

FortiSIEM - Windows Agent 3.1.2 Installation Guide

Version 5.2.6

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



10/31/2022

FortiSIEM 5.2.6 Windows Agent 3.1.2 Installation Guide

TABLE OF CONTENTS

Change Log	4
FortiSIEM Windows Agent	5
Prerequisites	5
Supported Operating Systems	5
Supported Languages	6
Hardware Requirements	6
Software Requirements	6
Communication Ports	6
Other Installation Considerations	6
Installing Windows Agent	7
Managing Windows Agent	9
Configuring Windows Servers for FortiSIEM Agents	9
Configuring Windows Sysmon	9
Configuring Windows DNS	10
Configuring Windows DHCP	10
Configuring Windows IIS	11
Configuring Windows Event Forwarding	12
Configuring Auditing Policies	21
Enabling FIPS	22
Verifying Events in FortiSIEM	22
Uninstalling Windows Agent	22
REST APIs used for Communication	23
Troubleshooting from Windows Agent	23
Sample Windows Agent Logs	23
System Logs	23
Application Logs	24
Security Logs	24
DNS Logs	25
DHCP Logs	26
IIS Logs	26
DFS Logs	27
File Content Monitoring Logs	27
File Integrity Monitoring Logs	28
Installed Software Logs	28
Registry Change Logs	28
WMI logs	29

Change Log

Date	Change Description
09-05-2018	Initial version of FortiSIEM - Windows Agent & Agent Manager Installation Guide
10-08-2018	Revision 2: updated "Hardware and Software Requirements" - supported Desktop OS versions.
03-22-2019	Revision 3: updated content for Windows Agent 3.1.
06-05-2019	Revision 4: updated Prerequisites with "Other Installation Considerations" section.
07-23-2019	Revision 5: added instructions to setup event forwarding and to configure source-initiated subscription.
08-12-2019	Revision 6: added instruction to specify DNS log name and path in "Configuring Windows DNS" section.
09-09-2019	Revision 7: updated to agent version 3.1.2.
10-17-2019	Revision 8: changes to Configuring Windows Servers. Organizational changes.
10-30-2019	Revision 9: added support for Windows Server 2019 and Windows Server 2019 Core.
11-25-2019	Revision 10: changed the name of the event from AO-WUA to AccelOps-WUA. Added instructions to create InstallSettings.xml in case a copy is not included with binary distribution.
03-30-2020	Revision 11: Added additional sample File Integrity Monitoring Logs. Changes to the steps in Installing Windows Agent. Changes to the steps in Configure Security Audit Logging Policy.
05-22-2020	Revision 12: Changed the location of DNS logs to C:\DNSLogs.log.
10-31-2022	Revision 13: Updated Other Installation Considerations section.

FortiSIEM Windows Agent

FortiSIEM Windows Agents provides a scalable way to collect logs and other audit violations from a large number of Windows servers.

This section describes how to install, setup, maintain and troubleshoot FortiSIEM Windows Agent 3.1.2.

- [Prerequisites](#)
- [Installing Windows Agent](#)
- [Managing Windows Agent](#)
- [Configuring Windows Servers for FortiSIEM Agents](#)
 - [Windows Sysmon](#)
 - [Windows DNS](#)
 - [Windows DHCP](#)
 - [Configuring Windows Event Forwarding](#)
 - [Configuring Locale on Windows Servers](#)
 - [Configuring Source-Initiated Subscription](#)
 - [Configuring Auditing Policies](#)
 - [Enabling FIPS](#)
- [Verifying Windows Events in FortiSIEM](#)
- [Uninstalling Windows Agent](#)
- [REST APIs used for Communication](#)
- [Troubleshooting from Windows Agent](#)
- [Sample Windows Agent Logs](#)

Prerequisites

Ensure that the following prerequisites are met before installing FortiSIEM Windows Agent:

- [Supported Operating Systems](#)
- [Supported Languages](#)
- [Hardware Requirements](#)
- [Software Requirements](#)
- [Communication Ports](#)
- [Other Installation Considerations](#)

Supported Operating Systems

FortiSIEM Windows Agent 3.1.2 runs on the following Operating Systems:

- [Windows 7 Enterprise/Professional](#)
- [Windows 8](#)
- [Windows 10](#)

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2019 Core

Supported Languages

All languages in which Windows Operating System is available are supported.

Hardware Requirements

Component	Requirement
CPU	x86 or x64 (or compatible) at 2 GHz or higher
Hard Disk Free space	10 GB (minimum)
Server Operating System	- Windows Server 2008 R2 and above (strongly recommended) - Desktop Operating System: Windows 7, 8, 10 and above
RAM	- For 32 bit OS: 2 GB for Windows 7, 8, 10 minimum - For 64 bit OS: 4 GB for Windows 7, 8, 10, Windows Server 2008 / 2012 minimum

Software Requirements

Component	Requirement	Notes
Installed Software	.NET Framework 4.5	.NET Framework 4.5 can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=30653 , and is already available on Windows 8 and Windows Server 2012

Communication Ports

FortiSIEM Windows Agent 3.1.2 communicates outbound via HTTPS with Supervisor and Collectors.

1. The Agent registers to the Supervisor and periodically receives monitoring template updates if any, via HTTP(S).
2. The Agent then forwards the events to the Collectors via HTTP(S).

Ensure that Firewalls, if any, between the Agents and Supervisor/Collector permit HTTP(S) traffic on port 443.

Other Installation Considerations

Beginning with Windows Agent release 3.0:

- Agents must upload event data to a Collector. Therefore, minimum architecture is one Super appliance and one Collector appliance.
- The Collector must be installed as IPv4 only. Dual stack IPv4/IPv6 or IPv6 Collectors are not supported with Agents.
- Enable TLS 1.2 for Windows Agent to communicate with FortiSIEM Super/Worker/Collector nodes. Without TLS 1.2 enabled, Windows Agent installation will fail. By default, SSL3 / TLS 1.0 is enabled in Windows 7, 8 and 2008-R2. Before proceeding with the Windows Agent installation, please enable TLS 1.2 (if not already enabled) as follows:
 - a. Start elevated Command Prompt (i.e., with administrative privilege)
 - b. Run the following commands sequentially as shown.

```
REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client" /v DisabledByDefault /t
REG_DWORD /d 00000000
```

Installing Windows Agent



Before installing FortiSIEM Agent on FortSIEM Nodes, you must do detailed performance testing since FortSIEM nodes consume significant CPU to process a high volume of events in real-time.

During installation, the Windows Agent will register with FortiSIEM Supervisor.

The required parameters are:

- **SUPER_IP**: IP Address or Host name/FQDN of Supervisor node
- **ORG_ID**: FortiSIEM Organization Id to which this Agent belongs
- **ORG_NAME**: FortiSIEM Organization Name
- **AGENT_USER**: Agent user name (for registration only)
- **AGENT_PASSWORD**: Agent password (for registration only)

The optional parameters are:

- **HOST_NAME**: This name will be displayed in FortiSIEM CMDB. If this is not specified, the agent will try to discover the host name

For Service Provider installations, the Agent user name and password is defined in the Organization. See [here](#) for details.

For Enterprise installations, Agent user name and password is defined in **CMDB > User** page. You must create a user and check **Agent Admin**. See [here](#) for details.

