

# FortiSIEM - Windows Agent 4.x.x Installation Guide

Version 6.1.0

**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

**FORTINET TRAINING 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

08/11/2023
FortiSIEM 6.1.0 Windows Agent 4.x.x Installation Guide

# TABLE OF CONTENTS

# 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`. |
| 06-30-2020 | Revision 13: updated to agent version 4.0.0. |
| 11-25-2020 | Revision 14: updated "Uninstalling Windows Agent" section. |
| 01-04-2021 | Revision 15: updated "Installing Windows Agent" section. |
| 03-15-2021 | Revision 16: updated "Installing Windows Agent" section. |
| 07-22-2021 | Revision 17: updated "Installing Windows Agent" section. |
| 08-19-2022 | Revision 18: updated Prerequisites - Other Installation Considerations section. |
| 10-31-2022 | Revision 19: Updated Other Installation Considerations section. |
| 06-07-2023 | Revision 20: Added Windows 11 to Supported Operating Systems. |
| 08-11-2023 | Revision 21: Updated Software Requirements under Prerequisites. |

# FortiSIEM Windows Agent

FortiSIEM Windows Agents provide a scalable way to collect logs and other audit violations from a large number of Windows servers. This release adds these new features:

- User Entity Behavior Telemetry is collected by a kernel-level agent that installs together with FortiSIEM Agent. Note that this requires Disk Fair scheduling to be turned off. See Other Installation Considerations for more details.
- The ability to collect DNS Analytical logs and any binary logs in general.

This section describes how to install, setup, maintain, and troubleshoot FortiSIEM Windows Agent 4.x.x.



# Prerequisites

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

## Supported Operating Systems

FortiSIEM Windows Agent 4.x.x runs on the following Operating Systems:

- Windows 7 Enterprise/Professional
- Windows 8
- Windows 10
- Windows 11
- 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 the 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)<br>- Desktop Operating System: Windows 7, 8,10 and above |
| RAM | - For 32 bit OS: 2 GB for Windows 7, 8, 10 minimum<br>- For 64 bit OS: 4 GB for Windows 7, 8, 10, Windows Server 2008 / 2012 minimum |

## Software Requirements

| Windows Agent Version | Component | Requirement | Notes |
|---|---|---|---|
| 4.2 | 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. |
| 4.3.0+ | Installed Software | .NET Framework 4.6 or later | .NET Framework 4.6 can be downloaded from https://www.microsoft.com/en-us/download/details.aspx?id=48137. |

## Communication Ports

FortiSIEM Windows Agent 4.x.x 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

The FortiInsight UEBA module uses WinVeifyTrust APIs to validate that its executable hasn't been tampered with. This process requires the root certificate chain to be present on the endpoint device in question. FortiSIEM Windows Agent is signed using a DigiCert Authenticode Certificate, which requires the DigiCert Trusted Root G4 Certificate to be present in the Certificate Store.

Normally these certificates will be updated along with Windows Updates, however if the endpoint device does not allow for Certificate Authorities to be updated via this mechanism, you must install it manually for the FortiInsight UEBA module to work correctly.

These certificates can be found here:

https://www.digicert.com/kb/digicert-root-certificates.htm

Search for G4 root certificate, serial number: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C.

Or direct link to DER/CRT: https://cacerts.digicert.com/DigiCertTrustedRootG4.crt

Once the certificate has been downloaded, simply right click the certificate from the download and select "install certificate".

Follow the certificate wizard and import will complete.

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
```

- Switch off Disk Fair Share. If it is on, then the real user in UEBA may not be captured. You can switch it off by running the following commands in powershell:

```
$temp = (gwmi win32_terminalservicesetting -N "root\cimv2\terminalservices")
$temp.enableDiskFSS = 0
$temp.put()
```

  For more information on Disk Fair Share, see https://support.microsoft.com/en-gb/help/4494631/fair-share-technologies-enabled-by-default-in-remote-desktop-services.

# 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:

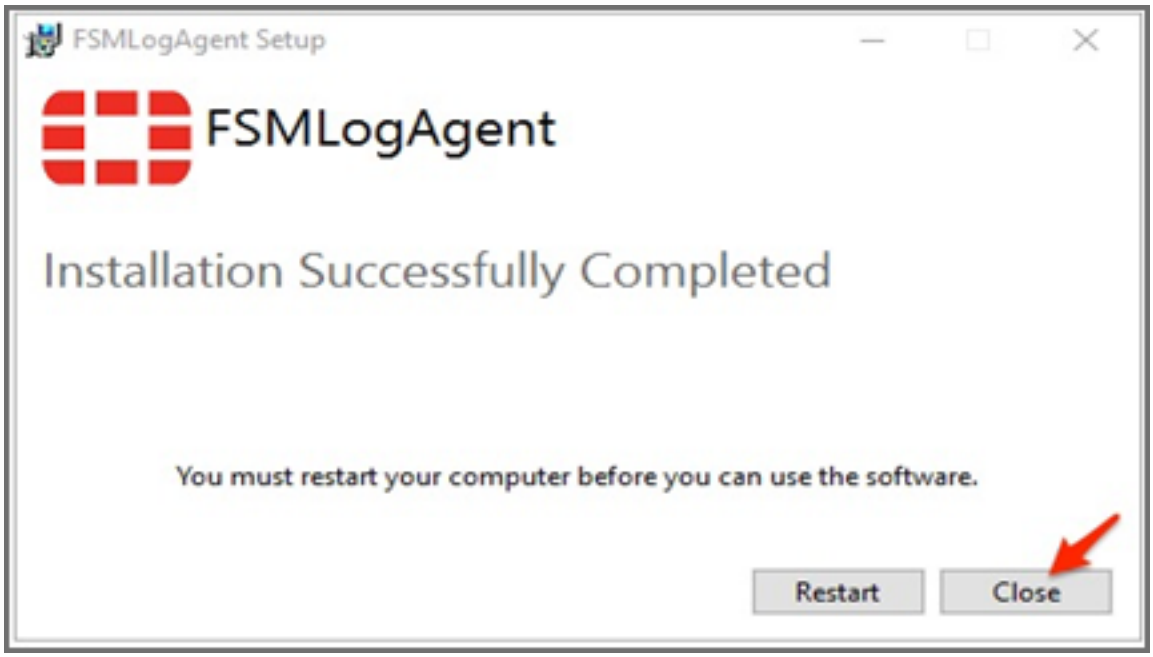
- **SUPER_IP**: IP Address or Host name/FQDN of Supervisor node
- **ORG_ID**: FortiSIEM Organization Id to which this Agent belongs
- **ORG_NAME**: FortiSIEM Organization Name
- **AGENT_USER**: Agent user name (for registration only)
- **AGENT_PASSWORD**: Agent password (for registration only)
- **HOST_NAME**: This name will be displayed in FortiSIEM CMDB. FortiSIEM recommends using a Fully Qualified Domain Name (FQDN), especially if SNMP or WMI is also going to be used against this device. FQDN allows for standardized naming convention.

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 4.x.x binaries: `FSMLogAgent-v4.x.x.exe` and `InstallSettings.xml` to the same folder.
3. Obtain the Organization ID, Organization Name and Agent registration credentials.
   a. When using the multi-tennant version of FortiSIEM, follow these substeps to find these items:
      i. Log in to FortiSIEM in Super Global mode as Admin user.
      ii. Go to **ADMIN** > **Setup** > **Organizations** and locate the Organization (ID, Name) to which this Agent belongs. If not present, create an Organization.
      iii. Locate the Agent Registration User and Password for the Organization. If not present, define them.
   b. When using the Enterprise version of FortiSIEM, use “1” for the Organization ID and “super” for the Organization Name.
4. Download the `InstallSettings.xml file`, and edit the fields for your environment.
   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. Make sure that `AGENT_PASSWORD` is enclosed within a `CDATA` block as in the sample InstallSettings.xml file. This enables the `AGENT_PASSWORD` to contain non-ASCII characters like "&", "<", ">", "!", "#", etc... Make sure that there are no leading and trailing white spaces between `CDATA[` and `]]`.
      For example, `<Password><![CDATA[ myPassword ]]></Password>` is not acceptable.
      It would need to be changed to `<Password><![CDATA[myPassword]]></Password>`.
      **Note**: When viewing the InstallSettings.xml file through a web browser, extraneous space characters may appear. Fortinet recommends saving the InstallSettings.xml file, then viewing it through a proper XML editor.
   c. It is recommended that you specify the Agent Host name in the `<HostName>AGENT_HOST_NAME</HostName>` tag. This will be the device name in the FortiSIEM CMDB. If this attribute is not specified, then the agent will pick up the NetBios Name, which will also be the device name in CMDB.
5. Install the Agent:
   Choose one of options listed to install your Windows Agent.
   a. **Option 1: GUI Installation**
      i. Log in to the Windows machine as Administrator.
      ii. Ensure that the `FSMLogAgent-v4.x.x.exe` in step 2 and `InstallSettings.xml` in step 4 are in the same folder (example: `copy to c:\Temp\`).
      iii. Double-click the `FSMLogAgent-v4.x.x.exe` package and the installation process will start. If any settings errors are detected, the install process will fail, otherwise it will succeed. The Agent will register to the Supervisor and start running.
      **Note**: If the installation returns a pop-up to restart your computer, click **Close**.




b. **Option 2: Command Line Installation**
   i. Log in to the Windows machine as Administrator.
   ii. Ensure that the `FSMLogAgent-v4.x.x.exe` in step 2 and `InstallSettings.xml` in step 4 are in the same folder (example: `copy to c:\Temp\`).
   iii. Launch **Command Prompt**, go to the Installation packages saved location, and run `FSMLogAgent-v4.x.x-mmddyyyy.exe` with the `/norestart` option.
   For example, `C:\Temp\FSMLogAgent-v4.1.0-03052021.exe /norestart`

   The installation process will start. If any settings errors are detected, the install process will fail, otherwise 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.

# Installing Windows Agent Without Supervisor Communication

In typical installations, FortiSIEM Agents register to the Supervisor node, but send the events by using the Collector. In many MSSP situations, customers do not want Agents to directly communicate with the Supervisor node. This

requirement can be satisfied by setting up the Collector as an HTTPS proxy between the Agent and the Supervisor. This section describes the required configurations.

- Step 1: Setup the Collector as an HTTPS Proxy
- Step 2: Install Agents to Work with the Collector

## Step 1: Setup the Collector as an HTTPS Proxy

Follow these steps to setup the Collector as an HTTPS proxy:

1. Log in to the Collector.
2. Go to `/etc/httpd/conf.d`.
3. Create the configuration file `agent-proxy.conf` with the content here.
4. Restart httpd, for example: `service httpd restart`.

**agent-proxy.conf Content**

