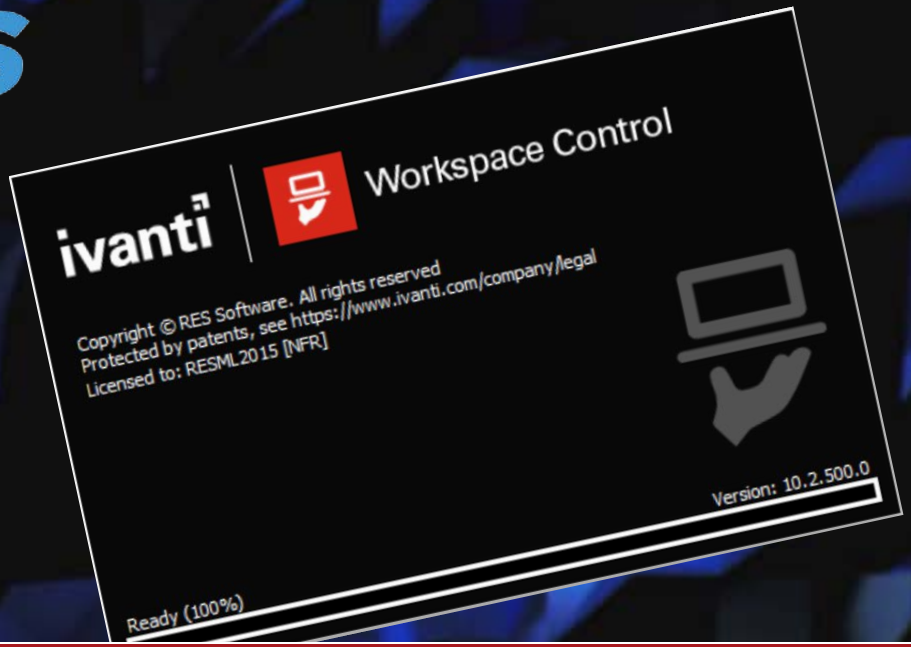
BSIDES Delft



All Ivanti is a secure Workspace

securify.nl/red

Agenda

All Ivanti is a secure Workspace

- About me
- Introduction
- Credentials
- Dynamic Privileges
- Whitelisting/blacklisting
- Conclusion

ivanti RES

About me

Yorick Koster

@yorickkoster

- Co-founder Securify
- Proactive Application Security
- Ethical Hacking
- Agile Security
- Red Teaming

- 15+ years in the field
- Focus on offensive security

Securify

- Security Code Reviews
- Penetration Testing / Ethical Hacking
- Mobile Security Testing
- Automated Security Testing
- Inline Agile Security
- Red Teaming
- Security Awareness
- Smart Contract Security

