Flextivity

Getting Started Guide

Before you set up your account, you may want to spend a few minutes thinking about what you want to get out of Flextivity. Of course, Flextivity helps you successfully manage basic security such as Anti-Malware protection and a powerful Network Firewall across the computers in your organization. However, Flextivity goes beyond this. We have included a few tools to help you get the most out of your deployment.

Acceptable Use Policies

Most employees really want to do a good job and be productive. Nonetheless, personal Internet use has been found to be one of the number one time wasters at work. Experiments have shown that people who are able to successfully resist the temptation to surf at work make more mistakes than they would if there were no temptation[1]. It's harder for them to learn new skills, too. The practical implication of this is that employers shouldn't have rules against surfing and then leave access to the web wide open. Instead, it's best to allow internet access only when it is appropriate.

Intego Flextivity gives you the flexibility to manage your acceptable use policy the way that works for you. Do you want to limit use on your office wifi, but let employees surf as they please when they take laptops home? With Flextivity, you can do that. Do you want to put reasonable limits on social media surfing in the office – say, 30 minutes over the course of a day? You can do that too. Intego Flextivity helps you balance trust and team morale while putting common sense checks in place.

To ensure this balance remains in place, we recommend transparency with your employees through an acceptable use policy. Outline what is appropriate – or inappropriate – use of company equipment. Be clear about what filtering or monitoring will be in place. And then follow that policy up with a conversation. People are more apt to be successful when they know what is being measured, and most don't mind being held accountable as long as they understand what they are being held accountable for.

Policies

In Flextivity a policy defines the settings for a related group of configuration settings or Policy Types. For example, two policies that you may configure are AntiVirus and Network Firewall. The AntiVirus policy lets you specify that real-time malware scanning should be enabled (in addition to a number of other settings.) When such a policy is applied to a device, real-time malware scanning will be enabled from that point forward.

This doesn't mean that you have to specifically configure a policy on each device. Flextivity has the concept of default policies for each Policy Type. When a new device appears in your Flextivity deployment, the default policies are automatically applied.

Default Policies

For most small businesses, one set of rules across your entire company is really all you need. Larger deployments may have a need for more complex rules, but it's easy to identify a minimum level of protection across all of your devices. Default policies let you do this. The first time you log in to set up your Flextivity account, we walk you through setting these default rules. If you do nothing else, these will be the policies that are applied to your devices and you will be up and running.

Flextivity has the following Policy Types:

- Antivirus: Ensures protection from malware. Allows control of basic anti-malware settings such as real-time and scheduled scanning, types of files scanned and what to do when malware is found.
- Network Firewall: Ensures protection from external attacks through the network. Controls settings determining who may communicate with the computer and to whom the computer may communicate.
- Network Time Access: Allows you to define when the computer may be active on the network and provide limits on different types of activity during a time of day. For example, you might configure the policy to allow access to social media for a maximum of 30 minutes during normal business hours.
- Web Filtering: Make sure that users stay away from inappropriate Web sites such as pornography.
- Screenshot Recording: Understand what users are really doing. Smart screenshot recording allows you to view what's happening on a user's computer when, for example, they go to a specific category of Web site or they type a certain keyword.
- Application Control: Control what types of applications may access the network or are even allowed to operate.
- Activity Logging: Tracks time spent on applications and websites, giving you an accurate picture of how your team members spend their day. Enabling activity logging will populate all of the Flextivity reports that you access through the web console.

See the "Policy Details" section later in this document for more information

Adding Computers to Flextivity

After you have set up your default policies (this might be as simple as just clicking through the first run screens since we provide you with a logical starting point) you will add devices into Flextivity.

When you created your account on Flextivity, we created a custom software installation package specifically for you. All you need to do is install that package on a device, and it will be added as a candidate for management in your organization. There is no need to enter any configuration information on the new client. This package can be installed in multiple ways:

- E-mail your users a link to the download package and instruct them to execute it. Once again, they will not need to enter any information, they simply have to execute the package.
- Download the package and place it on an internal server

