A PRACTICAL GUIDE TO CYBER SECURITY

FOR TOP LEVEL EXECUTIVES

Mike Foster

A Practical Guide to Cyber Security for Top Level Executives

Mike Foster

CEH, CISA, CISSP

A Practical Guide to Cyber Security for Top Level Executives

No part of this publication may be reproduced or transmitted in any form or by any means, mechanical or electronic, including photocopying and recording, or by any information storage and retrieval system, without permission in writing from author or publisher (except by a reviewer, who may quote brief passages and/or show brief video clips in a review). Disclaimer: The Publisher and the Author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specially disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the Publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the Publisher nor the Author shall be liable for damages arising here from. The fact that an organization or website is referred to in this work as a citation and/or a potential source of further information does not mean that the Author or the Publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

Published by The Foster Institute, Inc.
Printed in the United States of America
2016

SECURE
THE FOSTER INSTITUTE
1-800-657-7107 | www.FosterInstitute.com

CONTENTS

INTRODUCTION

You are interested in improving security. But sometimes it is tough, even for busy IT departments, to know where to start.

This guide is designed to help both executives and IT professionals along the journey to making your organization more secure.

Each chapter contains information for two key groups of people: There are "plain English" explanations for executives, as well as how-to information to get your IT professionals jump-started quickly.

One purpose of this book is to dispel confusion. There is a lot of bad advice out there, even from seasoned IT professionals.

Even worse, the attackers are always one step ahead, finding ways around protections that used to work. There is a constant flow of new products that claim to protect your organization from all security threats and even whiten your teeth at the same time.

Chapters two through five are arguably the most important things you can do, as of this writing, to protect your organization's computers from attacks.

And yes, some of the suggestions in this booklet seem difficult to implement. Attackers are relentless and very sophisticated, so you need to be too.

One of the best things is that your organization may already own everything you need in order to implement these strategies. That is a relief. You can help your organization become significantly more secure without needing to invest more money beyond what you've already spent.

Use all of these suggestions at your own risk. All mistakes are mine. Nothing is guaranteed.

This book is targeted to offices that use Microsoft Windows servers and workstations. However, since so many executives ask about wanting to protect their own personal computers, here is what can apply:

	Personal Windows Computer at Home	Apple Macs
Chapter 2 – Application Whitelisting	n/a	n/a
Chapter 3 – Click-to-Play	Yes	Yes
Chapter 4 – Patches	Yes	Yes
Chapter 5 – Local Administrators	Yes	Sort of
Chapter 6 – One-Tap Logon	Yes	Yes
Chapter 7 – Web Content Filtering	Yes	Yes
Chapter 8 – Image Backup	Yes	Yes
Chapter 9 – EMET	Yes	n/a
Chapter 10 –Encrypted Storage Areas	Yes	Yes

Chapter 1

A Memo from the Executive Team to the IT Department

The first step to protecting yourself is to communicate openly with your internal IT department.

If your organization relies on an outsourced company, all of this applies, and maybe even more. As dedicated as your outsourced firms are, they still don't have as much at stake if you suffer a devastating hacker attack.

The following memo to your IT team is mandatory if you want to ensure great success. Use it.

Before you start the conversation, there are a few things your IT department will want you to know.

Sometimes they need you to buy stuff. Thank goodness, you can probably implement everything in this book utilizing the tools you've already paid for. Nevertheless, if one of your servers is six years old, it is time to replace it.

Communicate openly with your IT professionals. Find out their challenges and allow them to be part of the decision making process in your organization. These days, almost everything affects, or is affected by, IT in organizations.

Your IT team is very busy. Many executives have no way to judge how long something will take when it comes to IT. Sometimes an IT professional performs a miracle, and their executive is incapable of appreciating what was involved. That's the nature of IT.

IT departments are not going to be excited about your adding to their list of things to do unless you temporarily permit them to postpone something else.

Since IT professionals are so busy, they have to choose what to work on first. Think of it like triage in the ER. Heart attacks get attention first, boo-boos last. But, unfortunately in organizations, executives only get to see part of the picture.

There are two categories of problems IT professionals need to solve: Problems that are visible, and problems that are invisible. The IT professionals know they need to do both. But they don't have time. So, unless you've discussed this, they feel forced to prioritize visible problems to stay in your good graces. After all, they are rewarded for fixing visible problems. But often nobody appreciates them if they fix an invisible problem or proactively prepare for possible events.

An example of a visible problem would be if users were unable to send or receive e-mail attachments. That's visible, people are frustrated, and IT professionals are expected to fix that.

An example of an invisible problem is that perhaps your network's servers do not have a functioning anti-virus solution. This problem is "invisible" to you since there is a good chance that nobody knows outside of your IT team.

Now, throw into the mix the fact that most IT professionals are so busy that they will never get caught up.

So, executives, what would you expect them to work on? Issues that are visible, or invisible? If they want to be appreciated, or avoid getting criticized, they will naturally work on the visible. Sometimes IT professionals are doing everything they can to just keep their heads above water.

Then, when the servers get hacked, sometimes executives blame the IT department. Be sure you have the discussion about visible vs. invisible tasks now, and provide your support so they can get their jobs done the most effectively.

Use the following memo to start the conversation and assess the risk your organization faces.

Memo: Cyber-Security Risk Assessment of Our Organization

Memo From:	**Today's Date:**
To:	**Due 5 days from now**

I participated in an event on the topic of cyber-security. It heightened my awareness of the need for me to be closely involved in assessing and reducing our risk to this growing threat.

My next step is to have you brief me on several aspects of our cyber-security risk profile. I am well aware that there are many factors that may have limited your ability to implement some of these strategies. My intent is not to grade your performance; rather, it is to get a candid picture of our risk today to facilitate decisions on what the team needs to do going forward.

I have a sense of urgency about this. Please report back no later than 5 days from now. If that is insufficient time to complete the list, bring me what you do have and then bring the remainder 5 days later.

Thanks in advance,

____

1. **Provide a summarized report showing the application, version, and number of computers on which the application is installed, using the format below. NEWT can help. Our list will be longer:**

Application	Version	Computers
Adobe Flash Player	10.1	390
Adobe Flash Player	21.0	777
Adobe Reader 9.3.4	9.3	150
Adobe Reader 9.4.0	9.4	2770
Google Chrome	40.0	10
Google Chrome	66.19	251

Java 7 Update 67	7.0	135
Java 8 Update 91	8.0	2
Microsoft SQL Server	11.1	10
Mozilla Firefox	45.0	844

2. **When we meet, I'd like to discuss:** Uninstalling all non-essential applications, and upgrading to the most recent version of applications, especially browsers, Flash, Java, and Adobe Reader.

3. **Brief me on the extent to which we implement Application Whitelisting.**

4. **When we meet, I'd like to discuss disabling Flash and Java in browsers, or using click-to-play** in browsers including Firefox, Chrome, Safari, etc.

5. **How aggressive are we at applying critical security patches?**
    - I understand about the benefits and risks of deploying those patches.
    - I understand there are tools such as Ninite, LANGuard, and others that might help you.
    - There is a three-step process that mitigates the risk of patches causing problems.

6. **Provide me with a list, not percentage, of missing critical security patches for the following**. (Going forward, please send me that list every Thursday)
    - Flash, Java, Reader and browsers including Safari, Firefox, Internet Explorer, Chrome, etc.
    - Operating Systems.

7. **Show me a list of the domain users whose user accounts are local administrators on their computers.**
    - What will it take to shrink the list to zero?
    - I understand that some programs can make this difficult. It was recommended to me that Microsoft's program LUA BugLight can help you avoid needing to provide local admin access.

8. **Do we use desktop virtualization for all users, not just remote users?**
    - VDI (Virtual Desktop Infrastructure) – Users each get a whole virtual computer.
    - RDSH (Remote Desktop Session Host) – Users share applications on a server**.**

9. **Brief me on our current authentication policy and any changes you recommend.** Include the following in your assessment:
    - Centrally managed enterprise versions of password managers for web passwords.
    - Two-step logon for administrator accounts at a minimum, then remote users, and perhaps all users.
    - Have we considered one-tap logon via an app on a smart phone?

I might decide to bring in a cyber-security specialist for the sole purpose of assisting you, acting as another set of eyes, and to be a resource for you. You are busy. I want to help you protect our organization. That way, we can all sleep better at night.

Chapter 2

Application Whitelisting

Many cyber security experts will tell you that Application Whitelisting is the number one most effective tactic you can use to increase your level of cyber-security.

You are likely aware of the potential and potent dangers that exist when a user clicks on a bad link in an email message. Opening an email attachment can be just as dangerous. Similar problems occur when a user plugs a virus-infected USB storage device into a computer.

You can reduce the risk of devastation by utilizing a wonderful technology called application whitelisting.

Application whitelisting is, in essence, the opposite of anti-virus. Anti-virus tools, while important to have, work to block viruses that it knows about. When a virus is detected, the anti-virus tool will prevent the virus from executing. But sometimes viruses, especially polymorphic viruses that change themselves every several hours, can slip past an anti-virus program.

Application whitelisting tools, on the other hand, look for approved programs in order to permit them, and only them, to run. In essence, with application whitelisting, you specify which application programs are allowed to run on your computers. There is no reason to be concerned with which programs are not allowed to execute. When protecting your organization from cyber-threats, application whitelisting has the possibility of being significantly more effective than anti-virus. However, the two technologies can and should be used simultaneously.

Another way to grasp the concept of application whitelisting is to imagine a party that is by invitation only. When people come up to the door of the party's location, they are permitted to enter, or they are turned away, based upon whether or not their name is on the guest list.

To implement application whitelisting, you and your IT professionals make a list of "approved programs" such as Microsoft Word, Excel, PowerPoint, IE, Firefox, Chrome, Adobe Reader, and any other programs you use. NEWT Professional is an example of a tool that can generate an inventory of installed applications, although there are many tools available. Your IT department may already have such a tool.

Using the documented application inventory, you and your team can identify which programs are essential to your organization. Then your IT professionals can configure application whitelisting in such a way that only those applications are permitted to function. Your IT professionals can also configure application whitelisting solutions in such a way that upgrades and patches are allowed to run as well without specific administrator intervention.

Now here's some good news: You already own Microsoft's application whitelisting tool called AppLocker. That means the tool is free! Microsoft's AppLocker works with many versions of the Windows OS. If you have a home or basic version of Windows, you might need to upgrade. Please note though that AppLocker cannot block older 16-bit DOS applications, Java files, and Perl scripts. Refer to Microsoft documentation for a complete list.

Other than using Microsoft's AppLocker, other security product providers are adding application approval to their suites. The third party tools generally can make the process of implementing and maintaining application whitelisting easier for IT professionals.

Know that application whitelisting isn't well known. As a result, it is not "in demand," nor is it widespread, though it should be. As a result, application whitelisting tools and experience is somewhat limited. Therefore, when you introduce this topic to your IT team, it may be the first time they've heard of it.

Be prepared for possible resistance, but be insistent. They may give you a list of reasons why application whitelisting will cause problems on your network. While there were difficulties years ago, the technology has matured to the point that it is solid and reliable if configured properly. You and your organization's finances and reputation are what will be hurt the most in a breach. Add the protection that whitelisting can provide. Don't let this be postponed.

IT professionals are very busy with all of the other tasks for which they are responsible. They often cannot spare the time to learn and configure AppLocker or any other application whitelisting tool. Therefore, free up time in their schedule by encouraging them to postpone some other task on their long list of things to do.

Additionally, why should a busy IT department have to set aside time to learn something they will only use once? The answer is simple: Because you need application whitelisting! The information in this chapter will give them a jump-start. You may even consider having someone very familiar and experienced with configuring application whitelisting to walk him or her through the setup process.

Remember, if a security control is difficult for IT professionals to implement, then attackers can assume the control is missing and that makes attacks that would normally be blocked more attractive.

Your safety net for implementing application whitelisting is the audit only mode. That is, application whitelisting tools can all operate in an "audit only" mode. That means, as you are testing your application whitelisting solution, you do not have to be concerned about generating an outage on your machines. Computers will continue to function as usual, and you will be able to preview which applications would and would not have been blocked.

This "audit only" mode has two big benefits that will help you feel more comfortable when you implement application whitelisting. First, you have plenty of opportunities to be sure everything is configured before you engage the actual application whitelisting. Second, the audit mode is your "safety net" in the event that a good program was overlooked in the approval process of application whitelisting. If the security control causes a widespread outage and you need to "get everyone up and running again," you can temporarily put the application whitelisting tool into the audit only mode and everyone will be able to work until you resolve the problem.

The implementation of application whitelisting can be simplified by wizards. The core objective of application whitelisting is to create rules that define which applications are approved to execute and which are not. Rules are what application whitelisting is all about, and the wizards can make the process much easier. However, the wizards can be evil too, tempting your IT professionals to implement too much security before the basics are handled first. Some rules are good to implement right away; other rules need to wait until a later phase.

Encourage your IT professionals to refer to Microsoft's documentation of how to use something called GPOs to deploy the rules based on departments, roles, etc. Remember that commercial tools can help automate this entire process.

As great as application whitelisting is, be aware that it is not complete protection. A notable exception is that application whitelisting won't necessarily block programs that run inside of your browser. You will be able to specify which web browsers are approved, but once the browser is running, then application whitelisting will not block content based on tools such as Java, Flash, or Reader. Protect these problems using other information within this book. A technique called click-to-play is covered in the next chapter.

The bottom line is that every business should implement application whitelisting. Your organization will be even more secure. I'd even go so far as to say that implementing application whitelisting can be the single most powerful way to increase security protection for your entire network. Ultimately, when you embrace this technology, you will be on the leading edge, not the bleeding edge.

How to Implement AppLocker to Enhance Windows Security

Executives, these are instructions for you to provide your IT department if they would benefit by having a quick-start guide. The instructions are for the Microsoft tool AppLocker. AppLocker is very powerful, has many capabilities, and is available for no charge from Microsoft. The instructions below are basic and enable you to achieve great value in less time.

A phased approach to implementing AppLocker is highly recommended.

Before implementing AppLocker, it is highly recommended that you revoke local administrator rights for all users. That task is addressed elsewhere in this book.

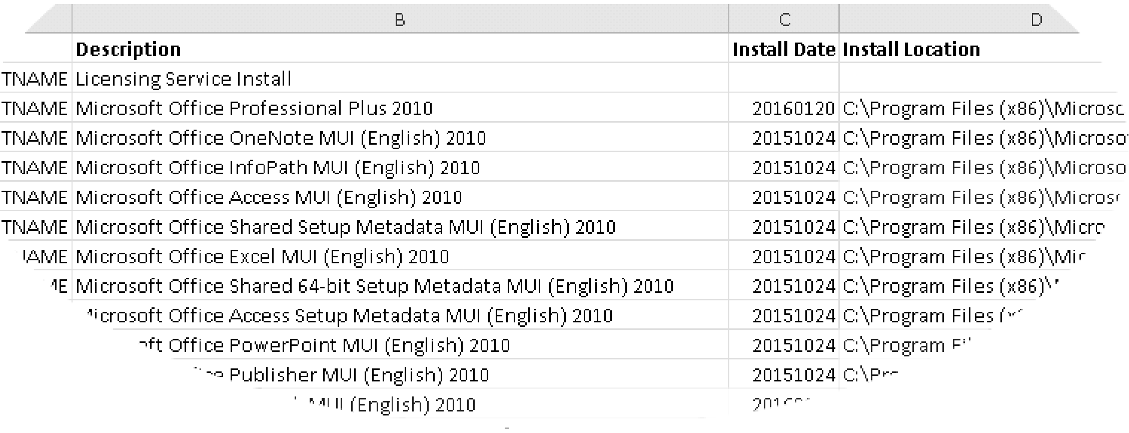
Note: Without proper planning and execution, AppLocker can prevent line of business applications from running and thereby negatively affect user productivity and their ability to get their work done.

Fortunately, there are ample opportunities to test prior to engaging the blocking feature. The testing is accomplished by using an audit mode prior to activating the protection. You'll be able to know what will, and won't, be blocked before you engage the application whitelisting feature.

Phase 1: Planning

The first step is to ensure that all line of business applications are identified prior to defining and enforcing AppLocker rules. In other words, you need to know what programs your organization needs to use. To do that, gather a software inventory of installed applications, then export that software inventory to an Excel spreadsheet. This phase can be automated by using Windows Management Instrumentation (WMI) or by using third party software. One of the programs other customers have used is a program called NEWT.

Your inventory will be much longer, and here is an example of part of a spreadsheet:



	B	C	D
	Description	Install Date	Install Location
STNAME	Licensing Service Install		
OSTNAME	Microsoft Office Professional Plus 2010	20160120	C:\Program Files (x86)\Microsc
OSTNAME	Microsoft Office OneNote MUI (English) 2010	20151024	C:\Program Files (x86)\Microso
OSTNAME	Microsoft Office InfoPath MUI (English) 2010	20151024	C:\Program Files (x86)\Microso
OSTNAME	Microsoft Office Access MUI (English) 2010	20151024	C:\Program Files (x86)\Micros
TNAME	Microsoft Office Shared Setup Metadata MUI (English) 2010	20151024	C:\Program Files (x86)\Micro
AME	Microsoft Office Excel MUI (English) 2010	20151024	C:\Program Files (x86)\Mi
E	Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010	20151024	C:\Program Files (x86)\
	icrosoft Office Access Setup Metadata MUI (English) 2010	20151024	C:\Program Files (
	ft Office PowerPoint MUI (English) 2010	20151024	C:\Program F
	Publisher MUI (English) 2010	20151024	C:\Pr
	MUI (English) 2010	201	

Once a master software inventory has been compiled in the spreadsheet, review that inventory and identify the software to determine what applications are essential for business. The fewer applications you have, the more secure your system will be.

