enable Prerequisite Login Agreement

Site :: HTTP

HTTP Port and HTTPS Port

Experienced network technicians operating in non-standard network environments can change the ports through which Bomgar traffics. These port settings should be adjusted only in the case where ports other than the standard 80 and 443 are used for web access.

Site :: /login Prerequisite Login Agreement

Enable Login Agreement

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

Agreement Title

Customize the title of the agreement.

Agreement Text

Provide the text for the login agreement.

Email Configuration: Configure the Software to Send Emails

Configuration :: Email Address

Note: *If an appliance is designated as a backup appliance or a traffic node, the email configuration for that appliance will be overwritten with the email configuration defined on the primary master appliance.*

From Address

Set the email address from which automatic messages from your Bomgar Appliance will be sent.

Configuration :: SMTP Relay Server

Configure your Bomgar Appliance to work with your SMTP relay server in order to send automatic email notifications of certain events.

SMTP Relay Server

Enter the hostname or IP address of your SMTP relay server.

SMTP Port

Set the SMTP port to contact this server on.

SMTP Encryption

If your SMTP server supports SSL encryption, choose **SSL** or **TLS**. Otherwise, select **None**.

SMTP Username

If your SMTP server requires authentication, enter a username.

SMTP Password

If your SMTP server requires authentication, enter a password.

Configuration :: Admin Contact

Default Admin Contact Email Addresses

Enter one or more email addresses to which emails should be sent. Separate addresses with a space.

Send a test email when the settings are saved

If you wish to receive an immediate test email to verify that your SMTP settings are accurately configured, check this option before clicking the **Save Changes** button.

Send Daily Communication Notice

You can have the Bomgar Appliance send a daily notification to ensure that alert communication is working correctly.

In addition to the test email and daily communication notices that can be configured above, emails are sent for the following events:

- During any failover operation, the product version on the primary node does not match the product version on the backup node.
- During a failover status check, any of the following problems are detected.
    - The current appliance is the primary node and a shared IP address is configured in /login, but its network interface is not enabled.
    - A shared IP address is configured in /login but is not listed as an IP address in /appliance.
    - The backup node could not contact the primary node, and it also could not contact any of the test IP addresses configured on the **Management > Failover** page.
    - The backup node could not contact any of the test IP addresses configured on the **Management > Failover** page.
    - The backup node's backup operations are disabled on the **Management > Failover** page.
    - The backup node unexpectedly failed to perform a probe of itself, indicating that it is malfunctioning.
    - The backup node failed to contact the primary node using the primary node's hostname.
    - Automatic failover is disabled, and the backup node failed to probe the primary node.
    - Automatic failover is enabled, and the backup node failed to probe the primary node. The backup node will automatically become the primary node if the primary node remains unresponsive.
    - Automatic failover is enabled, and the backup node is automatically becoming the primary node because the primary node was down for too long.
    - The primary node failed to perform a data sync with the backup node sometime in the past 24 hours.

Outbound Events: Set Events to Trigger Messages

Outbound Events :: HTTP Recipients

You can configure your Bomgar Appliance to send messages to an HTTP server or to an email address when different events are triggered.

The variables sent by the Bomgar Appliance arrive as an HTTP POST method and can be accessed by calling the method used to retrieve POST data in your coding language. If the server does not respond with an HTTP 200 to indicate success, the Bomgar Appliance will re-queue the current event and retry it later.

Add New HTTP Recipient, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Outbound Events :: Add or Edit HTTP Recipient

Name

Create a unique name to help identify this object.

URL

Enter the destination URL for this outbound event handler.

Disabled

Use the **Disabled** checkbox to quickly stop the messages for the event handler you set up, as in the event of planned integration testing, for instance.

CA Certificate

When operating over an HTTPS connection, you must upload the certificate authority's root certificate advertised by the outbound event server.

Events to Send

Choose which events should trigger messages to be sent.

Retry Interval

Set how often to retry a failed attempt.

Retry Duration

If an event continues to retry and fail, set how long it should continue to retry before being dropped.

Email Contact

Enter one or more email addresses to which notification should be sent if an error should occur.

Send Email Alert After

Set how long after an error the email should be sent; if the problem is resolved before this time is reached and the event succeeds, no error notification will be sent.

Resend Email Alerts

Set how often error emails should be sent if a failed status should continue.

Outbound Events :: Email Recipients

Add New Email Recipient, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

Current Status

Displays a brief status message from the SMTP relay server. As long as the appliance is able to send messages to the relay server, the status will show **OK**. Otherwise, review your SMTP relay server settings.

Retry Duration

If an event continues to retry and fail, set how long it should continue to retry before being dropped.

