websense

Web and Data Endpoint clients Webinar 2: Diagnostics and Troubleshooting

Websense Support Webinar
October, 2013

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense TRITON

Presenter

Greg Didier

- Title:
  - Technical Trainer eSupport
- Accomplishments:
  - 10 years supporting Websense products
- Qualifications:
  - Technical Support mentor
  - Product trainer
  - Knowledge base writer

Objectives

- Demonstrate Hybrid Web and Data Endpoint diagnostic resources
  - Diagnostic tools
  - Debug logs
  - Configuration files
  - Health status
  - Clientinfo.exe
  - Wireshark
- Topics
  - Connectivity
  - Upgrading Endpoints
  - Best practice tips

Endpoint Clients

- Hybrid Web Endpoint
- Data Endpoint
- Web Endpoint (Cloud Web Security)
  - Similar to hybrid Web Endpoint
  - See prior Webinars: November 2012, December 2012, January 2013
- Remote Filtering Client Endpoint
  - See prior Webinar: April 2012

Upgrading Endpoints

- For upgrade path and system requirements:
  - Deployment and Installation Center
  - Release Notes for incremental Endpoint releases/builds
- Mac Endpoint clients
  - Users are prompted to re-login
- Data Endpoint
  - Disable all endpoint discovery and fingerprinting tasks
    - Your incident reports should stop displaying new endpoint discovery incidents
- Rules of thumb
  - Restart Endpoint client after installation
    - Exception-- Data Endpoint in discovery mode
  - Whenever possible, keep versions of combined Endpoints the same
- For install or upgrade issues, enable Windows installer logging
  - Disable this registry edit when complete

Hybrid Web Endpoint

- A component of Websense Web Security Gateway Anywhere

Websense® Web Security Gateway Anywhere

DATASHEET

Comprehensive real-time protection against the latest advanced threats.

Your business and its data are under constant attack. Traditional anti-virus and firewall solutions no longer provide sufficient protection. In fact, they can put you at risk for data loss and litigation. Protecting your network and data against advanced threats, spear-phishing and exploit kits is crucial. Websense® Web Security Gateway Anywhere protects on-site and remote employees from the latest threats in a unified hybrid solution.

Why is Websense the best choice?

Web Security Gateway Anywhere integrates advanced threat defenses, threat monitoring dashboard and forensic reporting with data capture

PROTECTIONS
WEB ☑ EMAIL ☐ DATA ☐

PLATFORMS
SOFTWARE ☐ APPLIANCE ☐ CLOUD ☐ HYBRID ☑

Advanced Defenses

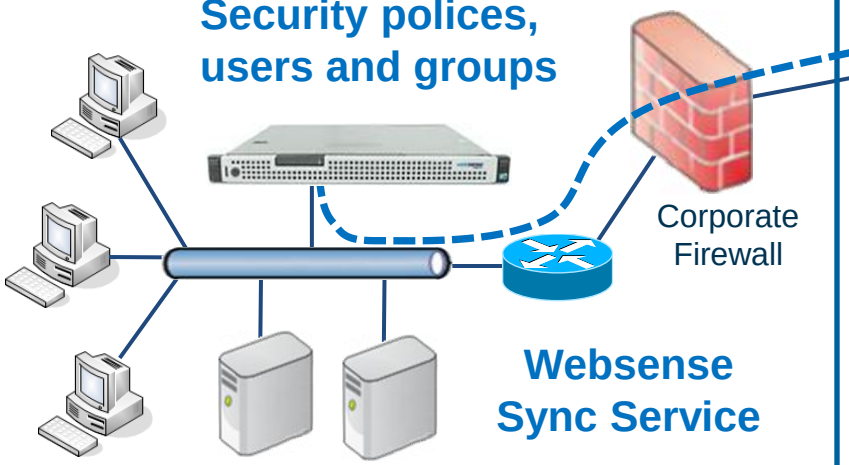
- ACE real-time inline defenses for on-site and remote users
- TruWeb DLP with data theft defenses for data containment
- Advanced threat dashboard with forensic reporting details
- Optional ThreatScope malware analysis sandbox service

Improved Protection

- Reduce malware incidents and risks of data theft and damage to reputation

Hybrid Web Endpoint Communications

http://pac.hybrid-web.global.blackspider.com:8082/proxy.pac?p=8h6hxmgf



V-Series Appliance-Based Deployment
Websense Web Security Gateway Anywhere

Internet

Hybrid
Service

Pac file URL request
Ports: 8082 or 80

Proxy communications
Port: 8081

Endpoint **Clients**

Hybrid Web Endpoint

- Check synchronization health
  - Web Security > Status > Hybrid Service > 

  - Do not install Endpoint client if you have synchronization issues
  - http://<Data Endpoint Server>:55832/viewer
    - Displays communication errors between Sync Service and hybrid service for Policy, Users, Logs, Account, etc.
- Endpoint client connects to hybrid service and…
  - Locate your customer account using the unique WSCONTEXT string
  - Sends user names
- Wireshark transaction headers information
  - http://home.webdefence.global.blackspider.com/headers_decryption

Hybrid Web Endpoint

- Images for prior slide:

Communication Type	Date and Time
Most recent communication by Sync Service	2013-10-21 15:42:56
Directory information sent by Sync Service	✗ 2013-09-19 16:27:00
Reporting information received by Sync Service	✗ 2013-10-21 15:22:06
Reporting information sent to Log Server	✗ 2013-10-21 15:24:42
Policy information sent by Sync Service	✗ 2013-10-21 15:09:33
Account information sent by Sync Service	✗ 2013-10-21 15:11:16

	Date and Time
rvice	2013-10-21 15:42:56
ice	✓ 2013-09-19 16:27:00
Service	✓ 2013-10-21 15:22:06
er	✓ 2013-10-21 15:24:42
Policy information sent by Sync Service	✓ 2013-10-21 15:09:33
	✓ 2013-10-21 15:11:16

Deploy Web Endpoint Manually

Download the latest version of the Web Endpoint for manual deployment.