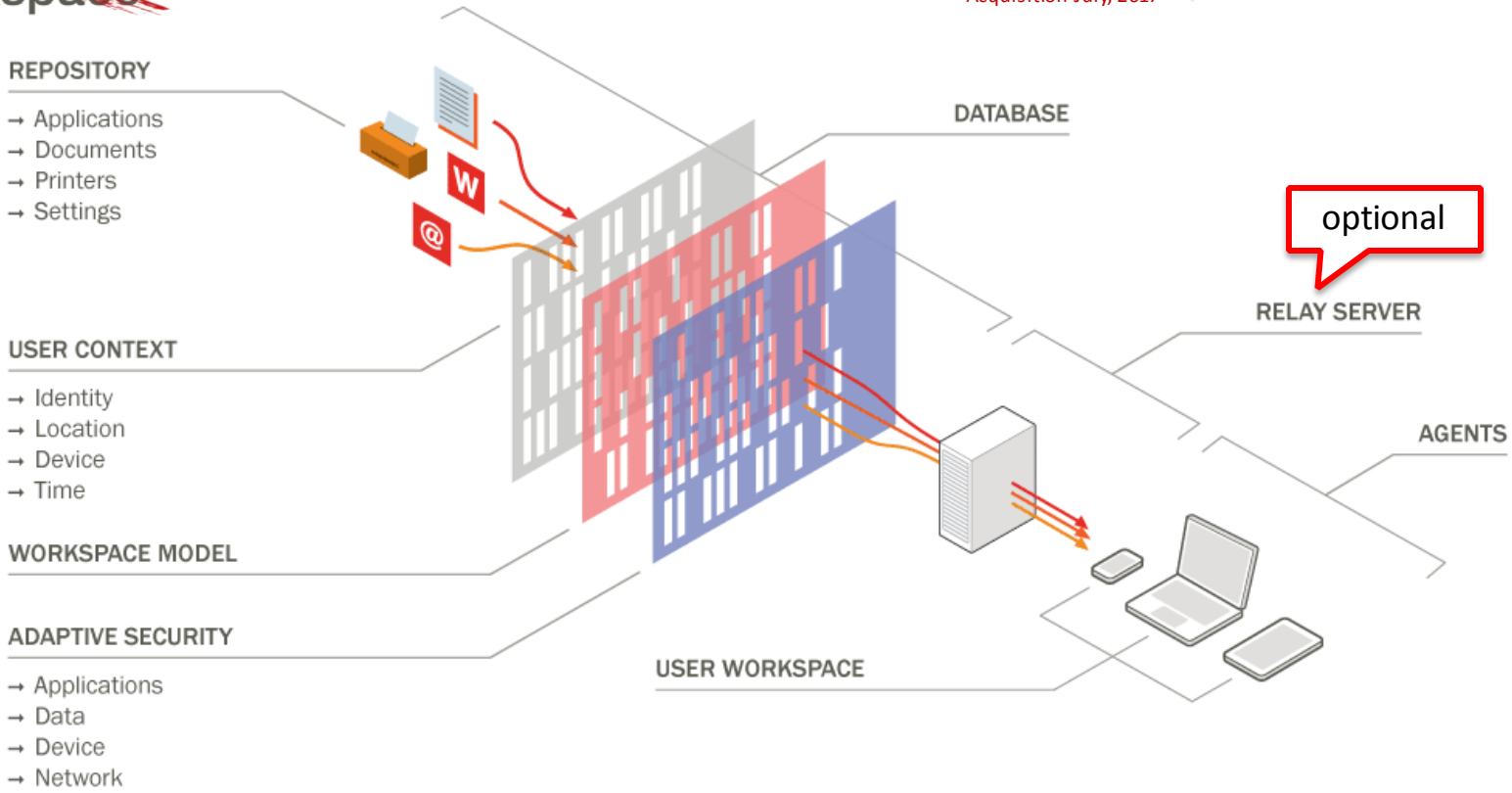
Introduction

RES ONE® Workspace

ivanti

Acquisition July, 2017

Workspace Control

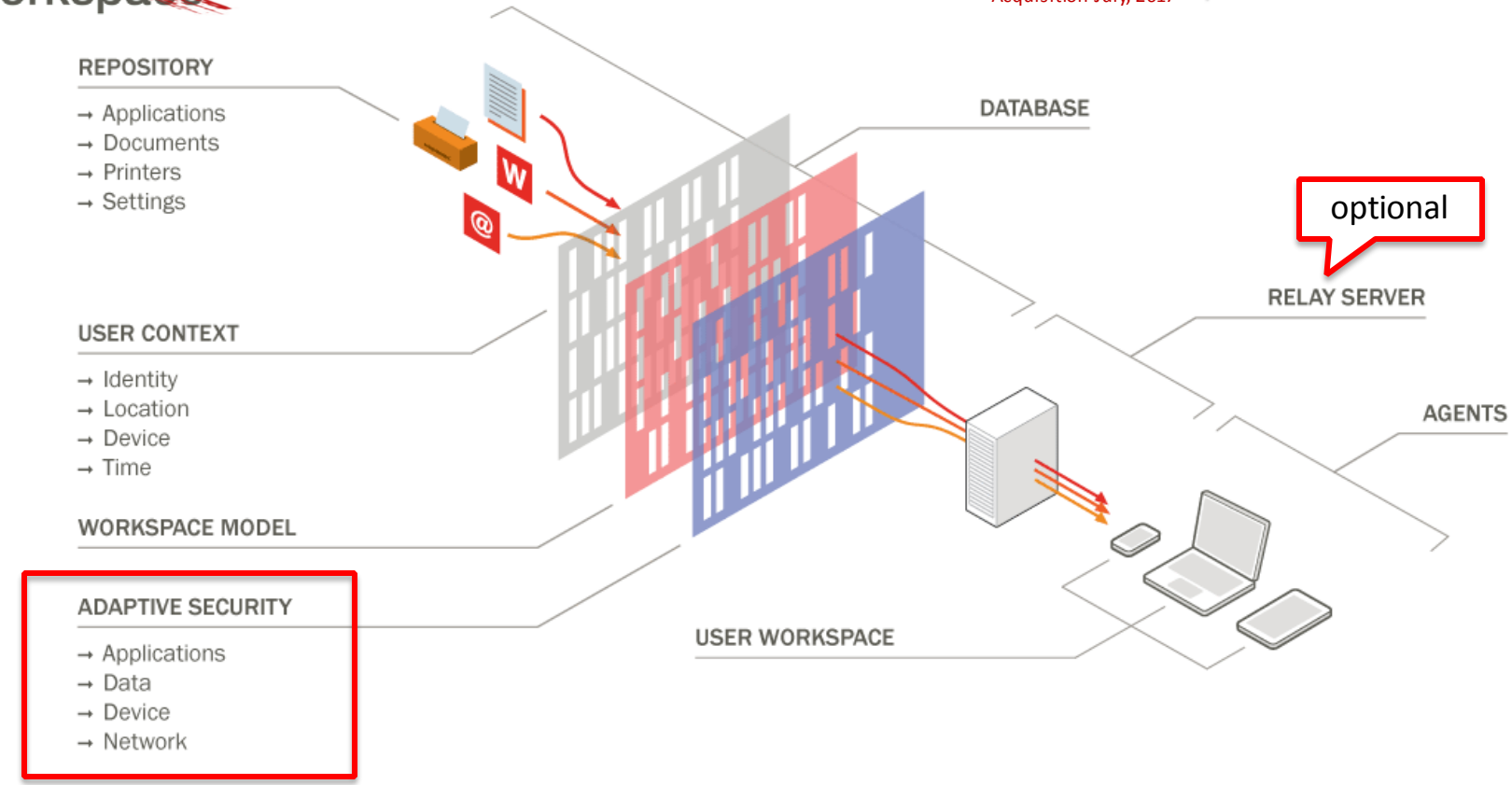


RES ONE Workspace

ivanti

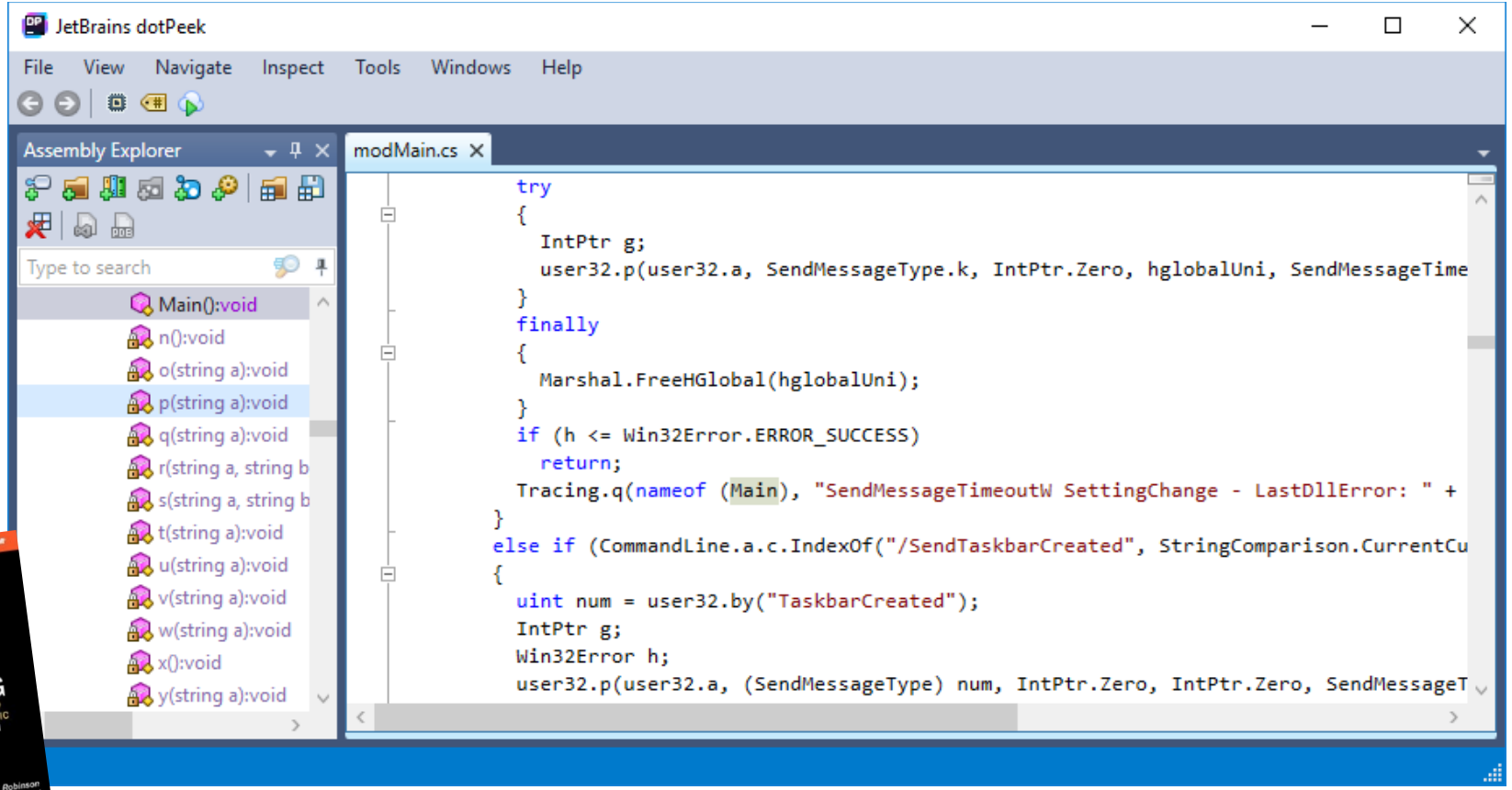
Acquisition July, 2017

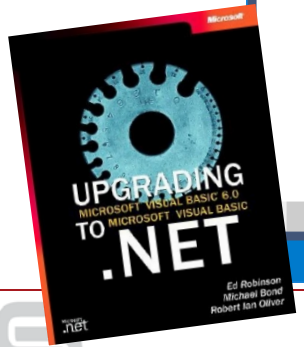
Workspace Control



Build on .NET Framework

(mostly)





Tracing

RES Trace Viewer

To use the Ivanti Works

1. **Download the**
2. Use **"Run as A**
3. **Adjust the filt**
   Do not hesitate
4. **Choose "Yes"**
5. **Save** the Trace

5. After reproducing the

Enable_WM_Tracing_x6
486 bytes

Enable_WM_Tracing_x8
438 bytes

RESPFTraceView.exe.zip
68.1 K

RES ONE Workspace - Trace Viewer

File Help

Time	ProcessID	ThreadID	Executable	SessionID	Username	Info
2018-05-12 22:18:50.082	5744	8	pfwsmgr	2	Securify	ProcessInterceptionHandlerBase.ProcessPreStart; - Process Arg...
2018-05-12 22:18:50.082	5744	8	pfwsmgr	2	Securify	ProcessInterceptionHandlerBase.ProcessPreStart; - Parent Proc...
2018-05-12 22:18:50.082	5744	8	pfwsmgr	2	Securify	ProcessInterceptionHandler.SkipInterception; Process was start...
2018-05-12 22:18:50.082	5744	8	pfwsmgr	2	Securify	ProcessInterceptionHandler.ProcessPreStartNotification; Skippin...
2018-05-12 22:18:50.082	5744	8	pfwsmgr	2	Securify	ProcessInterceptionHandlerBase.ProcessPreStart; - Block Proce...
2018-05-12 22:18:50.082	5744	8	pfwsmgr	2	Securify	ImgGuardDriver.OnInterceptionNotificationsFunction; processPr...
2018-05-12 22:18:50.082	5744	8	pfwsmgr	2	Securify	ImgGuardDriver.OnInterceptionNotificationsFunction; actionflags...
2018-05-12 22:18:50.098	5848	1	pwrgrid	2	Securify	DoShellExecuteEx; Result: True
2018-05-12 22:18:50.098	5848	1	pwrgrid	2	Securify	DoShellExecuteEx; Waiting for process to complete
2018-05-12 22:18:50.724	5744	1	pfwsmgr	2	Securify	fIngReceiveWindows; Adding new task for Untitled - Paint
2018-05-12 22:18:50.724	5744	1	pfwsmgr	2	Securify	fstrExecuteJob; Start, job='GETPROCENVVARS', host='', timeou...
2018-05-12 22:18:50.724	5744	1	pfwsmgr	2	Securify	fstrExecuteJob; AT1 = 3604
2018-05-12 22:18:50.724	5744	1	pfwsmgr	2	Securify	fstrExecuteJob; AT2 = PFAPPID
2018-05-12 22:18:50.724	2632	15	res	0	SYSTEM	IPDaemon_DataIn; RemoteHost=::ffff:127.0.0.1, RemotePort=...
2018-05-12 22:18:50.724	2632	15	res	0	SYSTEM	IPDaemon_DataIn; Local connection
2018-05-12 22:18:50.724	2632	5	res	0	SYSTEM	Operator.DataIn; RemoteHost = ::ffff:127.0.0.1
2018-05-12 22:18:50.724	2632	5	res	0	SYSTEM	Operator.DataIn; Processing message 'GETPROCENVVARS' for u...
2018-05-12 22:18:50.724	2632	5	res	0	SYSTEM	fstrProcessJob; Job Received (GETPROCENVVARS)
2018-05-12 22:18:50.739	5744	1	pfwsmgr	2	Securify	fIngCheckTask; Title: Untitled - Paint ,AppID: 33 , AppGuid: {35A...
2018-05-12 22:18:50.739	5744	1	pfwsmgr	2	Securify	fIngCheckTask; Last Appguid {35AA6936-60CE-4346-BE91-F5CF...
2018-05-12 22:18:50.739	5744	1	pfwsmgr	2	Securify	UpdateSwitch; set to back color
2018-05-12 22:18:50.739	5744	1	pfwsmgr	2	Securify	fIngReceiveWindows; ysnUpdateIcon = True ; ysnUpdateSwitch ...
2018-05-12 22:18:50.739	5744	1	pfwsmgr	2	Securify	fstrExecuteJob; Start, job='GETPROCENVVARS', host='', timeou...
2018-05-12 22:18:50.739	5744	1	pfwsmgr	2	Securify	fstrExecuteJob; AT1 = 3604
2018-05-12 22:18:50.739	5744	1	pfwsmgr	2	Securify	fstrExecuteJob; AT2 = PFAPPID
2018-05-12 22:18:50.739	2632	14	res	0	SYSTEM	IPDaemon_DataIn; RemoteHost=::ffff:127.0.0.1, RemotePort=...
2018-05-12 22:18:50.739	2632	14	res	0	SYSTEM	IPDaemon_DataIn; Local connection

Start Clear Auto scroll Copy Show Perf points Find... Filters...

