⊗ Central
by LogMeIn

TOP 10
LogMeIn Central Features to Support a Remote Workforce

More IT teams are supporting a remote workforce than ever before. As an IT professional, it can be a challenge to support remote workers while balancing both employee productivity and company security. LogMeIn Central is here to help you address that challenge with reliable remote monitoring and management for your ever-changing IT environment.

Whether you're a new LogMeIn Central user or a seasoned veteran, we want to make sure that you understand how LogMeIn Central can help you to support your remote workforce. This guide will give you step-by-step instructions for familiarizing yourself with the most powerful and valuable features that Central offers for supporting a remote workforce.

Before doing anything else

Log in to your Central account with your LogMeIn ID.

Install the LogMeIn Central agent onto at least one computer in your network. Learn the step-by-step process **here**.

Table of Contents

Task #1
Execute a Remote Control Session

What is it?
Remote Control is the ability to see and interact with a computer screen as though you were sitting directly in front of it.

How will it help me?
Our **Remote Control** has 99.9% uptime allowing you to securely and intuitively access computers or servers from any computer or mobile device in any location. Regardless of where your employees or you are working, you'll be able to interact with the computer as if you were sitting directly in front of it. By providing multi-monitor support and putting security first with screen blanking and computer locking, Central protects and simplifies your business.

Use case
Hannah is an IT technician who supports her globally dispersed remote workforce from her home office. She utilizes Central's remote control to access and manage her endpoints for her remote employees. Whenever an employee submits a ticket that requires her to be in front of their computer, she can quickly remotely access their desktop to execute required tasks and get her employees up-and-running again.

Time: 3 Min
Try it for yourself ...

1. Navigate to the **Computers** tab in the left-hand menu

2. Click the computer icon 🖥 in the **Direct Connect** column for the endpoint that you would want to access

3. Input the username and password for the computer you are accessing

4. Begin your remote session! Accomplish everything that you can do in front of a computer from any location

Additional Resources
Visit our documentation site **here** for additional help.

Task #2
Remotely access a computer without impacting the end-user

What is it?

Background Access allows you to see the background of a machine from any location without interrupting an end user. With the ability to transfer files, run an installation from an MSI, update a user's password, see all the tasks being run, and more, background access is a powerful tool for troubleshooting issues and aiding remote employees.

How will it help me?

Background Access allows you to troubleshoot and do prescriptive maintenance without interrupting the end-user from either the LogMeIn website or Client App. This helps you to maintain your remote employees' machines without interrupting their productivity.

Use case

Mike is a help desk technician at a law firm where the lawyers are working remotely. At the firm, lawyers bill in six-minute increments so it is imperative to the firm's bottom line that Mike can manage the lawyers' computers without interrupting their work or productivity. Mike relies on **Background Access** to install software and troubleshoot potential issues to avoid end user interruption.

Time: 6 Min
Try it for yourself ...

1. Navigate to the **Computers** tab in the left-hand menu

2. Click the dashboard icon 🏠 in the **Direct Connect** column for the endpoint that you would want to see implement a background access session

3. Input the username and password for the computer you are accessing

4. View the **Dashboard** to see system information, events, processes, network traffic and more as well as perform maintenance to a machine

5. Click **Computer Management** in the left-hand menu to view all the endpoint manipulation options available to perform without interrupting the end-user

Additional Resources
Visit our documentation site **here** for additional help.

If you want to...

- **End a process the computer is running:**

  On the **Dashboard page**, click on the item that you want to end in the **Processes** box. In the details for that item, click the red X in the upper-left of the page to end that process.

- **Install or remove files from a machine:**

  Click on **File Manager** in the left-side panel to see side-by-side the files on your computer as well as the target machine. Drag-and-drop files on and off the machine to add or remove files.

- **View the events on a machine:**

  Click on **Computer Management** in the left-side panel and choose **Event Viewer**. Here you can find the list of events on a machine.

- **Determine what is draining processing power on a machine:**

  Under **Computer Management**, choose **Processes**. In **Processes**, you can sort by **CPU %** to see which processes are draining your machine. You can also kill off a process, by clicking the red X in the upper-left corner.

