SERVER AUTO DEFAULT PLAN CONTENTS

The table below lists the default applications included in the Morphisec UTP 5.6 Server Auto Default Plan. To learn more about how to configure and customize protection plans, see *Morphisec Unified Threat Prevention Security Center Administration Guide*.

IMPORTANT NOTES:

- We document changes to the Client and Server Auto Default Protection Plans in our Release Notes (What's New) documents, as changes occur. **No changes are automatically applied to your Protection Plan**, so as not to interfere with your operational guidelines and organizational architecture standards. This ensures that required testing is not bypassed, and that no changes are applied to your client or server endpoints without your explicit consent.

  Thus, features that were used in Beta, and then move to production, retain the settings that you applied in the beta phase. Features that are new, and are deployed directly to production, will assume the default settings, as described in the Advanced Attributes table.

  For more information, contact support@morphisec.com.

- The Server Auto Default Protection Plan was modified to turn UAC Bypass mitigation **off** in Morphisec version 5.2. If you are upgrading from a version older than 5.2, it is recommended that you manually turn this feature off.
- **C:\users** and **c:\temp** are *not* automatically included in the Server Auto Default Plans. We recommend manually adding the **c:\users** and **c:\temp** folders to your Server Auto Default Plan, to protect user-specific applications and file sharing applications such as Dropbox or Google Drive.

Application	Description
*.scr	Prevents scr executables using evasive in-memory evasive attack techniques.
acrord32.exe	Protects Acrobat Reader from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.
AutoIt3.exe	AutoIt v3 is a scripting language designed for automating and simulating keystrokes, mouse movement and window/control manipulation. AutoIt3.exe launches the AutoIt v3 program. This control prevents abuse of Autoitv3 from evasive in-memory attacks.

Application	Description
C:\Users\*\AppData	Protects the Application Data folder in your user folder (usually hidden) including Documents, Music, and other library folders from exploitation by in-memory evasive malware or techniques.
C:\ProgramData\*	Protects any programs launched from C:\ProgramData from exploitation by in-memory evasive malware or techniques.
chrome.exe	Protects Chrome from being used as a platform to deliver fileless malware and protects in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.
ciscowebexstart.exe	Protects the collaboration software, WebEx, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.
CMstp.exe	The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections. This control prevents exploitation of the application using in-memory evasive techniques.
Csc.exe	Prevents uncompiled malicious code from compiling itself using C# compiler and extends protection to newly complied artifacts.
cscript.exe	Protects against evasive VBS attacks.
EQNEDT32.exe	Protects against various equation editor vulnerabilities (ex: CVE-2017-11882).
excel.exe	Protects Excel from being used as a platform to deliver fileless malware and protects in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.
firefox.exe	Protects Firefox from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.

Application	Description
FortiClient.exe	Protects FortiClient from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.
g2mstart.exe	Protects the collaboration application, GotoMeeting, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.
gotomeeting.exe	Protects the collaboration software, GotoMeeting, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.
httpd.exe	Protects this components of the Apache HTTP server from being used to deliver fileless attacks, and avoids exploitation of vulnerabilities for in-memory evasion.
iexplore.exe	Protects Internet Explorer from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.
InstallUtil.exe	InstallUtil.exe can be misused by whitelisting bypass techniques. Morphisec protects against in-memory evasive attacks leveraging those techniques.
KeePass.exe	Protects the open-source password manager from being used to deliver fileless attacks, and avoids exploitation of vulnerabilities for in-memory evasion.
MSACCESS.exe	Protects MSACCESS Database engine from in-memory evasive attacks.
msedge.exe	Protects Microsoft Edge from being used as a platform to deliver fileless malware and prevents vulnerabilities from being exploited by in-memory evasive malware or techniques.
mshta.exe	Mshta.exe is a utility that executes Microsoft HTML Applications (HTA). HTA files have the file extension .hta. HTAs are standalone applications that execute using the same models and technologies of Internet Explorer outside of the browser. This control prevents exploitation of MSHTA.exe from evasive in-memory attack techniques.