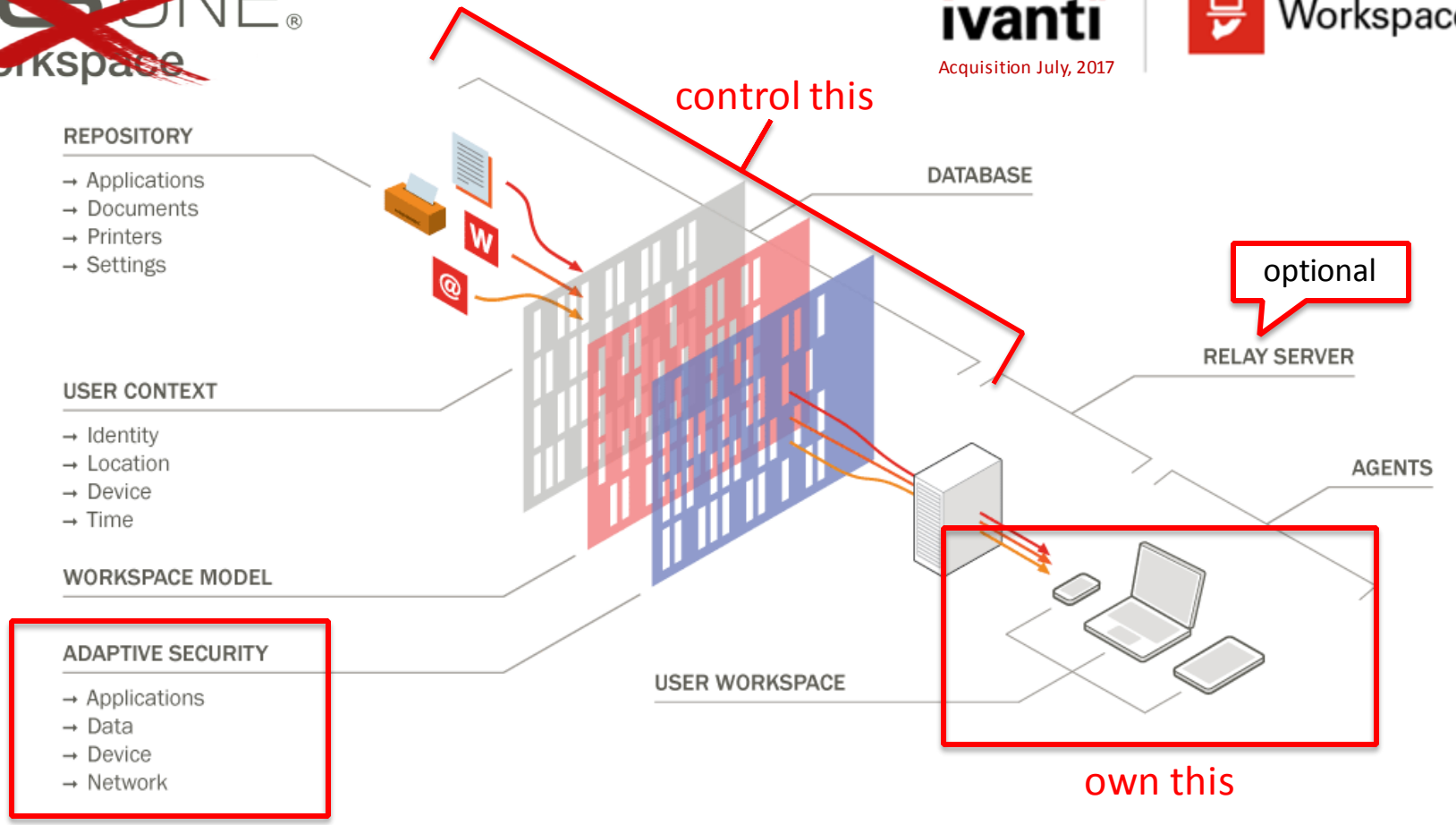
Credentials

RES ONE Workspace

ivanti

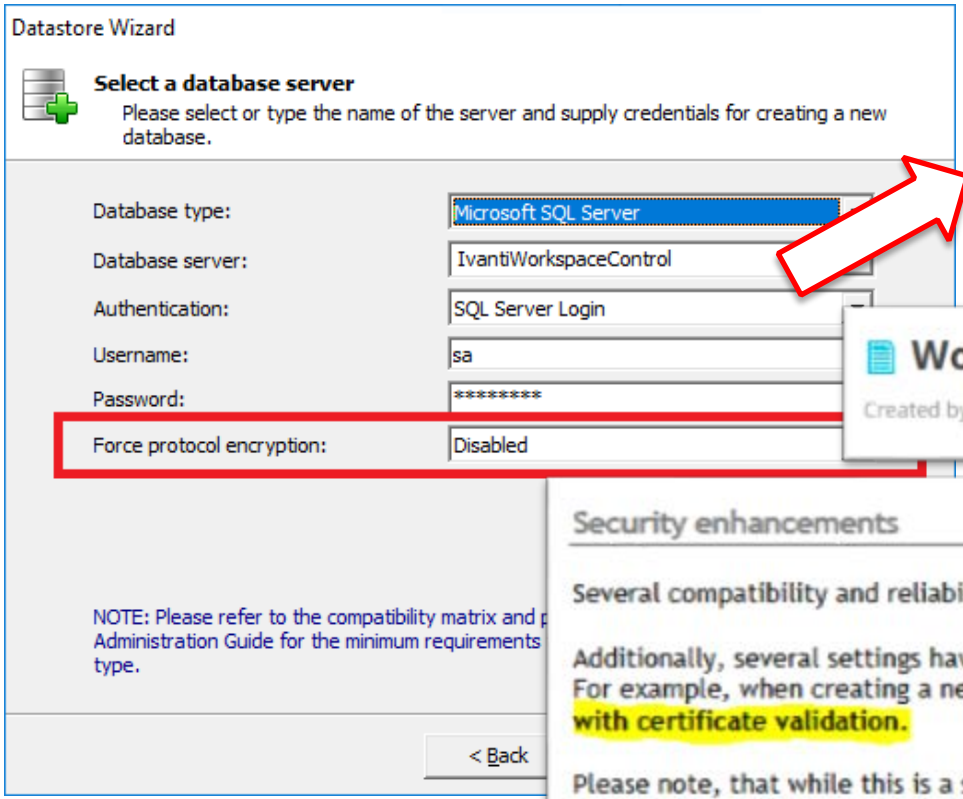
Acquisition July, 2017

Workspace Control



Getting credentials

Database




```
[MSSQL] Cleartext Client   : 172.16.123.67
[MSSQL] Cleartext Hostname : [redacted]
[MSSQL] Cleartext Username : RES
[MSSQL] Cleartext Password : [redacted]
[*] Skipping previously captured hash for RES
```

Workspace Control Software 10.2.0.0

Created by hannahc on Dec 21, 2017 7:55 AM. Last modified by hannahc on Jan 2, 2018 7:23 AM.

Security enhancements

Several compatibility and reliability enhancements have been made to improve security.

Additionally, several settings have been changed to a more secure option by default.
For example, when creating a new Datastore, **Force protocol encryption is now set to Enabled, with certificate validation.**

Please note, that while this is a secure setting, it does mean that the **Database server** must be specified by its hostname, which must match the Common name (CN) or Subject alternative name (SAN) in the database server certificate. Using an IP address is not possible with this setting.

https://community.ivanti.com/docs/DOC-62842

Getting credentials

Installation scripts (which everyone removes of course)

HOWTO: Perform an unattended installation of RES Workspace Manager

To install RES Workspace Manager unattended on a computer and to connect it to an existing datastore, you can apply the following public properties to the ".msi" package:

DBTYPE: Specifies the database type. This can be MSSQL, DB2, ORACLE or MYSQL.
DBSERVER: Specifies the database server that RES Workspace Manager should connect to.
DBNAME: Specifies the database name that RES Workspace Manager should connect to.
DBUSER: Specifies the database username that RES Workspace Manager should use to connect to the database.
DBPASSWORD: Specifies the database password that RES Workspace Manager should use to connect to the database.
DBPROTOCOLENCRYPTION: Specifies whether protocol encryption should be used when connecting to Microsoft SQL Server. Values are "yes" or "no" (default is "no").
ADDTOWORKSPACE: Specifies the names of the workspaces that this computer should be a member of after finishing installation. Separate multiple workspace names using bagpipes "|" (optional).

Example:

```
Msiexec /i c:\RES_WM_2014.msi DBSERVER=SQLSERVER01 DBNAME=RESWM DBUSER=WMUser
DBPASSWORD=WMUserPassword DBTYPE=MSSQL DBPROTOCOLENCRYPTION=No /qn
```

https://community.ivanti.com/docs/DOC-63291

Getting credentials

Password storage

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\RES\Workspace Manager

- Mozilla
- mozilla.org
- MozillaPlugins
- ODBC
- Policies
- Python
- RegisteredApplications
- RES
  - Workspace Manager
    - Data
    - Settings

Name	Type	Data
DBEncryption	REG_DWORD	0x00000000 (0)
DBName	REG_SZ	RESONEWorkspace
DBPassword	REG_BINARY	70 00 92 01 bb 00 3a 00 34 00 6f 00 d4 …
DBPasswordConverted	REG_DWORD	0x00000001 (1)
DBPasswordEx	REG_BINARY	5d ea 76 50 f4 48 7b c1 17 10 47 3d 53 2c bd 2b
DBServer	REG_SZ	DESKTOP-5G8HK7E
DBState	REG_DWORD	0x00000001 (1)
DBType	REG_SZ	MSSQL
DBUser	REG_SZ	IvantiWorks

same for relay server config
FIPS mode not better

```
if (num5 == -1 && destinationIndex == -1 || num5 < destinationIndex)
  return numArray;
for (int index = destinationIndex; index <= num5 - 2; ++index)
  array[index] = (byte) ((ulong) ((int) array[index] ^ (int) array[index + 2]) ^ (ulong) (num4 * (long) array[index + 1] % 256L));
; index >= destinationIndex + 2; --index)
e) ((ulong) ((int) array[index] ^ (int) array[index - 2]) ^ (ulong) (num3 * (long) array[index - 1] % 256L));
inationIndex; index <= num5 - 1; ++index)
e) ((ulong) ((int) array[index] ^ (int) array[index + 1]) ^ (ulong) (num2 * (long) array[index + 1] % 256L));
 index >= destinationIndex + 1; --index)
) ((ulong) ((int) array[index] ^ (int) array[index - 1]) ^ (ulong) (num1 * (long) array[index - 1] % 256L));
```