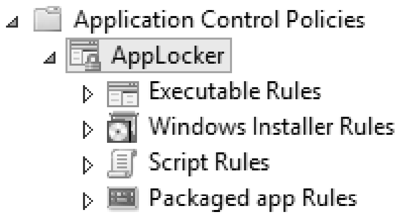
If there are some software vendors for which all of their software needs to be trusted, make note of those vendors too.

Finally, decide which users and PCs you want AppLocker rules applied to, decide which types of executables you want to restrict (i.e. EXEs, MSI installers, and scripts), and decide who will be responsible for maintaining the AppLocker system in the long run.

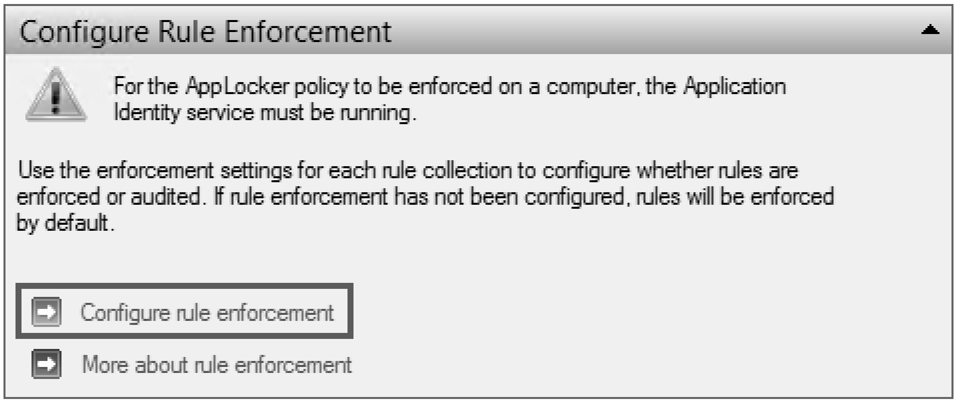
Phase 2: Creating a Group Policy Object (GPO) and Defining AppLocker Rules

To create the GPO, you'll use a test computer. Perform the following steps on the test computer:

- Install all applications listed in the Excel spreadsheet.
- Install the Group Policy Management console (GPMC).
- Create a new GPO; name it AppLocker.
- Edit the new AppLocker GPO, then drill down into the Application Control Policies and select the AppLocker node.



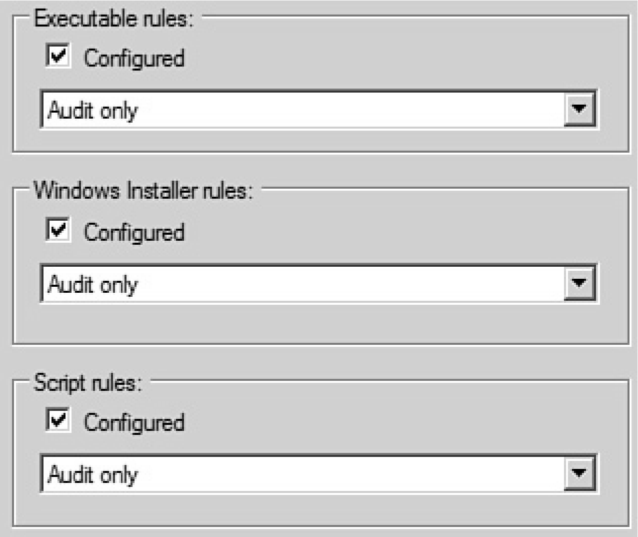
- Click on "Configure rule enforcement" and enable "Audit only" mode for each type of executable content you wish to control. Using the audit only mode provides you the opportunity to test the configuration without affecting user productivity. Audit only doesn't actually block the applications; it just shows you what applications would have been blocked so that you can tune the configuration.


Configure Rule Enforcement

For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.

Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.

Configure rule enforcement
More about rule enforcement



Executable rules:

☑ Configured

Audit only

Windows Installer rules:

☑ Configured

Audit only

Script rules:

☑ Configured

Audit only

- Under Executable Rules, run the "Create Default Rules..." wizard to create the baseline rules to allow built-in Windows apps to run.

- Under Executable Rules, run the "Automatically Generate Rules" wizard to capture all executables installed under the "Program Files" and "Program Files (x86)" folders of the Windows system drive. You may also want to rerun this wizard against other non-standard folder locations where you know line of business applications are installed.

- Referring to your Excel spreadsheet, create additional rules for all remaining applications. Limit the scope of each rule so that it applies to the appropriate group of users, then specify the conditions for which the rule should be triggered. For example, you may want to create a rule to allow all Adobe software, in which case you would use the "Publisher" condition. Or you may wish to allow all executables contained within a specific path, in which case you should use the "Path" condition.

- If you wish to create AppLocker rules for scripts and MSI installers, then create default, automated, and custom rules for those execution types as well.

Phase 3: Enable Audit Mode on a Single Test PC, then Find Exceptions

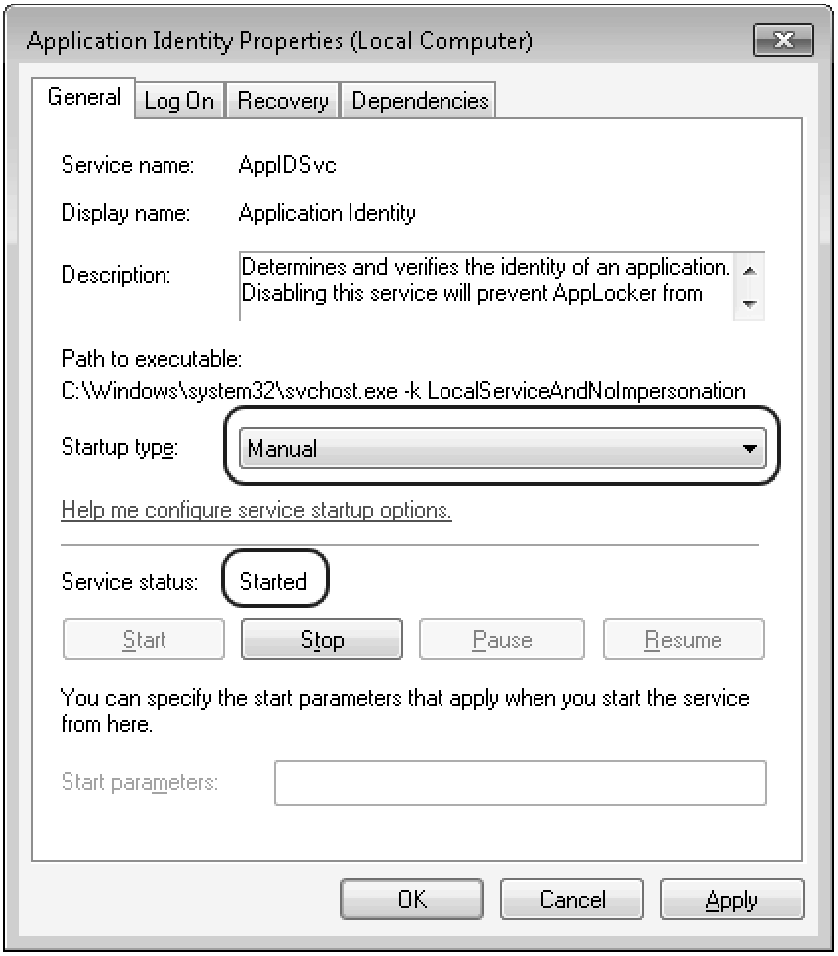
Perform the following steps on a single test PC.

NOTE: To minimize risk, you may wish to create a new computer organizational unit (OU) in Active Directory, then move the computer account of the test PC into that new test OU.

- Using the GPMC, link the AppLocker GPO to the appropriate OU (this must be an OU containing the computer account of the test PC).

- Run gpupdate on the PC.

- Using the Control Panel services applet, start the Application Identity service on the PC, but leave it in Manual startup mode.



Application Identity Properties (Local Computer)

Service name: AppIDSvc

Display name: Application Identity

Description: Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation

Startup type: Manual

Help me configure service startup options.

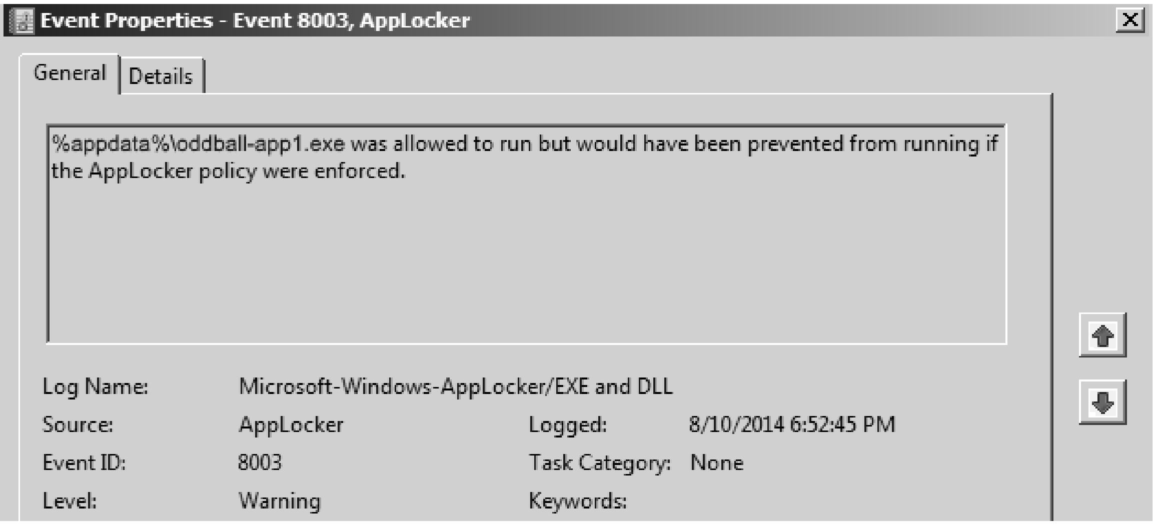
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

- Run each and every line of business application, the programs that are essential to your organization, and any important utilities or third party applications.

- Review, using ID filtering, the AppLocker event log for event IDs 8003 (blocked EXEs) and 8006 (blocked scripts). Note the path and filename of each exception.


Event Properties - Event 8003, AppLocker

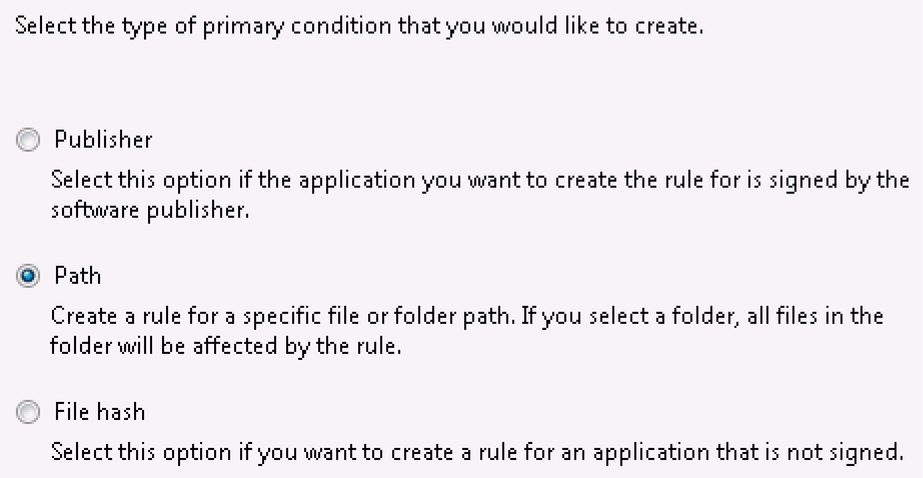
%appdata%\oddball-app1.exe was allowed to run but would have been prevented from running if the AppLocker policy were enforced.

Log Name: Microsoft-Windows-AppLocker/EXE and DLL
Source: AppLocker
Logged: 8/10/2014 6:52:45 PM
Event ID: 8003
Task Category: None
Level: Warning
Keywords:

Phase 4: Reconfigure AppLocker GPO to Add Rules for Exceptions

Perform the following steps on a test PC:

- Using the GPMC, add new rules for any exceptions noted above (based on event IDs 8003 and 8006 from test PC).


Select the type of primary condition that you would like to create.

○ Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

● Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

○ File hash
Select this option if you want to create a rule for an application that is not signed.

- Run gpupdate on the PC.

- Re-run each and every line of business application and any important utilities or third party applications.

- Repeat the above steps as needed until no new event IDs 8003 and 8006 are appearing in the AppLocker event logs.

Phase 5: Extend the Testing to a PC in Each Department within Your Enterprise

- Using the GPMC, link the AppLocker GPO to the appropriate OU (this must be an OU containing the computer accounts of all the test PCs).

Perform the following steps on each test PC selected (these steps can be automated):

- Run gpupdate on the PC.

- Using the Control Panel services applet, set the Application Identity service to start automatically, then start the service.

- Run each and every line of business application and any important utilities or third party applications installed on each test PC.

- Review, using ID filtering, the AppLocker event log for event IDs 8003 (blocked EXEs) and 8006 (blocked scripts). Note the path and filename of each exception and incorporate any new exceptions into the AppLocker GPO ruleset, run gpupdate again.

- Repeat until no new event IDs 8003 and 8006 are appearing in the AppLocker event logs of any test PCs.

Phase 6: Extend the Testing to All PCs in the Enterprise

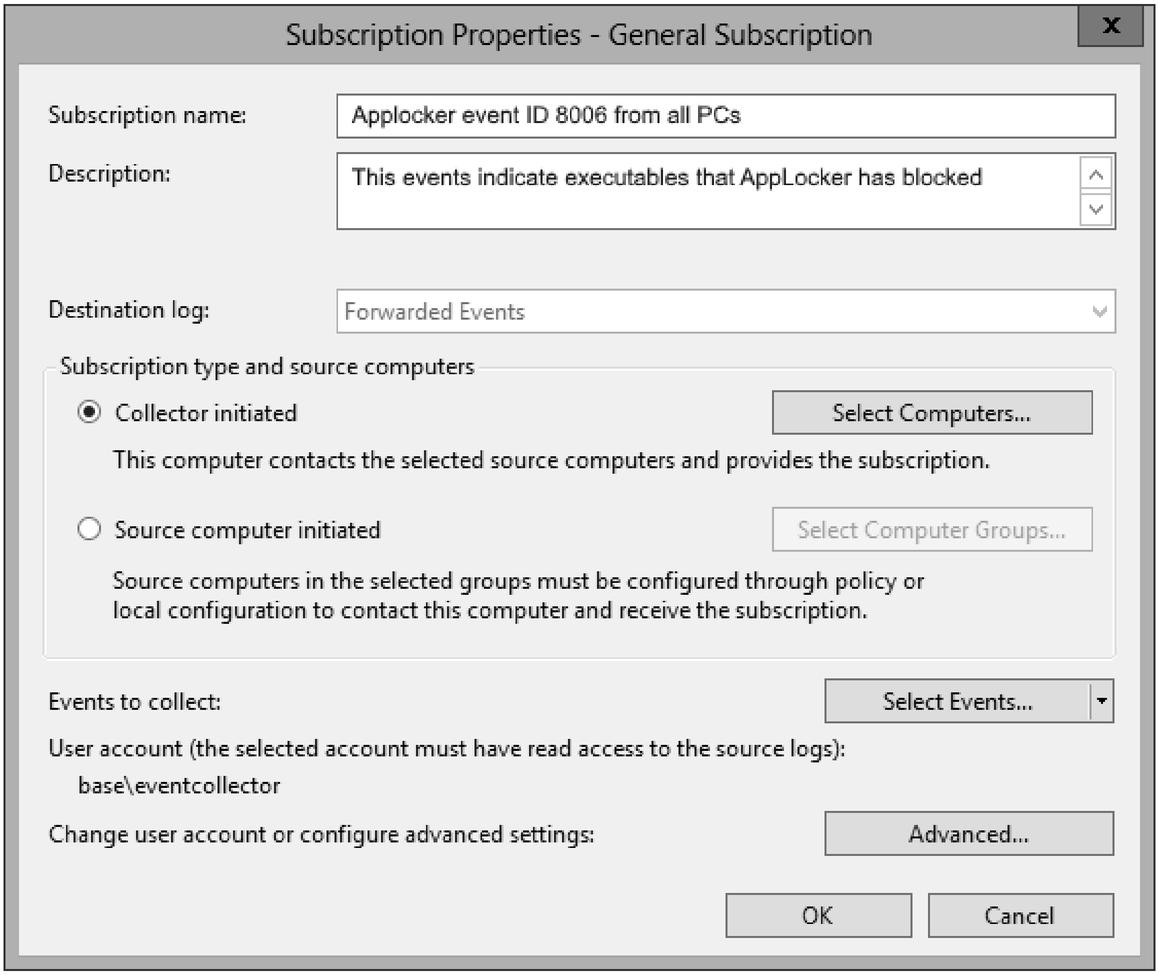
- Using the GPMC, link the AppLocker GPO to the appropriate OU (this must be an OU containing all the computer accounts of PCs that AppLocker rules should apply to).

Perform the following steps on each PC. Note that automation can be used to avoid manually having to implement these steps on each PC:

- Run gpupdate on the PC.

- Using the Control Panel services applet, set the Application Identity service to start automatically, then start the service.

- Optional: Configure event forwarding on each PC so that all AppLocker 8003 and 8006 events are forwarded automatically to a collection server. That way, any new exceptions can be identified easily from one central event log. Then, as exceptions arise, edit the AppLocker GPO to incorporate rules for the new exceptions. This can be used on an ongoing basis to more easily identify applications that need to be added to the AppLocker GPO ruleset.