GPO script command: WSCONTEXT=9be558100548393d2e2596070b275a65

If you are using a Group Policy Object (GPO) script to deploy the endpoint, add this command to your script file. See Help for further details.

View Web Endpoint Files

Hybrid Web Endpoint

- Examine your PAC file
  - Standard PAC file URL for hybrid Web
    - http://pac.hybrid-web.global.blackspider.com/proxy.pac
  - Customer specific PAC file URL for hybrid Web
    - http://pac.hybrid-web.global.blackspider.com/proxy.pac?p=8h6hxmgf
  - **HWSConfig.xml** installer file for 'hybrid Web Endpoint'
    - http://hybrid-web.global.blackspider.com:8082/proxy.pac?cli=ep
  - **HWSConfig.xml** installer file for 'Web Endpoint' (Cloud Web Security)
    - http://webdefence.global.blackspider.com:8082/proxy.pac
- To re-request a new PAC file, close and then reopen the Web browser
- For hybrid Web Endpoint, ensure the PAC file URL in use matches the policy specific PAC file URL listed in the Web Security console
  - Unfiltered Destinations– sites that hybrid service users may access directly

Hybrid Web Endpoint

- Image for prior slide:

Proxy Auto-Configuration (PAC) File

Configure browsers on client machines to use one of the following URLs to retrieve hybrid proxy configuration details. By default, PAC file communication uses port 8082. If port 8082 is closed, use the alternate PAC file URL.

Default (port 8082):
http://pac.hybrid-web.global.blackspider.com:8082/proxy.pac?p=8h6hxmgf

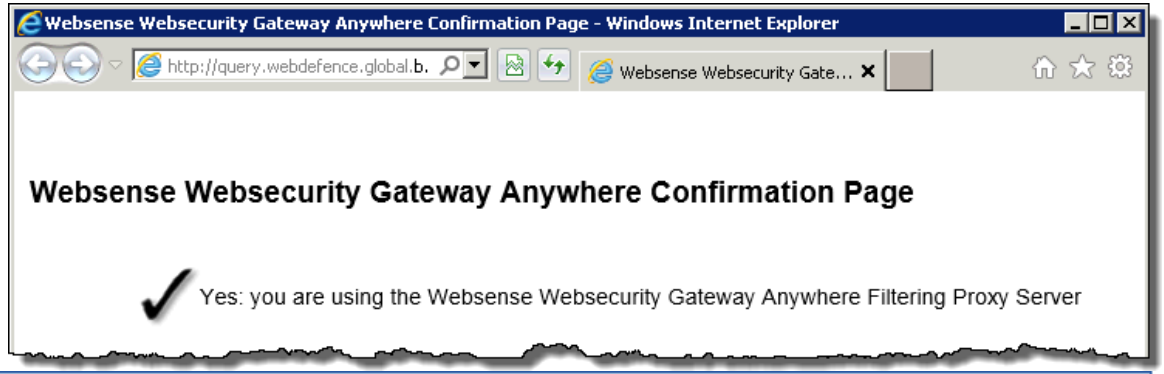
Alternate (port 80):
http://pac.hybrid-web.global.blackspider.com/proxy.pac?p=8h6hxmgf