Type: MSSQL
Server: 192.168.144.154
Name: IvantiWorkspaceControl
Username: IvantiWorkspaceContr
Password: Resforever123!
State: 0
Encryption: 0

Mitigate

Protect credentials, use Least Privileges

- Use Relay server if you can (haven't looked at it yet)

- Alternatively, use Windows authentication
- Implement Least Privileges, most users shouldn't be able to make changes

- Enable TLS with certificate validation
- Block outgoing connections when device not connected to internal network

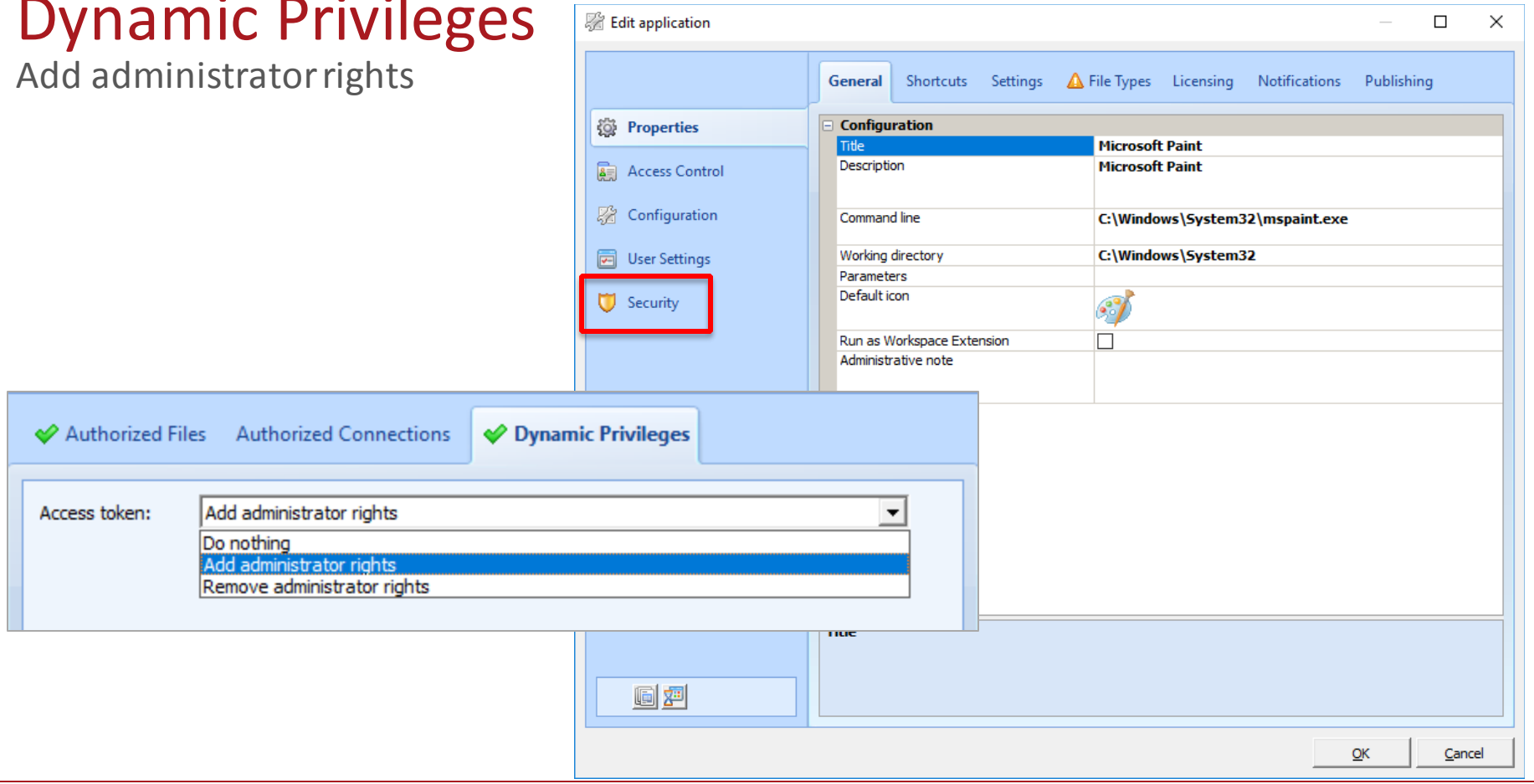
- Remove installation scripts

- Upgrade to Ivanti 10.3.10.0 or later
- Ivanti should really use Windows Data Protection API

Dynamic Privileges

Dynamic Privileges

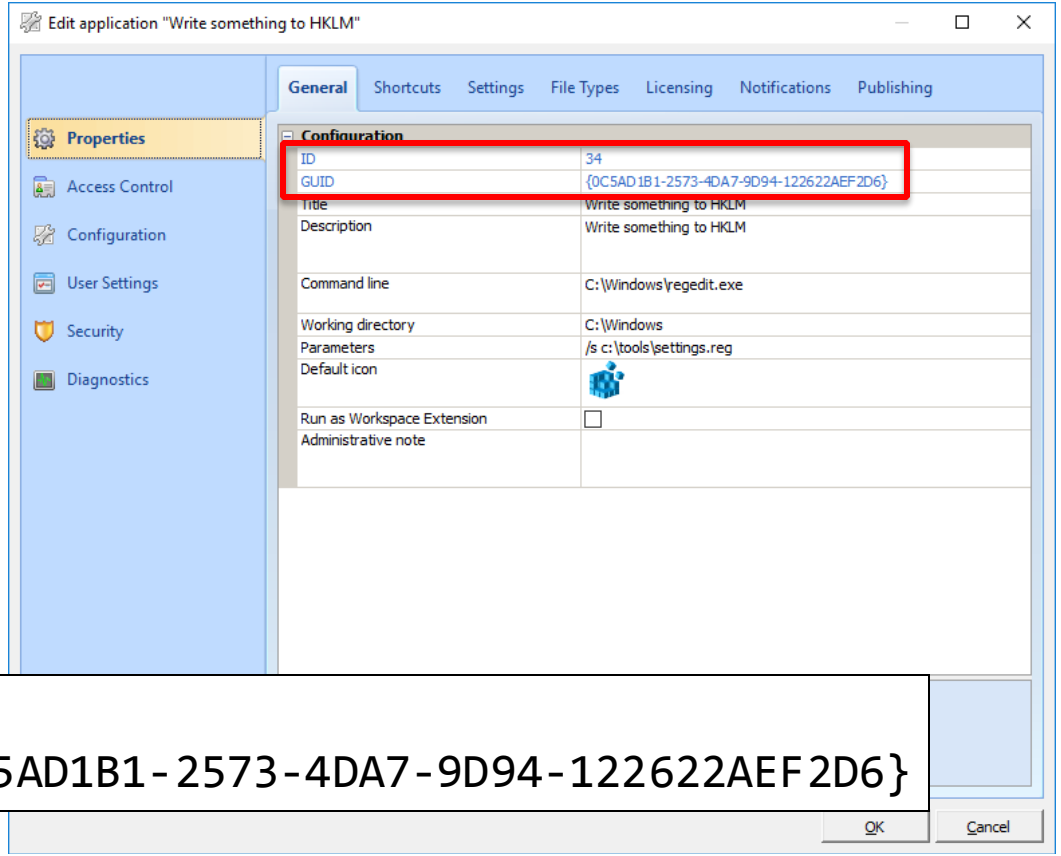
Add administrator rights



Dynamic Privileges

Write to HKLM

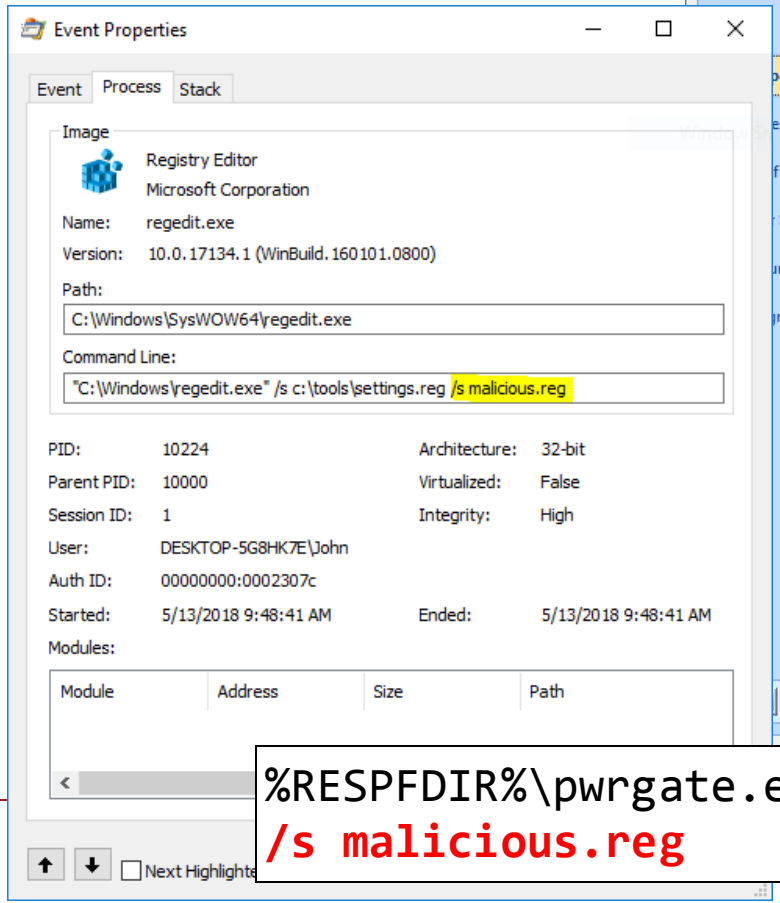
- Run elevated regedit.exe, let user change something in HKLM
- Invoke application via ID or GUID