Subscription Properties - General Subscription

Subscription name: Applocker event ID 8006 from all PCs

Description: This events indicate executables that AppLocker has blocked

Destination log: Forwarded Events

Subscription type and source computers

● Collector initiated

This computer contacts the selected source computers and provides the subscription.

○ Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

User account (the selected account must have read access to the source logs):

base\eventcollector

Change user account or configure advanced settings:

Continue with phase 6 until you are confident that all line of business applications have been incorporated into the AppLocker GPO ruleset. This will likely take a week or more, as not all applications are used on a daily basis. You'll want to observe the results until you feel fairly confident that your organization's users will be able to use the programs essential to their business roles.

If a user does experience a problem, you can always switch back to audit only mode, so they can resume work, until you have time to approve the application they need.

Phase 7: Enable AppLocker Enforcement Mode

Perform one last review of the AppLocker rules, then enable enforcement mode via the GPMC. At this point, any executables, scripts, or MSI installers for which there is no matching AppLocker rule will be blocked. Any blocked applications will appear in the AppLocker event log with IDs 8004 (EXEs) or 8007 (MSI installers or scripts).

Ongoing Management

Once AppLocker is enabled and enforcing its application execution ruleset, you may need to periodically review the AppLocker ruleset, particularly when installing new applications. For most applications that install to the default Program Files folder (C:\Program Files (x86)\ or to C:\Program Files\), the existing rules should not prevent such applications from running properly. However, for non-standard applications (for example, ones that install to the root of the system drive), you will have to create a new path-based AppLocker rule accordingly.

Also, it's important to periodically review the AppLocker event logs on PCs to identify ID 8006 events. Using either event forwarding or by attaching a task to these events (i.e. send out an email), you can automate this process.

NOTE: To temporarily disable AppLocker enforcement on a particular PC, you can change the "Application Identity" service's startup type to "Disabled," then reboot the PC. To re-enabled enforcement, change the startup type back to "Automatic," then start the service.

This information is directed at organizations using a Windows domain.

For apple computers, there is a feature called Limit Applications and it permits you to do just that.

Home office and family users of can use features available in the capable Microsoft Family Safety to restrict applications.

Chapter 3

Click-to-Play

Most people know the dangers of a user clicking on a link in an email message, opening an attachment, or visiting a website with malicious software. Such a seemingly harmless act by a single worker can compromise the security of an entire organization. The technology called "click-to-play" is designed to reduce the likelihood of an attack being successful.

Click-to-play compliments application whitelisting. Use both. While application whitelisting is useful, it only evaluates programs when the program tries to execute. Application whitelisting won't monitor behavior inside an application once the application is running. For example, when your IT department has application whitelisting enabled, they can specify which browsers are approved to run on users' computers. But when a user clicks on a link in an approved web browser, and the link exploits a vulnerability in the browser or a browser plugin, then the exploit won't be stopped by application whitelisting.

The Adobe Flash plugin and the Java browser plugin are infamous for security vulnerabilities. In fact, there have been over 600 security vulnerabilities for Adobe Flash since 2010 (source: https://www.cvedetails.com/product/6761/Adobe-Flash-Player.html?vendor_id=53).

For the Java runtime (JRE), there have been over 400 security vulnerabilities since 2010 (source: https://www.cvedetails.com/product/19117/Oracle-JRE.html?vendor_id=93).

Clearly, these two plugins represent a significant risk to your enterprise, and the safest thing is to simply disable them altogether. However, that's not always practical so IT departments need a way to minimize the risk.

One method of protecting your enterprise from plugin exploits is to enable click-to-play.

Click-to-play is a feature that's integrated into most modern web browsers. Simply put, it blocks content that a plugin would normally render and replaces it with a placeholder image. In other words, rather than scripts and flash content launching automatically when a user visits a website, there is an icon showing the user that there is content available to execute. To permit the content to execute, the user just clicks on the placeholder image or an icon in the address bar.

For home offices and Apple computers, the click-to-play functionality can be configured for each browser. For more information, please skip down to the section below entitled, "How to Enable Click-To-Play for Mozilla Firefox – Adobe Flash, Java, and Other Plugins."

The focus of the following information is to provide details on how to centrally manage click-to-play for Adobe Flash and Java JRE using Microsoft Active Directory Group Policy. This approach is beneficial, especially in larger organizations, since IT professionals do not need to visit each machine individually to enable click-to-play features.

The following instructions pertain to Internet Explorer, Google Chrome, and Mozilla Firefox only. But your IT department can follow these examples of tools and techniques in order to protect other browsers too. These instructions will also be helpful as a guide even if the configuration settings of browsers have changed after this writing.

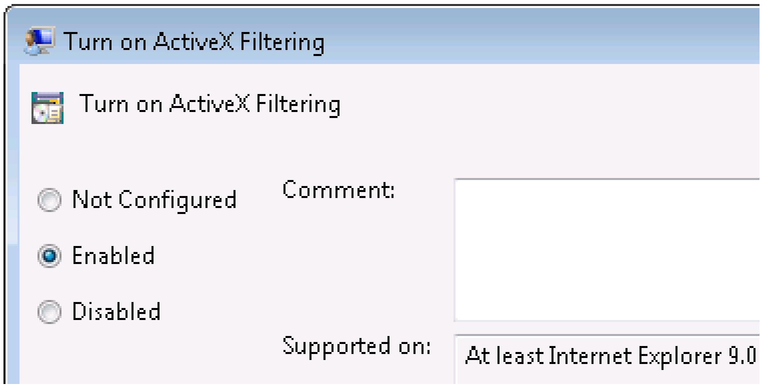
Note that click-to-play configurations are changing rapidly. The following instructions are current as of this revision of this document, and they are a helpful guide for your IT professionals. If they encounter a slight change in the options offered on their interface, they will still be able to accomplish what they need to do.

How to Enable Click-To-Play for Internet Explorer (IE) via GPO – Adobe Flash, Java, and Other Plugins

- From a Domain Controller, open the Group Policy Management Console (GPMC), drill down into the Group Policy Objects level, then create a new Group Policy Object (GPO) named "Click-To-Play."

- Edit the new "Click-To-Play" GPO, then drill down into User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer.

- Edit the setting "Turn on ActiveX Filtering", enable it, then click OK.



Turn on ActiveX Filtering

Turn on ActiveX Filtering

○ Not Configured

● Enabled

○ Disabled

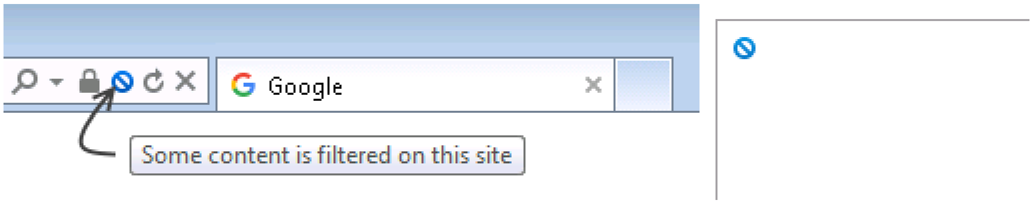
Comment:

Supported on: At least Internet Explorer 9.0

- Close the GPMC editor window for the “Click-To-Play” GPO.

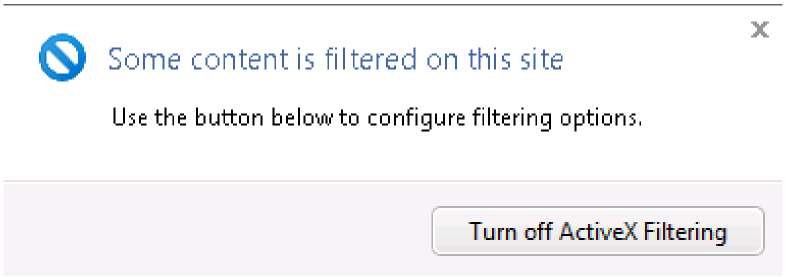
- From the main GPMC window, make sure that the GPO is linked to the OU containing the users for whom click-to-play should be enabled.

Once enabled, any site containing content requiring an ActiveX control (i.e. Adobe Flash, Java, etc.) will no longer render automatically and will be replaced by a placeholder. Also, a blue filter icon appears in the address bar:



Some content is filtered on this site

Clicking on the blue filter icon causes the following message to appear:



Some content is filtered on this site

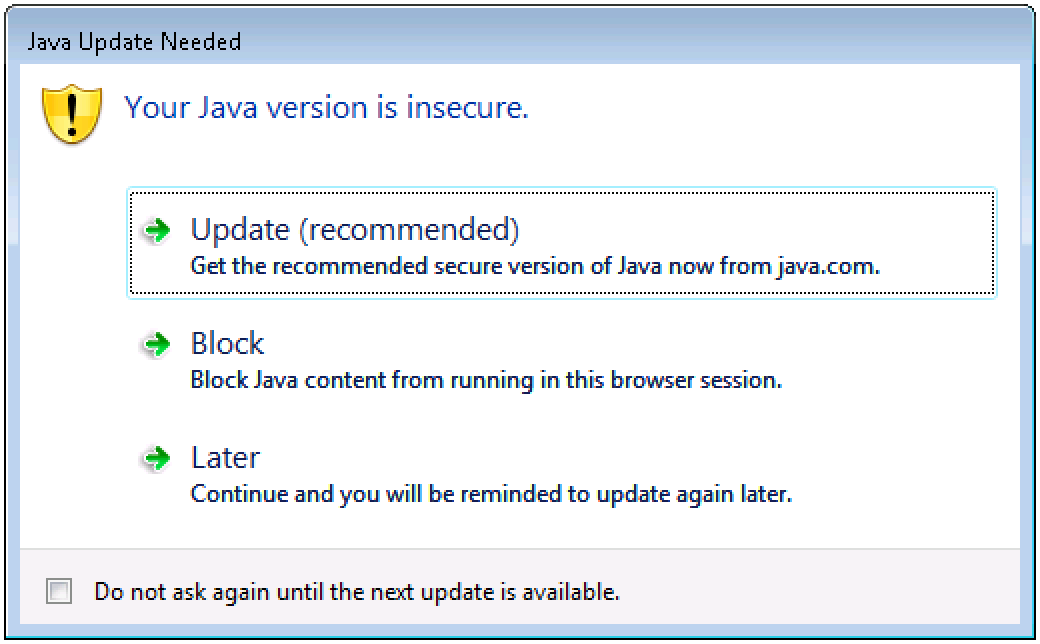
Use the button below to configure filtering options.

Finally, clicking on the “Turn off ActiveX Filtering” button will enable ActiveX controls for that site only.

Changes to Java Content Rendering in Internet Explorer (IE)

If Java is required for a line of business web app, then it needs to be enabled in the browser. If not, then you need to disable Java content for Internet Explorer and other browsers. This can be configured using the Java applet in the Control Panel (see the Security tab).

As of the August 2014 Cumulative update for Internet Explorer (versions 8 through 11), Internet Explorer now displays a warning for out-of-date ActiveX controls, including older Java ActiveX controls, by default. See Microsoft KB article 2991000 for details. Also, KB article 2996954 introduces a registry setting that will remove the Update button from the out-of-date ActiveX control blocking feature.



Java Update Needed

Your Java version is insecure.

Update (recommended)
Get the recommended secure version of Java now from java.com.

Block
Block Java content from running in this browser session.

Later
Continue and you will be reminded to update again later.

□ Do not ask again until the next update is available.

However, this doesn't prevent zero-day attacks as the message will not appear if the Java runtime is the most recent version. To mitigate against zero-day attacks, use ActiveX Filtering as outlined above.

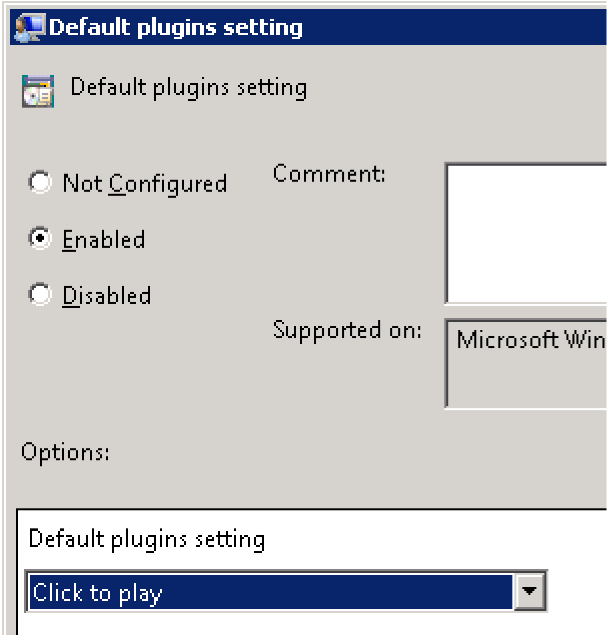
How to Enable Click-To-Play for Google Chrome via GPO – Adobe Flash, Java, and Other Plugins

- Download the Google Chrome administrative templates, then add them to the Group Policy Management Console (GPMC).

- From a Domain Controller, open the Group Policy Management Console (GPMC), drill down into the Group Policy Objects level, then create a new Group Policy Object (GPO) named "Click-To-Play."

- Edit the new "Click-To-Play" GPO, then drill down into User Configuration -> Policies -> Google -> Google Chrome -> Content Settings.

- Double-click on the "Default plugins setting" item, enable it, then set the value to "Click to play."



Default plugins setting

Default plugins setting

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: Microsoft Win

Options:

Default plugins setting

Click to play

- Click OK.

- Close the GPMC editor window for the "Click-To-Play" GPO.

- From the main GPMC window, make sure that the GPO is linked to the OU containing the users for whom click-to-play should be enabled.

NOTE: Although this guide doesn't detail it here, you may exclude specific domain names and URLs from "click-to-play" enforcement by configuring the "Allow plugins on these sites" setting, which you'll find in the Content Setting. Also, as an alternative to the built-in click-to-play feature, third party Chrome extensions are available for controlling the rendering of Flash content. Group policy can be used to automate the delivery of these third-party extensions, if desired.

How to Manually Enable Click-To-Play for Mozilla Firefox – Adobe Flash, Java, and Other Plugins

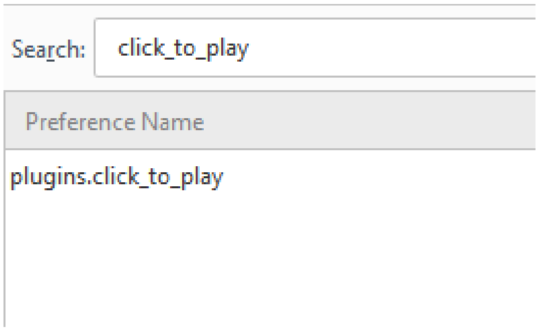
For home offices and Apple computers, the click-to-play functionality can be configured in browser settings for each browser. The following instructions will serve as a guide to help you locate and set the appropriate settings in your browser.

Newer versions of Mozilla Firefox enable click-to-play by default, so it's not necessary to centrally configure it via Active Directory GPO. More information on the default behavior of Firefox's click-to-play feature is available here: https://support.mozilla.org/en-US/kb/why-do-i-have-click-activate-plugins.

To check the status of Firefox click-to-play, follow these instructions:

- Open Firefox.

- In the address bar, type in about:config and press ENTER.
- In the search box, type in click_to_play.



Search: click_to_play

Preference Name

plugins.click_to_play

- In the value column, confirm that the value is set to true. If it's set to false, double-click on "plugins.click_to_play" entry to toggle the value to true.

NOTE: As an alternative to the built-in click-to-play feature, third party Firefox add-ons are available for controlling the rendering of Flash and Java content. One example is the QuickJava add-on: https://addons.mozilla.org/en-US/firefox/addon/quickjava/. Third-party add-ons for Firefox can be centrally deployed by copying the XPI file (i.e. via login script) to the extensions folder within the Firefox installation path on the target PCs. The XPI filename must match the unique ID of the add-on (i.e. for QuickJava, the filename would be {E6C1199F-E687-42da-8C24-E7770CC3AE66}.xpi).

For home offices and Apple computers, see the section above with the heading that starts with the words, "How to manually enable click-to-play..."

Chapter 4

Patches

Patches are one of the most difficult components of IT security. They are extremely challenging but, right behind application whitelisting, they offer the second most important protection from cyber-attacks.

Executives must grasp the concepts in this chapter in order to ensure this important security control is used effectively.

Applying critical security patches is so important for security, and so difficult and time consuming to do, that some organizations are employing IT professionals whose sole responsibility is to apply patches. Larger organizations need patch management teams.

1. Some IT professionals do not make patches a priority. This is the most common situation.
    a. Sometimes they decide, unilaterally, that the likelihood of a patch causing harm is greater than the likelihood of getting hacked, and/or
    b. They are just overwhelmed with too many other projects and tasks.

2. Some IT professionals will be aggressive at applying patches because they believe that the patches are an essential component of cyber-security, as long as they:
    a. Adopt an effective patching process (please see below) that diminishes the likelihood of a patch causing harm, and
    b. IT departments receive from the organization's executives the necessary time and management tools to be able to apply the patches.

You want the latter scenario. If your IT professionals are stuck in the former, you need to nudge them out of that rut.

Provide IT departments with the time and resources needed to properly manage the patching process.

Whether or not to apply patches is the executives' decision, not the IT department's decision. After all, if there is a successful cyber-attack due to a missing patch, the executives are ultimately responsible and will suffer the consequences.

This is a risk decision. Perhaps the biggest problem is that some IT departments fail to empower their executives so that the executives have the ability to make an informed decision about how aggressive they want their IT department to be related to installing patches. Or the executives don't want to participate in the process.

