LogMeIn Central
User Guide
## Contents

Welcome to LogMeIn Central

Your LogMeIn Account

Installing and Deploying LogMeIn Host Software

Organizing, Finding and Working with Host Computers

Using the Management Cloud: LogMeIn Central Core Features

---

### Welcome to LogMeIn Central

### Your LogMeIn Account

- How to Sign up for a LogMeIn ID
- Managing Your LogMeIn Account
  - How to Change Your LogMeIn ID (account email)
  - How to Change Your LogMeIn Account Password
  - How to View or Change Billing Information
  - How to View Subscription Information
- How to Create Alert Rules in an Alert Package
  - LogMeIn Central Alert Rule Types
- About the Impact of Group Changes (Moved Computers) on User Access
- Creating a Computer Group
- How to Delete a Computer from Your Account
- How to Move a Computer to Another Account
- How to Find a Computer on a Phone or Tablet
- How to Find a Computer on a PC or Mac
- View a List of Available Computers via Phone or Tablet
- How to Find a Computer on a PC or Mac
- How to Rename a Computer
- How to Move a Computer to Another Account
- How to Delete a Computer from Your Account
- Using the Favorites List
- Managing Groups of Computers
  - Creating a Computer Group
  - About the Impact of Group Changes (Moved Computers) on User Access

### Installing and Deploying LogMeIn Host Software

- Installing LogMeIn on a PC or Mac
- Installing LogMeIn Host Software (Add a computer)
- How to Add a Computer via Phone or Tablet
- System Requirements – Host Computer
- LogMeIn and Firewalls
- How to Configure Proxy Settings
- Deploying LogMeIn Host Software
  - How to Deploy LogMeIn Host Software
  - How to Modify an Installation Package
  - About Deployment Methods
  - Mass Deployment of LogMeIn Host Software (Silent Install)
- How do I connect a "not accessible" computer to my account?

### Organizing, Finding and Working with Host Computers

- Working with Computers in Your LogMeIn Account
  - Using Custom Fields to Organize Computers
  - Viewing a List of Available Computers via PC or Mac
  - Viewing a List of Available Computers via Phone or Tablet
  - How to Find a Computer on a PC or Mac
  - How to Find a Computer on a Phone or Tablet
  - How to Rename a Computer
  - How to Move a Computer to Another Account
  - How to Delete a Computer from Your Account
  - Using the Favorites List
- Managing Groups of Computers
  - Creating a Computer Group
  - About the Impact of Group Changes (Moved Computers) on User Access

### Using the Management Cloud: LogMeIn Central Core Features

- Working with Alerts
- LogMeIn Central Alert Rule Types
- How to Create Alert Rules in an Alert Package
Files for LogMeIn: Storage for your files and folders .................................................................123
How to access your files on your desktop with Files for LogMeIn .................................................123
How to share files with Files for LogMeIn ..........................................................................................124
    Share a file or folder (read-only access) .......................................................................................124
    Share a folder with Users (view, modify, delete) .........................................................................124
    How to stop sharing (remove link) .............................................................................................124
How to upload and download files with Files for LogMeIn ..............................................................125
    Upload files or folders ..............................................................................................................125
    Download a file .........................................................................................................................125

Accessing and Managing Remote Computers ..................................................................................126
Connecting to a Host Computer ...........................................................................................................126
    System Requirements – Client Device .......................................................................................126
    How to Connect from LogMeIn.com .........................................................................................126
    How to Connect using the LogMeIn Client Desktop App ............................................................128
    How to Connect via Phone or Tablet ..........................................................................................130
    How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN .........................134
    How to Set Up Automatic Authentication .................................................................................138
Remote Control ..................................................................................................................................139
    System Requirements – Client Device.......................................................................................139
    Remote Control from a PC or Mac ...............................................................................................140
    Remote Control from a Phone or Tablet .....................................................................................149
File Management ...............................................................................................................................158
    File Manager from a PC or Mac ..................................................................................................158
    File Manager from a Phone or Tablet .........................................................................................162
Remote Management of LogMeIn Hosts .............................................................................................166
    Using the LogMeIn Dashboard ....................................................................................................167
    Managing the Rights of Windows Users and Groups .................................................................167
    Monitoring Events in the Application, Security, and System Logs .............................................168
    Working with Services ...............................................................................................................168
    Working with Processes .............................................................................................................169
    Working with Drivers ..................................................................................................................169
    Editing the Registry ....................................................................................................................170
    Opening the Command Prompt ...................................................................................................171
Rebooting the Host ..............................................................................................................................172
Enabling Windows Automatic Logon (autologon) ..............................................................................172
Viewing a Host Computer Desktop without Taking Control ..............................................................173
Working with Environment Variables ...............................................................................................173
Changing Virtual Memory Settings ....................................................................................................173
Changing System Time on a Host ......................................................................................................174
Managing Shared Resources .............................................................................................................174
Setting Automatic Change Process Priorities ....................................................................................175
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Host Performance Information</td>
<td>175</td>
</tr>
<tr>
<td>Viewing CPU Load</td>
<td>176</td>
</tr>
<tr>
<td>Viewing Memory Load</td>
<td>176</td>
</tr>
<tr>
<td>Viewing Disk Space Utilization</td>
<td>177</td>
</tr>
<tr>
<td>Viewing Drive and Partition Information</td>
<td>177</td>
</tr>
<tr>
<td>Viewing Open TCP/IP Ports</td>
<td>177</td>
</tr>
<tr>
<td>Viewing Network Traffic Information</td>
<td>178</td>
</tr>
<tr>
<td>Viewing a List of Open Files</td>
<td>178</td>
</tr>
<tr>
<td>Viewing a List of Registry Keys Open on a Host</td>
<td>179</td>
</tr>
<tr>
<td>Viewing a List of DLLs in Use</td>
<td>179</td>
</tr>
<tr>
<td>Viewing LogMeIn Connection Details</td>
<td>179</td>
</tr>
<tr>
<td>Viewing Installed Applications</td>
<td>179</td>
</tr>
<tr>
<td>Viewing Loaded Device Drivers</td>
<td>180</td>
</tr>
<tr>
<td>Configuring How LogMeIn Works on a PC or Mac</td>
<td>180</td>
</tr>
<tr>
<td>Controlling Remote Control Performance</td>
<td>180</td>
</tr>
<tr>
<td>Customizing Remote Control Sessions</td>
<td>182</td>
</tr>
<tr>
<td>Advanced Host Settings</td>
<td>186</td>
</tr>
<tr>
<td>Controlling Access to Host Computers</td>
<td>189</td>
</tr>
<tr>
<td>Ad Hoc Support: Accessing Unmanaged Computers</td>
<td>197</td>
</tr>
<tr>
<td>Task One: Setting Up an Ad Hoc Support Session</td>
<td>197</td>
</tr>
<tr>
<td>Task Two: Conducting an Ad Hoc Support Session</td>
<td>199</td>
</tr>
<tr>
<td>Ad Hoc Support Troubleshooting</td>
<td>200</td>
</tr>
<tr>
<td>About the LogMeIn API and API Key</td>
<td>203</td>
</tr>
<tr>
<td>Working with LogMeIn Hamachi</td>
<td>204</td>
</tr>
<tr>
<td>Audience</td>
<td>204</td>
</tr>
<tr>
<td>LogMeIn Hamachi Fundamentals</td>
<td>204</td>
</tr>
<tr>
<td>What Is LogMeIn Hamachi?</td>
<td>204</td>
</tr>
<tr>
<td>The LogMeIn Hamachi Client</td>
<td>205</td>
</tr>
<tr>
<td>LogMeIn Hamachi Network Types</td>
<td>206</td>
</tr>
<tr>
<td>LogMeIn Hamachi Subscription Types</td>
<td>208</td>
</tr>
<tr>
<td>Managing LogMeIn Hamachi Clients and Networks</td>
<td>210</td>
</tr>
<tr>
<td>LogMeIn Hamachi Security</td>
<td>211</td>
</tr>
<tr>
<td>Installing LogMeIn Hamachi</td>
<td>211</td>
</tr>
<tr>
<td>Hamachi System Requirements</td>
<td>211</td>
</tr>
<tr>
<td>How to Install the Client to a Local Computer</td>
<td>212</td>
</tr>
<tr>
<td>How to Deploy the Client to a Remote Computer</td>
<td>213</td>
</tr>
<tr>
<td>How to Install a Hamachi Client in Client-Only mode</td>
<td>214</td>
</tr>
<tr>
<td>How to Update the Hamachi Client</td>
<td>214</td>
</tr>
<tr>
<td>Managing LogMeIn Hamachi Clients</td>
<td>215</td>
</tr>
<tr>
<td>How to Set Default Settings for Deployed Clients</td>
<td>215</td>
</tr>
<tr>
<td>How to Attach an Unattached Client to a LogMeIn Account</td>
<td>215</td>
</tr>
<tr>
<td>How to Rename a Client On the Website</td>
<td>217</td>
</tr>
<tr>
<td>How to Add/Remove a Client to/from a Network</td>
<td>217</td>
</tr>
<tr>
<td>How to Add a Hamachi Mobile Client</td>
<td>217</td>
</tr>
<tr>
<td>How to Change the Client Interface</td>
<td>220</td>
</tr>
<tr>
<td>How to Detach (Delete) a Client from Your Account</td>
<td>221</td>
</tr>
<tr>
<td>Using Tags to Help Manage Clients in Your Account</td>
<td>221</td>
</tr>
<tr>
<td>Managing LogMeIn Hamachi Networks</td>
<td>222</td>
</tr>
<tr>
<td>How to Set the Default Response to Network Join/Exit Requests</td>
<td>222</td>
</tr>
<tr>
<td>How to Add a Hamachi Network</td>
<td>223</td>
</tr>
<tr>
<td>How to Add a Hamachi Network from the Client</td>
<td>225</td>
</tr>
<tr>
<td>How to Rename a Network</td>
<td>225</td>
</tr>
<tr>
<td>How to Approve or Reject Join Requests</td>
<td>226</td>
</tr>
<tr>
<td>How to Edit Network Settings</td>
<td>226</td>
</tr>
</tbody>
</table>
Welcome to LogMeIn Central

LogMeIn Central is LogMeIn’s subscription-based remote management solution. Foremost, LogMeIn Central is a powerful toolkit for accessing and managing remote computers. LogMeIn Central also lets you deploy and configure LogMeIn Hamachi networks and clients.

Resources

Sign up for a trial or purchase a subscription: [LogMeIn Central Product Page](LogMeIn Central Product Page)

FAQ and Knowledge Base [help.LogMeIn.com](help.LogMeIn.com)

💡 Tip: The [LogMeIn Community](LogMeIn Community) is an excellent source of information from other LogMeIn users.
Your LogMeIn Account

Use your LogMeIn ID to access LogMeIn products and services on every platform with a single login.

How to Sign up for a LogMeIn ID

Sign up for a LogMeIn ID to use LogMeIn software and services. No obligation. No credit card required.

Your LogMeIn ID provides a single login experience for the following LogMeIn products and services on every platform.

• LogMeIn (client and host)
• Central
• join.me

Note: You need to log in separately to LogMeIn Rescue.

2. Click Log In in the upper-right corner.
   The Log in or sign up page is displayed.
3. Click Sign up.
4. Fill in the registration form and follow all on-screen instructions.
   Upon completing the account form you will be sent a confirmation email.
5. Carefully follow all instructions in the email you receive from LogMeIn regarding account activation.
   Can't find an email from LogMeIn? Check your junk or spam folder.

Managing Your LogMeIn Account

How to Change Your LogMeIn ID (account email)

Change the email address you use when you log in to LogMeIn.

No host connection is required to manage your LogMeIn account details. The Internet and a browser is all you need.

2. Log in to your account using your LogMeIn ID (email address) and password.
   The Computers page is displayed.
3. At the top of the page, click Settings and then Account Settings.
   The Account Settings page is displayed.
4. Click Change next to your current LogMeIn ID.
   The Change LogMeIn ID page is displayed.
5. Type a new email address in the New email field, enter it again, and click Change ID.
   An email containing a confirmation link is sent to the new address.
6. Click the confirmation link that was sent to your new email address.
7. Log in with your new LogMeIn ID (email address) and password. Once logged in, your new LogMeIn ID will be committed to the LogMeIn system.

**How to Change Your LogMeIn Account Password**

Change the password you use to log in to LogMeIn.com, join.me, and cubby.com.

No host connection is required to manage your LogMeIn account details. The Internet and a browser is all you need.

**Changing your password**

2. **Log in** to your account using your LogMeIn ID (email address) and password. The **Computers** page is displayed.
3. At the top of the page, click **Settings** and then **Account Settings**. The **Account Settings** page is displayed.
4. Next to your password, click **change**. The **Change password** page is displayed.
5. Complete the **current password**, **new password**, and **Retype new password** fields. The Password Strength Meter will measure the strength of your new password.
6. Click **Save**.

You are ready to use your new password the next time you log in to LogMeIn.com, join.me, or cubby.com.

**Resetting a forgotten password**

1. Go to [www.LogMeIn.com](http://www.LogMeIn.com) and click **Log In** in the navigation bar. The **Login** window is displayed.
2. Click **Forgot your password?**.
3. Enter your LogMeIn ID (email address) and click **Submit**. An email is sent to you with further instructions.
4. Check your mailbox, and click the link in the email (or copy and paste it into your browser).
5. Enter and confirm your new password. The Password Strength Meter will measure the strength of your new password.
6. Click **Create new password**.

You are ready to use your new password the next time you log in to LogMeIn.com, join.me, or cubby.com.

**How to View or Change Billing Information**

LogMeIn account holders use the **Billing** page to view and edit contact and billing information for their LogMeIn account.

To access the **Billing** page, log in to LogMeIn and click **Settings** at the top of the page, and then select **Billing**.

**Fields are grey? Can’t make edits?** Only account holders can edit information on the **Billing** page. For example, when your active profile is called "User of Xxxx" you won’t be able to edit billing information.

**Tip:** The name in the **Company Name** field in the Contact Information section is used to define the profile name of your LogMeIn account. Other users will see this Company Name listed as part of the profile they use to access shared resources in your account.
Billing history?

Fastpath: Settings > Billing > Billing History

Only account holders can view Billing History.

Copy of your invoice?

Fastpath: Settings > Billing > Billing History > Print Receipt

Only account holders can print a receipt.

How to View Subscription Information

View information about your subscriptions to LogMeIn products and services.

2. Log in to your account using your LogMeIn ID (email address) and password. The Computers page is displayed.
3. At the top of the page, click Settings and then Subscriptions. All subscriptions to LogMeIn products and services that are associated with your LogMeIn ID are listed. The information displayed includes Product, Type, Start date, Expiration date, and Renewal Price.

Tip: Here are more ways to access a list of subscriptions in LogMeIn Central.

• Deployment > View all subscriptions
• Configuration > Subscriptions
• Reports > Report Viewer > Category (LogMeIn Licenses) > Report (Subscriptions)

Reports > Report Viewer

Securing Your Account and the Login Process

Enable settings that help prevent unauthorized access to your LogMeIn account.

LogMeIn users must be authenticated by both the LogMeIn gateway and host computers. An email address and password verification is performed whenever a user logs on to the LogMeIn website or via a LogMeIn app. Users are advised to enable one or more of LogMeIn’s extra security features to strengthen this authentication step.

Tip: Want to know more about security? Read more about securing your LogMeIn remote environment.
Account Audit Log

Use the Audit Log feature to access detailed account activity information.

1. **Log in** to your account using your LogMeIn ID (email address) and password.
   The Computers page is displayed.
2. At the top of the page, click **Settings > Account Settings**.
   The Account settings page is displayed.
3. Under **Audit log**, click **view**.
   The Audit log window is displayed.
4. Select an **event type** and **time period** to filter audit information.

   The audit log preserves events related to the following account activities and settings:
   - Login Initiated
   - Login Failed
   - Two-step verification successful
   - Two-step verification failed
   - Login successful
   - Logout
   - Password confirmation successful
   - Password confirmation failed
   - Two-step verification enabled
   - Two-step verification disabled
   - Two-step verification settings changed
   - Password reset requested
   - Password reset successful
   - Password change successful
   - Password change failed
   - Account email change requested
   - Account email change successful
   - Account email change failed
   - Email notifications settings changed
   - Email notifications recipients changed
   - Social account connected
   - Social account disconnected
   - Product updates emails enabled
   - Product updates emails disabled
   - Name changed
   - Timezone changed
   - Language changed
   - Trusted device expiry changed
   - Trusted device added
   - Trusted device revoked

Account Audit Notifications

Use the Account Audit feature to keep track of activity in your LogMeIn account.
1. Log in to your account using your LogMeIn ID (email address) and password. The Computers page is displayed.

2. At the top of the page, click Settings > Security. The Security page is displayed.

3. Under Audit Settings select events for which you want to receive automatic email notification. Some account events are turned on by default and cannot be disabled. Don’t see the Audit Settings section? Make sure that you have selected your personal profile (Account Holder of...).

- Audit your security level. Receive notification on the following events:
  - Emailed security codes are enabled
  - Emailed security codes are disabled
  - Printed security codes are enabled
  - Printed security codes are disabled
  - A new sheet of printed security codes is printed

- Audit your users (LogMeIn Central and Pro account with 10+ seats). Receive notification on the following events:
  - A user is invited
  - A user accepts the invitation
  - A user is deleted
  - An invited user’s login fails
  - An invited user logs in successfully
  - Audit computers in your account

- Audit computers in your account. Receive notification on the following events:
  - An installation package is generated
  - A computer is added
  - A computer is deleted
  - A computer shortcut is generated
  - A computer shortcut is invalidated

- Audit changes to the above settings. Receive notification on the following event:
  - Notification settings change

4. Save your changes.

Tip: To edit the recipient list and account related notifications, go to Settings > Account Settings > Email notifications. Notifications will be sent to the specified email addresses (for multiple recipients, separate email addresses with a semi-colon).

How to Set a Password Strength Requirement

A login policy can be applied to all users in a LogMeIn Central account, including the account holder. This helps administrators better secure their Central account by managing password strength and two-factor authentication policies.

Only LogMeIn Central users with Login policy management permission can edit or enforce a login policy.
The policy is valid when logging in to LogMeIn.com, LogMeIn apps for iOS and Android, and the LogMeIn Client desktop app.

1. In LogMeIn Central, click **Users > Login Policy**. The **Login Policy** page is displayed.
2. Choose a policy for **Password strength**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Standard | Use the default password strength setting:  
  - At least six characters  
  - No other requirements |
| Strong  | Force users to create a robust password meeting the following requirements:  
  - Seven characters or more  
  - Made of capital letters, lowercase letters, and numbers  
  - Changed every 90 days  
  - Does not match the user’s LogMeIn ID  
  - Does not match any of the user’s four most recent passwords |

Upon next login, the policy is applied to all users in the account.

💡 **Tip:** As a courtesy to your users, you may want to notify them when you apply policy changes. LogMeIn does not automatically notify users of policy changes.

**Two-Step Verification**

Two-step verification adds a second layer of protection to your account.

Once you set up two-step verification, your login procedure changes: After entering your LogMeIn ID and password, you are also required to verify your identity using either a mobile authenticator app or text message (or using a backup method, which can be either text message or email).

With two-step verification, you will be **able** to log in with the following components, versions, sites:

- LogMeIn.com
- LogMeIn host software for Windows, 4.1.4141 and above
- LogMeIn host software for Mac, 4.1.4132 and above
- LogMeIn for iOS app, all versions
- LogMeIn for Android app, all versions except "Ignition" branded versions
- join.me (all components), all versions

You will be **unable** to log in to the following components:

- Legacy versions of LogMeIn Ignition for Windows: Please switch to the LogMeIn Client desktop app before using two-step verification
- Legacy versions of LogMeIn Ignition for Android: Please upgrade to the LogMeIn for Android app

**Guidance from PCI DSS v3.0**

Two-step verification is a requirement in PCI DSS v3.0.
How to Setup Two-Factor Authentication for Your Own Account

Two-step verification works with LogMeIn products and components that allow login via accounts.logme.in, LogMeIn's common login service. Certain legacy products and components do not meet this requirement.

Setup involves two main tasks.

- First, set up your **primary method** for receiving login codes (this will be LastPass Authenticator)
- Second, set up either text message or email as a **backup method** in case your primary is not available.

Let's take a closer look. This procedure describes setup using our own LastPass Authenticator. The procedure is similar for other popular authenticator apps.

1. **Log in** to your account at LogMeIn.com using your LogMeIn ID (email address) and password.
2. At the top of the page, click **Settings** and then **Account Settings**.
   The **Account Settings** page is displayed.
3. Under **Security**, look for **Two-step verification** and click **get started**.
   Read the introductory information and click again to get started.
   The **Protect your account** page is displayed.
4. On the **Protect your account** page, click **Set up mobile app**.
5. If you already have LastPass Authenticator, simply click **Next**.

   **Tip:** You can download the app from this site: https://lastpass.com/auth/.

   The **Set up mobile** page is displayed. You should see a scannable QR code.
6. Launch LastPass Authenticator on your device and scan the QR code, as follows:
   a) On the LastPass Authenticator app, tap the **+ (plus)** sign.
   b) Physically hold your device in front of the LogMeIn website to scan the code.
   A message is displayed confirming that your device has been paired to your LogMeIn account. Tap to dismiss the message.
7. Returning to the LogMeIn website, you must now choose the **backup method** to use when your primary method is unavailable. Here's how:
   a) To receive login codes via text message:
      - Click **Set up text message**.
      - Enter the phone number to which login codes should be sent and click **Next**. A code is sent.
      - Go to your phone and open the text message from LogMeIn.
      - Enter the code on the **Verify phone number** page.
      - Click **Finish text setup**.
   b) To receive login codes via email:
      - Click **Set up email**.
      - Enter the email address you want to use to receive codes. To use the same address you use to log in to LogMeIn, click **Use your LogMeIn ID**.
      - Go to your email inbox and open the message from LogMeIn.
      - Enter the code on the **Set up email** page in your browser.
      - Click **Finish email setup**.
8. Finally, click **Activate** at the bottom of the page to actually turn on two-step verification.

After setup, the following is expected:
• LastPass Authenticator: Tap the on-screen notification to confirm your identity.
• Authenticator app other than LastPass Authenticator: Enter a one-time code that you get from the paired authenticator app.
• Text message: Enter the one-time code sent to the number.
• Primary method is unavailable: Request a code via your backup.

Guidance from PCI DSS v3.0
Two-step verification is a requirement in PCI DSS v3.0.

How To Force All Users to Use Two-Factor Authentication
Force all users accessing your LogMeIn account to follow a two-step process to verify their identity.

Only LogMeIn Central users with Login policy management permission can edit or enforce a login policy.

The policy is valid when logging in to LogMeIn.com, LogMeIn apps for iOS and Android, and the LogMeIn Client desktop app.

1. In LogMeIn Central, click Users > Login Policy. The Login Policy page is displayed.
2. Under Login process, select Two-factor authentication. The You are about to require two-factor authentication confirmation prompt is displayed.
3. Click Switch on. Users must follow a two-step process to verify their identity. They can choose any method currently available for LogMeIn. The policy cannot force them to use a specific method. For details, see Two-Step Verification on page 13.

Upon next login, Two-factor authentication is applied to all users in the account.

Tip: As a courtesy to your users, you may want to notify them when you apply policy changes. LogMeIn does not automatically notify users of policy changes. If users need assistance setting up two-step verification, direct them to: How to Setup Two-Factor Authentication for Your Own Account on page 14.

Tip: When using LogMeIn Central in a browser, Login Policy does not allow you to save devices. This only applies if the Master Account Holder enables Two-factor authentication under Users > Login Policy.

How to Force a User Group to Use Two-Factor Authentication
Force all members of a User Group to follow a two-step process to verify their identity when logging in to their LogMeIn account.

Only LogMeIn Central users with User management permission can edit or enforce a login policy.

1. In LogMeIn Central, click Users > Manage. The Users page is displayed.
2. Click edit permissions next to the name of the User Group you want to edit. The Edit page is displayed.
4. Click Save.
Users must follow a two-step process to verify their identity. They can choose any method currently available for LogMeIn. The policy cannot force them to use a specific method. For details, see Two-Step Verification on page 13.

Upon next login, the user must set up **Two-factor authentication**.

**Tip:** As a courtesy to your users, you may want to notify them when you apply policy changes. LogMeIn does not automatically notify users of policy changes. If users need assistance setting up two-factor verification, direct them to: How to Setup Two-Factor Authentication for Your Own Account on page 14.

**Tip:** When using LogMeIn Central in a browser, Login Policy does not allow you to save devices. This only applies if the Master Account Holder enables Two-factor authentication under Users > Login Policy.

### How To Force Individual Users to Use Two-Factor Authentication

Force an individual user to follow a two-step process to verify their identity when logging in to their LogMeIn account.

Only LogMeIn Central users with User management permission can edit or enforce a login policy.

1. In LogMeIn Central, click Users > Manage. The Users page is displayed.
2. Click the email address of the user you want to edit. The Edit page is displayed.
3. Under Extra Security, select Enforce two-factor authentication for this user.
4. Click Save.

Upon next login, the user must set up **Two-factor authentication**.

**Tip:** As a courtesy to your users, you may want to notify them when you apply policy changes. LogMeIn does not automatically notify users of policy changes. If users need assistance setting up two-factor verification, direct them to: How to Setup Two-Factor Authentication for Your Own Account on page 14.

**Tip:** When using LogMeIn Central in a browser, Login Policy does not allow you to save devices. This only applies if the Master Account Holder enables Two-factor authentication under Users > Login Policy.

### How to switch off two-step verification

You may want to switch off two-step verification if you get a new device or no longer want to take advantage of the feature.

**Remember:** You may be required by your administrator to use two-step verification.

1. Log in to your account using your LogMeIn ID (email address) and password. The Computers page is displayed.
2. At the top of the Computers page, click **Settings** and then **Account Settings**. The Account settings page is displayed.

3. Under **Security**, click **Switch off**.
   You may be prompted to confirm your identity and review your settings before actually switching off two-step verification.

4. To remove pairing for all existing devices, select **Clear all settings when I switch off**.
   **Tip:** LogMeIn will still be listed in your app, but any login codes it generates will not be accepted. To avoid confusion, we recommend removing LogMeIn from your app.

5. Click the **Switch off** button.

### Trusted Devices

Save time when logging in to your LogMeIn account by skipping password entry and/or two-factor authentication on devices you trust.

**How do I designate a device as trusted?**  
When logging in to your LogMeIn account on any given device, you can select the following options, depending on your security settings: **Don’t ask me for a password. I trust this device.** **and/or** **Don’t ask me for a code. I trust this device.**

**What is a trusted device?**  
On a device you designate as trusted, you are not required to enter a password and/or verification code to access your LogMeIn account.

**How do I remove a trusted device?**  
Go to **Account settings > Trusted devices** and click **view devices**. Review the list and remove devices as required.

**What’s the "trust period"?**  
By setting a trust period you are telling LogMeIn how long you want to trust your devices. For each trusted device you will only be asked to verify your identity when logging in outside the trust period. Each login renews trust for a given device. To set your trust period, go to **Account settings > Trust period** and click **change**.

**Tip:** In LogMeIn Central, if **Two-factor authentication** is enabled under **Users > Login Policy** by the Master Account Holder, the Login Policy does not allow you to save devices.

### Additional Security Options

Configure how you log in, receive notifications of security events and more.

**Fastpath:** To access account security options, log in to your LogMeIn account and click **Settings > Security**.

**Who can use this feature?** LogMeIn Central Account Holders and users with permission to **Enable account-level security features**.

**Tip:** Want to know more about security? Read more about **securing your LogMeIn remote environment**.

### Time-out

The amount of idle time allowed before you will be logged out of your LogMeIn Central session.
Remember Login Credentials

By enabling this feature, you can securely save your host username and password to the client computer from which you are connecting. See How to Set Up Automatic Authentication on page 138.

One-time Emailed Security Codes

When you enable Emailed Security Code for your LogMeIn account, each time you log in you are sent an email containing a security code that you must enter to access your account.

Note: This feature should not be confused with two-step verification codes that you may receive via email. See Two-Step Verification on page 13.

To activate emailed security codes for your LogMeIn account:

1. Log in to your account using your LogMeIn ID (email address) and password.
   The Computers page is displayed.
2. At the top of the page, click Settings > Security.
   The Security page is displayed.
4. Enter a single email address to which a code should be sent upon login.
   Tip: The email account should be accessible from a wireless device to ensure you receive the code promptly, wherever you are.
5. Click Save.
   A test security code is sent to the defined address.
6. Go to your email account and locate the email from LogMeIn.com Auto-Mailer with the subject Emailed test code: xxxx-xxxx.
7. Enter the code from the email in the Test code field.
   Each code can be used only once.
   The Emailed Security Code feature is now enabled.

Upon next login to your account, you will receive an email from LogMeIn.com Auto-Mailer with the subject Your LogMeIn Security Code: xxxx-xxxx. Enter this code in the Security code field on the LogMeIn site when prompted.

Tip: Emailed security codes are only valid for 30 minutes.

To disable the feature, go to the Security page, clear the Emailed Security Code option, and save your change.

Printed Security Codes

When you enable the Printed Security Code feature for your LogMeIn account, LogMeIn generates a list of one-time security codes that you must enter in order to access your account.

1. Log in to your account using your LogMeIn ID (email address) and password.
   The Computers page is displayed.
2. At the top of the page, click Settings > Security.
   The Security page is displayed.
4. Click to generate a new list of one-time security codes.
   The list of codes is displayed in a new window.
5. Print the list.
   Be sure to keep the printed list safe.

Each time you log in to your LogMeIn account you will be prompted to enter one of the security codes
from the printed list before you can access your account.

Remember: Each code can be used only once.

Tip: To disable the feature once all printed codes on the list have been used, select Stop
prompting for security codes when all security codes have been used up.
Installing and Deploying LogMeIn Host Software

Installing LogMeIn on a PC or Mac
You must install LogMeIn on each computer you want to be able to access remotely.

Use the **Deployment** page to install LogMeIn host software to one or more remote computers that you want to add to your LogMeIn account. Deployment supports mass installation as well.

See also **Installing LogMeIn Hamachi** on page 211.
See **Deploying LogMeIn Host Software** on page 23.

Installing LogMeIn Host Software (Add a computer)
Each computer you want to access must be running the LogMeIn host software. In a sense, the LogMeIn host software safely and securely "opens the door" to a computer for a qualified remote user.

Here is how to add a computer to your account:

1. Go to **www.LogMeIn.com**.
2. **Log in** to your account using your LogMeIn ID (email address) and password.
   The **Computers** page is displayed.
3. On the **Computers** page, click **Add Computer**.
4. Choose an option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add this computer</td>
<td>To add the computer you are using, click <strong>Add this computer &gt; Download installer</strong>. Follow the on-screen instructions to download and install LogMeIn.</td>
</tr>
<tr>
<td>Add different computer</td>
<td>To add a computer other than the one you are using, click <strong>Add different computer &gt; Generate link</strong>. Follow the on-screen instructions to download and install LogMeIn.</td>
</tr>
</tbody>
</table>

**Note:** A one-time link expires after 24 hours or after the first install.

Installation also includes the LogMeIn Client desktop app, a tool you can use to connect to your LogMeIn computers.

A computer can be attached to one LogMeIn account at a time.

How to Add a Computer via Phone or Tablet
Generate a link from your phone or tablet that can be used to add a computer to your account.

1. Launch the LogMeIn app on your device and log in using your LogMeIn ID and password.
Tip: Only Master Account Holders can add computers via phone or tablet. Make sure that you have selected your personal profile (Account Holder of...).

2. On the My Computers page, tap the menu icon and select Add Computer.

![My Computers](image)

Note: On tablets, you can add a computer by simply tapping the + icon.

3. Tap Share link to generate a deployment link.

![Add Computer](image)

4. Share the deployment link via your preferred method.

When the recipient clicks the link, LogMeIn host software is installed to the computer the recipient is using.

Note: The link is valid for 24 hours and can only be used once.

System Requirements – Host Computer

Before installing LogMeIn host software on the computer you want to access remotely, make sure the device meets the following requirements.

Supported Operating Systems

- Windows 7 or newer (including 64-bit)
- On Intel-based Macs: OS X 10.10 (Yosemite) or newer
- Windows Server 2008R2 or newer (including 64-bit)
- Linux, Chromebook and Windows RT are not supported
**Important:** Make sure you are using up to date, officially supported third-party technology together with LogMeIn. LogMeIn is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed). Learn more

### Internet Connection

Remote control performance depends on several factors, such as screen resolution, color depth, type of activity, available bandwidth and latency.

- For connecting and doing non-remote control work, any always-on internet connection is sufficient.
- For remote control, we require a 1.5 Mbit/s (192 Kbyte/s) or higher connection speed on each end, as per [FCC guidelines for video streaming](https://www.fcc.gov/advisories/video-streaming-guidelines). For optimal experience in Full HD resolution, a 2 Mbit/s (256 Kbyte/s) connection is recommended.

For details, see [How much bandwidth is required to use LogMeIn?](https://www.logmein.com/support/wifi/)

### LogMeIn and Firewalls

LogMeIn is compatible with all major security suites. Some configuration may be required to make LogMeIn work when the host is behind a firewall.

**Important:** If prompted, you must allow LogMeIn program files to communicate over the Internet for the service to function properly. For hardware firewalls, you must allow TCP port 443 traffic.

**Table 1: LogMeIn components**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogMeIn.exe</td>
<td>LogMeIn Desktop Application</td>
</tr>
<tr>
<td>LogMeInSystray.exe</td>
<td>LogMeIn Control Panel</td>
</tr>
<tr>
<td>LogMeInToolkit.exe</td>
<td>LogMeIn Client</td>
</tr>
<tr>
<td>LMIIgnition.exe</td>
<td>LogMeIn Service</td>
</tr>
</tbody>
</table>

For troubleshooting assistance, visit [help.LogMeIn.com](https://help.logmein.com).

Specific Knowledge Base articles cover known issues with numerous leading security products, including McAfee, Norton Internet Security, PC-Cillin, ZoneAlarm, Kaspersky, and AOL Spyware.

**Tip:** The [LogMeIn Community](https://www.logmein.com/community/) is an excellent source of information from other LogMeIn users.

### How to Configure Proxy Settings

Specify the proxy server LogMeIn will use as an intermediary between your web browser and the Internet.

**Tip:** Proxy servers are primarily used by companies and organizations. Home users generally will not need this option.

1. Access the host preferences:
• From the host computer, open the **LogMeIn Control Panel** and follow this path: **Options > Preferences > Advanced**
• From a client device, connect to the host **Main Menu** and follow this path: **Preferences > Advanced**

2. Under **Proxy Settings**, set the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy server address &amp; port</td>
<td>If you do not use a proxy server, leave this field empty. If you use a proxy, make sure the address and port information in this field match the information in your browser settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To find your proxy address and port in Internet Explorer, go to <strong>Internet Explorer &gt; Tools &gt; Internet Options &gt; &gt; Connections &gt; LAN Settings</strong>; or click <strong>Get proxy settings</strong> to retrieve available proxy settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Uncheck the box next to <strong>Use automatic configuration script</strong>. Instead, you should manually enter the proxy as an IP address and make sure the proxy port number is also set.</td>
</tr>
<tr>
<td>Proxy user name</td>
<td>Complete this field if the proxy server requires authentication.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>Complete this field if the proxy server requires authentication.</td>
</tr>
</tbody>
</table>

3. Click **OK** or **Apply**. Your settings are applied immediately to the host.

**Deploying LogMeIn Host Software**

Use the **Deployment** page to install LogMeIn host software to one or more remote computers and add the computers to your LogMeIn account.

**Who can use this feature?** The **Deployment** page is available to LogMeIn Central Account Holders and users who have **Deployment** permission.

**Key Terms**

To deploy LogMeIn host software, you must create an **installation package** and define a **deployment method**.

**Installation Package**

- When you create an installation package, you are answering the following questions:
  - Do you want new computers to be in a specific computer group?
  - Do you want to apply special host settings?
  - Do you want to activate alerts? Only available in Automation or Monitoring Modules.
Deployment Method

When you define the deployment method, you are answering the following questions:

• How do you want the actual installation to be executed? Using what technology, so to speak.
• Do you want to send an installation link (a clickable URL) by email, chat, or similar?
• Do you want to provide a centrally accessible installer?
• Do you want to provide a self-extracting installer?
• Do you want to run a batch file from the command prompt of the remote computer?

How to Deploy LogMeIn Host Software

Install LogMeIn host software to one or more remote computers and add the computers to your LogMeIn account.

1. In LogMeIn Central, go to the Deployment page.
   The Installation Package page is displayed.
3. Fill in the necessary fields and select the appropriate options for the remote installation.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>For your own reference, type a brief description that you will use to identify the installation package.</td>
</tr>
<tr>
<td>Installations allowed</td>
<td>Enter the maximum number of computers that will be able to use the installation package. Select Unlimited to allow any number of computers to use the package.</td>
</tr>
<tr>
<td>Expiration date</td>
<td>Default is one week. Select Never expires to allow installations from this package at any time in the future.</td>
</tr>
<tr>
<td>When no more seats are available, send an email to these addresses</td>
<td>Send a notification to the specified email addresses when you run out of available seats.</td>
</tr>
</tbody>
</table>

4. Under Configuration, select from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer group</td>
<td>Select the Computer Group to which you want to add the new hosts.</td>
</tr>
<tr>
<td>Alert package</td>
<td>Select the Alert Package to apply to new Windows hosts. Only available in Automation or Monitoring Modules.</td>
</tr>
<tr>
<td>Host preference package</td>
<td>Select the Host Preference Package to apply to new Windows hosts.</td>
</tr>
</tbody>
</table>

5. Optionally, click Advanced Settings to set proxy settings and additional options for remote installation.
The computer description is the host's name as displayed on your computer list. By default, LogMeIn uses the host's name as the computer description.

**Remember:** If you allow users to rename computers, you may not be able to recognize them on your computer list!

The LogMeIn installer will change the power settings of each new Windows host that has been otherwise set to sleep after a specific period of inactivity. Windows hosts connected to a standard AC power source (outlet) will be prevented from sleeping, thus ensuring access via LogMeIn.

**Proxy settings for the installation** If applicable, enter your proxy server settings.

6. Click **Save Settings**.
   The **Deploy Installation Package** page is displayed.

7. On the **Deploy Installation Package** page, select the **Deployment method** to be used by the installation package.
   For detailed information about each deployment method, see **About Deployment Methods** on page 26.

   **Note:** Your LogMeIn account information is included in the installer regardless of the deployment method.

   **Important:** If there is a problem with the deployment settings, you will see an alert. For information about alerts, see **Troubleshooting Installation Packages and Deployment** on page 26.

8. Optionally, click **Your personal notes** and enter comments.

9. Send the installation link or download the installer file, as appropriate. Follow on-screen instructions per method.

   **Tip:** Use the Account Audit feature to receive notification each time you deploy an installation package. See **Account Audit Notifications** on page 11.

### How to Modify an Installation Package

**Important:** Changing a deployment will instantly update any active installer packages **except** when you change proxy settings or the **Allow users to change the computer description during installation** option, in which case you must regenerate the installer package.

1. In LogMeIn Central, click the **Deployment** page.
2. On the **Deployment** page, click the name of the installation package you want to modify.
3. On the **Deploy Installation Package** page, click **Edit Installation Package**.
4. On the **Edit Installation Package** page, change the necessary deployment properties and click **Save Settings**.
About Deployment Methods
Four methods are available for distributing installation packages.

You must apply a deployment method to each installation package. See How to Deploy LogMeIn Host Software on page 24.

<table>
<thead>
<tr>
<th>Deployment Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Link</td>
<td>When the recipient clicks the link, LogMeIn host software is installed to the computer the recipient is using. Click <strong>Send Email with Link</strong> to send an email using your default email client. Alternatively, copy the link and paste it to your preferred chat tool. Ask the recipient to click the link and follow all on-screen installation instructions. <strong>Remember:</strong> LogMeIn will be installed on the computer where the recipient opens the link and runs the installer.</td>
</tr>
<tr>
<td>Installer File (.msi)</td>
<td>Download the <strong>LogMeIn.msi</strong> installer that must be run on the host computer manually. Click <strong>Download Installer File</strong> to download the LogMeIn installer package. Users must run this pre-configured installer to install the LogMeIn host on their computers. <strong>Note:</strong> Optionally, you can set up a Microsoft Windows Group Policy to automatically install LogMeIn hosts.</td>
</tr>
<tr>
<td>Installer Executable (.exe)</td>
<td>Download a self-extracting installer package. Click <strong>Download Installer Executable</strong> to download the LogMeIn installer package. Users must run this pre-configured installer to install the LogMeIn host on their computers.</td>
</tr>
<tr>
<td>Command or Batch File</td>
<td>Download a batch file or create a command that you can run from command prompt. You must download the <strong>LogMeIn.msi</strong> installer to use the batch file or command from <a href="https://secure.logmein.com/logmein.msi">https://secure.logmein.com/logmein.msi</a>. Click <strong>Download as Batch file...</strong> to download a batch file. Select <strong>Silent installation</strong> to install the host without user interaction.</td>
</tr>
</tbody>
</table>

Troubleshooting Installation Packages and Deployment
You may experience the following problems while attempting to distribute an installation package:
<table>
<thead>
<tr>
<th>Problem</th>
<th>Error Message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation package is disabled.</td>
<td>Installation package is disabled</td>
<td>Click <strong>enabled</strong> under status to enable deployment.</td>
</tr>
<tr>
<td>There is a problem with deployment that the alert specifies.</td>
<td>Installation package has expired Installation limit has been reached</td>
<td>Select <strong>Edit</strong> next to the installation package name and make necessary changes on the Deployment &gt; Installation Package page. For example, apply a different Host Preference Package.</td>
</tr>
<tr>
<td>There are multiple problems with deployment.</td>
<td>Installation package cannot be distributed</td>
<td>Select <strong>Edit</strong> next to the installation package name and make necessary changes on the Deployment &gt; Installation Package page. For example, installation limits may have been reached.</td>
</tr>
</tbody>
</table>

### Mass Deployment of LogMeIn Host Software (Silent Install)

You can run your own script to deploy LogMeIn host software to multiple computers at an organization.

**Important:** You must be familiar with Windows Active Directory to mass deploy the host software.

### Task 1: Prepare Your Installer Package and Batch Script

Ensure that all required deployment files for your chosen deployment method are in the correct place on your network. For more information, see About Deployment Methods on page 26.

1. Place your files in a shared folder that is accessible to everyone at your organization. For example, in a `\company\public` folder.

2. **Optional** (batch file deployments only): Edit your batch script so that it references the location of the MSI installer package, such as `\company\public\LogMeIn.msi`.

### Task 2: Configure Your Active Directory

In your Active Directory, you must define the computers to which you want to install LogMeIn host software.

**Note:** These instructions assume that you have a Windows 2012 domain controller. There may be slight differences in other versions of Windows.

1. (Optional) Create a new organizational unit for the computers to which you want to deploy LogMeIn host software.
   a) Open **Active Directory Users and Computers** from **Control Panel > Administrative Tools**.
   b) Right-click a domain and select **New > Organizational Unit**.
   c) Name the new organizational unit (for example, `TestUnit`) and click **OK**.
   d) Configure the newly created organizational unit.
      - For **per-computer deployment**, right-click a computer object, click **Move...** and select the organizational unit (`TestUnit`).
      - For **per-user deployment**, right-click a user, click **Move...** and select the organizational unit (`TestUnit`).
2. Create a Group Policy Object (GPO).
   a) Open Group Policy Management from Control Panel > Administrative Tools.
   b) Right-click the organizational unit (TestUnit) and click Create a GPO in this domain, and link it here....
   c) Name the policy (for example, GPO Pro Deploy) and click OK.
   d) Right-click the GPO and click Edit to open the Group Policy Management Editor.
   e) Configure policies.
      - For per-computer deployment, navigate to Computer Configuration > Policies.
      - For per-user deployment, navigate to User Configuration > Policies.
   f) Choose a deployment method.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Script and Installation package | 1. Select Windows Settings > Scripts (Startup/Shutdown)  
2. Right-click Startup and select Properties.  
3. Click Add on the Startup Properties dialog. |
| Installation package only (.msi) | 1. Expand Software Settings.  
2. Right-click Software installation and select New > Package.... |

   g) Browse to your batch script or installation package and click OK to close the dialog.

**Task 3: Update the Group Policy On the Host Computer**

As a last step, you must update the group policies of the hosts to run the installer package automatically when a user logs in.

1. On the host computer, open a command prompt and type gpupdate /force to force a group policy update.
   This ensures that the policy is applied immediately to the host computer.
2. Reboot the host computer and login.
   LogMeIn host software is installed upon login.

**How do I connect a "not accessible" computer to my account?**

When LogMeIn host software is installed on a computer but the computer is not attached to a LogMeIn account, the computer may show as Enabled but Offline or you see the following message: LogMeIn – not accessible – setup not completed.