Application	Description
nginx.exe	Protects the nginx web/proxy server from being used to deliver fileless attacks, and avoids exploitation of vulnerabilities for in-memory evasion.
Node.exe	Protects Node from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.
osqueryd.exe	Protects the osqueryd daemon from being used to deliver fileless attacks, and avoids exploitation of vulnerabilities for in-memory evasion.
outlook.exe	Protects Outlook from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by in-memory evasive malware or techniques.
powerpnt.exe	Protects PowerPoint from being exploited by in-memory evasive attacks.
powershell.exe	PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. This control protects abuse of Powershell from in-memory evasive attacks.
RegAsm.exe	RegAsm.exe (Assembly Registration Tool) - The Assembly Registration tool reads the metadata within an assembly and adds the necessary entries to the registry, which allows COM clients to create .NET Framework classes transparently. Once a class is registered, any COM client can use it as though the class were a COM class. Adversaries can use RegAsm to proxy execution of code through a trusted Windows utility; it is also utilized in whitelisting bypass attacks. RegAsm can bypass process whitelisting through use of attributes within the binary to specify code that should be run before registration or unregistration.
regsvr32.exe	Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs) on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries. Regsvr32.exe can also be used to specifically bypass process whitelisting. This control protects regsvr32 from being exploited by in-memory evasive attacks.

Application	Description
rundll32.exe	The rundll32.exe program can be called to execute an arbitrary binary. Adversaries can use rundll32 as part of "living off the land" techniques for evading security tools which do not monitor the rundll32 program.
sihost.exe	Protects against the Microsoft CTF Vulnerability CVE-2019-1162.
skype.exe	Protects the collaboration software, Skype, from being exploited by in-memory evasive attacks.
skypeApp.exe	Protects the collaboration application, Skype, from being exploited by in-memory evasive attacks.
slack.exe	Protects the collaboration software, Slack, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.
taskeng.exe	Propagation of our protection to any executed task - protection against persistent evasive attacks and effective against supply chain attacks.
teams.exe	Protects the collaboration software, Microsoft Teams, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.
teamviewer.exe	Protects TeamViewer from being exploited by in-memory evasive attacks.
vlc.exe	Protects against in-memory evasive attacks that target malicious videos that may exploit VLC Media Player.
w3wp.exe (Cloud and SaaS Deployment Only)	Protects Microsoft Exchange and Sharepoint servers from in-memory, evasive attacks or techniques.
webex.exe	Protects the collaboration software, WebEx, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.

Application	Description
webexmta.exe	Protects the collaboration application, WebEx, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.
WinRAR.exe	Propagates Morphisec protection against in-memory evasive attacks to any possible archived artifact (scripts or executables).
winword.exe	Protects Word from being used as a platform to deliver fileless malware and prevents vulnerabilities from being exploited by in-memory evasive malware or techniques.
wscript.exe	Protects against evasive VBS attacks.
zoom.exe	Protects the collaboration software, Zoom, from being used as a platform to deliver fileless malware and prevents in-memory vulnerabilities from being exploited by evasive techniques.

Advanced Attributes in Protection Plans

The Advanced attributes section of Protection Plan settings includes new protection mechanisms, and features which extend protection coverage. For more details about these features, see the *Morphisec UTP User Guide*.

NOTE: Altering the application list and Advanced attributes of the Server Auto Default Protection Plan, causes the updated values to become the new default for future Server Auto Default plans.

Feature	Default Setting
UAC Bypass Mitigation	Off
Credential Theft	On
Script Execution Alerts	On
Protect Network Drives/Folders	On

Feature	Default Setting
Protect System Processes	On
Minidump	Off
Extended Forensics	On
Enable Running Processes	On
Remotely Launched Processes	On
PrintNightMare Patch	On
Shadow Copy Mitigation	On
SAM Hashes Protection (Beta)	On
VB Script Blocking Notifications	On
For Windows 7 – Restricted Zones Protection	On