Outbound Events :: Add Email Recipient

Before you set up your Bomgar Appliance to send event messages to an email address, verify that your Bomgar Appliance is configured to work with your SMTP relay server. Go to the **Management > Email Configuration** page to verify settings.

Name

Create a unique name to help identify this object.

Email Address

Enter the email address to receive notice of the selected events. You can configure up to ten email addresses, separated by commas.

Disabled

Use the **Disabled** checkbox to quickly stop the messages for the event handler you set up, as in the event of planned integration testing, for instance.

Require External Key

If this option is checked, emails will be sent only for sessions which have an external key at the time the event occurs.

Events to Send

Choose which events should trigger messages to be sent.

Subject

Customize the subject of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Body

Customize the body of this email. Use any of the macros listed below this field in the /login page to customize the text for your purposes.

Failover: Set Up a Backup Appliance for Failover

Failover :: Configuration

New Backup Site Connection Details: Host Name or IP Address

Enter the hostname or IP address of the Bomgar Appliance you wish to use as the backup in a failover relationship.

TLS Port

Enter the TLS port allowing this primary appliance to connect to the backup appliance.

Reverse Connection Details To This Primary Site: Host Name or IP Address

Enter the hostname or IP address of this Bomgar Appliance, which you wish to use as the primary in a failover relationship.

TLS Port

Enter the TLS port allowing the backup appliance to connect to this primary appliance.

Failover :: Status

This host's status

View the hostname of this site, along with its status of primary site instance or backup site instance.

Peer host's status

View the hostname of this site, along with its status of primary site instance or backup site instance. Also view the date and time of the last status check.

Status History

Expand or collapse a table of status events that have occurred.

Failover :: Primary or Backup Site Instance Status

Text confirms that you are either on the primary or backup site instance for your host site.

Sync Now

Manually force a data sync from the primary appliance to the backup appliance.

Become Backup/Primary

Switch roles with the peer appliance, essentially forcing a failover for planned maintenance or a known failover event.

Check this box to pull a data-sync from the site instance at example.com while becoming the backup/primary.

If you want to synchronize data from the peer appliance prior to swapping roles, select this checkbox. If this option is selected, all users on the existing primary appliance will be disconnected during the data sync, and no other operations will be available until the swap is complete.

Check this box to become a backup even if the peer site instance at example.com cannot be contacted.

On the primary site instance, you have the option to become the backup even if the peer appliance cannot be contacted. If this option is unchecked, failover will be canceled if both appliances cannot be kept in sync in terms of their failover roles (one primary and one backup).

For example, if you know the current backup appliance is online but cannot be reached by the primary due to a network connection issue, you may wish to check this option to make the primary the backup before the network connection is restored. In this example, you would also need to access the current backup and make it the primary.

Break Failover Relationships

Break the failover relationship, removing each appliance from its role as primary or backup.

Failover :: Primary or Backup Site Instance Configuration

Shared IPs

Control the shared IP address the site instance uses in the event of a failover by selecting the checkbox for the failover IP address. If you change the relationship between the sites, the checked IP addresses will disable when a primary site becomes a backup, and will enable when a backup becomes a primary site. You should manually mirror the setting on the peer site, as the setting is not shared.

Failover :: Backup Settings

The settings you configure here will be enabled only when the site instance you are configuring is in a backup role.

When on the primary site instance, select **Backup Settings >** to expand or collapse the page displaying the configuration fields.

Enable Backup Operations

Enable or disable site backups.

Automatic Data-Sync Interval

You can control the timing details of the automatic data-sync interval.

Data-Sync Bandwidth Limit

Set bandwidth parameters for data-sync.

Enable Automatic Failover

Quickly enable or disable automatic failover.

Primary Site Instance Timeout

Set how long the primary site must be unreachable before failing over.

Network Connectivity Test IPs

Enter IP addresses for the backup site to check to determine whether the backup's inability to reach the primary is because the primary is offline or the backup has lost its network connection.

API Configuration: Enable the XML API and Configure Custom Fields

API :: Configuration

Enable XML API

Choose to enable the Bomgar XML API, allowing you to run reports and issue commands such as starting or transferring sessions from external applications, as well as to automatically back up your software configuration.

***Note**: Only the **Command**, **Reporting**, and **Client Scripting API** calls are enabled/disabled by this setting. Other API calls are configured under Public Portals. See the API Programmer's Guide for more details.*

Allow HTTP Access to XML API

By default, access to the API is SSL-encrypted. However, you can choose to allow unencrypted HTTP access. It is highly recommended that HTTP access be disallowed as a security best practice.

API :: Custom Fields

Create custom API fields to gather information about your customer, enabling you to more deeply integrate Bomgar with your existing programs. Custom fields must be used in combination with the Bomgar API. See the API Programmer's Guide for more details.