```
ProxyPass /phoenix/rest/register/windowsAgent https://{actual IP address of the Supervisor
     node}/phoenix/rest/register/windowsAgent
ProxyPassReverse /phoenix/rest/register/windowsAgent https://{actual IP address of the
     Supervisor node}/phoenix/rest/register/windowsAgent
ProxyPass /phoenix/rest/windowsAgent/update https://{actual IP address of the Supervisor
     node}/phoenix/rest/windowsAgent/update
ProxyPassReverse /phoenix/rest/windowsAgent/update https://{actual IP address of the
     Supervisor node}/phoenix/rest/windowsAgent/update

SSLProxyEngine on

SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerExpire off
```

## Step 2: Install Agents to Work with the Collector

Follow these steps to install the Windows Agents to work with the Collector.

1. If you already have agents registered with the Supervisor, then uninstall them.
2. Re-install the Windows Agents, following the instructions here. During installation, set the Supervisor IP to the IP address of the Collector node.

# 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

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.

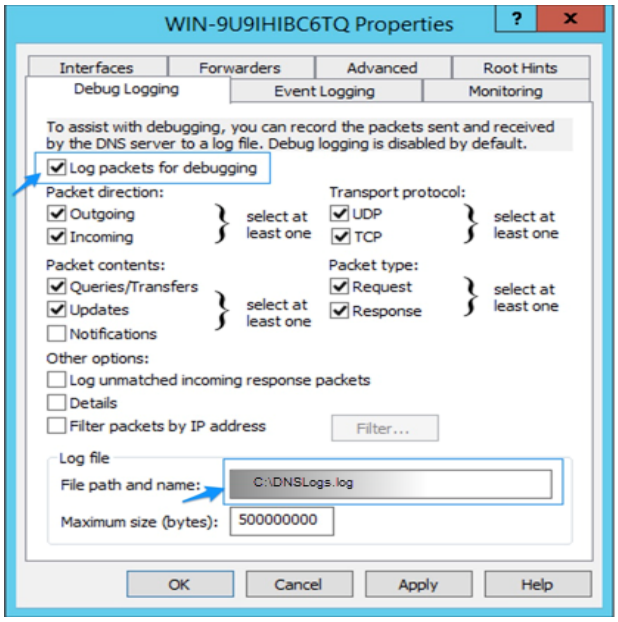
## Configuring Windows DNS

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:

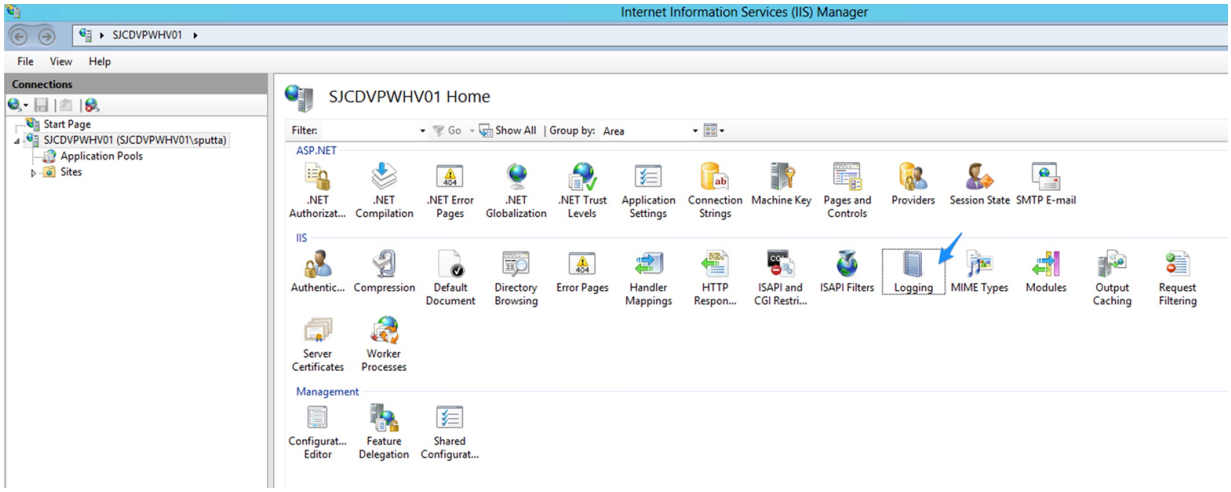
1. Log in to the Windows machine.
2. Configure DHCP logging:
   a. Launch **DHCP Manager**.
   b. Select the specific DHCP Server and click **IPv4** > **Properties**.
   c. Enable **DHCP Audit Logging**.