If IT departments can educate their executives as to the importance of applying patches effectively, then:

- The executives will be more likely to provide funds, resources, and tools to facilitate the patching process.
- If applying a patch does ever cause a problem, the executives will be more understanding.

As long as IT departments follow an effective patching process, it is unlikely that there will ever be a patch problem.

A sample memo from executives to IT will address many of the important points (see Chapter 1). Here are the vital points from the memo earlier that pertain to this topic:

1. **How aggressive are we at applying critical security patches?**
   a. I understand about the benefits and risks of deploying patches.
   b. We need to discuss how aggressive we want to be now.

2. **Provide me with a list, not percentage, of missing critical security operating system patches**. (Going forward, please send me that list every Thursday.)

3. **Provide a summarized application inventory showing the application, version, and number of computers on which the application is installed, using the format below. Our list will be longer:**

Application	**Version**	**Computers**
Adobe Flash Player	10.1	39
Adobe Flash Player	21.0	182
Adobe Reader 9.3.4	9.3	50
Adobe Reader 9.4.0	9.4	170
Google Chrome	40.0	10
Google Chrome	66.19	51
Java 7 Update 67	7.0	35
Java 8 Update 91	8.0	2
Microsoft SQL Server	11.1	1
Mozilla Firefox	45.0	44

4. **When we meet, I'd like to discuss:**
   a. Uninstalling all non-essential applications.

   b. Upgrading to the most recent version of the applications or explain exceptions.

5. **Provide me with a list, not percentage, of missing critical security application patches**. (Going forward, please send me that list every Thursday.)
   a. To save time, focus first on security patches for Flash, Reader, and Java.
   b. Next focus on browsers including Safari, Firefox, Internet Explorer, Chrome, etc.

Note to executives: Keeping up with patches is a full-time job. There is no such thing as “being finished.”

If you want to, see below for additional information and recommendations about an effective patch strategy.

Patches are Essential – Just Be Careful

For cyber-security, and often for reliability and performance, applying free patches are one of the single most important things you can do to your network. Patches fix “problems” on your network hardware and software.

However, patches can be risky. There is always the chance that a patch may break the functionality of something that is already working properly.

A very common problem, even for companies who use Managed Service Providers, is that IT professionals do not want to apply patches because there is a chance that the patch could cause some application to malfunction.

IT professionals, be they in-house or outsourced, are often so reluctant to apply patches that they will fall back on the, “We are going wait until the patch is tested before we apply it” excuse. That may be a valid reason, but consider the associated risk, which can be an extreme risk.

Therefore, a responsible IT department makes sure the executives understand the risks and potential outcomes. Since executives will suffer the most if there is a successful hacker attack that could have been prevented by a patch, they are the ones who need to decide how much of a risk they are willing to take on (the application of a patch causing problems vs. not patching critical security holes).

The unfortunate reality is that it is easier for IT departments to postpone applying critical security patches because IT departments are understaffed, overwhelmed with other tasks, and they do not want to risk causing any problems on the network. After all, if an attacker ever breaks in through a security hole, then everyone can blame the application for having the hole. The fact that there was a patch available to seal the security hole—a patch that wasn’t applied—needn’t enter into the conversation as to why the organization was devastated by an attack. What the executives don't know won't hurt the IT department's reputation.

Of course, it is extremely unlikely that IT departments—the ones who are not aggressive applying critical security patches—intentionally put their organization at risk. To the contrary, they usually justify in their own minds that not applying patches is best for the company. So be prepared for push-back if you have an IT department that delays the application of critical security patches.

It is the executive team's fault if an attack is successful because of a missing patch. Do not blame anyone else.

When you think about it, the IT department is heavily incentivized to not apply patches. Only the most responsible IT departments, the ones to which you've provided the time and resources, keep patches current. That protects your systems, your organization, and your job against a myriad of potential attacks.

What Should You Patch?

Of course, new patches are available for many products on a regular basis.

The patches that may help you the most are <u>critical</u> security patches to:

- Applications:
    - Adobe Flash
    - Adobe Reader
    - Java
    - Microsoft Office
- Browsers:
    - Chrome
    - Firefox
    - Internet Explorer
    - Safari
    - Opera
    - Any other browsers you use
- Operating Systems:
    - Apple OSX
    - Microsoft Windows
    - Microsoft Server Operating Systems
    - All other operating systems you use
- Infrastructure Devices
    - Routers
    - Switches
    - Firewalls
    - All other components of your infrastructure

Remember, focus first on the critical security patches. If IT departments are too overwhelmed to deal with patches, it is easier for you to support them if they limit the patches to only critical security patches at first.

These patches are important because hackers will likely exploit them first. Hackers exploit these first because the patches are difficult to apply, and therefore less likely to be patched. That leaves a gaping hole for an attacker.

Of course, critical security patches to your web filtering tools, anti-malware, etc. need to be applied too.

How Aggressive Should You Be?

Being aggressive means applying patches sooner rather than later. It is imperative that patches be applied ASAP. But it is also imperative to not crash your production environment. Choosing aggressive patch management can help protect against attacks. And proper testing and deployment methodologies protect you against a patch wreaking havoc in your organization.

Manufacturers create patches to stop exploits once they are aware of the vulnerability. It may take the manufacturer weeks or months to release a patch, and the vulnerability could have existed weeks or months before it was discovered.

When attackers know about a vulnerability for which a patch has not been created, that vulnerability is called a zero-day exploit.

Once a patch is created, it does you no good until that patch is rolled out to the assets at your organization.

Rather than wait to deploy application patches, since waiting will potentially put your organization in a precarious and dangerous security position, consider testing the patches in a QA test environment that is isolated from your production environment.

A goal to shoot for might be for all patches to be tested and then applied within 48 hours after the patch is released. Some organizations may strive to reach the level where patches are current up until 30 days prior. It just has to be the executives that make the ultimate informed decision about how aggressively crucial security patches are applied.

Microsoft generally releases patches on the second Tuesday of every month. That makes it easier for IT professionals to set aside time to apply Microsoft patches in a timely manner. Because of an incident involving Microsoft and Google, Microsoft is now more likely than ever before to distribute patches at unpredictable times throughout the month. Furthermore, there is often no way to predict when patches for applications and infrastructure devices will be released. This is one of the many reasons that IT departments often have one worker whose sole job function is to apply critical security patches.

Recommended Patch Methodology – A How To

1. Meet with the Executives
    a. Be sure executives understand the real pros and cons of applying patches. Whomever is informing the executives needs to be unbiased and very objective during the explanations.
    b. Executives need to decide about how aggressive they want IT to be with applying patches.
    c. They can choose what patches to install. Most executives start with limiting the patch requirements to the critical patches related to security, as opposed to optional patches.
    d. The executives will be the ones ultimately responsible if there is a patch-related problem, or if a missing patch permits an attacker to breach the network.
    e. Therefore, the executives need to make the decision.
    f. Executives must consider the chance that a patch might cause an outage vs. the expensive damage (financially and to the reputation of the organization) that could occur if the patch is not applied and an attacker exploits the vulnerability.
    g. The steps below help make the patching process more effective and have less risk.
    h. The IT professionals' job is to information the executive about the real pros and cons of the patches.

2. Upgrade Operating Systems
    a. It is best to use the 64-bit versions of operating systems. They are usually more secure than the 32-bit versions.
    b. When keeping older versions of operating systems:
        i. There are instances when organizations elect to leave older versions of operating systems in place.
            1. Sometimes upgrading to the next OS version can create unstable systems and unexpected results, especially in relation to the other systems in your environment.
            2. Sometimes upgrading to the next OS version can result in needing to purchase updated applications that cost thousands of dollars when the existing version of the application works fine
        ii. If you elect to use an older version of an operating system, then be sure to use effective compensating controls.
        iii. Search Microsoft's site for the "Microsoft Windows Application Compatibility Infrastructure" also known as the Shim Infrastructure: http://technet.microsoft.com/en-us/library/dd837644(WS.10).aspx
    c. Microsoft offers tools to assist in upgrades. Search their site for the Microsoft Assessment and Planning Toolkit MAP that will help you plan the upgrade.

   d. Search their site too for the Microsoft Deployment Toolkit MDT, which will assist your IT professionals as they deploy the upgraded OS versions.

3. Patch your Operating Systems
   a. Operating systems are relatively easy to patch compared to patching applications.
   b. Remove all unnecessary features from the operating system. You won't need to patch features you don't use anyway.
   c. You may decide to initiate the patching process immediately for workstations and wait until the next Friday afternoon to patch the servers. That would provide a cushion before the next week in the unlikely event that the staged deployment and roll back plan failed to protect you as you patched your servers.
   d. For more information, download and refer to the Microsoft Security Update Guide. The second edition is available here: http://www.microsoft.com/security/msrc/whatwedo/securityguide.aspx

4. Keep an Inventory of Your Applications
   a. Create an inventory of all applications installed. Your IT department may already have a tool for this task. If they don't, NEWT Professional is one option and is available from Komodo Laboratories.
   b. Pay special attention to the versions of the applications listed above.
   c. You will be surprised at some of the applications you discover.
   d. Make sure users do not have the ability to install their applications.
      i. For example, do not allow users to be local administrators on their machines.
      ii. Reconfigure your group policy objects and user systems in such a way that users cannot install their own applications.
      iii. An IT professional can install applications when necessary.
   e. Remember to include applications used on servers and users' portable devices such as laptops.
   f. Many enumeration tools, such as endpoint protection tools, host based IDS/IPS, patching tools, etc., will provide you with a detailed inventory of all of your applications.
      i. A rudimentary tool is to open a command prompt and issue the command: wmic product list > yourfile.txt.
      ii. Then, you can import that txt file, using fixed width format, into a spreadsheet and see information about some of the installed applications.

5. Delete all Applications that are Not Essential for Business
   a. Some users may need an application.
   b. But for everyone who doesn't need it, remove that application from their devices.
   c. This is very important since applications that are not installed do not need to be patched.

6. Upgrade all Applications to the Latest Version
    a. Attackers are more successful against older versions of
        i. Operating Systems
        ii. Applications
        iii. Firmware
    b. It is important to use the most recent versions of your operating system and especially the applications listed above.
    c. Knowing that they have limited resources, it is easy to see why operating system vendors and application development companies sometimes stop focusing on patches to older versions of their applications in order to focus on supporting the new versions.
    d. If you are not going to apply a patch for any reason, you need to use compensating controls.
    e. Some specifics for Java:
        i. Be cautious when upgrading Java.
        ii. It is still important to have the most recent version of Java.
        iii. Some applications, including some web applications, will not function with the newest version of Java.
        iv. If that is the case, then upgrade to the highest level of Java that your applications will support.
        v. Even if some machines need an older version of Java, install the most recent Java on the rest of your computers.
        vi. Since Java is more difficult to patch, it frequently is not patched. Therefore, Java is one of the first applications that attackers will target. Keep Java as up to date and patched as possible.
        vii. If you do need to use an older version of Java on a machine, consider isolating that computer on a separate filtered subnet and use strict filtering rules.
    f. Some specifics for Internet Explorer:
        i. Websites are a major source of attacks.
        ii. More recent versions of Microsoft's browser Internet Explorer, and Edge, are significantly better, including security, than any other prior Microsoft browser.
        iii. Microsoft makes major security improvements with each release of Windows and each release of Windows Server.
        iv. Sometimes the most secure versions of Internet Explorer require the most recent operating systems.
        v. If you are going to use Internet Explorer, use the newest version that is supported on your operating systems.

7. Test the Patches
    a. Deploying patches can sometimes cause unexpected problems.
    b. Therefore, deploy patches into a test environment rather than your production environment.
    c. Desktop and server virtualization can help IT with the testing process by providing a method to host and operate server and workstation

configurations on a single host machine, or a small number of physical machines, for testing.

d. If you don't have a test environment, consider patching a few "test" computers such as those in the IT department and to users who consider themselves adept at helping you test machines.
e. For applications that are commonplace, there is a smaller chance of a patch causing a problem. However, applications that are not mainstream applications are more likely to experience a problem since fewer entities that are testing the OS patch with that particular application. So be sure to emphasize the testing of your applications that are relatively uncommon applications.

8. Backup all of Your Systems
   a. Hopefully you already have good backups anyway.
   b. Applying patches to servers can be even more concerning than applying patches to workstations since, if the patch causes a malfunction, many or even all of your users may be affected. So be sure to keep snapshot backups of your servers immediately prior to patching them.

9. Centrally Manage the Patching Process
   a. It is crucial to centrally manage and apply critical security patches.
   b. Central management provides your IT professionals a way to monitor and control the patching process.
   c. To apply patches to operating systems, use Microsoft WSUS, Microsoft SCCM, System Center Essentials, or some other tool to assist the IT department as they apply OS patches.
   d. For application patches, consider central management tools such as BigFix, Desktop Central by ManageEngine, GFI LanGuard, LabTech (often used by Managed Service Providers—as are some of these other tools), Dell KACE, Kaseya, Lumension, Ninite, Secunia, Shavlik, etc. There are many management tools. None of them are perfect, so always provide enough time in your IT department's schedule so that they can test the solutions before buying.
   e. Another option is to use Microsoft SCCM or System Center Essentials if you deploy the third party patches to applications.
   f. Another option is to consider subscribing to managed services from an IT firm to centrally manage and monitor patch status across your network. They are sometimes referred to as MSP (Managed Service Providers).
      i. If you do elect to use Managed Services, please discuss this document with them and discuss how aggressive you want them to be. It is very common for MSPs to be non-aggressive because they have even more incentives to be so.
      ii. Share with them the methodology within.

10. Use Staged Deployment
    a. Once the patches pass the testing process, apply the patches on a few machines first.

   b. Then, if those machines are fine, deploy they patches to 25% of your computers.
   c. If those are fine, then 50%.
   d. The idea of using the staged deployment is that, if the patch causes a problem that wasn't detected during the testing phase, at least only some of your machines will be affected.
   e. Finally, finish installing the patch to the remaining computers.

11. Have a Pre-Tested Rollback Plan in Place in Case You Need to Remove the Patch Quickly. Sample plans include, in order of preference:
    a. Using the built-in "remove patch" function with the patch.
    b. Reinstalling the application.
    c. Restoring from a backup.

12. Make a List of Hardware Devices and Their Versions Too
    a. Apply critical security patches.
    b. Sometimes the patches are called firmware updates.
    c. You may elect to install patches that increase reliability and add features.
    d. If supported, make a backup of the device's configuration before updating the firmware. That way, if the installation of the firmware causes your configuration settings to be lost, it is more likely that you will be able to restore your configuration.

The intent of this detailed information is to provide guidance and stress the importance of adopting a patch strategy. The strategy needs to be as aggressive as you are willing to adopt. The information above helps you protect your organization from patch-related problems.

Note to executives: Patches are an ongoing challenge that must be continuously addressed. There is no finish line; new patches are released frequently. Therefore, do not expect your IT team to bring all of your patches up-to-date immediately. It could take them as long as a year to catch up.

Some small to midsize organizations even leave all of their workstations set to automatically apply patches. Servers still needs to be managed, especially since sometimes patches require a reboot of a computer, and rebooting servers needs to be scheduled.

However, keep in mind that the automatic update feature for the operating system probably doesn't apply updates to your browsers, adobe reader, Adobe flash, and Java. It is imperative that you keep these applications patched as well. In fact, patching applications is perhaps even more important than applying operating system patches. And you need to patch both.

Apple offers an update process as well on each computer. The patches can be configured to be applied automatically.

For home offices, strongly consider enabling the automatic patching feature on your laptops and desktops. Since the automatic patching process is generally turned on by default, your computer may already be installing patches automatically. Keep your backups current in case a patch does cause a problem.

Chapter 5

Local Administrators

Some user accounts are configured to be local administrators of their own computers. This is a serious mistake.

Allowing users to have administrator status greatly reduces their workstation and your network security. One of the biggest problems is that the user can install applications on their own computers—applications that may be insecure.

Here's something attackers know that you also need to know: The more power a user has, the more power an attacker will have when the attacker takes over that user's account on your network. Attackers can cause a great deal more damage if your IT professionals are so busy that they do not modify settings that are misconfigured in a "standard installation" of Windows.

Therefore, ask your IT professionals: "Are any of our users configured to be a local administrator on their computer?"

A common problem is when one or more of an organization's applications require your IT department to configure your users as local administrators on their machines.

Do not fall prey to their requirement unless you understand that complying might be a critical mistake. This is a common scenario and information about how to resolve this issue is provided below. Especially useful is the section entitled "Tools that Can Identify Permissions Issues"

Just know that it will take your IT department time to work on this. Find ways to free up time in their already busy schedule. This is certainly worth the effort.

Note that there is a bonus section at the end of this chapter. It helps your IT Professionals protect against a hacker technique, called traversal, that facilitates an attacker gaining full access to your network very quickly.

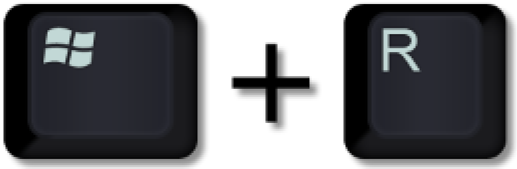
The following instructions are for your organization. You can also make similar changes on your home computers, and those guidelines are provided at the end of this chapter.