This may happen, for example, if you delete your computer from your account via LogMeIn.com; the LogMeIn host software remains on your PC or Mac, but it is not associated with a LogMeIn account.

To enable your computer for remote access, you must associate it with a LogMeIn account.

1. Go to the computer that you want to be able to access remotely.
2. Open the LogMeIn Control Panel.
3. On the Overview tab or About tab, click Switch Account....
4. Enter the LogMeIn ID (email) and password for the account you want to use to access the computer. The Switch account... page is displayed.
5. Click Continue.
   LogMeIn must be restarted before the changes take effect.
Organizing, Finding and Working with Host Computers

Working with Computers in Your LogMeIn Account

Using Custom Fields to Organize Computers
The custom fields feature extends computer property information and integrates with your computer list seamlessly. Assign data of your choice to the computers you manage to find and sort them easier, or to add descriptive information.

<table>
<thead>
<tr>
<th>Some examples of what you can achieve</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Find computers by location</strong></td>
</tr>
<tr>
<td>• You receive an alert for a computer that you maintain for a large organization. Find its location in the building with a quick search.</td>
</tr>
<tr>
<td>• You receive alerts for multiple computers that they suddenly went offline. Location data reveals whether the issue is location-specific.</td>
</tr>
<tr>
<td><strong>Sort computers by service status</strong></td>
</tr>
<tr>
<td>• Track and prioritize your maintenance backlog using service status information.</td>
</tr>
<tr>
<td><strong>Add to-dos</strong></td>
</tr>
<tr>
<td>• Keep your action items in a central place and follow up to-dos efficiently.</td>
</tr>
<tr>
<td><strong>Assign custom data</strong></td>
</tr>
<tr>
<td>• Looking for the phone extension of a workstation? Look it up in a custom field in your computer list.</td>
</tr>
</tbody>
</table>

How to Define Custom Fields
The custom fields feature extends computer property information and integrates with your computer list seamlessly. Assign data of your choice to the computers you manage to find and sort them easier, or to add descriptive information.

1. On the Computers page, click above your computer list.

   **Remember:** Custom fields are visible only in Detail View.

   The Custom Fields dialog is displayed.

2. Enter a name for the field and click **Add new field**.

   Each field presents the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Visibility</strong></td>
<td>To show or hide a field in the computer list, click <em>visible</em> or <em>hidden</em>.</td>
</tr>
</tbody>
</table>
### How to Define Custom Fields

The custom fields feature extends computer property information and integrates with your computer list seamlessly. Assign data of your choice to the computers you manage to find and sort them easier, or to add descriptive information.

**Remember:** To assign custom values to a computer, you must first define custom fields. For details, see How to Define Custom Fields on page 30. You can also use custom fields to achieve the same goal as nested grouping (groups within groups) would.

1. On the **Computers** page, click once in a custom field column.

   **Remember:** You can edit field values only in Detail View.

2. Edit or delete computer-specific data.

   • Enter a value and click ✓ to assign it to the computer.

   **Tip:** When you start typing, Central brings up a list of recently assigned values for the field.

   • Clear the contents of a field to delete a value.

Changes are saved instantly.

You are now ready to assign custom data to your computers.

### How to Assign and Work with Custom Data

#### Option

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete</strong> To remove a field, click the <strong>Delete</strong> icon.</td>
</tr>
</tbody>
</table>

**Important:** Assigned field values are permanently lost.

Changes are saved instantly.
**Find computers**
Use the Search box above your computer list to find computers by a specific custom field value.

**Display relevant information**
When your computer list starts to become cluttered, you can show or hide custom field columns as you would with other properties using the column selector in the header bar.

### Viewing a List of Available Computers via PC or Mac

**From the LogMeIn Client desktop app**

Use the LogMeIn Client desktop app to view a list of computers in your account.

To launch the LogMeIn Client desktop app:

- Option 1. Click the LogMeIn system tray (or menu bar) icon and select **Connect to computers**.
- Option 2. Using the Start menu or Finder, start the **LogMeIn Client**.

**Don't see the computers you are looking for?** Remember to choose the correct **Profile** at the top of the LogMeIn Client interface.

![LogMeIn Client desktop app](image)

**From LogMeIn.com**

Log in to your account at LogMeIn.com to view a list of computers in your account.

Use the **List buttons** to change how computers are displayed.
Hide Groups on the Computer list

Click the View Computers button at the top of the LogMeIn Central user interface and then Show computers in groups to view your computers in a simple list, without showing groups.

View Groups using the Groups panel

Click the View Computers button at the top of the LogMeIn Central user interface and then Show group panel to view your computer groups in a list next to your Computer list.

Figure 1: The Computer Groups button

Figure 2: The Computer Groups panel button
The custom fields feature extends computer property information and integrates with your computer list seamlessly. Assign data of your choice to the computers you manage to find and sort them easier, or to add descriptive information.

**Manage Groups**

Click **edit** to work with an existing groups.

- Delete a group
- Change the computers in a group

**Tile View**

Try **Tile view** for a graphic view of computers in your account. Tile view is ideal if you have only a few computers in your account.

![Figure 3: Tile view](image)

**List View**

Try **List view** for a clean, simple view of computers in your account. List view shows the most computers at one time, making it an excellent choice if you have many computers in your account.

![Figure 4: List view](image)

**Tip:** To open the session in a new browser tab, click the blue "down arrow" next to a computer and select **Remote Control in new window**.

**Direct to Remote Control**

Click a computer name to go directly to remote control. Control-click or middle-click to open the session in a new browser tab.

**Detail View**

Try **Detail view** for a good balance between the graphic quality of Tile view and practicality of List view.
### Figure 5: Detail view

**Customize available columns**

Click the column selector in the header bar to view a list of available columns.

#### Health
Shows the status of Windows features on your hosts, including Windows Updates and Anti-virus. Hover your mouse over the icon to see the updates.

- Available on Windows hosts only.

#### Status
Shows which state the computer is in:

- Offline
- In Session
- Available

Click on these icons to take remote control of the host.

#### Computer
The Computer Description given when LogMeIn is installed. Click the Computer Description to control the host.

#### Version
The version number of the LogMeIn host software installed on the host. Click the version number to install the most up to date version of the LogMeIn Control Panel software on the host.

#### Direct Connect
- Take Remote Control of the host
- Enter File Manager
- Enter the Dashboard. For more information on the Dashboard, see *Using the LogMeIn Dashboard* on page 167.

#### Last Online
Shows the last time and date when the host was online.

#### Note
Add information about the host. Character limit: 500
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Shows the status of Windows Updates on the host machine.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Available on Windows hosts only." /></td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>Shows the status of Anti-virus software on the machine. For more information,</td>
</tr>
<tr>
<td></td>
<td>see <em>Viewing Anti-virus Status and Details</em> on page 72.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Shows an indicator of unacknowledged alerts on a host. For more information</td>
</tr>
<tr>
<td></td>
<td>on alerts, see <em>Working with Alerts</em> on page 45.</td>
</tr>
<tr>
<td>Properties</td>
<td>Takes you to the Host Properties screen.</td>
</tr>
<tr>
<td>Inventory</td>
<td>Takes you to the Host Properties &gt; Computer inventory section to run an</td>
</tr>
<tr>
<td></td>
<td>Inventory on a single host. For more information see <em>About Inventory Reporting</em></td>
</tr>
<tr>
<td></td>
<td>on page 117.</td>
</tr>
</tbody>
</table>

For additional Custom Fields, see *Using Custom Fields to Organize Computers* on page 30.

**Direct to Remote Control**

Click a computer name to go directly to remote control. Control-click or middle-click to open the session in a new browser tab.

Viewing a List of Available Computers via Phone or Tablet

In mobile apps, the *My Computers* page lists all computers in your account that are running LogMeIn host software.
Figure 6: The My Computers screen on an Android, with an active search for the term "Mac"

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Online" /></td>
<td>Online. You can connect to the computer.</td>
</tr>
<tr>
<td><img src="image" alt="Offline" /></td>
<td>Offline. You cannot connect to the computer. See also <em>Why does my computer show as Offline?</em> on page 233</td>
</tr>
<tr>
<td><img src="image" alt="Wake On LAN" /></td>
<td>The computer is ready for a wake-up signal via Wake On LAN. This is displayed when a computer is asleep and meets all Wake On LAN requirements. These computers are not shown if you are filtering out offline computers. For more information, see <em>How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN</em> on page 134.</td>
</tr>
</tbody>
</table>

**Computer buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Log out or change your active profile" /></td>
<td>Log out or change your active profile. The Profile option is available when you are a user of another LogMeIn account holder's computers.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| ![Settings](image) | **Settings:**  
  • Show or hide offline computers  
  • Change **Save Viewed Files** settings  
  • Clear saved login credentials  
  • Set timeout for your sessions  
  • Enable the Alert Viewer  
  • View the "Get Started" guide  
  • Send feedback to LogMeIn  
  • Check for updates |
| ![Refresh](image) | Refresh the computer list.  
  **Tip:** You can also pull down the computer list to refresh results. |
| ![Switch](image) | Switch between open pages:  
  • Go to **Local Files** to view files transferred to your device using File Manager  
  • Go to **Computers** to launch Remote Control or File Manager  
  • Go to any open instance of the File Manager to work with files  
  • Open the Alert Viewer to view and acknowledge triggered alerts |

**How to Find a Computer on a PC or Mac**

To find a specific computer, you can filter and sort computers in your LogMeIn account.

2. Log in to your account using your LogMeIn ID (email address) and password.  
   The **Computers** page is displayed.
3. Start typing into the **Search** field in the top-right corner. You can enter multiple search words.  
   Computers with properties or custom field data that contain your search words are automatically displayed.
4. To filter your results, click the drop-down list next to the **Search** field and select a filter.

You can sort your results in Details View by clicking a column name. Sorting and filtering are kept when you change your view.

**Note:** You can limit the maximum number of computers displayed on one page by selecting a limit from the drop-down list at the bottom of the page.

**How to Find a Computer on a Phone or Tablet**

To find a specific computer, you can search for computer or group names on your phone or tablet.

1. Open the LogMeIn app.
2. In the Search field above the computer list, type your search expression.  
   The computer list is filtered by your criteria.
Tip: Pull down the computer list to refresh results.

How to Rename a Computer

Go to the LogMeIn website to change the name by which a computer is listed in your LogMeIn account.

**Important:** This does not change the actual Computer Name as set at the operating system level (for example, under System Properties > Computer Name in Windows).

**Remember:** Use your browser for this action.

2. Log in to your account using your LogMeIn ID (email address) and password. The Computers page is displayed.
3. On the Computers page, click Properties > General Settings for the computer you want to rename.
4. Enter a new computer name in the Computer description box.
5. Click Change to save the new name.

How to Move a Computer to Another Account

To move a computer to another account, use the LogMeIn Control Panel.

1. On the computer you want to move, open the LogMeIn Control Panel and click the About tab.
2. On the About tab, click Switch Account. You are prompted to log in.
3. Log in using a LogMeIn ID that has access to the account that should receive the computer.
4. If prompted, assign a subscription.
5. Enter a description (name) for the computer.
6. Click Continue. The LogMeIn host software restarts. The computer is assigned to the new account.
How to Delete a Computer from Your Account

You can clean up your computer list by deleting computers from your account.

Remember: Use your browser for this action.

Important: When you delete a computer, all associated current and historical data is permanently lost.

2. Log in to your account using your LogMeIn ID (email address) and password. The Computers page is displayed.
3. To delete a single computer:
   a) On the Computers page, click Properties. The Host Properties page is displayed.
   b) At the bottom of the Host Properties page (General Settings tab), click Delete this computer.
      The computer is removed from your list. The host software remains on the computer. Nothing is uninstalled.
4. To delete multiple computers:
   a) On the Computers page, change the computer view to Detail View.
   b) Click the checkbox for each computer you want to delete.
   c) Click the Delete icon above the computer list and confirm deletion.
      The computers are removed from your list. The host software remains on each computer. Nothing is uninstalled.

Using the Favorites List

The Favorites list gives you easy access to commonly used computers and features.

On the LogMeIn Central Computers page, type a search string in the Search field in the upper-right corner.

Click the Add this search to favorites link to add the search parameters to your Saved Searches list.
Managing Groups of Computers

Organize computers according to location, function, access permissions, or any criteria you specify. For example, you might place all servers in one group, PCs in another, and Macs in a third.

Who can use this feature? Computer groups can be managed by all LogMeIn Central account holders and any LogMeIn Central user with the Computer Group Management permission set on the Users page.

View Groups using the Groups list

Use the Groups list at the top of the page of the LogMeIn Central interface to filter computers by group or status.

![Groups list screenshot]

Figure 7: The Groups list

- Click a group to display all computers in the group on the Computers page
- Click Show All Groups to show all computers in all groups on the Computers page
- Click a filter to display computers that are in session, inline, or were recently accessed

View Groups using the Groups panel

Click the View Computers button at the top of the LogMeIn Central user interface and then Show group panel to view your computer groups in a list next to your Computer list.

![Groups panel screenshot]

Figure 8: The Computer Groups panel button
The custom fields feature extends computer property information and integrates with your computer list seamlessly. Assign data of your choice to the computers you manage to find and sort them easier, or to add descriptive information.

**Hide Groups on the Computer list**

Click the **View Computers** button at the top of the LogMeIn Central user interface and then **Show computers in groups** to view your computers in a simple list, without showing groups.

![Figure 9: The Computer Groups button](image)

**Manage Groups from the Computers page**

On the Computers page in Tile view or Detail view, click **edit** to work with groups.

*Note:* The [Default Group] has no edit option. By default, all new Computers are added to [Default Group] unless otherwise specified.

- Edit a group name
- Delete a group
- Change the computers in a group

**Creating a Computer Group**

1. Log in to [https://secure.logmein.com](https://secure.logmein.com).
2. Under **Computers**, select **Add Group**.
3. Create a **Group name** and click **Add**. The **Edit Computer Group** page appears.

---

### About the Impact of Group Changes (Moved Computers) on User Access

Computers can be reassigned, or moved, from one group to another. This table summarizes the different types of group and computer permissions and the potential impact of a changed group or moved computer.

<table>
<thead>
<tr>
<th>Selection status</th>
<th>Sample</th>
<th>Impact when a computer is moved from the group</th>
</tr>
</thead>
<tbody>
<tr>
<td>A computer is selected as part of a group <strong>but not</strong> selected individually</td>
<td><img src="image" alt="Groups/Computers" /></td>
<td>If a computer is moved to another group that is accessible by the user, it will be accessible to the user. If moved to a group that is not accessible to the user, a computer will not be accessible to the user.</td>
</tr>
<tr>
<td>A computer is selected individually <strong>but not</strong> as part of a group</td>
<td><img src="image" alt="Groups/Computers" /></td>
<td>If a computer is moved anywhere else in the account, it will remain accessible to the user.</td>
</tr>
<tr>
<td>A computer is selected individually <strong>and</strong> as part of a group</td>
<td><img src="image" alt="Groups/Computers" /></td>
<td>If a computer is moved anywhere else in the account, it will remain accessible to the user.</td>
</tr>
<tr>
<td>Selection status</td>
<td>Sample</td>
<td>Impact when a computer is moved from the group</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Neither a group nor any individual computers have been selected</td>
<td><img src="image" alt="Groups/Computers" /></td>
<td>No access has been given to either a group or an individual computer, so no computer in the group is visible or accessible to the user.</td>
</tr>
</tbody>
</table>
Using the Management Cloud: LogMeIn Central Core Features

Working with Alerts

Alerts notify you of specific events or problems that occur on one or multiple LogMeIn Windows or Mac hosts in a Premier account. This feature provides a quick and easy way to monitor any number of hosts from one client.

In LogMeIn Central, click the Alerts page to view, edit, or add alerts for specific computers or groups of computers.

To activate alerts, first create an Alert Package, and then assign the package to computers or groups of computers.

Who can use this feature? The Alerts feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premier</td>
<td>Automation</td>
<td>Alert Management</td>
</tr>
<tr>
<td></td>
<td>Insight</td>
<td></td>
</tr>
</tbody>
</table>

LogMeIn Central Alert Rule Types

Alert rules are combined into Alert Packages that are assigned to computers and groups of computers. Premier, Automation or Insight only.

<table>
<thead>
<tr>
<th>Alert Rule</th>
<th>Description</th>
</tr>
</thead>
</table>
| Workstation template | Select this template to use a predefined selection of alerts commonly assigned to workstations. The package contains the following alerts:  
  • Application: Crashes, Starts, and Stops  
  • Hardware Inventory: Memory Added and Memory Removed  
  • Event: Failed Login |
| Server template    | Select this template to use a predefined selection of alerts commonly assigned to servers. The package contains the following alerts:  
  • Event: Failed Login  
  • CPU Utilization: CPU Utilization  
  • Computer: Offline 10 minutes  
  • Software Inventory: Uninstalled software |
| Kiosk template     | Select this template to assign a predefined selection of alerts to computers running in kiosk mode, for example a dedicated or public display. The package contains the following alerts:  
  • Application: Crashes, Starts, and Stops |
<table>
<thead>
<tr>
<th>Alert Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU Utilization</strong></td>
<td>Use the CPU Utilization alert to monitor processor utilization on a computer or across a group of computers. If a device has more than one CPU, you can configure the alert to check utilization of either an individual or all CPUs. CPU Utilization is measured as a percentage of the whole. An alert is triggered when the Usage threshold is breached and held for the specified Duration.</td>
</tr>
<tr>
<td><strong>Memory Usage</strong></td>
<td>Use the Memory Usage alert to monitor computer memory utilization on a computer or across a group of computers. Memory Usage is measured as a percentage of the whole. An alert is triggered when the Usage threshold is breached and held for the specified Duration.</td>
</tr>
<tr>
<td><strong>Free Disk Space</strong></td>
<td>Use the Free Disk Space alert to monitor the space remaining on a defined disk drive on a computer or across a group of computers. An alert is triggered when free disk space falls below the defined minimum as expressed in MB or as a percentage of the total size of the disk.</td>
</tr>
<tr>
<td><strong>Folder Size</strong></td>
<td>Use the Folder Size alert to monitor the total size of a particular folder on a computer or across a group of computers. The Folder path must be the same on each computer in a group. If the Folder path is invalid for a given computer, then the alert will be ignored for that particular device. An alert is triggered when the folder size exceeds the maximum size (measured in KB, MB, or GB).</td>
</tr>
<tr>
<td><strong>File Size</strong></td>
<td>Use the File Size alert to monitor the total size of a particular file on a computer or across a group of computers. The File path must be the same on each computer in a group. If the File path is invalid for a given computer, then the alert will be ignored for that particular device. An alert is triggered when the file size exceeds the maximum size (measured in KB, MB, or GB).</td>
</tr>
<tr>
<td><strong>Computer (Online/Offline)</strong></td>
<td>Use the Computer alert to monitor the availability of computers in your account. An alert is triggered when a particular computer goes offline and stays offline for the specified Duration or comes online and stays online for the specified Duration.</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>Use the Application alert to monitor the activity of a particular program on a computer or across a group of computers. An alert is triggered when an application starts, stops, or crashes. Define the application name. The full path to the executable file is not required. If the application is not found on a given computer, then the alert will be ignored for that particular device.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>Use the Service alert to monitor the activity of a particular service running on a computer or across a group of computers. An alert is triggered when</td>
</tr>
<tr>
<td>Alert Rule</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td><strong>Windows hosts only.</strong> Use the Event alert to monitor event code activity on a computer or across a group of computers. This rule will alert when an event log entry that matches the specified criteria is written to one of the standard Windows event logs. You can define multiple event source, event category or event identifiers to look for, and you can also define exceptions. You can use wildcards where text can be entered: the asterisk (*) will match any substring while the question mark (?) will match any single character.</td>
</tr>
<tr>
<td>Hardware Inventory</td>
<td>Use the Hardware Inventory alert to monitor changes to hardware components on a computer or across a group of computers. An alert is triggered when the selected component is added or removed, as defined.</td>
</tr>
<tr>
<td>Software Inventory</td>
<td>Use the Software Inventory alert to monitor changes to software components on a computer or across a group of computers. An alert is triggered when a component is installed or uninstalled, as defined.</td>
</tr>
<tr>
<td>System Inventory</td>
<td>Use the System Inventory alert to monitor changes to Windows profiles, Local Users, and settings on a computer or across a group of computers. An alert is triggered when the selected system component is added or removed, as defined.</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>Use the Anti-virus alert to be notified of issues with anti-virus software on a computer or across a group of computers. You can choose to be alerted when LogMeIn detects no anti-virus installations, an out of date definition file, a threat requiring immediate attention (a &quot;red&quot; threat), or when real-time protection is switched off.</td>
</tr>
<tr>
<td>Windows Update</td>
<td><strong>Windows hosts only.</strong> Monitor the status of Windows Update. An alert is triggered when LogMeIn detects a Windows Update report and the specified criteria are met.</td>
</tr>
</tbody>
</table>

### How to Create Alert Rules in an Alert Package

The first step in the Alert process is to create an **Alert Package** containing Alert Rules.

**Who can use this feature?** The **Alerts** feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Alert Management</td>
</tr>
<tr>
<td>• Premier</td>
<td>• Insight</td>
<td></td>
</tr>
</tbody>
</table>

An Alert Package is a set of rules that you can save and apply to a computer or group of computers.

1. In LogMeIn Central, go to the **Alerts > Manage Alert Packages** and add or edit an Alert Package.
The **Add Alert Package** page is displayed.

2. Add rules to the package.
   a) Click **Add New Alert Rule** and select the type of rule to add.
   b) Edit the rule to meet your needs.

3. To manage email options for a triggered alert, select **When alert is triggered, also send an email**. Additional email options are displayed:
   - **Send email when alert is acknowledged**
   - **Include links to remote control and inventory**. The email will include a link that launches remote control or opens an inventory report for the impacted host.
   - **Send email when status returns back to normal**
   - : The email text box's maximum allowance is 128 characters. Where possible, use email distribution groups to send to multiple recipients.

4. To make a self-healing alert, select **When alert is triggered, also start a One2Many task**. This option is only available when you have existing One2Many tasks. Choose a One2Many task that will address the alert.

5. Continue to add rules as required.
   💡 **Tip:** Click **Export** to save the Alert Package in an .xml file for later use.

6. Click **Save**.
   The package is saved and ready to be assigned to computers or groups of computers.
   💡 **Tip:** To import a saved Alert Package (.xml), click **Import**.

Check the LogMeIn Community for **Alert Packages posted by other LogMeIn users**.

### How to Assign an Alert Package

Alert Packages must be assigned to computers or groups of computers to take effect.

**Who can use this feature?** The **Alerts** feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Alert Management</td>
</tr>
<tr>
<td></td>
<td>• Insight</td>
<td></td>
</tr>
</tbody>
</table>

1. In LogMeIn Central, go to the **Alerts > Manage Alert Packages** page.
   A list of available Alert Packages is displayed.

2. Click **Click here to assign** next to the package you want to assign.
   The **Select Target Computers for Alert Package** page is displayed.

3. Select computers and groups.
   💡 **Important:** Only one Alert Package at a time can be assigned to a host.

4. Click **Save and Close**.
   The Alert Package is applied to all selected computers and groups.

The package is applied to all computers and groups in the left panel.
When do the changes take effect? The package is deployed within one minute to any host that is online. For any host that is offline, the package is stored and deployed when the host next comes online.

How to Manage Incoming Alerts on a PC or Mac

Use the Alert Viewer to view and manage triggered alerts. Triggered alerts should be acknowledged.

Who can use this feature? The Alerts feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Alert Management</td>
</tr>
<tr>
<td></td>
<td>• Insight</td>
<td></td>
</tr>
</tbody>
</table>

Tip: You can also automatically run One2Many tasks in response to triggered alerts. For details, see How to Create Alert Rules In an Alert Package on page 47.

On the Computers page, computers with triggered alerts are identified with a red number signifying the number of alerts awaiting attention.

Figure 10: Triggered Alerts in Tile view

![Triggered Alerts in Tile view](image)

Figure 11: Triggered Alerts in Detail view

1. On the LogMeIn Central Computers page, click the link showing the number of triggered alerts. The Alert Viewer is displayed.
2. For any alert listed on the Alert Viewer, select the check box next to the computer name.
3. Click Acknowledge Selected. The selected items are marked as acknowledged.

Tip: You can also see a list of triggered alerts by going to Alerts > Alert Viewer.

How to Manage Incoming Alerts on a Phone or Tablet

Use the Alert Viewer to view and acknowledge triggered alerts.

Who can use this feature? The Alerts feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Alert Management</td>
</tr>
<tr>
<td></td>
<td>• Insight</td>
<td></td>
</tr>
</tbody>
</table>
**Important:** To manage alerts with the LogMeIn app, you must enable the **Alert Viewer** in the settings. Tap 📢 to bring up the settings screen and select **Enable Alert Viewer**.

**Note:** When unacknowledged alerts are present, the Alert Viewer is enabled by default.

1. Open the LogMeIn app.
2. Tap 🔍 or swipe left to access the Alert Viewer. The latest 100 alerts are shown. You can show up to 200 at a time.
3. Tap an alert to see its details.
   For each alert, you can perform the following actions:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Remote Control" /></td>
<td>Remote control the computer that triggered the alert.</td>
</tr>
<tr>
<td><img src="image" alt="File Manager" /></td>
<td>Start the File Manager for the computer that triggered the alert.</td>
</tr>
<tr>
<td><img src="image" alt="Acknowledge" /></td>
<td>Acknowledge the alert.</td>
</tr>
</tbody>
</table>

**About Self-healing Alerts**

A self-healing alert is a standard alert that you have set to automatically run a One2Many task when triggered.

**Who can use this feature?** The **Self-Healing Alerts** feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Alert Management</td>
</tr>
</tbody>
</table>

To make a self-healing alert, go to **Alerts > Manage Alert Packages** and edit or add an Alert Package as you normally would. For any Alert Rule, select **When alert is triggered, also start a One2Many task**.

**Tip:** This option is only displayed when you have existing One2Many tasks.

To view the results of One2Many tasks that have been run in response to triggered alerts, go to **Alerts > Self-healing Alert History**.

Results can be sorted as follows:

- Running
- Completed today
- Completed this week
- Completed this month
- All completed
One2Many

Execute, manage, and monitor administrative tasks on multiple computers directly from LogMeIn Central.

What can you achieve with One2Many?

Who can use this feature? The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

• Install or update software
• Execute a remote command
• Run a batch file or executable
• Update registry settings
• Distribute files
• Execute complex custom administrative jobs

How does it work? At a glance.

1. **Create a task.** Tasks contain the program you want to install, the files you want to distribute, the command you want to run, or the settings you want to push. Create and save multiple tasks. You can then run them according to a specific plan. Each task can be associated with multiple plans. Sample tasks: **Install Adobe Reader** or **Run Virus Scanner**.

2. **Create a plan.** Plans define the computers that will receive the task and tell the task how and when to run. Each plan can only be associated with one task. Sample plans: **All Servers in Building 7** or **Windows 8.1 Desktops**.

3. **Run the plan.** Either run the plan immediately or according to a schedule.

**Tip:** You can also automatically run One2Many tasks in response to triggered alerts (also known as self-healing alerts). For details, see How to Create Alert Rules in an Alert Package on page 47.

**Sample Task/Plan combination**

Your goal is to distribute a new virus scan software to the sales team's LogMeIn Windows hosts. You want this to happen on December 14 at 21:00.

• First, you create a task called "Install Virus Scan Software" and include the relevant .msi file as a resource.
• Next, you create a plan called "Sales PCs Dec14 21:00" that includes all computers in the group "Sales PCs" and schedules the task to run on December 14 at 21:00.
• When creating the plan, you ensure that the task "Install Virus Scan Software" is assigned to the plan. Otherwise the plan won't know what to do.
Host-side requirements
Make sure your hosts are running the latest version of the host software.

Client-side requirements
You must have Flash version 9 or above to upload task resources and manage credentials. Without Flash, all you can do is run plans for existing tasks and execute remote commands that do not require uploaded files.

How to Execute a Remote Command

Who can use this feature? The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

**Important:** This type of task can only be deployed to Windows hosts.

1. In LogMeIn Central, go to the One2Many > Tasks page.
2. Click **Create Task**.
   The Create Task page is displayed.
3. Select **Execute a remote command**.

4. Name the task in the **Task name** field.
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. Under **Language**, select the language in which to run the task.

<table>
<thead>
<tr>
<th>Language</th>
<th>Character Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMD</td>
<td>1000</td>
</tr>
<tr>
<td>PowerShell</td>
<td>15000</td>
</tr>
</tbody>
</table>

6. Type the **Command to execute**.
7. Choose whether to assign a plan now, or later:
   • To save your task and create a new plan that will be used to run the task, click **Save and continue**
   • To save the task without assigning a plan, click **Save and close** (you will be able to assign a plan later)

See **How to Create a Plan for Executing One2Many Tasks** on page 59 to continue.
Tip: Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the One2Many > Plans page. You can view logs for completed tasks on the One2Many > History page.

How to Run a Batch File or Executable on Remote Hosts

Who can use this feature? The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premier</td>
<td>Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

Important: This type of task can only be deployed to Windows hosts.

1. In LogMeIn Central, go to the One2Many > Tasks page.
2. Click Create Task.
   The Create Task page is displayed.
3. Select Run a batch file or executable.
4. Name the task in the Task name field.
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. To locate and upload resources required to complete the task, click Browse....
6. Enter Optional parameters.
   For example, you want setup.exe to be executed with the following options: setup.exe /q /s /z.
   Parameters must be valid commands for the files attached to the task.

   Important: Programs must run silently and cannot require user input.

   Note: The Full command field shows you the exact command that will be sent to your hosts. Use it to confirm that the syntax of the command matches your expectations.
7. To override default logging and create a custom log file, select Use custom log file and type a path to the log.
8. Choose whether to assign a plan now, or later:
   • To save your task and create a new plan that will be used to run the task, click Save and continue
   • To save the task without assigning a plan, click Save and close (you will be able to assign a plan later)
See *How to Create a Plan for Executing One2Many Tasks* on page 59 to continue.

**Tip:** Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the *One2Many > Plans* page. You can view logs for completed tasks on the *One2Many > History* page.

---

### How to Distribute Files to Remote Hosts

**Who can use this feature?** The *One2Many* feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

**Important:** This type of task can only be deployed to Windows hosts.

1. In LogMeIn Central, go to the *One2Many > Tasks* page.
2. Click **Create Task**.
   
   The *Create Task* page is displayed.
3. Select **Distribute files**.

4. Name the task in the **Task name** field.
   
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. To locate the files you want to distribute, click **Browse**....
   
   You can upload multiple files.
6. Set the **Destination Folder**.
   
   This field is displayed after you have selected a file to distribute.

   **Tip:** The path may contain environment variables.

7. Under **Overwrite existing files**, choose whether or not to overwrite files that already exist on the targeted hosts.
8. Under **Folder creation behavior**, select **Create folders if they don't already exist** to push files in folders.
9. Choose whether to assign a plan now, or later:

   - To save your task and create a new plan that will be used to run the task, click **Save and continue**
   - To save the task without assigning a plan, click **Save and close** (you will be able to assign a plan later)
See *How to Create a Plan for Executing One2Many Tasks* on page 59 to continue.

Tip: Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the **One2Many > Plans** page. You can view logs for completed tasks on the **One2Many > History** page.

---

### How to Install, Uninstall, or Update Software on Remote Hosts

**Who can use this feature?** The **One2Many** feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

1. In LogMeIn Central, go to the **One2Many > Tasks** page.
2. Click **Create Task**.
   The **Create Task** page is displayed.
3. Under **Select for Windows**, select **Install or update software**.
4. Name the task in the **Task name** field.
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. To locate and upload resources required to complete the task, click **Browse...**
6. Enter valid MSI parameters under **Optional Parameters**.
   To uninstall software, select the **Uninstall** option.
   **Important:** Installs must run silently and cannot require user input.
   **Note:** The **Full command** field shows the exact command that will be sent to the hosts. Use it to confirm that the syntax of the command matches the expectations.
   **Tip:** Consult the Windows Installer SDK for additional documentation on command line syntax.
7. Choose whether to assign a plan now, or later:
   • To save your task and create a new plan that will be used to run the task, click **Save and continue**
   • To save the task without assigning a plan, click **Save and close** (you will be able to assign a plan later)

See *How to Create a Plan for Executing One2Many Tasks* on page 59 to continue.

Tip: Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the **One2Many > Plans** page. You can view logs for completed tasks on the **One2Many > History** page.
How to Update Registry Settings on Remote Hosts

**Who can use this feature?** The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

---

**Important:** This type of task can only be deployed to Windows hosts.

1. In LogMeIn Central, go to the One2Many > Tasks page.
2. Click Create Task.
   The Create Task page is displayed.
3. Select Update registry settings.
4. Name the task in the Task name field.
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. To locate and upload the REG file required to complete the task, click Browse...

   **Note:** The Full command field shows you the exact command that will be sent to your hosts. Use it to confirm that the syntax of the command matches your expectations.

6. Choose whether to assign a plan now, or later:
   • To save your task and create a new plan that will be used to run the task, click Save and continue
   • To save the task without assigning a plan, click Save and close (you will be able to assign a plan later)

   See *How to Create a Plan for Executing One2Many Tasks* on page 59 to continue.

---

**Tip:** Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the One2Many > Plans page. You can view logs for completed tasks on the One2Many > History page.

---

**How to Create a Custom Task for Complex Jobs**

Use a custom task to execute a set of complex administrative actions that require multiple resources and commands.

**Who can use this feature?** The One2Many feature is available for the following:
When might you use a custom task? For example, within a single task you may want to run an updated .msi for anti-virus software and upload virus definition files. Also, you want to perform a full scan on all local drives and copy the resulting log files to your company file server. Another example: You may want to upload files of numerous types (.exe, .bat, .dll, .cmd) and use an install.bat command to execute the job.

**Important:** This type of task can only be deployed to Windows hosts.

1. In LogMeIn Central, go to the **One2Many > Tasks** page.
2. Click **Create Task**.
   The **Create Task** page is displayed.
3. Select **Custom**.
4. Name the task in the **Task name** field.
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. To locate and upload resources required to complete the task, click **Browse...**.
6. If required, type a **Command to execute**.
   **Tip:** Click the **variables** link to see a list of environment variables you can use in a command.
7. Type a **Successful exit code** if the command you run returns a custom value on successful execution. This value is zero by default.
8. To override default logging and create a custom log file, select **Use custom log file** and type a path to the log.
9. Choose whether to assign a plan now, or later:
   - To save your task and create a new plan that will be used to run the task, click **Save and continue**
   - To save the task without assigning a plan, click **Save and close** (you will be able to assign a plan later)

See **How to Create a Plan for Executing One2Many Tasks** on page 59 to continue.

**Tip:** Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the **One2Many > Plans** page. You can view logs for completed tasks on the **One2Many > History** page.
How to Install or Update Software on Mac Remote Hosts

Who can use this feature? The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

Note: DMG files must contain only the application that you want to install.

1. In LogMeIn Central, go to the One2Many > Tasks page.
2. Click Create Task.
   The Create Task page is displayed.
3. Under Select for Mac, select Install or update software.

4. Name the task in the Task name field.
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. Choose whether to assign a plan now, or later:
   • To save your task and create a new plan that will be used to run the task, click Save and continue
   • To save the task without assigning a plan, click Save and close (you will be able to assign a plan later)

See How to Create a Plan for Executing One2Many Tasks on page 59 to continue.

Tip: Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the One2Many > Plans page. You can view logs for completed tasks on the One2Many > History page.

How to Create a Custom Task for Mac

Use a custom Mac task to execute a set of complex administrative actions that require multiple resources and commands.

Who can use this feature? The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>
Important: This type of task can only be deployed to Mac hosts.

1. In LogMeIn Central, go to the One2Many > Tasks page.
2. Click Create Task.
   The Create Task page is displayed.
3. Under Select for Mac select Custom Mac.
4. Name the task in the Task name field.
   Since you may end up with many saved tasks, be sure to use a clear and specific name.
5. To locate and upload resources required to complete the task, click Browse....
6. If required, type a Command to execute.
   Tip: Click the variables link to see a list of environment variables you can use in a command.
7. Type a Successful exit code if the command you run returns a custom value on successful execution. This value is zero by default.
8. Choose whether to assign a plan now, or later:
   • To save your task and create a new plan that will be used to run the task, click Save and continue
   • To save the task without assigning a plan, click Save and close (you will be able to assign a plan later)

See How to Create a Plan for Executing One2Many Tasks on page 59 to continue.

Tip: Once you have assigned a task to a plan and have run the plan, you can monitor progress and view logs on the One2Many > Plans page. You can view logs for completed tasks on the One2Many > History page.

How to Create a Plan for Executing One2Many Tasks

Plans define the computers that will receive the task and tell the task how and when to run.

Who can use this feature? The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

1. To create a plan, you must access the Create plan page in one of the following ways:
   • Option 1: Go to the One2Many > Plans page and click Create Plan.
   • Option 2: On the Create Task page, click Save and continue.
   • Option 3: On the Tasks page, click Run. Select Create a new plan in the resulting dialog.

   The Edit Plan page is displayed

2. Name the plan in the Plan name field.
Tip: When naming plans, try to focus on the group of computers to which the plan is assigned (for example Sales Laptops, All Servers in Building 7, Windows XP Desktops, or similar).

3. Use the Task to run drop-down list to choose the task that you want to execute with this plan.

   Important: You can only assign one task to a plan.

4. Choose to run the task now or later under When to run task.
   - Choose Run the plan now to run the plan immediately after saving the plan and assigning credentials.
   - Choose Schedule plan to run later to set the plan to run at a specific time or according to a recurring hourly, daily, weekly, or monthly schedule.

5. Under Other options, choose from the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource transfer timeout</td>
<td>Abort the associated task on any host to which task resources fail to transfer within the defined period.</td>
</tr>
<tr>
<td>Task timeout</td>
<td>End processes specified in the associated task on any host for which the task fails to complete within the defined period.</td>
</tr>
<tr>
<td>Attempt to wake up computers that are switched off</td>
<td>This setting only applies to hosts meeting all Wake On LAN requirements. See the LogMeIn User Guide for details.</td>
</tr>
<tr>
<td>When plan completes, send an email summary to</td>
<td>Enter the email addresses where you want to send a notification when the plan is completed.</td>
</tr>
<tr>
<td>Notes</td>
<td>Enter a note to help you or your colleagues work with this plan.</td>
</tr>
</tbody>
</table>

6. Under Select computers, select LogMeIn host computers to be included in the plan. The action in the associated task will be applied to the selected hosts.

7. Choose whether to enter host login credentials now, or later:
   - To enter credentials now, click Save and continue. See Working with Host Login Credentials on page 60 for details.
   - To save the plan without entering credentials, click Save and close.

   Important: Tasks can only be executed on LogMeIn hosts after successful authentication.

Working with Host Login Credentials

Make it easy to log in to your hosts by securely storing host credentials.

Who can use this feature? The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
</tbody>
</table>
1. To manage credentials, you must access the Global credential management page in one of the following ways:
   - Go to Configuration > Credentials.
   - During the process of creating a One2Many plan, you will be prompted to enter credentials before you can run a plan. Tasks can only be executed on LogMeIn hosts after successful authentication.

2. Select a computer or computers on the list of available hosts.

3. Enter credentials for the selected host(s).
   To verify credentials before they are saved, select the Verify credentials box.
4. Click Apply to Selected Computers to save.

**How to Track Plan Results and View Logs**

Use the One2Many > History page to view log files for completed tasks.

**Who can use this feature?** The One2Many feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Automation</td>
<td>• Create and Modify One2Many tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run One2Many tasks</td>
</tr>
</tbody>
</table>

**Note:** To view tasks still in progress, go to the One2Many > Plans page and click the Running plans filter.

1. In LogMeIn Central, go to the One2Many > History page. A list of executed plans is displayed.

**Tip:** Use filters or the search field to locate specific plans.
2. Click **View** next to any plan on the list.

Plan results are displayed.

3. On the **Plan** tab of the results page, click **View log file** to view the logs.

**Troubleshooting One2Many**

**Does the task run locally?**

Tasks must run without any user interaction. Ensure the task runs locally, and there are no prompts for user action.

**Can you ping upload.logmein.com**

One2Many downloads all tasks from upload.logmein.com. Ensure that upload.logmein.com is accessible. For more information, see *Whitelisting and LogMeIn*.

**Can the admin profile access C: \Windows\Temp**

The credentials you use for the host must be able to write to C: \Windows\Temp. A temporary directory is created in C: \Windows\Temp and the task is executed there.
Managing Windows and Microsoft Updates

With Update Management you can control how Windows and Microsoft updates are installed on all supported hosts in your account. (Also referred to as Patch Management.)

Who can use this feature? The Update Management feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Security</td>
<td>• Windows update Management</td>
</tr>
</tbody>
</table>

Required LogMeIn software

Required host software: Version 4.1.1868 or higher

Required host operating systems

The host must run an officially supported Windows operating system. See System Requirements – Host Computer on page 21.

Tip: Consult Microsoft documentation for comprehensive information about Windows and Microsoft updates.

Note: In Windows 10 Home Edition the Windows Update Settings can't be changed.


How to View Update Status

In LogMeIn Central, go to the Updates page.

Remember: A Premier or Insight subscription is required to use this feature.

Color coded shield icons indicate the update status of each supported host:

- 🟢 Service is set to check for updates automatically. All important updates are installed.
- 🟠 Service is set to check for updates automatically. Important updates are pending.
- 🟡 Host will attempt to reboot automatically after installing updates. This icon is only available on the Updates page.
- 🔴 Service is set to never check for updates, or the service cannot be accessed.
- ⚠️ Host reboot required
Filtering computers on the Updates page

To filter computers displayed on the Updates page, use the drop-down list at the top of the page. Available filters:

- Operating system
- Update status
- Subscription

How to Change Update Settings for a Single Host

**Remember**: A Premier or Insight subscription is required to use this feature.

1. In LogMeIn Central, from either the Computers page or Updates page, click the shield icon or Properties > Updates next to the computer you want to change. The Change settings page is displayed.

2. Change how Windows installs updates. Some settings may be managed by the system administrator. See Windows documentation for details. All settings are the same as in Windows.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important updates</td>
<td>Select how important updates are downloaded and installed.</td>
</tr>
<tr>
<td>Software to update</td>
<td>Choose to install either Windows updates only or Microsoft product updates along with Windows updates (for example, Microsoft Office updates).</td>
</tr>
</tbody>
</table>

The updates that only a system administrator can change are grayed out.

3. To display delivery options, click Change next to How the settings above are delivered to hosts. These settings are not applied to hosts, but rather tell LogMeIn how to deliver the Updates-related settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempt to connect to computers for</td>
<td>LogMeIn will attempt to change how Windows installs updates for this period of time.</td>
</tr>
<tr>
<td>Wake up computers</td>
<td>Send a Wake On LAN command before attempting to deliver changes to update settings. Hosts must meet all Wake On LAN requirements. See How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN on page 134.</td>
</tr>
</tbody>
</table>

4. Click Apply Settings.

How to Change Update Settings for Multiple Hosts

**Remember**: A Premier or Insight subscription is required to use this feature.
1. In LogMeIn Central, go to the Updates page.
2. Click the checkbox for each computer or group of computers you want to manage.
3. Click Change settings.
4. Change how Windows installs updates. Some settings may be managed by the system administrator. See Windows documentation for details. All settings are the same as in Windows.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important updates</td>
<td>Select how important updates are downloaded and installed.</td>
</tr>
<tr>
<td>Software to update</td>
<td>Choose to install either Windows updates only or Microsoft product updates along with Windows updates (for example, Microsoft Office updates).</td>
</tr>
</tbody>
</table>

**Tip:** Don’t want to change a particular setting across multiple computers? Choose Keep current setting of the computers to leave a setting unchanged.

You will be notified whenever there is a host to which settings cannot be applied. Click the X computers link to see which computers were excluded.

5. To display delivery options, click Change next to How the settings above are delivered to hosts. These settings are not applied to hosts, but rather tell LogMeIn how to deliver the Updates-related settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempt to connect to computers for</td>
<td>LogMeIn will attempt to change how Windows installs updates for this period of time.</td>
</tr>
<tr>
<td>Wake up computers</td>
<td>Send a Wake On LAN command before attempting to deliver changes to update settings. Hosts must meet all Wake On LAN requirements. See How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN on page 134.</td>
</tr>
</tbody>
</table>

6. Click Apply Settings.

**How to Choose Which Updates to Apply**

You can choose which Microsoft and Windows updates to install to your hosts.