3. Check for DHCP events. If logs are present, FortiSIEM Agent will automatically collect these logs: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

## Configuring Windows IIS

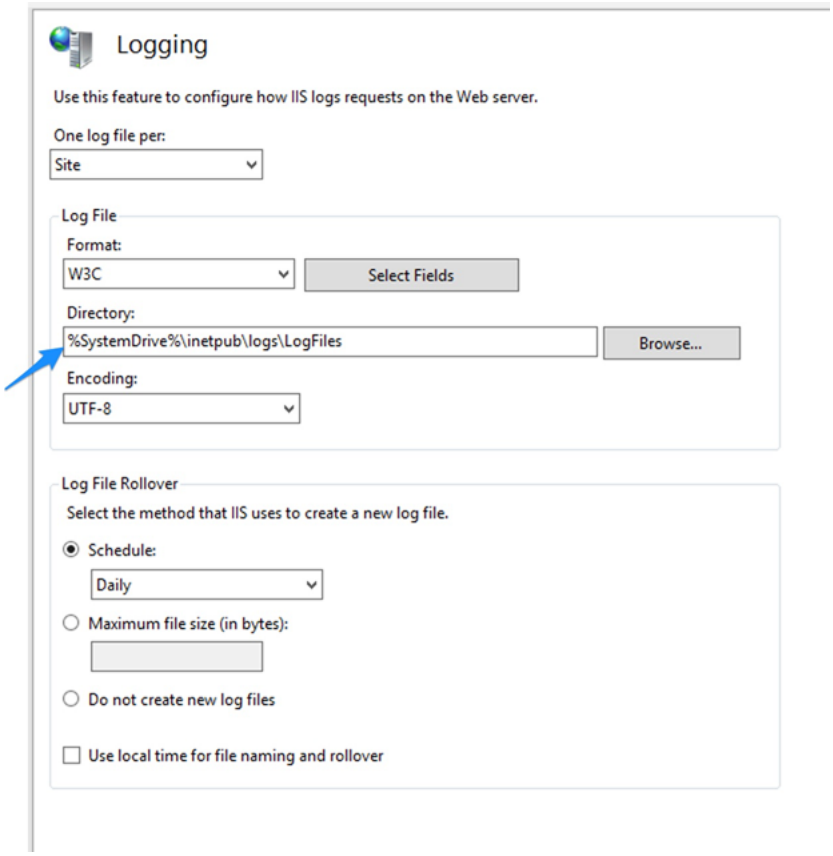
Follow these steps to configure the IIS Server:

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.




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

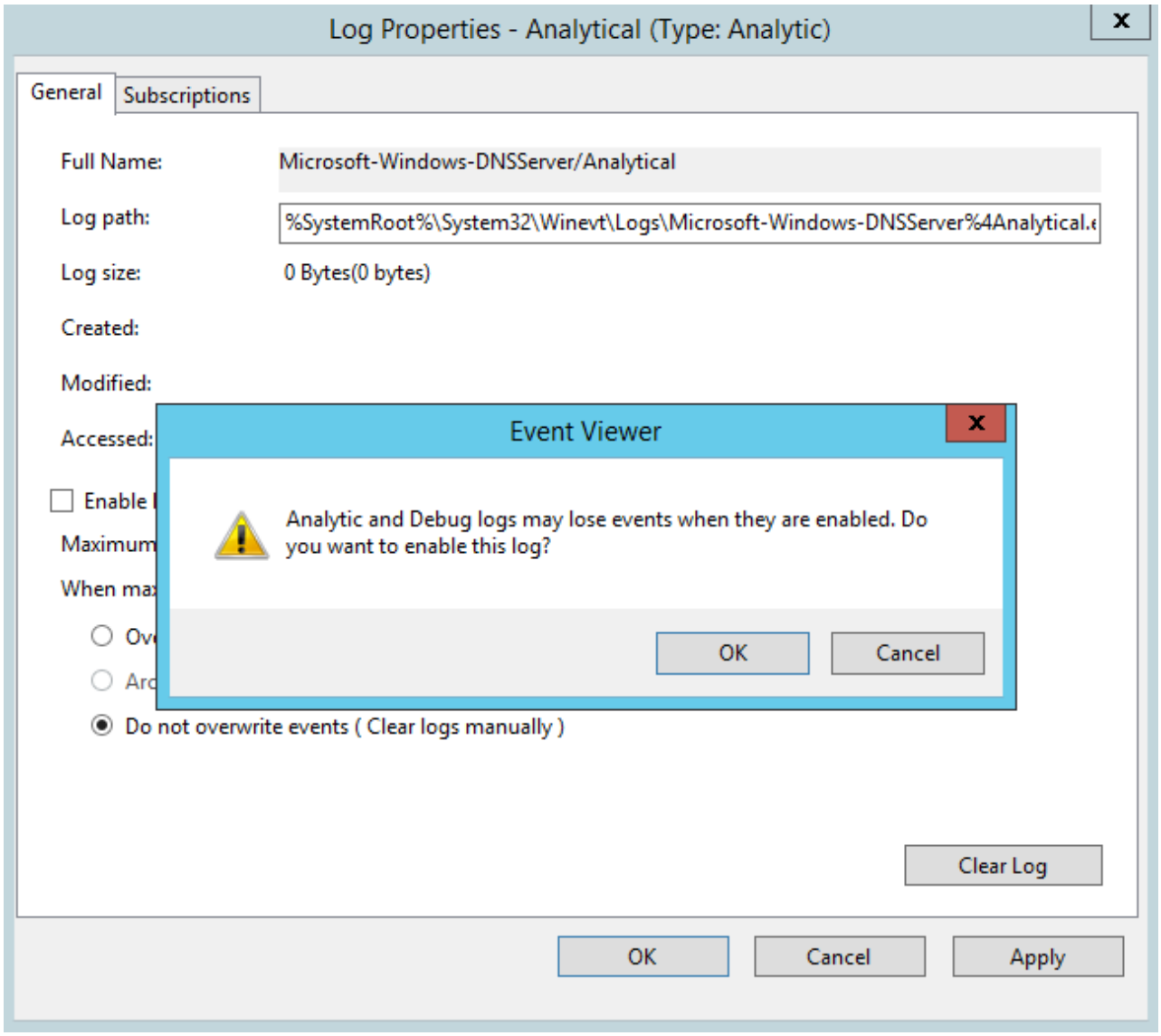
## Configuring DNS Analytical Logs

If the DNS server is running Windows Server 2012 R2, download the hotfix from http://support.microsoft.com/kb/2956577

You can find more information on this topic in Enable Analytic and Debug Logs in the Microsoft User Guide.

Follow these steps to configure FortiSIEM Windows Agent to collect DNS Analytical logs:

1. Enter `eventvwr.msc` at an elevated command prompt and press **Enter** to open the Event Viewer.
2. In the Event Viewer, navigate to **Applications and Services Logs\Microsoft\Windows\DNS-Server**.
3. Right-click **DNS-Server**, point to **View**, and click **Show Analytic and Debug Logs**. The **Analytical** log is displayed.
4. Right-click **Analytical** and then click **Properties**.
5. Under **When maximum event log size is reached**, choose **Do not overwrite events (Clear logs manually)**.
6. Select the **Enable logging** checkbox.
7. Click **OK** when you are asked if you want to enable this log. See the following example.



8. Click **OK** again to enable the DNS Server Analytic event log.
9. Note the **Full Name** value in the screenshot in Step7: **Microsoft-Windows-DNSServer/Analytical**. This name must be entered in FortiSIEM.