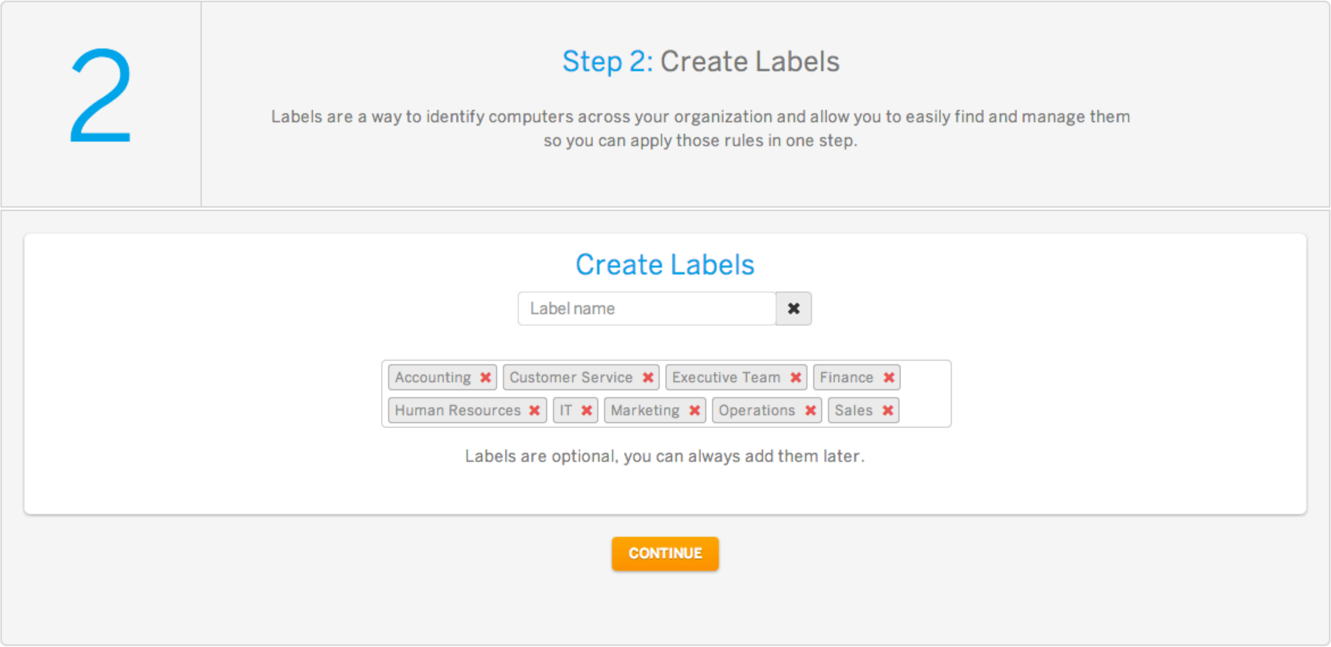
- Use Apple Remote Desktop or similar other endpoint management solutions

Once the installer package is executed on the client devices you will see them as unauthorized devices when you log into Flextivity. This allows you to control which devices consume seats from your license. Simply click the “Authorize” button on the device in Flextivity and the default policies you created before will be pushed to the device.

Organizing with Labels

Have you noticed how your Gmail account lets you create labels for your email so that you can find them more easily later? Labels in Flextivity work in much the same way. You can create any label that you like, and then apply one or more labels to any computer on your account. Later, you can use those labels to filter search results, filter report results, or easily identify a group of computers that should have a rule or policy applied. To really understand how this helps us, let’s walk through an example.

Lauren is founder and CEO of Pepino Interactive, a graphic design and digital agency with 30 employees. Lauren’s employees have a variety of roles and responsibilities, with many different needs. Lauren starts out by creating labels for the individual departments in her company. This will let her easily apply rules for groups of similar employees. She will also be able to easily filter activity reports for each department.



Labels are a way to identify computers across your organization and allow you to easily find and manage them so you can apply those rules in one step.

Labels are optional, you can always add them later.

- Accounting
- Customer Service
- Executive Team
- Finance
- Human Resources
- IT
- Marketing
- Operations
- Sales

She creates a couple more labels for managers and partners, since she knows she will want less restrictive policies for these people.

- Managers
- Partners

Now, when Lauren’s employees install the Flextivity client, she can label their computers appropriately as she authorizes them in the web console.

Reports

Congratulations!

Congratulations, at this point you are successfully using Flextivity to manage computers in your company. Many users will never need much more information to be successful with Flextivity. See the Going Deeper With Flextivity section for more information on how you can get the most from Flextivity.

Going a Little Deeper with Flextivity

More About Policies:

Creating Your Own Policies

When you first set up Flextivity we guided you through using some simple slider controls to select the policies that are applied to devices when they are authorized into Flextivity.

However, you might have reasons to apply different polices to different users. For example, you will very likely have much different security restrictions for your managing partner than you do for the receptionist.

Flextivity allows you to create custom policies. You can apply custom policies to individual computers or to groups of computers selected using labels.

Antivirus

We recommend enabling antivirus protection on all of your devices. By default, our standard protection includes real time scanning for malware targeting OS X, Linux and Windows, protecting your computers as well as keeping you from passing on malware to others. A full scan will also be completed once a day.

If you wish, you have the option to choose more or less conservative settings or customize your own policy to best suit your needs.