Follow the steps below to install FortiSIEM Windows Agent:

1. Log in to the Windows machine where Windows Agent will be installed.
2. Copy Windows Agent 3.1.2 binaries: `AoWinAgt-x64.msi` or `AoWinAgt-x86.msi` and `InstallSettings.xml` to the same folder.
3. Find the Organization ID, Organization Name and Agent registration credentials.
 - a. Log in to FortiSIEM in Super Global mode as Admin user.
 - b. Go to **ADMIN > Setup > Organizations** and locate the Organization (ID, Name) to which this Agent belongs. If not present, create an Organization.
 - c. Locate the Agent Registration User and Password for the Organization. If not present, define them.

4. If the `InstallSettings.xml` file was not included with your distribution, then create it:
 - a. Use your favorite text editor to create an XML file named `InstallSettings.xml` in the same folder where you copied the Windows Agent binaries. Use the following code as a template.
 - b. Provide the values for the Organization name (`ORG_NAME`) the Agent Registration User name (`AGENT_USER`) and Password (`AGENT_PASSWORD`) from step #3.

```

        <?xml version="1.0" encoding="utf-8"?>
    <InstallConfig Version="1">
        <Org>
            <ID>ORG_ID</ID>
            <Name>ORG_NAME</Name>
        </Org>
        <Super>
            <Name>SUPER_IP</Name>
            <Port>443</Port>
        </Super>

        <HostName>test.abcd.com</HostName>

        <Registration>
            <Username>ORG_NAME/AGENT_USER</Username>
            <Password>AGENT_PASSWORD</Password>
        </Registration>
        <Proxy>
            <Server></Server>
            <Port></Port>
        </Proxy>
        <SSLCertificate>ignore</SSLCertificate>
    </InstallConfig>

```

5. Install the Agent:
 - a. Log in to the Windows machine as Administrator.
 - b. Make sure that the MSI in step #2 and `InstallSettings.xml` in step #4, are in the same folder.
 - c. Double-click the MSI package and the installation process will start.
If any settings errors are detected, the install process will fail; else it will succeed. The Agent will register to the Supervisor and start running.
6. Check **CMDB** for successful registration:
 - a. Log in to FortiSIEM in Super Global mode as Admin user.
 - b. Go to **CMDB** and search for the Agent Host name.
 - c. Check the **Status** column.
7. Make sure the Templates and Host to Template association policies are defined for this Host:
 - a. Log in to FortiSIEM in Super Global mode.
 - b. Go to **ADMIN > Setup > Windows Agent** and make sure the templates and host to template associations are defined.
One of the host-to-template association policies must match this agent. The first matched policy will be selected.

Managing Windows Agent

Stopping Agent

1. Log in to the Windows machine where the Agent is installed.
2. Go to **Services > FortiSIEM Windows Agent**.
3. Stop FortiSIEM Windows Agent service.

Starting Agent

1. Log in to the Windows machine where the Agent is installed.
2. Go to **Services > FortiSIEM Windows Agent**.
3. Start FortiSIEM Windows Agent service.

Configuring Windows Servers for FortiSIEM Agents

- [Configuring Windows Sysmon](#)
- [Configuring Windows DNS](#)
- [Configuring Windows DHCP](#)
- [Configuring Windows IIS](#)
- [Configuring Event Forwarding](#)
- [Configuring Auditing Policies](#)
- [Enabling FIPS](#)

Configuring Windows Sysmon

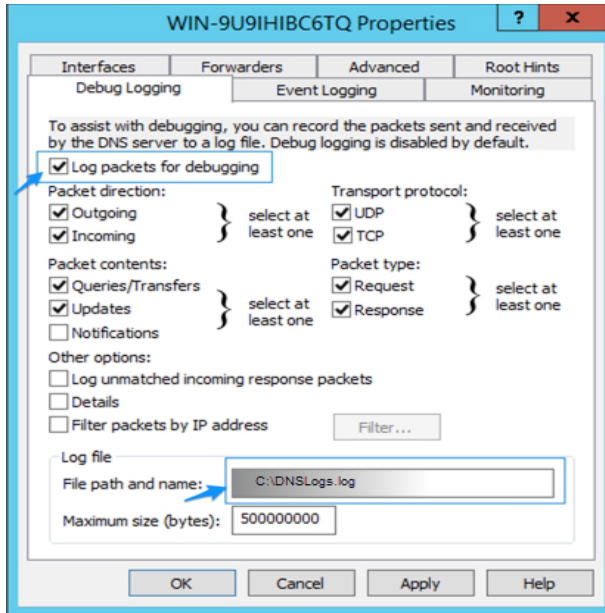
The supported Sysmon versions are 5.02 and above. The latest Sysmon download instructions are available [here](#).

1. Log in to the Windows machine.
2. Download the popular Sysmon configuration file and save it as <https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml>
3. Save the configuration file as `sysmonconfig.xml`
4. Check whether the Sysmon executable is installed or not by running: `Sysmon64.exe -c`
 - a. If Sysmon is running, update the Sysmon configuration by using the command with administrator rights:
`sysmon.exe -c sysmonconfig.xml`
 - b. If Sysmon is not available on the system, download and install using the command with administrator rights:
`sysmon.exe -accepteula -i sysmonconfig.xml`
5. Check the new configuration using the command: `Sysmon64.exe -c`
6. Check for Sysmon events:
 - a. Go to **EventViewer > Applications** and **Service Logs > Microsoft > Windows > Sysmon > Operational**.
 - b. Check for Sysmon logs on the right panel.
 - c. Right-click on **Operational** and choose **Properties**.
 - d. Note the **Full Name** (typically 'Microsoft-Windows-Sysmon/Operational') for FortiSIEM configuration.

Configuring Windows DNS

Follow the steps below to configure DNS server:

1. Log in to the Windows machine.
2. Configure DNS logging:
 - a. Launch **DNS Manager**.
 - b. Select the specific DNS Server and click **Properties**.
 - c. On **Debug Logging** tab, enable **Log packets for debugging**.
 - d. Specify the log file name and path, for example `C:\DNSLogs.log`.



3. Check for DNS logs. If logs are present, FortiSIEM Agent will automatically collect these logs.
 - a. Go to **EventViewer > Applications** and **Service Logs > DNS Server**.
 - b. Check for DNS logs on the right panel.

Configuring Windows DHCP

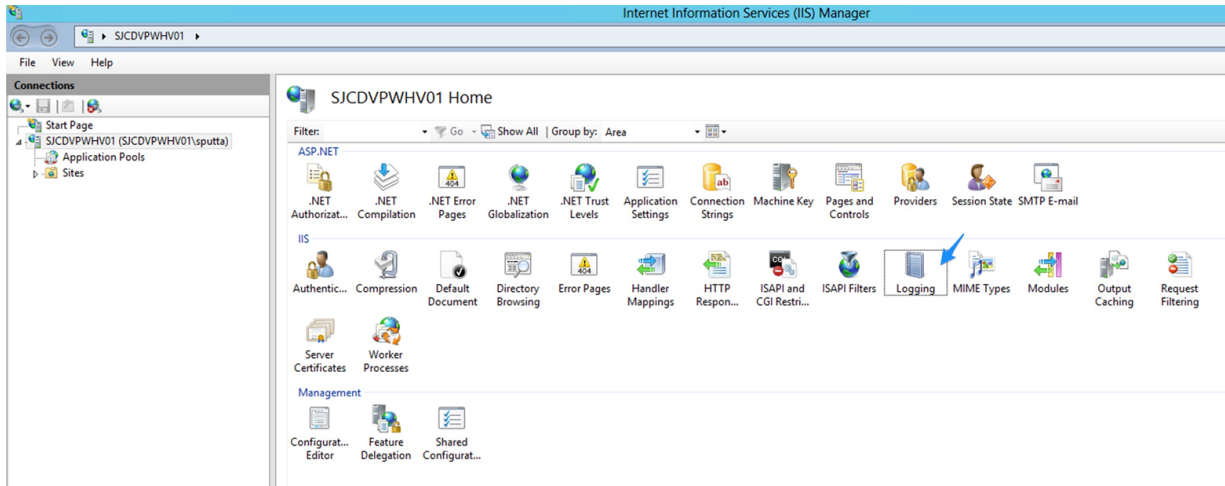
Follow the steps below to configure DHCP server:

1. Log in to the Windows machine.
2. Configure DHCP logging:
 - a. Launch **DHCP Manager**.
 - b. Select the specific DHCP Server and click **IPv4 > Properties**.
 - c. Enable **DHCP Audit Logging**.
3. Check for DHCP events. If logs are present, FortiSIEM Agent will automatically collect these logs:
 - a. Go to **EventViewer > Applications** and **Service Logs > Microsoft > Windows > DHCP Server**.
 - b. Check for DHCP logs on the right panel.

Configuring Windows IIS

Follow these steps to configure the IIS Server:

1. Log in to the Windows machine.
2. Configure IIS logging:
 - a. Launch **IIS Manager**.
 - From the **Start** menu, click **Programs** or **All Programs**, and point to **Administrative Tools**.
 - On **Administrative Tools**, Click **Internet Information Services (IIS) Manager**.
 - b. Select the specific **IIS Server** and click the **Logging** icon on the panel on the right side.



- c. Specify the log path if default path (%SystemDrive%\inetpub\logs\LogFiles) does not exist.

The screenshot shows the 'Logging' configuration window for IIS. It includes the following fields and options:

- One log file per:** Site
- Log File:**
 - Format:** W3C (with a 'Select Fields' button)
 - Directory:** %SystemDrive%\inetpub\logs\LogFiles (highlighted with a blue arrow, with a 'Browse...' button)
 - Encoding:** UTF-8
- Log File Rollover:**
 - Select the method that IIS uses to create a new log file.
 - Schedule:** Daily
 - Maximum file size (in bytes):** [Empty text box]
 - Do not create new log files**
 - Use local time for file naming and rollover**

3. Check for IIS events. If logs are present, FortiSIEM Agent will automatically collect these logs:
- Go to IIS logs default path, example: C:\inetpub\logs\LogFiles\.
 - Check for IIS traffic logs.

Configuring Windows Event Forwarding

Using Windows Event Forwarding, it is possible for Windows Servers (called Event Source Computers) to forward events to a central Windows Server where FortiSIEM Windows Agent (called Event Collector Computer) is running. The Agent can then send to FortiSIEM Collector/Worker/Supervisor nodes. This is an alternative to running FortiSIEM Agent on every Windows Server. The disadvantage of this approach is that only Windows (Security, application, and system) events can be collected in this way, while FortiSIEM native Agent can collect other information such as FIM, Custom log, Sysmon, etc. FortiSIEM can parse the forwarded Windows events so that the actual reporting Windows server is captured and all the attributes are parsed as sent by native agents.

- [Configuring Locale on Windows Servers](#)
- [Configuring Source-Initiated Subscription](#)

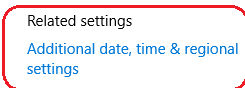
Configuring Locale on Windows Servers

- [Configure Locale on Windows 10](#)
- [Configure Locale on Generic Servers](#)

Configure Locale on Windows 10

To set the locale of Collector machine to en-US:

1. Go to the **Windows Settings** page.
2. Go to **Time And Language**, and choose the **Language** option.
3. Change the **Windows Display Language** to **English (United States)**.
4. Select the **Region** option on the left.
5. Choose the option **Additional Date, time & regional settings** on the right side of the page.



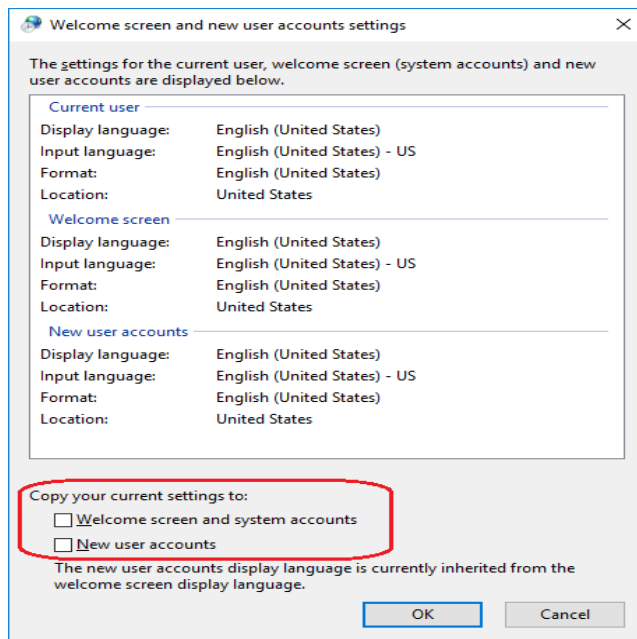
Do you have a question?

[Get help](#)

Make Windows better

[Give us feedback](#)

6. Choose the option **Region** and open the **Administrative** tab.
7. Click the **Change system locale...** button and change the locale to **English (United States)** in the provided dialog box. Click **OK**.
8. In the **Administrative** tab, click the **Copy Settings...** button.
9. In that property page tab, select both check boxes: **Welcome screen and system accounts** and **New user accounts**. Click **OK**.