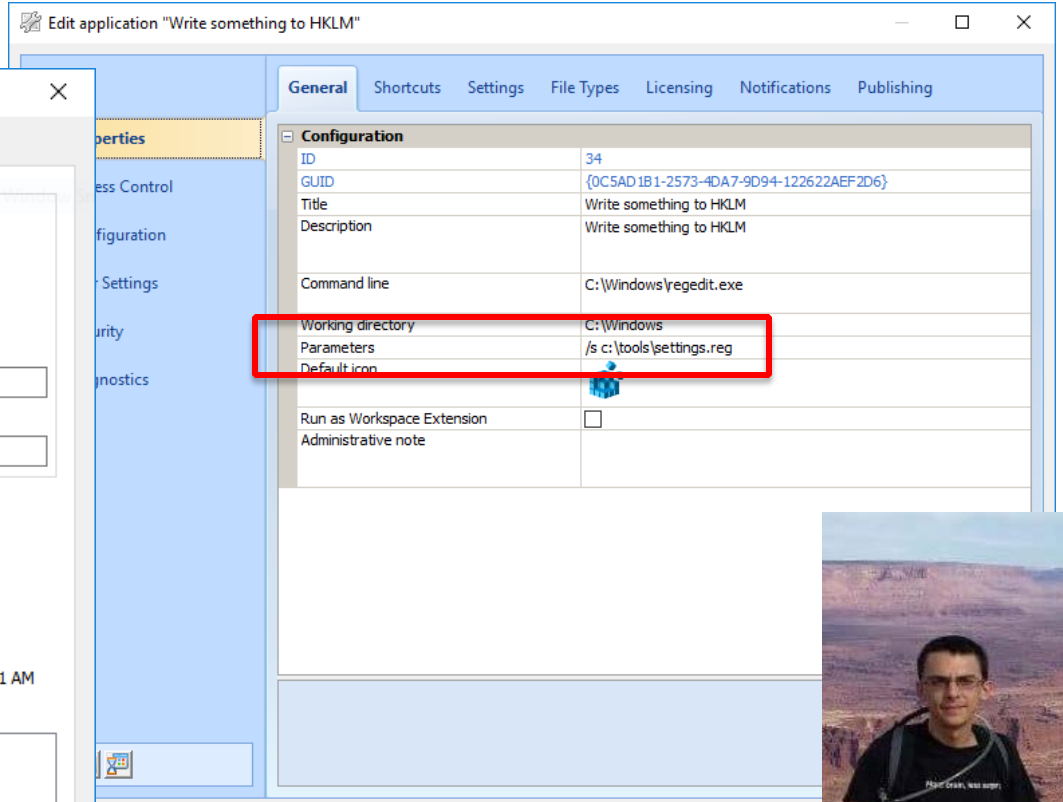



```
%RESPFDIR%\pwrgate.exe 34
%RESPFDIR%\pwrgate.exe {0C5AD1B1-2573-4DA7-9D94-122622AEF2D6}
```

Dynamic Privileges

Pass extra parameters






```
%RESPFDIR%\pwrgate.exe 34
/s malicious.reg
```

Dynamic privileges

Auto add admin rights

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE

- SOFTWARE
  - Caphyon
  - Classes
  - Clients
  - Google
  - Hewlett-Packard
  - Intel
  - Macromedia

Name	Type	Data
(Default)	REG_SZ	(value not set)
I shouldn't be able to write here	REG_SZ	

Automatic shortcuts

Replace existing unmanaged shortcuts	☐
Create Start Menu shortcut	☑
If managed shortcut was not used	Intercept new process and apply configuration
Personalized Start Menu	Ignore
Desktop	Intercept new process and apply configuration
Quick Launch / Pin to taskbar	Take no action
Pin to Start Menu	Take no action

Regedit

regedit.exe:8756 Properties

Image | Performance | Performance Graph | GPU Graph

Threads | TCP/IP | Security | Environment | Strings

User: DESKTOP-5G8HK7E\John

SID: S-1-5-21-3504069232-950747955-176138969-1002

Session: 1 Logon Session: 2307c

Virtualized: No Protected: No

Group	Flags
BUILTIN\Administrators	Mandatory
BUILTIN\Users	Mandatory
CONSOLE LOGON	Mandatory
DESKTOP-5G8HK7E\None	Mandatory
Everyone	Mandatory
LOCAL	Mandatory
Mandatory Label\High Mandatory Level	Integrity
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory

Group SID: S-1-5-32-544

Privilege	Flags
SeBackupPrivilege	Disabled
SeChangeNotifyPrivilege	Default Enabled
SeCreateGlobalPrivilege	Default Enabled
SeCreatePagefilePrivilege	Disabled
SeCreateSymbolicLinkPrivilege	Disabled
SeDebugPrivilege	Disabled
SeImpersonatePrivilege	Default Enabled

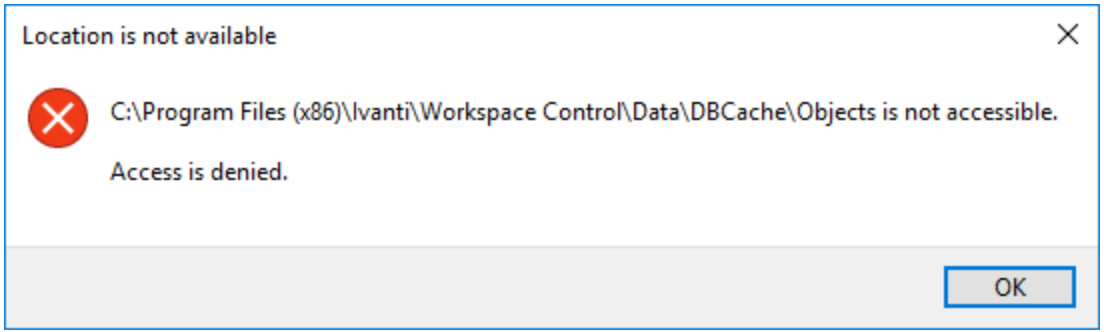
Permissions

OK Cancel

Dynamic privileges

Audit apps.xml

- Get a copy of %RESPFDIR%\Data\DBCache\Objects\apps.xml
- Look for *add_admin_rights*
- Review use of Environment Variables & UNC paths
- Review NTFS permissions
- Be aware that the application may be access control restricted
  - Identity (eg, User or Group)
  - Location and Devices
  - Date and Time
  - Workspace Container



Dynamic privileges

Audit apps.xml

```
 <application>
    <guid>{0C5AD1B1-2573-4DA7-9D94-122622AEF2D6}</guid>
    <configuration>
      <menu />
      <title>Write something to HKLM</title>
[...]
    <accesscontrol access_mode="or">
      <accesstype>group</accesstype>
      <grouplist>
        <group sid="S-1-5-XXXXX" type="group">CORP\PowerUsers</group>
      </grouplist>
      <notgrouplist />
    </accesscontrol>
[...]
    <security_privileges>
      <access_token>add_admin_rights</access_token>
    </security_privileges>
```

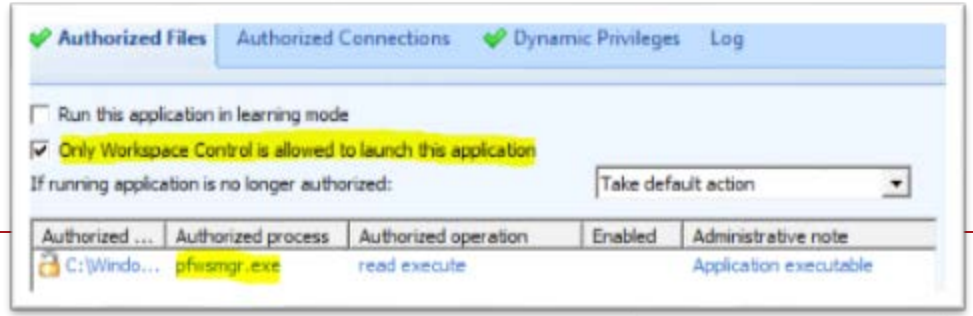
Mitigate

Dynamic privileges

- Don’t user dynamic privileges, seriously
  - Removing admin rights is probably okay

- But if you must:
  - Restrict as much as possible (ACL it)
  - Wrap the functionality to disregard arbitrary arguments (eg, script it)
  - Avoid applications that run on the interactive Desktop (have a GUI)
  - Disable intercepting of process
  - Only allow Workspace Control to launch the application

- Most of the times you don’t need it!



Whitelisting/Blacklisting

Application whitelisting

- I ❤ whitelisting
- Not a silver bullet
- An example:
  - Sysadmins want to use PowerShell
  - Malware abuses PowerShell
  - Install PowerShell on your default image,
  - but only give it to people that need it
  - You can even bind it to a location or workstation

File Certificate-based Application Whitelisting

In the v10.1 release, in July 2017, we introduced improved security management in the Management Portal. Basically, this version focused on a redesign of existing application whitelisting feature including a technical preview of whitelist management using file certificate. More information can be read in this blog. This Workspace Control v10.2 release contains the final version of this simplified and powerful application whitelisting feature.

Certificate-based whitelisting

Let's take the Microsoft Office 2016 suite as an example. If you want to whitelist applications like Word, Excel, Outlook and PowerPoint you need a whitelist rule per application and per application version when using application whitelisting based on executables or file hashes. Of course, while application whitelisting based on file hashes is very secure, it does require quite some maintenance because if an update of Microsoft Office is installed, the file hashes will change.

