



Control Service  
Get the Most Out of Your Free Trial

Free Trial

This document will provide you with a framework for your trial, showcasing some of the most exciting features and helping you see where it can help you manage your mobile work force (and the non-mobile ones, too).

To really see what MaaS360 Control Service can do, we recommend that you install it on both IT computers and a few of your “road warriors” laptops. However, we recommend you check the out-of-compliance remediation piece on a test computer.

## Before you start the checklist, be sure to:



### Create a password and add a security question and answer.

Now that you've registered, you have access to the MaaS360 Management Center. Click the link at the top of the Mobility Dashboard to change your password and enter a security question. This step will help you if you forget the password we sent to you in your email.



### Download the software.

The email we sent you when you registered (from MaaS360@fiberlink.com) contained the link to the MaaS360 Control Service software and the license key. Download the application and install it on your computer. You will begin to see data in the Device Summary Report within three hours.




### Send the download link to your test users.

Copy the link and license key into another email, and send it to your test users. As they load the software, you will see more and more data in the Device Summary Report. You will be able to see data in the other reports 24 hours after the software is installed.

## Enjoy complete visibility and control!

# Day One: Configure and Explore

You can see data on the first day in the Device Summary Report. After one of your test users installs the software, it takes less than three hours to see data in this report. This will help you track the progress of the roll-out.

- Log in to the MaaS360 Management Center. The Home Screen appears automatically.
- Click Manage Policies link for the Manage Policies feature. This allows you to specify what the MaaS360 Control Service will monitor, and how it will respond to out-of-compliance events.
- Review the items MaaS60 Control Service can monitor. Hover over the  icon to see additional information about the corresponding item. By default, MaaS360 Control Service will monitor your end users' anti-virus and personal firewall applications, and will warn your users if their computers are out of compliance.

Click the [Restrict certain applications from running on the device](#) check box to display types of applications you may not want your users to run. When a user tries to run one of these applications, the MaaS360 Control software on the device will identify that a restricted application was launched. It will remediate the device by closing the application and will log the event for policy enforcement reporting purposes.

- Click the [Games](#) check box, then click [Save](#).



The next time your end users' computers contact the Fiberlink servers, they will receive the updated policy.

- Now let's look at a MaaS360 report.  
Click the Home Tab, then Device Summary.



This report provides device-level information in a near real-time environment.

- Click one of the computer names (it will be underlined and blue). The first tab shown on the report is the Hardware tab. See how quickly you can find the manufacturer, model and the amount of free space on the system drive for the device.

**Q:** How hard was it for you to get this information previously?

- The other tabs show information about device identity, device capacity, software inventory, and patch management.

Click the Operating System tab. It shows you information about the operating system and lists missing patches for that device.

- Click the Network tab to see the IE Proxy Settings and the Network Adaptors. Click the Type heading in the Network Adaptors section to sort the data in that column alphabetically. This is typical of all MaaS360 Control Service reports.

- Click the All Applications tab. This report shows all the applications on all the computers where the MaaS360 Control Service has been installed. Scroll down to see them all.

**Q:** Do you see any applications you didn't expect? Any that shouldn't be there?

- Click the Security Applications tab to see your security applications, organized by type.
- Click the Connection Manager tab to see information about the connection managers installed on the endpoint.

## Day One: Configure and Explore (Continued)

- Now let's take a look at the software you've just installed. On a computer with the MaaS360 Control Service software, look at the system tray at the bottom right side of your screen. It will have one of the following icons, which will show the compliance status of the device:



In compliance.



Not in compliance, but no action is being taken.



Not in compliance, and action is taken.



Compliance is pending.

These icons are visible even when the MaaS360 Control Service user interface (UI) is closed.

**Q:** Is your device in compliance?

- Double-click on the icon to open the MaaS360 Control Service UI. It shows you the applications that the software is monitoring, with one of the following icons:



In compliance. The application is running according to policy.



Out of compliance, with warning. No restrictive action has been enforced. If this condition persists, contact your Help Desk.



Out of compliance, with enforcement. A disconnect or restrict action has been enforced. You should contact your Help Desk.



Not currently monitored.

If your device is out of compliance, you will see an expanded description. Click the Troubleshooting link for help in resolving the situation.

- Close the MaaS360 Control Service UI.