- **Schedule a computer reboot:**

  Under **Computer Management**, choose **Reboot Options**. Select **Scheduled Reboot** and choose the date and time that you would like the reboot to occur.
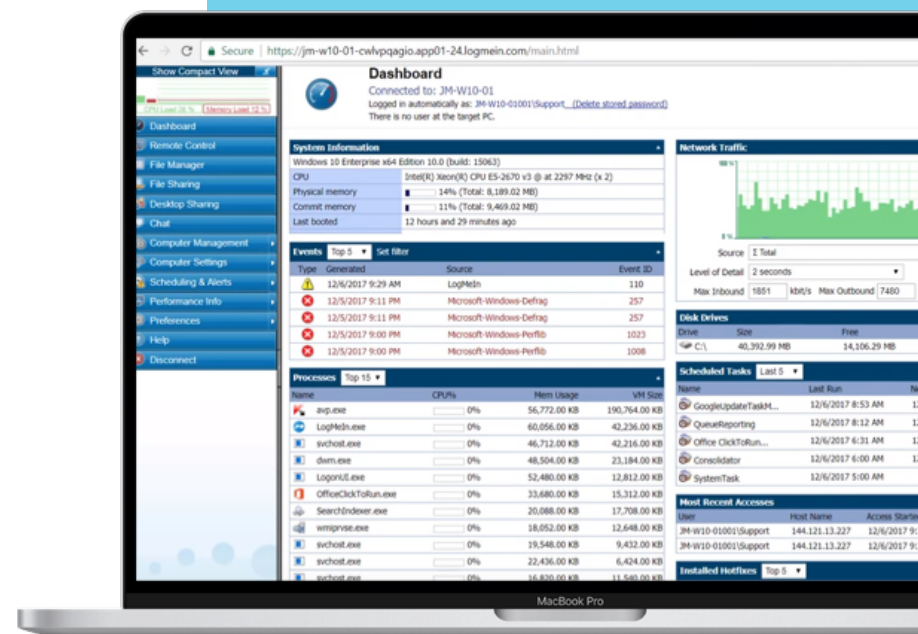
Task #3
Remote Installation and Deployment

What is it?
LogMeIn Central allows you to deploy to your users' computers, from any location. There are four options for remote deployment: installation link, installer file (.msi), installer executable (.exe), or a silent install with a command or batch file. Silent installs with a command or batch file require no assistance from your end-users and can be completed in mass.

How will it help me?
With remote deployment, you do not need to wait to be in front of the computer or in an office to remotely access and manage the endpoints of your remote employees.

Use case
Sophie has a new remote employee who just joined her company. With LogMeIn Central, Sophie runs a command file to silently install the software on her employee's computer so that she can manage that computer no matter where she or the employee is located.

TIP: Prior to creating your Central deployment package, finalize your Host Preference Packages. **Host Preference Packages** allow you to create customized settings that will be applied to your computers. For example, with Host Preferences Packages, you can determine if your users are able to turn off LogMeIn or if the content of a remote control session is recorded. In deployment, you will be able to link a Host Preference Package to the deployment to ensure the correct customizations.

Time: 6 Min
Try it for yourself ...

1. Navigate to the **Deployment** page

2. Click **Add Installation Package**

3. Fill in the necessary fields and select the appropriate options for the remote installation

4. Under **Configuration**, select the **Computer Group**, **Alerts package**, and **Host Preference Packages**

5. Click **Save Settings**

6. On the **Deploy Installation Package** page, select the Deployment method to be used by the installation package (installation link, installer file (.msi), installer executable (.exe), or a silent install with a command or batch file)

7. Execute installation

Additional Resources
Visit our documentation site **here** for additional help.

Task #4
Manage users and provide remote access to employees

What is it?

User Management is how you add and assign different user permissions within LogMeIn Central. With **User Management**, you can organize your technicians by user group and assign access to different features within Central. With this feature, you are also able to provide your employees with the ability to remotely access their work computers from anywhere

.

In Central, you can invite an **unlimited number of users at no extra cost**. This can provide additional value for those who require remote access for their users to access their work desktops remotely. With **User Management**, you can restrict the computers your user can remotely access to only their personal computer or the computers within their environment.

How will it help me?