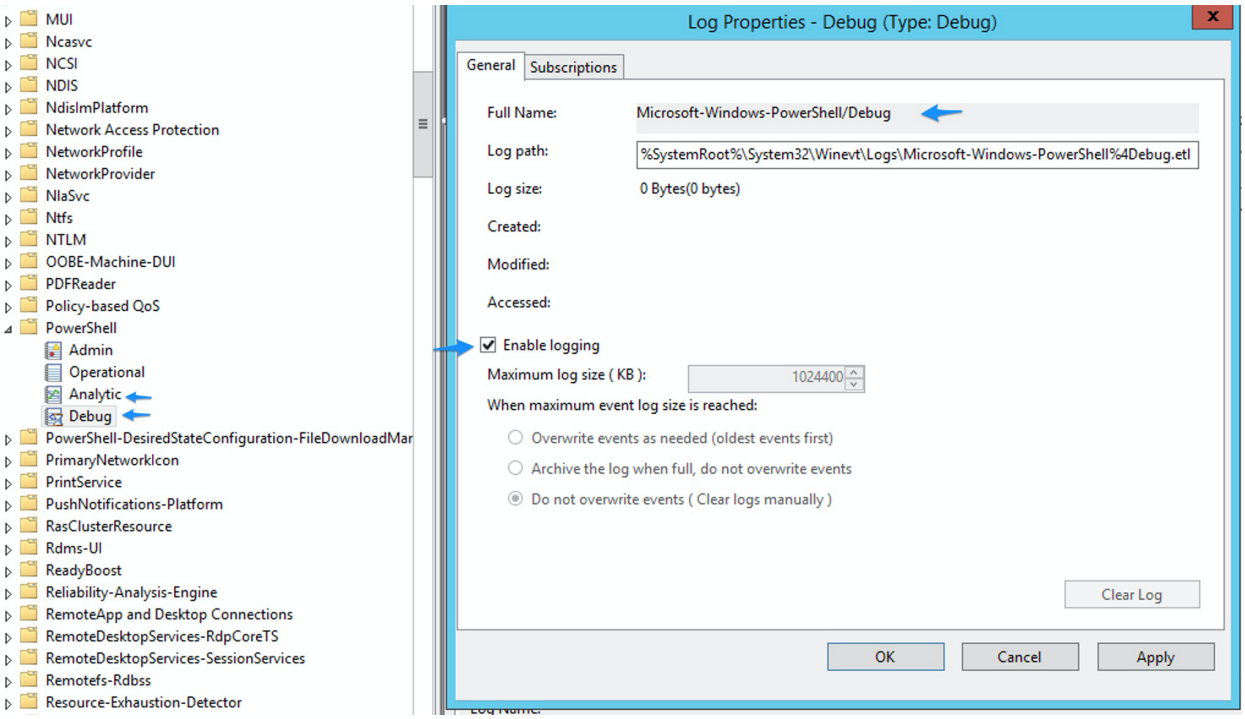
## Configuring Generic Binary Logs

Analytic and Debug logs are disabled by default, because these logs can quickly fill the disk with a large number of entries.

For this reason, you will probably want to turn them on for a specified period to gather some troubleshooting data and then turn them off again.

Follow these steps to configure FortiSIEM Windows Agent to collect Generic Binary logs:

1. Enter `eventvwr.msc` at an elevated command prompt and press **Enter** to open the Event Viewer.
2. In the Event Viewer, navigate to **Applications and Services Logs > Microsoft > Windows >**, then select an **Application** that needs to capture Analytic/Debug logs.
3. Right-click **Application**, point to **View**, and click **Show Analytic and Debug Logs**. The **Analytic/Debug/Diagnostic** log is displayed.
4. Right-click **Analytic/Debug/Diagnostic** and then click **Properties**.
5. Under **When maximum event log size is reached**, choose **Do not overwrite events (Clear logs manually)**.
6. Select the **Enable logging** checkbox, and click **OK** when you are asked if you want to enable this log. See the following example “PowerShell Debug logs”.




7. Click **OK** again to enable the **Application Analytic/Debug/Diagnostic** event log.
8. Note the **Full Name** in the screenshot in Step 6: **Microsoft-Windows-PowerShell/Debug**. This name must be entered in FortiSIEM.