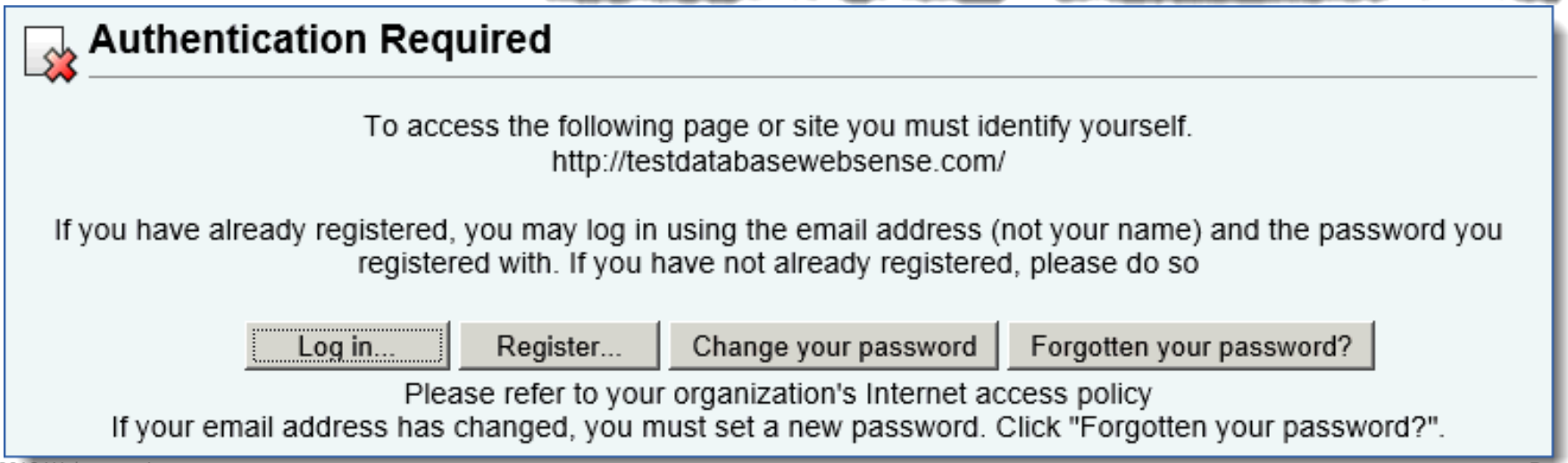
Hybrid Web Endpoint

- How do you know if Web Endpoint client is working?
  - Users should not be prompted for authentication
  - Endpoint client should provide user identification
  - Users on Endpoint machines should be logging into the network or logging in with cached credentials
  - Transparent identification is not supported when logging on locally
- Test URLs indicates if a user is going through Hosted service
  - http://query.webdefence.global.blackspider.com
  - http://query.webdefence.global.blackspider.com/?with=all
- **ClientInfo.exe**
  - C:\Program Files\Websense\Websense Endpoint
  - Collects and writes important diagnostic files to desktop
  - ClientInfo<hostname><date>.zip

Hybrid Web Endpoint

- Images for prior slide:





Hybrid Web Endpoint

- **DebugDump.txt**
  - Displays Web Endpoint event driven entries such as proxy service status and changes, PAC file status, profile changes, whitelist queries, etc.
  - C:\Program Files\Websense\Websense Endpoint
- Enabling verbose logging requires adding a registry key (CAUTION!)
  - **HKEY_LOCAL_MACHINE\SOFTWARE\Websense\Agent\Common**

KEY	TYPE	VALUE	DESCRIPTION
pxy_debug_mode	DWORD	1/0	1 writes more debug information

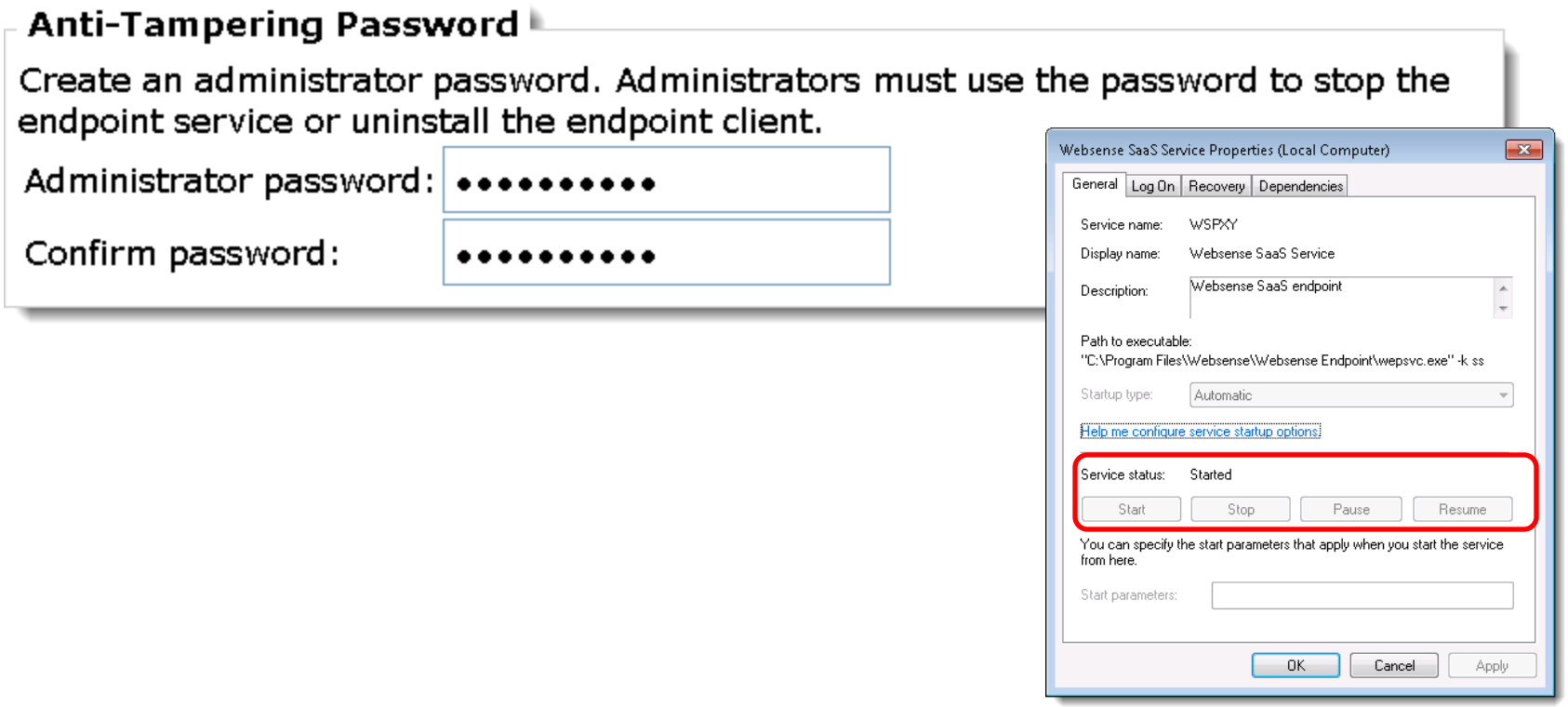
    - For Web Endpoints build version 1122 and later
  - You can add or modify the registry key even with anti-tampering enabled
  - To implement, restart Endpoint service or reboot the machine
  - To disable verbose logging, set value to zero or delete key and restart

Hybrid Web Endpoint

- Stop and start Web proxy service
  - `wepsvc -stop -password xxxx wspxy`
  - `wepsvc -start wspxy`
  - C:\Program Files\Websense\Websense Endpoint
- When troubleshooting, stop the Web proxy service (wspxy)
  - Avoid uninstalling Endpoint client
- Confirm current environment variables
  - `SET U > set.txt`
- Verify or update Group Policy information for machine or user
  - `GPRESLT /V > gp.txt`
  - `GPUpdate.exe /force`