With unlimited users, you can organize all your users at no additional cost and maintain strong security standards by having one log-in per user. This helps to maintain compliance standards when allowing users to remotely access their desktop or when IT teams perform routine computer maintenance.

Time: 5 Min
Try it for yourself ...

1. Navigate to the **Deployment** page

2. Click **Add Installation Package**

3. Fill in the necessary fields and select the appropriate options for the remote installation

4. Under **Configuration**, select the **Computer Group**, **Alerts package**, and **Host Preference Packages**

5. Click **Save Settings**

6. On the **Deploy Installation Package** page, select the Deployment method to be used by the installation package (installation link, installer file (.msi), installer executable (.exe), or a silent install with a command or batch file)

7. Execute installation

Additional Resources
Visit our documentation site **here** for additional help.

Use cases

1. Dustin is an IT technician responsible for setting up his employees with the ability to remotely access their work desktop from any computer. With Central, Dustin can utilize **User Management** to assign each of his employees with remote access to their work desktop. This ensures that his team members can access the tools to perform their jobs while maintaining strong compliance standards.

2. Connor is an IT Director that manages a team of 8 with a variety of specialties and skill-levels. He uses **User Management** to regulate which team members have access to the different features within Central. With his help desk technicians, Connor provisions their accounts to only have access to Remote Access. For his security professionals, Connor provisions them with access to the Managed Antivirus and Windows & Application Updates. This helps him ensure that only his team members with the knowledge to perform a task can access that feature.

TIP: User Management is where you set up **Two-Factor Authentication** for your employees accessing Central. With provisioning **Two-Factor Authentication**, users will be prompted to authenticate their identity via the LastPass Authenticator App (or any other TOTP-based authenticator app) prior to gaining access to Central. It is recommended to use **Two-Factor Authentication** to decrease the risk of unauthorized access to your Central account. You can customize this setting by User Group or individual users. For additional security, consider also customizing a login policy to ensure your users are employing strong passwords when accessing Central. Learn how to set this up **here**.

TIP: User group permissions take precedent over individually set permissions

Additional Resources
To learn more about setting up two-factor authentication, visit our documentation site **here**.

Task #5
Create computer groups

Try it for yourself ...

What is it?

Computer Grouping allows you to organize your endpoints within Central's environment to meet your needs. Your team will be able to apply packages of settings and user permission-levels based on these groups, so be sure to brainstorm what groupings would be the most useful for your team (see examples below).

How will it help me?

Computer Grouping will not only be a way to visually organize your endpoints on the **Computers** tab, but will also help when applying updates, reporting, and setting permissions on different groups of computers. This helps you to organize each of your remote computers to best suite your needs.

Use case

1. Jed is an IT technician that uses Central daily to support his clients at an MSP. To help him keep track of which endpoints belong to which client, he relies on Computer Grouping. With **Computer Grouping**, he can quickly and visually identify which computers he is accessing.

1. Navigate to the Computers tab in the left-hand menu

2. Select **Add Group** at the top of the page

3. Add your group name and click **Add**

4. Select the computers that you want to be included in this group and click **Save**

TIP: On the **Computers** page, you can create **Custom Fields** to further organize your endpoints.

Additional Resources
Visit our documentation site **here** for additional help.

Use case

2. Luke is the systems administrator for his company. He utilizes **Computer Grouping** to keep track of the computers that he uses to test updates. Prior to issuing a Windows or third-party application patch company wide, Luke runs the patch on his test computer group to ensure that it will not cause any issues.

Example Computer Groupings

- **Business Functions** (e.g. Marketing, Sales, Engineering)

- **Customer** (e.g. Law Firm A, Law Firm B, Law Firm C)

- **Functionality** (e.g. Servers, Desktops)

- **Business Unit**

TIP: To view only the computers in a specific group on the **Computers** page, click the **View Computers** button at the top of the LogMeIn Central user interface and then **Show group panel**. You will then see your computer groups in a list next to your computer list which you can select to only see the computers in a specific group.

Task #6
Create a policy with LogMeIn Antivirus powered by Bitdefender

What is it?