Create New Field, Edit, Delete

Create a new object, modify an existing object, or remove an existing object.

API :: Custom Fields :: Add or Edit

Display Name

Create a unique name to help identify this object. This name is displayed in the access console as part of the session details.

Code Name

Set a code name for integration purposes. If you do not set a code name, one will be created automatically.

Show in Access Console

If you check **Show in Access Console**, this field and its values will be visible wherever custom session details are displayed in the access console.

Support: Contact Bomgar Technical Support

Bomgar Support Contact Information

The support page provides contact information should you need to contact a Bomgar Technical Support representative.

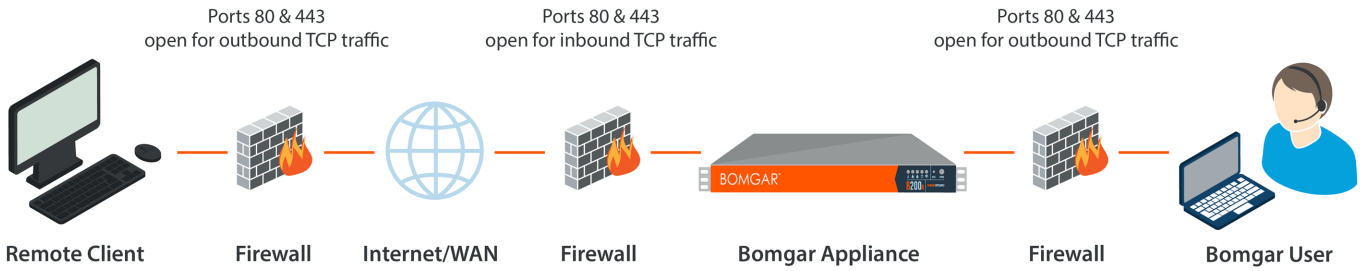
Advanced Technical Support from Bomgar

In the event that a Bomgar Technical Support representative should need access to your appliance, they will provide you with support, access, and override codes to enter on this page to create an appliance-initiated, fully encrypted support tunnel back to Bomgar for quick resolution of complex issues.

Ports and Firewalls

Bomgar solutions are designed to work transparently through firewalls, enabling a connection with any computer with internet connectivity, anywhere in the world. However, with certain highly secured networks, some configuration may be necessary.

TYPICAL NETWORK SETUP: 15.1



- Ports 80 and 443 must be open for outbound TCP traffic on the remote system's and local user's firewalls. More ports may be available depending on your build. The diagram shows a typical network setup; more details can be found in the Bomgar Appliance Hardware Installation Guide.
- Internet security software such as software firewalls must not block Bomgar executable files from downloading. Some examples of software firewalls include McAfee Security, Norton Security, and Zone Alarm. If you do have a software firewall, you may experience some connection issues. To avoid such issues, configure your firewall settings to allow the following executables, wherein {uid} is a unique identifier consisting of letter and numbers:
  - bomgar-scc-{uid}.exe
  - bomgar-scc.exe
  - bomgar-pac-{uid}.exe
  - bomgar-pac.exe
  - bomgar-pec-{uid}.exe
  - bomgar-pec.exe

  For assistance with your firewall configuration, please contact the manufacturer of your firewall software.
- Example firewall rules based on appliance location can be found at www.bomgar.com/docs/privileged-access/getting-started/deployment/dmz/firewall-rules.htm.

If you should still have difficulty making a connection, contact Bomgar Technical Support at help.bomgar.com.

Disclaimers, Licensing Restrictions and Tech Support

Disclaimers

This document is provided for information purposes only. Bomgar Corporation may change the contents hereof without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. Bomgar Corporation specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionality, services, and processes described herein are subject to change without notice.

BOMGAR, BOMGAR BOX, mark B, JUMP and UNIFIED REMOTE SUPPORT are trademarks of Bomgar Corporation; other trademarks shown are the property of their respective owners.

Licensing Restrictions

One Bomgar Privileged Access Management license enables one support representative at a time to troubleshoot an unlimited number of remote computers, whether attended or unattended. Although multiple accounts may exist on the same license, two or more licenses (one per concurrent support representative) are required to enable multiple support representatives to troubleshoot simultaneously.

One Bomgar Privileged Access Management license enables access to one endpoint system. Although this license may be transferred from one system to another if access is no longer required to the first system, two or more licenses (one per endpoint) are required to enable access to multiple endpoints simultaneously.

Tech Support

At Bomgar, we are committed to offering the highest quality service by ensuring that our customers have everything they need to operate with maximum productivity. Should you need any assistance, please contact Bomgar Technical Support at help.bomgar.com.

Technical support is provided with annual purchase of our maintenance plan.