Hybrid Web Endpoint

- Images for prior slide:



Hybrid Web Endpoint

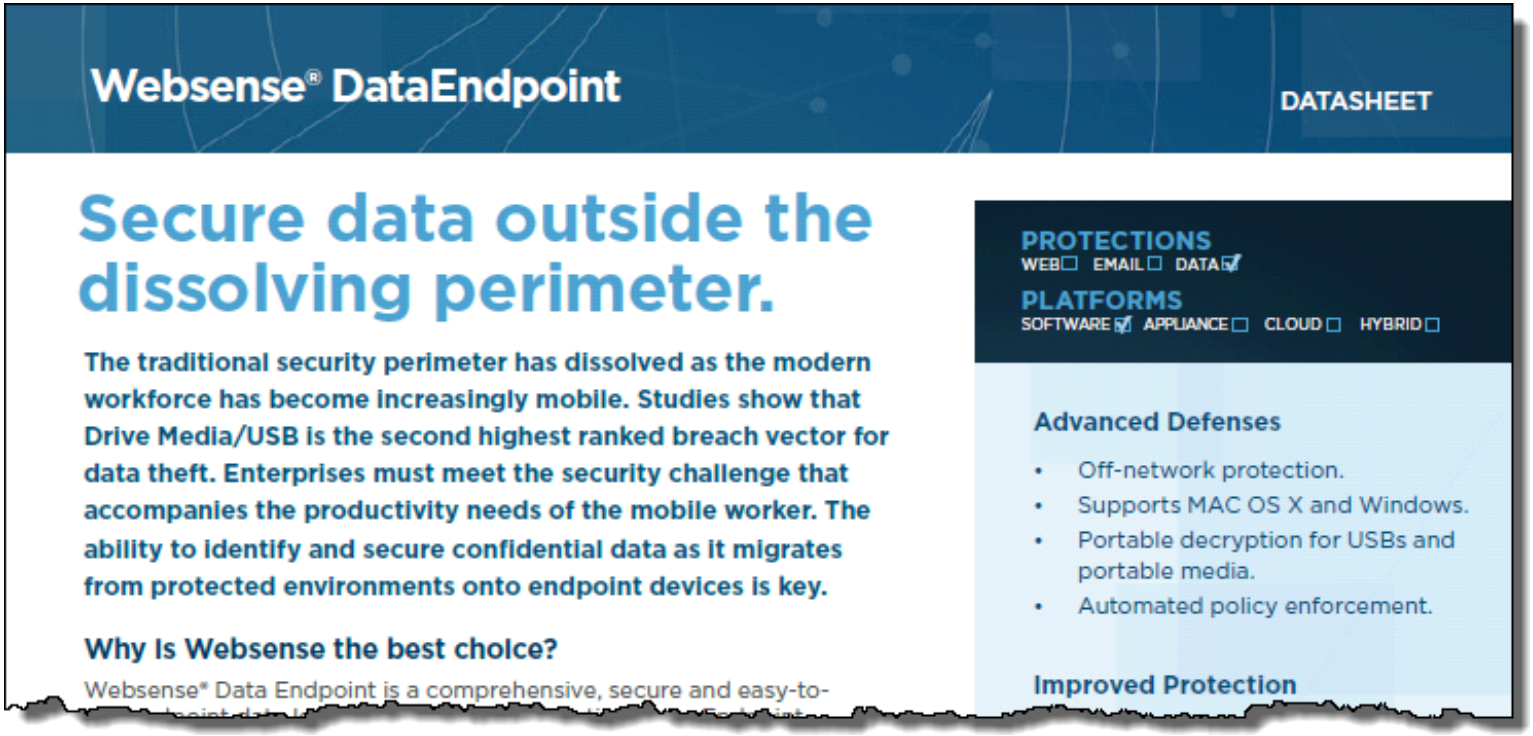
- Problematic applications
  - Symptoms: No or intermittent communications to external source, poor performance, application consuming abnormal resources
  - Do not enforce proxy settings on problematic application
    - Hybrid
      - Blocked file types settings are synchronized to hosted service
    - Cloud Web allows filtering applications by extensions
      - Select Settings > Bypass Settings > Endpoint Bypass
- Test on more than one machine, Web browser and OS type
- Installing Web Endpoint with MSI installer logging enabled
  - Add "`/lve C:\LogFile.txt`" to the installer string
  - `msiexec /package "<path>\Websense Endpoint.msi" /lve C:\LogFile.txt`
    - Writes LogFile.txt to the root of client machine

Demonstration

- Hybrid Web Endpoint
  - Lets look under the hood to find some helpful diagnostic and troubleshooting information.

Websense Data Endpoint

- A component of Websense Data Security Suite



Websense® DataEndpoint

DATASHEET

Secure data outside the dissolving perimeter.

The traditional security perimeter has dissolved as the modern workforce has become increasingly mobile. Studies show that Drive Media/USB is the second highest ranked breach vector for data theft. Enterprises must meet the security challenge that accompanies the productivity needs of the mobile worker. The ability to identify and secure confidential data as it migrates from protected environments onto endpoint devices is key.

Why Is Websense the best choice?