LogMeIn Antivirus powered by Bitdefender is a robust antivirus that is fully integrated with LogMeIn Central. With LogMeIn Antivirus, you can set custom policies for groups of computers to easily manage your antivirus. A full list of features included in the antivirus is available **here**.

How will it help me?

Remote employees tend to be more likely to download malware as they cannot quickly sanity check an email by another employee. Therefore, it is essential to have a strong antivirus in place that is configured to your remote employee's needs.

By setting policies with LogMeIn Antivirus, you can centrally configure the antivirus to meet the needs of your organization or users. From scheduling scans to excluding folders to blocking USB storage devices, policies allow you to provision your antivirus requirements efficiently.

Ues cases

1. Garrett provides IT consulting and support for three different small businesses. Each small business has a different set of requirements for their antivirus. With LogMeIn Antivirus policies, Garrett can create a specific policy to address the requirements for each client and then assign the correct computers to those policies.

Time: 4 Min
Try it for yourself ...

1. **Navigate** to the Antivirus tab in the left-hand menu and select LogMeIn Antivirus Policy

2. Choose to **Create New Policy** or edit the **Default Policy**

3. Customize the **Policy** based on your organizations specifications

4. Select **Save**

Additional Resources
Visit our documentation site **here** for additional help.

Use cases

2. At a mid-size company with remote employees, Hunter manages deploying and monitoring the antivirus in Central. He sets specific policies for different departments within the organization depending on their needs. For Human Resources and Finance, he sets an aggressive policy to ensure that the sensitive information on their machines remain secure. For contractors, he sets a more permissive policy as they are not privy to sensitive data.