## 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, and 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.



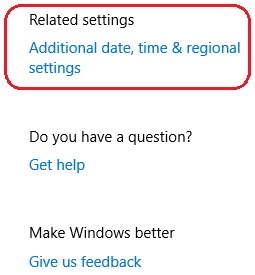
# Configuring Locale on Windows Servers



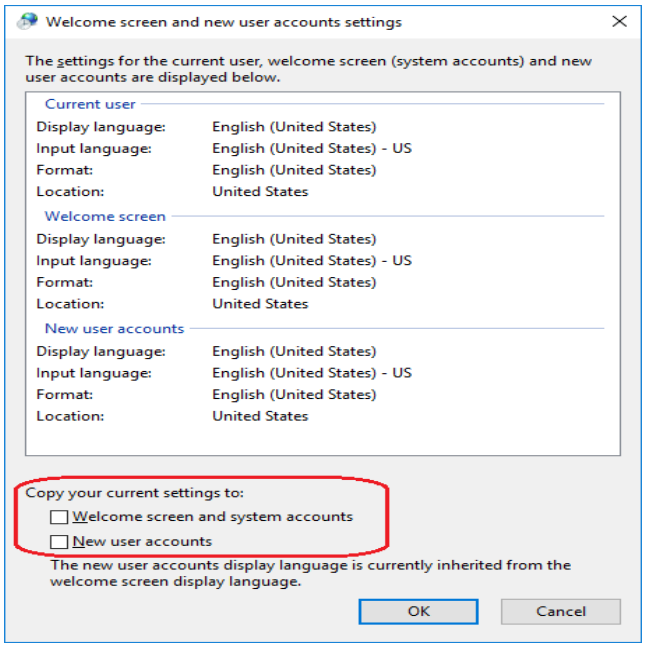
### Configure Locale on Windows 10

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.



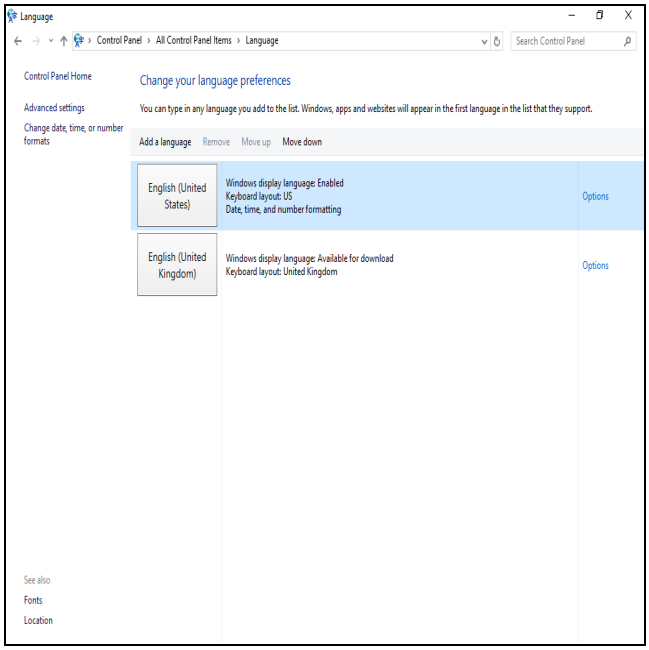

6. Choose the option **Region** and open the **Administrative** tab.
7. Click the **Change system locale...** button and change the locale to **English (United States)** in the provided dialog box. Click **OK**.
8. In the **Administrative** tab, click the **Copy Settings...** button.
9. In that property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



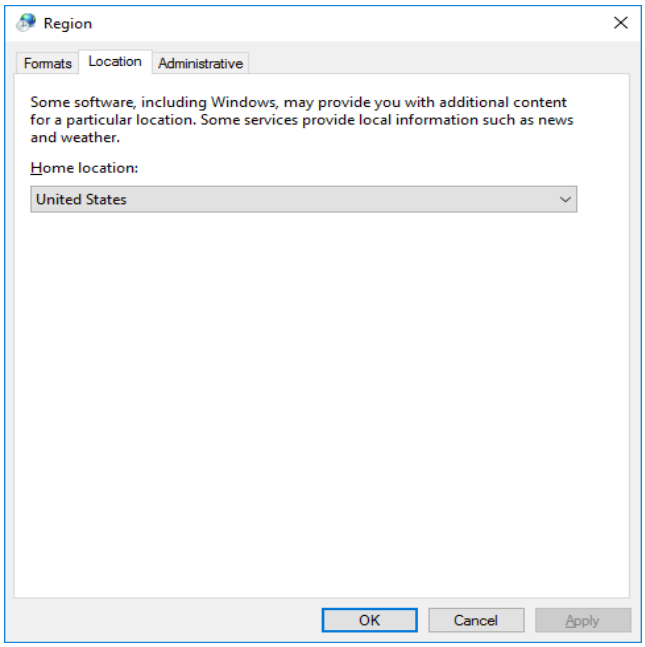

10. Restart your computer.

### Configure Locale on Generic Servers

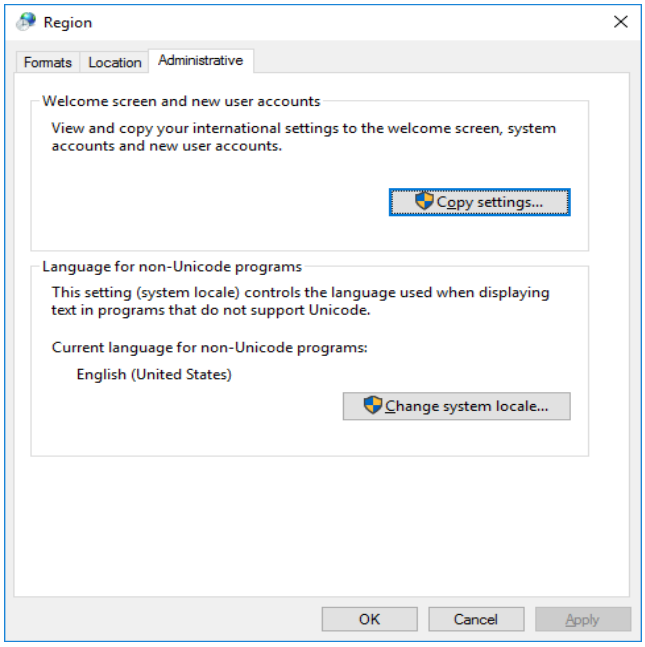
1. Go to the **Control Panel**.
2. Choose the **Language** option.
3. Select the language **English (United States)** and move it to top of the list.
4. Select the option **Change date, time, or number formats** on the left side of the page.



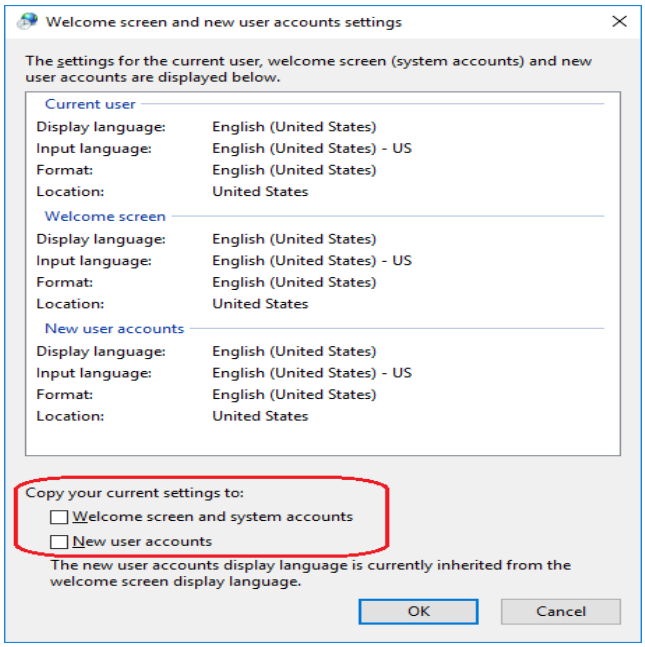
5. In this property page tab, select the **Location** tab and choose the **Home Location** as **United States**. Click **Apply**.




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 examle, **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):

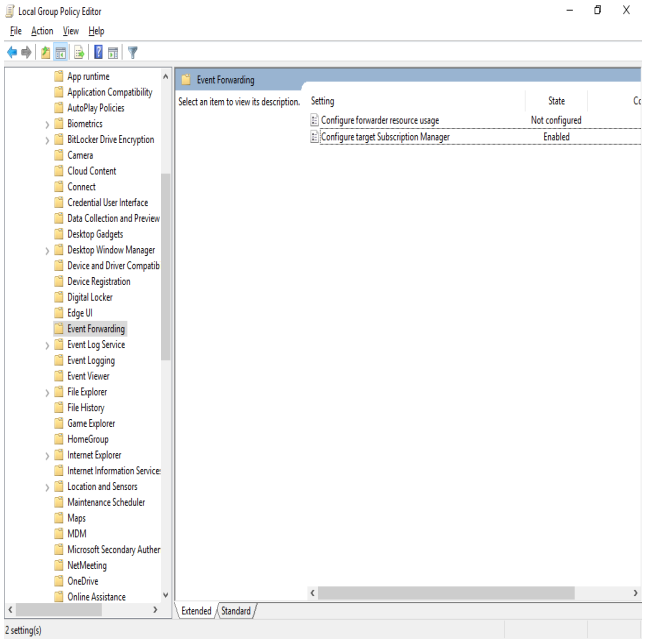
   ```
   netsh advfirewall firewall add rule name="Winrm HTTP Remote Management" protocol=TCP
   dir=in localport=5985 action=allow