Websense® Data Endpoint is a comprehensive, secure and easy-to-

PROTECTIONS
WEB☐ EMAIL☐ DATA☑

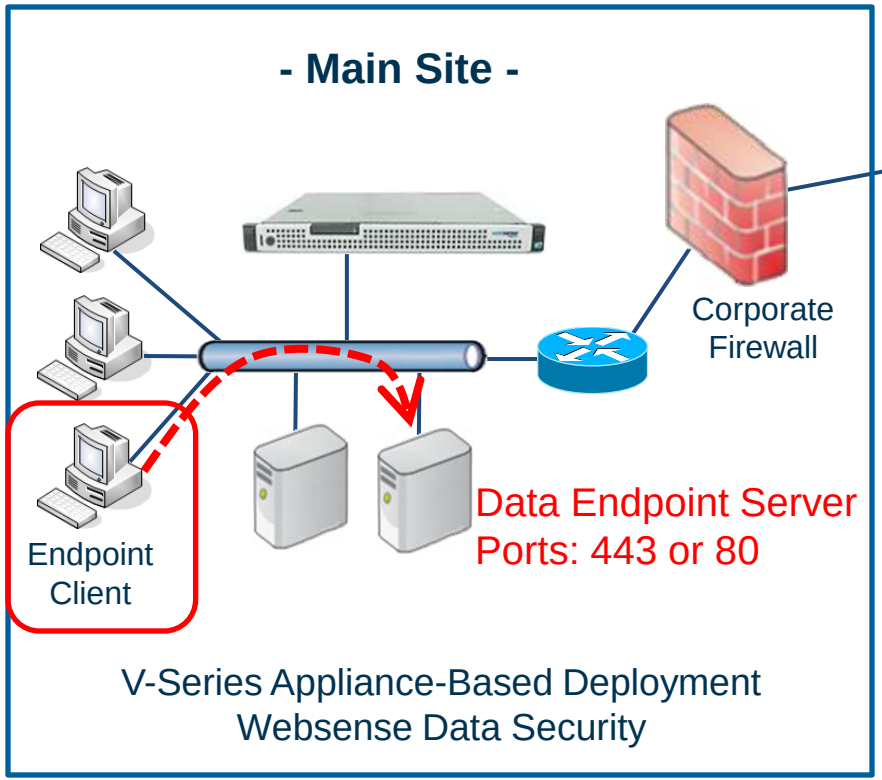
PLATFORMS
SOFTWARE☑ APPLIANCE☐ CLOUD☐ HYBRID☐

Advanced Defenses

- Off-network protection.
- Supports MAC OS X and Windows.
- Portable decryption for USBs and portable media.
- Automated policy enforcement.

Improved Protection

Data Endpoint Communications



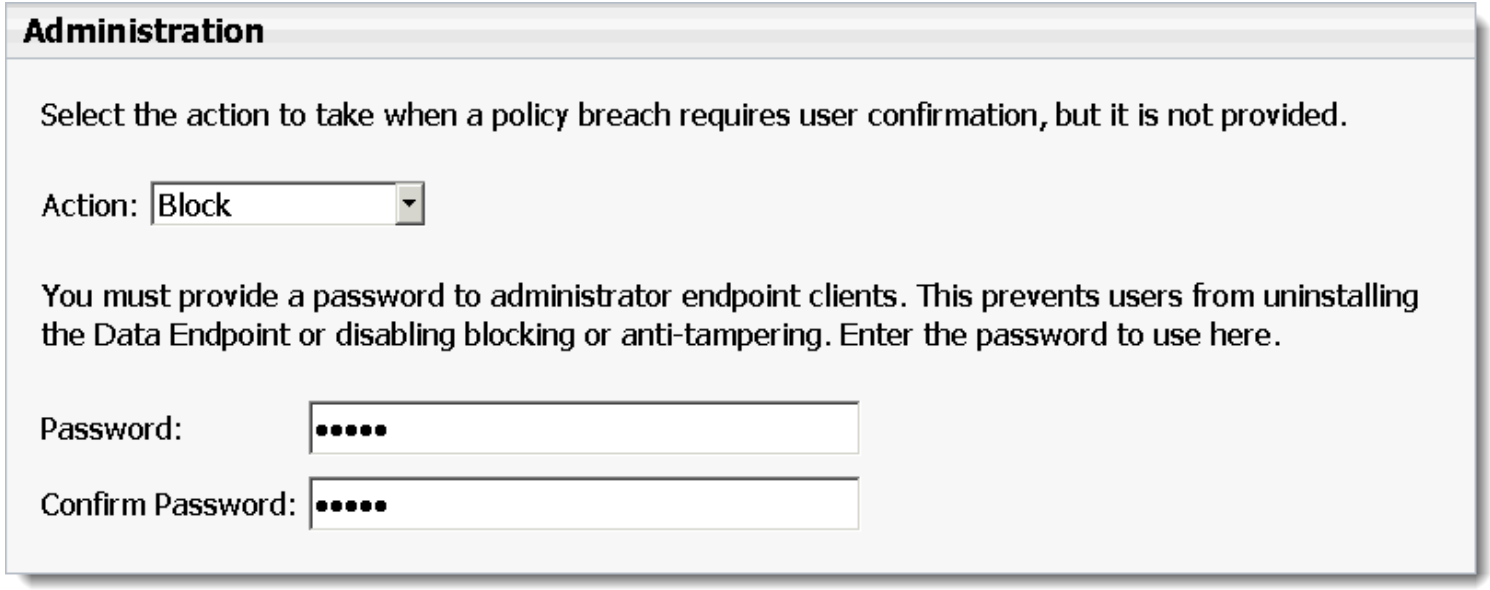
- Data Endpoint clients retain the last data security policy obtained while on-premise
- Data Endpoints check for updates every 60 minutes (default)
  - Not designed for emergency changes or updates