Note: To assign the Antivirus Policy to a group or computer

1. Navigate to the Manage tab under Antivirus

2. Check the group or computer that you would like to assign an antivirus policy to

3. Select Assign LogMeIn Antivirus policy from the Actions menu

4. Choose the Policy that you would like to assign to the selected computers

5. Select Assign
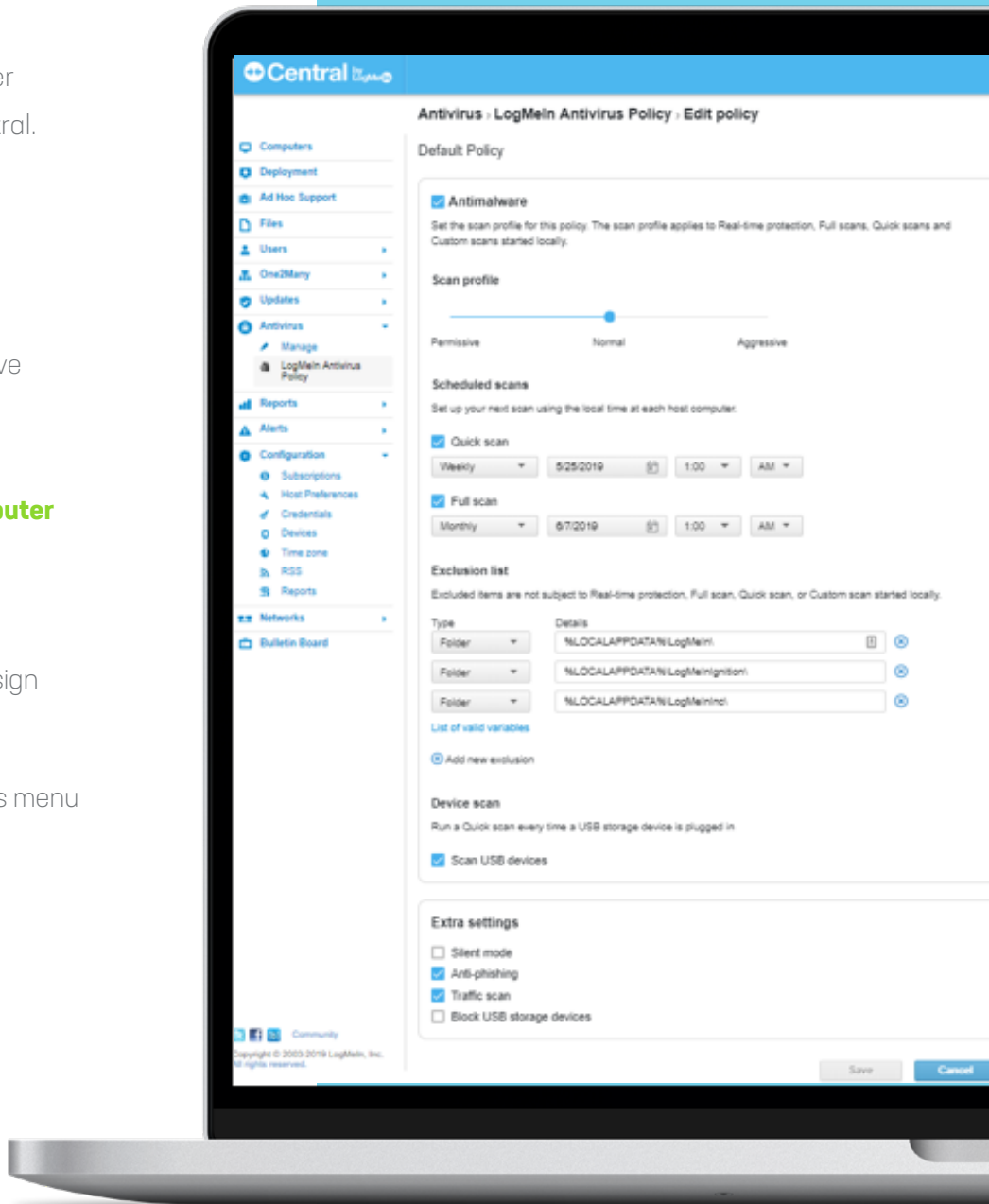
Task #7
Run a Windows or application update

What is it?

Windows and Application updates provide insight into which version your endpoints have deployed and allow you to push Windows or third-party application updates to your endpoints. See which applications are supported **here**.

How will it help me?

It is essential that your endpoints are patched with the latest versions of Windows or third-party applications to avoid cybercriminals taking advantage of known vulnerabilities. This is especially true when supporting remote employees. With Central, your team can quickly identify outdated Windows or vulnerable third-party applications and automatically deploy patches to keep your software up to date and protected against threats.

Use case

1. Beth works in IT at a marketing agency. The marketing team utilizes Adobe to create polished collateral for their clients. In order to ensure that the marketing team is always using the latest version of Adobe, Beth configured Central to automatically install updates. Not only does this keep her marketing team on the latest software version, but it also prevents cyber-criminals from taking advantage of any known vulnerability in software.

Time: 8 Min
Try it for yourself ...

Windows Update

1. Navigate to the **Updates** tab in the left-hand menu and select **Windows**

2. Endpoints requiring Windows updates will have Yellow or Red shields next to the computer name

3. Select the computers that you would like to install Windows updates on

4. Choose **Apply Updates**

NOTE:

To customize your Windows update settings, select the computers that you would like to customize and then press **Change Settings**.
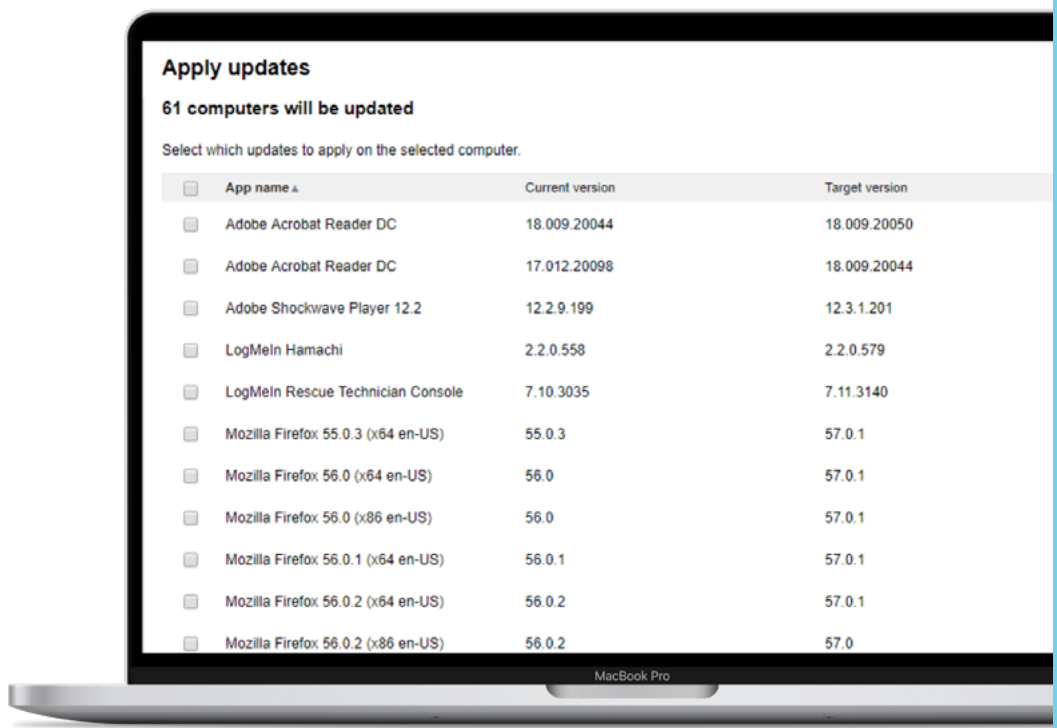
Additional Resources
Visit our documentation site **here** for additional help.