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

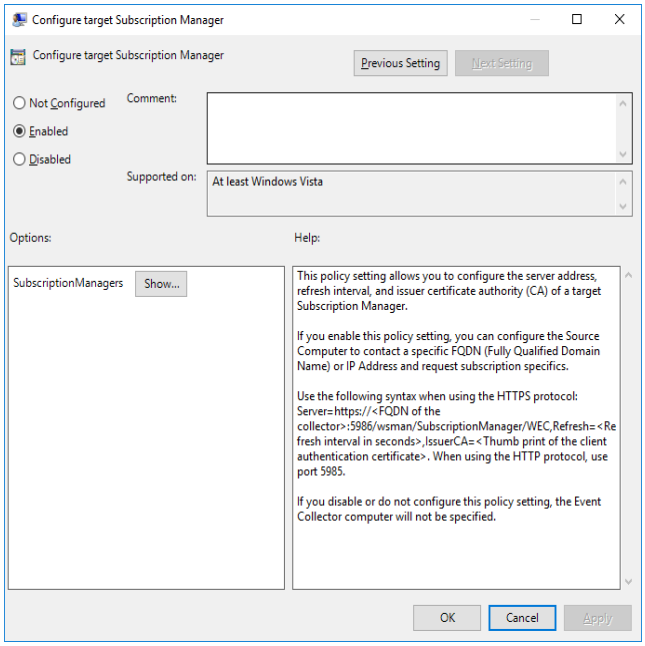
**Configure the Domain Controller or Source Computer**