Data Endpoint Client

- **WDEUtil.exe**
  - Utility: Stops/starts Endpoint service and disables/enables anti-tampering, Super-Bypass and Blocking-Capabilities
    - If present, passphrase is required
  - Command line examples (run as administrator)
    - Stop Data Endpoint service (wsdlp)
      - `WDEUtil.exe -stop wsdlp -password <password>`
    - Start services
      - `WDEUtil.exe -start wsdlp`
    - Disable anti-tampering protection
      - `WDEUtil.exe -set DisableAntiTampering=true`
    - Enable anti-tampering protection
      - `WDEUtil.exe -set DisableAntiTampering=false`

Data Endpoint Client

- Image for prior slide:



Data Endpoint Client

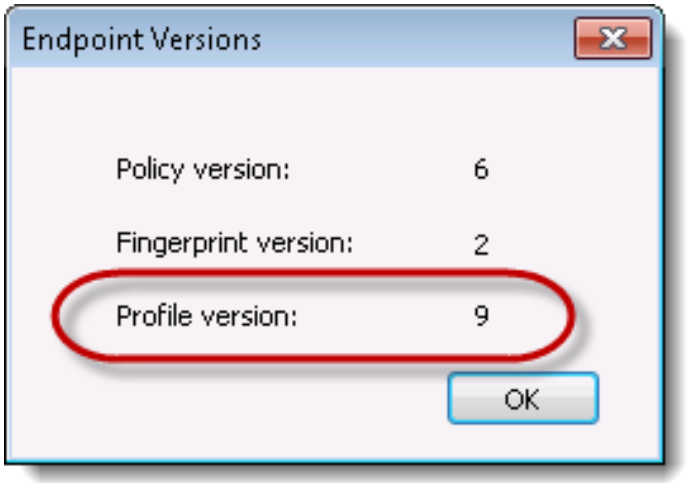
- What if an application and Data Endpoint do not play well together?
- To restore an application's functionality, unhook/exclude its process
  1. Query qipcap.dll to list currently hooked processes
     - `tasklist /FI "MODULES eq qipcap.dll"` (32-bit)
     - `tasklist /FI "MODULES eq qipcap64.dll"` (64-bit)
  2. Identify your currently excluded processes
     - `Select NAME,STR_VALUE from WS_ENDPNT_GLOB_CONFIG_PROPS where NAME = 'generalExcludedApplications'`
     - Execute your SQL queries against the **wbsn-data-security** database
  3. Add your EXE to the excluded executables displayed in the prior query
     - `update ws_endpnt_glob_config_props set str_value = 'gsmeta.exe,ginforsrv.exe,phped.exe,1new.exe,2new.exe,etc.exe' where name = 'generalExcludedApplications'`
     - Do not enter spaces between the comma separated EXE names

Data Endpoint Client

- To restore an application's functionality, unhook its process (CONTINUED)
  4. Invoke a Data Security profile change
     - A policy change does not push out excluded executables
  5. Verify Endpoint receives the update
     - The Endpoint profile version should increment/advance
     - Check the **<ExcludedApps>** xml container in the **dser_profile.xml** file
       - The container should include your excluded process
       - C:\Program Files\Websense\Websense Endpoint
  6. Processes remains hooked until the Endpoint machine restarts
     - Restarting Endpoint service (wsdlp) does not release the hooked process
  7. Confirm the process no longer appears in the task list
     - Query **qipcap.dll** again to display currently hooked processes

Data Endpoint Client

- Image for prior slide:



- **Excluded applications**
  - C:\Program Files\Websense\Websense Endpoint**dser_profile.xml**
  - The ‘ExcludedApps’ container lists all excluded applications

  - The image above lists the default excluded applications

Data Endpoint Client

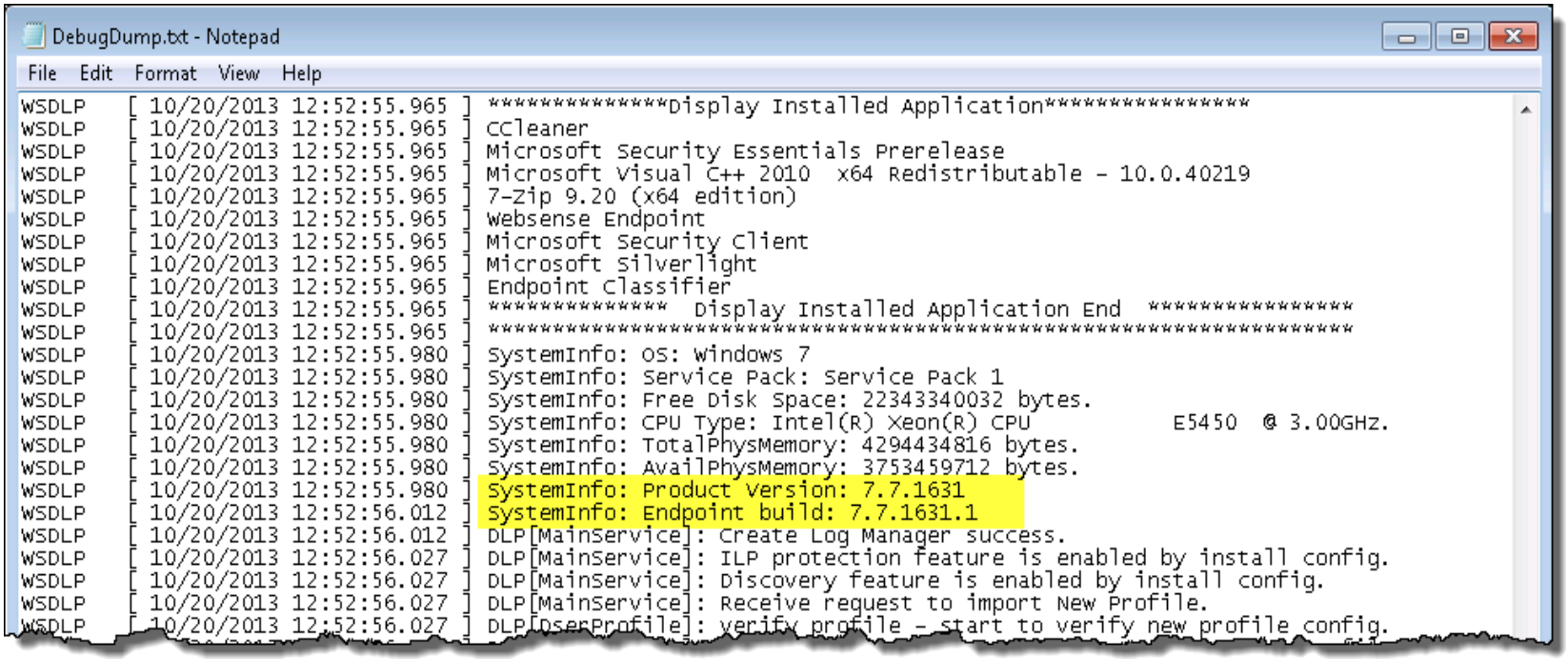
- Logging: Disable anti-tampering and change priority value to "debug"
  - **EndPointClassifier.log**
    - Provides analysis information, Data Security manager communications, fingerprint entries, configuration topics, transaction details, etc.
    - C:\Program Files\Websense\Websense Endpoint\logs
    - To enable logging, modify the log configuration file:
      - C:\Program Files\Websense\Websense Endpoint\conf**EndPointClassifier.log.config**
  - **EndPointAdapter.log**
    - Contains transaction filters, incoming transaction details, Endpoint adapter operations, configuration\system status messages
    - C:\Program Files\Websense\Websense Endpoint\logs
    - To enable logging, modify the log configuration file:
      - C:\Program Files\Websense\Websense Endpoint\conf**EndPointAdapter.log.config**