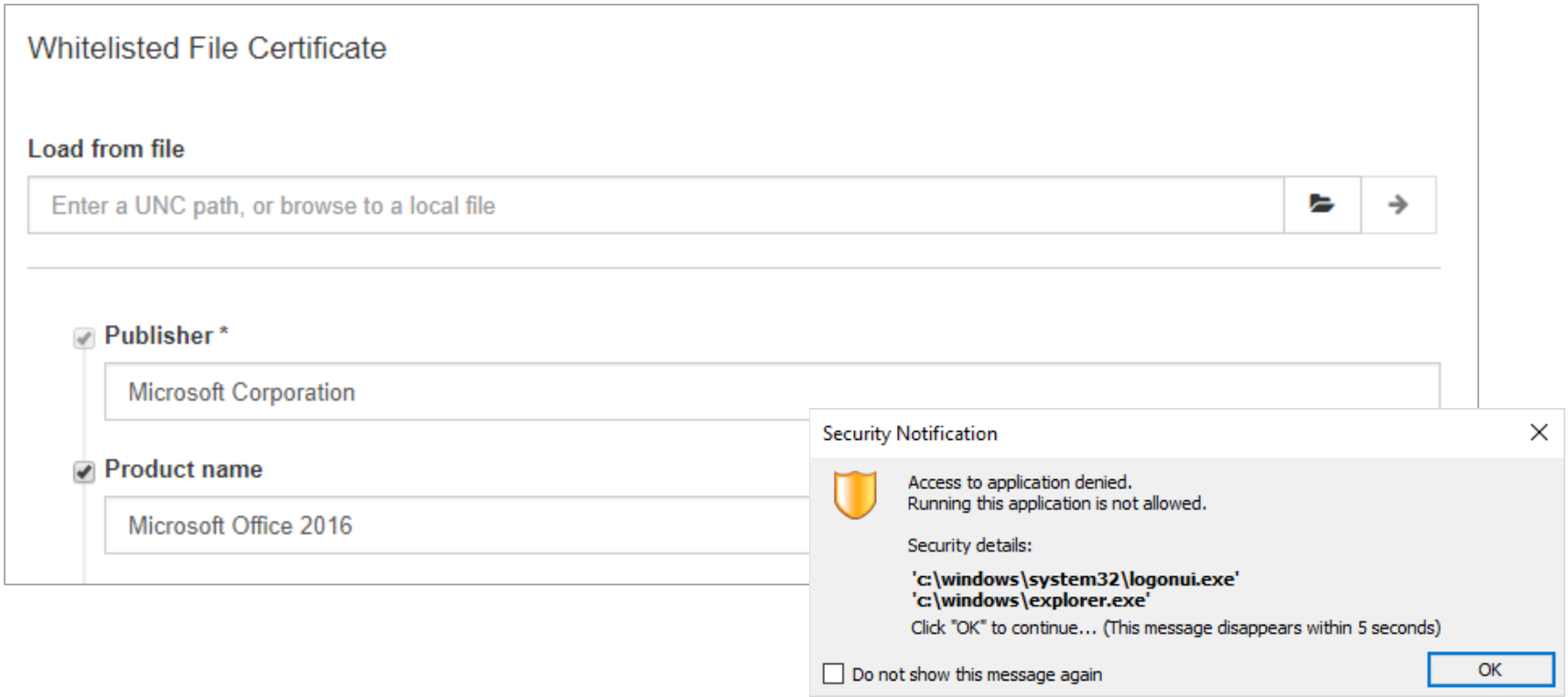
With application whitelisting based on file certificates you can easily create a whitelist rule based on the digital signature of the Microsoft Office applications. In this example a rule is created which whitelists all the applications with the publisher 'Microsoft Corporation' and product name 'Microsoft Office 2016':

Not mature enough at this moment

https://www.ivanti.com/blog/introducing-ivanti-workspace-control-10-2/

Certificate-based whitelisting

Doesn’t work well with path-based whitelisting



Certificate-based whitelisting

Likely end up blacklisting

PUBLISHER	PRODUCT NAME	ORIGINAL FILE NAME	FILE VERSION	MODE
Microsoft Corporation	Microsoft® .NET Framework	AddInProcess.exe		⊘
Microsoft Corporation	Microsoft® .NET Framework	MSBuild.exe		⊘
Microsoft Corporation	Microsoft Edge			✔
Microsoft Corporation	Microsoft® .NET Framework	AddInProcess32.exe		⊘
Microsoft Corporation	Microsoft® .NET Framework	AddInUtil.exe		⊘
Microsoft Corporation	Microsoft Office 2016			✔
Microsoft Windows	Windows® Search			✔
Microsoft Windows	Microsoft® Windows® Operating System			✔
Microsoft Windows Publisher	Microsoft® Windows® Operating System			✔
VMware, Inc.	VMware Tools			✔

Application whitelisting

Path-based whitelisting

Authorize file

Settings | File Hashes | Log | Access Control | Workspace Control

Authorized file (path): C:\Windows\System32\notepad.exe

Enabled

Administrative note:

Allow only this specific process to launch or access this file:

Allow any process to launch or access this file

Authorized operation: Read Execute Modify Logging

EXAMPLES:
C:\Program Files\Application\Example1.exe
C:\Program Files\Application\AllowedVBScript.vbs
C:\Program Files\Application*.exe
\\Server1\Fileshare1\Application\Example2.exe

NOTE: All applications accessible by the user are automatically authorized. All other executables are NOT authorized. All files other than executables (like .pdf, .doc or .vbs) are accessible by default, unless otherwise configured in Security.

OK Cancel

C:\Program Files (x86)\windows nt\accessories\wordpad.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

OK

Security Notification

Access to application denied.
Running this application is not allowed.

Security details:

'c:\program files (x86)\windows nt\accessories\wordpad.exe'

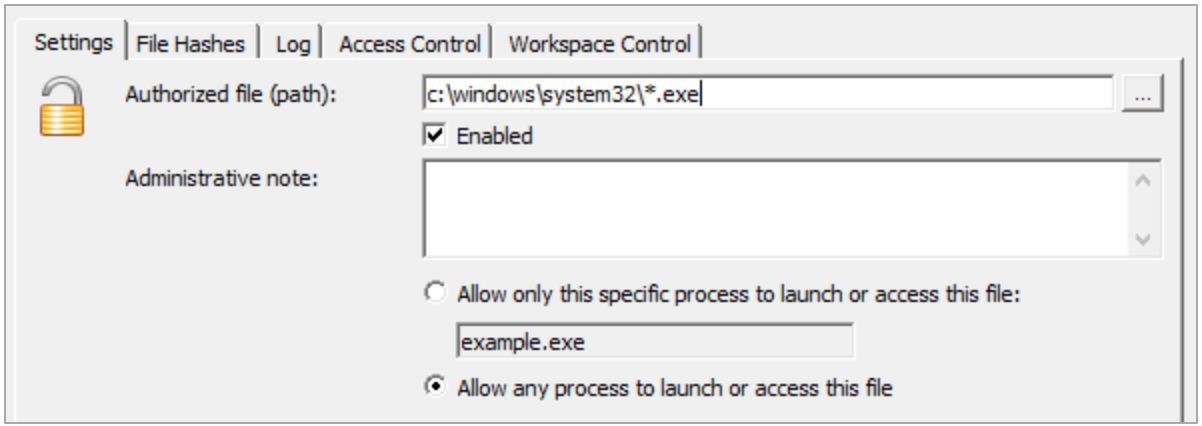
Click "OK" to continue... (This message disappears within 20 seconds)

Do not show this message again OK

Application whitelisting

Blacklisting?

No blacklisting for path-based whitelisting



https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

https://github.com/api0cradle/UltimateAppLockerByPassList
https://github.com/api0cradle/LOLBAS

Application whitelisting

Find bypasses

- Get a copy of %RESPFDIR%\Data\DBCache\Objects\apps.xml
- Get a copy of %RESPFDIR%\Data\DBCache\Objects\sec_globauth.xml
- Review use of Environment Variables & UNC paths
- Review NTFS permissions
- Easier to try and run every application and work from there (**including 32-bit**)
- Use Sysinternals if you can

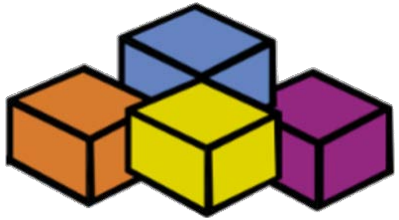
```
function TryExecute(folderspec)     {
       var f = fso.GetFolder(folderspec);

       var subfolders = new Enumerator(f.SubFolders);
       for(; !subfolders.atEnd(); subfolders.moveNext()) {
              TryExecute((subfolders.item()).path);
       }

       var fc = new Enumerator(f.files);
       for (; !fc.atEnd(); fc.moveNext()) {
              path = fc.item().Path.toLowerCase();
              if(endsWith(path, '.exe')) {
                     try {
                            ShellExecute(path);
                            logMsg(path);
                     } catch(e) {
                            // do nothing
                     }
              }
       }
}
```

Application whitelisting

Bypasses



- A lot of research already done in this area
- Bypass with Office ❤ VBA
- No DLL whitelisting…
- Let's focus on Workspace Control
  - Its applications are whitelisted by default

There are currently three different lists.