How to Review User Accounts to Identify Local Administrators

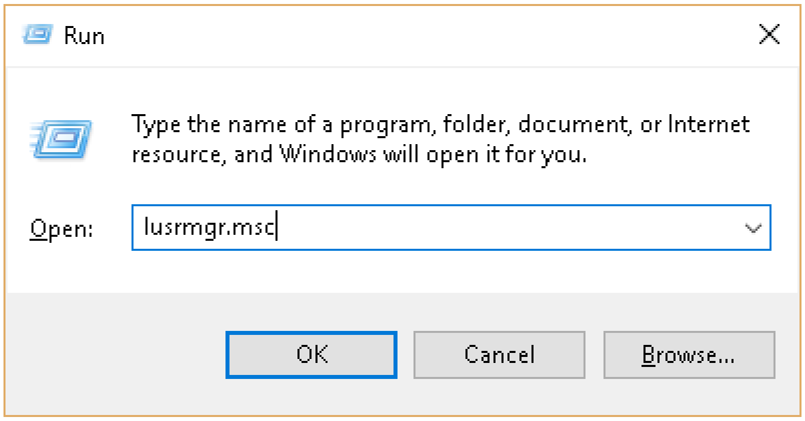
These instructions are for computers at your business. At the end of this chapter is information about how you can change your account on your home computer to be a local standard user in order to protect your home computer.

How to View the List of Local User Accounts

- If necessary, logoff any end user sessions on the PC (Start -> Logoff, or equivalent).
- Login to the user's PC as an administrator.
- Holding the Windows key (bottom left corner of your keyboard), press R.



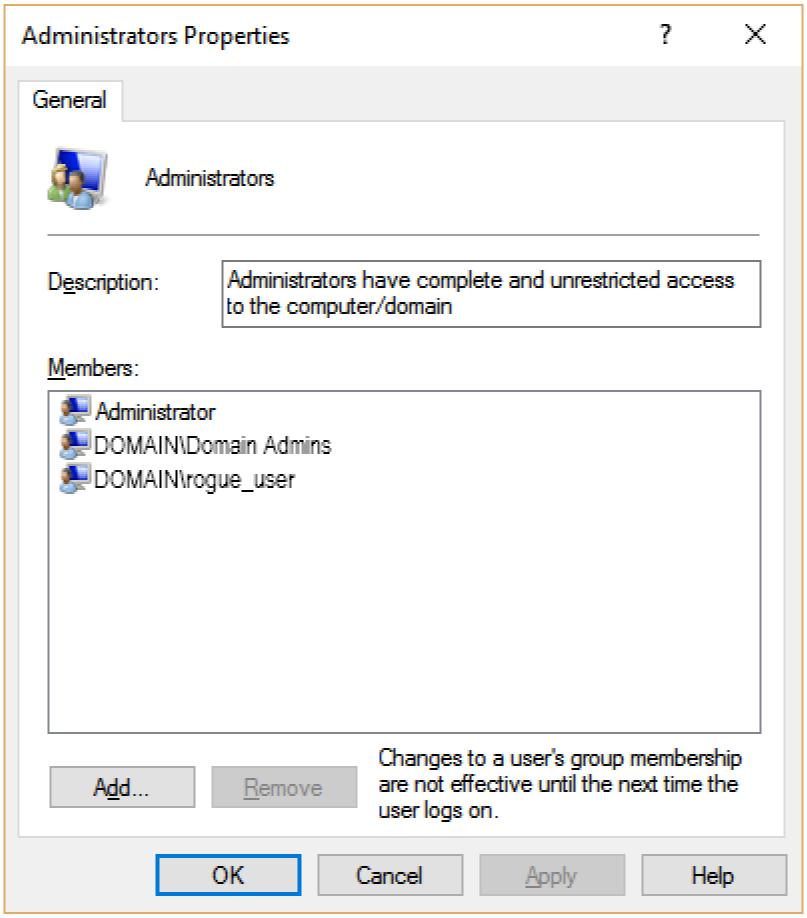
- In the box that appears, type in "lusrmgr.msc" and click OK.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: lusrmgr.msc

- From the Local Users and Groups window, select "Groups."
- From the list of Groups, double-click on the Administrators group.
- Review the list of local administrators.



Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator
DOMAIN\Domain Admins
DOMAIN\rogue_user

Changes to a user's group membership are not effective until the next time the user logs on.

- If a given user has been incorrectly assigned local administrator rights, remove that user from the Administrators group by selecting their account and clicking on the Remove button.

NOTE: Sometimes, entire user groups have been added as local administrators. Unless you have poorly written software that requires users to be local administrators, you should remove all unnecessary members of the local “Administrators” group. Typically, the only members of the Administrators group should be the default local “Administrator” account and the “Domain Admins” group. Be careful not to remove all accounts from the Administrators group. See the section below titled “Dealing with Applications that Require Administrator Rights.”

Advanced Topics for Larger Environments

Although the above procedure allows you to remove local administrator rights of a user on a single PC, it’s an impractical method if you need to manage local Administrators on dozens or hundreds of PCs.

For larger environments, you can gather a list of local Administrators members from all PCs by incorporating, into your login script(s), code that will gather that information and then dump it to a central log file.

HINT: One “simple” method is to incorporate this command into a login script:

```
wmic path win32_groupuser where
(groupcomponent=“win32_group.name=\”administrators\”,domain=\”%COMPUTERNAME%\”“)>>\\servername\share\local_admins.txt
```

NOTE: Although it is possible to remotely run wmic using the “Node” switch, it may not work if you have Windows firewall (or some other software firewall) running on the remote PC.

Once you’ve identified all “rogue” members of the local administrators group on your PCs, you can then create a script to remove those users/groups from the Administrators group of select PCs.

After all “rogue” members have been removed from the local Administrators group, you can make use of Group Policy to assign an Active Directory group (i.e. PCLocalAdmins) to the local Administrators group of all PCs automatically. You can then centrally manage the members of that one group (using the “Active Directory Users and Computers” console) to affect change on all PCs at once without having to touch end user PCs.

Dealing with Applications that Require Administrator Rights

So why do some applications require administrator rights? Well, in many cases, such applications need to make changes to system level objects, such as making changes to a registry key or value that only administrators have rights to.

However, there are also plenty of poorly coded applications that want administrator rights only because the developer didn’t take the time to code the application properly for a standard user.

For such applications, it may take only a small tweak of permissions somewhere in order to get it to run without issues as a standard user. Examples would be granting NTFS file permissions to a single system file, or perhaps additional permissions to a registry or two key. Although relaxing permissions may weaken security somewhat, doing so is still far safer than giving a user full administrative privileges.

The challenge is identifying what elevated privileges an application needs…

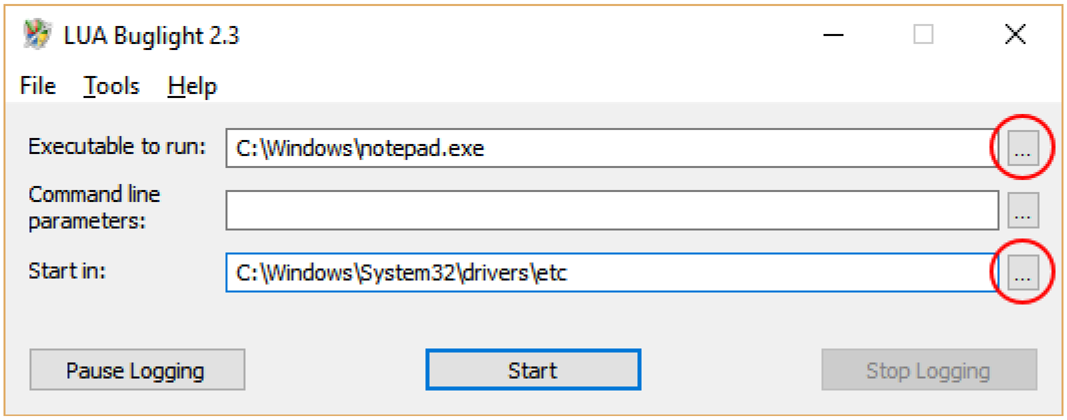
Tools that Can Identify Permissions Issues

There are a couple of free tools, developed by Microsoft, that can help you pinpoint why an application fails to run as a standard user.

One tool is called Process Monitor.

But a better tool for this purpose is the lesser known LUA BugLight, which is available from the Microsoft website as a ZIP archive. Within the ZIP archive is a single EXE file, so no installation is necessary.

- Launch LUA BugLight.
- Using the browse buttons, select the name of the executable you wish to troubleshoot, as well as the starting directory:

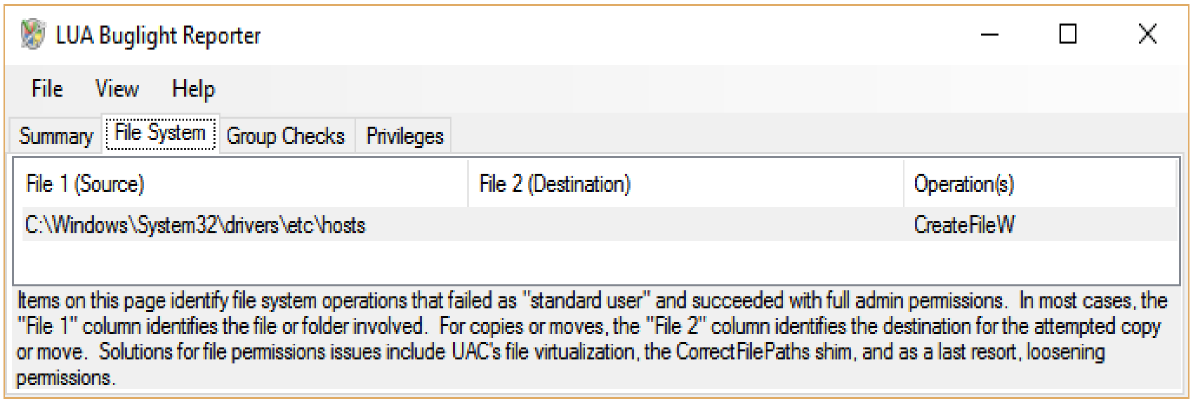


Executable to run: C:\Windows\notepad.exe

Command line parameters:

Start in: C:\Windows\System32\drivers\etc

- Click the Start button to launch the application.
- If prompted by UAC controls, click Yes.
- Run the application and perform as many actions as possible to thoroughly check it out.
- Close the application.
- On the LUA BugLight app window, click the “Stop Logging” button.
- The LUA BugLight Reporter window will automatically open, showing various tabs based on what it found.
- On each tab, suggestions for resolving the issues found are detailed at the bottom of the window:



File 1 (Source)	File 2 (Destination)	Operation(s)
C:\Windows\System32\drivers\etc\hosts		CreateFileW

Items on this page identify file system operations that failed as "standard user" and succeeded with full admin permissions. In most cases, the "File 1" column identifies the file or folder involved. For copies or moves, the "File 2" column identifies the destination for the attempted copy or move. Solutions for file permissions issues include UAC's file virtualization, the CorrectFilePaths shim, and as a last resort, loosening permissions.

Using the summary information provided by LUA BugLight, you may be able to identify file system or registry permissions that can be tweaked to allow the application to run without issues as a standard user.

Unfortunately, if a lack of privileges is identified on the Privileges tab, then the application may require administrator rights and only the developer can resolve that. In that case, until the developer makes the changes to their application, you can use other compensating controls. Once control is called sandboxing.

Sandboxing Applications

One workaround, using third-party software, is to run problem applications in a so-called sandbox environment. A sandbox is essentially an isolated, virtual environment in which an application is run. By using a sandbox environment, the application can be more safely run using administrator permissions.

Bonus Section: Managing Local Administrator Passwords

If more than one local administrative account has the same password on a machine, then when an attacker discovers the password on one machine, they can easily traverse the network and take control of other machines too.

How to Change Local Administrator Passwords Remotely

It’s pretty straight-forward to change a local administrator’s password on the PC itself. Just login as the local administrator, press CTRL-ALT-DELETE, then click on Change password. However, if you have dozens or hundreds of PCs to change then a better method is needed.

It is always better when IT departments do not need to go visit each individual machine on a network.

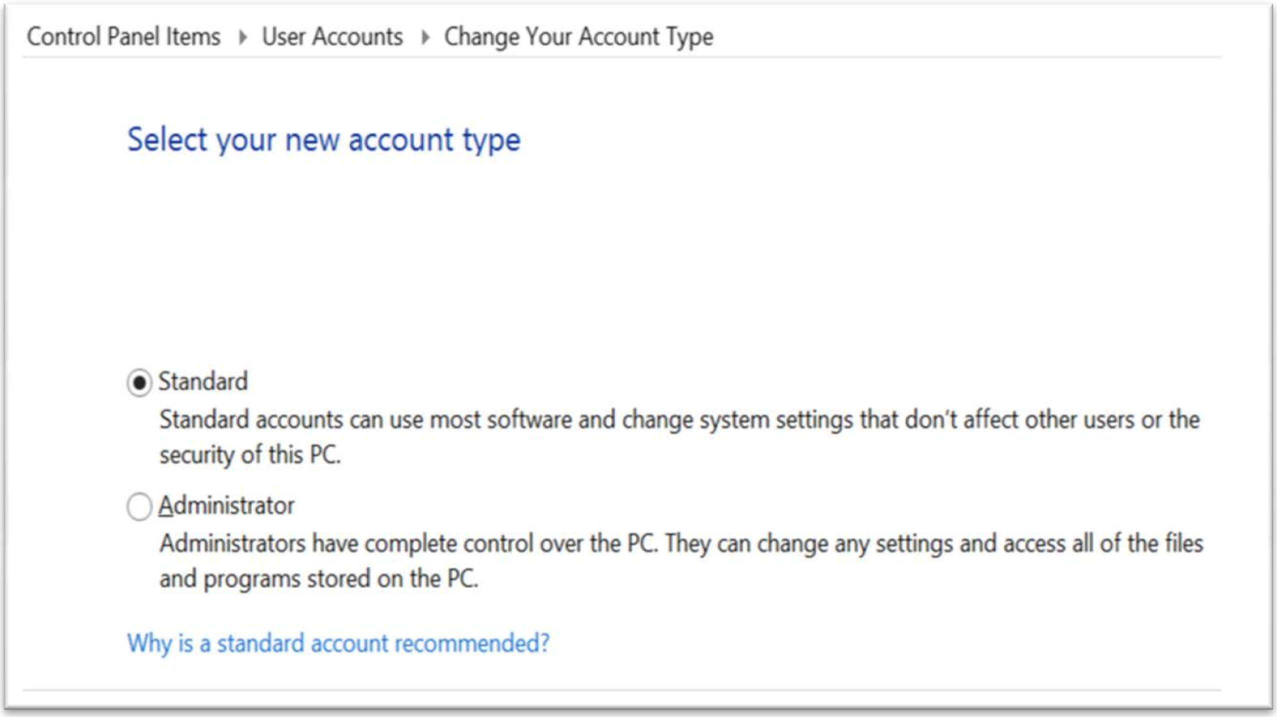
While there are many ways to change local administrator passwords remotely, the most secure and best choice is Microsoft LAPS.

Microsoft Local Administrator Password Solution, or LAPS, is a free utility that lets you more easily manage local administrator passwords on domain joined computers. Passwords generated by LAPS are stored in Active Directory (requires extension of the AD schema) and are accessible only to authorized users. Connections from LAPS to target PCs are authenticated using Kerberos and encrypted using AES.

Unfortunately, there’s a LAPS client component that must be installed on each PC, since LAPS is implemented as a Group Policy client side extension. However, the client software is packaged as an MSI file, so it can be silently installed via Group Policy, or via scripting. The client component requires .NET framework 4.0 (or newer) and PowerShell 2.0, which are both installed by default on Windows 7 or newer PCs.

An excellent blog post by Kyle Beckman of 4sysops.com provides detailed instructions on installing and configuring Microsoft LAPS, so please see his documentation.

For the Home Office: – How to Change Your Account to be a Standard Local User Account


Control Panel Items ▸ User Accounts ▸ Change Your Account Type

Select your new account type

● Standard

Standard accounts can use most software and change system settings that don't affect other users or the security of this PC.

○ Administrator

Administrators have complete control over the PC. They can change any settings and access all of the files and programs stored on the PC.

Why is a standard account recommended?

For home offices, the process is fairly straight-forward and will add a great deal of security protection to your computers.

First, go to control panel and create a new user account that will become the new administrator:

- Go into User Accounts in Control Panel.
- Create a new user. You can use whatever name you want to use, such as "superhero," and use a unique password that is different than your usual password.

Second, in the same part of control panel, set the new user that you just created to be an Administrator.

Third, demote your own account to Standard, and you will be more protected when logging on as your normal name.

- Log in as the new administrator you just created.
- Change your account to be a standard user.

Now, login as your account from now on. If you need to do anything administrative, your computer will prompt you for the administrator password.

Chapter 6

One-Tap Logon

This chapter covers one-tap login. If you already understand all about password security, including two-step login, then feel free to skip to the how-to section below. Otherwise, in case you are interested, the following paragraphs are a brief overview.

Once upon a time, while travelling around the nation doing IT Security Consulting, I found myself sitting next to a member of Oracle's Security Team. I asked, "What is the one single best bit of security advice Oracle could give their customers?" The response was immediate: "Change your default passwords."

In other words, users need to change their passwords to something other than the standard password that manufacturers set when a user buys their product or service. Of course, since that default password is publicly known, anyone can break in if the user never changes the password to something unique to their organization. Even today, I frequently encounter SQL database servers, servers holding vast amounts of sensitive information, which are still configured with the default password.

Simply stated, passwords are not helpful if everyone knows the password.

A few weeks later, I met with a CEO who had lost half-a-million dollars (so far) because his IT professional had set a password in their main application to the exact name of his company. Of course, the CEO had no idea that the password was so predictable.

But what if your passwords are indeed very secure? Don't stop there. The thing is, most people think "passwords" are what keep the bad guys out of your computers, but the passwords aren't enough.

You are probably aware that a specific group of hackers has collected more than a billion username and password combinations … so far.

It is easy to become numb about the news of stolen passwords. In the biggest discovery, so far, more than 420,000 websites have been hacked—and they are just finding out about it now. What if yours are one of the 1.2 billion username and password combinations?