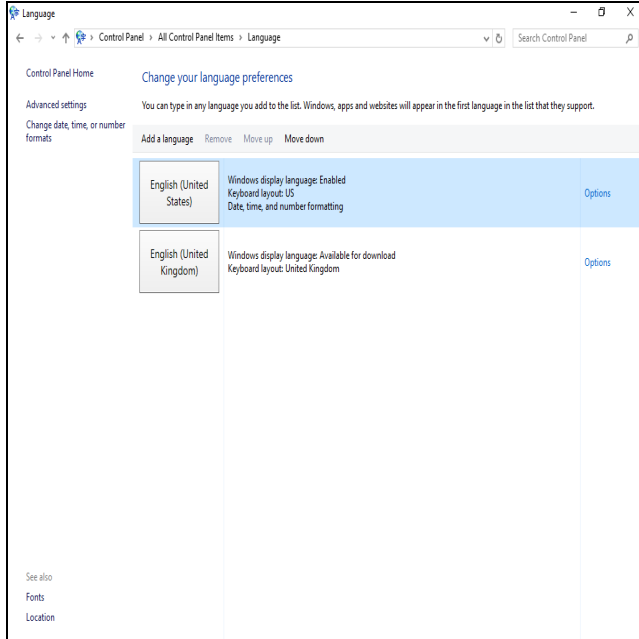


10. Restart your computer.

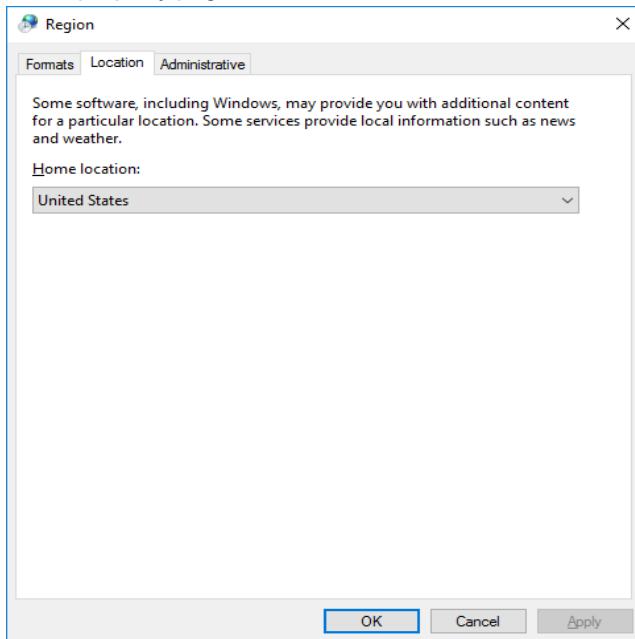
Configure Locale on Generic Servers

1. Go to the **Control Panel**.
2. Choose the **Language** option.

3. Select the language **English (United States)** and move it to top of the list.
4. Select the option **Change date, time, or number formats** on the left side of the page.

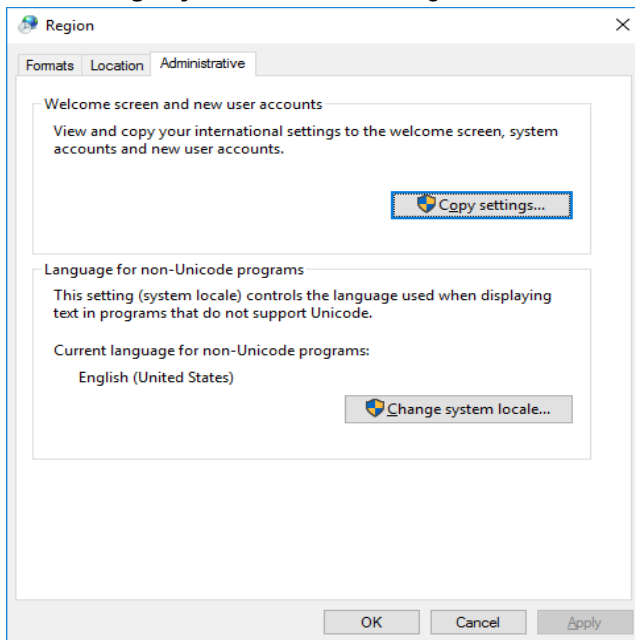


5. In this property page tab, select the **Location** tab and choose the **Home Location** as **United States**. Click **Apply**.

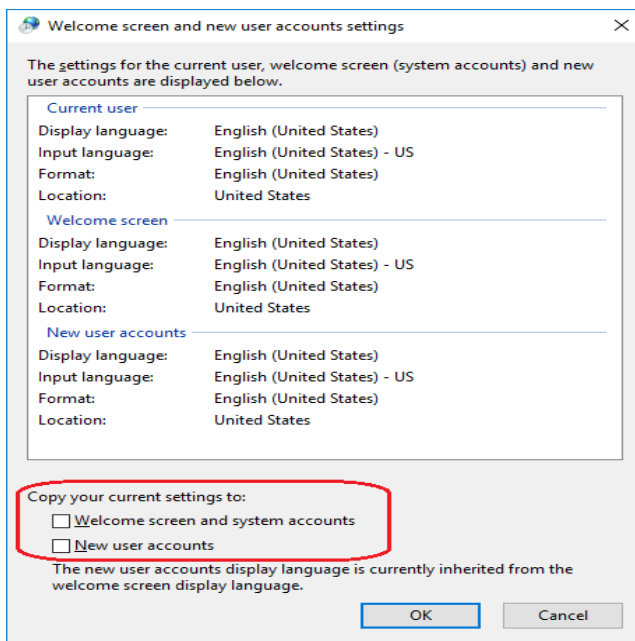


6. Select the **Administrative** tab.

7. Click **Change system locale....** Change the locale to **English (United States)** in the provided dialog. Click **OK**.



8. In the **Administrative** tab, click **Copy Settings....**
9. In this property page tab, select both check boxes: **Welcome screen and system accounts** and **New user accounts**. Click **OK**.



10. Restart your computer.

Configuring Source-Initiated Subscription

- Configure the Event Collector Computer
- Configure the Event Source Computer
- Configure the Domain Controller or Source Computer

Configure the Event Collector Computer

You must complete the following steps on the Event Collector computer where the FSM Agent is installed:

1. Open a command prompt in an elevated privilege (for example, **Run as Administrator...**) and run this command to configure the Windows Remote Management (WinRM) service:

```
winrm qc -q
```

2. Run this command to configure the Windows Event Collector service:

```
wecutil qc /q
```

3. Copy and save the following XML in a file (`Configuration.xml`) and edit the values depending on your requirements or scenario.

The XML configuration will grant the `Domain Computers` and `Network Service` accounts as the local event forwarder for the source computers. The XML configuration will contain the language locale, which is same as the Collector computer's language locale.

```
<Subscription xmlns="http://schemas.microsoft.com/2006/03/windows/events/subscription">
    <SubscriptionId>FwdSubscription</SubscriptionId>
    <SubscriptionType>SourceInitiated</SubscriptionType>
    <Description>Source Initiated Subscription</Description>
    <Enabled>>true</Enabled>
    <Uri>http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>
    <!-- Use Normal (default), Custom, MinLatency, MinBandwidth -->
    <ConfigurationMode>Custom</ConfigurationMode>
    <Delivery Mode="Push">
        <Batching>
            <MaxItems>1</MaxItems>
            <MaxLatencyTime>1000</MaxLatencyTime>
        </Batching>
        <PushSettings>
            <Heartbeat Interval="30000" />
        </PushSettings>
    </Delivery>
    <Expires>2025-01-01T00:00:00.000Z</Expires>
    <Query>
```



```

        <![CDATA[
        <QueryList>
        <Query Path="Security">
            <Select>*</Select>
        </Query>
        </QueryList>]]>
    </Query>
    <ReadExistingEvents>>true</ReadExistingEvents>
    <TransportName>http</TransportName>
    <ContentFormat>RenderedText</ContentFormat>
    <Locale Language="en-US" />
    <LogFile>ForwardedEvents</LogFile>
    <AllowedSourceNonDomainComputers></AllowedSourceNonDomainComputers>
    <AllowedSourceDomainComputers>O:NSG:NSD: (A;;GA;;;DC)
    (A;;GA;;;NS)</AllowedSourceDomainComputers>
</Subscription>

```

4. From the Command Prompt, enter the following command to create the subscription according to the specified XML configuration file:

```
wecutil cs Configuration.xml
```

5. From the Command Prompt, enter the following command to add an inbound and outbound exception in the firewall for port 5985 (http):

```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP
dir=in localport=5985 action=allow
```

```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP
dir=out remoteport=5985 action=allow
```

Configure the Event Source Computer

You must complete these steps on the Event Source computer.