**Remember:** A Premier or Insight subscription is required to use this feature.

1. In LogMeIn Central, go to the Updates page.
2. Select the computers you want to update.
3. Click Apply updates.
   - The list of available updates for the selected hosts is displayed on two tabs (Important and Optional).
4. Select the updates that you want to install.
5. To select whether hosts should be restarted after installing Windows updates, choose **Restart computers if required to install the updates**. Hosts are only restarted if at least one of the installed updates require reboot.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediately after updates are applied</td>
<td>Select this option to restart the host when updates are downloaded and installed.</td>
</tr>
<tr>
<td>After updates are applied, at this time</td>
<td>Select this option to restart the host at a specific time. Optionally, select <strong>on this date</strong> to specify a date for rebooting the host.</td>
</tr>
<tr>
<td>Additional delay</td>
<td>Select this option to delay automatic restart. This delay benefits users who may be logged in to the host. When a user is present, a notification is shown regarding the pending reboot. Restart settings cannot be changed during the delay period.</td>
</tr>
</tbody>
</table>

6. To display delivery options, click **Change** next to **How the settings above are delivered to hosts**. These settings are not applied to hosts, but rather tell LogMeIn how to deliver the Updates-related settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempt to connect to computers for</td>
<td>LogMeIn will attempt to change how Windows installs updates for this period of time.</td>
</tr>
<tr>
<td>Wake up computers</td>
<td>Send a Wake On LAN command before attempting to deliver changes to update settings. Hosts must meet all Wake On LAN requirements. See <em>How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN</em> on page 134.</td>
</tr>
</tbody>
</table>

7. Click **Apply updates**.

   The updates are applied to any host that is online. For any host that is offline, the updates are applied when the host next comes online.

---

**How to Schedule Restart for Hosts after Installing Updates**

You can set your hosts to automatically reboot if an installed update requires restart.

*Remember:* A Premier or Insight subscription is required to use this feature.

*Important:* Automatic restart is only available when applying updates manually.

1. In LogMeIn Central, from the **Updates > Manage** page, select the computers you want to update.
   The available updates page is displayed.

2. Click **Change settings**.
   The **Update settings** page is displayed.

3. Click the link next to **Available updates for this computer**.

4. Select the updates from the list you want to be installed.

5. Select **Restart computers if required to install the updates**.
   Configure when the computer should be restarted.
### How to View Update History

Use the History tab to track the status of applied updates and changes made to update settings.

**Remember:** A Premier or Insight subscription is required to use this feature.

1. In LogMeIn Central, go to the **Updates > History** page.
2. Choose what you want to view.
   - Click **Running** to view updates or configuration changes that are in the process of being applied.
   - Click any other option to view updates or configuration changes that have already been applied.
3. Click **View** next to any item to see its details.

### Managing Third-Party Applications

With Application Updates you can control how third-party applications are installed on all supported Windows hosts in your account.

**Remember:** A Premier or Security subscription is required to use this feature.

Available on Windows hosts only.

For each computer covered by your Central Premier subscription, you can do the following:

- View list of pending application updates
- Install application updates
- View update settings
- Change update settings on a single host
- Change update settings on multiple hosts

Required host software: LogMeIn host software for Windows 4.1.0.9768 or newer.

**Who can use this feature?** Application Update is available to any Account Holder of a LogMeIn Central Premier subscription and to users in a Premier account with the following permissions: Application update management.
How to Activate Application Updates
Select the host computers for which you want to activate Application Updates.

Windows hosts only.

1. In LogMeIn Central, go to Updates > Applications.
2. Select host computers.
3. Click Change Settings.
   The Change Settings menu is displayed.
4. Select Manual or Automatic.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Information on available updates is collected but not installed.</td>
</tr>
<tr>
<td>Automatic</td>
<td>All available updates are installed.</td>
</tr>
</tbody>
</table>

**Note:** The software scans for updates between 12am and 6am or when the host is turned on after those times.

The End-User License Agreement pop-up appears.

5. Select the I accept all third-party End-User License Agreements and Terms of Service/Conditions that may be required to complete application update checkbox and click Accept.

The Updates > Applications screen is displayed.

During installation, you may encounter the following errors

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to download the Application Updater.</td>
<td>A third-party software or firewall is blocking the installation. See LogMeIn and Firewalls on page 22</td>
</tr>
<tr>
<td>Unable to extract the Application Updater.</td>
<td>A third-party software or firewall is blocking the installation. See LogMeIn and Firewalls on page 22</td>
</tr>
</tbody>
</table>

How to Update Third-Party Applications on a Single Host
Choose how applications are updated on the host.

Windows hosts only.

1. In LogMeIn Central, go to Updates > Applications page.
   The Updates > Applications page is displayed.
2. Select the host you want to update.
3. Click Apply Updates.
   The Apply updates page is displayed.
4. Select the applications you want to update.
5. Click Apply updates.
   A notification appears in the Updates > Applications page.
The updates are applied to any host that is online. For any host that is offline, the updates are applied when the host next comes online.

**How to Update Third-Party Applications on Multiple Hosts**

Apply application updates on multiple hosts.

- Available on Windows hosts only.

1. In LogMeIn Central, go to **Updates > Applications** page.
   
   The **Updates > Applications** page is displayed.

2. Select the hosts you want to update.

3. Click **Apply Updates**.
   
   The **Apply updates** page is displayed.

4. Select the applications you want to update.

   **Note:** LogMeIn Central detects every application with an available update. If multiple versions of an application are detected, each is displayed with its relevant version number.

5. Click **Apply updates**.
   
   A notification appears in the **Updates > Applications** page.

The updates are applied to any host that is online. For any host that is offline, the updates are applied when the host next comes online.

**Troubleshooting Application Updates**

How to deal with common issues related to Application Updates.

**Common Error Messages**

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to download the Application Updater.</td>
<td>A third-party software or firewall is blocking the installation. See LogMeIn and Firewalls on page 22</td>
</tr>
<tr>
<td>Unable to extract the Application Updater.</td>
<td>A third-party software or firewall is blocking the installation. See LogMeIn and Firewalls on page 22</td>
</tr>
</tbody>
</table>

**Disabling the Application Updater**

1. In LogMeIn Central, go to **Updates > Applications**.

2. Select the host computers you want to update.

3. Click **Change Settings**.
   
   The **Change Settings** menu is displayed.

4. Select **Disabled**.

5. Click **Apply updates**.

**How to View Update History**

Use the History tab to track the status of applied updates and changes made to update settings.
Remember: A Premier or Insight subscription is required to use this feature.

1. In LogMeIn Central, go to the **Updates > History** page.
2. Choose what you want to view.
   - Click **Running** to view updates or configuration changes that are in the process of being applied.
   - Click any other option to view updates or configuration changes that have already been applied.
3. Click **View** next to any item to see its details.

### Antivirus

Monitor anti-virus software running on LogMeIn host computers. Manage supported anti-virus software (Premier only).

**At a glance**

For each computer covered by your subscription, you can do the following:
- Monitor anti-virus status on the Computers list
- View detailed anti-virus information for each supported host
- Manage supported anti-virus software (Premier and Security only)
- Install and activate Kaspersky Endpoint Security on Windows hosts (Premier and Security only)
- Install and activate LogMeIn Antivirus on Windows hosts (Premier and Security only)

**Note:** LogMeIn only displays information on viruses that your anti-virus software is able to detect. It does not display information about malware and spyware.

**Who can use this feature?** All subscription levels are able to view host anti-virus status. Anti-virus management options are available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Security</td>
<td>• Anti-virus Management</td>
</tr>
</tbody>
</table>

**Required LogMeIn host software**

- Windows: LogMeIn host version 4.1.1868 or higher
- Mac: LogMeIn host version 4.1.0.5673 or higher

**Supported anti-virus software**

<table>
<thead>
<tr>
<th>Support level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full support</td>
<td>For anti-virus software that is fully supported:</td>
</tr>
<tr>
<td></td>
<td>• LogMeIn can read all relevant information from the anti-virus software installed on the host</td>
</tr>
<tr>
<td></td>
<td>• When virus definition was last updated</td>
</tr>
<tr>
<td></td>
<td>• Threat log</td>
</tr>
<tr>
<td></td>
<td>• Host's real-time protection setting</td>
</tr>
<tr>
<td>Support level</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• LogMeIn Central Premier and Security subscribers can do the following:</td>
</tr>
<tr>
<td></td>
<td>• Run commands on the host to manage its anti-virus software</td>
</tr>
<tr>
<td></td>
<td>• Enable real-time protection</td>
</tr>
<tr>
<td></td>
<td>• Check for the latest virus definition</td>
</tr>
<tr>
<td></td>
<td>• Run a full scan on the host</td>
</tr>
<tr>
<td>Partial support</td>
<td>For anti-virus software that is partially supported:</td>
</tr>
<tr>
<td></td>
<td>• LogMeIn can read all relevant information from the anti-virus software installed on the host</td>
</tr>
<tr>
<td></td>
<td>• When virus definition was last updated</td>
</tr>
<tr>
<td></td>
<td>• Host's real-time protection setting</td>
</tr>
<tr>
<td></td>
<td>• LogMeIn Central Premier and Security subscribers <em>may</em> be able to do the following:</td>
</tr>
<tr>
<td></td>
<td>• Run commands on the host to manage its anti-virus software</td>
</tr>
<tr>
<td></td>
<td>• Enable real-time protection</td>
</tr>
<tr>
<td></td>
<td>• Threat log</td>
</tr>
<tr>
<td></td>
<td>• Check for the latest virus definition</td>
</tr>
<tr>
<td></td>
<td>• Run a full scan on the host</td>
</tr>
<tr>
<td>Minimal support</td>
<td>LogMeIn can only read whether or not the virus definition is up-to-date.</td>
</tr>
</tbody>
</table>

**Viewing Anti-virus Status and Details**

To view the anti-virus status of your hosts, go to the *Computers* page and select *Detail view*.

In the *Anti-virus* column, color coded icons indicate the status of each host.

![Tip: ](image) Don't see the *Anti-virus* column? Click the column selector at the top-right of your computer list and choose *Anti-virus*.

**Status indicator icons:**

- 🔄 Host requires immediate attention because either *Real-time Protection* is turned off or there is no anti-virus software installed.
- 🔴 Host requires attention because there is an issue with the anti-virus software. For example, its virus definition is out of date or there are unacknowledged threats.
- 🟡 The anti-virus software is up and running and the host is not infected.
- 🂹 There is not enough information about the anti-virus software running on the host, but the available details do not suggest any problem with the host. Make sure that you have the latest LogMeIn host version, your computer is online, and the anti-virus software is enabled and supported by LogMeIn.

**View details for an individual host**

To view details for any individual computer, click the icon in the Anti-virus column.
The following details are displayed on the **Host Properties > Anti-virus** tab.

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV software name</td>
<td>Name of the supported anti-virus software running on the host.</td>
</tr>
<tr>
<td>Virus definition up-to-date</td>
<td>Displays whether the anti-virus software has the latest virus definition database. Click <strong>Update now</strong> to download the latest virus definition file.</td>
</tr>
<tr>
<td>Virus definition version</td>
<td>The version of the database containing information on viruses.</td>
</tr>
<tr>
<td>Real-time Protection</td>
<td>Displays whether the anti-virus software is protecting the host in real time (<strong>On</strong>) or not (<strong>Off</strong>). When an anti-virus software is running in real-time mode, it can filter Internet traffic for viruses and scan files before you open or run them. <strong>Note:</strong> Even if real-time protection is turned off, the anti-virus software may periodically scan for viruses.</td>
</tr>
<tr>
<td>Last full scan time</td>
<td>Time of the last full scan. Click <strong>Run full scan now</strong> to use the installed anti-virus software to scan the computer for viruses.</td>
</tr>
<tr>
<td>Threat Log</td>
<td>A list of viruses detected by the anti-virus software. Click <strong>Acknowledge all threats</strong> to acknowledge the list of viruses. You cannot acknowledge a single threat. Viruses are not removed on the host when you acknowledge threats.</td>
</tr>
</tbody>
</table>

**View details for all hosts (Premier only)**

**Premium** subscribers can click **Anti-virus** on the left to view a table summarizing anti-virus details. The following information is displayed.

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Status indicator icons:</td>
</tr>
<tr>
<td></td>
<td>* Host requires immediate attention because either <strong>Real-time Protection</strong> is turned off or there is no anti-virus software installed.</td>
</tr>
<tr>
<td></td>
<td>* Host requires attention because there is an issue with the anti-virus software. For example, its virus definition is out of date or there are unacknowledged threats.</td>
</tr>
<tr>
<td></td>
<td>* The anti-virus software is up and running and the host is not infected.</td>
</tr>
<tr>
<td></td>
<td>* There is not enough information about the anti-virus software running on the host, but the available details do not suggest any problem with the host. Make sure that you run the latest LogMeIn host version, your computer is online, and the anti-virus software is enabled and supported by LogMeIn.</td>
</tr>
<tr>
<td>Anti-virus software</td>
<td>Name of the supported anti-virus software running on the host.</td>
</tr>
<tr>
<td>Detail</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Real-time Protection</td>
<td>Displays whether the anti-virus software is protecting the host in real time (On) or not (Off). When an anti-virus software is running in real-time mode, it can filter Internet traffic for viruses and scan files before you open or run them. Note: Even if real-time protection is turned off, the anti-virus software may periodically scan for viruses.</td>
</tr>
<tr>
<td>Virus definition</td>
<td>Displays whether the anti-virus software has the latest virus definition database. Click Update now to download the latest virus definition file.</td>
</tr>
<tr>
<td>Virus definition version</td>
<td>The version of the database containing information on viruses.</td>
</tr>
<tr>
<td>Last full scan time</td>
<td>Time of the last full scan. Click Run full scan now to use the installed anti-virus software to scan the computer for viruses.</td>
</tr>
<tr>
<td>Threats</td>
<td>A list of viruses detected by the anti-virus software. Click Acknowledge all threats to acknowledge the list of viruses. You cannot acknowledge a single threat. Viruses are not removed on the host when you acknowledge threats.</td>
</tr>
</tbody>
</table>

**Computer Health**

Health is an indicator shown on the Computers list.

Health indicator icons are color coded and represent the single most serious problem detected on a host. They are shown in the Health column in Detail view.

Health is determined by Windows updates, anti-virus settings, and alerts

Health indicator icons:

- 🔴 The host requires reboot to finish the installation of important Windows updates or the Windows updates service is not running on the host. There is a critical issue with the anti-virus software.
- ⚠ There is an issue with the anti-virus software, there are unacknowledged alerts, or the installation of important Windows updates is pending on the host.
- 🟢 The host is running the latest Windows updates, the most up-to-date virus definition, and there are no unacknowledged alerts.
- 🟢 Either you must update the host to see its full health report, or the anti-virus software is not fully supported.

**LogMeIn Antivirus**

Premier and Security subscribers can install and activate LogMeIn Antivirus on Windows computers in their LogMeIn Central account.

Once you have installed LogMeIn Antivirus to your computers, you can manage anti-virus status, updates, and more from within the Anti-virus dashboard in LogMeIn Central.
What is LogMeIn Antivirus

LogMeIn Antivirus uses real-time information to proactively identify and protect against unique, sophisticated threats.

The following features are included in LogMeIn Antivirus

• File Scan
• Behavioral Scan
• Traffic Scan
• Exclusion list
• Silent install

System Requirements for LogMeIn Antivirus

• Windows 7 or newer (including 64-bit)
• LogMeIn host version version 12572 or higher

Installing LogMeIn Antivirus

How to install and activate LogMeIn Antivirus on any Windows host.

Who can use this feature? The ability to activate and manage LogMeIn Antivirus is available to any Account Holder of a LogMeIn Central Premier or Security subscription and to users with the following permissions: Enable LogMeIn Central and Anti-Virus Management.

Important: To ensure optimal performance, all other anti-virus software, except Kaspersky Endpoint Security for Business, must be manually removed from the host.

1. In LogMeIn Central, go to Antivirus.
2. Select the checkbox for each computer you want to work with.
   The Actions button is activated at the top of the page. Required host software: On Windows, version 12572 or higher.
3. Click Actions > Install LogMeIn Antivirus.
   • For each host that is online with no conflicting anti-virus software installed, LogMeIn Antivirus is installed and activated.
   • If conflicting anti-virus software is detected, you must remove it before continuing.
   • If offline hosts are detected, you should bring them online before continuing.

   The host-side end user does not need to take action to complete the installation. Host-side users are not interrupted.

LogMeIn Antivirus remains active as long as a host remains attached to your LogMeIn Central account. Activation renews automatically every 30 days.

As with other LogMeIn Central features, if you have trouble with the LogMeIn Anti-virus installation, please contact LogMeIn Customer Support.

Removing LogMeIn Antivirus

LogMeIn Antivirus is a separate software and not removed when you uninstall the LogMeIn host software from a computer.

When you remove LogMeIn or detach a host from your account, LogMeIn Antivirus remains installed, but does not renew. LogMeIn Antivirus eventually notifies the host-side user that the service is no longer active.
To remove LogMeIn Antivirus from a host, you must manually uninstall it.

**Running a Scan with LogMeIn Antivirus**

Scan your computer for potential threats and malware.

1. In the taskbar menu, click the LogMeIn Antivirus icon. The LogMeIn Antivirus software is displayed.
2. Click the scan icon .
3. Choose from the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Scan</td>
<td>Scans major files and folders on the computer except hidden files and system files.</td>
</tr>
<tr>
<td>Full Scan</td>
<td>Scans all files on your computer.</td>
</tr>
<tr>
<td>Custom Scan</td>
<td>Allows you to customise what files and folders are scanned and when the scan runs. For more information, see <em>Creating a Custom Scan in LogMeIn Antivirus</em> on page 76.</td>
</tr>
</tbody>
</table>

The Antivirus starts scanning your system and creates a report.

**Creating a Custom Scan in LogMeIn Antivirus**

LogMeIn antivirus lets you create a customized antivirus scan

1. In the taskbar menu, click the LogMeIn Antivirus icon. The LogMeIn Antivirus software is displayed.
2. Click the scan icon . The Scan Tasks menu appears.
3. Choose New Custom Scan. The Custom Scan menu appears.
4. Under Target, select what drives, folders and files you want to scan.
5. Under Scan Options, select a scan level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggressive</td>
<td>Configures the scan settings for maximum protection against any type of malware.</td>
</tr>
<tr>
<td>Normal</td>
<td>Provides optimum balance between security and performance.</td>
</tr>
<tr>
<td>Permissive</td>
<td>Provides basic security but maximum performance.</td>
</tr>
<tr>
<td>Custom</td>
<td>Define the granularity of your scan and actions to take.</td>
</tr>
</tbody>
</table>

6. If running the scan is not important, check Run task with low priority.
7. Click Start Scan.
   - Optional: Under Save favourite scan, name and save scan settings for future use.
Applying Filters to LogMeIn Antivirus
The list showing all antivirus related events can be filtered by specific categories.

1. In the taskbar menu, click the LogMeIn Antivirus icon. The LogMeIn Antivirus software is displayed.

2. Click the Filters icon. The Filters menu is displayed.

3. Select what category you want to filter by.

<table>
<thead>
<tr>
<th>Name</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td>![Icon]</td>
<td>Settings related to account and licensing.</td>
</tr>
<tr>
<td>Antimalware</td>
<td>![Icon]</td>
<td>Notifications related to recent scans.</td>
</tr>
<tr>
<td>Update</td>
<td>![Icon]</td>
<td>Updates for the software.</td>
</tr>
<tr>
<td>Content Control</td>
<td>![Icon]</td>
<td>What features/modules have been enabled/disabled.</td>
</tr>
<tr>
<td>Device Control</td>
<td>![Icon]</td>
<td>Not available right now.</td>
</tr>
</tbody>
</table>

Creating a Policy for LogMeIn Antivirus
You can create a policy containing settings for LogMeIn Antivirus that you can apply to multiple hosts.

1. In LogMeIn Central, Go to Antivirus > LogMeIn Antivirus policy.
2. Choose the policy you want to edit or create a new one.
3. Select whether or not to enable Antimalware.
4. Under Scan profile, choose from the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggressive</td>
<td>Configures the scan settings for maximum protection against any type of malware.</td>
</tr>
<tr>
<td>Normal</td>
<td>Provides optimum balance between security and performance.</td>
</tr>
<tr>
<td>Permissive</td>
<td>Provides basic security but maximum performance.</td>
</tr>
</tbody>
</table>

5. Under Scheduled scans, choose from the following and set the scan schedule:
### Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick scan</td>
<td>Scans major files and folders on the computer except hidden files and system files.</td>
</tr>
<tr>
<td>Full scan</td>
<td>Scans all files on your computer.</td>
</tr>
</tbody>
</table>

6. Under **Exclusion list**, add any files or file types you do not want scanned.
7. Under **Device scan**, select whether or not to enable **Scan USB devices**.
8. Under **Extra settings**, you can set the following:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent mode</td>
<td>Run LogMeIn Antivirus in the background to prevent host-side users from accessing AV settings.</td>
</tr>
<tr>
<td>Antiphishing</td>
<td>Block known phishing and fraudulent websites when browsing.</td>
</tr>
<tr>
<td>Traffic scan</td>
<td>Scan HTTP, POP3 and SMTP traffic for viruses.</td>
</tr>
<tr>
<td>Block USB storage devices</td>
<td>Prevents USB devices from being used.</td>
</tr>
</tbody>
</table>

9. Click **Create** or **Save**.

### Can I See a List of Websites Blocked by the Antiphishing Module?

The Content Control filters allow you to see what sites are blocked.

1. On the host, in the taskbar, right-click on LogMeIn Antivirus. ![LogMeIn Antivirus icon]
2. Click **Show**. The LogMeIn Antivirus menu is displayed.
3. Click **Filter**.
4. Filter entries by Content Control.

Filtered websites are shown in the application's display.

### Access Control for Mobile Devices

Use LogMeIn Central to see who is using specific iPads or iPhones to access your LogMeIn computers.

**What can you do?**

LogMeIn Central users with **User management** permission can do the following on the **Configuration > Devices** page:

- View a list of iOS devices used to access computers in your account
- View a list of LogMeIn users who accessed your computers with a given mobile device
- Check the properties of the devices used to access your computers
• Handle lost or stolen devices by remotely wiping stored credentials

**Requirements**

• You must have **Enable LogMeIn Central** and **User management** permissions
• People accessing your computers must be using **LogMeIn for iOS**

**How iPads and iPhones are Added to the Devices List**

Devices are added automatically to the **Configuration > Devices** page when they first access one of your computers from a supported mobile device.

• You cannot add devices using a PC or Mac; the procedure must be initiated on an iOS device
• The individual using the device must be a user of your LogMeIn account with access rights to at least one computer in your account

**Tip:** Users with their own personal LogMeIn profile must ensure they are using their profile under your account.

**How to Clear Saved Host Credentials from a Device**

You can remotely delete all saved host login credentials from a mobile device.

1. In LogMeIn Central, go to the **Configuration > Devices** menu.
2. Click **Wipe Credentials** next to the device.
3. Click **OK**.

   The server-side key used to encrypt credentials on the client is deleted. The change is applied immediately, even if the client is offline.

Any user connecting from the device to a host computer will be prompted to enter a host user name and password.

**Important:** The user who is currently logged in will not be logged out, but they will be unable to start sessions to your hosts without logging in again.

**How to Remove Devices from the Devices List**

You can remove devices from the **Devices** list.

1. In LogMeIn Central, go to the **Configuration > Devices** menu.
2. Click **Remove from list** next to the device.

**Important:** This action does not change a user's access rights. To prevent a user from accessing your computers, change their access rights under **Users > Manage > edit permissions > Group/Computer Permission**.

3. When prompted to confirm removal of the device, select **Wipe all credentials on device** to clear any user names and passwords saved on the device. This helps prevents unauthorized access to your computers.
4. Click **OK**.

   The device is removed from the list.
I removed a device from the list, but it keeps appearing! Even if you remove a device from the list, it reappears when a user successfully uses it to access one of your computers.

Remember: To prevent a user from accessing your computers, change their access rights under Users.

How to View Device Users and Properties
You can view the list of LogMeIn users who accessed your computers with a given mobile device and check the device’s properties.

1. In LogMeIn Central, go to the Configuration > Devices menu.
2. Choose what information you want to see:
   - To view the list of LogMeIn users who accessed your hosts with a mobile device, click View list of Users next to the mobile device.
   - To view the name, type, and basic technical information about a device, click Properties next to the mobile device.
3. Click OK to close the dialog.

Remember: To prevent a user from accessing your computers, change their access rights under Users.

Deploying Host Preferences
Deploy settings to Windows hosts as part of a Host Preference Package.

Access Control
Deployable Host Preferences for controlling access to host computers.

Allow Full Control to Administrators (Host Preferences)
Deploy settings giving full control to users with an administrator account on the host.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

This option is selected by default (admin rights granted).

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
d) Click **Save**.

2. Under **Category**, select **Access Control**.
3. Select **Allow full control to administrators**.
4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.
5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Edit** or **Click here to assign** next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click **Save**.

### Allow Login Credentials to be Saved (Host Preferences)

Deploy settings allowing LogMeIn users with permission to use automatic authentication to securely save their username and password to the client when connecting to a host.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The **Host Preference Packages** feature is available to any Account Holder of a LogMeIn Central **Premier or Plus** subscription and to users in a **Premier or Plus** account with the **Configuration Management** permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

This option is selected by default (host credentials can be saved). Revoke this permission to prevent LogMeIn users from saving their credentials on the client when connecting to a host.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Add Package**.
      The **New Host Preference Package** page is displayed.
   c) Name your new Host Preference Package.
   d) Click **Save**.
2. Under **Category**, select **Access Control**.
3. Select **Allow login credentials to be saved**.
4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.
5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Edit** or **Click here to assign** next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click **Save**.

### Allow User Name to be Saved in a Cookie (Host Preferences)

Deploy settings allowing client-side users to save their Windows user name in a browser cookie. As a result, users will only need to enter a password to authenticate when connecting from the same client.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The **Host Preference Packages** feature is available to any Account Holder of a LogMeIn Central **Premier or Plus** subscription and to users in a **Premier or Plus** account with the **Configuration Management** permission.
Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

This option is selected by default (cookies can be saved). Revoke this permission to force users to manually enter a Windows user name when connecting.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Access Control.

3. Select Save user name in a cookie.

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

Hide Domain Names on Login Screen (Host Preferences)

Use a Host Preference Package to deploy settings that clear the list of active domains on the host authentication dialog box. This provides an extra layer of security by forcing the client-side user to know the exact name of the chosen domain.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

This option is not selected by default.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Advanced.


4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.
IP Address Lockout
Deployable Host Preferences for IP address lockout.

Deploy a Denial of Service Attack Blocker (Host Preferences)
Use the Denial of Service filter as a precaution against unwanted intruders who slow your host machine by continuously requesting the same service.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select IP Address Lockout.

3. Under Denial of Service attack blocker you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Use the Denial of Service filter as a precaution against unwanted intruders who slow your host machine by continuously requesting the same service.</td>
</tr>
<tr>
<td>Number of Invalid HTTP requests allowed</td>
<td>Specify the number of invalid requests to allow before the offending IP address is locked out.</td>
</tr>
<tr>
<td>Reset invalid attempt counter after</td>
<td>After this much time has elapsed, the invalid attempt count of the offending IP address will be reset to zero.</td>
</tr>
<tr>
<td>Keep attacker blocked for</td>
<td>All attempted connections from an offending IP address will be rejected for the amount of time specified.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

Deploy an Authentication Attack Blocker (Host Preferences)
Use the Authentication Attack Blocker to lock out those who try to get past your host logon screen without authorization.

Host Preference Packages can only be applied to LogMeIn Windows hosts.
Who can use this feature? The **Host Preference Packages** feature is available to any Account Holder of a LogMeIn Central **Premier or Plus** subscription and to users in a **Premier or Plus** account with the **Configuration Management** permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Add Package**.
      The **New Host Preference Package** page is displayed.
   c) Name your new Host Preference Package.
   d) Click **Save**.

2. Under **Category**, select **IP Address Lockout**.

3. Under **Authentication attack blocker** you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Use the Authentication attack blocker to lock out those who try to get past your host logon screen without authorization.</td>
</tr>
<tr>
<td>Number of Invalid attempts allowed</td>
<td>Specify the number of invalid authentication attempts to allow before the offending IP address is locked out.</td>
</tr>
<tr>
<td>Reset invalid attempt counter after</td>
<td>After this much time has elapsed, the invalid attempt count of the offending IP address will be reset to zero.</td>
</tr>
<tr>
<td>Keep attacker blocked for</td>
<td>All attempted connections from an offending IP address will be rejected for the amount of time specified.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Edit** or **Click here to assign** next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click **Save**.
a) In LogMeIn Central, go to the Configuration > Host Preferences page.
b) Click Add Package.
   The New Host Preference Package page is displayed.
c) Name your new Host Preference Package.
d) Click Save.

2. Under Category, select Appearance.

3. Under General Settings you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display CPU and memory information above the menu</td>
<td>Enable the Java applet that shows current processor and memory utilization in the top frame of the LogMeIn host interface in Dashboard view.</td>
</tr>
<tr>
<td>Default number of items per page for long lists</td>
<td>Set the number of items to be shown per page for lists (such as event logs, the services list). Most lists allow you to change the number of items shown.</td>
</tr>
</tbody>
</table>

4. Under Systray Settings you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the LogMeIn icon in the System Tray</td>
<td>Clear this option to hide the LogMeIn icon from the host system tray. The host user will be able to open LogMeIn using the Windows Start menu.</td>
</tr>
<tr>
<td>Disable LogMeIn notification messages</td>
<td>Suppress all LogMeIn messages communicated from the system tray. This is useful when messages could disrupt the end-user experience, such as on a kiosk or other public display.</td>
</tr>
</tbody>
</table>

5. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

6. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

**Network**

Deployable Host Preferences for network and connection settings.

**Deploy Preferences for Network and Connection Settings (Host Preferences)**

Modify how LogMeIn interacts with your local network and manages its connection.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
a) In LogMeIn Central, go to the Configuration > Host Preferences page.
b) Click Add Package.
   The New Host Preference Package page is displayed.
c) Name your new Host Preference Package.
d) Click Save.

2. Under Category, select Network.

3. Under General Settings you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of servicing threads</td>
<td>Specify the maximum number of threads the host can spawn to service client connections. This feature is useful if you have multiple LogMeIn users making simultaneous Dashboard, Main Menu, or File Manager connections to an important server. Remember: Only one Remote Control session is allowed at a time. Restart the LogMeIn service on the host to implement the change. The default value (50) should be enough to handle up to 10 concurrent sessions to a single host. Additional incoming sockets will be rejected and a log entry will report Socket refused, no more than 50 connections allowed.</td>
</tr>
<tr>
<td>Idle time allowed</td>
<td>Set the amount of time that can pass without activity in LogMeIn before a remote control session is disconnected.</td>
</tr>
<tr>
<td>File Transfer Compression</td>
<td>Choose the compression level to apply to data transferred from the host during remote control, including files transferred using the File Manager feature.</td>
</tr>
<tr>
<td>Detect and download updates automatically</td>
<td>Select this option if you want LogMeIn to check for the latest version of the LogMeIn host software. The host user will be prompted to update if a new version is found.</td>
</tr>
<tr>
<td>Install downloaded updates when LogMeIn is idle</td>
<td>Select this option to ensure that LogMeIn updates are only installed when LogMeIn is not in use. This protects users from losing active sessions. LogMeIn must restart itself (but not the host computer) after applying a software update. If this is done while LogMeIn is busy (for example, during an active remote control session or while a file transfer is in progress) then the connection will be dropped during the restart.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

Log Settings
Deployable Host Preferences for logs and session recording.
**Set Behavior for LogMeIn's Logs (Host Preferences)**

Set LogMeIn’s log behavior.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The **Host Preference Packages** feature is available to any Account Holder of a LogMeIn Central **Premier** or **Plus** subscription and to users in a **Premier** or **Plus** account with the **Configuration Management** permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Add Package**.
      The **New Host Preference Package** page is displayed.
   c) Name your new Host Preference Package.
   d) Click **Save**.

2. Under **Category**, select **Log Settings**.

3. Under **General Settings** you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keep logs for this many days</strong></td>
<td>Enter the number of days for which you would like to store log files.</td>
</tr>
<tr>
<td><strong>Location of event logs</strong></td>
<td>Specify a folder on the host where log files are saved. Leave blank to use the default location: LogMeIn installation directory, typically C:\Program Files\LogMeIn.</td>
</tr>
<tr>
<td><strong>Enable debug-level logging</strong></td>
<td>Include Windows events in the LogMeIn.log file. This facilitates LogMeIn troubleshooting efforts.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Edit** or **Click here to assign** next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click **Save**.

**Record Remote Control Sessions (Host Preferences)**

Record and save remote control sessions to host computers.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The **Host Preference Packages** feature is available to any Account Holder of a LogMeIn Central **Premier** or **Plus** subscription and to users in a **Premier** or **Plus** account with the **Configuration Management** permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
b) Click Add Package. The New Host Preference Package page is displayed.
c) Name your new Host Preference Package.
d) Click Save.

2. Under Category, select Log Settings.
3. Under Screen Recording you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record screen content of Remote Control sessions</td>
<td>Record and save all remote control sessions with the host. Sessions will automatically be recorded and saved to the defined location. No other action is required.</td>
</tr>
<tr>
<td>Automatically convert to .AVI format</td>
<td>Save session recordings as AVI files; otherwise files are saved as RCREC, a LogMeIn proprietary format. File size is similar for both recording types.</td>
</tr>
</tbody>
</table>

**Tip:** To convert RCREC recordings manually, open LogMeIn on the host and go to Options > Preferences > Advanced Settings > Screen Recording > Convert RCREC Files to AVI.

<table>
<thead>
<tr>
<th>Location of video files</th>
<th>Specify a folder on the host where screen recordings are saved. Leave blank to use the default location: LogMeIn installation directory, typically C:\Program Files\LogMeIn\x86.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete old files if folder size exceeds</td>
<td>Automatically delete the oldest archived RCREC remote control recordings when the total size of all RCREC recordings in the Location of video files exceeds the defined value. AVI files are not counted toward the limit and will not be deleted.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.
5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

**Remote Control**

Deployable Host Preferences for remote control.

**Deploy Preferences for Remote Control (Host Preferences)**

Deploy settings to control various aspects of the remote control experience.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.
1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package. The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Remote Control.

3. Under General Settings you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Desktop Sharing</td>
<td>Allow the host-side user to invite others to access the host via the Desktop Sharing feature.</td>
</tr>
<tr>
<td>Use display accelerator</td>
<td>The display accelerator makes remote control sessions faster and less CPU-intensive. Clear this option to help resolve problems experienced while viewing video or while using DOS-based or graphic-intense applications during remote control (such as display black-out or host computer restart when trying to start remote control).</td>
</tr>
<tr>
<td>Disable wallpaper and user interface effects on host computer</td>
<td>Disable the host's desktop wallpaper and all user interface effects during remote control. User interface effects include transition effects (fade, scroll), shadows under menus, and trailing effects while dragging windows.</td>
</tr>
<tr>
<td>Automatic clipboard transfer maximum size</td>
<td>Enter the maximum number of kilobytes of data that can be transferred between host and client using clipboard synchronization.</td>
</tr>
<tr>
<td></td>
<td><strong>Remember:</strong> Sync Clipboard must be activated on the remote control toolbar to copy and paste between host and client during remote control.</td>
</tr>
<tr>
<td>Control-Alt-Del hotkey combination</td>
<td>Choose the keyboard shortcut to be used for sending the Ctrl-Alt-Del command to the host during remote control</td>
</tr>
<tr>
<td>Default color quality</td>
<td>Remote Control sessions will start in the selected color quality mode. HD requires the highest network bandwidth. If you are unsure of available bandwidth, select Auto. To allow the host user to set color quality himself, select Host-user defined.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

**Deploy Security Preferences for Remote Control (Host Preferences)**
Deploy settings that help secure the remote control experience.

Host Preference Packages can only be applied to LogMeIn Windows hosts.
Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Remote Control.

3. Under Security you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable host keyboard and mouse</td>
<td>Prevent anyone at the host from using the mouse or keyboard during remote control. Only the client user will be able to input data.</td>
</tr>
<tr>
<td>Blank the host's monitor</td>
<td>Prevent anyone at the host from seeing your work during remote control. Anyone at the host device will see a blank screen on the physical monitor while the remote session is active.</td>
</tr>
<tr>
<td>Lock when connection has been lost</td>
<td>Force the host's operating system to lock when the client disconnects during remote control.</td>
</tr>
<tr>
<td>Lock when connection has been timed out</td>
<td>Force the host's operating system to lock when the client times out during remote control.</td>
</tr>
<tr>
<td>Always lock the host after remote control</td>
<td>Force the host's operating system to always lock when a remote control session is terminated.</td>
</tr>
<tr>
<td>Allow one-click login to desktop</td>
<td>Make it easier to unlock a host when connecting via remote control. LogMeIn will prompt you to send your saved Windows credentials with a single click. Clear this option to force anyone accessing the host to manually authenticate by entering a valid username and password.</td>
</tr>
<tr>
<td>Local keyboard &amp; mouse takes precedence over remote</td>
<td>Select this option if you want all keyboard and mouse actions on the client device to be processed before actions on the host. That is, the actions of the person running the remote control session will be processed before the actions of the person sitting at the computer being controlled.</td>
</tr>
<tr>
<td>Disable Drag &amp; Drop during Remote Control</td>
<td>Prevent users from dragging and dropping files between host and client.</td>
</tr>
</tbody>
</table>

Note: Once you have enabled this feature and started a remote session, you will be prompted to install a DPMS (Display Power Management Services) driver. Not all monitors, video cards, motherboards, or BIOS support DPMS. Check with your hardware vendor if you experience problems with the DPMS driver.
Add Visual and Audio Notifications when Taking Remote Control (Host Preferences)
Add audible and visual cues to the remote control experience.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Remote Control.
3. Under Visible and Audible Notification you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beep when the remote control session starts or ends</td>
<td>Set the host to emit a single beep when a remote control session is initiated or ended.</td>
</tr>
<tr>
<td>Beep continuously during remote control</td>
<td>Set the host to emit a beeping sound when it is being controlled remotely. Set the interval in the Beep Interval field.</td>
</tr>
<tr>
<td>Beep Interval</td>
<td>Enter the time period between notification beeps emitted while a host is being controlled remotely.</td>
</tr>
<tr>
<td>Flash Keyboard Indicator Lights</td>
<td>Make the host keyboard Number Lock, Caps Lock and Scroll Lock lights flash in sequence while a host is being controlled remotely.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.
5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.
Configure Host Side User’s Consent (Host Preferences)
Set how the host responds to remote control requests.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Remote Control.

3. Under Host Side User’s Consent you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request consent from host side user</td>
<td>Force the host user to permit or deny access when a client user attempts to open a remote control session. Clear this option to allow a client user to initiate a remote control session without asking for permission from the host user.</td>
</tr>
<tr>
<td>If user does not respond</td>
<td>Choose Start remote control if you want the remote control session to start even if the host user does not respond within the time set in the Time to wait for user’s consent field. Choose Reject request if you want the remote control session to be refused if the host user does not respond otherwise.</td>
</tr>
<tr>
<td>Time to wait for user’s consent</td>
<td>Enter the amount of time within which the host user must respond to the request for permission to initiate remote control. If this time expires, the setting in the If user does not respond field will be applied.</td>
</tr>
<tr>
<td>Request Message</td>
<td>This text will be presented to the host user in the remote control permission dialog box. The string %USER% will be the Computer Name of the host as set at the operating system level, plus the client user’s operating system account ID. The account LogMeInRemoteUser will be used on computers that have an empty administrator password.</td>
</tr>
<tr>
<td>Remote user has Full Control access rights to the host computer</td>
<td>Select this option to override the setting in the Request consent from host side user field. Users with Full Control or Remote Control &quot;D&quot; permission will not require the host user’s permission before initiating remote control. See also How to Specify User Access Rights on page 194.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
a) In LogMeIn Central, go to the Configuration > Host Preferences page.
b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
c) Choose computers and groups using the left and right arrows.
d) Click Save.

**Allow Remote Printing from a Host Computer (Host Preferences)**
Deploy settings to allow remote printing.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under **Category**, select Remote Control.

3. Under **Remote Printing** you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable remote printing</td>
<td>Allow the client-side user to print from the host to a printer connected to the client.</td>
</tr>
<tr>
<td>Force Bitmap Printing</td>
<td>Select this option if material printed using LogMeIn remote printing does not print properly (it is mirrored, has the wrong layout, has meaningless characters and content, etc.). Bitmap printing is slow, but reliable.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

**Allow Client-Side Drives to Connect to the Host (Host Preferences)**
Allow the client-side user to connect client-side drives to the host.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.
Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package. The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Remote Control.

3. Under Connecting Drives you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable connecting drives</td>
<td>Allow the client-side user to connect client-side drives to the host.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> To make the actual connection between host and client during the remote control session, click Options &gt; Connect Drives on the Remote Control toolbar.</td>
</tr>
<tr>
<td>Preferred drive letter on host for connected client drives</td>
<td>Choose the letter to be used on the host to signify drives connected from the client. If the chosen letter is unavailable, the next free letter will be used.</td>
</tr>
<tr>
<td>Allow client-side hard drives to connect to the host</td>
<td>Allow any hard drive on the client to connect to the host.</td>
</tr>
<tr>
<td>Allow client-side removable drives to connect to the host</td>
<td>Allow any removable drive connected to the client (such as a pen drive, digital camera, mp3 player, etc.) to be connected to the host.</td>
</tr>
<tr>
<td>Allow client-side network drives to connect to the host</td>
<td>Allow any network drive connected to the client to be connected to the host.</td>
</tr>
<tr>
<td>Directory format of client-side drives connected to the host</td>
<td>Description first: winxp32(C). Drive letter first: (C) winxp32.</td>
</tr>
<tr>
<td>Write-protect connected drives</td>
<td>Prevent client-side users from altering files on the host during remote control. All host files will be read-only to the remote user.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

**Allow Remote Sound from the Host Computer (Host Preferences)**

Allow sounds from the host to be played on the client.
Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Remote Control.

3. Under Remote Sound you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable remote sound</td>
<td>Allow sounds from the host to be played on the client.</td>
</tr>
<tr>
<td>Mute sound on host</td>
<td>Allow sounds from the host to be played on the client, but not on the host itself. This feature allows you to listen to sounds from the host without disturbing anyone who may be present at or near the host.</td>
</tr>
<tr>
<td>Encode quality</td>
<td>Select the quality level of the sound to be transferred from the host. High quality is recommended for high-speed connections only.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

Advanced
Additional Host Preferences that are deployable to a LogMeIn host.

Customize the Host Login Screen (Host Preferences)
Deploy custom branding and messaging that is shown to anyone making a connection to a host.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
b) Click **Add Package**.
   The **New Host Preference Package** page is displayed.
c) Name your new Host Preference Package.
d) Click **Save**.

2. Under **Category**, select **Access Control**.

3. Under **Customized Login Message** you have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Display a customized logo on the login screen</strong></td>
<td>Show a logo or other image to anyone making a connection to the host. The image saved as <code>customlogo.jpg</code> in the LogMeIn installation directory (usually <code>C:\Program Files\LogMeIn</code>) will be displayed on the LogMeIn login screen.</td>
</tr>
<tr>
<td><strong>Tip:</strong> You can push a file to multiple Windows computers using One2Many. See <strong>How to Distribute Files to Remote Hosts</strong> on page 54</td>
<td></td>
</tr>
<tr>
<td><strong>Display the following message on the login screen</strong></td>
<td>Enter the login screen message that anyone making a connection to the host will see.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Edit** or **Click here to assign** next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click **Save**.

---

**Disable HTML-based Remote Control (Host Preferences)**

Prevent users from using HTML based remote control.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The **Host Preference Packages** feature is available to any Account Holder of a LogMeIn Central **Premier or Plus** subscription and to users in a **Premier or Plus** account with the **Configuration Management** permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Add Package**.
      The **New Host Preference Package** page is displayed.
   c) Name your new Host Preference Package.
   d) Click **Save**.

2. Under **Category**, select **Advanced**.

3. Under **Remote control** select **Disable HTML-based remote control**.

4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.

5. Assign the Host Preference Package to computers or groups, as follows:
a) In LogMeIn Central, go to the Configuration > Host Preferences page.
b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
c) Choose computers and groups using the left and right arrows.
d) Click Save.

Disconnect Existing Remote Control Sessions from the Same User (Host Preferences)
Set the host to allow a new remote control connection from the Windows user who is already in session. The second remote control connection by the same Windows user will disconnect the existing session.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Advanced.

3. Under Remote control select Disconnect existing remote control session from the same user.

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

Disable HTTP Content Compression (Host Preferences)
Select this option if the client browser does not support HTTP compression.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.
2. Under **Category**, select **Advanced**.
3. Under **Network** select **Disable HTTP content compression**.
4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.
5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Edit** or **Click here to assign** next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click **Save**.