Tomorrow we will examine more MaaS360 Control Service reports. These reports add business intelligence to the raw data that has been collected, and provide the results in easy-to-understand graphs and charts.



## Day Two: How Business Intelligence Changes Your Day

On the second day, the other MaaS360 Control Service reports will be populated. The Device Summary Report we looked at yesterday is updated within a few hours throughout the day, but these reports require a little extra processing time, due to the volume of the data. They run every night, providing you with fresh information each day.

- Log in to the MaaS360 Management Center and look at the top of the screen. You can see how many of your devices have installed the trial and are now being monitored.
- In the My Watch List section, you can see a list of potentially dangerous situations, and how many of your monitored devices are in those situations.

For example, your Watch List will tell you how many devices have no anti-virus or personal firewall software installed – a clear invitation to all sorts of malware. It will also tell you how many devices have old anti-virus definitions, less than optimal disk space, missing critical OS patches, and more.

- MaaS360 automatically finds out where problems are starting and displays them right at the top of the Home screen. When you log in every morning, the first thing you'll see will be the most significant issues that face your organization.

There are two pages of Watch List items. Go to the second page and review the rest of them.

**Q:** Do any of your devices fall into any of these categories?

- But MaaS360 does more than that. It will provide you with the details you need to fix any problems you find. Each Watch List item is a link to a MaaS360 report.

Click one of the Watch List items, preferably one where at least one device meets the Watch List criteria.

- Spend some time exploring your Watch List. See how easy it is to find out the information you need to put out fires before they start.

How can this information help you solve problems and make decisions faster?

- When you're finished, click the Home tab.

Below the Watch Lists is the My Actions and Reports block, where you found the Device Summary Report yesterday.

- Click the [Hardware Inventory Overview](#). Keep in mind that the computer you use to manage your policy and look at reports does not need to have the MaaS360 Control Service software. The software only needs to be on the devices you want to monitor.

- You can see the different manufacturers of your devices in the first chart. Only the 10 most popular are shown. You can also see how close your users are to running out of space on their system drives. You can see the amount of installed physical memory and the number of users on each operating system.

**Q:** How would this information help your day-to-day operations?

## Day Two: How Business Intelligence Changes Your Day (Continued)

- MaaS360 reports allow you to mouse over a bar or pie section to see the number or percentage that is being displayed. For example, you can mouse over one of bars on the Device Summary by Manufacturer Report to see how many computers were made by that manufacturer.

**Q:** How many places did you have to go to, previously, to find out this information?

- You can find out additional information by clicking on one of the bar or pie sections. Click on one of the pie sections on the Operating System Summary Report. You are taken to the Operating System tab, and the only computers listed are the ones with the operating system you clicked on. A filter for the operating system you chose has been automatically set.

To see data for all the operating systems, click the [Clear Filters](#) button at the right side of the filters area.

- Click the Device Summary tab to return to the charts and graphs. Pick another item to click on, and see where it takes you. Spend a little time exploring the different tabs, sorting data in columns and filtering for specific information. If you don't see information you expect to see, make sure that you've cleared a previous filter. Also, it's important to remember that the filters are case-sensitive.

When you are finished, click the Home tab at the top, left-hand side of the main screen.

**Q:** How would this data help troubleshoot problems with your users?

- Now, let's look at the Software Inventory reports.

In the My Actions and Reports block, click [Software Inventory Overview](#).

- The Software Inventory reports appear on the Installed Software and Software Details tabs. With what you've already learned, can you find all the Microsoft applications your users have? Can you see how many users have each one?

**Q:** How can you use this information when purchasing or renewing software contracts?

- Click the Software Details tab. Filter for information about one user. At the bottom of the screen are links that allow you to download the information in a variety of formats and print it.

Keep in mind that this report can contain a great deal of data, depending on the number of users you have. For performance reasons, you will want to make sure you use the filters to keep the amount of information manageable.

- Clear the filter so you can see all users. Now filter for Limewire or another known malicious or unwanted program.

**Q:** Do any of your test devices have this application installed? (Note: Test devices are usually less likely to have unwanted applications.)

- Spend some time exploring the Software Inventory reports.

**Q:** How can this information help you with the tasks you do every day?

## Day Two: How Business Intelligence Changes Your Day (Continued)

- Next, click the Home tab to return to the Home Screen.  
Click Endpoint Security Overview in the My Actions and Reports section.