1. Open a Command Prompt in an elevated privilege (for example, **Run as Administrator...**) and run the following commands:

```
net localgroup "Event log readers" "NT Authority\Network Service" /add
```

```
net localgroup "Event log readers" "Domain Computers" /add
```

```
winrm qc -q
```

2. From the command prompt enter the following command to add an inbound and outbound exception in the firewall for port 5985 (http):

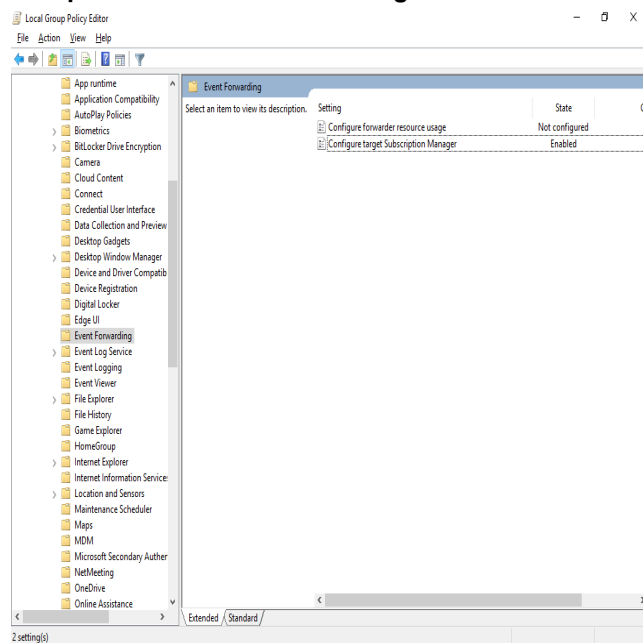
```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP dir=in localport=5985 action=allow
```

```
netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP dir=out remoteport=5985 action=allow
```

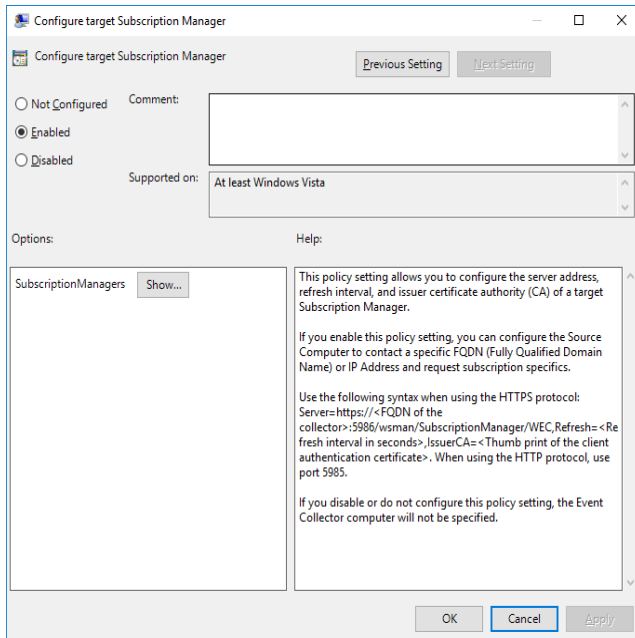
Configure the Domain Controller or Source Computer

The following policy changes must be performed on the Domain Controller (*for domain environments*) or Source Computers (*for non-domain environments*).

1. Run the local group policy editor (*for non-domain environments*) or the domain group policy editor (*for domain environments*).
2. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Event Forwarding**.



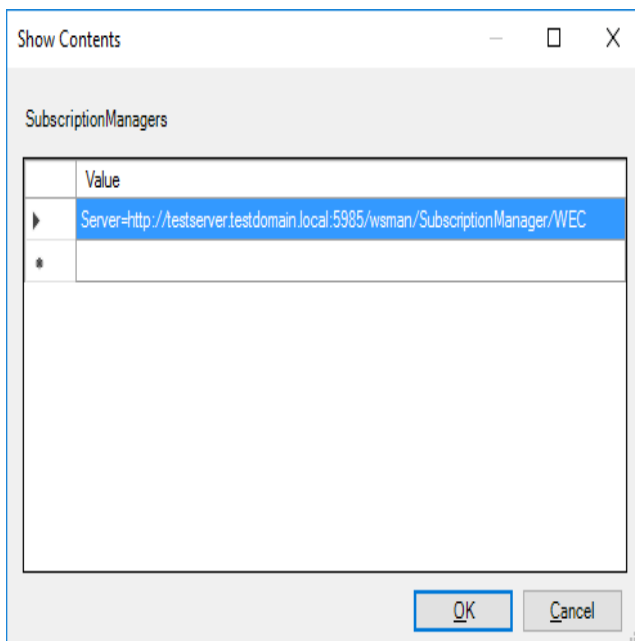
3. Open **Configure target Subscription Manager**.



4. Choose the **Enabled** option.

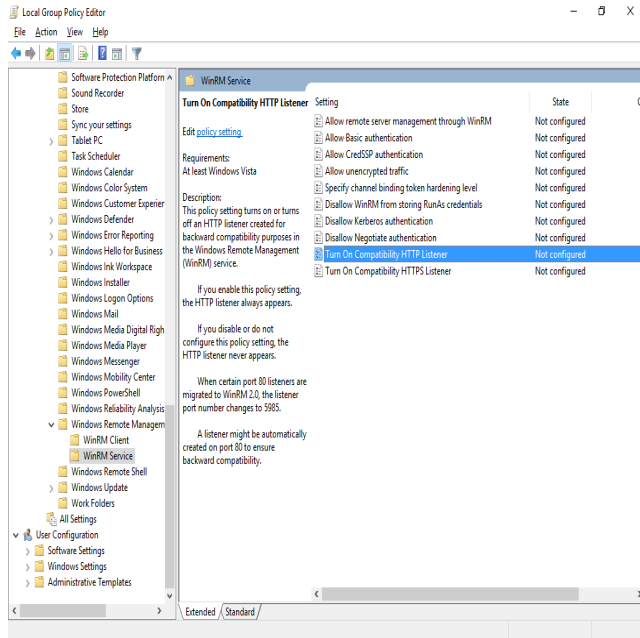
5. Click the **Show...** button beside **SubscriptionManagers**.

6. Add the value `Server=http://<Collector FQDN>:5985/wsman/SubscriptionManager/WEC` to the list and click **OK**.

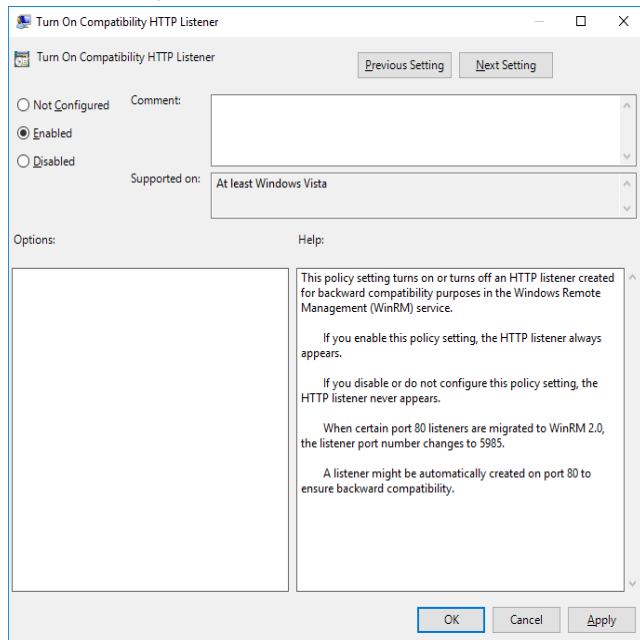


7. In the **Configure target Subscription Manager** dialog box, click **Apply** and then **OK**.

8. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management > WinRM Service**.