**Set the way LogMeIn Reports an Error (Host Preferences)**

Deploy settings that control how and when LMIGuardian.exe sends error notifications to LogMeIn when
the LogMeIn host shuts down due to an error.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

**Who can use this feature?** The **Host Preference Packages** feature is available to any Account Holder
of a LogMeIn Central **Premier or Plus** subscription and to users in a **Premier or Plus** account with the
**Configuration Management** permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows
hosts in your LogMeIn account.

LMIGuardian.exe is LogMeIn's error reporting component. It documents and records errors that occur
in the LogMeIn host software and allows error details to be sent directly to our development team for
analysis.

The Guardian does not gather or report any personal information.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Add Package**.
      The **New Host Preference Package** page is displayed.
   c) Name your new Host Preference Package.
   d) Click **Save**.
2. Under **Category**, select **Advanced**.
3. Under **Software error reporting > When LogMeIn shuts down due to an error** select one of the
   following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always send an error report</td>
<td>An error report will always be sent (no user action required).</td>
</tr>
<tr>
<td>Never send an error report</td>
<td>An error report will never be sent.</td>
</tr>
<tr>
<td>Ask the user what to do</td>
<td>The user will be prompted to send an error report and can choose to send the report or not.</td>
</tr>
</tbody>
</table>

4. Continue to add settings to the Host Preference Package. When ready, click **Finish and Save**.
5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the **Configuration > Host Preferences** page.
   b) Click **Edit** or **Click here to assign** next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click **Save**.
Set What Language the Host Software Uses (Host Preferences)
The LogMeIn host interface and messages will be displayed in this language. This setting has no impact on operating system settings.

Host Preference Packages can only be applied to LogMeIn Windows hosts.

Who can use this feature? The Host Preference Packages feature is available to any Account Holder of a LogMeIn Central Premier or Plus subscription and to users in a Premier or Plus account with the Configuration Management permission.

Host Preference Packages allow you to define and deploy preferences and security settings to Windows hosts in your LogMeIn account.

1. Create a Host Preference Package, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Add Package.
      The New Host Preference Package page is displayed.
   c) Name your new Host Preference Package.
   d) Click Save.

2. Under Category, select Advanced.

3. Under General Settings > Language select which language you want the LogMeIn host software to use.

4. Continue to add settings to the Host Preference Package. When ready, click Finish and Save.

5. Assign the Host Preference Package to computers or groups, as follows:
   a) In LogMeIn Central, go to the Configuration > Host Preferences page.
   b) Click Edit or Click here to assign next to the Host Preference Package you want to assign.
   c) Choose computers and groups using the left and right arrows.
   d) Click Save.

Managing Users

How to Add Users to Your LogMeIn Account

Invite others to access computers in your LogMeIn account.

Only LogMeIn Central users with User management permission can add users.


2. Log in to your account using your LogMeIn ID (email address) and password.
   The Computers page is displayed.

3. On the left menu, click Users > Manage.
   The Users page is displayed.

4. Click Add Users.
   The Invite users to access your computers page is displayed.

5. Enter the Email address of each user you want to invite.
   The address will be used to log in at LogMeIn.com.

Tip: Anyone with an email address can be added as a user. A LogMeIn account is not required in advance.
6. Optionally, add the new users to a User Group.
7. Select Grant All Permissions to enable all user permissions and allow access to all computers in the account. To specify which permissions a user can choose, see Specifying Permissions for Users and User Groups in your LogMeIn Account on page 106.
8. Click Send Invitation.

You can view the invitation email by clicking Preview Invitation Email.

The invited users are sent an invitation email. They must open the invitation and click the invitation link. Any invitee who is not yet a LogMeIn user will be prompted to create a LogMeIn account. Any invitee who is already a LogMeIn user will have a new profile added to his existing LogMeIn account: User of [your "Company Name"].

Example: Inviting a user who already has a LogMeIn account

Assume that you want to invite one of your colleagues to access computers in your Central account. Your colleague already has a LogMeIn account. Once they accept your invitation and logs in, your colleague will see multiple profiles in the drop-down box in the upper-right of the LogMeIn website interface.

Important: Your colleague will not be prompted to create a new password. They will use their own (existing) LogMeIn account password.

Their original profile (for their own LogMeIn account) will be called Account Holder of [his own "Company Name" as saved on the Billing page]. Their profile for your Central account will be called User of [your "Company Name" as saved on the Billing page].

Tip: Two-factor authentication settings are applied per account. If your account requires two-factor authentication, your users will be prompted to use two-factor authentication when accessing computers in your account, even if they already use two-factor authentication for their personal account.

Using ADFS with LogMeIn Central
How to Integrate LogMeIn Central with Microsoft Active Directory Federation Services.

Prerequisite: Set up ADFS
Set-up ADFS on your internal server network before proceeding.

A live ADFS environment with an externally addressable Microsoft Active Directory Federation Services (ADFS) server must be configured before implementing federated authentication for LogMeIn using ADFS.

ADFS is a software module downloaded and installed on Windows Server operating systems to provide users with Single Sign-On access to systems and applications located across organizational boundaries. For more information, see:

• Microsoft Support’s Key ADFS Concepts guide
• Microsoft Support’s How-to Guide

Once installed, go to Start > Administrative tools > AD FS 2.0 Management.

Important: Make sure your ADFS server is configured before you continue with the remaining tasks.
Task One: Provide information to LogMeIn

Provide the relevant information to LogMeIn and we make adjustments on your account. Contact your LogMeIn Account Manager to begin the ADFS process.

1. Verify domain ownership.

You must prove ownership of your domain before ADFS can be activated for your account. There are two methods of verification: HTML upload and DNS record.

<table>
<thead>
<tr>
<th>Option</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Verify domain ownership by HTML Upload | 1. Create an html file named `logmein-domain-confirmation.html` to the website for your planned ADFS domain.  
2. In the `logmein-domain-confirmation.html` file, include a random string. Example: `logmein-domain-confirmation jska7893279jkdhhkjdhask`  
3. After you have created the `logmein-domain-confirmation.html` file containing the random string, email your LogMeIn Account Manager with the string and they will confirm the `logmein-domain-confirmation.html` is visible and contains the correct information. |
| Verify domain ownership by DNS record | 1. Create a TXT for your domain's DNS entry with the value `logmein-domain-confirmation`.  
2. In the `logmein-domain-confirmation.txt` file, include a random string. Example: `logmein-domain-confirmation jska7893279jkdhhkjdhask`  
3. After you have created the `logmein-domain-confirmation` file containing the random string, email your LogMeIn Account Manager and they will confirm the `logmein-domain-confirmation` file is visible and contains the correct information. |

Tip: If you do not have a LogMeIn Account Manager, you can contact support.

2. Provide the URL of the ADFS server.

You must provide the endpoint URL of your ADFS proxy server to your LogMeIn Account Manager. To find your endpoint URL:

a) Launch AD FS 2.0 Management by going to Start > Administrative tools > AD FS 2.0 Management.

b) Go to Service > Edit Federation Service Properties.

c) Copy the Federation Service name and append it with /adfs/ls.

3. Provide email domains.

You must tell your LogMeIn Account Manager what email domain you will use with your ADFS login. If you have multiple domains, you must specify this to your LogMeIn Account Manager.

Important: Do not change your domain address. Contact your LogMeIn Account Manager if you need to change your domain address.
4. Provide your Token-Signing Certificate.
   You must provide your token signing certificate and provide this information to your LogMeIn Account Manager. You can get information on Token-Signing Certificates from Microsoft's TechNet site.

**Task Two: Establish a Trust Relationship**
Add LogMeIn as a Relying Party Trust in AD FS 2.0 Management.

1. In AD FS 2.0 Management, open the Add Relying Party Trust wizard by going to **Action > Add Relying Party Trust**.
2. Set the data as follows:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Input or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Data Source</td>
<td>Select Enter data about the relying party manually</td>
</tr>
<tr>
<td>specify a display name</td>
<td>Enter the Display name as LogMeIn authentication</td>
</tr>
<tr>
<td>Choose Profile</td>
<td>Select AD FS 2.0 profile</td>
</tr>
<tr>
<td>Configure URL</td>
<td>Enter the SAML Assertion Consumer Endpoint URL:</td>
</tr>
<tr>
<td></td>
<td><a href="https://accounts.logme.in/federated/saml2.aspx">https://accounts.logme.in/federated/saml2.aspx</a></td>
</tr>
<tr>
<td>Configure Identifiers</td>
<td>The following URL must be added to the list of Relying party identifiers:</td>
</tr>
<tr>
<td></td>
<td><a href="https://accounts.logme.in">https://accounts.logme.in</a></td>
</tr>
<tr>
<td>Choose Issuance Authorization</td>
<td>Select Permit all users to access this relying party</td>
</tr>
<tr>
<td>Rules</td>
<td></td>
</tr>
<tr>
<td>Ready to Add Trust</td>
<td>Select Open the Edit Claim Rules</td>
</tr>
<tr>
<td>Finish</td>
<td>Select Finish</td>
</tr>
</tbody>
</table>

**Task Three: Allow Data to be sent to LogMeIn**
Add a Transform Claim Rule for LogMeIn.

1. In AD FS 2.0 Management, open the Add Transform Claim Rule Wizard by going to **Action > Edit Claim Rules > Issuance Transform Rules > Add Rule**.
2. Set the data as follows:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Input or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Rule Type</td>
<td>Under Claim rule template select Send LDAP Attributes as Claims</td>
</tr>
<tr>
<td>Configure Claim Rule</td>
<td>Set Claim rule name to Email and name</td>
</tr>
<tr>
<td>Configure Claim Rule</td>
<td>Set Attribute store to Active Directory</td>
</tr>
<tr>
<td>Configure Claim Rule</td>
<td>Set the LDAP attributes as:</td>
</tr>
<tr>
<td></td>
<td>• E-Mail-Addresses: E-Mail Address</td>
</tr>
<tr>
<td></td>
<td>• Given-Name: Given Name</td>
</tr>
<tr>
<td></td>
<td>• Surname: Surname</td>
</tr>
</tbody>
</table>

3. Click Finish.
**Task Four: Browser Setup (Optional)**
Find out what to do if the browsers do not redirect automatically.

When users who have already authenticated to the domain try to log in to a LogMeIn service via Internet Explorer and Chrome, the browser should automatically recognize their intranet URL and use NTLM for FS server authentication. If the address is not recognized as intranet, you can add the FQDN of your ADFS to the Local intranet zone. This can be deployed to multiple computers via Group Policy. This ensures that users who have already logged in to the domain are able to log in to LogMeIn services with their domain email address alone. They will not need to enter a password since they have already been authenticated.

In **Internet Explorer**, set the Local Intranet website under Settings > Internet Options > Security > Local Intranet.

In **Firefox**:
1. Type `about:config` in the URL bar and press Enter.
2. Modify the `network.automatic-ntlm-auth.trusted-uris` to include the Local Intranet Website.
3. Click OK.

**Using Azure Active Directory with LogMeIn Central**
Integrate Azure Active Directory with LogMeIn Central for additional authentication.

**Prerequisites:**
- An Azure Active Directory Premium subscription.
- An active LogMeIn Central subscription.

*Note:* For more information using SAML with Azure Active Directory, see Microsoft's support site.

**Configure your Azure Active Directory Account**

2. Navigate to Azure Active Directory > Enterprise Applications > New application. The Add an application menu is displayed.
3. Select Non-gallery application. The Add your own application menu is displayed.
4. Give the new application a name and click Add.
5. Click Single sign-on > SAML.
6. Under Basic SAML Configuration, set the following values:
   - **Identifier (Entity ID)**: `https://accounts.logme.in`

7. Click Save.
8. Under SAML Signing Certificate, download the **Certificate (Raw)** and **Federated Metadata XML**.

**Allow Data to be sent to LogMeIn**
For more information, see Microsoft's support site.
Note: The following claims are required by LogMeIn, but they are usually part of the default Azure AD SAML configuration. The following claims must be included in the User attributes and claims configuration.

2. Navigate to **Azure Active Directory** > **Enterprise Applications** > **All applications**.
3. Click the previously configured application name. The **Set up Single Sign-On with SAML** menu is displayed.
4. Next to **User Attributes & Claims**, click the edit icon.
5. Under Claim Name, the following information is required:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Full Schema Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>The email address you registered with LogMeIn</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
</tr>
<tr>
<td>Given name</td>
<td>Your first/given name</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
</tr>
<tr>
<td>Surname</td>
<td>Your surname</td>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a></td>
</tr>
</tbody>
</table>

**Provide information to LogMeIn**
Provide the relevant information to LogMeIn and we make adjustments on your account. Contact your LogMeIn Account Manager to begin the SAML process.

1. Verify domain ownership.
   You must prove ownership of your domain before Azure Active Directory can be activated for your account. There are two methods of verification: HTML upload and DNS record.

   **Option**   | **Procedure**                                                                                                                                                                                                 |
   ------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
   Verify domain ownership by HTML Upload | 1. Create an html file named `logmein-domain-confirmation.html` to the website for your planned ADFS domain.  
   2. In the `logmein-domain-confirmation.html` file, include a random string. **Example**: `logmein-domain-confirmation jska7893279jkdhhkjdhask`  
   3. After you have created the `logmein-domain-confirmation.html` file containing the random string, email your LogMeIn Account Manager with the string and they will confirm the `logmein-domain-confirmation.html` is visible and contains the correct information.  

   Verify domain ownership by DNS record | 1. Create a TXT for your domain's DNS entry with the value `logmein-domain-confirmation`.  
   2. In the `logmein-domain-confirmation.txt` file, include a random string. **Example**: `logmein-domain-confirmation jska7893279jkdhhkjdhask`  
   3. After you have created the `logmein-domain-confirmation.txt` file containing the random string, email your LogMeIn Account Manager and
<table>
<thead>
<tr>
<th>Option</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>they will confirm the logmein-domain-confirmation file is visible and contains the correct information.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> If you do not have a LogMeIn Account Manager, you can <a href="#">contact support</a>.</td>
</tr>
</tbody>
</table>

2. From [https://portal.azure.com](https://portal.azure.com), the **Certificate (Raw)** and **Federated Metadata XML** must be given to your LogMeIn Account Manager.

   **Tip:** If you do not have a LogMeIn Account Manager, you can [contact support](#).

   Once your LogMeIn representative has configured the SAML 2.0 connection using the information provided, your users gain access to the appropriate LogMeIn account and permissions via the IdP as the authentication source. It may take up to 30 minutes for the SSO service to be established for the first time.

### How to View When Your Invited Users Last Logged in

You can view the time when an invited user last logged in to your account.

**Note:** Only LogMeIn Central subscribers (Account Holders) with **Enable LogMeIn Central** and **User management** permissions can view this information.

1. In LogMeIn Central, click **Users > Manage**. The **Users** page is displayed.
2. On the Users page, review the details in the **Last logged in** column.

   **Tip:** To see who logged in to your account most recently, click the header of the **Last logged in** column.

You only see the last logged in time of those users who either logged in directly to the Account Holder's profile, or switched from their own profile to the Account Holder's profile.

### How to Request Access to Computers in Another LogMeIn Account

Use the **Request Access** feature to gain access to computers in other **LogMeIn Central** and **LogMeIn Pro for business users** accounts.

Only LogMeIn Central subscribers (Account Holders) can request access. The recipient must have a **LogMeIn Central** or **LogMeIn Pro for small businesses** account.

1. In LogMeIn Central, click **Users > Manage**. The **Users** page is displayed.
2. On the Users page, click **Request Access**.
3. Enter the email address of the LogMeIn Account Holder responsible for the computers you want to access.
   
   The recipient must be a **LogMeIn Central** or **LogMeIn Pro for small businesses** Account Holder for the host you want to access.
Tip: To identify the Account Holder of a LogMeIn host computer, open the LogMeIn Control Panel on the host and check the account holder’s email on the Overview tab.

4. Click Send Request.

Remember: The recipient must be an account holder of a LogMeIn Central or LogMeIn Pro for small businesses account. Other subscription levels do not have access to the Users tab (Pro for individuals and Pro for power users).

Note: Upon approval, a profile is added to your account. There are two profile types:

• Account Holder of ["Company Name" as saved on the Billing page] for computers in your own account
• User of ["Company Name" as saved on the Billing page] for computers in other accounts

How to Add a User Group

Arrange your users into groups to make it easier to control permissions and computer access, particularly if you have many users in your account.

1. In LogMeIn Central, click Users > Manage.
   The Users page is displayed.
2. Click Add User Group.
   The Add Group dialog is displayed.
3. Name the group.
4. To create a computer group and/or a subscription group by the same name, select Computers and/or Subscriptions next to Include.
5. Click OK.

Now you must set permissions that will be applied to members of the group. See How to Edit User Group Permissions on page 109.

Specifying Permissions for Users and User Groups in your LogMeIn Account

Specify what permissions users and user groups have when accessing hosts in your account.

For information on adding users, see How to Add Users to Your LogMeIn Account on page 99.

1. Central.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LogMeIn Central</td>
<td>When selected, users will always work in the LogMeIn Central interface. Otherwise, users will always work in the simple LogMeIn interface.</td>
</tr>
<tr>
<td>Reports</td>
<td>Allow users to view LogMeIn Central reports. To view Hamachi reports, users must also have the following permission: Access networks in the account.</td>
</tr>
<tr>
<td>Alert management</td>
<td>Allow users to create and manage alerts. Premier, Automation or Insight only.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration management</td>
<td>Allow users to create host preference packages.</td>
</tr>
<tr>
<td>Computer group management</td>
<td>Allow users to create and manage groups of computers.</td>
</tr>
<tr>
<td>View inventory data</td>
<td>Allow users to view inventory reports. Users must also have the following permissions: Reports and Alert Management. Premier or Insight only.</td>
</tr>
<tr>
<td>Inventory management</td>
<td>Allow users to enable/disable inventory data collection for Windows hosts in this account. Only valid for users with access to all computers in the account. Premier or Insight only.</td>
</tr>
<tr>
<td>Create and modify One2Many tasks</td>
<td>Allow users to create and modify One2Many tasks. Premier or Automation only.</td>
</tr>
<tr>
<td>Run One2Many tasks</td>
<td>Allow users to run One2Many tasks. Premier or Automation only.</td>
</tr>
</tbody>
</table>

2. **Files**, you can grant access to files and folders stored in your account using the Files for LogMeIn feature. For more information, see [Files for LogMeIn: Storage for your files and folders](#) on page 123.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All files and folders in my account</td>
<td>Grant access to all files and folders stored in your account. This allows the user to read, modify, and delete your files and folders.</td>
</tr>
<tr>
<td>None</td>
<td>Do not allow the user to access the Files feature. None of your data stored in Files is made available unless you choose to share a link.</td>
</tr>
<tr>
<td>Only specific folders</td>
<td>To grant access to specific folders, go to the Files page and click Share folder for any folder. You can choose to either share a link that gives anyone read-only access to the folder or you can invite users who will be able to read, modify, or delete items in the folder.</td>
</tr>
</tbody>
</table>

**Remember:** You cannot invite users to individual files. Individual files can only be shared via link – meaning you can either share a file with anyone who has the link or with nobody at all.

3. **Management.**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User management</td>
<td>Allow users to edit and delete users in this account. To add users, users must also have the following permission: Enable LogMeIn Central.</td>
</tr>
<tr>
<td>Login policy management</td>
<td>Allow users to apply a login policy to all users in a LogMeIn Central account, including the account holder. See How to Set a Password Strength Requirement on page 12.</td>
</tr>
<tr>
<td>Login credentials can be saved</td>
<td>Allow users to enable the Remember Login Credentials option on the Account &gt; Security page, which allows users to save host login credentials when connecting to a LogMeIn host. See How to Set Up Automatic Authentication on page 138.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create desktop shortcut</td>
<td>Allow users to create desktop shortcuts for quick access to LogMeIn hosts.</td>
</tr>
<tr>
<td>Deployment</td>
<td>Allow users to install LogMeIn host software and LogMeIn Backup. To generate Installation Links, users must also have the following permission: <strong>Enable LogMeIn Central</strong>. To deploy Hamachi networks, users must also have the following permission: <strong>Network and Client Management</strong>.</td>
</tr>
<tr>
<td>Update and Anti-Virus Management</td>
<td>Allow users to manage Windows and Microsoft updates and to use the Anti-Virus Management feature. To manage updates on multiple computers, users must also have the following permission: <strong>Enable LogMeIn Central</strong>. Anti-Virus Management features are available for Premier and Security subscriptions only.</td>
</tr>
<tr>
<td>Enable account-level security features</td>
<td>Allow users to edit security settings on the account email address &gt; Account &gt; Security tab.</td>
</tr>
</tbody>
</table>

4. Define the LogMeIn interface users see when accessing LogMeIn host computers.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group settings apply</td>
<td>Allow users to see the LogMeIn interface made available to members of the assigned User Group.</td>
</tr>
<tr>
<td>Show advanced interface when available</td>
<td>Allow users to see the &quot;Detailed mode&quot; with remote management menus, such as Computer Management, Computer Settings, Performance Info, etc.</td>
</tr>
<tr>
<td>Show simplified LogMeIn interface</td>
<td>Allow users to see the &quot;Compact view&quot; without remote management menu options.</td>
</tr>
</tbody>
</table>

5. Group/Computer Permission.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group settings apply</td>
<td>Allow users to access all computers made available to members of the assigned User Group.</td>
</tr>
<tr>
<td>Note: Group settings apply is not visible when editing permissions for a group.</td>
<td></td>
</tr>
<tr>
<td>Access all computers in the account</td>
<td>Allow users to access all computers in the account.</td>
</tr>
<tr>
<td>Specify the groups and computers the selected user can access</td>
<td>Select an entire group by selecting the box next to the name in the left pane.</td>
</tr>
<tr>
<td>Important: Computers can be reassigned, or moved, from one group to another. If moved, a computer may become inaccessible to some users. See <em>About the Impact of Group Changes (Moved Computers) on User Access</em> on page 43.</td>
<td></td>
</tr>
</tbody>
</table>
6. Set **Network (Hamachi)** permissions. For more information on LogMeIn Hamachi, see *Working with LogMeIn Hamachi* on page 204.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access networks in the account</strong></td>
<td>Allow users to access all Hamachi networks in the account.</td>
</tr>
<tr>
<td><strong>Network and Client Management</strong></td>
<td>Allow users to create and edit Hamachi networks and deploy Hamachi clients.</td>
</tr>
<tr>
<td><strong>Edit Client Defaults</strong></td>
<td>Allow users to change the default settings applied to deployed Hamachi clients.</td>
</tr>
<tr>
<td><strong>Edit Network Defaults</strong></td>
<td>Allow users to change the default settings applied to new Hamachi networks.</td>
</tr>
</tbody>
</table>

7. Once the user has accepted the invitation, the following security permissions become available under **Extra Security**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Emailed security code</strong></td>
<td>Require users to enter a security code when accessing the profile [User of &quot;Company Name&quot;]. LogMeIn sends the code via email to the specified address. Each code can be used only once.</td>
</tr>
<tr>
<td><strong>Printed security code</strong></td>
<td>Require users to enter a security code from a printed list when accessing the profile [User of &quot;Company Name&quot;]. LogMeIn generates a list of one-time security codes for printing. Each time a user accesses the profile, he will be prompted to enter a code from the printed list. The user will be able to generate a new list of codes on the Account &gt; Security tab.</td>
</tr>
<tr>
<td><strong>Enforce two-factor authentication for this user</strong></td>
<td>Require users to follow a two-step process to verify their identity. They can choose any method currently available for LogMeIn. The policy cannot force them to use a specific method. For details, see <em>Two-Step Verification</em> on page 13.</td>
</tr>
</tbody>
</table>

### How to Edit User Group Permissions

You can assign permissions to individual users as well as all users in a group. The permissions of a group member consist of the permissions of the individual user and that of the user group he belongs to.

**Important:** You cannot edit permissions for the [Default Group].

1. In LogMeIn Central, click **Users > Manage**. The **Users** page is displayed.
2. Click **edit permissions** next to the user group whose permissions you want to change. The **Edit User Group Permissions** page is displayed.
3. Change user group permissions, as required. For descriptions, see *Specifying Permissions for Users and User Groups in your LogMeIn Account* on page 106.

**Important:** Users in a group inherit group permissions except for Access Subscription Groups, Interface, and Group/Computer.
4. Click **Save**.

**Tip:** To remove a user group, click **Delete this Group**. Users in the deleted group are moved to the [Default Group] and will lose permissions inherited from the deleted group.

<table>
<thead>
<tr>
<th>How Do User Group Settings Affect Individual User Permissions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the user permissions page, permissions inherited from the user group are marked with a symbol next to the permission's name.</td>
</tr>
<tr>
<td>You cannot change these permissions at the individual user level.</td>
</tr>
</tbody>
</table>

### How to Define Which Computers a User Can Access

Set computer access permissions for an existing user.

Only LogMeIn Central users with **User management** permission can add users.

For information about user group permissions, see How to Edit User Group Permissions on page 109.

2. **Log in** to your account using your LogMeIn ID (email address) and password.
3. The **Computers** page is displayed.
4. On the left menu, click **Users > Manage**.
5. The **Users** page is displayed.
6. Click the **email address of the user** whose permissions you want to change.
7. The **Edit user** page is displayed.
8. Set the computers that the user can access.
   
   **Tip:** Scroll down to the **Group/Computer Permission** section.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group settings apply</strong></td>
<td>Allow users to access all computers made available to members of the assigned User Group.</td>
</tr>
<tr>
<td><strong>Access all computers in the account</strong></td>
<td>Allow users to access all computers in the account.</td>
</tr>
<tr>
<td><strong>Specify the groups and computers the selected user can access</strong></td>
<td>Select an entire group by selecting the box next to the name in the left pane. <strong>Important:</strong> Computers can be reassigned, or moved, from one group to another. If moved, a computer may become inaccessible to some users. See About the Impact of Group Changes (Moved Computers) on User Access on page 43.</td>
</tr>
<tr>
<td><strong>Grant access to all files in your account</strong></td>
<td>Select <strong>Accessible Files &gt; All files in my account</strong> to grant access to your files stored in your account. This feature is only available to Central subscribers who have migrated content from Cubby.</td>
</tr>
</tbody>
</table>
6. Click **Save**.

**How to Move Users to Another Group**

Important considerations when moving users to another group:

- If you move a user from the [Default Group] to a user group, the user keeps his user-level permissions and also inherits group-level permissions granted by the group.
- If you move a user from one group to another, the user inherits the permissions of the new group and loses those permissions that were granted by the original group.

1. In LogMeIn Central, click **Users > Manage**. The **Users** page is displayed.
2. Select the email address of the user you want to move to another group.
3. Use the **User Group** drop-down list to select the new group for the user.
4. Click **Save**.

**Working with Reports**

LogMeIn Central Reports allow you to work with a range of data and charts pertaining to your account's activities.

**Important:** For many reports, including Alerts, Journal, and all inventory reports, data can be collected only from hosts in a Premier account. To experience full reporting functionality, make sure you are a Premier subscriber.

**Who can use this feature?** The full set of LogMeIn Central reports and charts is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Insight</td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View Inventory Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inventory Management</td>
</tr>
</tbody>
</table>

See also *Viewing Report and Alert Data in Charts* on page 120.

**LogMeIn Central Report Types**

LogMeIn Central offers default report types that can be generated, filtered, customized, and then saved for easy retrieval.

Some reports have no dependency on your LogMeIn subscription type, others are only available to Premier and Insight subscribers.

**LogMeIn Reports by Subscription Type**

<table>
<thead>
<tr>
<th>Account Activity and Usage</th>
<th>Basic</th>
<th>Plus</th>
<th>Premier and Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Account Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote Access Sessions (In Last Month)</td>
<td>• Remote Access Sessions (In Last Month)</td>
<td>• Remote Access Sessions (In Last Month)</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Remote Sessions (In Last Month)</td>
<td>• Remote Sessions (In Last Month)</td>
<td>• Remote Sessions (In Last Month)</td>
</tr>
<tr>
<td></td>
<td>• User Account Access (In last week)</td>
<td>• User Account Access (In last week)</td>
<td>• User Account Access (In last week)</td>
</tr>
<tr>
<td>Computer Alerts</td>
<td>none</td>
<td>none</td>
<td>• Alerts (in last week)</td>
</tr>
<tr>
<td>Hardware Inventory</td>
<td>none</td>
<td>none</td>
<td>• CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hardware History</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hardware History (unfiltered)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Installed Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Motherboard</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Network interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Service Tag</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Storage Hardware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Top Disk Usage</td>
</tr>
<tr>
<td>Inventory Report</td>
<td>none</td>
<td>none</td>
<td>For Premier and Insight subscribers, the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Inventory Report presents data about</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LogMeIn host computers in a single</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>composite report. For more</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>information, see About</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Inventory Reporting on</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>page 117.</td>
</tr>
<tr>
<td>LogMeIn Host Software</td>
<td>none</td>
<td>none</td>
<td>• Host Software Installs</td>
</tr>
<tr>
<td>Details</td>
<td></td>
<td></td>
<td>(in Last Year)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Installation Packages (Created in Last</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Month)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Journal Entries (In Last Month)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Last Boot Date</td>
</tr>
<tr>
<td>LogMeIn Licenses</td>
<td>none</td>
<td>none</td>
<td>• Computer Subscription Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Subscriptions</td>
</tr>
<tr>
<td>Software Inventory</td>
<td>none</td>
<td>none</td>
<td>• Installed Applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Installed Operating System Snapshot</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Software History</td>
</tr>
</tbody>
</table>
## Account Activity and Usage

<table>
<thead>
<tr>
<th>Account Audit</th>
<th>Lists activity in your LogMeIn account. Reported details include computers added or deleted, failed logins, subscription changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Sessions (In Last Month)</td>
<td>Lists remote sessions. Reported details include host name, user, start time, end time, duration.</td>
</tr>
<tr>
<td>Remote Access Sessions (In Last Month)</td>
<td>Lists remote control sessions. Reported details include host name, user, start time, end time, duration.</td>
</tr>
<tr>
<td>User Account Access (In last week)</td>
<td>Lists all occasions when your LogMeIn account was accessed. Reported details include user, user IP address, and time of account login.</td>
</tr>
</tbody>
</table>

**Remember:** Reports can be customized. Click **Filter** after you generate the default report to change date range, fields, sort order, and more.

## Computer Alerts

| Alerts (In Last Week) | Lists all alerts for the selected period. Reported details include alert type, event, time generated, status, and applicable Alert Package. Premier or Insight only. |

**Remember:** Reports can be customized. Click **Filter** after you generate the default report to change date range, fields, sort order, and more.

## Hardware Inventory

<table>
<thead>
<tr>
<th>CPU</th>
<th>Lists the CPU type and speed. Premier or Insight only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware History</td>
<td>Lists a full hardware inventory on Date1 compared to a full inventory on Date2. Premier or Insight only.</td>
</tr>
<tr>
<td>Hardware History (unfiltered)</td>
<td>Lists only the changes to hardware that occurred between Date1 and Date2. Premier or Insight only.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Installed Memory</td>
<td>Lists the total memory size and size per module. Premier or Insight only.</td>
</tr>
<tr>
<td>Motherboard</td>
<td>Lists the chipset and number of memory slots. Premier or Insight only.</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>Lists the name and MAC address of each network interface. Premier or Insight only.</td>
</tr>
<tr>
<td>Service Tag</td>
<td>Lists the service tag of host computers supporting this feature (for example, Dell computers). Premier or Insight only.</td>
</tr>
<tr>
<td>Storage Hardware</td>
<td>Lists storage drives by name, type, serial number, capacity. Premier or Insight only.</td>
</tr>
<tr>
<td>Top Disk Usage</td>
<td>Lists disks by assigned drive letter, partition, size, free space, and percentage in use. Premier or Insight only.</td>
</tr>
</tbody>
</table>

**Remember:** Reports can be customized. Click **Filter** after you generate the default report to change date range, fields, sort order, and more.

**Inventory Report**

For Premier and Insight subscribers, the Inventory Report presents data about LogMeIn host computers in a single composite report. For more information, see About Inventory Reporting on page 117.

To filter, use the search field. To add or remove columns, click the column icon in the top-right of the report.

Reported data:

- Computer Description
- Make/Model
- Service Tag
- Asset Tag
- Last logged on user
- CPU
- CPU Speed (MHz)
- RAM (MB)
- Total storage (GB)
- Total free space (GB)
- External IP
- MAC Address
- IP Address
- Subnet Mask
- Primary DNS
- Secondary DNS
- DHCP Server
- Primary WINS
- Secondary WINS
- OS
• Age of OS
• Last boot date
• Existing Battery

**Tip:** The *Asset Tag* must be manually created in the *Registry*. Navigate to `HKEY_LOCAL_MACHINE > SOFTWARE > LogMeIn > V5 > Inventory` and create a *String Value* with a *Value name* of `Asset Tag` and set the *Value data* to the value you want to appear in the Inventory Report.

**Important:** Please use care when accessing the Windows Registry. Consult with your IT support if you are unsure how to proceed.

The Inventory Report can also be accessed via API. Using the public API you can request data for any chosen fields for any subset of hosts. For details see [http://developer.logmein.com/](http://developer.logmein.com/).

**LogMeIn Host Software Details**

<table>
<thead>
<tr>
<th>Installation Packages (Created In Last Month)</th>
<th>Lists host installation links sent from your account, including status details. Premier or Insight only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Software Installs (In Last Year)</td>
<td>Lists host installations executed from your account. Premier or Insight only.</td>
</tr>
<tr>
<td>Journal Entries (In Last Month)</td>
<td>Lists journal entries made on the host dashboard of Windows computers in your account. Premier or Insight only.</td>
</tr>
<tr>
<td>Last Boot Date</td>
<td>Lists the most recent OS start-up date. Premier or Insight only.</td>
</tr>
</tbody>
</table>

**Remember:** Reports can be customized. Click **Filter** after you generate the default report to change date range, fields, sort order, and more.

**LogMeIn Licenses**

<table>
<thead>
<tr>
<th>Computers Subscription Status</th>
<th>Lists subscription details for each host in your account. Reported details include product type, contract term, renewal date, and host software version number. Premier or Insight only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriptions</td>
<td>Lists available subscriptions in your account. Reported details include product type, contract term, status, renewal date, number in use, number available. Premier or Insight only.</td>
</tr>
</tbody>
</table>

**Remember:** Reports can be customized. Click **Filter** after you generate the default report to change date range, fields, sort order, and more.

**Software Inventory**

<table>
<thead>
<tr>
<th>Installed Applications</th>
<th>Lists installed software. Reported details include application name, publisher, version, and install date. Premier or Insight only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed Operating System Snapshot</td>
<td>Lists the installed OS. Premier or Insight only.</td>
</tr>
<tr>
<td>Software History</td>
<td>Lists a full software inventory on Date1 compared to a full inventory on Date2. Premier or Insight only.</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Software History (unfiltered)</td>
<td>Lists only the changes to software that occurred between Date1 and Date2. Premier or Insight only.</td>
</tr>
<tr>
<td>System History</td>
<td>Lists system history on Date1 compared to system history on Date2. Premier or Insight only.</td>
</tr>
<tr>
<td>System History (unfiltered)</td>
<td>Lists only the system changes that occurred between Date1 and Date2. Premier or Insight only.</td>
</tr>
</tbody>
</table>

**Remember:** Reports can be customized. Click **Filter** after you generate the default report to change date range, fields, sort order, and more.

### User and Computer Access Rights

<table>
<thead>
<tr>
<th>Computer Access Permissions</th>
<th>Lists what each user has permission to do with each host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Users</td>
<td>Lists local, not LogMeIn, user accounts. Premier or Insight only.</td>
</tr>
<tr>
<td>User Permissions</td>
<td>Lists users in your account and their permissions as set on the LogMeIn Central Users page. Includes User Group when applicable. Premier or Insight only.</td>
</tr>
<tr>
<td>User Profiles</td>
<td>Lists Windows User Profiles. Premier or Insight only.</td>
</tr>
</tbody>
</table>

**Remember:** Reports can be customized. Click **Filter** after you generate the default report to change date range, fields, sort order, and more.

### Executive Report

**Remember:** A Premier or Insight subscription is required to use this feature.

The Executive Report is a fixed-format report providing a 30-day overview of key data. The single-page report contains:

- Pie charts for Windows Update, Anti-Virus, OS Type, and Disk Space status
- Graphs for Remote Control, Alerts, and Virus Threats

### How to Create a Custom Report Using Report Viewer

Start with a default report, choose the specific data you want to see, and save your new report for easy retrieval.

1. In LogMeIn Central, go to the **Reports > Report Viewer** page.
2. Select a report **Category**.
3. Select the specific **Report** that you want to use as a base.
4. Click **View Report**. The base report is created with no filters applied.
5. Click **Filter** to begin applying data filters.
6. Click **Apply** to refresh the report.
7. Click **Save** to save the filtered report as a custom report. The **Save Report** dialog is displayed.

8. Name the new report and click **Save**. The report is added to the **Report** drop-down list for easy retrieval.

**Note:** To add a report to your favorites list, click **Favorites** in the top-right corner and then click **Add this report to favorites**.

---

**About Inventory Reporting**

Central offers a variety of reports for keeping track of hardware and software inventory on Windows host computers.

**Who can use this feature?** The **Inventory Reporting** feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Insight</td>
</tr>
</tbody>
</table>

To begin collecting hardware, operating system, and software information from all Windows hosts in your account, you must activate the inventory feature. See **How to Activate Inventory Reporting** on page 119.

Once you have activated inventory, and if you have proper permissions, you will be able to view the following inventory reports.

**Important:** When exporting reports, it is not possible to export the reports with filters applied. All exported reports contain unfiltered information.

**Hardware Inventory**

Available at **Reports > Report Viewer**.

- **CPU**
  - This report has information on the type and speed of the CPU running on the host.

- **Hardware History**
  - This report gives information on hardware installed on your host computers that has changed during a given date range.

- **Hardware History (unfiltered)**
  - This report gives information on hardware installed on your host computers during a given date range but does not filter out anything that has not changed.

- **Installed Memory**
  - This report gives information on the memory components installed on your host computers.

- **Motherboard**
  - This report gives information on the motherboard chipset on your host computers, as well as available memory modules.

- **Network interfaces**
  - This report gives information on any physical and virtual network drivers on your host computers (such as MAC addresses, IP addresses), as well as the network gateway through which hosts are connecting.

- **Service Tag**
  - This report gives information on the Service Tag seen in the BIOS of your host computers.
**Storage Hardware**
This report gives information about the size (capacity) and type of any storage or media drives connected to your host computers (such as Disk drives, external hard drives).

**Top Disk Usage**
This report gives disk usage information such as available/used space on the hard drives of your host computers.

**Software Inventory**
Available at Reports > Report Viewer.

- **Installed Applications**
  This report gives information such as version numbers and update details for software installed or updated on your host computers during a given date range.

- **Installed Operating System Snapshot**
  This report gives information about the operating systems installed on your host computers.

- **Software History**
  This report gives information about software installed on your Computers and if the version number or update has recently changed over a given date range.

- **Software History (unfiltered)**
  This report gives information such as version numbers and update details for software on your host computers. It does not filter out software that has not changed.

- **System History**
  This report gives information about system level changes like logons, restarts and other system related operations on your Computers over a given date range.

- **System History (unfiltered)**
  This report gives information about system level changes like logons, restarts and other system related operations on your Computers over a given date range. It does not filter out system information that has not changed.

**Inventory Report**
Available at Reports > Inventory Report. The inventory report lists the following information and features of Computers in the account.

- Computer Description
- Make/Model
- Service Tag
- Asset Tag
- Last logged on user
- CPU
- CPU Speed (MHz)
- RAM (MB)
- Total storage (GB)
- Total free space (GB)
- External IP
- MAC Address
- IP Address
- Subnet Mask
- Primary DNS
• Secondary DNS
• DHCP Server
• Primary WINS
• Secondary WINS
• OS
• Age of OS
• Last boot date
• Existing Battery

Tip: The Asset Tag must be manually created in the Registry. Navigate to HKEY_LOCAL_MACHINE > SOFTWARE > LogMeIn > V5 > Inventory and create a String Value with a Value name of Asset Tag and set the Value data to the value you want to appear in the Inventory Report.

Important: Please use care when accessing the Windows Registry. Consult with your IT support if you are unsure how to proceed.

The Inventory Report can also be accessed via API. Using the public API you can request data for any chosen fields for any subset of hosts. For details see http://developer.logmein.com/.

Computer Inventory
The Computer Inventory gives information for a single host. For more information, see How to View Inventory Report Information for an Individual Computer.

How to Activate Inventory Reporting
Activate the Inventory feature to begin collecting Inventory data from all Windows hosts in your account.

Remember: A Premier or Insight subscription is required to use this feature.

1. In LogMeIn Central, go to the Configuration > Reports page.
2. Select the Enable inventory reporting option.
3. Click Save Settings.

When do the changes take effect? The Inventory setting is deployed to any online Windows host within one minute. For any offline host, the package is stored and deployed when the host next comes online.

How to View Inventory Report Information for an Individual Computer

Remember: A Premier or Insight subscription is required to use this feature.

1. On the LogMeIn Central Computers page, click Properties for the chosen computer.
2. Click the Computer Inventory tab.
3. Choose a data view:
   • Choose Single Date Snapshot to view data for the selected machine on a chosen date
   • Choose Compare Snapshots by Date to compare the inventory of the selected machine on two different dates
   • Choose History to view all inventory changes for the selected machine since Inventory was enabled
4. Click **Apply**.
   Inventory data is displayed.

5. Refine your results using the **Select Inventory Category** drop-down list.
   Your results are filtered according to the selected category.

About Time Zones in Reports

All specific times in LogMeIn reports are shown according to the time zone of the person generating the report.

**How does it work?** All time data is stored in the LogMeIn database in UTC. When you download a report, times are converted to the time zone set at your account email address > Account > Personal Information > Time Zone.

**Example.** You are in New York. Your LogMeIn account is set to Eastern Standard Time (UTC-5). You start a session with a computer in London at 13:00 UTC-5, which is the same as 18:00 UTC. When you generate a report, the Session Start will be shown as 13:00.

Viewing Report and Alert Data in Charts

**How to Add a Chart**

Charts give you rich reporting and analysis within the LogMeIn Central workspace. Each chart is a representation of data pulled from a specific LogMeIn Central report or Alert Package.

**Who can use this feature?** The full set of LogMeIn Central reports and charts is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
<th>User Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Premier</td>
<td>• Insight</td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View Inventory Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inventory Management</td>
</tr>
</tbody>
</table>

1. In the LogMeIn Central, you can create charts in two places:
   - **Reports** page
   - **Alerts** page

2. Click **Add Chart**. The **Add Chart** dialog box is displayed.

3. Select a **Category** and **Report/Alert type**.
   For details, see LogMeIn Central Report Types on page 111 and LogMeIn Central Alert Rule Types on page 45.

4. Name the chart.

5. Choose the **Chart type** (usually table, bar, or pie).

6. Select the data to be displayed.

7. Follow the on-screen instructions to complete your chart.

8. Click **Save**.
   Your chart appears on the active dashboard tab.
Moving and editing charts

To move a chart, grab it by the header and drag it to the preferred location on the tab. You cannot move a chart to another tab.

To edit a chart, click the wrench icon.

To drill-down from chart view to standard view, click anywhere in the chart space.

Using Default Charts

The LogMeIn Central Chart Dashboard and Alert Dashboard offer default charts to get you started using the charting feature. Customize and save the default charts, or keep them as they are for easy reference.

Remember: A Premier or Insight subscription is required to use this feature.

Restoring Default Charts and Alerts

- To restore default charts, go to Configuration > Reports > Restore Default Charts.
- To restore default alerts, go to Configuration > Reports > Restore Alert Dashboard.

Default Reporting Charts

Access Info tab
• Account Logins
• Remote Access Sessions
• Total Computer Usage by Day

User Info tab
• Total User Activity by Day
• User Summary
• Most Active Users
• Account Audit

Computers tab
• Active Subscription Summary
• Most Active Computers
• Upcoming Subscription Renewals

Management tab
• Low Disk Space (% Free)
• Top 10 Installed Applications
• Top Alerts in Last Week
• Installed Operating Systems
• Unused seats

Default Alerts
• Top Alerts (by Computer)
• CPU Alerts
• Disk Space Alerts
• Computer Online/Offline Alerts
Files for LogMeIn: Storage for your files and folders

Files for LogMeIn gives you a new way to retrieve and share files from anywhere. You get 1TB of storage per Pro or Central subscription.

Requirements

• An active LogMeIn Pro or LogMeIn Central subscription
• The latest version of a leading browser: Firefox, Chrome, Safari; Internet Explorer 10 or above

Note: Shared links can be opened in any leading browser (Chrome, Firefox, Safari, IE, Edge) on any major operating system (mobile or desktop). No LogMeIn account required.

Getting started with Files for LogMeIn

1. On a Windows or Mac computer, go to www.LogMeIn.com.
2. Log in to your account using your LogMeIn ID (email address) and password.
3. On the Computers page left menu, click Files.
4. You’re ready to try Files.