Changing passwords frequently helps, but it is an inconvenience. Besides, tools called key-loggers allow attackers to capture your password as you type it in. There are software key-logger programs, considered malware or bad guy software, and even physical key-logger devices that can be inserted between a computer keyboard's cable and the computer itself.

The Problem with Traditional Passwords

Traditional passwords just aren't enough anymore. People have been relying on passwords for decades, trusting them as a key strategy to protect sensitive information. Passwords are no longer adequate. Here are just a few examples why:

- People reuse the same passwords for more than one website or service. Imagine what happens when someone uses the same password for more than one, perhaps 10 or more, websites and corporate accounts. If only one of those is hacked, then all of the other accounts are compromised now too.
- Hackers can crack even strong passwords if web service providers don't limit the number of password guessing attempts before automatically locking out accounts.
- Web services frequently use email addresses as usernames, making it easier for hacker's to crack usernames and passwords.
- People choose password reset challenge questions that are easily guessed or harvested from social media accounts (i.e. pet names, best friends, etc.) and phishing attacks.
- People save passwords on mobile devices and web browsers to avoid having to type in complex passwords over and over again. If the device gets hacked, then all those passwords get hacked too.
- Passwords are relatively easy to crack, unless they are complex or at least 15 characters long. However, remembering complex passwords is challenging for most people, which leads to password reuse, writing passwords down, or coercing IT staff to bend the rules.
- Key-logging programs can capture everything typed into a computer, making it easy for hackers to harvest passwords from that stream of information.

Clearly, human nature is the real problem with passwords. Organizations like yours need a solution that relaxes password complexity rules, requires less frequent password changes, yet offers better overall security.

Password Managers

Password managers can help you, as they remember your passwords for you so you can have a different password at every site. Therefore, you only need to remember one password, the password to your password manager. Choices abound including LastPass, DashLane, Roboform and many others. There are "enterprise" versions to use in your company, and they are inexpensive.

Yes, there is always a risk that an attacker might breach the password manager and gain access to all of your passwords.

Since you can never feel positive that password managers will keep your passwords secure, you'll want to adopt a strategy to deal with this.

Separate your passwords into two groups:

1. Passwords You Need to Keep Really Secure. Write these down and enter them manually. Example: Bank passwords.
2. Passwords that Protect what You Feel are Lower Security Resources. Example: Airline website logins.

If you are going to use a password manager program to remember your passwords, only trust it with the second group of passwords. Remember your most important password in your mind.

A side benefit of using a password manger is that, for passwords that are stored in the password manager, a user won't be typing keystrokes to enter the password, so a key-logger program won't be able to capture that password.

Even still, there are many problems with passwords and managing them has become very complicated. But there is a solution that can help protect your logins. You can't just use a password; you must use something else too.

Two-Step Login

Perhaps the best solution to the problems that plague password security is called "two step login." Historically, as your IT department will know, two-step login has been called "multi-factor" and "two-factor" authentication, aka 2FA. Two-step login systems add a second step to the login process. In most cases, the first step to login is for you to enter a username and password, and the second step is connected to something you physically have.

Here is an example of this solution: You enter a username and password into a website, and then your mobile phone buzzes and tells you to enter the code, such as 777888, to complete the login process.

Now an attacker would need to steal your mobile phone too before they could log on with your username and password. Obviously, if the attacker is in another country, then it is more difficult for them to steal your phone.

Other examples of "second steps" include:

- The "credit card verification value" (CVV) that's printed on the back of your credit card, which you sometimes must provide to make online purchases.
- A retinal or thumbprint scanner, which are examples of biometric second steps.

So if you are using two-step login, you may not even care if someone else knows your password.

Many online services, such as DropBox, PayPal, Google Apps, and many other sites already support two-step login. You just have to enable that feature.

See https://www.google.com/landing/2step/ to set up your Google account's two-step verification.

There is a useful website that documents which websites support two step logon. See it at TwoFactorAuth.org. As an executive, to protect your home computers, use this site to identify services that you use, and enable two-step login immediately. Your IT debarment can take care of the process for your office.

Why are Two-Step Login Solutions More Secure than Passwords Alone?

Since most attacks are Internet based, requiring a second step, which is in the physical possession of the legitimate user, makes it much harder for an account to be compromised. Take for example an account protected with a biometric second step, such as a thumbprint. Obviously, without the correct thumb to scan, a hacker will have a tough time remotely compromising that account.

Also, when two-step login solutions are implemented, password complexity and expiration rules are typically relaxed somewhat to make it less likely that users will reuse passwords, write them down, etc.

In the event that a user's username and password are hacked, the attacker would still need to be able to complete the second step. If that second step involves something the real user has in his/her possession, such as a mobile phone, then the hacker won't be successful unless they already have local or remote access to the phone too. Furthermore, when you receive the alert asking for your second step, even though you were not attempting to login anywhere, you will realize that someone else has discovered your username and password, so you will go reset your password as soon as possible. Most two-step login solutions will also alert IT staff of the failed login attempt.

However, it can be inconvenient for a user to need to look at their phone, view the text message, read the code, and then type the code into the login screen. This can be especially frustrating if the user is using phone for a voice conversation at the same time. So that brings us to the point of this entire chapter, "one-tap" login. You will not be able to change all of your services to support one-tap login, but you can change some of them, and especially your Windows login process. The login process to Windows needs to be as secure as possible, yet still be convenient to use.

"One-Tap" Login

There are a number of two-step login solutions in the marketplace that leverage a device that almost all of us carry with us at all times: a mobile phone. These solutions typically involve a user entering a username and password, and then they receive a text messaging. A more modern solution that uses a mobile phone is known as "one-tap" authorization. In this case, an app that is installed on the user's mobile phone pops up a window asking the user to tap a button on the screen in order to complete the login process.

The "one-tap" mobile-centric two-step login process varies only slightly from the standard Windows login process:

- The user sits down in front of the Windows PC and presses the usual CTRL-ALT-DEL sequence on the keyboard – no change.
- The user types in his/her username and password (the first step) – no change.
- A push notification is automatically sent to the user's phone, notifying him/her of the login attempt and prompting for approval.
- If the request is expected, then the user will tap the "Approve" button and the Windows login process will continue. Otherwise, if the request is unexpected, the user will tap the "Deny" button. Taking no action is the equivalent of tapping "Deny." In either case, the Windows login process will be aborted.

For two-step login solutions that use a code that's sent by text messaging (i.e. PayPal, SMS Passcode), there's typically a box provided on the Windows PC where the user types in the PIN code. This discussion; however, focuses on the more user friendly "one-tap" solutions.

How to Deploy a "One-Tap" Solution

NOTE: The exact steps needed to deploy a "one-tap" mobile-centric two-step login solution vary among products. Although these instructions focus on Duo Security's "Duo Mobile" as an example, competing products have similar setup so the following discussion will still benefit the reader. The Foster Institute is not promoting or endorsing Duo Security, nor does it receive any kind of compensation from Duo Security for distributing these recommendations.

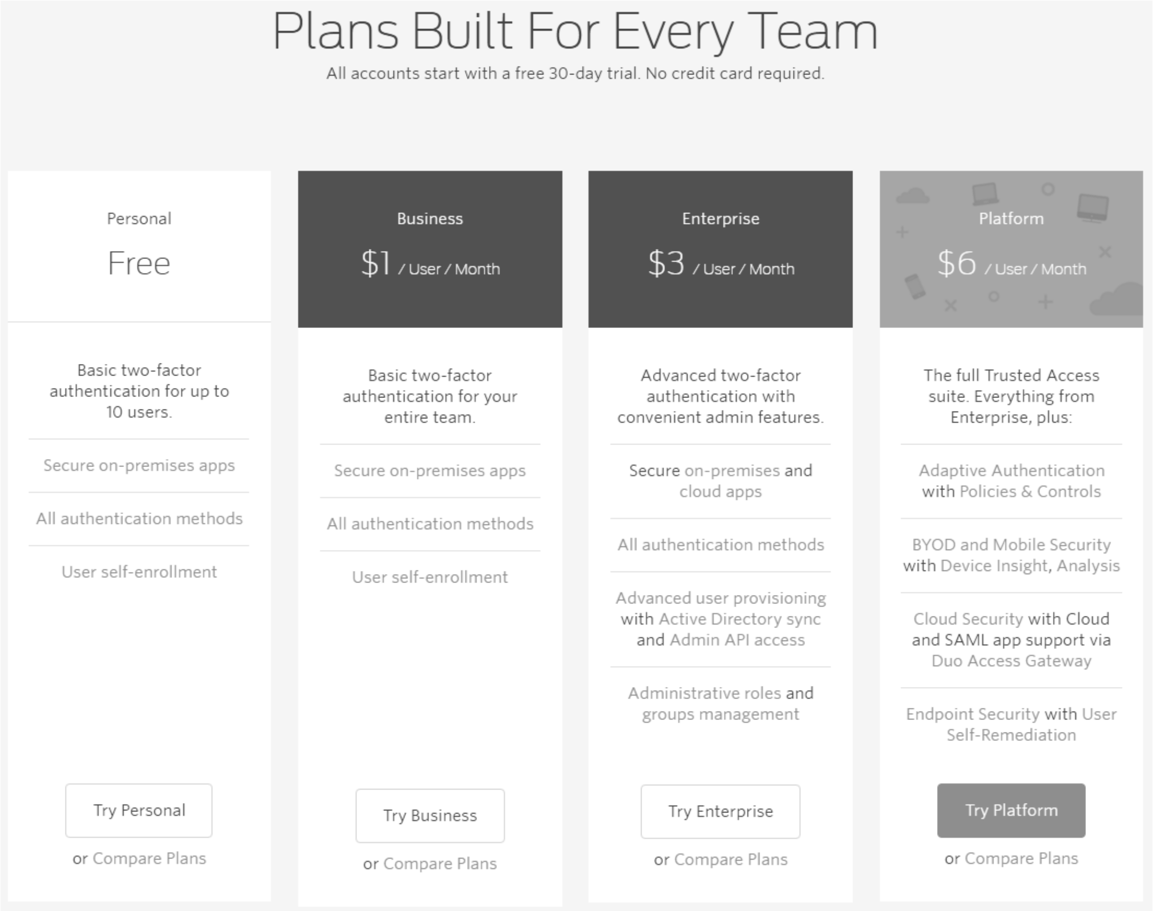
Purchasing the Product or Service

The first step requires purchasing licenses or subscriptions from the one-tap login vendor. The sites may use the technical terms and acronyms such as "multi-factor authentication," aka MFA, or "two factor authentication," aka 2FA.

Use a subscription based, Software as a Service (SaaS) providers as they typically:

- Allow you to add and remove users at any time.
- Let you pay for your usage of the software on a per user, per month basis.
- Have more frequent updates to their software.
- Provide all hosting infrastructure, so you only need to install agent software on PCs and phones.

In our example, this step involves filling out a short form on the vendor's website to create an account.



Plans Built For Every Team

All accounts start with a free 30-day trial. No credit card required.

Personal	Business	Enterprise	Platform
Free	$1 / User / Month	$3 / User / Month	$6 / User / Month
Basic two-factor authentication for up to 10 users.	Basic two-factor authentication for your entire team.	Advanced two-factor authentication with convenient admin features.	The full Trusted Access suite. Everything from Enterprise, plus:
Secure on-premises apps	Secure on-premises apps	Secure on-premises and cloud apps	Adaptive Authentication with Policies & Controls
All authentication methods	All authentication methods	All authentication methods	BYOD and Mobile Security with Device Insight, Analysis
User self-enrollment	User self-enrollment	Advanced user provisioning with Active Directory sync and Admin API access	Cloud Security with Cloud and SAML app support via Duo Access Gateway
		Administrative roles and groups management	Endpoint Security with User Self-Remediation
Try Personal	Try Business	Try Enterprise	Try Platform
or Compare Plans	or Compare Plans	or Compare Plans	or Compare Plans

Configuring the Basics

This step typically involves visiting a web-based administrative console and providing the following basic information:

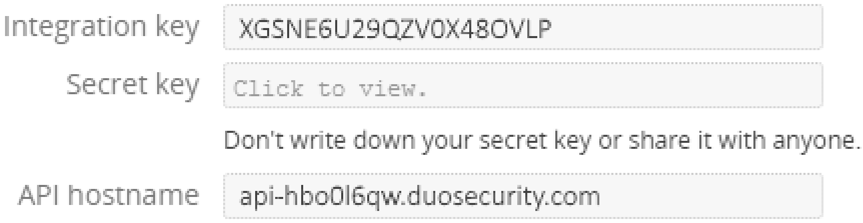
- General settings: Company name, region, time zone, authentication methods to enable, branding (i.e. company logo that will appear in authentication requests), etc.
- Billing information: Credit card info, subscription level, number of subscriptions (users), length of term, etc.
- Administrators: Defining who will have access to the administrative console.

Creating an Application Integration

Most of these one-tap login solutions integrate with a variety of web and on-premises authentication systems, with each authentication method requiring a specific type of integration. Since these guidelines are only discussing one-tap login as it applies to

Windows PC and server logins, below is an application specific integration for that one use case.

For Duo Security, that means creating a Microsoft RDP integration. The creation of that integration generates an integration key, secret key, and API hostname. When configuring the agent software on PCs in the enterprise, the technician will type in that information during installation so that the agent can connect to the correct integration and configure itself.



Integration key XGSNE6U29QZV0X48OVLP

Secret key Click to view.

Don't write down your secret key or share it with anyone.

API hostname api-hbo0l6qw.duosecurity.com

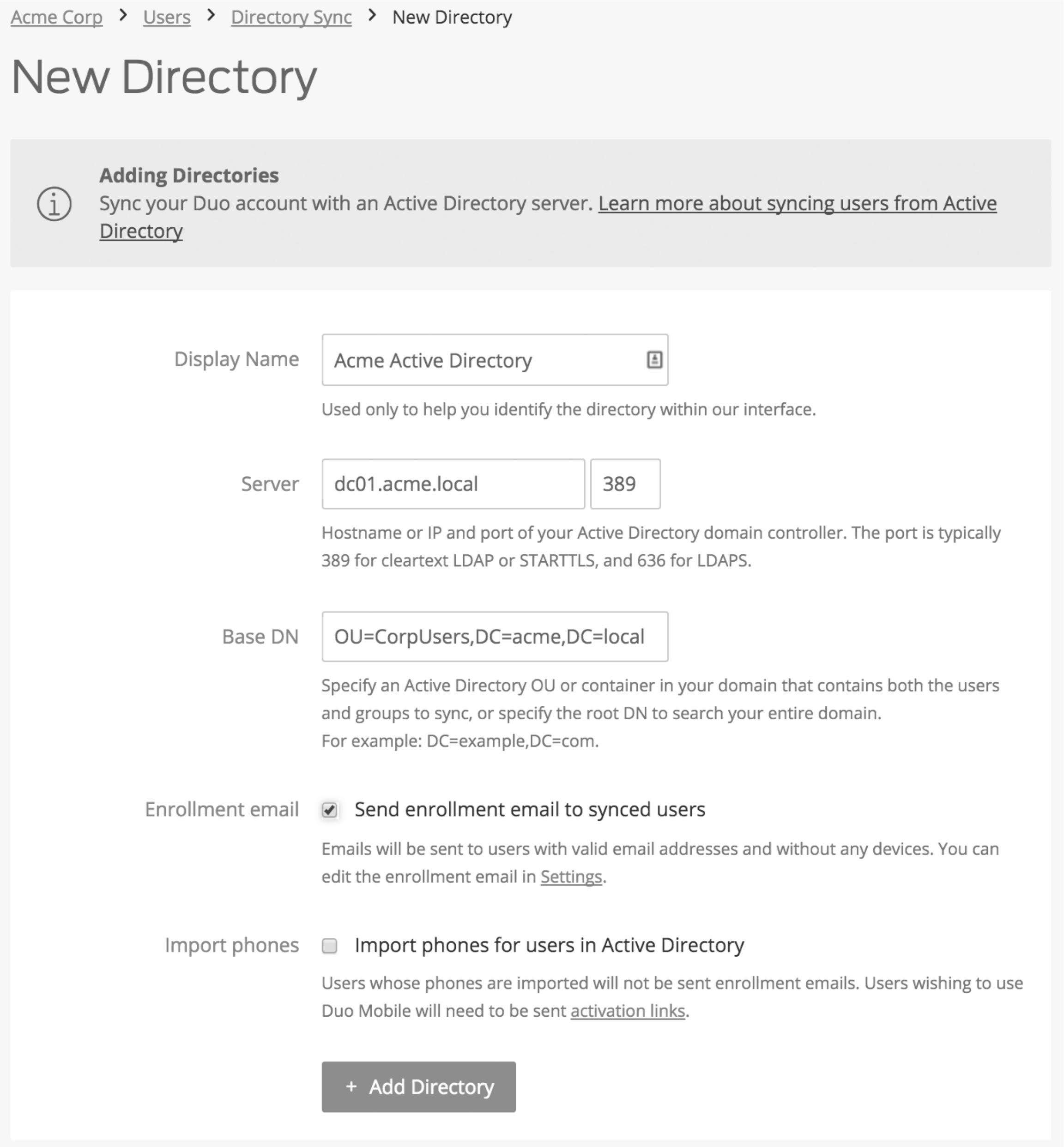
Creating User Accounts

This steps varies a bit among vendors, with some offering advanced synchronization with other authentication systems (i.e. on premises Active Directory, ADFS, RADIUS, SAML, Windows Azure AD, etc.), while others have bulk enrollment options or may even require you to manually create user accounts.

Duo Security provides many user creation options including: an AD sync agent (to sync your existing users in Active Directory), bulk enrollment (using an Excel spreadsheet), SAML (via Duo Access Gateway), Azure AD (via Duo Access Gateway), self-enrollment, and manual enrollment.