Firewall

When setting up a new firewall policy for your devices, our the settings default to allowing the end user to select the appropriate firewall profile the first time they connect to any given network. If you need to be more restrictive, you can hide the profile selection from the user to enforce rules for known or unknown networks. Devices running a firewall policy will have access to the Flextivity Application Monitor, which shows employees how their applications are using the network.

Network Time Access

Limiting access to the Internet during certain times of the day is one of many tactics that be used to boost productivity and help keep your team on task. The default configuration for NTA policies is fairly lenient, restricting surfing on social media websites and blogs to one hour each between 8 am and 6 pm. Let's say one of your employees reaches their one hour limit on social media websites such as Facebook and Twitter. They will see a message letting them know that they have reached their limit for the day on social media sites, and any attempts to view social media content will be blocked for the rest of the business day.

You are free to change the schedule to match your office hours, increase or decrease the level of restriction, or disable NTA altogether to allow your team to surf as they please.

Web Filtering

Intego has three web filtering options for you to choose from, with levels of protection ranging from permissive to very restrictive. You can also set your own custom filtering rules. When employees attempt to access blocked content, they will see a message telling them that the site was blocked. They will also have the option to request that the site be allowed in one click. Once the request is sent, an alert will appear in your Intego web console and once you determine whether there is a legitimate need to access the site, you can add an exception to the policy. Policies can also be configured to allow access to questionable categories, and log visited websites that match those categories so that you can view a report of websites that may be distracting to your team.

Screenshot Recording

Enabling screenshot recording on your devices will allow Intego's software to capture screenshots either on an interval, or through Smart Record, which triggers a recording session when suspicious activity is encountered.

Smart Record

Intego’s Smart Record is designed to give employers deeper insight into the context around events that occur on company owned computers. Flextivity looks for typed words or phrases or visited website categories that might be suspicious. When these events occur, Flextivity will record a series of screenshots over a five-minute period. If suspicious activity continues, the screen recordings will continue. You will receive an alert to let you know what triggered the recording. Then, you can log into the Flextivity web console to view the screenshots as they are uploaded.

Intego manages Smart Record triggers for events that could be related to sexual harassment, bullying, job searching, or corporate espionage. You can also add your own custom Smart Record triggers. We created this feature because in our experience, most employers are too busy running their business to monitor regular screenshots of employee computers. But to protect their company and their employees, they still want to benefit from insight into situations that may be a cause for concern. Intego Smart Record captures that context and allows you to make an informed decision about each situation.

Should you choose to set your screenshot recording to scheduled intervals instead of using Smart Record, the screenshots accessed in the Intego Cloud web console will be organized by day. Presently, the smallest interval available for interval recording is one screenshot every 15 minutes. This will likely generate more screenshots than you will have time to review, but can be used for general purpose monitoring and reinforce your activity reports as you are getting a feel for how your employees spend their time.

Application Control

When you first set up Intego Cloud, your ability to control applications running on your computers is limited to restricting application use to only signed applications. Once you install the Intego software on your company’s computers, we will compile a list of all the software installed on your computers. After the first few weeks, you can use the activity reports to get insight on how your team members are spending their time. If you find that there are applications that you need to restrict so that temptation is avoided and your team can better focus, you can later edit your application control policies to include those restrictions.

If you choose to create a policy restricting applications, you can choose to keep the policy from launching altogether, or only restrict that application from accessing the Internet. If you want to add an application, but you do not see it in the list, this means that it is not already installed on a computer that is managed by the Intego software. Install the software first, and the application should be added to the list within a few hours.

Activity Logging

Enabling activity logging will track how your employees spend time using applications and browsing websites. We will show you application names, document names, website URLs and website page names that are used most often by your team members. Default reporting views give you an aggregate of this data to easily identify trends. More specific usage information can be viewed by filtering Flextivity reports by label or individual device. To get the most out of Flextivity reporting, we recommend that activity logging is only disabled on an as needed basis. You may need to disable activity logging for devices that are used by employees with sensitive roles, such as human resources or finance, especially if you believe that revealing the names of the documents in their workspace will expose sensitive information to other Flextivity admins.

Location Based Rules

With more employees on the go, laptops in the office have become commonplace. Whether the laptop is provided by the company, or is BYOD (Bring Your Own Device), location based rules let you strike a balance between protection and leniency. For example, you may want to use a web filtering policy in the workplace to prevent inappropriate surfing, but allow employees to surf as they wish when they go home at the end of the day. You can create special rules based on where a computer is located, assuming that you know the wireless network that your computers will be using.

---

1. Bucciol, Houser and Piovesan, Tempatation at Work, Harvard Business School ↩