What happens at the end of your trial or subscription?

• Everything in your Files drive remains in read-only mode for 14 days:
  • You can download existing files and folders, but you can't upload new data
  • Existing public links remain active, but you can't create new ones
• If you are an account holder with invited users:
  • The feature is dropped from LogMeIn Pro for all invited users
  • You can no longer manage permissions for this feature (Accessible Files)
• After 14 days the feature will no longer be available for use

How to access your files on your desktop with Files for LogMeIn

Connect your storage space as a network drive for easy access from your PC or Mac.

Requirements:

• Windows 7, 8, 8.1, 10 with the latest version of the LogMeIn Client
• Mac OS X 10.9 or above with the latest version of the LogMeIn Client

1. Open the LogMeIn Client.
2. At the bottom of the LogMeIn Client under LogMeIn Files, click Open.
   
   Your Files drive is added to Windows Explorer under Computer as LogMeIn Files – [your LogMeIn ID].

Note: Files for LogMeIn tries to create a share drive letter. It starts with Z:\ and works backwards through the alphabet until it finds an available letter.
Important: The space listed as available under your Files drive refers to your main hard drive. It is not reflective of the 1TB of space available in your LogMeIn account.

To stop using Files in this way, click File > Close LogMeIn Files drive. No data is lost.

How to share files with Files for LogMeIn

Share your files and folders with other users using Files for LogMeIn.

Note: You must be a Master Account Holder to share files.

Share a file or folder (read-only access)

You can share files and folders by sending a link to others using email, chat, or your preferred tool. Anyone with the link is able to view the file or folder (read-only access). Here's how to generate and copy the link.

1. On the Files page, click the item you want to share.
2. In the share column, click the link share file or share folder.
3. Click Generate link.
4. Copy the generated URL to your clipboard.
5. Send the link to others using email, chat, or your preferred tool.

Share a folder with Users (view, modify, delete)

You can turn Files into a collaboration tool by sharing folders with specific users who will be able to view, modify and delete all content in the shared folders.

1. On the Files page, click the folder you want to share.
2. In the share column, click the link share folder.
3. Under Users, enter the email addresses of the people you want to collaborate with. They do not need to be LogMeIn users already.
4. Click Share with users.
   An invitation email is sent from LogMeIn Auto-Mailer.
   The invited users must open the invitation and click the invitation link. Any invitee who is not yet a LogMeIn user will be prompted to create a LogMeIn account. Any invitee who is already a LogMeIn user will have a new profile added to his existing LogMeIn account: User of "[your "Company Name"]".

How to stop sharing (remove link)

To stop sharing a linked item, you must remove its link.

1. On the Files page, select an item.
2. In the Share column, click the shared link icon. The Share dialog is displayed.
3. Click Remove link.

How to upload and download files with Files for LogMeIn

Upload single files or entire folders to Files for LogMeIn.

Upload files or folders

- **Important:** The maximum file size a single file can be is 2GB.

1. On the Files page, click the upload file (all browsers) or upload folder icon (Chrome only).

- **Tip:** You can also drag and drop any of your local files (all browsers) or folders (Chrome only) to the Files page.

2. Browse your local files/folders and select items to upload.
3. Click Open to upload.
   Upload progress is indicated at the bottom of the Files page.

Download a file

- **Option A.** Right click any file and click Download
- **Option B.** Double click a file

- **Important:** You cannot download a folder, only individual files.
Accessing and Managing Remote Computers

Connecting to a Host Computer

System Requirements – Client Device

The computer, phone, or tablet you use to remotely access a LogMeIn computer must meet certain technical requirements.

**Important:** Make sure you are using up to date, officially supported third-party technology together with LogMeIn. LogMeIn is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed). Learn more

PC and Mac Client-side Operating System

- Windows 7 or newer (including 64-bit)
- Windows Server 2008R2 or newer (including 64-bit)
- On a Mac: OS X 10.10 (Yosemite) or newer
- Linux, Chromebook and Windows RT are **not** supported

PC and Mac Client-side Browser

While we recommend connecting via the LogMeIn Client desktop app, you can still access LogMeIn host computers through a supported browser.

On Internet Explorer and older versions of other leading browsers, a plugin is required for a full-featured experience.

Phone or Tablet

Install LogMeIn on any iOS or Android device that meets the requirements shown in the current AppStore or GooglePlay listing.

Internet Connection

Remote control performance depends on several factors, such as screen resolution, color depth, type of activity, available bandwidth and latency.

- For connecting and doing non-remote control work, any always-on internet connection is sufficient.
- For remote control, we require a 1.5 Mbit/s (192 Kbyte/s) or higher connection speed on each end, as per FCC guidelines for video streaming. For optimal experience in Full HD resolution, a 2 Mbit/s (256 Kbyte/s) connection is recommended.

For details, see [How much bandwidth is required to use LogMeIn?](#)

How to Connect from LogMeIn.com

Connect to LogMeIn host computers in your LogMeIn account from LogMeIn.com.
Connect to any computer that meets these conditions:

• LogMeIn host software must be installed and running on the host
• The host must be turned on
• The host must be connected to the Internet
• The host must not be in Sleep mode or Hibernation mode

**Tip:** If the host computer is on a network with other LogMeIn host computers then you may be able to wake it using Wake On LAN. To review Wake On LAN requirements, see *How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN* on page 134.

• The host must not already be controlled by another LogMeIn user

**Note:** Multiple users can connect to a host simultaneously; however, only a single remote user can control it. For example, one user can control a computer while another uses *File Manager* or *Management Tools*.

To connect from your browser:

2. **Log in** to your account using your LogMeIn ID (email address) and password. The *Computers* page is displayed.
3. On the *Computers* page, click the computer you want to access.

**Tip:** Control-click or middle-click to open the session in a new browser tab. On a Mac, use Command-click.

LogMeIn will attempt to make a connection to the host. You will be prompted to authenticate to the host.

**Tip:** You can set LogMeIn to securely save your host username and password to the client computer from which you are connecting. This will allow you to automatically authenticate when you next connect from the same computer. See *How to Set Up Automatic Authentication* on page 138.

4. **Log in** to the computer using the appropriate authentication method:

   • If prompted, enter the username and password you would enter if you were sitting in front of the host computer.
   • If prompted, enter the Computer Access Code you created when you installed LogMeIn to the host computer.

**Remember:** **Do not enter your LogMeIn ID and password**. This will result in Error 1326 or Error 5 (incorrect user name and password).

Your session begins upon successful authentication. The first time you start a remote session you may be asked to install the LogMeIn Client app or an Internet Explorer browser plug-in to the computer you are using to initiate the remote session.
How to Connect using the LogMeIn Client Desktop App

Connect to LogMeIn host computers in your LogMeIn account from your PC or Mac directly using the LogMeIn Client desktop app.

Connect to any computer that meets these conditions:

- LogMeIn host software must be installed and running on the host
- The host must be turned on
- The host must be connected to the Internet
- The host must not be in Sleep mode or Hibernation mode

💡 Tip: Wake on LAN is only available from LogMeIn.com

- The host must not already be controlled by another LogMeIn user

>Note: Multiple users can connect to a host simultaneously; however, only a single remote user can control it. For example, one user can control a computer while another uses File Manager or Management Tools.

1. Launch the LogMeIn Client desktop app:
   - Option 1. Click the LogMeIn system tray (or menu bar) icon and select Connect to computers.
   - Option 2. Using the Start menu or Finder, start the LogMeIn Client.

   Can't find the LogMeIn Client desktop app? Download it from the LogMeIn.com desktop app page.

2. Log in to your account using your LogMeIn ID (email address) and password. The computer list is displayed.

3. Click the computer you want to access and select an action.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📹 Remote Control</td>
<td>Access and control remote computers</td>
</tr>
<tr>
<td>📁 File Manager</td>
<td>Transfer files between computers and more</td>
</tr>
<tr>
<td>🌟 Command Prompt</td>
<td>Access remote computers in the background</td>
</tr>
<tr>
<td>🏡 Main Menu</td>
<td>Manage remote computers</td>
</tr>
<tr>
<td>📩 Info</td>
<td>View computer details</td>
</tr>
</tbody>
</table>

💡 Tip: To connect to a specific computer automatically when the LogMeIn Client starts, select the computer and the default action under View > Options > General > Connect to....
LogMeIn will attempt to make a connection to the host. You will be prompted to authenticate to the host.

**Tip:** You can set LogMeIn to securely save your host username and password to the client computer from which you are connecting. This will allow you to automatically authenticate when you next connect from the same computer. See *How to Set Up Automatic Authentication* on page 138.

4. Log in to the computer using the appropriate authentication method:
   - If prompted, enter the username and password you would enter if you were sitting in front of the host computer.
   - If prompted, enter the Computer Access Code you created when you installed LogMeIn to the host computer.

   **Remember:** Do not enter your LogMeIn ID and password. This will result in Error 1326 or Error 5 (incorrect user name and password).

   Your session begins upon successful authentication.

** Automatically Connect to a Computer when LogMeIn Client Starts**

Follow this procedure to set LogMeIn Client to automatically create a connection to a specific computer when you start and successfully log in.

1. On the LogMeIn Client, click View > Options. The LogMeIn Client Options window is displayed.
2. In the LogMeIn Client Options window, select Connect to the following computer when LogMeIn Client starts. The Connect to and Default action drop-down boxes are activated.
3. Available options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>If you have multiple profiles, you may need to change your active profile to see the computer you want.</td>
</tr>
<tr>
<td>Connect to</td>
<td>Select the computer to which the LogMeIn Client connects upon start-up.</td>
</tr>
<tr>
<td>Default action</td>
<td>To go directly to a remote control session, select Remote Control.</td>
</tr>
<tr>
<td></td>
<td>To go directly to the File Manager, select File Manager</td>
</tr>
<tr>
<td></td>
<td>To go directly to the LogMeIn host main menu, select Main Menu.</td>
</tr>
</tbody>
</table>

4. Click OK to save your settings. The next time you start and successfully log in to the LogMeIn Client, the selected action is automatically made for the chosen host.

Upon connection, you must login to the host with a valid user name and password.
How to Connect Using a Desktop Shortcut

Save time by connecting directly to a computer using a secure shortcut on a client computer.

Who can use this feature? This feature is available to any Account Holder of a LogMeIn Central or a user with the following permission: Create Desktop shortcut.

1. Create a LogMeIn desktop shortcut on the client computer, as follows:
   • Go to www.LogMeIn.com and log in to your account using your LogMeIn ID (email address) and password.
   • Go to Computers > Properties of a computer > Desktop Shortcut.
   Follow the on-screen instructions.

2. Use the newly created shortcut to connect to the host:
   • Double-click the shortcut on the client desktop. You do not need to log in to your LogMeIn account.
   • Log on to the host using the appropriate authentication method.
   Your session begins upon successful authentication.

Tip: For maximum security, you should not use a LogMeIn desktop shortcut on a public or shared computer.

How to Connect via Phone or Tablet

LogMeIn provides apps that you can use to connect to your LogMeIn computers from your iOS or Android devices.

• LogMeIn for iOS – Remote access from your iOS device to your Macs or PCs
• LogMeIn for Android – Remote access from your Android device to your Macs or PCs


Whenever you connect to a host computer running LogMeIn, you must authenticate yourself to the host computer. That means you need to prove that you have the right to use the remote (host) computer by entering a user name and password that the computer recognizes. Do not enter your LogMeIn ID and password. This will result in Error 1326 or Error 5 (incorrect user name and password).

Which user name and password do I enter?

Enter the user name and password you use to access your computer. It should be the same information you enter when you see a logon screen like one of these samples.
Most computers with multiple users or on a corporate network require you to authenticate in this way. For example, on a Windows PC you are typically forced to press Ctrl-Alt-Delete and enter your user name and password. When connecting via LogMeIn to such a computer, you will be asked to enter the same user name and password you use when logging in locally.

**Remember:** Do not enter your LogMeIn ID and password. This will result in Error 1326 or Error 5 (incorrect user name and password).

Do you need to change your Windows password? On many Windows computers you can press Ctrl+Alt+Del, and then click Change a password. If your computer uses a Microsoft account for Windows login (Windows 8 and above), follow these instructions from Microsoft.

**Don't know your computer user name?** Learn how to find it here: Why can’t I log in to my computer? (error 5 / 1326 / 1327 / Login failed.) on page 235

**What’s a Computer Access Code?**

On some computers you may be prompted to enter a Computer Access Code. Usually you are prompted to create a Computer Access Code when you install LogMeIn to a computer that is not configured to require a Windows or Mac user name and password (when you start the computer, it is ready to go without entering a password). The Computer Access Code gives you assurance that only people who know the special code can access your computer.

**Important:** Do not lose your Computer Access Code. It can be changed from the host itself, but cannot be retrieved!

**Remember:** Do not enter your LogMeIn password when asked for a Computer Access Code.

**Advanced Users:** In Windows, the Computer Access Code is actually linked to a hidden Administrator account called LogMeInRemoteUser. The Computer Access Code is the password for the user LogMeInRemoteUser.

**How to Change Your Computer Access Code**

LogMeIn is unable to retrieve a lost Computer Access Code, but you can change the access code directly on the host computer.

This procedure is only valid on host computers already set to use a Computer Access Code.

1. Go to the computer that you want to be able to access remotely.
2. Click the LogMeIn icon and then LogMeIn Control Panel.

![Figure 12: Windows host](image)

![Figure 13: Mac host](image)

3. Click the Options tab.
5. Type and confirm your new Computer Access Code.
6. Click **OK** to save your change.

**Alternate solution: "control userpasswords2"**
On a Windows host, you can reset the Computer Access Code without opening the LogMeIn host interface using the so-called `control userpasswords2` method.

1. Go to the computer that you want to be able to access remotely.
2. On the host, open the **Run** window: On Windows 7, 8, and Vista, go to **Start** and type `run` in the **Search** field.
3. Type `control userpasswords2` and click **OK**.

4. On the list of users, select **LogMeInRemoteUser**.
5. Click **Reset Password**.
6. Type and confirm your new Computer Access Code.
7. Click **OK** to save your change.

**Alternate solution: Create "LogMeInRemoteUser"**
On a Windows host, you can set a Computer Access Code by creating a user called LogMeInRemoteUser. If you are not comfortable working with tools such as Windows Computer Management, feel free to contact LogMeIn for assistance.

1. Go to the computer that you want to be able to access remotely.
2. Create the user called **LogMeInRemoteUser**, as follows:
   a) On the host, open the **Computer Management** window: On Windows 7, 8, and Vista, go to **Start** and type **Computer Management** in the **Search** field.
   b) In the **Computer Management** window, click **Local Users and Groups**.
   c) On the left panel, open the **Users** folder and right-click to display the menu. Select **New User**. The **New User** window is displayed.
d) In the **New User** window under **User name**, type **LogMeInRemoteUser** (one word, exactly as shown).
e) Enter and confirm a password.

**Important:** This password is one and the same as your Computer Access Code.

f) Select **Password never expires**.

g) Click **Create**. A new user called LogMeInRemoteUser is created.

h) Close the **New User** window. The **Computer Management** window is displayed.

3. Add LogMeInRemoteUser to the Administrators group, as follows:

a) On the left panel, open the **Groups** folder and double click **Administrators**.

b) In the **Administrators Properties** window, click **Add**.

c) Under **Enter the object names to select**, enter LogMeInRemoteUser.

**Tip:** If you receive a Name Not Found error, select the computer's domain under **Locations** and set it to the local computer: computername\LogMeInRemoteUser.

d) Click **OK** and close the **Computer Management** window.

4. Restart the LogMeIn service, as follows.

a) On Windows 7, 8, and Vista, go to **Start** and type **Services** in the **Search** field.

b) On the list of services, right-click **LogMeIn** and select **Restart**.

When you next log in to this computer using LogMeIn, you will be prompted to enter the password you created for LogMeInRemoteUser. In other words, the password for LogMeInRemoteUser is exactly the same as your Computer Access Code.

**How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN**

When all requirements are met, you will be able to use Wake On LAN to switch on a computer that is in sleep mode (PC and Mac) or powered off (PC).

**Minimum Requirements**

- The computer you are trying to wake up must be on a wired connection (not on WiFi)
- A second LogMeIn host computer must be switched on and in the same network in order to send the wake request

**Important:** Make sure you are using up to date, officially supported third-party technology together with LogMeIn. LogMeIn is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed). [Learn more](#)

**Wake On LAN for a Windows PC**

How to enable Wake On LAN on a Windows PC.

- Make sure Wake On LAN is enabled in the BIOS of the computer you want to wake up. Consult the user guide of your computer or motherboard to locate the appropriate BIOS switch, usually **Wake On LAN from S5**.
- Open the **LogMeIn Control Panel** and navigate to **Options > Preferences > Advanced Settings**. Under **Wake On LAN**, select **Enable 'Wake On LAN' from sleep and power off**. Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.
Any computer that is ready for Wake On LAN shows the **Switch On** button next to the computer. Click the button to wake the computer. It may take several minutes for the computer to wake.

![Wake On LAN in the browser](image)

Figure 14: Wake On LAN in the browser

![Wake On LAN on a phone or tablet](image)

Figure 15: Wake On LAN on a phone or tablet

**Still Not Working?** See *Troubleshooting Wake On LAN issues on a Windows PC* on page 136.

### Wake On LAN for a Mac

How to enable Wake On LAN on a Mac.

- On the computer you want to wake up, under **System Preferences > Energy Saver**, enable **Wake for Network Access**.

- **Can't access this feature?** If your Mac is part of a domain or a network, your domain administrator may have restricted some of the features and settings available on your MAC. Contact your administrator for more information.

- Open the **LogMeIn Control Panel** and navigate to **Options > Preferences > Advanced Settings**. Under **Wake On LAN**, select **Enable 'Wake On LAN' from sleep and power off**.

Any computer that is ready for Wake On LAN shows the **Switch On** button next to the computer. Click the button to wake the computer. It may take several minutes for the computer to wake.

![Wake On LAN in the browser](image)

Figure 16: Wake On LAN in the browser

![Wake On LAN on a phone or tablet](image)

Figure 17: Wake On LAN on a phone or tablet

**Important:** You cannot wake a Mac that is powered off. Make sure your Mac is in sleep mode and not powered off.

**Still Not Working?** See *Troubleshooting Wake On LAN on a Mac* on page 137.
Troubleshooting Wake On LAN issues on a Windows PC
Here are some steps you can take to troubleshoot issues when trying to wake a PC.

Minimum Requirements
• The computer you are trying to wake up must be on a wired connection (not on WiFi)
• A second LogMeIn host computer must be switched on and in the same network in order to send the wake request

Important: Make sure you are using up to date, officially supported third-party technology together with LogMeIn. LogMeIn is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed). Learn more

Hardware Requirements
To ensure best results, make sure the following items are using up-to-date drivers or firmware:
• Motherboard Chipset
• Network Adapter (if you have recently updated to Windows 10, make sure the Network Adapter drivers are updated)
• BIOS

Tip: In the BIOS under Power Management, Deep Sleep must be turned off.

Consult your computer or hardware manufacturer for assistance in downloading and installing drivers and firmware.

Tip: When Wake On LAN is possible, the LED light of both your network adapter and ethernet port should be lit up or blinking. These are commonly located on the back of your computer. If these lights are not lit up or blinking, the issue is with your network adapter or ethernet port hardware and you may want to contact the manufacturer.

Enabling Wake On LAN on Windows 10
1. Open the Quick Access Menu by pressing the Windows key and X at the same time.
2. Click Device Manager.
The Device Manager window is displayed.
3. Expand the list of Network adapters.
4. Right-click the primary network adapter and select Properties.
The first adapter in the list is usually the primary adapter.
5. Select the Power Management tab.
6. Select the boxes for Allow this device to wake the computer and Only allow a magic packet to wake the computer.
7. Select the Advanced tab.
8. In the Property box, highlight Wake on Magic Packet.
9. Set Value to Enabled.
10. Select OK.
11. Restart your computer.
Further Resources and Information

To see a full list of available states on your host machine, in command line type `powercfg -a` and verify that states S3, S4 and S5 are available.

💡 Tip: To open a command line, press the Windows key and R at the same time on your keyboard to open a Run box, then type in `cmd` and select OK.

ACPI (Advanced Configuration and Power Interface) standards:

• S0 – System is fully powered on
• S1 – Power on Suspend(POS): Power to the CPU and RAM is maintained.
• S2 – CPU powered off.
• S3 – Standby, Sleep or Suspend: RAM still has power
• S4 – Hibernation: Memory is saved to the hard drive and the system is powered down.
• S5 – Shut Down: The power supply still supplies power to the power button.

For additional information, visit the Microsoft support site.

Troubleshooting Wake On LAN on a Mac

Here are some steps you can take to troubleshoot issues when trying to wake a Mac.

Minimum Requirements

• The computer you are trying to wake up must be on a wired connection (not on WiFi)
• A second LogMeIn host computer must be switched on and in the same network in order to send the wake request

⚠️ Important: Make sure you are using up to date, officially supported third-party technology together with LogMeIn. LogMeIn is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed). Learn more

Hardware Requirements

First, confirm that you meet the hardware requirements for using Wake on LAN:

• Confirm that the computer is on a wired network (not WiFi). Wake On LAN is not supported for Mac hosts on a wireless network.
• Make sure the host is in Stand-by, sleep, or hibernation (ACPI specification S3 or S4) mode.
• You cannot wake a Mac that is powered off.

Adjust the Power Management settings in a System Configuration file

Check the Power Management settings on the Mac you want to wake up.

1. Open Finder.
2. Navigate to SystemConfiguration by going to Go > Go to folder and typing `/Library/Preferences/SystemConfiguration/`.
4. Set the `<integer>` Wake On LAN `</integer>` value to 1 for the following `<keys>`:
   a) `<key>` AC Power `</key>`
   b) `<key>` Battery Power `</key>`
c) <key> UPS Power </key>

5. Restart the Mac.
   Wake On LAN should be available.

**Adjust the Power Management settings in Terminal**

1. Open **Finder**.
2. Navigate to **Terminal** by going to **Go > Utilities** and double-clicking on **Terminal**.
   The **Terminal** window is displayed.
3. Type `pmset -g live`.
   A table with settings and values is displayed.
4. Look for the value `womp` and verify that it is set to 1.
   If it is not set to 1, you can set it with the command `sudo pmset -a womp 1`.

**Further Resources and Information**

Make sure the host is in Stand-by, sleep, or hibernation (ACPI specification S3 or S4). You cannot wake a Mac that is powered off.

ACPI (Advanced Configuration and Power Interface) standards:
- **S0** – System is fully powered on
- **S1** – Power on Suspend (POS): Power to the CPU and RAM is maintained.
- **S2** – CPU powered off.
- **S3** – Standby, Sleep or Suspend: RAM still has power
- **S4** – Hibernation: Memory is saved to the hard drive and the system is powered down.
- **S5** – Shut Down: The power supply still supplies power to the power button.

For additional information, visit the [Apple support site](https://support.apple.com).

**How to Set Up Automatic Authentication**

LogMeIn Central offers a combination of settings that allow you to securely save host credentials to a client computer. This allows you to automatically authenticate to a host when you next connect from the same client.

1. Make sure that automatic authentication is active for your user profile:
   a) Log in at [www.LogMeIn.com](https://www.LogMeIn.com).
   b) At the top of the page, click **Settings > Security**.
   c) Under **Remember Computer Login Credentials**, confirm that the following is selected: **Give users the option to store host computer login credentials on clients**.

   **Tip**: If the section is not available or is grayed out, then you do not have permission to use this feature. Contact the LogMeIn Central Account Holder who gave you access to computers in his account and ask for the **Login credentials can be saved** permission.

2. Make sure automatic authentication is active on the host. **Allow login credentials to be saved** must be selected for the Host Preference Package applied to the host.
   This option is active by default when no Host Preference Package is applied.

3. Reconnect to the host and select the **Save credentials** box during authentication.
   Your Windows or Mac authentication information is securely saved to the client computer.
The next time you log in to the same host from the same client, the authentication window will be displayed briefly, but you will not need to enter your user name or password. Your saved credentials will be sent to the host automatically.

**Do you want to turn off automatic authentication?** Once connected to a host, click **Delete saved credentials** at the top of the host Dashboard (Detailed Mode) or Main Menu (Compact View).

## Remote Control

### System Requirements – Client Device

The computer, phone, or tablet you use to remotely access a LogMeIn computer must meet certain technical requirements.

**Important:** Make sure you are using up to date, officially supported third-party technology together with LogMeIn. LogMeIn is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed). Learn more

**PC and Mac Client-side Operating System**

- Windows 7 or newer (including 64-bit)
- Windows Server 2008R2 or newer (including 64-bit)
- On a Mac: OS X 10.10 (Yosemite) or newer
- Linux, Chromebook and Windows RT are **not** supported

**PC and Mac Client-side Browser**

While we recommend connecting via the LogMeIn Client desktop app, you can still access LogMeIn host computers through a supported browser.

On Internet Explorer and older versions of other leading browsers, a plugin is required for a full-featured experience.

**Phone or Tablet**

Install LogMeIn on any iOS or Android device that meets the requirements shown in the current AppStore or GooglePlay listing.

**Internet Connection**

Remote control performance depends on several factors, such as screen resolution, color depth, type of activity, available bandwidth and latency.

- For connecting and doing non-remote control work, any always-on internet connection is sufficient.
- For remote control, we require a 1.5 Mbit/s (192 Kbyte/s) or higher connection speed on each end, as per **FCC guidelines for video streaming**. For optimal experience in Full HD resolution, a 2 Mbit/s (256 Kbyte/s) connection is recommended.

For details, see **How much bandwidth is required to use LogMeIn?**
Remote Control from a PC or Mac

Starting Remote Control
Choose the most convenient way to gain control of a host computer.

From the LogMeIn Central Computers page
Log in to LogMeIn.com and click the name of the computer you want to control.

From the Host Main Menu
Once connected to the host Main Menu, click Remote Control.

From the LogMeIn Client desktop app
Connect to host computers from your PC or Mac directly.

For details, see How to Connect using the LogMeIn Client Desktop App on page 128.

Once Remote Control has started...
Once you have launched remote control and successfully authenticated to the host computer, you see the host computer’s desktop and the LogMeIn remote control toolbar.
Changing How You View the Host

How to View the Host Computer in Full Screen Mode
In Full Screen Mode the host display covers the entire client display. Full Screen mode gives you the most realistic “as if you were there” experience.

• On the Remote Control toolbar, click the Full Screen Mode button. The LogMeIn interface is minimized and the host computer’s display appears on your entire screen. Only the Remote Control toolbar remains visible.
• To exit full screen mode, click the Full Screen Mode button again.

Figure 19: The Remote Control toolbar

Tip: For best results during Full Screen viewing, go to Options > Resolution Settings and select Match Resolution.

How to Keep the Remote Control Toolbar Visible During Full Screen Mode
In Full Screen Mode, the Remote Control toolbar is hidden to allow maximum visibility.

• To keep the toolbar visible, click the pin icon on the Full Screen version of the Remote Control toolbar.

The toolbar remains open.

How to Magnify a Section of the Host Screen
The Magnifying Glass feature opens a box that you move on the host screen to view a small area in high resolution without otherwise adjusting your resolution.

The Magnifying Glass is available when screen size is less than 100% of its original size.
Note: To adjust your screen size, see *How to Change Screen Size During Remote Control* on page 142.

1. On the Remote Control toolbar, click **Options > Magnify**. The magnifying glass is activated.
2. Drag the box. Any area within the box is displayed in 100% of its original size.
3. Click the **Magnify** button again to deactivate the magnifying glass.

![Figure 20: The Remote Control toolbar](image)

**How to Change Screen Size During Remote Control**

View the host display on the client device in a way that you find comfortable.

1. On the Remote Control toolbar, click **Options > View**.

2. Select the appropriate setting. Your selection is applied immediately.

**How to Work with Multiple Host Monitors**

When connected to a host with multiple monitors, the **Monitors** button will be available on the remote control toolbar.

Click the **Monitors** button to switch between monitors.

![Monitors button](image)
**Tip:** On a Windows PC, try this shortcut. Press **Left CTRL key-Left Windows key-Right/Left Arrow key** to switch monitors. To see all monitors at once, keep moving through until you can see all available monitors on the client display.

**Note:** The Java and HTML remote control clients do not offer multiple monitor support.

**Multi-Monitor Display**

**Important:** Multi-Monitor Display is not available for LogMeIn Central Basic accounts.

When both the client and host have multiple monitors, host-side monitors can be cloned "one-to-one" to the client. Screens are automatically cloned upon connection.

When using the LogMeIn Client to connect, this "one-to-one cloning" happens automatically upon connection. You can also click the **Monitors** icon to switch between host-side monitors.

This illustration shows how the host-side monitors are reproduced "one-to-one" on the client computer.

![Multi-Monitor Display Illustration]

Click the **Monitors** button to switch between cloned monitors.

**About HD Remote Control**

High-definition (HD) quality provides a premium remote control experience. With HD remote control you can seamlessly watch videos and stream music from one computer to another.

**Fastpath:** To turn on HD while controlling a computer from a PC or Mac, go to the Remote Control toolbar and click **Options > Color Quality**.
Remember: A Plus or Premier subscription is required to use this feature.

For more information, see How to Change the Color Quality of the Host Screen on page 144.

Tip: HD quality provides the least amount of latency and the smoothest transition with an automatically adjusting resolution.

How to Change the Color Quality of the Host Screen

Choose a color quality setting during remote control.

1. On the Remote Control toolbar, click Options > Color Quality. The Color Quality options are displayed.
2. Select the appropriate setting.
   - For better image quality, select Low quality or Medium quality.
   - For best image quality and performance, select HD quality.

Remember: A Plus or Premier subscription is required to use this feature.

Tip: HD quality provides the least amount of latency and the smoothest transition with an automatically adjusting resolution.

Tip: Choose Automatically adjust color settings to allow LogMeIn to detect the optimal setting.

Your selection is applied immediately.

How to Optimize Remote Control Performance at Slower Connection Speeds

Adjust your network connection speed to achieve optimal performance during remote control.
On the Remote Control toolbar, click **Options > Network.**

- Select **Slow** to optimize your connection on lower speed connections
- Select **Fast** to exploit a high bandwidth connection
- Select **Auto** to allow to detect the optimal settings

**Customizing the Remote Control Toolbar**

Add icons to the remote control toolbar for easy access to favorite remote control features. All features available under the **Options** menu can be added.

![Toolbar customization menu](image)

**Figure 21: The toolbar customization menu**

**Security During Remote Control**

You can prevent others from viewing the host screen and from using the host mouse and keyboard.

**Tip:** Want to know more about security? Read more about [securing your LogMeIn remote environment](#).

**How to Blank the Host Screen During Remote Control**

Protect your data by blanking the host display during a remote control session.

1. On the Remote Control toolbar, click **Options > Blank Screen.**
   You can turn this feature on or off at any time.
2. If prompted, install the DPMS driver (Display Power Management Services) driver.
   This happens the first time you use the screen blanking feature on the host.
   Not all monitors, video cards, motherboards, or BIOS support DPMS. Check with your hardware vendor if you experience problems with the DPMS driver. In case of incompatibility, you may not be able to use this feature with some host computers.

Anyone at the host device sees a blank screen on the physical monitor while the remote session is active.
Tip: When you connect to a computer for the first time, you are presented with the option to automatically blank the remote screen during all your future sessions. To change your remote control preferences, click Blank Screen in the toolbar.

How to Block Input During Remote Control
Lock the host keyboard and mouse to prevent anyone sitting at the host machine from entering data during a remote control session.

- On the Remote Control toolbar, select Options > Lock Keyboard. You can turn this feature on or off at any time.

Moving Data During Remote Control

How to Copy and Paste Between Devices (Clipboard Synchronization)
Use Clipboard Synchronization to save time and avoid errors by directly copying and pasting information between devices during remote control.

This feature is not available during a view-only Monitor Host Screen session.

- On the Remote Control toolbar, select Options > Sync Clipboard.

Anything copied on either device is available to be pasted to the other.
- When copying between devices with the same operating system (PC to PC, Mac to Mac), copy and paste as normal.
- When controlling a PC host from a Mac client:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy from the PC (host)</td>
<td>Ctrl + c</td>
</tr>
<tr>
<td>Paste to the Mac (client)</td>
<td>cmd + v</td>
</tr>
<tr>
<td>Paste to the PC (host)</td>
<td>Ctrl + v</td>
</tr>
</tbody>
</table>

- When controlling a Mac host from a PC client:
  a) Set your PC-to-Mac keyboard mapping. See How to Set PC-to-Mac Keyboard Mapping on page 183.
  b) Follow these guidelines:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy from the Mac (host)</td>
<td>[mapped cmd key] + c</td>
</tr>
<tr>
<td>Paste from the Mac (host) to the PC (client)</td>
<td>Ctrl + v</td>
</tr>
<tr>
<td>Paste to the Mac (host)</td>
<td>[mapped cmd key] + v</td>
</tr>
</tbody>
</table>
How to Connect Drives During Remote Control
Use the Connect Drives feature to make files on the client accessible to the host without copying or moving any data.

Get Connected
To connect client-side drives to the host, start a remote control session and click Options > Connect Drives on the Remote Control toolbar. You can turn this feature on or off at any time.

Available on Windows hosts only.

Find the Connected Drive
To access connected client-side drives, open Computer in Windows 7 or This PC in Windows 8 or 10. Client-side drives are listed as Network Drives or Drives connected from [client name].

Connected Drives: Example
You have a Spyware cleaner program saved on a removable disk (such as a USB stick) attached to the client. You want to run the Spyware cleaner on the host.

1. Start a LogMeIn remote control session.
2. Connect drives at Options > Connect Drives.
3. During remote control, open Computer or This PC on the host.
4. Under Network Drives, locate and run the executable file for the Spyware cleaner to run it directly from the drive attached to the client. There is no need to copy or move any files.

Remember: Some programs may require additional configuration or a license key before they will run on the host.

Using Presentation Tools
Use the whiteboard and the laser pointer to highlight items on the host screen.

How to Draw on the Host Screen
Use the Whiteboard to activate a pencil tool that you can use to draw freehand images on the host computer's screen.

1. On the Remote Control toolbar, click Options > Whiteboard.
   The pencil tool is activated.

   Note: You cannot control the host while Whiteboard is enabled.

2. Draw on the host screen.
   The pencil tool leaves a red line on the host screen. All drawings appear on both the client and host.
3. To erase drawings, click Options > Whiteboard.

How to Use the Laser Pointer
The Laser Pointer is a small red dot that the client-side user moves around the host screen to highlight features for the host-side user.

To the host-side user, the laser pointer appears as a simple red dot.

Note: You cannot control the host while Laser Pointer is enabled.

2. To exit, click Laser Pointer again.

Remote Sound
Use the Remote Sound feature to listen to sounds played on the host computer while you are at the client.

Important: This feature is only available for LogMeIn Pro, LogMeIn Central Plus and LogMeIn Central Premier subscribers. It is not available for LogMeIn Central Basic subscribers.

Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

Mute
To mute remote sound during remote control, click the loudspeaker icon on the Remote Control toolbar.

Adjust the volume
To adjust the volume during remote control, drag your mouse across the volume bars on the Remote Control toolbar.

Change sound quality
To change sound quality during remote control, click Options > Sound on the Remote Control toolbar and adjust the Quality slide bar.

Remote Printing
You can print from the host computer to a printer connected to the client.

Remember: A Plus or Premier subscription is required to use this feature.

Make sure at least one printer is connected to the client.


Tip: You will be able to connect one or more printers when multiple client-side printers are available. For best results, only print to one printer at a time, otherwise this can lead to issues with the document reaching the print spooler successfully.

The selected printer (or the client’s default printer if there is only one printer available) will be ready to receive print jobs from the host.
2. On the host, print as you normally would during regular use.
3. Make sure the client printer is selected in the Print dialog box: [Printer Name] via LogMeIn.
4. Click Print on the Print dialog box. The file will print to the selected client-side printer.

Having trouble printing? See Troubleshooting Remote Printing on page 238.

Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

System Management (Quitting Programs on the Host)
Remotely list and quit applications running on the host.

How to Open the Windows Task Manager on the Host Computer (Ctrl-Alt-Del)
During a remote session, the Ctrl-Alt-Del key combination entered on the client will only be registered by the client.

This feature is not available during a view-only Monitor Host Screen session.

Available on Windows hosts only.

- On the Remote Control toolbar, click Options > Ctrl-Alt-Del button. The Windows Task Manager opens on the host computer.

Tip: You can also use a hotkey to send the Ctrl-Alt-Del command to the host. The default is Ctrl-Alt-Insert. To change the hotkey, open the host preferences and go to General > Remote Control > Interaction and select a key combination from the Ctrl-Alt-Del hotkey combination drop-down list.

How to Force Quit Applications on a Mac Host (Command-Alt-Escape)
This feature is not available during a view-only Monitor Host Screen session.

Available on Mac hosts only.

- When controlling a Mac from a Windows PC, press Windows Key-Alt-Esc on the client keyboard. The Force Quit Applications window opens on the host.
- When controlling a Mac from a Mac, click Options > Cmd-Alt-Esc on the Remote Control toolbar. The Force Quit Applications window opens on the host.

Remote Control from a Phone or Tablet

About HD Remote Control on an iOS Device
High-definition (HD) quality provides a premium remote control experience. With HD remote control you can seamlessly watch videos and stream music from a Windows or Mac computer to your iOS device.

Remember: A Plus or Premier subscription is required to use this feature.

Fastpath: To change to HD during remote control, click Gear (Settings) icon > Color Quality > HD quality.
HD quality requires higher network bandwidth and computer performance than other options. In general, most recently purchased computers can provide the required performance. Network bandwidth depends on your service provider.

How to Zoom in and Zoom out
When viewing a host computer's desktop, you can zoom in and out in several ways.

- Pinch your fingers together or apart.
- Tap the Magnifying Glass (zoom) icon to zoom to wherever the mouse is pointing.
- Tap the Zoom Slider icon to display a slide on the right side of the screen. Use the slide to zoom in or out to wherever the mouse is pointing.

How to Change Mouse Behavior During Remote Control
Choose how the pointer behaves on the host computer's screen.

You can only change this setting during an active remote session.

1. On the main remote control screen, tap the Gear (Settings) icon.

The Settings page is displayed.

2. Tap Scroll Mode to choose how you want the mouse to move on the host computer:
   - Choose Screen moves if you want the remote desktop to move "underneath" the pointer, which remains stationary in the center of the touchscreen.
   - Choose Mouse moves if you want the pointer to move as you drag, similar to a laptop touchpad.
   - On an iPad and Android tablets and devices running Honeycomb, you can also choose Direct, which allows you to tap directly on the remote screen. You can simply tap a button on the host screen without first having to move the pointer to the button.

3. Save your settings.

App Touch Controls for Phone/Tablet: Click, Scroll, and Drag
Various gestures and swipes allow you to reproduce a range of mouse-click actions.

- A single tap acts as a single mouse click.
- To switch the behavior of a single click between left click and right click, tap the Mouse button.
- A double tap acts as a double click.
- A double tap and hold allows you to grab and then drag.
- A two-finger tap acts as a right click.
• A two-finger drag reproduces the mouse wheel scrolling action.
• On devices supporting three-finger swipe, a horizontal three-finger swipe switches between host monitors and a vertical three-finger swipe opens the keyboard.

Tip: On an iPad you can tap the on-screen mouse buttons for right-click and left-click.

How to Select and Copy Text During Remote Control
To select text on the host computer (the computer you are controlling), you must double-tap, hold, and then drag.

Important: Selecting and copying works according to the behavior of the host computer operating system (Windows or Mac OS), not your phone or tablet operating system.

What can be copied and pasted from the host to the client? You can copy text from the host and paste it to your phone or tablet. Other items, such as files or images, can be copied from one location on the host and pasted to another, but not to your phone or tablet.

How can you paste to another application? For devices that do not support multi-tasking you must exit the LogMeIn app and then open the application to which you want to paste the copied content. Similarly, to copy content from your device to the host, you must make a copy before you launch the LogMeIn app. Text copied from the client will be ready for pasting to the host when your remote session begins.

1. At the beginning of the text you want to select, double tap and hold (iOS) or tap and hold (Android), then drag to select the text.
   You must position the mouse correctly. On iOS, the magnifying glass is not displayed to help set the insertion point.
2. Lift your finger when your selection is complete.
3. To copy, do a two-finger tap to simulate a right-click and bring up the context menu.

How to Switch Between Monitors
You can only change this setting during an active remote session with a host computer that uses multiple monitors.

Tip: On an iPhone or iPod touch, shake the device to switch between monitors ("shake swaps screen"). On devices supporting three-finger swipe, make a three-finger swipe left or right to switch between monitors.
1. On the main remote control screen, tap the **Gear (Settings)** icon.

![Gear icon]

The *Settings* page is displayed.

2. Tap **Monitor**.

A list of available monitors is displayed.

3. Make a selection:
   - To view a specific monitor, tap the monitor you want to view
   - To show all monitors simultaneously, tap **All Monitors**

   **Note:** This is also where you can turn off the *Shake Swaps Screen* behavior.

4. Save your settings.

**How to Access the Onscreen Keyboard**

Use the onscreen keyboard to enter text, commands, and other information directly to the host computer.

- On the main remote control screen, tap the **Keyboard icon**.

![Keyboard icon]

**Tip:** On devices supporting three-finger swipe, make a three-finger swipe up/down to show/hide the keyboard.

The onscreen keyboard is displayed.

- Tap the screen where you want to begin typing.
- The lower keyboard is the standard keyboard for your device.
  - Tap **ABC** and **123** to switch between letters and numbers.
  - While using numbers, tap `#+=` and **123** or **ALT** to switch between special characters (including punctuation marks) and numbers.
  - On iOS, tap the **Globe** to access international keyboards.
  - On Android, tap and hold the **ABC** or **123** button and select **Input method** to access international keyboards. Refer to device documentation for further information regarding international keyboards.

**Important:** Characters will not be displayed if your selected international keyboard has a character set that the host computer does not support.

- The upper keyboard is unique to LogMeIn.
Shift is "sticky" and will remain "on" when tapped to allow you to enter key combinations and to act as the Caps Lock key.

Ctrl and Alt are both "sticky" and will remain "on" when tapped to allow you to enter key combinations.

The Win key acts as the Windows logo key. Use it to open the Windows Start menu. It is "sticky" to allow for key combinations and shortcuts.

The Menu key acts as the Application key. Use it to open context menus in Windows applications. It is "sticky" to allow for key combinations and shortcuts.

The Extra keys icon brings up various special keys.

You may have to swipe left and right to access all available special keys.

Function keys: F1 - F12
Special keys: Esc (Escape), Caps (Caps lock), PrtScr (Print Screen), Ins (Insert), Del (Delete), Scroll (Scroll Lock), Home, End, Pause, PgUp (Page Up), PgDn (Page Down)
Direction keys: Tab and arrows (up, down, left, right)

To turn off the keyboard, tap Hide or X.

How to Use Ctrl-Alt-Delete and Common Key Combinations
When connected to a Windows PC, use the Key Combinations icon to access the Ctrl-Alt-Del key combination.

On the main remote control screen (not the onscreen keyboard), tap the Key Combinations icon.
The Ctrl–Alt–Del command is sent to the host computer.

**Working with Remote Sound**
With remote sound, you can use your device to listen to sounds that are being played on the host computer.

**How to Change the Volume**
1. On the main remote control screen, tap the **Gear (Settings)** icon.

The **Settings** page is displayed.
2. Tap the **Host Volume** slide bar to change the volume.
3. Save your settings.

**How to Change Sound Quality**
1. On the main remote control screen, tap the **Gear (Settings)** icon.

The **Settings** page is displayed.
2. Tap **Sound Quality**.
3. Select the quality of remote sound playback on your device.
4. Save your settings.

**How to turn off remote sound**
1. On the main remote control screen, tap the **Gear (Settings)** icon.

The **Settings** page is displayed.
2. Under **Remote Sound settings**, slide **Remote Sound** to **OFF**.

**How to Manage Saved Login Details**
Protect your login information by clearing saved credentials (user names and passwords) from your device on the **Settings** page in the LogMeIn app.
Example: Deleting Login Information
You are running LogMeIn on your work computer. When you normally log in to your work computer, you must authenticate to Windows using your Windows user name and password. To save time when you connect via the LogMeIn app, you select the Remember login option.

The Problem. Your network administrator forces you to change your Windows password every 30 days. The password remembered by the LogMeIn app will no longer be valid once you have changed the password you use to access your work computer.

The Solution. Go to the Settings page in the app and delete all logins (clear user name and password) to clear your old Windows credentials from the app. The next time you access your work computer from your phone or tablet, you will need to manually enter your user name and password.

How to Protect Information During Remote Control
You can blank the host display and/or lock the host keyboard to protect your information during remote control.

You can only change this setting during an active remote session.