Data Endpoint Client

- **DebugDump.txt**
  - General log file—lists installed applications, machine hardware statistics, logged user, Endpoint version, data protection events, operating system hooking, etc.
  - C:\Program Files\Websense\Websense Endpoint**DebugDump.txt**
  - No verbose logging mode available for Data Endpoint
- **localConfig.xml**
  - Identifies the Data Security Web Servers supplying configuration settings
  - C:\Program Files\Websense\Websense Endpoint**localConfig.xml**
- **ClientInfo.exe**
  - Collects and writes important diagnostic files to desktop
    - **ClientInfo<hostname><date>.zip**

Data Endpoint Client

- Image for prior slide:

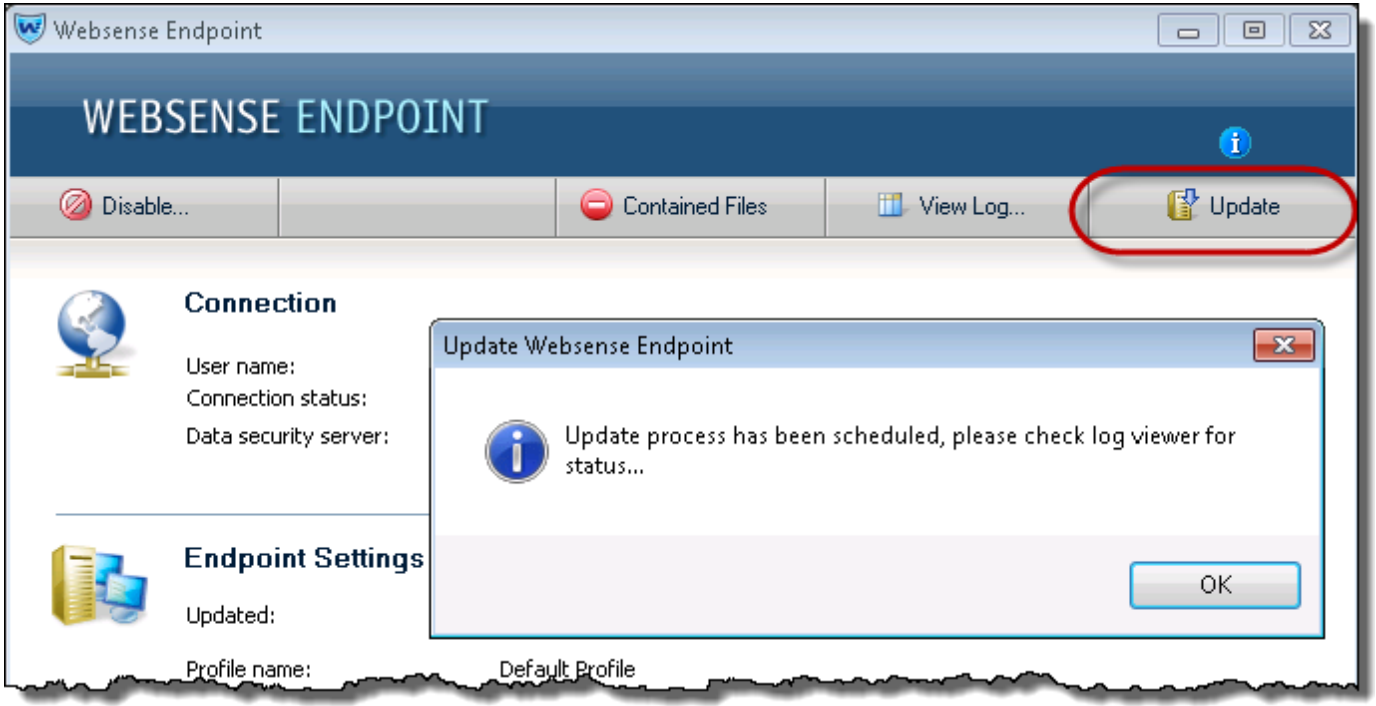


Data Endpoint Client

- Data Endpoint clients do not immediately receive new policy updates
  - Endpoints download policy and profile changes in pre-defined time intervals
- To force a new policy or profile update
  - Click the Endpoint user interface "Update" button (if available)
  - `wepsvc -update wsdlp` (from command line, run as administrator)
  - Restart Endpoint service
  - Reboot Endpoint machine
- Identifying between driver or policy issues
  - `wdeutil -set DisableAntiTampering=true -password [password]`
    - Policies still apply—if issue disappears then a driver issue exists
  - `wdeutil -set EnableSuperBypass=false -password [password]`
    - Anti-tampering still applies—if issue disappears then a policy issue exists

Data Endpoint Client

- Image for prior slide:

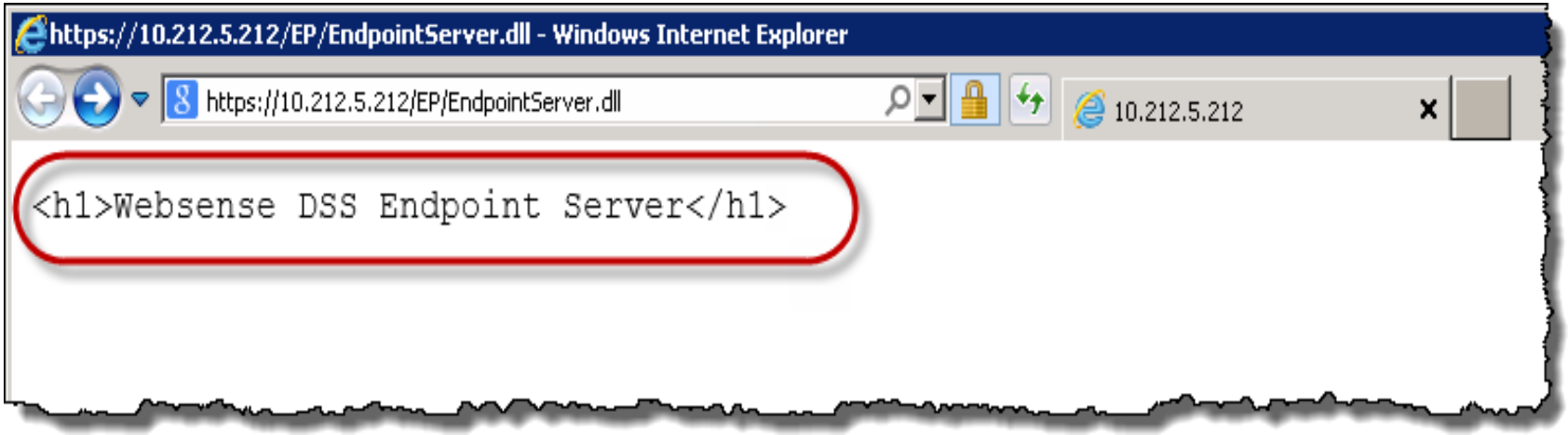


Data Endpoint Client

- Confirm Endpoint client can access the Data Endpoint Web server
  - https://<Endpoint Server name or IP>/EP/EndpointServer.dll
  - http://<Endpoint Server name or IP>/EP/EndpointServer.dll
  - URLs located in the **localConfig.xml** file (case sensitive)
- Installing Data Endpoint with MSI installer logging enabled
  - Installation package is an EXE with a nested MSI installer
  - Add "`/lve C:\LogFile.txt`" to the installer string