Since this guide only focuses on adding one-tap login to the Windows PC or Windows Server login process, this discusses how to the AD sync agent (for larger companies) and bulk/manual enrollment (SMBs) options.

For AD sync, you install a small agent on a Windows PC or Windows Server on your premises. During installation, you supply the application integration keys and API hostname and the rest of the configuration is done within the web based administrative console.



Acme Corp > Users > Directory Sync > New Directory

New Directory

Adding Directories
Sync your Duo account with an Active Directory server. Learn more about syncing users from Active Directory

Display Name: Acme Active Directory
Used only to help you identify the directory within our interface.

Server: dc01.acme.local 389
Hostname or IP and port of your Active Directory domain controller. The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

Base DN: OU=CorpUsers,DC=acme,DC=local
Specify an Active Directory OU or container in your domain that contains both the users and groups to sync, or specify the root DN to search your entire domain.
For example: DC=example,DC=com.

Enrollment email: ☑ Send enrollment email to synced users
Emails will be sent to users with valid email addresses and without any devices. You can edit the enrollment email in Settings.

Import phones: ☐ Import phones for users in Active Directory
Users whose phones are imported will not be sent enrollment emails. Users wishing to use Duo Mobile will need to be sent activation links.

From the administrative web console, the AD sync feature requires the IP address or hostname of an on-premises Windows Domain Controller (DC), the LDAP port of that DC, and the BaseDN.

For manual and bulk enrollment, users are created either directly in the web based admin console (manual) or by importing a CSV file (bulk) with each row of data representing a single user. The user account wizard requires a username (to match the Windows PC username), the person's full name, and an email address.

Adding Phones to User Accounts

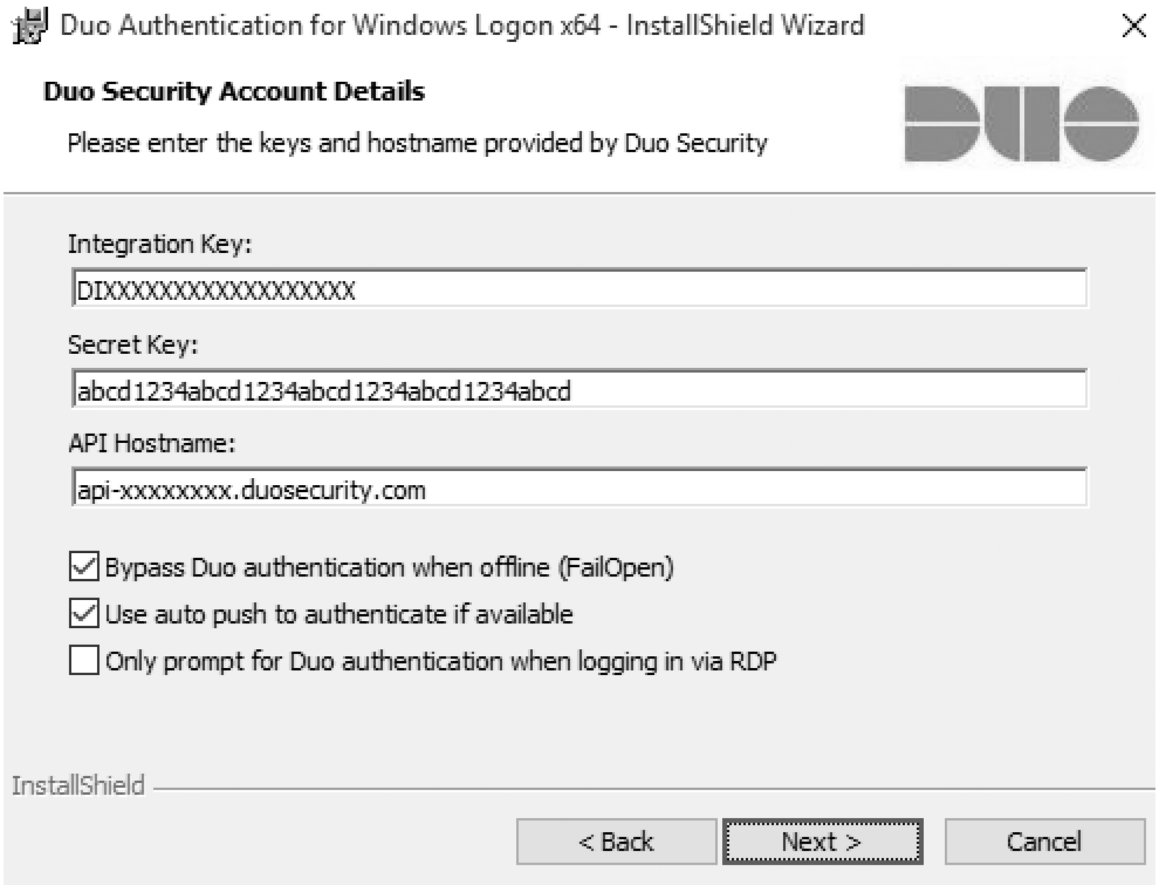
Phones are added to the administrative console either by manually typing in the phone number and sending an activation link to the user, or via AD sync.

Installing the Duo Mobile App on Phones

The Duo Mobile app needs to be installed on each registered phone. The process is the same as installing any app; visit the app store and install it. Once installed, an activation link can be sent by the administrator, which the user taps to automatically configure the Duo Mobile app.

Deploying the Duo Security Agent to Windows PCs and Servers

The Duo Security agent can be manually installed on each PC, installed from a command line, or centrally deployed. In each case, the RDP app integration keys and API hostname are needed so that the agent can configure itself.



Duo Authentication for Windows Logon x64 - InstallShield Wizard

Duo Security Account Details

Please enter the keys and hostname provided by Duo Security

Integration Key: DIXXXXXXXXXXXXXXXXXX

Secret Key: abcd1234abcd1234abcd1234abcd1234abcd

API Hostname: api-xxxxxxxx.duosecurity.com

☑ Bypass Duo authentication when offline (FailOpen)

☑ Use auto push to authenticate if available

□ Only prompt for Duo authentication when logging in via RDP

Proof of Concept

This phase typically consists of a limited deployment to a few PCs and phones. User training is typically minimal and intuitive, since the user's phone simply alerts them as needed. Typically, issues arise when mobile devices are not properly activated or push notifications have been disabled on the device.

Enterprise-Wide Deployment

This phase typically consists of an automated deployment of the Windows agent, getting users to install the app on their phones, and pushing out activation requests to users. As with the testing phase, typically issues arise when mobile devices are not properly activated or push notifications have been disabled on the mobile devices.

Ongoing Management

As with most IT systems, user adds/deletes/changes will occur. If you chose to deploy Active Directory synchronization, then you'll only need to add and activate phones when configuring new user accounts, since the accounts are created automatically. If you populate the phone field in Active Directory, phones can be added automatically when new user accounts are created. Adding phones varies among one-tap login solutions, so the details of the required steps are left to the reader to research.

Adding a new phone is generally a simple process, whereby you supply the phone number, then send out an activation link to the user via SMS text. The user will then need to install the Duo Mobile app (or equivalent) and then activate the device via the text message activation link.

Sometimes, it is necessary to reactivate a phone. For example, if the user retains the same phone number but purchases a new device, then reactivation of the phone is required. To reactivate a phone, you'll need to drill down in the web admin portal to the phone object, then click on the link provided to reactivate the device. Reactivating phones varies among one-tap login solutions, so the details of the required steps are left to the reader to research.

For home offices, even if you choose not to use some form of one-tap logon app, different web sites offer a plethora of options for two step logon. Some of the sites will want to text you a message when you logon, or use some other method to verify your identity.

To make your experience even easier, some sites will offer to remember your computer so that, as long as you use the same computer to log on, you won't be prompted for the second step.

Popular sites such as Drop Box, PayPal, LinkedIn, Google, offer two step logon options. You may have to dig into the settings to find the security options, but it is well worth the added effort you'll invest. This adds protection in case your password is ever compromised. The site twofactorauth.org has a list of sites that support two step logon too.

Chapter 7

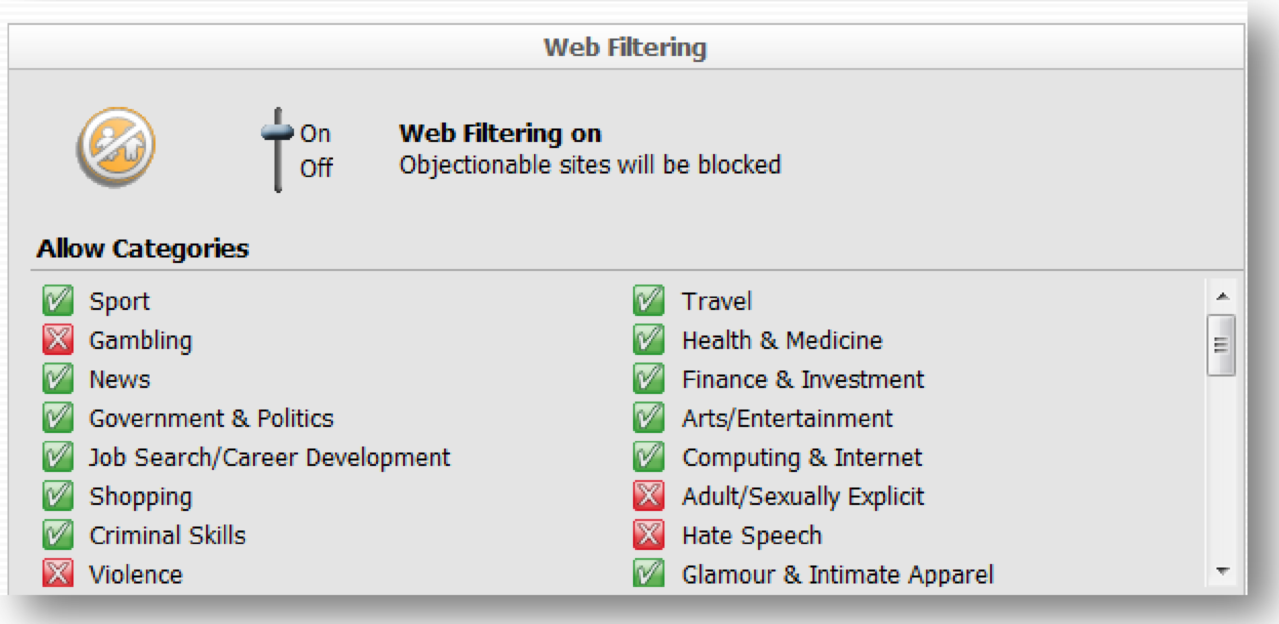
Web Content Filtering

Blocking potentially malicious websites will help protect your system when a user "clicks on a link" or visits a website that contains malicious software such as malvertising.

Using web content filtering protects an organization's network so much that permitting users to be online without web content filtering is reckless.

Tools exist that allow you to block or allow websites based on categories such as news, gambling, travel, shopping, etc. Some organizations choose to disable the ability for users to access websites that contain content that may not be essential for them to do their job.

An example web content filtering interface is:



Web Filtering

On
Off

Web Filtering on
Objectionable sites will be blocked

Allow Categories

- ☑ Sport
- ☒ Gambling
- ☑ News
- ☑ Government & Politics
- ☑ Job Search/Career Development
- ☑ Shopping
- ☑ Criminal Skills
- ☒ Violence
- ☑ Travel
- ☑ Health & Medicine
- ☑ Finance & Investment
- ☑ Arts/Entertainment
- ☑ Computing & Internet
- ☒ Adult/Sexually Explicit
- ☒ Hate Speech
- ☑ Glamour & Intimate Apparel

Sometimes a discussion about what sites to filter will lead to disagreements between people at an organization. Examples include access to social media sites from work computers, booking travel online, online music or video sites, shopping online, etc. In order to keep the decision process short, determine what categories you want to "block."

Additionally, just by enabling web content filtering, a common feature is to block sites that are known to contain malicious software. Web content filtering is one of the most effective ways to fight "drive-by-downloads."

Discuss with your IT team what categories you want them to block. You can make exceptions to permit specific sites if they are blocked by a category, but all of the detailed settings can become tedious. Some of you will be willing to go into such a granular configuration. If you are not, remember to at least block some of the categories. Every category or site you block adds to your level of security.

There are often categories named something like, "sites known to contain malware." Even if you block no other categories, those are good to block.

There is often a category that identifies "unknown status" sites. New web sites are posted every day. The sites in this category are sites that your filter doesn't know about yet. There is always a chance the sites may contain malware. Since most filters stay current, you may elect to block these as well.

Sometimes web content filters permit you to block based on the countries where the site is hosted.

There are many ways to filter web content. Some third party anti-virus software offers the ability to filter content. At the very least, the tools will usually offer the ability to block sites known to have malicious content.

Another option is to control filtering in physical firewalls. Many firewalls support web content filtering.

Expect to pay a yearly subscription for the filtering. Web content constantly changes, so keeping the filtering tool current is valuable.

There are even services and hardware that whose sole purpose is to provide web content filtering.

If your solution is inadequate, then upgrade the firewall or add a tool that will provide this functionality. The more you restrict, the higher your level of protection. Just be sure you can still be productive and access the sites you need to access.

Some tools will provide reports about what content is being accessed if you want to, and are permitted to, monitor the activity.

For home offices, all of the information above stays the same. This is helpful protection for all offices and even families. Some families buy firewalls that are designed for small offices to use in their home. They feel that the added protection for their family is worth the investment in the firewall.

Chapter 8

Bonus Information Specifically for SOHO

Image Backup

Note: This chapter is focused on home office users who want a solid backup strategy for individual computers. At organizations with servers, using image backups are essential, especially on the servers, and on a much grander scale. It is sometimes referred to with terms like “snapshots.”

First, don’t change or eliminate the backup you have now; just supplement it with image backup.

Think of an image backup as being like a picture of your computer, workstation, or server. It is an exact bit-by-bit copy—a clone.

Since an image backup is an exact duplicate of a hard drive, you can use it to quickly restore a machine to its exact state at the time of the backup. This includes the operating system, the registry, the program files, the data files, and the computer or network settings. And all this happens in one fell swoop. It’s like taking a Polaroid snapshot of the computer or server. Here’s how image backup can help.

The time it takes to restore from an image backup depends on how much data is stored on the computer.

If all you have is your data backed up, not the programs, and you crash, here is what you will need to do:

1. Re-install your operating system.
2. Apply all the patches.
3. Re-install Office.
4. Apply all the patches.
5. Re-install your other programs.
6. Patch those too.
7. Finally, you can restore your data from your backup method. If you use online backup, and have a great deal of data, it could take hours to restore.
8. But your shortcuts, recent files, task bar, and everything else you’ve personalized will be gone.

Or, if you have image backup, it is much easier:

1. Restore from your image backup.
2. Use your online backup service to restore only the files that changed since you last made an image backup.

If all you have is an online backup, or some other backup that only backs up your data, then recovering from a crash is often 48-hour ordeal. You won't be busy all of that time, but you will spend a lot of time watching the wheel that took the place of the hourglass while you wait for your computer.

Frequently, a restore from an image backup can be finished in less than half an hour. That is one of the reasons why image backup is so helpful: A 30 minute restore is so much faster than going through the long process listed above.

Windows users: Some popular tools for Windows include Symantec Ghost from www.symantec.com, True Image from www.acronis.com, and ShadowProtect from www.storagecraft.com. Of all the choices, Ghost is probably the easiest for a novice user.

Apple users: A great tool for Mac users is Carbon Copy Cloner.

If your computer crashes, or if you get attacked by a virus such as ransomware, and you need to get it going again quickly, you don't want to find out then that you will need another way to boot your computer before you can restore the image.

If you purchase and download an image backup program from the Internet, pay the small fee to have them ship you the CD. Or follow the instructions yourself to burn a bootable CD, DVD, or a USB drive. You'll need to prepare, in advance, to be able to boot the computer from CD, DVD, or a USB drive in case it is required during the restore process.

Some tools provide a way that you can boot directly from the backed-up image, but you need to know how to tell your computer to boot from a different location.

With many computers, you have to hold down a key on the keyboard during boot-up in order to tell the machine to boot from the CD. Sometimes it is as easy as holding down the C key.

To find out how to get your computer to boot from the CD/DVD or USB drive, Google the phrase: How to boot from CD [computer-model]. Replace the words "computer model" with the model of your computer.

Test it now. Don't find out that it won't work the hard way when you need to perform a recovery of your computer.

Perform in image backup frequently, alternating between two different backup drives. Why? Because if your computer should ever crash (and you have to admit that would be a huge headache), you can restore it very quickly, even if one of the drives fails too.

Having the ability to reset a computer back to the way it was before is very important, especially if you feel there is a chance that the computer may have experienced a cyber-security related attack.

Keep backing up your workstation computers the way you always have, and add image backup to that strategy. Do it today.

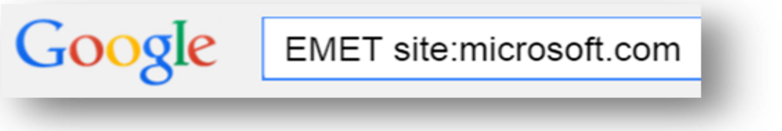
Home Offices are the focus of this chapter. The same functionality can be utilized in organizations as well. Image backup tools are useful, not only for backing up, but for deploying a standard configuration to new computers.

Chapter 9

The Microsoft Enhanced Mitigation Experience Toolkit (EMET)

The Microsoft Enhanced Mitigation Experience Toolkit (**EMET**) is a utility that helps prevent vulnerabilities in software from being successfully exploited.