1. On the main remote control screen, tap the Gear (Settings) icon.

   The Settings page is displayed.

2. Change Blank Screen to On.

   Tip: Having trouble turning this feature on? Probably the host computer is waiting for you to install the driver that allows this feature to work. Switch to the host computer and install the required driver.
The host computer’s monitor will be blank during the remote session. Anyone sitting at the remote location will see a blank screen. Your actions remain unobserved.

3. Change Lock Keyboard to On.
   The host computer’s keyboard will be locked during the remote session. Anyone sitting at the remote location will be unable to use the host keyboard.

4. Save your settings.

If you do not want to be notified each time you use Screen Blanking or Lock Keyboard, change the Screen Blanking and Keyboard Lock options to Off in the Notifications section.

**Tips for Improving Your Experience**
Change display properties and network speed to maximize response times or simply to make it easier to view and navigate the remote screen.

**How to Change Display Color Quality**
Adjust the color quality of the remote screen to optimize performance by changing the amount of information transferred during remote control.

You can only change this setting during an active remote session.

Adjust color settings to change the look of the screen during remote control. The change does not impact the host computer itself.

1. On the main remote control screen, tap the Gear (Settings) icon.

   ![Gear Icon]

   The Settings page is displayed.

2. Tap Color Quality.
• For better image quality, select **Low quality** or **Medium quality**.
• For best image quality and performance, select **HD quality**.

**Remember:** A *Plus* or *Premier* subscription is required to use this feature.

**Tip:** HD quality provides the least amount of latency and the smoothest transition with an automatically adjusting resolution.

• We recommend using **Auto**.

3. Save your settings.

This setting will be remembered and applied the next time you connect to the same computer.

**How to Change Display Resolution**
Change the display resolution of the host computer to improve your remote control experience.

You can only change this setting during an active remote session.

1. On the main remote control screen, tap the **Gear (Settings)** icon.

   The **Settings** page is displayed.

2. Tap **Resolution**.

   The list of available screen resolution settings is displayed.

3. Tap the preferred screen resolution.

4. Tap **Settings**.

   This setting is applied to the host computer.

5. Save your settings.

The new setting will be in effect. Anyone sitting at the host will immediately experience the resolution change. When you end the remote control session, the host computer's screen resolution will return to its previous state.

This setting will be remembered and applied the next time you connect to the same computer.

**How to Set Network Speed**
You can select your network connection type to maximize remote control performance.

You can only change this setting during an active remote session.

1. On the main remote control screen, tap the **Gear (Settings)** icon.

   The **Settings** page is displayed.

2. Tap **Network Speed**.

   • Select **Slow** to optimize your connection on lower speed connections.
- Select **Fast** to fully exploit high bandwidth connections.
- Select **Auto** to allow LogMeIn to set this connection automatically according to the kind of connection it detects.

3. Save your settings.

### How to Protect Connection for Remote Control and File Manager

You can prevent your Remote Control and File Manager sessions from closing by setting a session timeout.

1. Tap the **Gear (Settings)** icon. The **Settings** page is displayed.
2. Slide **Show warning before timeout** to **ON** to display a warning one minute before your session times out. The warning message reads: _Open now to keep active sessions._
3. Save your settings.

### File Management

#### File Manager from a PC or Mac

**How to Transfer Files Between Computers using File Manager**

Transferring files between computers is as easy as selecting files and dragging them to the appropriate folder. Otherwise, use the appropriate options on the File Manager toolbar.

**Remember:** A **Plus** or **Premier** subscription is required to use this feature.

To access File Manager, click the File Manager icon on the **Computers** page or on the LogMeIn left menu once connected to the host.

**Tip:** Use the simplified File Manager toolbar to show only basic file operations. You can change how the toolbar is displayed at any time in the host preferences under **Preferences > General > Appearance** by selecting **Use simplified File Manager**.
Important: Directory symbolic links, directory junctions, and file symbolic links cannot be transferred through File Manager.

<table>
<thead>
<tr>
<th>Option</th>
<th>Icon</th>
<th>Shortcut</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td><img src="image" alt="Copy Icon" /></td>
<td>Ctrl+C</td>
<td>Copy the selected file or folder from the existing location to the selected new location. The copied file or folder is now in both locations.</td>
</tr>
<tr>
<td>Move</td>
<td></td>
<td>Ctrl+X</td>
<td>Cut a file or folder from the existing location and move it to the new location. The moved file or folder is now only in the new location.</td>
</tr>
<tr>
<td>Synchronize</td>
<td><img src="image" alt="Synchronize Icon" /></td>
<td>Ctrl+S</td>
<td>Update the current folders to the client and host so that their contents are the same. Files and folders that exist only on one side are copied normally. If both folders contain one or more files that are different on the client and host, the newer version will be copied that is the one with the most recent modified date. The folders must be open, not simply selected.</td>
</tr>
<tr>
<td>Replicate</td>
<td><img src="image" alt="Replicate Icon" /></td>
<td>Ctrl+R</td>
<td>Files and folders that do not exist in the destination folder are copied normally. Files that already exist in the destination folder will be differentially transferred from the source folder. If a destination folder contains a file or a folder that does not exist in the source it will be deleted from the destination. This is very useful if you update the Source folder and want to push those changes to the Destination.</td>
</tr>
</tbody>
</table>

How to Navigate and Sort Files using File Manager

Navigate and Sort options are accessed via a drop-down menu on the File Manager toolbar. Shortcut keys are available for each item.

**Remember:** A Plus or Premier subscription is required to use this feature.

**Note:** The host computer's files are displayed in the right frame, the client computer's in the left. Use the Tab key to switch between the two frames.

To access File Manager, click the File Manager icon on the Computers page or on the LogMeIn left menu once connected to the host.
<table>
<thead>
<tr>
<th>Option</th>
<th>Shortcut (Windows client)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>F5</td>
<td>Refreshes the folders on both the client and host computer.</td>
</tr>
<tr>
<td>Up</td>
<td>Backspace</td>
<td>Moves up to the parent directory.</td>
</tr>
<tr>
<td>Drive list</td>
<td>Ctrl+Backspace</td>
<td>Displays the available root drives on the selected computer.</td>
</tr>
<tr>
<td>Select left drive</td>
<td>Alt+F1</td>
<td>Click to select the disk drive you want to view in the left pane of the File Manager window.</td>
</tr>
<tr>
<td>Select right drive</td>
<td>Alt+F2</td>
<td>Click to select the disk drive you want to view in the right pane of the File Manager window.</td>
</tr>
<tr>
<td>Go to folder…</td>
<td>Ctrl+G</td>
<td>Click this item to open a box where you can type the name of a specific folder or directory you want to view.</td>
</tr>
<tr>
<td>Sort by Name</td>
<td>Ctrl+1</td>
<td>Sort the directory contents by file name.</td>
</tr>
<tr>
<td>Sort by Type</td>
<td>Ctrl+2</td>
<td>Sort the directory contents by file type.</td>
</tr>
<tr>
<td>Sort by Size</td>
<td>Ctrl+3</td>
<td>Sort the directory contents by file size.</td>
</tr>
<tr>
<td>Sort by Date</td>
<td>Ctrl+4</td>
<td>Sort the directory contents by the date files were last modified.</td>
</tr>
<tr>
<td>Show…</td>
<td></td>
<td>Select <strong>Show folders for all users</strong>, <strong>Show hidden files</strong>, and/or <strong>Show system files</strong> in any combination.</td>
</tr>
</tbody>
</table>

**How to Edit Files using File Manager**

Edit options are accessed on the File Manager toolbar or by right clicking on a file. Shortcut keys are available for each option.

*Remember:* A Plus or Premier subscription is required to use this feature.

To access File Manager, click the File Manager icon on the **Computers** page or on the LogMeIn left menu once connected to the host.
How to Select Files using File Manager

File selection options are accessed on the File Manager toolbar. Shortcut keys are available for each option.

Remember: A Plus or Premier subscription is required to use this feature.

To access File Manager, click the File Manager icon on the Computers page or on the LogMeIn left menu once connected to the host.
<table>
<thead>
<tr>
<th>Option</th>
<th>Icon (Windows client)</th>
<th>Shortcut (Windows client)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select files</td>
<td>+</td>
<td>+ (on the numeric keypad)</td>
<td>Opens a dialog box you can use to select multiple files</td>
</tr>
<tr>
<td>Unselect files</td>
<td>-</td>
<td>- (on the numeric keypad)</td>
<td>Opens a dialog box you can use to clear selected files</td>
</tr>
<tr>
<td>Select all</td>
<td>Ctrl+A</td>
<td></td>
<td>Selects all files in the current location</td>
</tr>
<tr>
<td>Select none</td>
<td>Ctrl+- (on the numeric keypad)</td>
<td></td>
<td>Clears all selections in the current location</td>
</tr>
<tr>
<td>Invert selection</td>
<td>*</td>
<td>* (on the numeric keypad)</td>
<td>Change the current selection status to its opposite (any selected item becomes cleared and any unselected items becomes selected)</td>
</tr>
</tbody>
</table>

**Example: How can I select or unselect files with the file selector?**

The following list provides examples of using the file selector feature of the File Manager:

<table>
<thead>
<tr>
<th>What to select</th>
<th>Syntax in the file selector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select all files.</td>
<td>*</td>
</tr>
<tr>
<td>Select all files and folders.</td>
<td>*</td>
</tr>
<tr>
<td>Select all .exe files in a directory.</td>
<td>*.exe</td>
</tr>
<tr>
<td>Select all files and folders, then unselect</td>
<td>1. Click <strong>Select files</strong> and then enter *</td>
</tr>
<tr>
<td>all .jpg files.</td>
<td>2. Click <strong>Unselect files</strong> and then enter * .jpg</td>
</tr>
</tbody>
</table>

**Important:** You can only unselect complete directories, not files within directories.

**File Manager from a Phone or Tablet**

**Getting Around in File Manager on a Phone or Tablet**

**Remember:** A *Plus or Premier* subscription is required to use this feature.

File Manager is available for both iOS and Android.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch between open pages</td>
<td>Tap the pages icon. Tap the page you want to view.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch between open pages</td>
<td>Tap the pages icon. Tap the page you want to view.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Open Local Files</td>
<td>Tap the <strong>Local Files</strong> page to view files that are available on your phone or tablet.</td>
</tr>
<tr>
<td>Open File Manager</td>
<td>Tap <strong>My Computers</strong>, tap a computer, and then tap the <strong>File Manager</strong> button.</td>
</tr>
</tbody>
</table>
| View a file            | To open a file, double-tap it. You should be able to open these common file types on most devices:  
• iWork documents  
• .jpg, .tiff, .gif, .png (images)  
• .doc and .docx; .xls and .xlsx; .ppt and .pptx (Microsoft Office)  
• .htm and .html (web pages)  
• .key; .numbers  
• .pages  
• .pdf  
• .txt; .rtf  
• .vcf  
• .csv  
• .aac  
• .mp3  
• .aiff  
• .wav  
• .m4v  
• .mp4  
• .mov  
• .avi |
| Drill down into folders| To see the contents of a folder, double-tap it or tap the arrow icon. |
| Move back a level       | To move back, tap a folder at the top of the page. |
| Other options          | Add a new folder, sort the files in a folder, or select all files in a folder. |

**How to Copy Files from a Phone/Tablet to a Computer or Cloud**

You can transfer files and folders from your phone or tablet to your PC or Mac. On an iOS device, you can also transfer to a cloud storage service.

**Remember:** A *Plus* or *Premier* subscription is required to use this feature.

1. Select the files you want to copy from the **Local Files** on your device. Here's how.
   a) Tap the pages icon.
   b) Tap the **Local Files** page.
   c) Tap your way to the files you want to copy.
   d) Tap each file or folder you want to copy.
Tip: You can copy photos and images (.jpg, .jpeg, .tif, .tiff, .gif, .png, .bmp, .bmpf, .ico, .cur, .xbm) just as you would any other file.

2. Choose the action to perform. In this case, Copy.
   The package of copied files is created.

3. Choose a destination.
   - To copy to a computer, go to the My Computers page, find the computer that will receive the files, and tap the File Manager button.
   - To copy to a cloud storage service, go to My Cloud Bank and select a service. Only available on iOS devices!

4. Drop the package of files at the chosen destination. Here's how.
   a) Tap your way to the location where you will paste the files.
   b) Tap Drop Here.

Your files are copied.

Tip: You can store files using LogMeIn Files by tapping on LogMeIn Files.

Tip: On iOS, you can use iTunes File Sharing to move files into LogMeIn Documents (called Local Files on your device). From there, you can transfer them easily to your LogMeIn computers or to a cloud storage service. This may not be available if you are using an older iPhone or iPod touch.

How to Copy Files to a Phone or Tablet
You can transfer files and folders from your computer or cloud to your phone or tablet.

Remember: A Plus or Premier subscription is required to use this feature.

1. Select the computer or cloud with the files you want to copy. Here's how.
• To copy from a computer, go to the My Computers page, select the computer with the files you want to copy, and tap the File Manager button.

• To copy from a cloud storage service, go to My Cloud Bank and select a service. Only available on iOS devices!

2. Choose the files you want to copy.
   a) Tap your way to the files you want to copy.
   b) Tap each file or folder you want to copy.

3. Choose the action to perform. In this case, Copy.

4. Choose a destination.
   • To copy to your device, open the Local Files page. You may need to swipe left or right to find it.
   • To copy to a computer, go to the My Computers page, find the computer that will receive the files, and tap the File Manager button.
• To copy to a cloud storage service, go to **My Cloud Bank** and select a service.

5. Drop the package of files. Here's how.
   a) Tap your way to the folder where you will paste the files.
   b) Tap **Drop Here**.

      Your files are copied.

• Image files (.jpg, .jpeg, .tif, .tiff, .gif, .png, .bmp, .bmpf, .ico, .cur, .xbm) saved to the LogMeIn Photos folder are also available in your device’s **Photo Library**.

• Only image and video files are copied to your device’s Photo Library. Other files will be copied to the **Saved From Computers** folder.

---

**How to Email Files from a Phone or Tablet**

You can send files via email from the Local Files folder on your device.

![Remember: A Plus or Premier subscription is required to use this feature.](image_url)

You can only email from the Local Files folder on your device. You cannot email from a computer or cloud.

1. Select the files on your device that you want to send in an email. Here’s how.
   a) Tap the **Local Files** page.
   b) Tap your way to the files on your device you want to email.
   c) Tap each file or folder you want to email.

2. Choose the action to perform. In this case, **Email**.
   On an iPhone or iPod touch, tap the files icon at the bottom of the screen to show the menu.
   Your default email client is displayed with the selected files attached to an email.

3. Type and send your email.

---

**Remote Management of LogMeIn Hosts**

**Who can use this feature?** The **Remote Management** feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Plus</td>
<td>• Security</td>
</tr>
<tr>
<td>• Premier</td>
<td></td>
</tr>
</tbody>
</table>

To access remote management features:

• From the LogMeIn website, go to the **Computers** page and click the **Dashboard** link.

• From the LogMeIn Client, go to the **Main Menu**. Once connected, click **Show Detailed Mode**.
Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

**Using the LogMeIn Dashboard**

Use the Dashboard to monitor Windows processes and services.

Important: This feature is only available for LogMeIn Pro, LogMeIn Central Plus and LogMeIn Central Premier subscribers. It is not available for LogMeIn Central Basic subscribers.

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

Available on Windows hosts only.

The LogMeIn Dashboard gives snapshots of multiple Windows features that can be monitored from the web browser or client app.

- **System Information**: View information about the PC, including Memory, Operating System version, and CPU type.
- **Processes**: View a list of active processes and the percentage of the CPU they are using.
- **Most Recent Accesses**: View the Windows user account most recently used to authenticate to the host.
- **Installed Hotfixes**: View emergency patches and Windows hotfixes installed on the host, if any. For more information, see this post from Microsoft.
- **Events**: View a list of the most recent events reported in Event Viewer on the host. To filter out and set exclusions for certain event types, click Set filter.
- **Network Traffic**: View information on activity and data being sent over the host's network connection.
- **Disk Drives**: View information on host's hard disks and partitions, including size and available space.
- **Scheduled Tasks**: View a list of Scheduled tasks that have run on the host, including when the tasks were last ran and when they are due to run again.
- **Journal**: Use the Journal to create and view notes about the host and/or sessions.

**Managing the Rights of Windows Users and Groups**

User Manager supports all features of Windows Computer Management for Local Users and Groups, including full Active Directory support.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Computer Management > User Manager

---

Copyright © 2019 LogMeIn, Inc.
Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Click a user on the User tab:
  - Change the password and password settings
  - Rename the user
  - Disable the account
  - Delete the user
  - Assign a Home Directory
  - Assign a Logon Script
  - Assign a Profile Path

- Click a group on the Groups tab:
  - Assign members to the group
  - Rename the group
  - Delete the group
  - Edit the Description

Monitoring Events in the Application, Security, and System Logs

LogMeIn Event Viewer supports features similar to the Windows Event Viewer, including the Application Event Log and Security Event Log.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Computer Management > Event Viewer

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Click an entry to view event details
- Clear the contents of a log file by clicking X (Clear Log) on the toolbar
- Click the Event Filter icon to filter a long list of events

Working with Services

The LogMeIn Services feature is similar to Windows Services.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.
Fastpath: Connect to a Windows computer and go to Computer Management > Services

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Select a service:
  - Click the Properties icon to view or edit details
  - Click Play to start a stopped item
  - Click Stop to stop a running item
  - Click Restart to restart a running item

Note: When specifying a user account to be used by a service, it must be in DOMAIN\USER form. Type .\USER to use a local account.

Working with Processes
The LogMeIn Processes feature is similar to the Processes tab in Windows Task Manager.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Computer Management > Processes

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

Working with Drivers

Remember: A Plus or Premier subscription is required to use this feature.
Available on Windows hosts only.

**Fastpath:** Connect to a Windows computer and go to **Computer Management > Drivers**

**Remember:** Once connected, you must be in *Detailed Mode* (Dashboard) to see remote management options.

- Select a driver:
  - Click the **Properties** icon to view or edit details
  - Click **Play** to start a stopped item
  - Click **Stop** to stop a running item
  - Click **Restart** to restart a running item

**Editing the Registry**

LogMeIn Registry Editor functionality corresponds to the Windows Registry Editor.

**Remember:** A *Plus* or *Premier* subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** Connect to a Windows computer and go to **Computer Management > Registry Editor**

**Remember:** Once connected, you must be in *Detailed Mode* (Dashboard) to see remote management options.

Registry keys (HKCR, HKCU, HKLM, etc.) are displayed in a tree structure.

- Click an item to view details
  - Click the **Plus** icon to create a new value
- Click the Key icon to change access permissions

- Click the Delete icon to remove a key

**Note:** You can edit values that are either of text (REG_SZ, REG_EXPAND_SZ or REG_MULTI_SZ) or integer (REG_DWORD) type; and REG_QWORD type values. Binary values are displayed, but cannot be edited.

**Opening the Command Prompt**

Open a fully functional command prompt on a host.

**Remember:** A Plus or Premier subscription is required to use this feature.

The Telnet client provides encryption and data compression for security and speed. It works with the ActiveX plugin (Internet Explorer) or LogMeIn Client app (Firefox 26+, Chrome 32+). A Java or HTML-based version is available as a fallback.

**Using Your Browser**

- Available on Windows hosts only.

1. Connect to a Windows computer.
   - The Dashboard panel is displayed.
2. Go to **Computer Management > Command Prompt**.

**Remember:** Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

**Using the LogMeIn Client App**

- Available on Windows hosts only.

1. Select a Windows computer from the list.
2. Click to open the command prompt.
Rebooting the Host

**Remember:** A Plus or Premier subscription is required to use this feature.

**Fastpath:** Connect to a Windows computer and go to Preferences > Advanced > Reboot Options

- **Restart LogMeIn**
  Restart the LogMeIn service. This does not reboot the host.

- **Normal Reboot**
  Close all processes and reboot the host in an orderly fashion.

- **Emergency Reboot**
  Available on Windows hosts only. Windows will shut down properly and flush all outstanding file operations to disk. Applications and other processes may not terminate gracefully, so you could lose unsaved data.

- **Hard Reboot**
  Reboot as quickly as possible. The operating system will not terminate gracefully, so you could lose unsaved data. Reboot is immediate (like pressing your computer’s reset button). You will not receive feedback from the service.

- **Safe-mode Reboot**
  Available on Windows hosts only. Restart the computer in safe-mode with networking (and LogMeIn) enabled. Safe-mode is a special way for Windows to load when there is a system-critical problem that interferes with the normal operation of Windows.

- **Scheduled Reboot**
  Schedule a date and time to automatically reboot the computer. This is useful if the reboot is not urgent and can take place during off-peak hours.

Enabling Windows Automatic Logon (autologon)

Enable autologon to bypass the Windows logon screen. Upon system startup, the system will attempt to log on to Windows with the specified autologon username and password.

**Remember:** A Plus or Premier subscription is required to use this feature.

- **Available on Windows hosts only.**

**Fastpath:** Connect to a Windows computer and go to Computer Management > Reboot

**Remember:** Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

**Caution:** Read the autologon security warning from Microsoft before using this feature.

**Note:** This is not the same as the automatic authentication feature available to LogMeIn Central subscribers. See "How to Set up Automatic Authentication" in the LogMeIn Central User Guide.

1. On the Reboot page, click Specify credentials to automatically login on the host after rebooting. The Automatic Login page is displayed.
2. Enter a User Name, Password, and a Domain.
3. Select the Automatic logon enabled box.
4. Click Apply.
5. Restart the host.

**Viewing a Host Computer Desktop without Taking Control**

Use the Monitor Host Screen feature to gain view-only access to a host computer's screen.

**Remember:** A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** Connect to a Windows computer and go to **Computer Management > Monitor Host Screen**

**Remember:** Once connected, you must be in **Detailed Mode** (Dashboard) to see remote management options.

**Working with Environment Variables**

LogMeIn Environment Variable management corresponds to Environment Variable management under System Properties in Windows.

**Remember:** A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** Connect to a Windows computer and go to **Computer Settings > Environment Variables**

**Remember:** Once connected, you must be in **Detailed Mode** (Dashboard) to see remote management options.

- Select a variable:
  - Click the **Properties** icon to view or edit details
  - Click the **Plus** icon to create a new value

**Changing Virtual Memory Settings**

LogMeIn Virtual Memory management corresponds to Virtual Memory management under System Properties in Windows.

**Remember:** A Plus or Premier subscription is required to use this feature.
Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Computer Settings > Virtual Memory

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

1. Change Minimum (Initial) size and Maximum size.

   Tip: To remove the paging file from the drive, enter 0 in both fields.

2. Click Apply.

3. Restart the host.

Changing System Time on a Host

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Computer Settings > Time

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Enter the desired values and click Apply.

   Note: Time is displayed according to time settings on the host.

Managing Shared Resources

View and manage shared resources on the host, including shared folders, administrative shares, printers, scanners, and similar.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Computer Settings > Shared Resources

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Click a folder’s Path link to open the folder in LogMeIn File Manager
- Click the Change Access Permissions button to open a dialog box where you can add new permissions or remove existing permissions for the chosen object
Setting Automatic Change Process Priorities

You can automatically update the priority class under which a process runs. This is useful for forcing lengthy, CPU-intensive tasks into the background on a machine where responsiveness of other processes is critical.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Computer Settings > Automatic Priorities

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

1. Click the Plus icon to create a new priority.
   The Automatic Priorities dialog box is displayed.
2. Enter the name of the executable in the Process Name field.
3. Choose the target priority class under Priority.
4. Select one or more Processor Affinity boxes to force a process to execute on a specific processor (or processors).
5. Click Add.

Viewing Host Performance Information

Who can use this feature? The Host Performance Information feature is available for the following:

<table>
<thead>
<tr>
<th>Basic/Plus/Premier Subscription</th>
<th>Modular Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Plus</td>
<td>• Base</td>
</tr>
<tr>
<td>• Premier</td>
<td></td>
</tr>
</tbody>
</table>

To access remote management features:

• From the LogMeIn website, go to the Computers page and click the Dashboard link.
From the LogMeIn Client, go to the **Main Menu**. Once connected, click **Show Detailed Mode**.

**Remember:** Once connected, you must be in **Detailed Mode** (Dashboard) to see remote management options.

### Viewing CPU Load

View metrics for CPU load on all processors on a host.

**Remember:** A **Plus** or **Premier** subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** Connect to a Windows computer and go to **Performance Info > CPU Load**

**Remember:** Once connected, you must be in **Detailed Mode** (Dashboard) to see remote management options.

- Hold your mouse over a graph to see when the sample was taken (each shows a different sampling frequency – 2 seconds, 10 seconds, 5 minutes, 1 hour)
- Use the numbered buttons to switch between CPUs if the host has more than one

![Graphs with buttons](image)

- Click any item in the Most CPU-Intensive Processes list to view process details

### Viewing Memory Load

View metrics for system memory load on a host.

**Remember:** A **Plus** or **Premier** subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** On the **Computers** page of the LogMeIn website, click **Dashboard** to connect to a Windows computer and then go to **Performance Info > Memory Load**

**Remember:** Once connected, you must be in **Detailed Mode** (Dashboard) to see remote management options.

- Use the drop-down list to choose the data type displayed in the graphs:
  - Memory Load
• Physical Memory Load
• Commit Memory Load

• Hold your mouse over a graph to see when the sample was taken (each shows a different sampling frequency – 2 seconds, 10 seconds, 5 minutes, 1 hour)

**Viewing Disk Space Utilization**

View metrics for disk space utilization per logical disk on a host.

**Remember:** A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > Disk Space

**Remember:** Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

• Use the drop-down list to switch between available disks
• Hold your mouse over a graph to see when the sample was taken (each shows a different sampling frequency – 2 seconds, 10 seconds, 5 minutes, 1 hour)

**Viewing Drive and Partition Information**

View details regarding physical drives and partitions and logical drives on a host.

**Remember:** A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > Drive and Partition Info

**Remember:** Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

• To manage files on a drive, click a drive link

**Viewing Open TCP/IP Ports**

**Remember:** A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

**Fastpath:** On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > Open TCP/IP Ports
Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

1. Specify the type of port(s) you want to view
   - Listening ports (ports that are listening for connections)
   - Connected ports (ports that have been connected to another computer)
   - Everything else (ports in various stages of being connected and disconnected)

2. Select Resolve IP addresses to resolve IP addresses appearing in the list of Local names. This can take a considerable amount of time to process.

3. Click Continue.
   A list of ports is displayed.

Once you have generated the list, you can change the ports you are viewing using the boxes on the toolbar and clicking Refresh.

Viewing Network Traffic Information

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > Network Load

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- To view traffic for a network, click any listed network
- To see total network traffic, click Inbound Network Traffic or Outbound Network Traffic

Viewing a List of Open Files

View a list of all files currently open on a host, along with the names of associated processes.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > Open Files

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Click a process to view process details
- To end a process, click End Process on the toolbar
Viewing a List of Registry Keys Open on a Host

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: Connect to a Windows computer and go to Performance Info > Registry Keys in Use

- Click a process to view process details
- To end a process, click End Process on the toolbar

Viewing a List of DLLs in Use

View a list of all currently loaded dynamic link libraries and the processes that use them.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > DLLs in Use

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Click a process to view process details
- To end a process, click End Process on the toolbar

Viewing LogMeIn Connection Details

Display all connections being served by LogMeIn, including the IP address and host name of any computer making a remote connection, the type of connection, and the name of the Windows user associated with the connection.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > LMI Connections.

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

Viewing Installed Applications

View a list of applications installed on a host. The list is populated from Add or Remove Programs on the host's Control Panel.
Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > Installed Applications

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

- Move your mouse over a listed application to view available data, such as estimated size, installation source, registration data, and time and date of last use
- Click any Installation Directory link to work with files in the File Manager

Viewing Loaded Device Drivers

The information is view only.

Remember: A Plus or Premier subscription is required to use this feature.

Available on Windows hosts only.

Fastpath: On the Computers page of the LogMeIn website, click Dashboard to connect to a Windows computer and then go to Performance Info > Loaded Device Drivers

Remember: Once connected, you must be in Detailed Mode (Dashboard) to see remote management options.

Configuring How LogMeIn Works on a PC or Mac

Controlling Remote Control Performance

How to Optimize a Computer for Remote Control

Available on Windows hosts only.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   - From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under Performance, set the following options (as required):
Select this option to disable the host's desktop wallpaper and all user interface effects during remote control. User interface effects include transition effects (fade, scroll), shadows under menus, trailing effects while dragging windows, and Windows Aero effects.

Select this option to make remote control sessions faster and less CPU-intensive. Do not use the display accelerator if you are having problems with Windows Aero. See also Troubleshooting Display Issues on page 241.

**Tip:** Having problems with Aero after remote control? First, make sure you end your remote control sessions from the LogMeIn toolbar (do not simply close your browser or app). If you are still having problems, turn off the display accelerator and restart your computer.

Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

3. Click OK or Apply.
   Your settings are applied immediately to the host.

### How to Set Compression for Data Transferred from the Host

Choose the compression level to apply to data transferred from the host during remote control, including files transferred using the File Manager feature.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: **Options > Preferences > Advanced**
   - From a client device, connect to the host **Main Menu** and follow this path: **Preferences > Advanced**

2. Under Network, choose the appropriate **File transfer compression** option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive</td>
<td>Dynamically modifies the compression ratio according to available bandwidth and CPU.</td>
</tr>
<tr>
<td>No compression</td>
<td>Data is not compressed.</td>
</tr>
<tr>
<td>Fast</td>
<td>Compared to Best, this option uses less host CPU, but more bandwidth. Unlike with Adaptive, the compression level is fixed.</td>
</tr>
<tr>
<td>Low</td>
<td>Keeps bandwidth and CPU usage at a minimum.</td>
</tr>
<tr>
<td>Normal</td>
<td>A good balance between effective file compression and balanced host CPU utilization.</td>
</tr>
<tr>
<td>Best</td>
<td>The host CPU will compress data as much as possible before transfer. Compared to Fast, this option uses less bandwidth, but more CPU. Unlike with Adaptive, the compression level is fixed.</td>
</tr>
</tbody>
</table>

Tip: Having problems with Aero after remote control? First, make sure you end your remote control sessions from the LogMeIn toolbar (do not simply close your browser or app). If you are still having problems, turn off the display accelerator and restart your computer.

Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

3. Click OK or Apply.
   Your settings are applied immediately to the host.

### How to Set Compression for Data Transferred from the Host

Choose the compression level to apply to data transferred from the host during remote control, including files transferred using the File Manager feature.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: **Options > Preferences > Advanced**
   - From a client device, connect to the host **Main Menu** and follow this path: **Preferences > Advanced**

2. Under Network, choose the appropriate **File transfer compression** option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive</td>
<td>Dynamically modifies the compression ratio according to available bandwidth and CPU.</td>
</tr>
<tr>
<td>No compression</td>
<td>Data is not compressed.</td>
</tr>
<tr>
<td>Fast</td>
<td>Compared to Best, this option uses less host CPU, but more bandwidth. Unlike with Adaptive, the compression level is fixed.</td>
</tr>
<tr>
<td>Low</td>
<td>Keeps bandwidth and CPU usage at a minimum.</td>
</tr>
<tr>
<td>Normal</td>
<td>A good balance between effective file compression and balanced host CPU utilization.</td>
</tr>
<tr>
<td>Best</td>
<td>The host CPU will compress data as much as possible before transfer. Compared to Fast, this option uses less bandwidth, but more CPU. Unlike with Adaptive, the compression level is fixed.</td>
</tr>
</tbody>
</table>
Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

3. Click OK or Apply.
Your settings are applied immediately to the host.

Customizing Remote Control Sessions

How to Set Remote Control Permission Defaults (Host-side User's Consent)
You can control when and how remote users will be able to start a remote session. For example, you can require the host-side user to give permission to any person attempting to log in remotely.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   - From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under Host-side user's consent, set the following options (as required).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request consent from host-side user</td>
<td>Select Request consent from host-side user to force the host user to permit or deny access whenever a client user attempts to open a remote control session. Clear this option to allow a client user to initiate a remote control session without asking for permission from the host user.</td>
</tr>
<tr>
<td>Request message</td>
<td>This text will be presented to the host user in the remote control permission dialog box. The string %USER% will be the Computer Name of the host as set at the operating system level, plus the client user's operating system account ID. The account LogMeInRemoteUser will be used on computers that have an empty administrator password.</td>
</tr>
<tr>
<td>Time to wait for user's consent</td>
<td>Enter the amount of time within which the host user must respond to the request for permission to initiate remote control. If this time expires, the setting in the If user does not respond field will be applied. Minimum 3 seconds, maximum 30 seconds.</td>
</tr>
<tr>
<td>If user does not respond</td>
<td>Choose Start Remote Control if you want the remote control session to be started even if the host user does not respond within the time set in the Time to wait for user's consent field. Choose Reject request if you want the remote control session to be refused if the host user does not respond.</td>
</tr>
<tr>
<td>Never wait for user consent in these cases</td>
<td>Select Remote user has Full Control access rights to the host computer to allow the client user to always be able to start remote control when he has Full Control rights over the host. Select Host side user is not present to allow the client user to always be able to start remote control, even when no user is logged on to the host, the host is locked, or the host screen saver is active.</td>
</tr>
</tbody>
</table>

3. Click OK or Apply.
Your settings are applied immediately to the host.
How to Set Keyboard and Mouse Priority for Remote Control
Choose the user whose data entry actions should be processed first when both users enter data simultaneously during a remote control session. Follow these steps to resolve the error Your input is being blocked.

Available on Windows hosts only.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   - From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under Interaction > Keyboard and mouse priority, choose the user whose data entry actions should be processed first when both users enter data simultaneously during a remote control session:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host side user</td>
<td>Choose this option if you want the actions of the person at the computer being controlled (the host) to be processed before the actions of the person performing remote control.</td>
</tr>
<tr>
<td>Remote user</td>
<td>Choose this option if you want the actions of the person running the remote control session (the client-side user) to be processed before the actions of the person sitting at the computer being controlled.</td>
</tr>
</tbody>
</table>

Tip: If you receive the error message Your input is being blocked while controlling a host computer, make sure Remote user is selected.

3. Click OK or Apply.
   Your settings are applied immediately to the host.

How to Set PC-to-Mac Keyboard Mapping
When controlling a Mac from a PC, you can define the behavior of special keys found only on the Windows keyboard.

Available on Mac hosts only.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   - From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under PC to Mac keyboard mapping, select one of the following options:
   - Select Alt = Alt, Windows = Command to assign the PC Alt key to equal the Mac Alt key and the Windows logo key to equal the Mac Command (“Apple”) key
   - Select Alt = Command, Windows = Alt to assign the PC Alt key to equal the Mac Command (Apple) key and the Windows logo key to equal the Mac Alt key.

3. Click OK or Apply.
   Your settings are applied immediately to the host.
How to Lock Your PC/Mac after Remote Control
Protect data on the host computer by setting the host to lock when remote control ends or is disconnected.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   - From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under Locking the Host Computer, select from the following options (as required):

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always lock the host after remote</td>
<td>Select this option to always lock the host's operating system when a remote</td>
</tr>
<tr>
<td>control</td>
<td>control session ends.</td>
</tr>
<tr>
<td>Lock when connection has been lost</td>
<td>Select this option to lock the host's operating system if the client</td>
</tr>
<tr>
<td></td>
<td>disconnects during remote control.</td>
</tr>
<tr>
<td>Lock when connection has been</td>
<td>Select this option to lock the host's operating system if the client</td>
</tr>
<tr>
<td>timed out</td>
<td>connection times out during remote control (see also How to Set Remote</td>
</tr>
<tr>
<td></td>
<td>Control Time-out on page 184).</td>
</tr>
</tbody>
</table>

3. Click OK or Apply. Your settings are applied immediately to the host.

How to Set Remote Control Time-out
Set the amount of time that can pass without activity in LogMeIn before a remote control session is disconnected.

Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Advanced
   - From a client device, connect to the host Main Menu and follow this path: Preferences > Advanced

2. Under Network, set the Idle time allowed.
3. Click OK or Apply. Your settings are applied immediately to the host.

How to Record Remote Control Sessions
Set LogMeIn to record and save a video file of each remote control session with the host.

Windows
Available on Windows hosts only.

Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.
1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Advanced
   - From a client device, connect to the host Main Menu and follow this path: Preferences > Advanced

2. Under Screen Recording, select Record screen content of Remote Control sessions.

3. You can also choose from the following actions and options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video format</td>
<td>Choose RCREC to save files using LogMeIn's proprietary RCREC format. Choose AVI to use the standard AVI format. File size will be similar for both recording types.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> To view RCREC recordings, you must convert them to AVI format with the Rescue AVI Converter, which is designed for LogMeIn Rescue, but works with LogMeIn as well.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Remote Control sessions in HD mode are recorded in WebM format. When you switch from HD to another resolution, the HD quality recording is closed and your lower quality Remote Control session is recorded into a new file. This file will have the video format you have originally selected (AVI or RCREC). Similarly, when you switch to HD resolution, the recorded AVI or RCREC file is closed and a new WebM file is created.</td>
</tr>
<tr>
<td>Location of video files</td>
<td>Specify the location where video files will be saved. Type a path to an available directory or click Browse to define a location on the host. The default location is C:\Program Files\LogMeIn\x86</td>
</tr>
<tr>
<td>View files</td>
<td>Click to view a list of available recordings.</td>
</tr>
<tr>
<td>Convert RCREC files to AVI</td>
<td>Click to open the RCREC to AVI Conversion Wizard. Follow all on-screen instructions.</td>
</tr>
<tr>
<td>Delete old files if folder size exceeds</td>
<td>Select this option to automatically delete the oldest archived RCREC remote control recordings when the total size of all RCREC recordings in the Location of video files exceeds the defined value. AVI files are not counted toward the limit and will not be deleted.</td>
</tr>
</tbody>
</table>

4. Click OK or Apply.
   Your settings are applied immediately to the host.

All remote control sessions will be recorded and saved in the chosen file format to the defined location.

**Important:** All sessions will be recorded without exception until recording is disabled. To disable recording, clear the Record screen content of Remote Control sessions option and apply the change.
Advanced Host Settings

How to Display/Remove the LogMeIn System Tray Icon

- Available on Windows hosts only.

1. Access the host preferences:
   • From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   • From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under Appearance, clear the Show the LogMeIn icon next to the clock option to remove the icon.
3. Click OK or Apply.
   Your settings are applied immediately to the host.

How to Prevent LogMeIn Notification Messages from Appearing

You can choose to suppress all LogMeIn messages communicated from the system tray. This is useful when messages could possibly disrupt the end-user experience, such as on a kiosk.

1. Access the host preferences:
   • From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   • From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under Appearance, select the Disable LogMeIn notification messages option to suppress all LogMeIn messages communicated from the system tray.
3. Click OK or Apply.
   Your settings are applied immediately to the host.

How to Configure Proxy Settings

Specify the proxy server LogMeIn will use as an intermediary between your web browser and the Internet.

💡 Tip: Proxy servers are primarily used by companies and organizations. Home users generally will not need this option.

1. Access the host preferences:
   • From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Advanced
   • From a client device, connect to the host Main Menu and follow this path: Preferences > Advanced

2. Under Proxy Settings, set the following options:
### Option

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy server address &amp; port</strong></td>
</tr>
</tbody>
</table>

**Tip:** To find your proxy address and port in Internet Explorer, go to Internet Explorer > Tools > Internet Options > Connections > LAN Settings; or click Get proxy settings to retrieve available proxy settings.

**Note:** Uncheck the box next to Use automatic configuration script. Instead, you should manually enter the proxy as an IP address and make sure the proxy port number is also set.

| **Proxy user name** | Complete this field if the proxy server requires authentication. |
| **Proxy password** | Complete this field if the proxy server requires authentication. |

3. Click OK or Apply.

Your settings are applied immediately to the host.

---

### How to View LogMeIn Event Log Files

The host will always log the following events to the application log:

- Service Start/Stop
- Login/Logout
- Remote Control Start/Stop

Follow this procedure to view log files:

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Advanced
   - From a client device, connect to the host Main Menu and follow this path: Preferences > Advanced

2. Under Event Logs, click the View Files button.
   A list of available log files is displayed.

3. On the list, double-click the file you want to view.
   - The active log file is named LogMeIn.log
   - Older logs are stored with the naming convention LMIYYYYMMDD.log (example: the log file for January 10, 2009, would be LMI20090110.log)
   - On a Windows host, click Download all logs in one compressed file to access all available logs in a single compressed archive

4. You can also set the following options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of event logs</td>
<td>Define the folder where the files are to be saved. Leave blank to use the default location (the LogMeIn installation directory, typically <code>C:\Program Files\LogMeIn</code>).</td>
</tr>
<tr>
<td>Keep event logs for</td>
<td>Enter the number of days for which you would like to store log files.</td>
</tr>
<tr>
<td>Enable debug-level logging</td>
<td>Select this option to include system events in the LogMeIn.log file. This facilitates LogMeIn troubleshooting efforts.</td>
</tr>
</tbody>
</table>

5. Click **OK** or **Apply**. Your settings are applied immediately to the host.

**How to Set LogMeIn to Check for Software Updates**
Set LogMeIn to check for and install the latest version of the LogMeIn host software upon log in to your account.

*Can't access this feature?* If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

1. Access the host preferences:
   - From the host computer, open the **LogMeIn Control Panel** and follow this path: **Options > Preferences > Advanced**
   - From a client device, connect to the host **Main Menu** and follow this path: **Preferences > Advanced**

2. Under **Software Updates**, select **Download and install updates automatically** to set LogMeIn to check for and install the latest version of the LogMeIn host software upon log in to your account.

3. Click **OK** or **Apply**. Your settings are applied immediately to the host.

**How to Set LogMeIn (LMI Guardian) to Report Software Errors**
LMI Guardian.exe is LogMeIn's error reporting component. It documents and records errors that occur in the LogMeIn host software and allows error details to be sent directly to our development team for analysis.

The Guardian does not gather or report any personal information.

Follow this procedure to control how and when the Guardian will send error notifications to LogMeIn.

*Available on Windows hosts only.*

1. Access the host preferences:
   - From the host computer, open the **LogMeIn Control Panel** and follow this path: **Options > Preferences > Advanced**
   - From a client device, connect to the host **Main Menu** and follow this path: **Preferences > Advanced**

2. Under **Software error reporting**, choose one of the following options:
Option | Description
--- | ---
Always send an error report | An error report will always be sent (no user action required).
Never send an error report | An error report will never be sent.
Ask the user what to do | The user will be prompted to send an error report and can choose to send the report or not.

Can't access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

![LogMeIn Guardian error message](image)

**Figure 24: Sample LogMeIn Guardian detected error message**

3. Click **OK** or **Apply**.
   Your settings are applied immediately to the host.

**Controlling Access to Host Computers**

**How to Add Extra Security using a Personal Password**

Use a personal password to create an extra layer of security for a host computer.

1. Access the host preferences:
   - From the host computer, open the **LogMeIn Control Panel** and follow this path: **Options** > **Preferences** > **Security**
   - From a client device, connect to the host **Main Menu** and follow this path: **Preferences** > **Security**

2. Under **Personal Password**, enter your personal password and then enter it again to confirm.

   **Tip:** The personal password must be at least 6 but no longer than 15 characters and can only contain the Latin characters A-Z, a-z; and numbers 0-9.

3. Click **OK** or **Apply**.
   Your settings are applied immediately to the host.
When you next connect to this computer from this account you will be prompted to enter a subset of characters from the Personal Password before being granted access. Upon entering the correct characters (for example, the first, the fourth and the seventh) you are granted access.

Figure 25: Sample Personal Password dialog box for password

**Securing Host Computers with RSA SecurID**

To add an extra layer of security over the simple username/password authentication, you can configure LogMeIn host software to require RSA SecurID authentication.

- Available on Windows hosts only.
- Supported versions of RSA SecurID Authentication Agent: 7.1.x; 7.0.x; 6.4.x; 6.1.x. Currently not supported: 7.2.1. For information on the RSA SecurID product, visit [www.rsa.com](http://www.rsa.com).

To activate this feature, follow this procedure:

1. Set up an RSA SecurID server (RSA Authentication Manager).
2. Set up RSA ACE Client software on each computer that will use RSA authentication.
3. On each computer that will use RSA authentication, click **Start > Control Panel > RSA ACE Client settings**. Configure the service.
4. If you have the RSA software installed on the host computer, open the LogMeIn Control Panel and click **Options > Preferences > Security > RSA SecurID**. The **RSA SecurID Authentication** window is displayed. Use this window to set the following options:
   - **Disabled**: When this option is selected, LogMeIn will not prompt for a SecurID during logon
   - **Required for all users**: When this option is selected, all users will be prompted for a SecurID during logon
   - **Required for specified users**: When this option is selected, only specified users will be prompted for a SecurID during logon
   - **Fail authentication attempts if the RSA SecurID server is not available**
   - **Force User ID to match Login Name**
   - **Use Domain name in User IDs**
5. Click **Apply** to save your settings.
Using IP Filters to Restrict Access

How to Create an IP Filter Profile
Create IP Filter Profiles to allow or deny connections to a host from specific IP addresses.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Security
   - From a client device, connect to the host Main Menu and follow this path: Preferences > Security

2. Under IP Address Filtering, click Edit Profiles to begin creating a filter profile.
   The IP Filtering dialog box is displayed.