9. Open **Turn On Compatibility HTTP Listener**.
10. Choose the option **Enabled**.



11. Click **Apply** and then **OK**.
12. Close the group policy editor.
13. Start the Command Prompt in admin mode and run the following command:
`gpupdate /force`

Configuring Auditing Policies

The following policy changes must be performed on the Domain Controller (for domain environments) or Source Computers (for non-domain environments).

- [Configure Security Audit Logging Policy](#)
- [Configure File Auditing Policy](#)

Configure Security Audit Logging Policy

Since Windows generates a lot of security logs, specify the categories of events that you want to be logged and available for monitoring by FortiSIEM.

1. Log in to the machine where you want to configure the policy as an administrator.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand **Local Policies** and select **Audit Policy**.
You will see the current security audit settings.
4. Select a policy and edit the **Local Security Settings** for the events you want to be audited. The recommended settings are:

Policy	Description	Settings
Audit account logon events and Audit logon events	For auditing log in activity.	Select Success and Failure .
Audit object access events	For auditing access to files and folders. There is an additional configuration requirement for specifying which files and folders, users and user actions will be audited. See the next section, <i>Configuring File Auditing Policy</i> .	Select Success and Failure .
Audit system events	Includes system up/down messages.	

Configure File Auditing Policy

When you enable the policy to audit object access events, specify which files, folders, and user actions will be logged. Be very specific with these settings, and set their scope to as narrow as possible to avoid excessive logging. For this reason, you should also specify system-level folders for auditing.

1. Log in to the machine where you want to set the policy with administrator privileges.
On a domain computer, a Domain administrator account is needed.
2. Open Windows Explorer, select the file you want to set the auditing policy for, right-click on it, and select **Properties**.
3. In the **Security** tab, click **Advanced**.
4. Select the **Auditing** tab, and click **Add**.
This button is labeled **Edit** in Windows 2008.
5. In the **Select User or Group** dialog, click **Advanced**, and find and select the users whose access to this file you want to monitor.
6. Click **OK** after adding the users.

7. In the **Permissions** tab, set the permissions for each user added.
The configuration is now complete. Windows will generate audit events when the users you specified take the actions specified on the files or folders for which you set the audit policies.

Enabling FIPS

Follow the steps below to enable FIPS on a Windows system:

1. Click **Start > Run** and enter the command `secpol.msc` to open the **Local Security Policy** window.
2. Select **Security Settings > Local Policies > Security Options**.
3. In the right pane, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** and select **Enabled**.
4. Click **Apply** and then **OK**.

Verifying Events in FortiSIEM

Follow the steps below to verify the events in FortiSIEM:

1.
 - a. Go to **ANALYTICS** tab.
 - b. Click the **Filters** field.
 - c. Create the following condition: **Attribute**= Raw Event Log, **Operator** = CONTAIN, **Value** = AccelOps-WUA and click **Save & Run**.
Note: All event types for all Windows Server generated logs are prefixed by **AccelOps-WUA**.
 - d. Select the following **Group By**:
 - i. Reporting Device Name
 - ii. Reporting IP
 - e. Select the following **Display Fields**:
 - i. Reporting Device Name
 - ii. Reporting IP
 - iii. COUNT(Matched Events)
 - f. Run the query for the last 15 minutes.
The Query will return all hosts that reported events in the last 15 minutes.

Uninstalling Windows Agent

Follow the steps below to uninstall FortiSIEM Windows Agent:

1. Log in to the Windows machine where the Agent is installed.
2. Go to `Control Panel\Programs\Programs and Features`.
3. Uninstall **FortiSIEM Windows Agent**.

REST APIs used for Communication

A Windows Agent uses the following REST APIs:

Purpose	URL	Notes
Registration to Supervisor	https://<SuperFQDN>:<port>/phoenix/rest/register/windowsAgent	Supported Port is 443
Status update to Supervisor	https://<SuperFQDN>:<port>/phoenix/rest/windowsAgent/update	Supported Port is 443
Event Upload to Collectors	https://<CollectorFQDNorIP>:<port>/winupload_direct?<AgentID>	Supported Port is 443

Troubleshooting from Windows Agent

The debugging information is available in two log files:

- Agent Service logs are located in C:\ProgramData\AccelOps\Agent\Logs\AoWinAgt.log
- Agent Application logs are located in C:\ProgramData\AccelOps\Agent\Logs\ProxyTrace.log

Sample Windows Agent Logs

FortiSIEM Windows Agent Manager generates Windows logs in an easy way to analyze "attribute=value" style without losing any information.

- System Logs
- Application Logs
- Security Logs
- DNS Logs
- DHCP Logs
- IIS Logs
- DFS Logs
- File Content Monitoring Logs
- File Integrity Monitoring Logs
- Installed Software Logs
- Registry change Logs
- WMI Logs

System Logs

```
#Win-System-Service-Control-Manager-7036
Thu May 07 02:13:42 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
```

```
[monitorStatus]="Success" [eventName]="System"
[eventSource]="Service Control Manager" [eventId]="7036" [eventType]="Information"
[domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:13:41"
[deviceTime]="May 07 2015 10:13:41"
[msg]="The Skype Updater service entered the running state."

Thu May 07 02:13:48 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="System"
[eventSource]="Service Control Manager" [eventId]="7036" [eventType]="Information"
[domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:13:47"
[deviceTime]="May 07 2015 10:13:47"
[msg]="The Skype Updater service entered the stopped state."
```

Application Logs

```
#Win-App-MSEExchangeServiceHost-2001
Thu May 07 03:05:42 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="Application" [eventSource]="MSEExchangeServiceHost"
[eventId]="2001" [eventType]="Information" [domain]="" [computer]="WIN-2008-249.ersijiu.com"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 11:05:42"
[deviceTime]="May 07 2015 11:05:42"
[msg]="Loading servicelet module Microsoft.Exchange.OABMaintenanceServicelet.dll"

#MSSQL
#Win-App-MSSQLSERVER-17137
Thu May 07 03:10:16 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="Application"
[eventSource]="MSSQLSERVER" [eventId]="17137" [eventType]="Information" [domain]=""
[computer]="WIN-2008-249.ersijiu.com" [user]=""
[userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 11:10:16" [deviceTime]="May 07
2015 11:10:16"
[msg]="Starting up database 'model'."
```

Security Logs

```
#Win-Security-4624(Windows logon success)
Thu May 07 02:23:58 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="Security"
[eventSource]="Microsoft-Windows-Security-Auditing" [eventId]="4624" [eventType]="Audit
Success" [domain]=""
[computer]="WIN-2008-249.ersijiu.com" [user]="" [userSID]="" [userSIDAcctType]=""
[eventTime]="May 07 2015 10:23:56"
[deviceTime]="May 07 2015 10:23:56" [msg]="An account was successfully logged on."
[[Subject]][Security ID]="S-1-0-0" [Account Name]="
[Account Domain]="" [Logon ID]="0x0" [Logon Type]="3" [[New Logon]][Security ID]="S-1-5-21-
3459063063-1203930890-2363081030-500"
[Account Name]="Administrator" [Account Domain]="ERSIJIU" [Logon ID]="0xb9bd3" [Logon
GUID]="{00000000-0000-0000-0000-000000000000}"
[[Process Information]][Process ID]="0x0" [Process Name]=" [[Network Information]]
[Workstation Name]="SP171" [Source Network Address]="10.1.2.171"
[Source Port]="52409" [[Detailed Authentication Information]][Logon Process]="NtLmSsp"
```



```
[Authentication Package]="NTLM" [Transited Services]=""  
[Package Name (NTLM only)]="NTLM V2" [Key Length]="128" [details]=""
```