Use cases

2. At an MSP firm, Sujatha is responsible for keeping her client's Windows up-to-date. With Windows updates, Sujatha can see when a new update is available and automatically roll it out for Windows operating systems and other Microsoft software.

Apply updates

61 computers will be updated

Select which updates to apply on the selected computer.

	App name ▲	Current version	Target version
☐	Adobe Acrobat Reader DC	18.009.20044	18.009.20050
☐	Adobe Acrobat Reader DC	17.012.20098	18.009.20044
☐	Adobe Shockwave Player 12.2	12.2.9.199	12.3.1.201
☐	LogMeIn Hamachi	2.2.0.558	2.2.0.579
☐	LogMeIn Rescue Technician Console	7.10.3035	7.11.3140
☐	Mozilla Firefox 55.0.3 (x64 en-US)	55.0.3	57.0.1
☐	Mozilla Firefox 56.0 (x64 en-US)	56.0	57.0.1
☐	Mozilla Firefox 56.0 (x86 en-US)	56.0	57.0.1
☐	Mozilla Firefox 56.0.1 (x64 en-US)	56.0.1	57.0.1
☐	Mozilla Firefox 56.0.2 (x64 en-US)	56.0.2	57.0.1
☐	Mozilla Firefox 56.0.2 (x86 en-US)	56.0.2	57.0

MacBook Pro

Application Update

1. Navigate to the **Updates** tab in the left-hand menu and select Applications.

2. Endpoints requiring application updates will have Yellow or Red shields in the **Status** column.

3. Select the computers that you would like to install Windows updates on.

4. Choose **Apply Updates.**

NOTE:

To choose whether you want your updates to be manual (application updater will collect available updates but will not install any of them) or automatic (all available updates will be installed), navigate to **Change Settings**.

Task #8
Write a One2Many script

What is it?

One2Many is one of the most powerful tools in Central. With One2Many, you can write command line or PowerShell scripts to perform tasks such as uninstall a Windows update, reboot a computer or server, distribute files, and much more from any location.

How will it help me?

One2Many allows you to perform tasks across all your computers simultaneously. Save your team valuable time and resources by making changes across your entire infrastructure.

Use cases

1. As part of Donna's MSP client agreement, she is responsible for setting-up the computer for her client's new remote employees. This includes ensuring that the software and files that the new employees require are on the computer day 1. As there are usually about 20 new employees a month, Donna saves time by distributing the software and files onto all the new computers simultaneously via One2Many. She's also able to go above and beyond with One2Many by setting the company's logo as the desktop background for these new employees.

Time: 6 Min
Try it for yourself …

Create your Task

1. Navigate to the One2Many tab in the left-hand menu and select **Task**

2. Select **Create Task**

3. Choose the task that you would like to run and select **Save and Continue**

Build your plan

1. Navigate to the One2Many tab in the left-hand menu and select Plan

2. Select Create Plan

3. Name your plan and select the task to be run

4. Choose when the task will run, and on which target computers

Additional Resources
Visit our documentation site **here** for additional help.