3. Type a Name for your filter and click Add a new profile.

4. Choose a filter type:
   - Choose allow to make a filter that allows specified addresses to access this host
   - Choose deny to make a filter that prevents specified addresses from accessing this host

5. Under Address, enter the IP address you want to allow or deny.
   Accepted wildcards are an asterisk (*) that matches any number of characters, and a question mark (?) that matches a single character only.

6. Enter a Subnet that you want to allow or deny.

7. Click Add filter.
   The filter is added to the IP Filters in Profile box.

8. Repeat from step 2, above, to add additional filters to the Filter Profile.

   **Important**: Filters are checked in the order they are listed in the IP Filters in Profile box. Ordering is crucial. Use the up and down arrows next to the IP Filters in Profile box to set proper order.

9. Click OK when you are finished adding filters to the Profile.
   Your Filter Profile is saved and you are returned to the IP Filtering page.

10. You must apply your Filter Profile before it can take effect. On the IP Filtering page, select a Filter Profile from the Profiles list and click Use Profile.
    The Filter Profile is activated on the host.

When a connection is made to the host, the remote IP address will be checked against the filter or filters in the applied Filter Profile. Access will be granted or denied accordingly.

IP Filtering Examples
These examples will help you understand how to use the IP Filtering feature.

**IP Filtering Example 1**
Allow connections from IP address 215.43.21.12 and the network 192.168.0.0, and deny all other connections.

```
ALLOW 215.43.21.12
ALLOW 192.168.0.0 (255.255.0.0)
```
IP Filtering Example 2

Allow connections from IP address 215.43.21.12 and the network 192.168.0.0, but not from the address 192.168.0.12, and deny everything else.

ALLOW 215.43.21.12
DENY 192.168.0.12
ALLOW 192.168.0.0 (255.255.0.0)

-or-

ALLOW 192.168.*
DENY.*

Note: Denying the connection from 192.168.0.12 comes before allowing connections to the 192.168.0.0 network. If LogMeIn was to find the ALLOW item first, it would let IP address 192.168.0.12 through, since it matches the condition. To prevent this, the address 192.168.0.12 is checked before the network to which it belongs.

IP Filtering Example 3

Allow all connections, except those coming from 192.168.0.12

DENY: 192.168.0.12

IP Filtering Example 4

Deny all connections from the network 192.168.0.0 except for the subnet 192.168.12.0; allow all other connections

ALLOW: 192.168.12.0 (255.255.255.0)

-or-

ALLOW: 192.168.12.*
DENY: 192.168.0.0 (255.255.0.0)

-or-

DENY: 192.168.*

Detecting and Locking out Potential Intruders

Set up a Denial of Service filter and an Authentication Attack filter to help detect and temporarily lock out potential intruders.

Tip: You can view failed login attempts and lockouts in the log file if you have logging enabled.

How to Set up a Denial of Service Attack Blocker

Use the Denial of Service attack blocker as a precaution against unwanted intruders who slow your host machine by continuously requesting the same service.

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Security
• From a client device, connect to the host Main Menu and follow this path: Preferences > Security

2. Under Intrusion control, click Show Details and set the following Denial of Service attack blocker options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select this option to activate the attack blocker.</td>
</tr>
<tr>
<td>Number of invalid HTTP requests allowed</td>
<td>Specify the number of HTTP requests to allow before the offending IP address is locked out.</td>
</tr>
<tr>
<td>Reset invalid attempt counter after</td>
<td>After the amount of time specified in this box has elapsed, the invalid attempt count of the offending IP address will be reset to zero.</td>
</tr>
<tr>
<td>Keep attacker blocked for</td>
<td>All attempted connections from an offending IP address will be rejected for the amount of time specified in this field.</td>
</tr>
</tbody>
</table>

3. Click OK or Apply. Your settings are applied immediately to the host.

To allow access from blocked addresses, click Unblock all.

How to Set up an Authentication Attack Blocker

Use the Authentication Attack blocker to lock out those who try to get past your host logon screen without authorization.

1. Access the host preferences:
   • From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Security
   • From a client device, connect to the host Main Menu and follow this path: Preferences > Security

2. Under Intrusion control, set the following Authentication attack blocker options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Select this option to activate the attack blocker.</td>
</tr>
<tr>
<td>Number of invalid attempts allowed</td>
<td>Specify the number of invalid authentication attempts to allow before the offending IP address is locked out.</td>
</tr>
<tr>
<td>Reset invalid attempt counter after</td>
<td>After the amount of time specified in this box has elapsed, the invalid attempt count of the offending IP address will be reset to zero.</td>
</tr>
<tr>
<td>Keep attacker blocked for</td>
<td>All attempted connections from an offending IP address will be rejected for the amount of time specified in this field.</td>
</tr>
</tbody>
</table>

3. Click OK or Apply. Your settings are applied immediately to the host.

To allow access from blocked addresses, click Unblock all.
Controlling Who can Access your Host Computers (User Access Control)
An attempt to log in without proper User Access Control permissions may result in error 4320 ("Operator or Administrator has refused the request").

What type of user can access LogMeIn host computers?
• Users with Administrator credentials on the host computer (at the operating system level)
• Non-administrator users who have been granted permission to access the host via the User Access Control feature in LogMeIn

What happens if a user without proper permission attempts to connect?
An attempt to log in without proper User Access Control permissions may result in error 4320 ("Operator or Administrator has refused the request").

How does this relate to my LogMeIn account?
User Access Controls apply to a Windows or Mac account, not a LogMeIn account. A LogMeIn user may be able to see a computer listed in his LogMeIn account, but still may not have permission at the operating system level to actually access the host.

An Example
User Access Controls give you extra control over the actions members of your organization can take on specific host computers.

• Assume you have a server called "Server One"
• "Server One" is accessible through your LogMeIn Central account
• "Technician1" and "Technician2" are Users of your LogMeIn Central account.
• "Server One" has three Windows user accounts: (1) Administrator (2) Technician1 and (3) Technician2
• "Technician1" and "Technician2" are set as Standard or Restricted Users of "Server One"
• You, as an Administrator, log in to LogMeIn Central and access "Server One"; you authenticate to "Server One" using your Administrator Windows credentials
• "Technician1" or "Technician2" will only be able to log on to "Server One" using their "Technician1" or "Technician2" credentials once you, the Administrator, have logged on to "Server One" and set the proper User Access Controls in LogMeIn

How to Specify User Access Rights
User Access Controls apply to a Windows or Mac account, not a LogMeIn account. A LogMeIn user may be able to see a computer listed in his LogMeIn account, but still may not have permission at the operating system level to actually access the host.

1. Access the host preferences:
   • From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Security
   • From a client device, connect to the host Main Menu and follow this path: Preferences > Security
2. Under User Access Control, select from the following general options:
### Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow full control to administrators</td>
<td>Select this option to grant full permissions to anyone with administrative rights on the host computer.</td>
</tr>
<tr>
<td>Hide list of domains on the Remote Access login screen</td>
<td>Available on Windows hosts only. Select this option to clear the list of active domains in the host authentication dialog box. This provides an extra layer of security by forcing the remote user to type the exact name of the chosen domain.</td>
</tr>
</tbody>
</table>

#### Option

3. **Under User Access Control**, click **Show details**. The User Access Controls dialog is displayed.

4. In the **Name** field, type (or browse for) the name of the user for whom you want to set permissions.

5. Set the user's permissions using the following options. Some options are only available on computers running LogMeIn Pro.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>Give the user full control over all features.</td>
</tr>
<tr>
<td>Compact view only</td>
<td>Limit the host user to Main Menu view of the HTML interface (as opposed to the Dashboard).</td>
</tr>
<tr>
<td>Use IP filter profile</td>
<td>Use this drop-down list to apply an existing IT filter profile to this user. This allows you set the IP address (or range) from which the user can access the host.</td>
</tr>
<tr>
<td>Login</td>
<td>Allow the user to log into the host. By revoking this permission, you can temporarily disable a user's access to the host without having to clear any other permissions.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Allow the user to read (view-only) or write (change) settings under the Preferences menu.</td>
</tr>
<tr>
<td>Event Viewer</td>
<td>Allow the user to read (R) or delete (D) Windows event logs.</td>
</tr>
<tr>
<td>File System</td>
<td>R: Allow the user to list drives, folders and files; read and download files; view file attributes, shared folder information and access control lists; and use File Manager</td>
</tr>
<tr>
<td></td>
<td>W: Allow the user to copy, paste, rename and edit files; create and share folders; edit attributes and access control lists</td>
</tr>
<tr>
<td></td>
<td>D: Allow the user to delete files; remove shares; and disconnect users from shared files</td>
</tr>
<tr>
<td>Registry</td>
<td>R: Allow the user to view registry keys and values; list installed applications</td>
</tr>
<tr>
<td></td>
<td>W: Allow the user to create and rename registry keys; add and change registry values</td>
</tr>
<tr>
<td></td>
<td>D: Allow the user to delete registry keys and values</td>
</tr>
<tr>
<td>Performance Data</td>
<td>Allow the user to view running processes/services/drivers, change process priorities and service startup parameters, and create/delete scheduled tasks.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reboot</td>
<td>Allow the user to restart, initiate and schedule system reboots, and hard-reset the computer.</td>
</tr>
</tbody>
</table>
| Remote Control         | • R: Allow the user to view and monitor the host desktop and chat with a host user  
                             • W: Allow the user to view and control the remote desktop  
                             • D: Allow the user to take control over the remote desktop without the interactive user’s permission |
| Whiteboard             | Allow access to the Whiteboard feature during Remote Control.                                                                                |
| Chat                   | Allow access to the Chat feature.                                                                                                           |
| User/Group Accounts    | • R: Allow the user to see which Windows or Mac users and groups have access rights to the host  
                             • W: Allow the user to grant access rights to Windows or Mac users and groups and to modify their access rights  
                             • D: Allow the user to delete Windows or Mac users and groups from the list of users for the host |
| System Configuration   | • R: Allow the user to list and view system configuration data, such as environment variables, virtual memory settings, drive and partition information and network adapters  
                             • W: Allow the user to modify system configuration data, such as environment variables, virtual memory settings, drive and partition information and network adapters  
                             • D: Allow the user to delete environmental variables |
| Command Prompt         | Allow access to the host Command Prompt feature.                                                                                          |
| Processes              | • R: Allow the user to view running processes, services and drivers; list DLLs and objects that these processes use; and view scheduled tasks  
                             • W: Allow the user to change process priorities and service startup parameters; control services; create and modify scheduled tasks  
                             • D: Allow the user to terminate running processes and services; delete scheduled tasks |
| Desktop Sharing        | Allow the user to use the Desktop Sharing feature.                                                                                       |

6. Click **Add**.  
The user is added to the User list.  
7. Click **OK** to exit the User Access Control dialog box.  
8. Click **OK** or **Apply**.  
   Your settings are applied immediately to the host.
Ad Hoc Support: Accessing Unmanaged Computers

The ad hoc support feature provides one-time access to remote Windows PCs that have not been added to your account ("unmanaged" computers with no LogMeIn host software installed).

This guide helps technicians through the process of remotely supporting their customers using the ad hoc support feature.

**Tip:** To better understand your customer's experience, see the *Ad Hoc Support Step-by-Step Connection Guide*.

**Important:** You must have an available seat in your account to conduct ad hoc support sessions.

**Note:** Not available for trial subscriptions.

Ad Hoc Support in a Nutshell

1. Support provider sets up a new session in LogMeIn Central.
2. As a result of step 1, an email is sent to the user who is requesting support. It contains a deployment link that carries a pre-defined password.
3. A temporary host is installed on the user's computer.
4. The user activates the session using a security code.
5. 24 hours after activation, the session is automatically ended and the temporary host is removed from the user's computer.

**Important:** You can only provide ad hoc support to Windows PCs.

Considerations

**Important:** Consider the following when using ad hoc support:

- Users on a Windows PC must have administrator privileges in order to receive ad hoc support.
- The number of concurrent/active ad hoc support sessions is limited to one support session per user profile and five support sessions per company.
- While the session is active, the Central user can access the remote computer any number of times via Remote Control, File Manager (Plus or Premier required) or the Dashboard (Plus or Premier required).
- The session remains alive when the remote computer goes offline.
- Ad hoc support cannot be used with computers already running the LogMeIn host software.

Task One: Setting Up an Ad Hoc Support Session

**Important:** You can only provide ad hoc support to Windows PCs.
Start an ad hoc support session

Remember: Only a single ad hoc support session can be active at a time per user profile.

1. In LogMeIn Central, click Ad Hoc Support.
2. Enter the email address of the user receiving support.

```plaintext
1. Who needs help?

✉️ → 🔄 JohnDoe@acme corp.com
```

Figure 26: Step 1

3. Create a password.
   This is the password that you must enter when logging in to the user's computer once the ad hoc support session has been activated.

```plaintext
2. Create a temporary Administrator password to their Windows PC

   🔐

   Remember this password. It won't be shown again.
```

Figure 27: Step 2

Important: Take note of this password, it will not be shown again.

In Windows, the password is actually linked to a hidden Administrator account called LogMeInRemoteUser. This account is automatically removed when the session ends and the LogMeIn Support Session app is removed.

4. Click Send email and prepare session.
   The instructions and deployment link are sent to the user.

Guide your customer through setting up their computer

Remember: You can learn more about your customer's experience in the Ad Hoc Support Step-by-Step Connection Guide.

1. Wait for the user to download and run the LogMeIn Support Session app.
2. Provide the user with the security code.

**Important:** Stay on this page and wait while the user's computer is set up for the session. Alternatively, make sure to take note of the security code before navigating to another page. It will not be shown again.

3. Ask the user to enter the security code when prompted. The security code is required to pair the user's computer with your account.

**Tip:** Is your user having trouble? See this article for tips: *Ad Hoc Support Troubleshooting* on page 200.

The session becomes activated once the user has entered the security code and the LogMeIn Support Session app has been set up.

**Remember:** A session is valid for 24 hours from the time of activation. During this period, the remote computer can be accessed any number of times from the *Ad Hoc Support Sessions* computer group on the *Computers* page.

**Task Two: Conducting an Ad Hoc Support Session**

Once an ad hoc support session is activated, the remote computer paired with your account can be accessed for 24 hours via Remote Control, File Manager or the Dashboard any number of times from the *Ad Hoc Support* page.

**Tip:** Active ad hoc support sessions are also displayed on the *Computers* page under the *Ad Hoc Support Sessions* computer group.

1. Select a method to connect to the remote computer.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Control</td>
<td>Access the remote computer. See <em>Starting Remote Control</em> on page 140.</td>
</tr>
<tr>
<td>File Manager</td>
<td>Transfer files between computers. See <em>How to Transfer Files Between Computers using File Manager</em> on page 158.</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Manage the remote computer. See <em>Remote Management of LogMeIn Hosts</em> on page 166.</td>
</tr>
</tbody>
</table>

Remember: A *Plus* or *Premier* subscription is required to use this feature.

2. Enter the password you created in Step 2 as part of the ad hoc support session setup (*Step 2* on page 199).

Tip: Select *Initiate Chat with User after login* to immediately start a conversation with the user once connected.

You are now connected to the remote computer.

To terminate the session, click *End session now* on the *Ad Hoc Support* page in Central.

Note:
- Ending a remote connection via the File Manager, Remote Control or the Dashboard does not terminate the support session.
- Sessions are active for 24 hours. After this period, the session is automatically terminated and the temporary host is removed from the remote computer. To access the computer again via ad hoc support, you must start a new session.


**Ad Hoc Support Troubleshooting**
Information to help you resolve common issues with LogMeIn Central ad hoc support.

**My user reports that the session cannot start due to an invalid security code**
User error message: *Invalid security code*
**My user reports that the session has expired.**

*User error message: This instance of the Support Session has expired.*

<table>
<thead>
<tr>
<th>Possible reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user clicked an old ad hoc support session link.</td>
<td>Ask the user to click the activation link in the most recent email you sent.</td>
</tr>
<tr>
<td>More than 24 hours has passed since the session was activated.</td>
<td>Create a new ad hoc support session.</td>
</tr>
<tr>
<td>You have manually ended the session by clicking <em>End session now</em>.</td>
<td>Create a new ad hoc support session.</td>
</tr>
</tbody>
</table>

**My user reports a Group Policy error.**

*User error message: The Group Policy you are subject to may have prevented the session from starting.*

<table>
<thead>
<tr>
<th>Possible reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have created a password for logging in to the user’s computer that does not conform to the requirements of the Group Policy to which the user is subject.</td>
<td>Create a new ad hoc support session with a password that meets the requirements.</td>
</tr>
</tbody>
</table>

*Tip:* The most common restriction applies to password length. Create a password of at least 8 characters.

**My user reports that a previous support session has not yet been completely closed.**

*User error message: A previous session has not yet been completely closed.*

<table>
<thead>
<tr>
<th>Possible reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user is attempting to launch an already active session.</td>
<td>Another technician may be in an active support session. Ask the user to check the instructions email to see who initiated the session.</td>
</tr>
<tr>
<td></td>
<td>• <em>Another technician:</em> Until the session is ended, you cannot provide support. Ask the user to contact their support provider.</td>
</tr>
<tr>
<td></td>
<td>• <em>You:</em> The remote computer is accessible via ad hoc support. No further action is required.</td>
</tr>
</tbody>
</table>

Copyright © 2019 LogMeIn, Inc.
My user reports that the LogMeIn host software is installed on the computer.

User error message: LogMeIn host software is installed on this computer.

<table>
<thead>
<tr>
<th>Possible reason</th>
<th>Solution</th>
</tr>
</thead>
</table>
| The ad hoc support feature is intended for one-time remote access of computers that are not part of your account. | Connect to the computer on the **Computers** page.  
• If the computer is not in your account, ask the user to turn to the person who installed LogMeIn host software on their computer (their LogMeIn Master Account Holder). |

I cannot launch new ad hoc support sessions.

<table>
<thead>
<tr>
<th>Possible reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The maximum number of active support sessions has been reached for your company.</td>
<td>A maximum of <strong>five</strong> support sessions can be active simultaneously per company. Try again later.</td>
</tr>
<tr>
<td>All Central seats are in use.</td>
<td>Free up at least one Central seat to start a new support session.</td>
</tr>
<tr>
<td><strong>Important:</strong> You may be able to free up seats assigned to active ad hoc sessions by deleting the computer in the <strong>Ad Hoc Support Sessions</strong> group under the <strong>Computers</strong> page. However, make absolutely sure that the computer you are deleting is not being actively supported. The <strong>Last online/Online since</strong> flags are useful indicators for determining session state.</td>
<td></td>
</tr>
</tbody>
</table>

I can no longer connect to the remote computer.

<table>
<thead>
<tr>
<th>Possible reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer restart</td>
<td>If you initiated the restart, wait for the computer to come online again.</td>
</tr>
<tr>
<td>Connectivity dropout</td>
<td>Try connecting again in a few minutes. If the issue persists, contact the user to investigate.</td>
</tr>
</tbody>
</table>
| Computer shutdown or disconnect                     | The user may have inadvertently disconnected or shut down the computer. Ask the user to check the following:  
• The LogMeIn Support Session app is running and connected.  
• The computer is turned on.  
• The computer is connected to the internet. |
The remote computer is connected to the internet, but it is inaccessible via ad hoc support.

The LogMeIn Support Session app may be actively blocked by the firewall on the remote computer. Ask the user to whitelist the app in their firewall configuration to be able to provide remote support.

Related Topics

• LogMeIn and Firewalls on page 22

About the LogMeIn API and API Key

The API Key page generates a pre-shared key (PSK) for using the LogMeIn Central API.

Remember: You need a LogMeIn Central subscription (paid or trial).

Important: You must authenticate each action you call with your CompanyID + PSK pair.

From the Configuration > API tab, click Generate to create a pre-shared key. Copy this key and use it for API functions. For more information, visit https://developer.logmein.com/api/firststeps/.
Working with LogMeIn Hamachi

Audience

This section is primarily for IT professionals implementing LogMeIn Hamachi and LogMeIn Central as part of a remote services solution for their employer or other organization.

We recommend that the reader have knowledge of the following computer networking concepts:

- Network types
- Virtual Private Networks
- Connection methods
- Network architectures
- Network topologies

LogMeIn Hamachi Fundamentals

What Is LogMeIn Hamachi?

LogMeIn Hamachi is a virtual networking service that can be set up in minutes and enables secure remote access to your business network anywhere there is an Internet connection.

Unlike traditional hardware and software based VPN systems, Hamachi is an on-demand virtual networking service that allows you to focus your time and energy on providing the remote connections your users and systems need, and not the technology or infrastructure you are using to support them.

Who Should Use LogMeIn Hamachi?

Here are a few examples of how you can take advantage of Hamachi.

IT Support: Building a Mobile Office LAN

Many mobile workers use their laptops mobile devices in the office while connected to their company’s shared resources (file servers, network printers, mail servers, etc.). But if a user moves away from the local network, he will no longer be able to access these resources. Software that is configured to work inside the office becomes useless outside the office.

Using Hamachi, mobile workers become members of a Hamachi network wherein all shared resources are also network members. As a result, network configurations can remain unchanged. Hamachi sets up exactly the same networking environment for the mobile user no matter where he is.

Tip: Hub-and-spoke and gateway are the best networking modes for this scenario.

IT Support: Setting Up Network Access for Home Workers

Home workers can be more productive when they have secure access to shared IT resources. Using the Hamachi client, home workers gain a secure tunnel directly into their company’s network. They can work from home and still access the resources they need.
Tip: Hub-and-spoke and gateway are the best networking modes for this scenario.

Outsourced IT: Managing Multiple Networks
A service provider with a number of administrators on his team wants to set up and maintain multiple Hamachi networks for multiple customers. He uses LogMeIn Central to create Hamachi networks, deploy Hamachi clients, and apply default and custom settings for each customer. He can also manage other administrators in his organization, generate client activity reports, and manage network activity.

Small to Medium Sized Organizations: Virtual LAN
Organizations without a physical LAN can use the mesh network type to set up a virtual corporate LAN.

The LogMeIn Hamachi Client
The term Hamachi client refers to both the Hamachi software itself and any computer or smartphone with Hamachi client software installed. With proper permission from network owners, Hamachi clients can become members of any Hamachi network.

Figure 28: The LogMeIn Hamachi client for Windows

Figure 29: The LogMeIn Hamachi client for Mac
A command-line version of LogMeIn Hamachi is also available for Linux and officially supported on the following distributions:

- Ubuntu 16.04 LTS or newer LTS
- CentOS 7.2 or newer

**About the Relationship Between the Client and Your LogMeIn Account**
The Hamachi client can only be used with a LogMeIn ID, as an attached member of a LogMeIn account.

**About the Hamachi Virtual IP Address**
Every Hamachi client has one virtual IPv4 (IP) address in the 25.x.x.x range and one IPv6 address. The virtual IP address is globally unique and is used to access the client from any other Hamachi network with at least one common mesh or hub-and-spoke network.

Gateway networks integrate smoothly into the LAN in terms of addressing. 25.x.x.x addresses are not available for a gateway network. Instead, the local address space is used. See also *How to Assign an IP Range for Gateway Members on Windows* on page 224.

**LogMeIn Hamachi Network Types**
LogMeIn Hamachi provides three network types for flexibility in meeting diverse use case scenarios. They differ mainly in network topology.

For information about subscription types, see *LogMeIn Hamachi Subscription Types* on page 208.

**About Mesh Networks**
In a mesh network, every member is connected to every other member.

Organizations without a physical LAN can use the mesh network type to set up a virtual corporate LAN.

Mesh is also the typical choice for gamers, because network games constantly have to broadcast their current status to all other participants in the game.

![Figure 30: Mesh network](image)

**Note:** Mesh is the only network type that can be created directly from the Hamachi client interface.

**About Hub-and-Spoke Networks**
In a hub-and-spoke network, one or more computers act as hubs, while other clients connect as spokes. Spokes connect to hubs, but never to each other.

Hub-and-spoke is typically used when a workstation (spoke) needs to connect only to servers (hubs). For example, in a library, the catalog is a hub while workstations accessing the catalog are spokes.

Hub-and-spoke is ideal if you want strict control over connections between network members.
Important: If you set every member of a hub-and-spoke network to be a hub, you essentially turn the network into a mesh network. Similarly, if you set only spokes, your members will be unable to make a connection.

About Gateway Networks
Use the gateway network type to provide transparent access to your entire network from a centralized Hamachi gateway. Members of a gateway network, such as mobile workers, will see one computer acting as a gateway towards an entire LAN, thus making all network resources accessible.

Tip: Theoretically, a hub-and-spoke network would also be a good choice for enabling mobile LAN access; however, all shared resources would also need to be running the Hamachi client and be set up as hubs. This is fine insofar as these shared resources are servers with a Hamachi compatible operating system; however, the gateway network remains the best option since Hamachi currently cannot be installed on network devices such as printers, routers, access points, etc.

Important: Mac hosts cannot act as gateway nodes.

Characteristics
The gateway network type is a hybrid of the meshed and hub-and-spoke network types:
• As in a hub-and-spoke network, one computer acts as a hub (the gateway), while members act as spokes
• There can only be one gateway, which is typically a permanently online server connected to the LAN
• The number of members is virtually unlimited since even network devices that are not running the Hamachi client can be considered members
• Each member (Hamachi client) will see the gateway and the other members of the gateway’s LAN
• Hamachi clients will not see each other in a gateway network

Restrictions
For technical and security reasons there are strict rules for both the gateway and members:
• The gateway cannot be a member of any other Hamachi network
• The gateway cannot be a workstation that is the member of a domain
• The gateway must not be a DNS and/or DHCP server since the Hamachi network bridge interferes with the DNS and DHCP services.
• Members can join more than one gateway network, but can only be online in one network at a time. Gateway members can also be members of multiple non-gateway networks

**Role of the Hamachi Client in a Gateway Network**
• Gateway network members and the gateway device itself must be running the Hamachi client
• Network devices that are physically connected to the LAN do not need to run the Hamachi client to be made accessible to gateway network members

**Addressing**
Gateway networks integrate smoothly into the LAN in terms of addressing. 25.x.x.x addresses are not available for a gateway network. Instead, the local address space is used.

**LogMeIn Hamachi Subscription Types**
Every Hamachi user must have either a paid or free subscription to join or create Hamachi networks.

*Free, Standard, and Premium* LogMeIn Hamachi subscriptions are available at the network level. You can have an unlimited number of Free, Standard, and Premium networks in your account, in any combination. Standard and Premium subscriptions are purchased for and applied to individual networks.

Regardless of the type and number of subscriptions you purchase, you can attach a maximum of 256 clients to your LogMeIn account; the number of clients is independent of the number of members per network.

<table>
<thead>
<tr>
<th>Subscription type</th>
<th>Valid for this many networks</th>
<th>Members per network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Unlimited</td>
<td>5</td>
</tr>
<tr>
<td>Standard</td>
<td>1 (purchased individually, per network)</td>
<td>32</td>
</tr>
<tr>
<td>Premium</td>
<td>1 (purchased individually, per network)</td>
<td>256</td>
</tr>
</tbody>
</table>

The *Multi-Network* subscription option is applied across an entire LogMeIn account, allowing you an unlimited number of networks with up to 256 members per network. With Multi-Network you are still subject to the limit of 256 clients per account. The number of clients allowed at the LogMeIn account level is independent of the number of members per network. This means that you can have potentially far more members in your networks than clients attached to your account.

**Tip:** When attempting to add a new client, you may be informed that you have reached your client limit. If this occurs, you must create “free space” in your account by removing an unused client. Otherwise, the client can only join your network if it is attached to another account and joins your network as a guest.

<table>
<thead>
<tr>
<th>Subscription type</th>
<th>Valid for this many networks</th>
<th>Members per network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Network</td>
<td>Unlimited</td>
<td>256</td>
</tr>
</tbody>
</table>
Tip: The current and maximum number of network members are displayed on the Hamachi client next to the name of the network. For example, 11/256 means that there are 11 members in a network that can have up to 256 members.

What if I do not want to renew my subscription?
Standard, Premium, and Multi-network subscriptions are paid subscriptions that allow you to have more than five members in your network. If your network has more than five members, you should take the following into consideration before you cancel your subscription:

• Your network will not accept any new members.
• Only five members will be active. Other members will be disabled (offline) in your network until you resolve this issue by purchasing a subscription or evicting network members.
• Your network will still be fully functional but only for five randomly selected members.
• You can renew your expired subscription any time.

What if I never had a paid subscription?
For free networks, only five members remain active and you are unable to add new members. For example, a free network that was created with 14 members before introducing Standard, Premium, and Multi-network subscriptions will be functional for five random members and will not accept new members.

Important: If you have more than five members in a network and you choose to have a free subscription, you will not be able to add new members until you remove some of them from the network.

How to Change or Purchase Hamachi Subscriptions
Depending on the size of your network you can purchase several types of subscriptions. You can buy a Hamachi subscription either from the LogMeIn website or from the Hamachi client. See LogMeIn Hamachi Subscription Types on page 208.

How to Purchase Subscriptions from the LogMeIn Website
1. On the My Networks page, click Edit next to the network you want to work with. The Edit Network page is displayed.
2. Select the Subscription tab. Your current subscription is selected.
3. Select a subscription type that you want to use or purchase.
4. Switch to the selected subscription:
   • Click Change subscription if you have already purchased the selected subscription
   • Click Buy subscription to purchase a new subscription and follow all instructions

Your changes are applied.
How to Purchase Subscriptions from the Hamachi Client

1. Do one of the following to open the LogMeIn Hamachi website:
   - Click Manage > Manage Networks.
   - If you see a blue warning icon next to the name of your network then
     1. Click the blue warning icon next to the name of the network that you want to upgrade.
     2. Click Upgrade options.

   The Hamachi website opens in your browser.

2. Log in to your LogMeIn account:
   - Click Create Account if you do not have a LogMeIn account yet and follow all instructions.
   - Click the Login link if you have a LogMeIn account.

   The subscription purchase page opens.

3. Select the type and number of subscriptions you want to buy and click Buy Now.
4. Follow all instructions to complete your purchase.

Managing LogMeIn Hamachi Clients and Networks

Hamachi Web Management Features

Any Hamachi user with a LogMeIn account can manage attached clients and networks using the LogMeIn web site (My Networks page).
- Create mesh, hub-and-spoke, and gateway networks
- Remotely manage client settings
- Manage the default settings to be applied to a new network
- Edit or delete existing networks
- Install the Hamachi client to the local computer
- Deploy the Hamachi client to a remote computer
- Manage requests to join Hamachi networks

Hamachi Client Management Features

Hamachi clients provide access to the following features:
- Create mesh networks
- Manage the default settings to be applied to a new network
- Edit or delete existing networks created on the client
- Install the Hamachi client to the local computer
- Deploy the Hamachi client to a remote computer (Not available on Linux)
- Manage requests to join Hamachi networks created on the client

Free versus Paid Subscriptions

Hamachi is free for users if they have no more than five computers per network. The paid version offers fast relays and is subject to an annual subscription fee.

For information about subscription types, see LogMeIn Hamachi Subscription Types on page 208.
LogMeIn Hamachi Security
All LogMeIn Hamachi communications are encrypted and authenticated with industry-standard algorithms and protocols. Nobody will be able to see the data transmitted between two Hamachi peers. For detailed information, see the LogMeIn Hamachi Security Whitepaper.

LogMeIn Hamachi and Firewalls
If running a firewall application, you may need to ensure that Hamachi is able to access the Internet.

Please refer to the LogMeIn Hamachi Knowledge Base for up-to-date information for working with various popular security suites.

Installing LogMeIn Hamachi

Hamachi System Requirements

Important: A LogMeIn ID is required to attach Hamachi clients to networks. For details, see How to Sign up for a LogMeIn ID on page 8.

LogMeIn Hamachi has been tested with the following operating systems:

- Windows 7 (All versions), Server 2008 r2 (All versions)
- Windows 8, 8.1 (Desktop UI only)
- Windows 10
- Windows Server 2012 (All versions)
- Windows Server 2016 (All versions)
- Windows Server 2019 (All versions)
- Mac OS 10.6 (Snow Leopard) or newer on Intel-based Macs
- Linux distributions:
  - Ubuntu 16.04 LTS or newer LTS
  - CentOS 7.2 or newer

Important: Make sure you are using up to date, officially supported third-party technology together with LogMeIn. LogMeIn is designed for use with third-party products and services (browser, OS, etc.) that are officially supported by their respective vendors and well-maintained by the end user (latest patches and updates installed).

Note: Windows RT is not supported.

Gateway Node functionality is not available on the following platforms due to limitations within the operating systems themselves:

- Mac OS
- Windows Small Business Server editions
- Any operating system deployed on Microsoft Azure
How to Install the Client to a Local Computer

Follow this procedure to download and install the Hamachi client to a local computer. The client will be attached to your LogMeIn account.

**On Windows or Mac**

**Important:** You must be logged in to the LogMeIn account to which you want to attach the new Hamachi client.

1. In LogMeIn Central, switch to Network mode and click **Add Client** on the Computers tab (My Networks).
   The **Add Client** page is displayed.
2. Select **Install LogMeIn Hamachi on this computer** and click **Continue**.
3. Click **Install LogMeIn Hamachi**.
   The Hamachi installer is launched.
4. Follow the on-screen instructions.

The client is installed on the local computer as an attached member of the active LogMeIn account. You will be able to manage this client using LogMeIn Central.

**On CentOS (Linux)**

Install Hamachi via the command line.

1. Download Hamachi using the terminal.
   ```
   wget http://www.vpn.net/installers/logmein-hamachi-2.1.0.165-1.x86_4.rpm
   
   The installer package is downloaded to your current directory.
   ```
2. Install the package.
   ```
   sudo yum install logmein-hamachi-2.1.0.165-1.x86_4.rpm
   
   The client is installed on the local computer.
   ```

**Important:** Before you can connect to a network, you must attach the client to your LogMeIn account.

1. Execute `sudo hamachi login` to log in.
2. Execute `sudo hamachi attach [email@example.com]` using your LogMeIn ID (email address) to attach your client.

**On Ubuntu (Linux)**

1. **Option 1:** Install Hamachi via the command line.
   a) Download Hamachi using the terminal.
      ```
      wget http://www.vpn.net/installers/logmein-hamachi_2.1.0.165-1_amd64.deb
      
      The installer package is downloaded to your current directory.
      ```
   b) Install the package.
      ```
      sudo dpkg -i logmein-hamachi_2.1.0.165-1_amd64.deb
      ```
2. Install the package using the Ubuntu Software app.
a) Navigate to http://www.vpn.net/.
b) Click the appropriate package to download it.
c) Open the .deb package with Software Install.
   The Ubuntu Software window is displayed.
d) Click Install.
e) When prompted, enter the admin password for elevation.

The client is installed on the local computer.

**Important:** Before you can connect to a network, you must attach the client to your LogMeIn account.

1. Execute `sudo hamachi login` to log in.
2. Execute `sudo hamachi attach [email@example.com]` using your LogMeIn ID (email address) to attach your client.

**How to Deploy the Client to a Remote Computer**

Follow this procedure to send an installation link that the recipient can use to download and install the Hamachi client. The client will be attached to your LogMeIn account.

**Important:** You must be logged in to the LogMeIn account to which you want to attach the new Hamachi client.

**Note:** This functionality is not available on Linux.

All defaults set under Configuration > Client Defaults will be applied to the new client(s).

1. In LogMeIn Central, switch to Network mode and select the Deployment tab.
2. Click Add New Link.
   The Deploy LogMeIn Hamachi to remote computer(s) (Step 1 of 2) page is displayed.
3. Type a Description that you can use to recognize your installation link.
4. In the Maximum number of remote installations box type the maximum number of computers that will be able to use the link to install the Hamachi client.
   For example, you may want to send the link to all users in an entire department.
5. In the Expiration field you may choose when you want the validity of the link to expire.
6. Select the Network(s) that you want the client to be able to access.
7. Click Continue.
   The Deploy LogMeIn Hamachi to remote computer(s) (Step 2 of 2) page is displayed.
8. Send the link to the recipient(s):
   - Click Copy to place the link onto your clipboard for you to paste into an email or instant messaging service message to send to the user(s)
   - Click Send to open your default email client with the link in the body of the message for you to send to the user(s)
   - Click Test to view the message that will be displayed when the recipient clicks the link

   The link is sent to the recipient.

The recipient must click on the installation link to actually install the client on the chosen computer. Once installation is complete, the client can be used to create and connect to Hamachi networks.
How to Install a Hamachi Client in Client-Only mode

Follow this procedure to download and install the Hamachi client without associating it with a LogMeIn account.

**Important:** Do not log in to your LogMeIn account.

**Note:** Hamachi for Linux is installed in client-only mode by default. To detach a Linux client, see *How to Detach (Delete) a Client from Your Account* on page 221.

1. Go to the LogMeIn Hamachi product page.
2. Click the **Try it free** link.
3. Do not create a LogMeIn account.
4. Click the **Download Now** link at the bottom of the page. The Hamachi installer is launched.
5. Follow all on-screen instructions. After the installation is complete, the Hamachi client starts up automatically.

How to Update the Hamachi Client

This procedure must be executed on the client.

**On Windows or Mac**

The Hamachi client software can be updated from the client itself.

By default, the Hamachi client downloads updates automatically when you restart your client or when your client is online for a week. You should download updates manually if you turn off automatic updates.

- To check whether you receive automatic updates, go to **System > Preferences > Settings** and verify that the **Enable automatic update** option is selected.
- To manually download client updates, click **Help > Check for Updates**.

**On Linux**

Hamachi for Linux can be updated manually.

1. Open the terminal.
2. Execute the following command:
   ```bash
   sudo hamachi check-update
   ```
   The Hamachi version information is displayed.
3. If your client is not up-to-date, follow the steps in this article: *How to Install the Client to a Local Computer* on page 212.
Managing LogMeIn Hamachi Clients

How to Set Default Settings for Deployed Clients

You can enforce the graphic user interface and functionality applied to new clients deployed from LogMeIn Central.

1. In LogMeIn Central, go to the Networks > Network Settings page.
2. Select the Client Defaults tab.
3. Select an Interface Mode.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>The client will offer full functionality to end users.</td>
</tr>
<tr>
<td>Restricted</td>
<td>The client will offer a full graphic user interface, but client settings (including the right to change certain settings locally) can be defined on the web only.</td>
</tr>
<tr>
<td>Minimal</td>
<td>The client will offer no graphic user interface to the end user. Only the Hamachi system tray icon will be visible. Client settings can be defined on the web only.</td>
</tr>
</tbody>
</table>

4. For Restricted or Minimal mode, select the client settings to apply.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Choose this option to provide extra protection against sniffing. For business use, we highly suggest using encryption. Use of this option may cause minimal extra CPU load for both sender and receiver.</td>
</tr>
<tr>
<td>Compression</td>
<td>Choose this option to speed up large data transfers. Compression is particularly useful on low bandwidth connections. Use of this option may cause minimal extra CPU load for both sender and receiver.</td>
</tr>
<tr>
<td>Can create new network</td>
<td>Allow the client to be used to create new mesh networks.</td>
</tr>
<tr>
<td>Can join networks</td>
<td>Allow the client to be used to join networks other than those assigned on the web.</td>
</tr>
<tr>
<td>Can chat</td>
<td>Allow the client to be used for chat between Hamachi peers.</td>
</tr>
<tr>
<td>Keep chat logs</td>
<td>Allow the client to store chat logs.</td>
</tr>
<tr>
<td>Maintain log</td>
<td>Allow the client to store a Hamachi event log.</td>
</tr>
</tbody>
</table>

5. Click Save. Settings will be applied to all new clients attached to this account.

How to Attach an Unattached Client to a LogMeIn Account

An existing Hamachi client running in Client-only mode can be attached to a LogMeIn account at any time.

On Windows

This procedure must be executed on the client.
1. On the Hamachi client under the **System** menu, select **Attach to LogMeIn account**.
   The **Attach to LogMeIn Account** dialog box is displayed.

2. Enter the **LogMeIn Account ID (email address)** of the LogMeIn account to which you want to attach the client.

3. Select **Attach networks** to attach your existing networks to the selected LogMeIn Account.

4. Click **Attach**.
   Your relationship with the selected LogMeIn account shows as Pending.

The Account Holder or administrator will see the attachment request on the **Join Requests** page for the specified LogMeIn account. The Account Holder or administrator must approve or deny the request.

Once approved, the client can be managed using LogMeIn Central. All networks that were created on the unattached client are also manageable from your LogMeIn account if they are attached to the account.

**Tip:** Another option is to send an installation link to a user with an unattached client. The user will click the link to reinstall the Hamachi client as an attached member of your account.

**Important:** You cannot attach a network to a web account that was created on an attached client. You must delete the client from the web account first and then reattach it to add all networks that were created on the client.

---

**On Mac**

On a Mac, simply log in to the Hamachi client using the LogMeIn account to which you want to attach the client, as follows:

1. On the Hamachi client, click the Power icon.
   You are prompted to sign up or log in to continue using Hamachi.

2. Click either **Log In** or **Sign Up**, as required.
   Be sure to use the LogMeIn account to which you want to attach the client.
   The Login window is displayed.

3. Enter the information requested.

4. Select either **Login** or **Create Account**, as required.
   Your relationship with the selected LogMeIn account shows as Pending.

The Account Holder or administrator will see the attachment request on the **Join Requests** page for the specified LogMeIn account. The Account Holder or administrator must approve or deny the request.

Once approved, the client can be managed using LogMeIn Central. All networks that were created on the unattached client are also manageable from your LogMeIn account if they are attached to the account.

**Tip:** Another option is to send an installation link to a user with an unattached client. The user will click the link to reinstall the Hamachi client as an attached member of your account.

**Important:** You cannot attach a network to a web account that was created on an attached client. You must delete the client from the web account first and then reattach it to add all networks that were created on the client.
On Linux

Before you can connect to a network, you must attach the client to your LogMeIn account.

1. Execute `sudo hamachi login` to log in.
2. Execute `sudo hamachi attach [email@example.com]` using your LogMeIn ID (email address) to attach your client.

How to Rename a Client On the Website

1. In LogMeIn Central, go to the Networks > My Networks page. Your Hamachi networks and clients are listed.
2. On the My Networks page, click Edit next to the client you want to work with. The Edit Client page is displayed.
3. Select the Name tab and type a new Client Name.
4. Click Save.
   If the client is online, changes are applied immediately. If offline, changes are applied when the client comes online.

How to Add/Remove a Client to/from a Network

1. In LogMeIn Central, go to the Networks > My Networks page. Your Hamachi networks and clients are listed.
2. On the My Networks page, click Edit next to the client you want to work with. The Edit Client page is displayed.
3. Select the Networks tab.
   A list of available networks is displayed.
4. Select the networks you want the client to be able to access. Clear the networks that you do not want the client to be able to access.

   Remember: A client assigned as the gateway in a gateway network cannot be a member of any other network.

5. Click Save.
   If the client is online, changes are applied immediately. If offline, changes are applied when the client comes online.

   Tip: You can also add and remove clients by selecting My Networks > Edit (for a network) > Add/Remove members.

How to Add a Hamachi Mobile Client

The Hamachi mobile client gives you access to Hamachi networks from an iOS or Android smartphone or tablet.

The mobile client is deployed by sending the required VPN settings in a configuration file via email; it is not an app you download from a store.

   Note: Mobile Phone connections always use a relayed tunnel.
Follow these steps to configure mobile client settings and send them via email.

1. In LogMeIn Central, switch to Networks and click Add Client on the Computers tab (Networks). The Add Client page is displayed.
2. Select Add mobile client and click Continue.
3. Enter a Client Name and add the client to a network (optional) and click Create. The Edit Client page is displayed with the new client displayed on the Mobile tab.
4. To send the default configuration to an email recipient, enter an email address and click the appropriate button for the user's operating system. Otherwise, change settings before sending.
   - Send iOS
   - Send Other

   **Tip:** To preview the configuration file, click Preview iOS Config or Preview Android Config, as appropriate. This helps you understand what the user sees on their device when configuring their client.

5. Add the client to a network under Join network.
   a) Enter a Network ID and password.
   b) Click Join

   **Important:** A mobile client must be in a network to go online.

6. Under Connection protocol, choose how the device will connect to Hamachi servers. Minimum one selection.
   - IPSec
   - PPTP

   **Important:** Starting from iOS 10, VPN using PPTP is deprecated and a valid PPTP configuration will not be created. Apple have more information [here](#).