DNS Logs

```
#DNS Debug Logs  
#AccelOps-WUA-DNS-Started  
Thu May 07 02:35:43 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS  
[monitorStatus]="Success"  
[msg]="5/7/2015 10:34:05 AM 20BC EVENT The DNS server has started."  
  
#AccelOps-WUA-DNS-ZoneDownloadComplete  
Thu May 07 02:35:43 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS  
[monitorStatus]="Success" [msg]="5/7/2015 10:34:05 AM 20BC EVENT  
The DNS server has finished the background loading of zones. All zones are now available for  
DNS updates and zone  
transfers, as allowed by their individual zone configuration."  
  
#AccelOps-WUA-DNS-A-Query-Success  
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS  
[monitorStatus]="Success" [msg]="5/7/2015  
10:47:13 AM 5D58 PACKET 000000002B74600 UDP Rcv 10.1.20.232 0002 Q [0001 D  
NOERROR] A (8)testyjyj(4)yjyj(3)com(0)"Thu May 07 02:48:25 2015 WIN-2008-LAW-agent  
10.1.2.242 AccelOps-WUA-DNS [monitorStatus]="Success" [msg]="5/7/2015  
10:47:13 AM 5D58 PACKET 000000002B74600 UDP Snd 10.1.20.232 0002 R Q [8085 A DR  
NOERROR] A (8)testyjyj(4)yjyj(3)com(0)"  
  
#AccelOps-WUA-DNS-PTR-Query-Success  
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS  
[monitorStatus]="Success" [msg]="5/7/2015  
10:47:22 AM 5D58 PACKET 0000000028AB4B0 UDP Rcv 10.1.20.232 0002 Q [0001 D NOERROR]  
PTR  
(3)223(3)102(3)102(3)102(7)in-addr(4)arpa(0)"  
  
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DNS  
[monitorStatus]="Success" [msg]="5/7/2015  
10:47:22 AM 5D58 PACKET 0000000028AB4B0 UDP Snd 10.1.20.232 0002 R Q [8085 A DR  
NOERROR] PTR  
(3)223(3)102(3)102(3)102(7)in-addr(4)arpa(0)"  
  
#DNS System Logs  
#Win-App-DNS-2(DNS Server started)  
Thu May 07 02:39:17 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog  
[monitorStatus]="Success"  
[eventName]="DNS Server" [eventSource]="DNS" [eventId]="2" [eventType]="Information"  
[domain]="" [computer]="WIN-2008-LAW-agent"  
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:39:17"  
[deviceTime]="May 07 2015 10:39:17"  
[msg]="The DNS server has started."  
  
#Win-App-DNS-3(DNS Server shutdown)  
Thu May 07 02:39:16 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog  
[monitorStatus]="Success" [eventName]="DNS Server"  
[eventSource]="DNS" [eventId]="3" [eventType]="Information" [domain]="" [computer]="WIN-  
2008-LAW-agent" [user]="" [userSID]=""  
[userSIDAcctType]="" [eventTime]="May 07 2015 10:39:16" [deviceTime]="May 07 2015 10:39:16"  
[msg]="The DNS server has shut down."
```

DHCP Logs

```

AccelOps-WUA-DHCP-Generic
Thu May 07 05:44:44 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="00" [Date]="05/07/15"
[Time]="13:44:08" [Description]="Started" [IP Address]=" " [Host Name]=" " [MAC Address]=" "
[User Name]=" " [TransactionID]="0"
[QResult]="6" [Probationtime]=" " [CorrelationID]=" " [Dhcid.]=" "

#AccelOps-WUA-DHCP-IP-ASSIGN
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="10" [Date]="05/07/15"
[Time]="13:56:37" [Description]="Assign" [IP Address]="10.1.2.124" [Host Name]="Agent-
247.yj" [MAC Address]="000C2922118E"
[User Name]=" " [TransactionID]="2987030242" [QResult]="0" [Probationtime]=" " [
CorrelationID]=" " [Dhcid.]=" "

#AccelOps-WUA-DHCP-Generic(Release)
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="12" [Date]="05/07/15"
[Time]="13:56:33" [Description]="Release" [IP Address]="10.1.2.124" [Host Name]="Agent-
247.yj" [MAC Address]="000C2922118E"
[User Name]=" " [TransactionID]="2179405838" [QResult]="0" [Probationtime]=" " [
CorrelationID]=" " [Dhcid.]=" "

#AccelOps-WUA-DHCP-IP-LEASE-RENEW
Wed Feb 25 02:53:28 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-DHCP
[monitorStatus]="Success" [ID]="11" [Date]="02/25/15"
[Time]="10:53:19" [Description]="Renew" [IP Address]="10.1.2.123" [Host Name]="WIN-2008-
249.yj" [MAC Address]="0050568F1B5D"
[User Name]=" " [TransactionID]="1136957584" [QResult]="0" [Probationtime]=" " [
CorrelationID]=" " [Dhcid.]=" "

```

IIS Logs

```

#AccelOps-WUA-IIS-Web-Request-Success
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-IIS
[monitorStatus]="Success" [date]="2015-05-07"
[time]="03:44:28" [s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-
ip]="10.1.2.242" [cs-method]="GET"
[cs-uri-stem]="/welcome.png" [cs-uri-query]="-" [s-port]="80" [cs-username]="-" [c-
ip]="10.1.20.232" [cs-version]="HTTP/1.1"
[cs (User-Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/42.0.2311.135+Safari/537.36"
[cs (Cookie)]="-" [cs (Referer)]="http://10.1.2.242/" [cs-host]="10.1.2.242" [sc-status]="200"
[sc-substatus]="0" [sc-win32-status]="0"
[sc-bytes]="185173" [cs-bytes]="324" [time-taken]="78" [site]="Default Web Site"
[format]="W3C"

#AccelOps-WUA-IIS-Web-Client-Error
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-IIS
[monitorStatus]="Success" [date]="2015-05-07" [time]="03:44:37"
[s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-ip]="10.1.2.242" [cs-
method]="GET" [cs-uri-stem]="/wrongpage" [cs-uri-query]="-"
[s-port]="80" [cs-username]="-" [c-ip]="10.1.20.232" [cs-version]="HTTP/1.1" [cs (User-
Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+