- The Endpoint Security Summary tab shows a number of reports that focus on the security applications running on your users' computers. MaaS360 does not work like a firewall or monitor for viruses – it shows, instead, which applications are doing those jobs for you.

Look at the Installed Endpoint Security Applications bar chart. You can see the total number of computers MaaS360 has looked at, and how many have some sort of anti-virus and personal firewall software installed. You would expect that each bar would be the same – that all your users would have anti-virus and personal firewall software installed.

Continue reviewing the reports on this tab.

**Q:** What would you have done differently in the last 12 months if you had known what these reports show you?

- Click on the Summary by Device tab to see a list of the computers, and if they have a particular type of security software installed.

**Q:** Do you see any gaps in your security posture? How would this data help you if rolled out to your entire organization?

- Spend some time looking at the other tabs.

**Q:** Do any of the computers not have a personal firewall running? Are any missing critical OS patches?

- When you've finished, click the Home tab. Now we'll look at the Data Protection reports.  
Click Data Protection Overview in the My Actions and Reports block.

- The Data Protection Summary tab shows basic information about the different types of Data Encryption applications you have in your organization.

**Q:** Look at the Installed Data Protection Applications Report. How many of your users have Data Encryption software loaded on their computers? Should there be more?

- Click the Encryption tab. This report shows you the encryption posture of your devices

**Q:** Would it give you greater peace of mind to know that your company's data is encrypted, and to be able to prove it if you had to?

## Day Two: How Business Intelligence Changes Your Day (Continued)

- Before we end for today, let's see how the policy we set up yesterday (to restrict users from playing games) in action. Find a computer that has the MaaS360 Control Service software loaded on it. Make sure that the computer has been running (and has connected to the Internet) since you created the policy yesterday. The MaaS360 Control Service software on that computer will have downloaded the policy change you made, and it will be enforcing this policy. Try to play Solitaire on this computer. If you had previously set up your policy as described in Day One, the application will be launched and then immediately shut down.

Tomorrow we'll look at the Policy Enforcement module – the heart of the MaaS360 Control Service.



# Day Three: Policy Enforcement Gives You Control

Today we'll look at how the MaaS360 Control Service responded to any noncompliance events.

Keep in mind that these reports will only have data if you have defined the types of applications you want the MaaS360 Control Service to monitor, and at least one device is out of compliance.

- Log in to the MaaS360 Management Center.  
Let's start by reviewing the policy in use by your devices, because that's what drives the Policy Enforcement reports. Click Manage Policies in the My Actions and Reports block.
- If you've kept the settings we created on Day One, you'll be monitoring Anti-Virus and Personal Firewall applications. In addition, MaaS360 will not let users' computers run games.
- On a test computer that has the MaaS360 Control Service installed, access the Internet.
- Disable the computer's Anti-Virus software.

**Q:** Did you see a message over the Systray? What happened to the Systray icon?

- Right-click on the Systray icon to open the MaaS360 Control Service UI. Look at the new icon next to the Anti-Virus application. Click the [Troubleshooting](#) link to see additional details about the non-compliance.
- Log into the MaaS360 Management Center. Click [Policy Enforcement](#) in the My Actions and Reports block.

**Note:** You won't be able to see data from the out-of-compliance event we just created until tomorrow. You can, however, see out-of-compliance events that occurred before today.

- Look over the reports on the Policy Enforcement Summary tab. The reports have the same features we've seen in the other reports – you can use the filters to reduce the amount of data on the screen. You can mouse over one of the graphics (like a bar in a bar chart) and see how many items correspond to that graphic. You can click on a graphic to go to another report which shows more detail about that graphic.

**Q:** Can you see which devices have the most out-of-compliance events?

- Next, click the Enforcement Actions tab. This report shows you the actions MaaS360 Control Service took whenever your devices fell out of compliance. They will match what you specified using the Manage Policies feature (as described in Day One).

**Q:** Can you see the reasons your devices were flagged? Are they what you would have expected?

- Continue to review the data on the different tabs. Use the sort features and filters to see exactly what you need to see.

**Q:** Would it help you do your job to have this information at your fingertips all the time?

Tomorrow we will examine additional resources.