7. Optional connection settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send all traffic over VPN</td>
<td>Valid for all network types.</td>
</tr>
<tr>
<td></td>
<td>• When applied to a gateway network, the gateway peer relays all outside traffic.</td>
</tr>
<tr>
<td></td>
<td>• When applied to mesh or hub-and-spoke networks, the device's traffic to the public Internet is not relayed by other members. This means the device cannot connect to the Internet.</td>
</tr>
<tr>
<td></td>
<td>• This setting is always applied to Android devices that use a PPTP connection.</td>
</tr>
<tr>
<td></td>
<td>• To retain an Internet connection on an Android using PPTP in a mesh network</td>
</tr>
<tr>
<td></td>
<td>• In a mesh network, set the Forwarding Route to 25.0.0.0/8.</td>
</tr>
<tr>
<td></td>
<td>• In a gateway network, the forwarding route must match the client's assigned IP range</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Set gateway peer to filter broadcast traffic | Filter out network packets not specifically directed to the device.
Enable on-demand connection to these domains | When an iOS device connecting via IPSec attempts to reach a listed domain, the VPN connection will be activated.

8. To save changes to the configuration file, click Save.

![Remember] For iOS, if you change settings after sending the configuration file, you must send a new version.

Once the recipient opens and installs the emailed configuration, the client becomes an attached member of the active LogMeIn account. You will be able to manage this client using LogMeIn Central. The recipient gains access to your shared resources. For example, you can use Hamachi to give mobile users access to your corporate LAN, internal webservers, file servers, etc.

![Note] Mobile Phone connections always use a relayed tunnel.

**Setting up an iOS device as a Hamachi mobile client**
This procedure assumes you or an administrator has sent configuration details to your device.

![Remember] The mobile client is deployed by sending the required VPN settings in a configuration file via email; it is not an app you download from a store.

1. **On the device**, install the Hamachi configuration profile.
   a) Open the email containing the configuration file as an attachment.
   b) Tap the attachment to open the Install Profile page.
   c) Tap Install.
   d) If prompted, confirm your choice.

2. If prompted to Enter your password for the VPN account "123-456-789", enter the device configuration password including dashes, as provided by your administrator or on the Edit Client page.
   The message Profile Installed is displayed.

3. To connect, go to **Settings > General > VPN** and choose Hamachi as your VPN. If you are not a member of any Hamachi network, you may see the following error: The VPN server did not respond.

   ![Important] Starting from iOS 10, VPN using PPTP is deprecated and a valid PPTP configuration will not be created. Apple have more information [here](#).

**Setting up an Android device as a Hamachi mobile client**
This procedure assumes you or an administrator has sent configuration details to your device.

![Remember] The mobile client is deployed by sending the required VPN settings in a configuration file via email; it is not an app you download from a store.
1. On the device, open the email containing the following three files as attachments.
   - **PFX** The client certificate.
   - **CA** Issuer of the client certificates.
   - **RootCA** Self-signed root certificate.

2. Save all attachments and locate them on the device.
   **No attachments?** When the connection type is PPTP, no certificates are attached. Certificates are attached only with IPSEC.

3. Extract the Hamachi client certificate, file type **PFX**, as follows:
   a) Tap the file.
   b) When prompted to enter a password to extract the certificate, enter the device configuration password (for example, `abcd-a1b2-c1d2`). Include dashes. Case sensitive.
   c) Name the certificate.

4. Install both the Hamachi CA and RootCA certificates, as follows:
   a) Tap the files.
   b) Name the certificates. The names need not match the name used in step 3.

5. Add a VPN profile for Hamachi for each connection protocol (IPSec and PPTP), as follows:
   a) Go to **Settings > More settings > VPN**
   b) Tap **Add VPN Network**.

6. Connect.
   **No Internet Connection?** To retain an Internet connection on an Android using PPTP:
   - In a mesh network, set the Hamachi VPN profile **Forwarding Route** to `25.0.0.0/8`
   - In a gateway network, the **Forwarding Route** must match the client's assigned IP range

### How to Change the Client Interface

**Note:** This functionality is not available on Linux.

1. In LogMeIn Central, go to the **Networks > My Networks** page. Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the client you want to work with. The **Edit Client** page is displayed.
3. Select the **Settings** tab.
4. Select an **Interface Mode**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full</strong></td>
<td>The client will offer full functionality to end users.</td>
</tr>
<tr>
<td><strong>Restricted</strong></td>
<td>The client will offer a full graphic user interface, but client settings (including the right to change certain settings locally) can be defined on the web only.</td>
</tr>
<tr>
<td><strong>Minimal</strong></td>
<td>The client will offer no graphic user interface to the end user. Only the Hamachi system tray icon will be visible. Client settings can be defined on the web only.</td>
</tr>
</tbody>
</table>

5. For Restricted or Minimal mode, select the client settings to apply.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Choose this option to provide extra protection against sniffing. For business use, we highly suggest using encryption. Use of this option may cause <em>minimal</em> extra CPU load for both sender and receiver.</td>
</tr>
<tr>
<td>Compression</td>
<td>Choose this option to speed up large data transfers. Compression is particularly useful on low bandwidth connections. Use of this option may cause <em>minimal</em> extra CPU load for both sender and receiver.</td>
</tr>
<tr>
<td>Can create new network</td>
<td>Allow the client to be used to create new mesh networks.</td>
</tr>
<tr>
<td>Can join networks</td>
<td>Allow the client to be used to join networks other than those assigned on the web.</td>
</tr>
<tr>
<td>Can chat</td>
<td>Allow the client to be used for chat between Hamachi peers.</td>
</tr>
<tr>
<td>Keep chat logs</td>
<td>Allow the client to store chat logs.</td>
</tr>
<tr>
<td>Maintain log</td>
<td>Allow the client to store a Hamachi event log.</td>
</tr>
</tbody>
</table>

6. Click **Save**.
   If the client is online, changes are applied immediately. If offline, changes are applied when the client comes online.

**How to Detach (Delete) a Client from Your Account**

You can detach a client from your LogMeIn account and remove it from all networks in your account. The Hamachi client software will remain installed on the local computer.

1. In LogMeIn Central, go to the **Networks > My Networks** page. Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the client you want to work with. The **Edit Client** page is displayed.
3. Select the **Delete** tab.
4. Click **Remove Client**. The client is detached from your account.

**Using Tags to Help Manage Clients in Your Account**

Add tags to Hamachi clients to help manage a complex account.

A tag is a label associated with a client. Tags help you identify and search for clients, but are not used in reporting or otherwise.

*Tip*: Once you have tagged your clients, use the **Search Clients** box to locate them.

**Tagging Example**

Assume you are a service provider managing multiple Hamachi clients for a large company. You want to categorize deployed clients according to department, so you add a tag to each client depending on the department to which the end user belongs.

- Tag each client used by a member of Marketing as "Marketing"
- Tag each client used by a member of Sales as "Sales"
- Tag each client being used by a member of Operations as "Ops"
When you need to locate a computer, type a tag name in the **Search Clients** box to find all clients appropriately tagged clients.

### How to Create and Manage Tags

1. In LogMeIn Central, go to the **Networks > Network Settings** page.
2. Select the **Tags** tab.
3. Click **Add New Tag**. The **Add New Tag** dialog box is displayed.
4. Type a **Tag name** and click **OK** or **Save**. The new tag is saved.

**Tip:** You can also work with tags by selecting **Networks > My Networks > Edit Client > Edit Tags**.

### How to Assign Tags to a Client

You can assign multiple tags to a single Hamachi client.

1. In LogMeIn Central, go to the **Networks > My Networks** page. Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the client you want to work with. The **Edit Client** page is displayed.
3. Select tags from the list and click **Save**.

### Managing LogMeIn Hamachi Networks

### How to Set the Default Response to Network Join/Exit Requests

Network defaults are automatically applied to all new networks in your account. Default settings are not applied to networks that join your account.

1. In LogMeIn Central, go to the **Networks > Network Settings** page.
2. Select the **Network Defaults** tab.
3. Select a **Network type**.
4. Select the default response to join requests.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept automatically</td>
<td>All requests to join the network will be accepted automatically. We recommend that you require a network password when using this option.</td>
</tr>
<tr>
<td>Must be approved</td>
<td>All requests to join the network must be approved on the web.</td>
</tr>
<tr>
<td>Members can be added on the web only</td>
<td>Clients will not be able to join the network from the client. Clients can be added to the network on the web only.</td>
</tr>
</tbody>
</table>
5. Under **Network Member Permissions**, select **Can leave network at will** to allow members to leave the network at any time. By disabling this option, you can prevent clients from leaving a network accidentally or upon connection failure.

6. Click **Save**.

**How to Add a Hamachi Network**

1. In LogMeIn Central, go to the **Networks > My Networks** page. Your Hamachi networks and clients are listed.

2. On the **My Networks** page, click **Add Network**. The **Add Network (Step 1)** page is displayed.

3. Name the network in the **Network name** field. Use the network name to help identify the network.

4. Select a **Network type**. See *LogMeIn Hamachi Network Types* on page 206.

   **Important:** Once a network is created, its network type cannot be changed.

5. Enter a **Network description** (optional).

6. Click **Continue**. The **Add Network (Step 2)** page is displayed.

7. Select the default response to join requests.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accept automatically</strong></td>
<td>All requests to join the network will be accepted automatically. We recommend that you require a network password when using this option.</td>
</tr>
<tr>
<td><strong>Must be approved</strong></td>
<td>All requests to join the network must be approved on the web.</td>
</tr>
<tr>
<td><strong>Members can be added on the web only</strong></td>
<td>Clients will not be able to join the network from the client. Clients can be added to the network on the web only.</td>
</tr>
</tbody>
</table>

8. Under **Network password**, select **A password is required to join this network** to protect your network.

   **Tip:** If you do not set a password, we recommend setting the Join Request behavior to **Must be approved** or **Members can be added on the web only**.

9. Click **Continue**. The **Add Network (Step 3)** page is displayed.

10. Follow the on-screen instructions.

11. Click **Finish**. Your network is created with a system-generated Network ID.

   **Note:** When you assign a gateway, you will lose your network connection for a few seconds while the Hamachi virtual network adapter bridges to the physical network adapter.
How to Configure a Hamachi Gateway on Windows to Recognize Multiple Subnets

Provide access to a network with multiple subnets via a Hamachi gateway.

By default, the client set as the gateway in a Hamachi gateway network will provide access to its own subnet (the one on which it is installed).

Follow this procedure to set an existing gateway to recognize additional subnets that are accessible from the gateway's subnet:

1. Open the Windows client that is set as the gateway.
2. Right-click the gateway network and select **Gateway settings** from the menu.
   The Gateway Settings dialog box is displayed.
3. Select the **Remote Networks** tab.
4. Click **Add** to add new remote networks.
   The Network Subnet dialog box is displayed.
5. Enter the **Network address** and **Subnet mask** in dotted decimal format.
6. Click **OK** or **Apply** to save your settings.

Members of the gateway network will be able to access resources on all recognized subnets.

How to Assign an IP Range for Gateway Members on Windows

Gateway members are assigned an IP address by the DHCP server in your gateway's LAN. If no DHCP server is present, the gateway must be configured to behave as a quasi-DHCP server and assign addresses from a defined range.

1. Open the Windows client that is set as the gateway.
2. Right-click the gateway network and select **Gateway settings** from the menu.
   The Gateway Settings dialog box is displayed.
3. Select the **IP Parameters** tab.
4. Clear the **Obtain IP settings automatically** box.
5. Under **Address range**, enter the appropriate addresses.

   **Important:** You must complete each field under **Address range**.

6. If you have a DNS server(s) in the network, you may enter their IP addresses and define a DNS suffix.
7. Click **OK** or **Apply** to save your settings.

How to Configure Home LAN Behavior for Gateway Network Members

Control how gateway network members should behave when they are physically located in the same network as the gateway (the "Home LAN").

1. In LogMeIn Central, go to the **Networks > My Networks** page.
   Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the network you want to work with.
   The **Edit Network** page is displayed.
3. Select the **Settings** tab.
4. Under **Home LAN Behavior**, select one of the following options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Disable members going online in the host network** | Authentication errors may occur if a client logs in to a gateway network from a Hamachi network and a physical network IP address. Choose this option to prevent members from going online to the gateway when they are physically located in the same network as the gateway. All network resources remain available through the physical network.  
   **Tip:** Ensure that ICMP traffic on the gateway is not blocked by a firewall. |
| **Disable network stack components**        | Choose this option to allow members to go online to the gateway when they are physically located in the same network as the gateway. When this option is selected, the stack components of the Hamachi network adapter are turned off. This resolves potential conflicts by preventing the operating system from attempting to authenticate through the Hamachi adapter toward the domain controller. Members go online in the gateway network. All local network resources remain available through both the physical and the Hamachi network. This option is useful if a user has limited access to the physical network resources but can have unlimited access to the same resources through the Hamachi network.  
   **Tip:** Ensure that ICMP traffic on the gateway is not blocked by a firewall. |
| **Do not restrict members**                 | Choose this option to allow members to attempt to go online when they are physically located in the same network as the gateway. If you experience authentication problems, choose one of the above options.                                                                                     |

5. Click **Save**.

**How to Add a Hamachi Network from the Client**

**On Windows or Mac**

This procedure must be executed on the client.

1. Click **Network > Create a new network**. Select **Menu > Create new network**.
2. Type the network ID and password of the network.
3. Click Select **Create**.

**On Linux**

1. Open the terminal.
2. Execute the following command:
   ```bash
   sudo hamachi create <network ID> [password]
   ```

**How to Rename a Network**

Use the network name to help identify the network.
**Important:** When joining a network from a client, use the system-generated network ID. The network ID cannot be changed.

1. In LogMeIn Central, go to the **Networks > My Networks** page.
   Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the network you want to work with.
   The **Edit Network** page is displayed.
3. On the **Members** tab, type a new name in the **Name** field.
4. Click **Save**.
   If the client is online, changes are applied immediately. If offline, changes are applied when the client comes online.

**Important:** You cannot rename an unattached network that was created from the client.

## How to Approve or Reject Join Requests

If you receive a request from another client to join your network, you can approve or reject that request. A request is automatically rejected if you do not approve it in two weeks.

1. In LogMeIn Central, go to the **Networks > My Networks** page.
   Your Hamachi networks and clients are listed.
2. You will see the following message when you have requests from clients waiting to join your account or networks: **You have x pending join requests.** Click the **pending join request** link.
   The Join Requests page is displayed.
3. Choose **Accept** or **Reject**, as appropriate.
4. Click **Save**.
5. Select the peer waiting for approval.
6. Select **Menu > Requests**.
7. Choose **Approve request** or **Reject request**, as appropriate.

**Note:** You may not be able to accept new members if your Hamachi subscription expires or if you reach the member limit of your network. See also *LogMeIn Hamachi Network Types* on page 206.

**Tip:** Are you on Linux? You can approve or reject requests from the command line with the following commands:

```bash
sudo hamachi approve <network ID> <client ID>
sudo hamachi reject <network ID> <client ID>
```

## How to Edit Network Settings

1. In LogMeIn Central, go to the **Networks > My Networks** page.
   Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the network you want to work with.
   The **Edit Network** page is displayed.
3. Select the **Settings** tab.
4. Type a **Welcome message** (optional).
   This message will be displayed to any client joining the network for the first time.

5. Type an **Announcement message** (optional).
   This message will be displayed when an existing member logs in to the network. Members also receive the announcement whenever it is updated.

6. Select the default response to join requests.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accept automatically</strong></td>
<td>All requests to join the network will be accepted automatically. We recommend that you require a network password when using this option.</td>
</tr>
<tr>
<td><strong>Must be approved</strong></td>
<td>All requests to join the network must be approved on the web.</td>
</tr>
<tr>
<td><strong>Members can be added on the web only</strong></td>
<td>Clients will not be able to join the network from the client. Clients can be added to the network on the web only.</td>
</tr>
</tbody>
</table>

7. Under **Network Member Permissions**, select **Can leave network at will** to allow members to leave the network at any time. By disabling this option, you can prevent clients from leaving a network accidentally or upon connection failure.

8. Click **Save**.

**How to Modify the Client's Role in a Network**

1. In LogMeIn Central, go to the **Networks > My Networks** page. Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the network you want to work with. The **Edit Network** page is displayed.
3. Click **Add/Remove Members**.
4. Change member settings as follows:
   - Hub or spoke for a hub-and-spoke network (multiple hubs are allowed)
   - Gateway or member for a gateway network (one gateway node only)
   - Member for a mesh network

   **Remember:** A client assigned as the gateway in a gateway network cannot be a member of any other network.

5. Click **Save**.
   If the client is online, changes are applied immediately. If offline, changes are applied when the client comes online.

**How to Change Network Password Settings**

1. In LogMeIn Central, go to the **Networks > My Networks** page. Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the network you want to work with. The **Edit Network** page is displayed.
3. Select the **Password** tab.
4. Activate or de-activate the password requirement.

**Tip:** If you do not set a password, we recommend setting the Join Request behavior to **Must be approved** or **Members can be added on the web only**.

5. To change the password, type a new password and re-enter to confirm.
6. Click **Save**.

### How to Delete a Network

1. In LogMeIn Central, go to the **Networks > My Networks** page. Your Hamachi networks and clients are listed.
2. On the **My Networks** page, click **Edit** next to the network you want to work with. The **Edit Network** page is displayed.
3. Select the **Delete** tab.
4. Click the **Delete** button.
   The network is permanently deleted. All client installations and client-to-account relationships are left intact.

### How to Leave a Network

This procedure must be executed on the client.

1. On the client, right-click on the network that you want to leave. Select the network that you want to leave.
2. Click **Leave network**. Click **Menu > Network > Leave network**.

**Important:** You cannot transfer the ownership of a network; therefore, you cannot leave a network that you created. You can only delete such networks.

**Note:** A network owner can prohibit members from leaving a network. To check if members are allowed to leave a network without the owner’s permission, see **How to Edit Network Settings** on page 226.

### How to Resolve Network Member Limit Issues

A blue warning icon next to the name of a network signals that there is an issue with the number of network members. In this case, you are either approaching the member limit of your network, or you have already exceeded it.

This procedure must be executed on the client.

1. On the client, click the blue warning icon and check the description of the issue. Alternatively, next to the name of your network, click the number displaying the network member limit.
2. Click **Upgrade options** to purchase a subscription that allows you to add more members to your network.
   The LogMeIn Hamachi website opens.
3. Follow the instructions to purchase a subscription. For information, see **How to Purchase Subscriptions from the Hamachi Client** on page 210.
How to Transfer a Hamachi Network to Your LogMeIn Account

**Important:** You can only transfer a network from the Hamachi client to your LogMeIn account if the network was created on the Hamachi client.

This procedure must be executed on the client.

1. On the client, right-click on the network that you want to transfer to your LogMeIn account.
2. Click **Transfer ownership to <your LogMeIn account>**.
   - The name of the LogMeIn account holder to whom the client is attached is displayed.
3. Click **OK** to transfer the network to the LogMeIn account.

   You will see the network listed among your networks in your LogMeIn account.

   **Tip:** Hover your mouse over the network name to see the current owner of that network.

   **Tip:** On Linux, networks created on the client can be transferred at the time of the attach request via the `sudo hamachi attach-net` command.

How to Change the Priority of the Virtual Network Adapter

Hamachi puts its virtual network adapter at the bottom priority in Windows. This is done to ensure there are no conflicts when Hamachi runs on an Active Directory Domain Controller or DNS server.

**Important:** If you are on a wireless network, you may run into unpredictable connection issues when making this change.

1. Go to the Advanced Settings of your computer:
   a) On Windows XP, go to **Control Panel** > **Network Connections** > **Advanced** > **Advanced Settings**
   b) On Windows 7, 8, or Vista, go to **Start**, type `ncpa.cpl` in the search field, and press **Enter**. Then press **Alt** to show the menu bar, and click **Advanced** > **Advanced Settings**.

2. Use the Up/Down buttons to reorder the network adapters to your preference.
   - Hamachi will perform best at the top, but the difference is very minor in all but very intense usage, and may cause compatibility issues with other Network-centric tasks.
Using LogMeIn in a Multilingual Environment

Available Languages

The LogMeIn website and LogMeIn host software are available in twelve languages.

To change the LogMeIn website language, use the language and location selector in the upper-right corner of the site.

Available Languages

• de – German
• en – English
• es – Spanish
• fr – French
• hu – Hungarian
• it – Italian
• ja – Japanese
• ko – Korean
• nl – Dutch
• pt-br – Brazilian Portuguese
• ru – Russian
• zh – Chinese

How to Set the Language Used by the LogMeIn Host

The LogMeIn host interface and messages will be displayed in this language. This setting does not impact operating system settings.

1. Access the host preferences:
   • From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > General
   • From a client device, connect to the host Main Menu and follow this path: Preferences > General

2. Under Appearance select the appropriate language in the Language drop-down box.

Can’t access this feature? If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your access to this feature. Contact your administrator for more information.

3. Click OK or Apply.
   On the host, you may need to exit and then reopen LogMeIn before the change will be visible.

Tip: To change the language used by File Sharing and the LogMeIn System Tray menu, you must change your operating system language settings. For example, in Windows, go to Control Panel > Region and Language. On a Mac, go to System Preferences > International > Language.
How to Set the Language Used by the LogMeIn Client

To change the language used by the LogMeIn Client, select View > Options > Language.

The chosen language is applied immediately to the LogMeIn Client interface. Existing remote control sessions must be restarted before the language change is applied.

About International Keyboard Mapping During Remote Control

During remote control between client and host with different regional settings, you may need to adjust keyboard settings to allow for proper data input.

When controlling PC or Mac from a PC, the client-side user will be able to choose one of three keyboard handling options. The setting is stored on the client for each host.

To set the keyboard option during remote control, click Options.

<table>
<thead>
<tr>
<th>Use host layout</th>
<th>Select this option to use the keyboard layout of the host. Characters and combinations entered on the client are read by the host according to their physical position on the keyboard. Client keyboard layout is ignored.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use client layout</td>
<td>Select this option to use the keyboard layout of the client. Characters and combinations are sent to the host exactly as entered on the client-side. Host keyboard layout is ignored.</td>
</tr>
<tr>
<td>Use legacy LogMeIn mapping</td>
<td>Select this option if you are accustomed to LogMeIn's legacy keyboard mapping and prefer not to change at this time.</td>
</tr>
</tbody>
</table>
Troubleshooting

For troubleshooting assistance, visit help.LogMeIn.com.

Tip: The LogMeIn Community is an excellent source of information from other LogMeIn users.

Troubleshooting Connection Issues

Can't connect? Try this first!
A checklist of the most common communication issues when connecting to LogMeIn host computers.

Firewall Configuration
Make sure the LogMeIn software is not being blocked by a firewall on the host computer. You will need to allow LogMeIn to make connections in the firewall rules. For details, see LogMeIn and Firewalls on page 22.

Warning: Common error code: 10061.

Proxy Settings
You may encounter connection issues if your proxy is not configured to work with LogMeIn.

Warning: Common error codes: 10049, 10061, 11004, 10060.

DNS Status
Follow the steps to fix problems with your DNS resolving our IP Address.

On Windows 7 and newer:
1. Open the Run dialog. (Press the Windows key and the R key at the same time.)
2. Type cmd and click OK.
3. In the command prompt, type ipconfig /flushdns and press the Enter key.

On Mac OS X:
1. Open Utilities > Terminal.
2. Type dscacheutil -flushcache and press the Enter key.

Warning: Common error code: 10049.

OpenDNS Service
You may encounter connectivity issues when using LogMeIn products with OpenDNS. This is due to OpenDNS categorizing LogMeIn domains as a proxy/anonymizer. LogMeIn support is unable to provide
further assistance with this issue. Please visit http://www.opendns.com/ for more information configuring OpenDNS.

**Internet load balancers and reverse proxies (satellite connections)**

To resolve IP mismatch issues behind an internet load balancer or a reverse proxy, follow these steps.

1. Copy this text:

   ```
   Windows Registry Editor Version 5.00
   [HKEY_LOCAL_MACHINE\SOFTWARE\LogMeIn\V5\Net]
   "BrokenProxy"=dword:00000000
   ```

2. Save it in Notepad or a similar editor on the host computer as IP Mismatch.txt.
3. Rename the file IPMismatch.reg. You may be asked to confirm that you want change the file extension from .txt to .reg. Confirm the change.
4. Double click the file and confirm that you want to import the file into the registry.

**Date and Time Settings**

If the date and time settings of your computer are incorrect, LogMeIn may show as **Enabled and Online**, but as **Offline** in your account.

To change the date and time of your system, click the clock on your Windows system tray or on your Mac menu bar.

**Why does my computer show as Offline?**

Check the following to make your host accessible.

**Is the host computer in Standby, Sleep, or Hibernation mode?**

Computers in Standby, Sleep, or Hibernation mode may be inaccessible via LogMeIn. For Wake On LAN requirements, see *How to Wake a Computer in Sleep Mode or Powered Off Using Wake On LAN* on page 134 to ensure that you can wake your computer from Standby, Sleep, or Hibernation mode. If you cannot use Wake On LAN, you can prevent your computer from entering a sleep mode by changing your Power Management settings.

**Windows**

1. Physically go to the computer that you want to be able to access.
2. Press and hold the **Windows key** and press the letter **R** on your keyboard.
3. Type `powercfg.cpl` and press **Enter**.
4. Set the option for Sleep or Standby to **Never**.
   
   Vista and 7 users can use the **Change when the computer sleeps** option in the left pane.
5. Make sure Hibernation is also disabled.

   **Note:** It is fine to allow the monitor to enter power saver mode.

**Mac OS X**

1. Physically go to the computer that you want to be able to access.
2. From your Mac Desktop, click the **Apple Menu** in the top left.
3. Select **System Preferences**.
4. Click on **Energy Saver**.
5. Move the slider for **Put the computer to sleep when it is inactive for...** to **Never**.
Is the LogMeIn service running on the host?
Make sure that LogMeIn is running on the host. You will need access to the host to perform this action.
• Open the LogMeIn Control Panel.
• Check whether the host is Accessible in the top-left corner.
• If it is Not accessible, switch the host on by clicking the power switch on the host interface.

Is the host computer connected to the Internet?
Make sure that the computer you want to control is connected to the Internet. LogMeIn requires an "always on" Internet connection such as DSL, Cable, or T1.

Is some other software interfering with LogMeIn?
If certain ports and LogMeIn components are blocked or prevented from accessing the web, connection cannot be established. See How do I configure a firewall to work with LogMeIn? for details.

Is the date and time correct on the host computer?
Incorrect date and time settings can make your computer appear offline. To resolve this problem, set your system clock to today’s date and time.
• On a Windows PC, double-click the clock icon in the Window’s Taskbar and choose Change date and time settings.
• On a Mac, select System Preferences from the Apple menu and choose Date & Time.

Why do I get a Host Not Found Error?
Your host appears online, but when you try to connect you get the following error: Host Not Found.
The host may have been switched off or lost its connection to the Internet since you last refreshed your computer list. Check the following to make your host accessible:

- Make sure the host is powered on and can connect to the Internet.
- Make sure that LogMeIn is running on the host. You will need access to the host to perform this action.
- Open the LogMeIn Control Panel.
- Check whether the host is Accessible in the top-left corner.
  - If it is Not accessible, switch the host on by clicking the power switch on the host interface.
  - If it is Enabled but offline, switch the host off and then back on by clicking the power button twice.

Why can't I log in to my computer? (error 5 / 1326 / 1327 / Login failed.)

Many users experience problems logging in to host computers.

An error 1326 or error 5 indicates that you are incorrectly entering your Windows/Mac user name or your Windows/Mac password. Error 1327 usually means you entered a blank password (that is, you did not enter any password at all).

You may also see:

Login failed. Enter the [Windows/Mac] user name and password you see when physically sitting at the remote computer.

If you are confident that you are entering a correct Windows/Mac password, then you may be entering an incorrect Windows/Mac user name.

Tip: One common reason for failed login is that users enter their LogMeIn ID and password, not their computer user name and password. See also Access Code? Password? About Authentication on page 130.
How to Retrieve Your User Name on a Windows PC

You can find your username is displayed on the LogMeIn Control Panel Options tab under Username and Password.

1. Physically go to the computer that you want to be able to access, or ask someone who is present at that computer to perform the following steps.

   Tip: In some cases, you may need to ask for help from the person who manages LogMeIn at your organization.

2. Right-click the LogMeIn Control Panel icon in the taskbar.

3. In the resulting menu, click the first menu item. This is the computer name. It is always listed above the menu item called LogMeIn Control Panel.

Your username is displayed on the LogMeIn Control Panel Options tab under Username and Password.

Remember: Any user in the Administrators group can be used to log in to the computer.

How to Retrieve Your User Name on a Mac

1. Physically go to the computer that you want to be able to access, or ask someone who is present at that computer to perform the following steps.

   Tip: In some cases, you may need to ask for help from the person who manages LogMeIn at your organization.

2. Click the Apple menu and go to System Preferences > Users and Groups.

3. Any user in the Administrators group can be used to log in to the computer.

My IP address has been blocked after too many failed login attempts. What can I do?

Repeated failure to enter a valid Windows/Mac user name and password can result in IP Lockout. This means you won't be able to continue to attempt to log in from the same computer until the lockout is resolved. The lockout remains in effect for 30 minutes by default.

Tip: One common reason for failed login is that users enter their LogMeIn ID and password, not their computer user name and password. See also Access Code? Password? About Authentication on page 130.

To clear an IP address lockout, you must have physical access to the host computer.

1. Physically go to the computer that you want to be able to access, or ask someone who is present at that computer to perform the following steps.

   Tip: In some cases, you may need to ask for help from the person who manages LogMeIn at your organization.

2. Open the LogMeIn Control Panel and follow this path: Options > Preferences > Security.

3. Under Authentication Attack Blocker, click Unblock all.
You should be able to return to the original client computer (the one that was locked out) and log in with valid credentials.

For more information about how LogMeIn protects your host computers, see How to Set up an Authentication Attack Blocker on page 193.

How do I resolve Error 4320?

An attempt to log in without proper administrator rights or User Access Control permissions may result in error 4320 ("Operator or Administrator has refused the request").

Follow these instructions to ensure you have proper User Access Control permissions on the host computer you are attempting to access. This will allow you to access the host computer even if you are unable to be added as an administrator at the operating system level.

1. Physically go to the computer that you want to be able to access, or ask someone who is present at that computer to perform the following steps.

   **Tip:** In some cases, you may need to ask for help from the person who manages LogMeIn at your organization.

2. Open the LogMeIn Control Panel and follow this path: Options > Preferences > Security.

3. Under User Access Control, click Show details.... The User Access Control window is displayed.

4. Under Users, select your user name from the list. You may need to browse for additional users.

   **Tip:** For example, if you sign in using a Computer Access Code, you may need to add the user named LogMeInRemoteUser: Click Browse > List users of selected domain and find LogMeInRemoteUser on the list.

5. Under Edit Selected User, you must select at least the Login permission to resolve the 4320 error.

6. Save your changes.

Troubleshooting Account Issues

How do I connect a "not accessible" computer to my account?

When LogMeIn host software is installed on a computer but the computer is not attached to a LogMeIn account, the computer may show as Enabled but Offline or you see the following message: LogMeIn - not accessible - setup not completed.

This may happen, for example, if you delete your computer from your account via LogMeIn.com; the LogMeIn host software remains on your PC or Mac, but it is not associated with a LogMeIn account.

To enable your computer for remote access, you must associate it with a LogMeIn account.

1. Go to the computer that you want to be able to access remotely.

2. Open the LogMeIn Control Panel.

3. On the Overview tab or About tab, click Switch Account....

4. Enter the LogMeIn ID (email) and password for the account you want to use to access the computer. The Switch account... page is displayed.
5. Click **Continue**.
   LogMeIn must be restarted before the changes take effect.

### Troubleshooting Remote Printing

**Remote Printing Disappeared, Does Not Work At All**
Check the following items.

> Remember: A *Plus* or *Premier* subscription is required to use this feature.

**Confirm that the client-side printer is working**
Check your client-side printer (the one to which you are trying to print). Make sure you can print a test page. If you cannot print locally, you will not be able to print remotely. Resolve any local issues before continuing.

**Update your browser**
With Internet Explorer remote printing only works with the ActiveX plugin. For best results on Firefox and Chrome, update your browser and install the *LogMeIn Client app*.

**Confirm that you have access to Remote Printing, that it is enabled, and that a printer is selected**
If LogMeIn was installed by an administrator or via an Installation Link from LogMeIn Central, your administrator may have restricted your right to use remote printing.

Here's how to confirm that you have access to Remote Printing, that it is enabled, and that a printer is selected:

1. On the remote control toolbar, click **Options**.
2. Under **Remote Printing**, confirm that at least one printer is selected (that is, make sure there is a check mark next to at least one printer).

   **Tip:** For easy access to remote printing settings, go to **Customize Toolbar > Connection Options > Connect Printer**. A printer icon is displayed in the toolbar. You can click the printer icon to see if your printer has been recognized or to change the active printer.

3. When printing, confirm that you are printing to *[Printer Name]* via LogMeIn.
Confirm that you are printing to [Printer Name] via LogMeIn

When you send your print job from the host, make sure the correct client-side printer is selected: [Printer Name] via LogMeIn.

Remote Printing Output is Mirrored

There are multiple ways to resolve this problem, depending on your configuration.

Remember: A Plus or Premier subscription is required to use this feature.

Turn on Force Bitmap Printing

1. Access the host preferences:
   - From the host computer, open the LogMeIn Control Panel and follow this path: Options > Preferences > Advanced
   - From a client device, connect to the host Main Menu and follow this path: Preferences > Advanced


3. Click OK or Apply.
   Your settings are applied immediately to the host.

4. Print the file again.
   When bitmap printing is activated, all material printed using remote printing will be 'printed' locally to a bitmap which is then sent to the remote printer. Bitmap printing is slow, but reliable.

Turn off display acceleration

1. On the client computer, go to Preferences > General.

2. Clear the Use display accelerator option.

Print the file again.

Change your remote control method to Java

1. From a client computer, connect to the host Main Menu.

2. Click the arrow next to Show Detailed Mode in the top left corner of the menu.

3. Click the icon to the left of the Remote Control option.

4. Select Java.

Remote Printing Output is Blank

There are multiple ways to resolve this problem, depending on your configuration.

Remember: A Plus or Premier subscription is required to use this feature.

Change the printer resolution

This procedure may vary depending on your operating system.

1. On the host, print as you normally would during regular use.

2. Make sure the client printer is selected in the Print dialog box: .
3. In the Print dialog box, click **Preferences**.
4. In the Printing Preferences dialog box, click **Advanced**.
5. Save your changes and print again.

**Enable Force Bitmap Printing**

1. Access the host preferences:
   - From the host computer, open the **LogMeIn Control Panel** and follow this path: **Options > Preferences > Advanced**
   - From a client device, connect to the host **Main Menu** and follow this path: **Preferences > Advanced**
2. Under **Remote Printing**, select **Force Bitmap Printing**.
3. Click **OK** or **Apply**.
   Your settings are applied immediately to the host.
4. Print the file again.
   When bitmap printing is activated, all material printed using remote printing will be 'printed' locally to a bitmap which is then sent to the remote printer. Bitmap printing is slow, but reliable.

**Still not working?** Go to **Preferences > General** and clear the **Use display accelerator** option. Print the file again.

**Remote Printing Does Not Work in Certain Programs**

On rare occasions, certain third-party software may not be compatible with remote printing.

**Remember:** A **Plus** or **Premier** subscription is required to use this feature.

Please search **help.LogMeIn.com** for current known issues.

**Remote Printing Output is Stuck in the Print Queue**

On a Windows PC, clear the print spooler to clean out your queue.

**Remember:** A **Plus** or **Premier** subscription is required to use this feature.

1. On the host, open the **Run** window by pressing the Windows key + R.
2. In the **Run** window, type **services.msc**.
   The Services window is displayed.
3. In the details pane, click **Print Spooler** once.
4. In the left pane, click **Stop**.
5. Delete all files in the **C:\Windows\System32\spool\PRINTERS** folder.
6. In the **Services** window left pane, click **Start**.

The print spooler queue is now cleared. Print the file again.

**Troubleshooting Display Issues**

Follow these instructions to help resolve problems experienced while viewing video or while using DOS-based or graphic-intense applications during remote control. Typical problems include display black-out, host computer restart when initiating remote control, or loss of Windows Aero functionality after remote control.

- Available on Windows hosts only.

1. Access the host preferences:
   - From the host computer, open the **LogMeIn Control Panel** and follow this path: **Options > Preferences > General**
   - From a client device, connect to the host **Main Menu** and follow this path: **Preferences > General**

2. Under **Remote Control > Performance**, make sure that **Use Display Accelerator** is **not** selected.

3. Click **OK** or **Apply**.
   
   Your settings are applied immediately to the host.
Index

2FA (two-factor authentication) 13
4320 237

A
access denied 5 235
accessible 233
account
  LogMeIn 8
account audit 10, 11, 17, 18
active directory 27
ad hoc support 197
Aero 180
alerts 45, 47, 50
  assign 48
  manage 49
  rule types 45
Android 130
anti-virus 71, 72, 74
attached client 206
attaching clients 215
audit log 11
audit notifications 11
authentication 60, 127, 128, 130, 189
  automatic 138
authentication attack filter 192, 193
autologon 172
Automatically connect to a specific computer 129
AV 72

B
batch file 53
billing information 9
black out the host monitor 145
blank screen
  during remote control 155
block input during remote control 155
block input on host during remote control 146
blocked keyboard and mouse input 183
Break/Fix 197

C
change
  computer access code 131
  computer name 39
  language 230
change password 227
charts 120
  create a chart 120
  default 121
Clear saved passwords 155

D
default settings 215
delete a computer 40
denial of service 192
deployment 64
  modify 25
deployment methods 26
desktop shortcut to a computer 130
Index

desktop viewing 173
device drivers 180
direct to remote control 127, 128
disconnection time
disconnected from remote control 184
disk space utilization 177
display accelerator 241
display black-out 241
display color 156
display multiple monitors 151
display size during remote control 142
distribution
distribution methods 26
DLLs 179
domain name servicing 217
DoS attacks 192
DOS based applications, graphics problems 241
double-click 150
DPMS 145
drag 150
draw during remote control 147
drive and partition information 177
drivers 169
dual monitors 142
draw during remote control 147

E
effects
disable 180
email
change LogMeIn account email 8
 emailed security codes 18
enabled but offline 233
error
4320 194
Esc key 152
events 168
exe 53

F
favorites list 40
File Manager 158
 compression 181
 open files for editing 160
 select files 161
 sort files 159
files
copying 158
moving 158
replicating 158
synchronizing 158
Files feature 124
firewall 211
firewalls 22
Force Quit 149
forgotten access code 131
full screen 141
function keys 152

G
gateway network 224
grab items 150
graphic intense programs during remote control 241
groups
 add a new group 41
delete a group 41
edit an existing group 41
hide 41

H
Hamachi 204
Hamachi client 205
Hamachi features 210
Hamachi installation for Windows 214
Hamachi license 208, 210
Hamachi network types 206
Hamachi subscription 208, 210
Hamachi update 214
Hamachi virtual IP address 206
history 62
Host Preference Package
 preferences that can be deployed 80, 83, 84, 85, 86, 88, 95

I
idle time 184
input blocked 183
input line
 used for remote sound 148
install software 55, 58
installation 20
 remote 24
 LogMeIn host 20
installation links 23
installation, remote 64
installed applications 180
international contact numbers 230
inventory
 activate 119
 view data for an individual computer 119
 invoice 9
IP address filtering 191
IP range 224
iPad 130
iPhone 130
iPod touch 130

J
join requests 226
Index

K
key combinations 152, 153
keyboard
  function keys 152
  international 152
  lock keyboard 155
  special characters 152
keyboard and mouse priority 183
keyboard mapping
  international 231
  PC to Mac 183
keys 170
kiosks 186

L
language 230, 231
keyboard mapping 231
  used by Desktop Sharing, File Sharing, system tray menu 230
  used by LogMeIn 230
laser pointer 147
license 208, 210
Linux 211
listing computers 32
LMIGuardian.exe 98, 188
lock the host after remote control 184
locked out 236
log files
  view 187
  viewing 62
login credentials 60
login failure 235
login policy 12
LogMeIn account
  change billing information 9
  change LogMeIn account email 8
  change LogMeIn account password 9
  reset LogMeIn account password 9
LogMeIn Client desktop app 128
LogMeIn Guardian 98, 188
LogMeIn ID 8

M
magnify screen during remote control 141
manage
  events 168
  shared resources 174
  Windows groups 167
  Windows users 167
managing host computers 30
mass deploy 27
memory load 176
Microsoft updates 64
mirror display driver 241
monitor a host 173
monitors
  switching between multiple host monitors 142
  working with multiple 151
mouse clicks 150
Mouse icon 150
mouse movement 150
mouse moves (option) 150
mouse wheel 150
moving files from one computer to another 158
MSI 55, 58
multi-monitor display 142
multi-monitor support 142
multiple subnets 224
mute 148

N
network
  add 223
  add from client 225
  default settings 222
  delete 228
  edit settings 226
  LAN settings 224
  leave 228
  rename 226
  transfer 229
network connection speed 144
network load data 178
network speed 157
network types
  gateway 207
  hub-and-spoke 206
  mesh 206
not accessible 233
notification messages
  disable 186
  notifications
    screen blanking 155
offline computer 233, 234
offline computers 36
one-click access 129
online computers 36
open a new tab 127
open files 178
open ports 177

P
password
  change LogMeIn account password 9
  clear saved 155
  Windows or Mac 130
patch management 64
pen drive
  connect during remote control 147
permission to remote control a host 182
permissions
user 65, 67, 99, 109
personal password 189
plan
definition 51
set up 59
prevent input on host during remote control 146
prevent input on host when connection is lost 184
prevent others from seeing you work during remote control 145
printed security codes 18
printing
from the host to the client 148
priorities 175
profile 36
profiles 99, 106
proxy settings 22, 186

R
RCREC 184
reboot 172
receipt 9
record remote control sessions 184
REG files 56
regional settings
keyboard 231
Registry Editor 170
registry keys
view a list 179
registry settings 56
remote control 241
customize the toolbar 145
go directly to 127, 128
move data 146
permission from a host user 182
presentation 147
record remote control sessions 184
security 145
system management 149
time out 184
remote deployment 23
remote printing 148
remote sound 148
remove a computer 40
reports 111
add a report 116
types 111
requirements 51
resolution 141
restart host 172
right-click 150
RSA SecurID 190

S
saved credentials 138
scheduling 59
screen moves (option) 150
screen resolution 157
screen size 142
scrolling wheel 150
security 189, 194, 211
authentication attack filter 193
denial of service 192
during remote control 155
host authentication 130, 189
IP address filtering 191
LogMeIn account 10, 17, 18
personal password 189
protecting passwords 155
remote control 145, 146, 184
security during remote control 146
select text 151
send files 54
Services
starting, stopping, restarting 168
session
timeout 158
session recording 184
share files 124
shared resources 174
shortcuts
how to enter shortcuts using key combinations 152
silent install 26, 27
single-click 150
single-click access 130
smartphone as client 126, 139
sound 148
sound card
used for remote sound 148
special keys 152
speed
change display color to improve 156
change Network Speed to improve 157
stop sharing files 124
subscription 208, 210
subscriptions
view a list of available 10
support session 197, 199
support session troubleshooting 200
switch active LogMeIn profile 36
switch between monitors 151
sync clipboard 146
system requirements 211
client device 126, 139
host 21
system tray
display/remove system tray icon 186

tags 221
assign 222
create 222
manage 222
task
  definition 51
Task Manager 149
taskbar 186
TCP/IP ports 177
time
  change system time 174
time out
  from remote control 184
  lock host 184
time zones in reports 120
timeout 158
track progress 62
transfer network 229	
two-factor authentication 12
two-step verification 12, 13
typing 152

U
unattached client 206
unknown user name or bad password 235
unmanaged computers 197
update
  host software 188
USB stick
  connect during remote control 147
user
  add 68, 70, 106
  move to group 111
  permissions 65, 67, 109
user access 43
user access control 194
user management 99
users
  gain access to another user’s computers 105
  invite 99

V
version
  update to latest LogMeIn software 188

video 241
view
  log files 187
view a host without taking control 173
viewing computers 32
  Detail view (more computers, fewer graphics) 34
  List view (best for large accounts) 34
  Tile view (fewer computers, more graphics) 34

W
wallpaper
  disable 180
wheel 150
whiteboard 147
Windows
  Application Event Log 168
  autologon 172
  Computer Management, Local Users and Groups 167
  Event Viewer 168
  Group Management 167
  password 130
  Processes 169
  Registry Editor 170
  Scheduling Priorities 175
  Security Event Log 168
  Services 168
  System Properties, Environment Variables 173
  System Properties, Virtual Memory 173
  User Management 167
Windows Task Manager 149
WSUS 64

Y
Your input is being blocked 183

Z
zoom in and out 150