```

```
(KHTML,+like+Gecko)+Chrome/42.0.2311.135+Safari/537.36" [cs(Cookie)]="-" [cs(Referer)]="-"
[cs-host]="10.1.2.242" [sc-status]="404"
[sc-substatus]="0" [sc-win32-status]="2" [sc-bytes]="1382" [cs-bytes]="347" [time-taken]="0"
[site]="Default Web Site" [format]="W3C"

#AccelOps-WUA-IIS-Web-Forbidden-Access-Denied
Thu May 07 03:30:39 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-IIS
[monitorStatus]="Success" [date]="2015-05-07" [time]="03:30:15" [s-ip]="10.1.2.249" [cs-
method]="POST" [cs-uri-stem]="/AOCACWS/AOCACWS.svc" [cs-uri-query]="-" [s-port]="80" [cs-
username]="-"
[c-ip]="10.1.2.42" [cs(User-Agent)]="-" [sc-status]="403" [sc-substatus]="4" [sc-win32-
status]="5" [time-taken]="1" [site]="Default Web Site"
[format]="W3C"
```

DFS Logs

```
#Win-App-DFSR-1002
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1002" [eventType]="Information" [domain]="" [computer]="WIN-
2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015 11:01:12"
[msg]="The DFS Replication service is starting."

#Win-App-DFSR-1004
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1004" [eventType]="Information" [domain]="" [computer]="WIN-
2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015 11:01:12"
[msg]="The DFS Replication service has started."

#Win-App-DFSR-1006
Thu May 07 03:01:10 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1006" [eventType]="Information" [domain]="" [computer]="WIN-
2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:10" [deviceTime]="May 07 2015 11:01:10"
[msg]="The DFS Replication service is stopping."

#Win-App-DFSR-1008
Thu May 07 03:01:11 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WinLog
[monitorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1008" [eventType]="Information" [domain]="" [computer]="WIN-
2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:11" [deviceTime]="May 07 2015 11:01:11"
[msg]="The DFS Replication service has stopped."
```

File Content Monitoring Logs

```
#AccelOps-WUA-UserFile
Thu May 07 05:40:08 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-UserFile
[monitorStatus]="Success" [fileName]="C:\test\i.txt"
[msg]="another newline addeddddddd"
```

File Integrity Monitoring Logs

```
#AccelOps-WUA-FileMon-Added
Thu May 07 05:30:59 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-FileMon
[monitorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:30:58" [fileName]="C:\\test\\New Text Document.txt"
[osObjAction]="Added" [hashCode]="d41d8cd98f00b204e9800998ecf8427e"
[msg]=""
```

```
#AccelOps-WUA-FileMon-Renamed-New-Name
Thu May 07 05:31:02 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-FileMon
[monitorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:30:58" [fileName]="C:\\test\\test.txt" [osObjAction]="Renamed
[New Name]" [hashCode]="d41d8cd98f00b204e9800998ecf8427e"
[msg]=""
```

```
#AccelOps-WUA-FileMon-Renamed-Old-Name
Thu May 07 05:31:02 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-FileMon
[monitorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:31:01" [fileName]="C:\\test\\New Text Document.txt"
[osObjAction]="Renamed [Old Name]" [hashCode]=""
```

```
#AccelOps-WUA-FileMon-Modified
Thu May 07 05:31:14 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-FileMon
[monitorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:31:13" [fileName]="C:\\test\\test.txt" [osObjAction]="Modified"
[hashCode]="23acb5410a432f14b141656c2e70d104"
[msg]=""
```

```
#AccelOps-WUA-FileMon-Removed
Thu May 07 05:31:29 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-FileMon
[monitorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:31:27" [fileName]="C:\\test\\test.txt" [osObjAction]="Removed"
[hashCode]="" [msg]=""
```

Installed Software Logs

```
#AccelOps-WUA-InstSw-Added
Thu May 07 05:28:17 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-InstSw
[monitorStatus]="Success" [osObjAction]="Added"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVersion]="9.20.00.0"
```

```
#AccelOps-WUA-InstSw-Removed
Thu May 07 05:28:30 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-InstSw
[monitorStatus]="Success" [osObjAction]="Removed"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVersion]="9.20.00.0"
```

Registry Change Logs

```
#AccelOps-WUA-Registry-Modified
Thu May 07 04:01:58 2015 WIN-2008-249.ersijiu.com 10.1.2.249 AccelOps-WUA-Registry
[monitorStatus]="Success"
[regKeyPath]="HKLM\\SOFTWARE\\Microsoft\\ExchangeServer\\v14\\ContentIndex\\CatalogHealth\\
{0d2a342a-0b15-4995-93db-d18c3df5860d}" [regValueName]="TimeStamp" [regValueType]="1"
```

```
[osObjAction]="Modified"
[oldRegValue]="MgAwADEANQAtADAANQAtADAANwAgADAAMwA6ADQAOQA6ADQANwBaAAAA"
[newRegValue]="MgAwADEANQAtADAANQAtADAANwAgADAANAA6ADAAMQA6ADQAOABaAAAA"

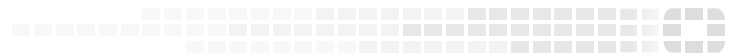
#AccelOps-WUA-Registry-Removed
Thu May 07 05:25:09 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-Registry
[monitorStatus]="Success"
[regKeyPath]="HKLM\\SOFTWARE\\RegisteredApplications" [regValueName]="Skype"
[regValueType]="1" [osObjAction]="Removed"
[oldRegValue]="UwBP AEYAVABXAEUAUGBFAFWAQwBsAGkAZQBwAHQAcwBcAEkAbgB0AGUAcgBuAGUAdAAgAEMAYQBsA
GwAXABTAGsAeQBwAGUAXABDAGEAcABhAGIAaQBsAGkAdABpAGUAcwBkAGgAZABoAGQAaABkAGgAZABoAGQAAAA="
[newRegValue]=""
```

WMI logs

```
#AccelOps-WUA-WMI-Win32_Processor
Thu May 07 03:53:33 2015 WIN-2008-LAW-agent 10.1.2.242 AccelOps-WUA-WMI
[monitorStatus]="Success" [__CLASS]="Win32_Processor"
[AddressWidth]="64" [Architecture]="9" [Availability]="3" [Caption]="Intel64 Family 6 Model
26 Stepping 5" [ConfigManagerErrorCode]="" [ConfigManagerUserConfig]="" [CpuStatus]="1"
[CreationClassName]="Win32_Processor" [CurrentClockSpeed]="2266" [CurrentVoltage]="33"
[DataWidth]="64" [Description]="Intel64 Family 6 Model 26 Stepping 5" [DeviceID]="CPU0"
[ErrorCleared]="" [ErrorDescription]=""
[ExtClock]="" [Family]="12" [InstallDate]="" [L2CacheSize]="0" [L2CacheSpeed]=""
[L3CacheSize]="0" [L3CacheSpeed]="0"
[LastErrorCode]="" [Level]="6" [LoadPercentage]="8" [Manufacturer]="GenuineIntel"
[MaxClockSpeed]="2266"
[Name]="Intel (R) Xeon (R) CPU E5520 @ 2.27GHz" [NumberOfCores]="1"
[NumberOfLogicalProcessors]="1"
[OtherFamilyDescription]="" [PNPDeviceID]="" [PowerManagementCapabilities]=""
[PowerManagementSupported]="0"
[ProcessorId]="0FEBFBFF000106A5" [ProcessorType]="3" [Revision]="6661" [Role]="CPU"
[SocketDesignation]="CPU socket #0"
[Status]="OK" [StatusInfo]="3" [Stepping]="" [SystemCreationClassName]="Win32_
ComputerSystem" [SystemName]="WIN-2008-LAW-AG"
[UniqueId]="" [UpgradeMethod]="4" [Version]="" [VoltageCaps]="2"
```



FORTINET®



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.