Use cases

2. David works on an internal IT team that just received a lot of complaints after the most recent Windows update was pushed out. With One2Many, David can uninstall the most recent software so that his end-users can continue to work while his team waits for Microsoft to release a fix.

3. At her company, Alex is responsible for setting up a preventative maintenance program for their company's endpoints. As part of her plan, she set up One2Many tasks to run every Friday that clean out temporary folders to ensure disk space, backs up user profiles, and more.

4. Richard runs a digital signage business where he needs to push software updates to his 250 devices. Through One2Many, Richard can test the updates on a handful of his signs before pushing out across all his devices.

Example - Attempt to reboot a computer via command script:

1. Select **Execute a Remote Command** under Create Task
2. Name your task and ensure the language is CMD
3. **Copy Script:**
   shutdown /r /t 60 /c "Workstation Rebooted via LogMeIn Central - This workstation will reboot in less than 60 seconds."
4. Select **Save and Continue**
5. Choose to **Create a New Plan or Select from plans assigned to other tasks**
6. Finalize plan and select **Save and Continue**

Tip:
The LogMeIn Central Community Forum is an excellent place to find pre-written scripts. Be sure to visit it here: **https://community. logmein.com/t5/LogMeIn-Central-Discussions/ One2Many-Script-Repository/td-p/51032**

Troubleshooting:
Is your script not running correctly? Try troubleshooting by...

- Make sure the script runs silently when executed locally

- Check the credentials provided for the plan are valid and have sufficient permissions

- Ensure that upload.logmein.com is not blocked by a firewall.

- Check that you have access to your C:\ Windows\Temp folder

More details on troubleshooting can be found **here**.

Task #9
Create an alert package

What is it?
Set up, track and act on alerts to monitor computer health and resolve concerns before they become problems. With LogMeIn Central, you can assign a specific alert to certain machines and receive an email notification when the alert is triggered.

How will it help me?
Stay on top of your remote endpoints and prevent downtime by creating custom alert packages. In each package, you can set alerts for items such as CPU usage, software inventory, offline / online, service alerts, and more to keep your team one-step ahead.

Use cases
Marissa oversees her company's POS devices. Whenever an end-user downloads an unapproved piece of software, Marissa wants to be alerted as some software slows down POS devices. Therefore, Marissa created an event alert that will trigger an email when one of non-approved software is downloaded to the device, so she can contact the manager of that store and have them remove the software.

Time: 5 Min
Try it for yourself ...

Create your Task

1. Navigate to the Alerts tab in the left-hand menu and select **Manage Alert Packages**

2. Select **Add Alert Package**

3. Build your **Alert Package** using the templates provided under **Add New Alert Rule**

   a. **NOTE:** You can only apply one alert package per endpoint so be sure to build multiple alerts into your packages.

4. Review our **Workstation, Server**, and **Kiosk** templates under **Add New Alert Rule** for best practices

5. Choose whether to receive an email when an alert is triggered and if to include a link to remote control and inventory in email.

6. **Save** and assign your **Alert Package** to endpoints of **Computer Groups** to finalize.

Additional Resources
Visit our documentation site **here** for additional help.

Tip:

Combine alerts with One2Many tasks to create self-healing alerts. Self-healing alerts are when a designated alert triggers a One2Many task. The benefit of self-healing alerts is that they run automatically so can resolve issues with no manual intervention.

Use cases:

- Joe created a self-healing alert to manage his backups. With this self-healing alert, Joe pairs his folder size alert with a script to automatically delete files. This prevents end-user loss in productivity while saving technicians time.