- LOLBins
- LOLLibs
- LOLScripts

The goal of these lists are to document every binary, script and library that can be used for Living Off The Land techniques.

https://github.com/api0cradle/LOLBAS

Application whitelisting

PowerGrid (pwrgrid.exe)

- A lot of applications are invoked via PowerGrid
- Large number of command line options
- Must have messed up somewhere, right?

```
internal static void cu(string a)
{
  try
  {
    if (!FileOperations.e(a, false))
      return;
    XmlDocument xmlDocument = sharedXMLHelper.u(a);
    if (xmlDocument != null)
    {
      sharedRegistryProcessing.e = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateMouseUserPrefs", false);
      sharedRegistryProcessing.f = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateKeyboardUserPrefs", false);
      sharedRegistryProcessing.g = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateKeyboardLayoutUserPrefs", false);
      sharedRegistryProcessing.h = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateLanguageBarUserPrefs", false);
      sharedRegistryProcessing.i = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateColorsUserPrefs", false);
      sharedRegistryProcessing.j = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateAccessibilityUserPrefs", false);
      sharedRegistryProcessing.m = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateCursorUserPrefs", false);
      sharedRegistryProcessing.n = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateAppearanceUserPrefs", false);
      sharedRegistryProcessing.k = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateDesktopUserPrefs", false);
      sharedRegistryProcessing.l = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateWindowMetricsUserPrefs", false);
      sharedRegistryProcessing.o = sharedXMLHelper.aj((XmlNode) xmlDocument.DocumentElement, "ActivateSoundUserPrefs", false);
      sharedRegistryProcessing.p = sharedXML
      sharedRegistryProcessing.q = sharedXML
      sharedRegistryProcessing.s = sharedXML
      modMain.k = sharedXMLHelper.aj((XmlNod
      sharedUserPreferences.cv();
    }
    FileOperations.k(a);
  }
```

```
string empty = string.Empty;
int num = a.IndexOf("/RWS ", StringComparison.InvariantCultureIgnoreCase) + 1;
if (num <= 0)
  return;
sharedUserPreferences.cu(a.Substring(num - 1).ba("/RWS ", "", StringComparison.Ordinal).Trim());
```

Application whitelisting

PowerGrid (pwrgrid.exe)

```
private static void cv()
{
  try
  {
    if (sharedPF8.cs("UpdatePerUserSystemParameters", "user32.dll"))
    {
      try
      {
        Win32Error b;
        ProcessHelper.b(new CreateProcessParameters("rundll32.exe user32.dll,UpdatePerUserSystemParameters 1,true"), out b);
      }
```

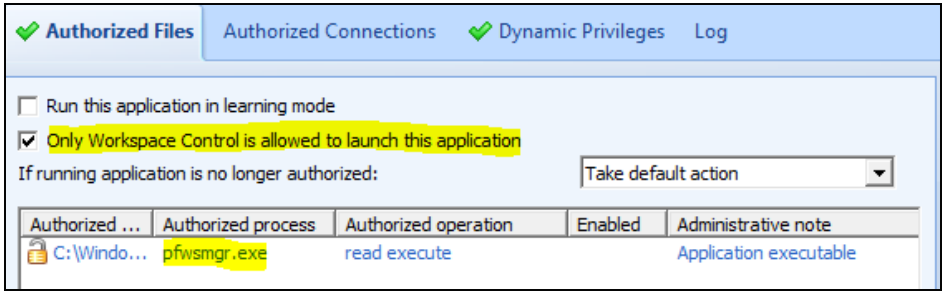
Time ...	Process Name	PID	Operation	Path
3:10:1...	pwrgrid.exe	6476	CreateFile	C:\Program Files (x86)\Ivanti\Workspace Control\rundll32.exe
3:10:1...	pwrgrid.exe	6476	CreateFile	C:\Users\John\Desktop\rundll32.exe
3:10:1...	pwrgrid.exe	6476	CreateFile	C:\Windows\SysWOW64\rundll32.exe

```
%RESPFDIR%\pwrgrid.exe /RWS <any xml file>
```

Mitigate

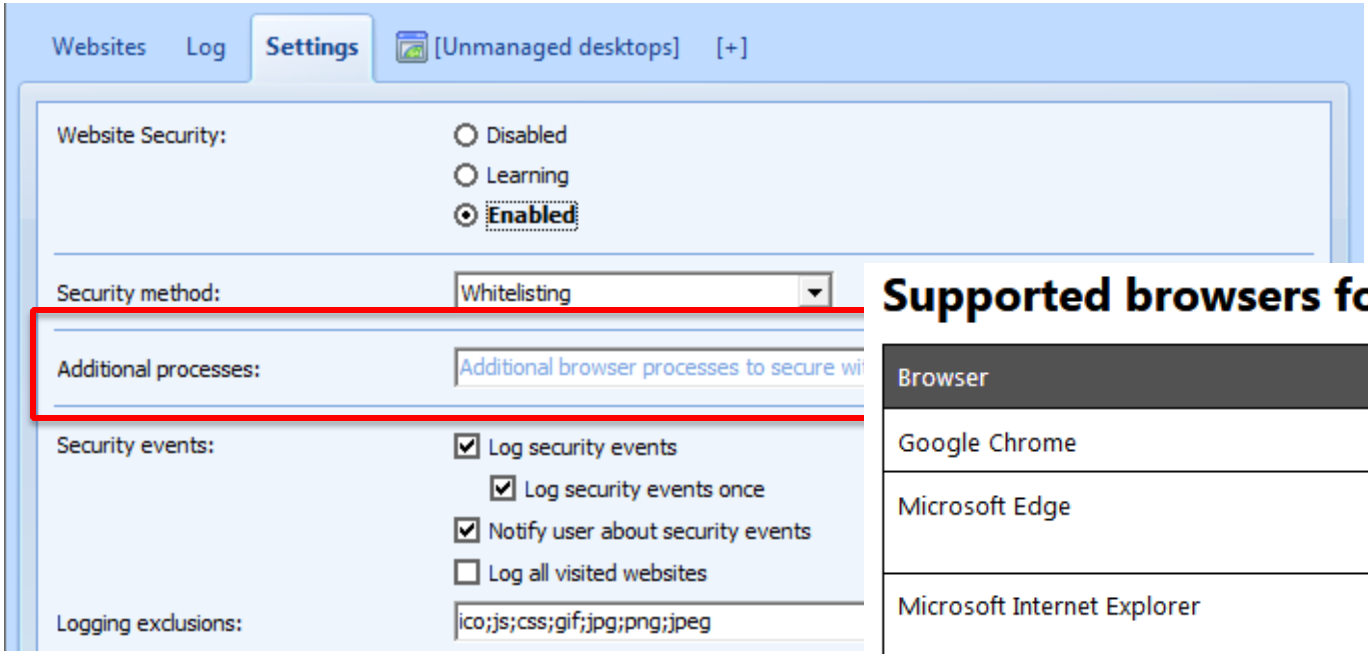
Application whitelisting

- Use application whitelisting!
- Accept that it won't be perfect
- Avoid certificate-based if you have strict path-based rules
- No blacklisting for path-based rules
  - Always add authorized process, don't wildcard
  - Only allow Workspace Control to launch application



Website Security

Blacklisting & whitelisting



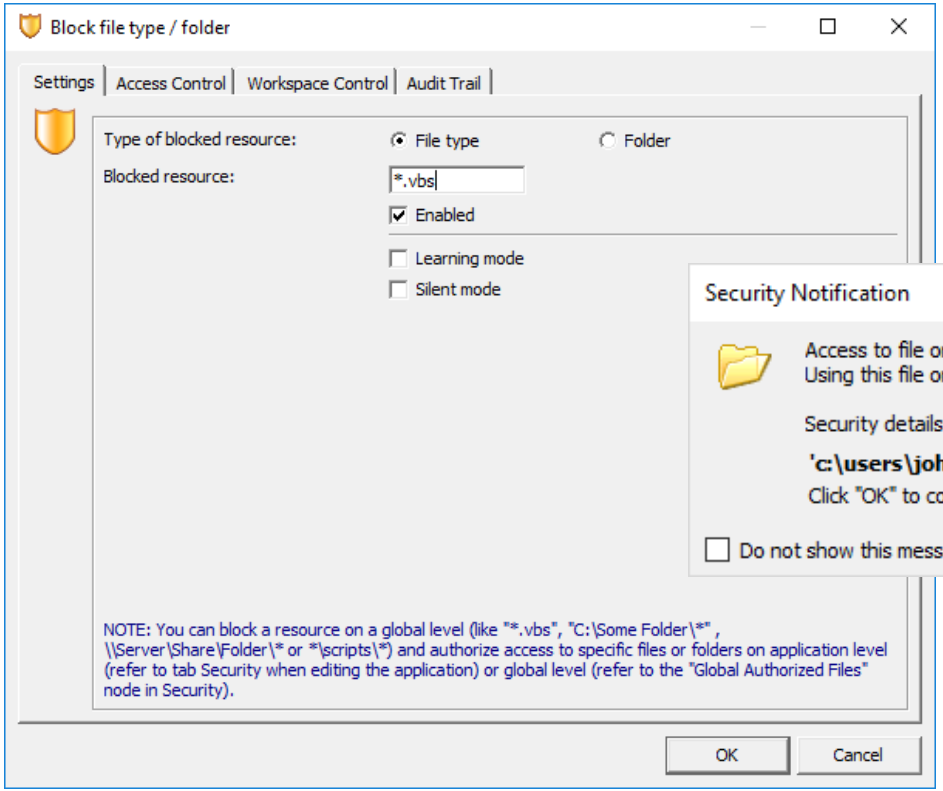
https://help.ivanti.com/res/help/en_US/iwc/10.2/CompMatrix/Browsers.htm

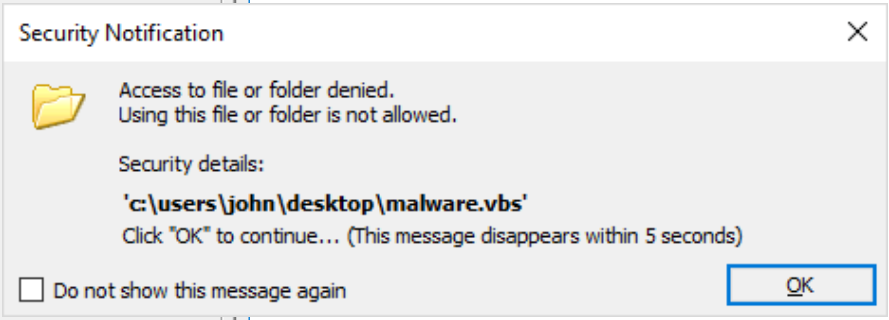
Supported browsers for Website Security

Browser	Version
Google Chrome	39 or higher
Microsoft Edge	Present in supported Microsoft Windows versions
Microsoft Internet Explorer	11
	10
	9
Mozilla Firefox	38 or higher
Opera	29 or higher