- If you want to, **download and install Microsoft EMET**. It is a free tool designed to protect your computers from some, though not all, hacker techniques.
- Many people consider EMET one of their secret weapons to ward off cyber-crooks.
- EMET is not designed to remove infections, just to hinder their success.
- To find EMET, it is best to be sure that you are on Microsoft's website. A good search term to use is: EMET site:Microsoft.com.



EMET site:microsoft.com

- The site operator tells Google to only return results from that site, in this case, Microsoft.com.
- EMET provides protection even when you install EMET "as is" with no customization needed. In addition, if you feel adventurous, it supports settings and configuration that will allow it to provide you with even more protection. More documentation is at Microsoft's website.

Your IT professionals can tune EMET's settings to protect more applications and adjust the level of protection.

For home offices, using EMET adds some level of protection, even if no additional configuration is performed.

Chapter 10

Bonus Information Specifically for SOHO

Creating Encrypted Storage Areas on Computers

When small organizations store files, especially if the organization does not have a file server, some computers contain important customer data on the internal drives such as the C: drive. If that computer is ever lost or stolen, then you should be concerned that the sensitive data might fall into the wrong hands.

A good security control is to create one or more dedicated places on the hard drive where you can store sensitive files. Then, if the computer is lost or stolen, it will be much more difficult for an unauthorized person to access files on that part of the drive.

To accomplish this, you will need something called a vdisk (short for "virtual disk") and a tool called BitLocker. You create vdisk with Windows, so there is nothing for you to buy. Microsoft includes BitLocker with many versions of the Windows OS. If you have a home or basic version of Windows, you might need to upgrade.

The way to create this secure area in plain English is as follows:

1. You will create a big storage place on your C: drive that will look like a new hard disk. That file is called a vdisk.
2. You will protect the new virtual disk with a password using BitLocker.

When you use your computer to open files, save files, make new folders, etc. everything will look like you have a new disk drive inside your computer.

When you keep your passwords secret, then in theory, if the computer ever falls into the wrong hands, those people will not be able to access any of the sensitive data.

The data will be protected using a technology called encryption. Encryption is designed to scramble data so thoroughly that someone can access the data only if they know the password to the disk.

Encryption won't help you at all if you login to your computer, unlock the secure drive, and then walk away. Anyone who wants to can sit down at the computer and see the data on the drive since you unlocked the drive. So, be sure to lock your computer when you walk away. The easiest way to do this is to hold down the "windows" key and tap the

L key. Keep your login password to yourself, as well as the different password that you use to unlock your virtual disk.

Furthermore, encryption won't help you if you are at your computer and an attacker has compromised your computer in some way. When you unlock the drive, then the attacker, who is already logged in with you, can see the same information that you can see, including the sensitive data on your encrypted vdisk.

But it is still very useful to have a secure file storage location that you can use to help protect your information in the event your computer is lost or stolen.

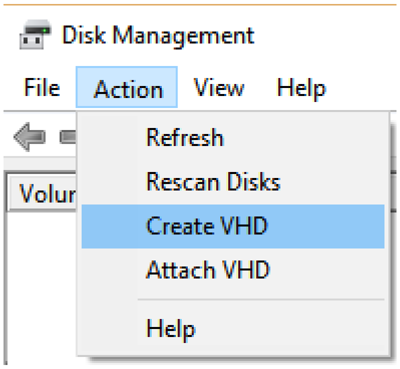
As an aside, you can use BitLocker to help protect your USB thumb drives, external hard drives, etc. if the drives are lost or stolen. Just don't tell anyone the password.

How to create a BitLocker encrypted virtual volume

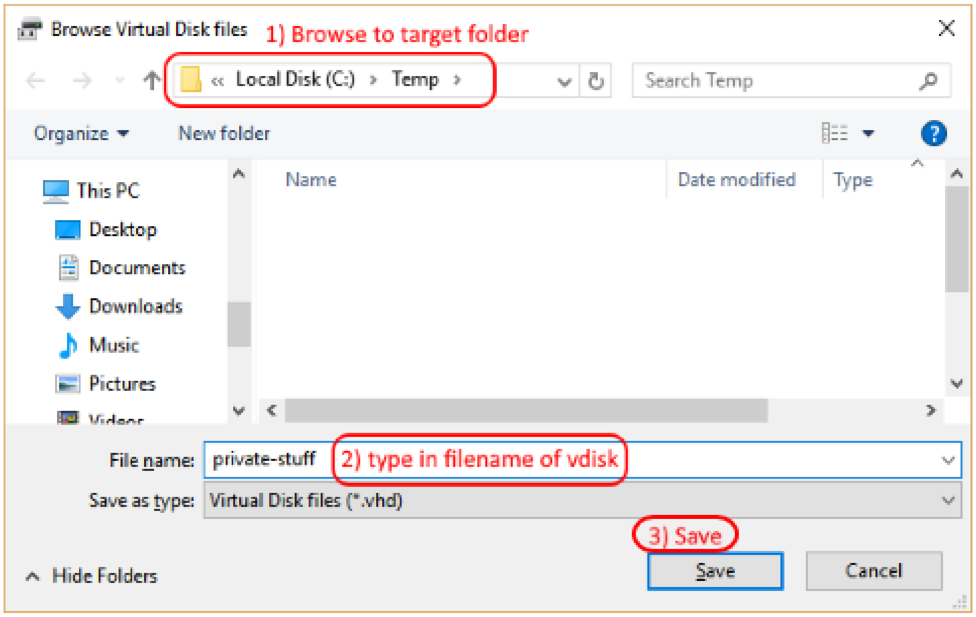
Step 1: How to Create a New vdisk

- Open the Disk Management console. On Windows 7 computers, click Start and in the Search box type "diskmgmt.msc." On Windows 8.1 and 10 computers, right-click on the Start Menu button and choose Disk Management from the menu.

- From the Disk Management console, click "Action" -> "Create VHD."



- From the "Create and Attach Virtual Hard Disk" window, click on the Browse button, navigate to a location where you'd like to store the encrypted virtual disk (vdisk), then type in a filename and click Save.



1) Browse to target folder

File name: private-stuff

2) type in filename of vdisk

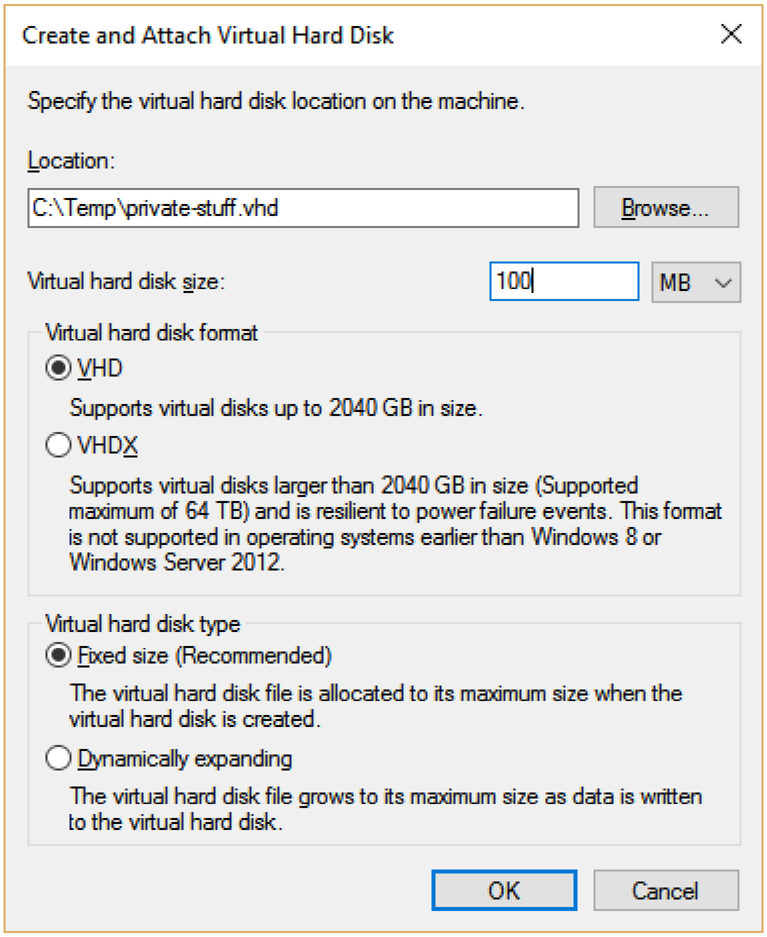
Save as type: Virtual Disk files (*.vhd)

3) Save

- For newer versions of Windows only, you'll have a choice between using the VHD format and the newer VHDX format for the new vdisk. Normally, you would choose the VHDX format; however, if you think you might transfer the vdisk to an older PC in the future, then choose the VHD format (which supports a maximum size of 2 TB).

- If disk space is at a premium, then you can choose the "dynamically expanding" disk type. That means that the file on your C: drive that holds the virtual hard disk will grows and grows as you store more data on that virtual drive. However, the safer and better performing choice is to create a fixed sized vdisk.

- When determining the size of vdisk you want to create, consider looking at how many gigabytes of data you are using on your computer already. Be sure to not fill up the computer's hard drive by creating a vdisk that is near the size of available space on your existing computer.



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location:

C:\Temp\private-stuff.vhd

Browse...

Virtual hard disk size: 100 MB

Virtual hard disk format

● VHD

Supports virtual disks up to 2040 GB in size.

○ VHDX

Supports virtual disks larger than 2040 GB in size (Supported maximum of 64 TB) and is resilient to power failure events. This format is not supported in operating systems earlier than Windows 8 or Windows Server 2012.

Virtual hard disk type

● Fixed size (Recommended)

The virtual hard disk file is allocated to its maximum size when the virtual hard disk is created.

○ Dynamically expanding

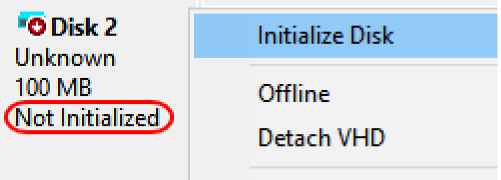
The virtual hard disk file grows to its maximum size as data is written to the virtual hard disk.

OK Cancel

- Click OK to create the new vdisk.

- Locate the new disk in the console, based on the size of vdisk you created. Hint: it's the one with the red icon, with status "Not initialized."

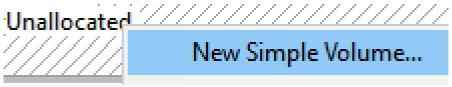
- Right-click on the new vdisk and choose "Initialize disk" from the menu.



Disk 2
Unknown
100 MB
Not Initialized

- From the "Initialize Disk" window, leave the partition style as "MBR" unless your vdisk is larger than 2 TB (in which case, select the GPT partition style instead). Click OK to initialize the disk.

- The new vdisk will now change status to "Online," but before it can be used you must create a volume on it. To do that, right-click on the word "Unallocated" and choose "New Simple Volume..." from the menu.



- From the "New Simple Volume Wizard" window, click Next on the Welcome screen.

- Click Next on the "Specify Volume Size" page.

- From the "Assign Drive Letter or Path" page, choose whatever available drive letter you like and click Next.

- On the "Format Partition" page, type in a volume label but leave the rest of the settings as is. Click Next.

- On the "Completing the New Simple Volume Wizard" page, review the settings and then click Finish.

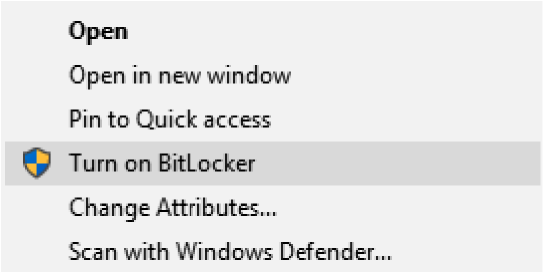
Congratulations, you've now created a new vdisk! If you open Windows Explorer, you'll see the new disk. All that's left to do is to tell Windows to encrypt the vdisk, so that anything you store on it will be encrypted too.

Step 2: How to Enable Encryption on the New vdisk

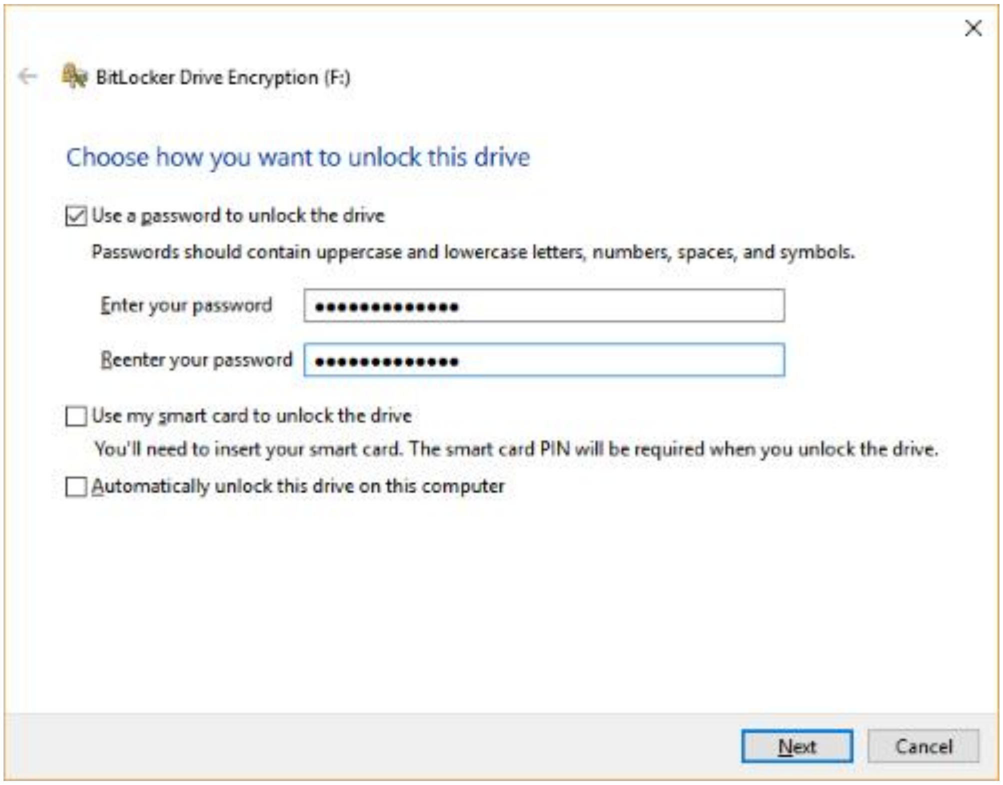
- Open Windows Explorer. On Windows 7 computers, click Start -> Computer. On Windows 8.1 and 10 computers, right-click on the Start Menu button and choose File Explorer from the menu.

- On the right-hand side of the File Explorer window, click on "This PC" (for Windows 7, choose Computer).

- Based on the drive letter you selected earlier, locate the new vdisk drive, right-click on it, and choose "Turn on BitLocker" from the menu.



- From the window that appears, select "Use a password to unlock the drive." Type in a secure password phrase, then click Next.



BitLocker Drive Encryption (F:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password •••••••••••••

Reenter your password •••••••••••••

□ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

□ Automatically unlock this drive on this computer

- Before selecting your choice for the question, “How do you want to back up your recovery key?”, consider the following, and you will use the last option:

  - Save to your Microsoft account: While this choice is convenient, realize that if your Microsoft account is hacked then your recovery key is compromised and your encrypted vdisk can be decrypted by anyone who has the key.

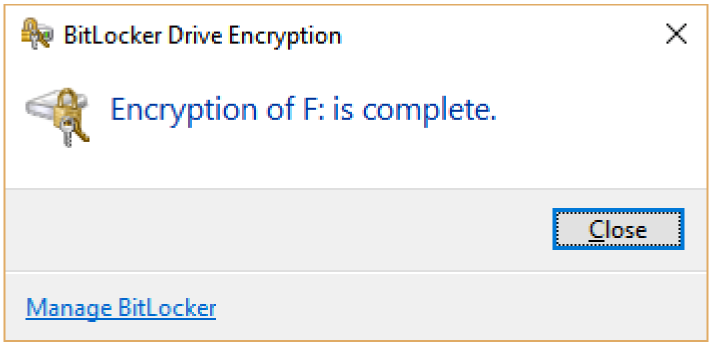
  - Save to a USB flash drive: While this choice keeps your recovery key more private, realize that if you lose the USB flash drive or if the drive fails then you will never be able to unencrypt your data.

  - Save to a file: Use this option carefully, as storing your recovery key on the same PC as where the encrypted vdisk resides makes it easy for a hacker to decrypt your data. So save the key to somewhere besides your own computer.

  - Print the recovery key: **Do this regardless of whatever other choice you select**. In other words, print a hardcopy of the recovery key and store it in a safe place. If you want to, then also choose one of the above backup methods to supplement the hardcopy.

- If you have a new version of Windows 10, then you will be asked “Choose which encryption mode to use.” Choose the new mode unless you expect to move the encrypted vdisk to an older PC.

- When asked “Are you ready to encrypt this drive”, click on the “Start Encrypting” button.



BitLocker Drive Encryption

Encryption of F: is complete.

- Click Close.

At this point, Windows has encrypted the vdisk and mounted the volume for use. You can now start saving documents and other data to the vdisk.

IMPORTANT NOTE: Until you reboot your PC, the encrypted vdisk is mounted and its contents are accessible to anyone using your PC without having to provide a password. Upon reboot, you will be prompted to provide a password to unlock the vdisk before it can be accessed (mounted). Once mounted, the drive will again be accessible without having to provide a password, until the next reboot.

Apple offers the same functionality in a feature called FileVault.

For home offices, encrypted partitions can be used to provide some level of protection to your sensitive data, as long as only authorized individuals know the key and the drive is locked. This strategy can be especially helpful on laptop computers if they are lost or stolen.