- One of Kevin's clients is looking for a way to wipe a computer when it is lost or stolen. To address this client's need, Kevin created a self-healing alert that paired his alert for when a computer comes online with a script that encrypts that computer. This allowed him to protect his client from loss of data.
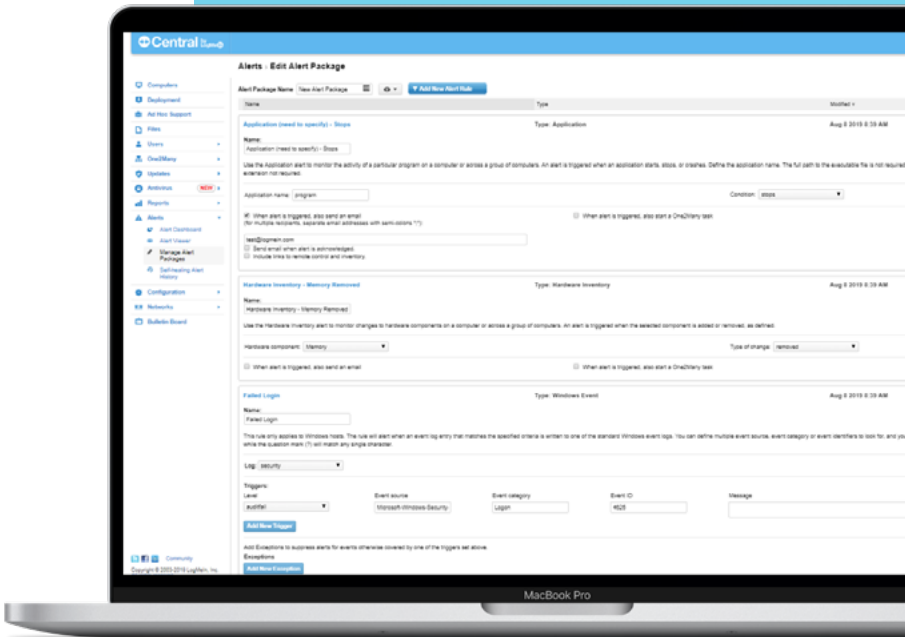
Task #10
Pull a custom report

What is it?

LogMeIn Central's **Report Viewer** allows you to pull & export detailed reports on everything from account activity and usage to hardware inventory to software inventory.

How will it help me?

Report Viewer can help you gain a better pulse on your remote IT infrastructure and provide much needed insight into both your machines and LogMeIn account. From understanding when you need to do a hardware refresh to troubleshooting problems on machines, reporting can help you stay ahead.

Return on Investment:

With our hardware inventory reports, Managed Service Providers can identify when clients may be ready for a hardware refresh. With this knowledge, they can step in as the reseller and fill their client's technology needs.

Time: 3 Min
Try it for yourself ...

1. Navigate to the **Reports** tab in the left-hand menu and select **Report Viewer**

2. In Category, select **Software Inventory**

3. Under **Report**, choose **Installed Applications** and select **View Report**

4. Filter, sort, or export this report to get an instant snapshot of your software inventory

Additional Resources
Visit our documentation site **here** for additional help.

Use cases

1. Samantha is an IT Admin who is constantly struggling with her end-users downloading unapproved software onto their laptops. This unapproved software lags the machines, which results in a higher number of end-user tickets. In order to get a handle on this unapproved software, Samantha uses the Report Viewer to view the list of software installed on each computer. This helps with diagnosing lag issues in addition to proactively requesting that these end-users uninstall unapproved software.

2. At an MSP, Patricia is responsible for managing the number of Microsoft licenses that her clients have in use to ensure that they do not overstep their current contract and owe additional money. Patricia utilizes Report Viewer to pull the software inventory for that client so that she can keep a constant pulse on the number of licenses in use.

Tip: Reporting API

For more advanced integrations or automated solutions refer to our API documentation here to get host connection URLs, access hardware and system inventory, application updates, antivirus, and custom field data.

⊗ Central
by LogMeIn®

SECURE, RELIABLE, INTUITIVE REMOTE MONITORING AND MANAGEMENT

Part of the LogMeIn Inc. Identity & Access Management portfolio, LogMeIn Central is a pure, cloud-based remote monitoring and management solution enabling IT professionals to effectively monitor, manage and secure their endpoint infrastructure. Whether you have remote employees or endpoints scattered across the globe, LogMeIn Central provides IT organizations with the speed, flexibility and insight needed to increase productivity, reduce IT costs and mitigate risk. Rated the #1 remote access tool for small businesses to manage multiple computers, LogMeIn Central equips every endpoint in your network with premium remote access so you can troubleshoot anytime, anywhere.

www.logmein.com/central