Data Security

Files (blacklist create)

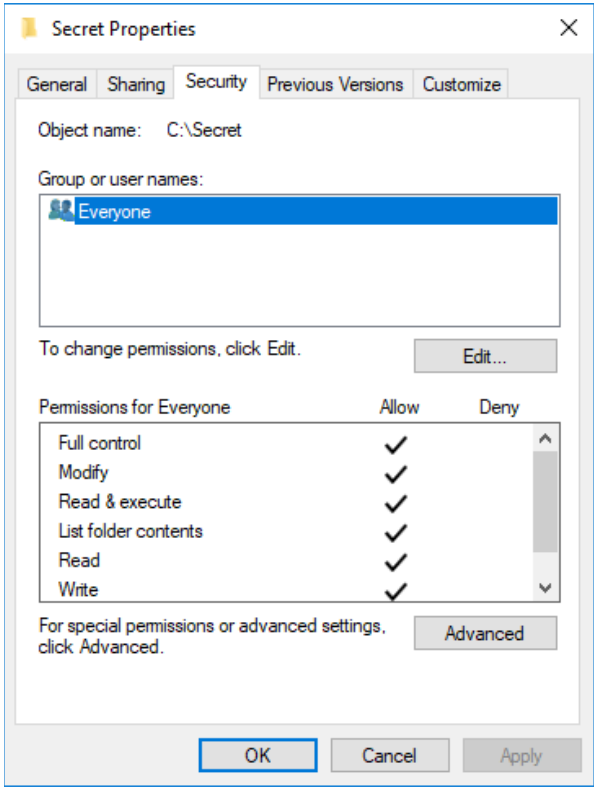


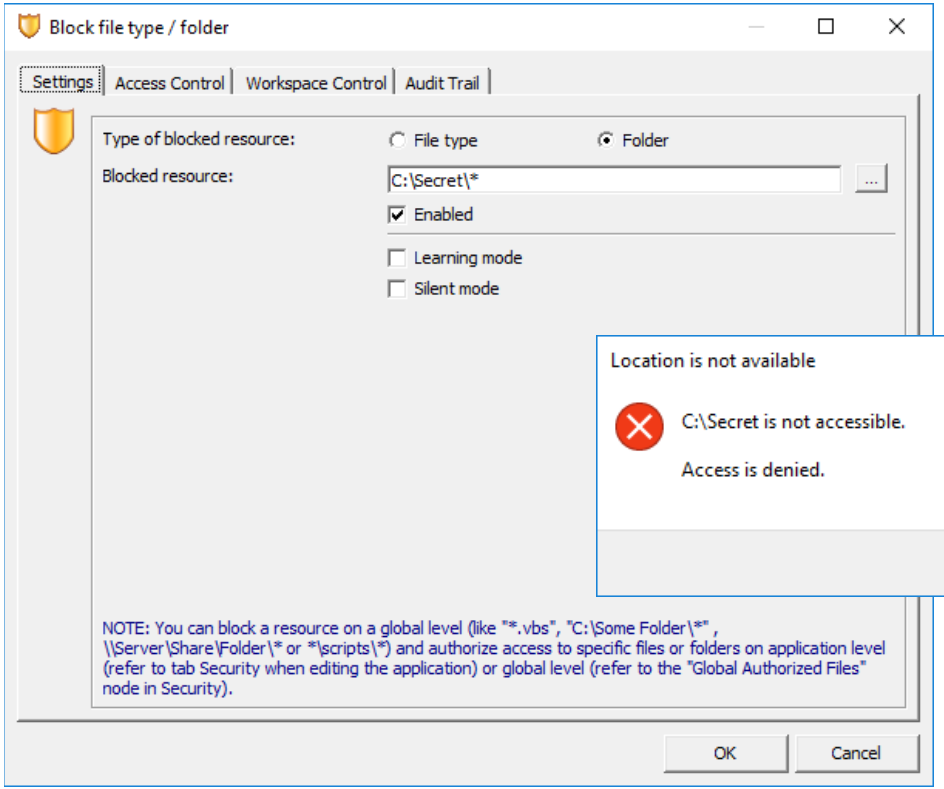


prevents creating files, not reading if the file is already there

Data Security

Folders (blacklist)

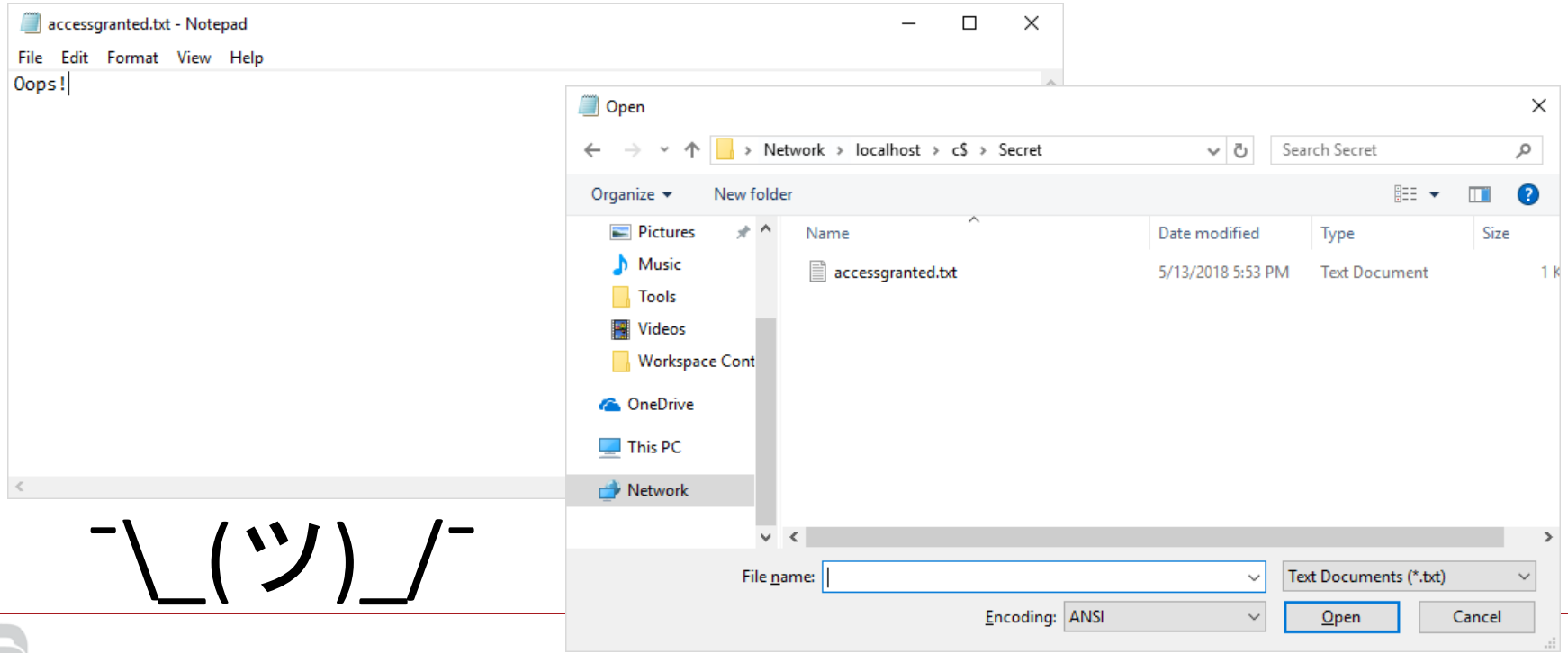




Data Security

Folders (blacklist)

```
notepad \\localhost\c$\Secret\accessgranted.txt
```



¯_(ツ)_/¯

Data Security

Read-only Blanketing

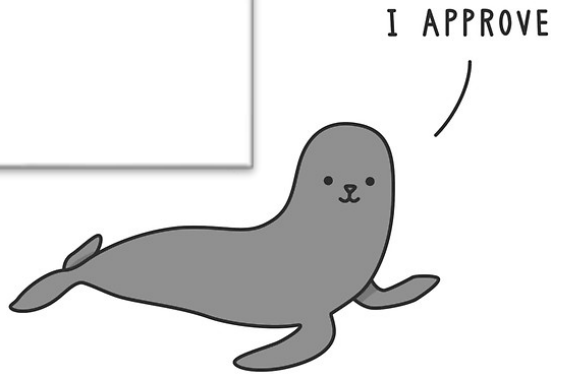
Read-Only Blanketing allows you to prevent users from:

- Saving data on local drives. If Read-Only Blanketing is enabled, data can only be saved on network drives.
- Accidentally overwriting or deleting system files and other important files on their desktops.

The following folders are automatically excluded from Read-Only Blanketing:

- The Recycle Bin on each local drive
- %userprofile%, %allusersprofile%
- Tmp and temp locations
- Spool in system32 folder
- Debug\usermode in system32 folder
- The server console

https://help.res.com/workspaceadminguide10/43770.htm



Don’t forget to set proper NTFS permissions though

Mitigate

Data Security

- Use Data Security to stop opportunistic attackers (again not perfect)
- NTFS permissions should be 1st line of defense
- Regularly audit your permissions
- Enable Read-only Blanketing if possible

- Upgrade to Ivanti Workspace Control 10.3.10.0 or later

Conclusion

In conclusion

All Ivanti is a secure Workspace

- Workspace Control provides number of features to harden the desktop
- Don’t trust on security features of Workspace Control alone, use Windows security
- When configured insecurely it will decrease security
- Regularly audit your configuration
- Don’t forget to upgrade

ivanti RES

BSIDES Delft

Questions