  - <path>\WebsenseEndpoint_64bit.exe /v"WSCONTEXT=xxxx /lve C:\LogFile.txt"
    - Writes LogFile.txt to root of client machine
- To report user names and display Endpoint shield on the client computer, enable Terminal Services and set it to Manual
- Disable auto updates

Data Endpoint Client

- Image for prior slide:



Data Endpoint Client

- Antivirus Interference
  - Exclude Data Endpoint processes prior to installation
  - When troubleshooting, disabling Antivirus drivers or services may not suffice, you should uninstall it completely
- Disk Encryption Troubleshooting
  - Ensure Data Endpoint installation path is not encrypted
    - If encrypted, test by decrypting it
    - If not encrypted, test by removing the encryption software
- Hardened operating system
  - May compromise access to services, directories, files, network resources, etc.
- Data Endpoint server responds slowly—too many open FIN_WAIT_2 states
  - Registry edit: Reduce the TCP fin_wait state time (**TCPFinWait2Delay**)
  - Install Data Endpoint server on it's own server

Demonstration

- Data Web Endpoint
  - Lets look under the hood to find some helpful diagnostic and troubleshooting information.

Additional Resources

- Web Endpoint
  - Proxy auto-configuration (PAC)
  - How do I query Cloud service for hidden connection information?
- Data Endpoint
  - Bypassing Endpoint clients
- Web and Data Endpoints
  - How to enable Windows Installer logging
  - Deployment and Installation Center

Webinar Announcement

Join us for our next webinar

“Troubleshooting and best practice tips for Hybrid Web Endpoint users”

November 20, 2013

8:30 A.M. PST (GMT -7)

To register:
www.websense.com/content/SupportWebinars.aspx

- Websense Training Partners offer classes online and onsite at your location.
- To find Websense classes offered by Authorized Training Partners in your area, visit:
  - www.websense.com/findaclass
- For more information, send emails to:
  - readiness@websense.com