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

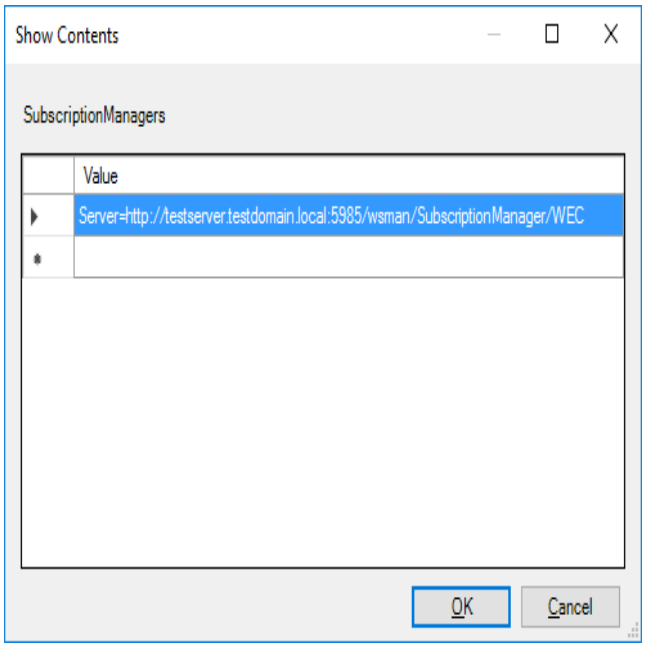
1. Run the local group policy editor (*for non-domain environments*) or the domain group policy editor (*for domain environments*).
2. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Event Forwarding**.



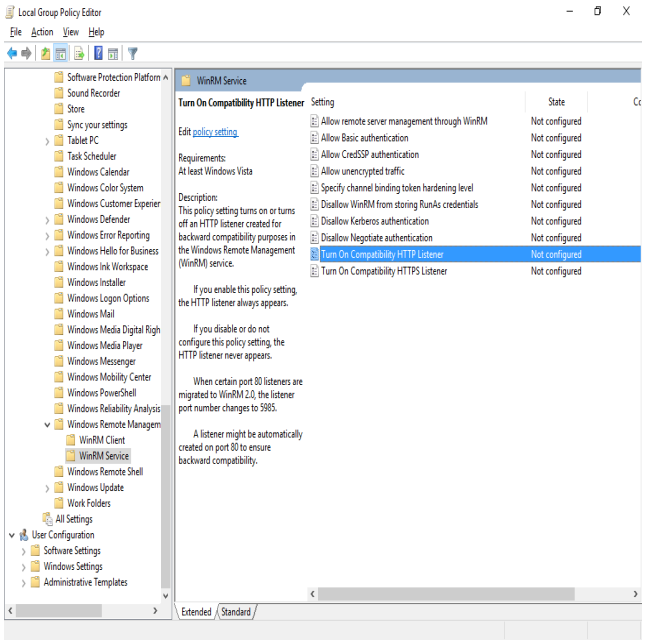

3. Open **Configure target Subscription Manager**.




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**.

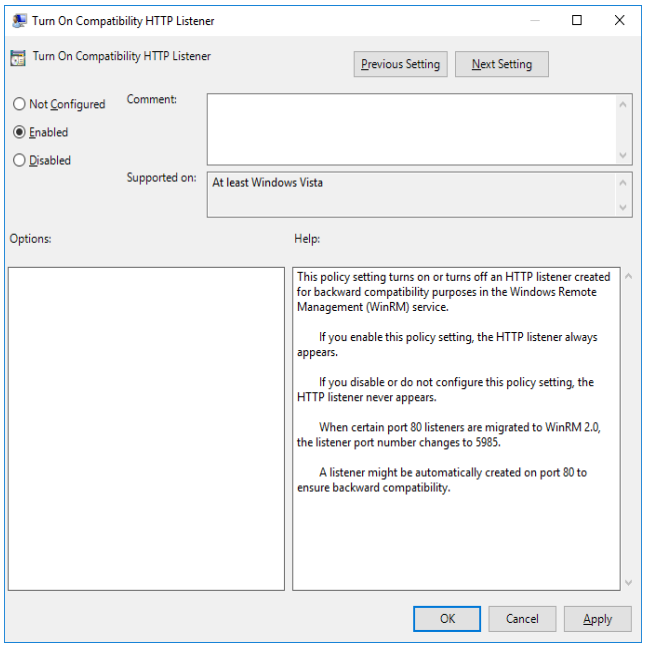



7. In the **Configure target Subscription Manager** dialog box, click **Apply** and then **OK**.
8. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management > WinRM Service**.




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 Audit File System Policy

### Configure Security Audit Logging Policy

Configure this policy to control Windows logging. Because Windows generates many 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 | For auditing log in activity. | Select **Success** and **Failure**. |

| Policy | Description | Settings |
|---|---|---|
| events | | |
| 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, *Configuring File Auditing Policy*. | Select **Success** and **Failure**. |
| Audit system events | Includes system up/down messages. | |

5. For an Enterprise Server's Domain Group Policy, make sure you set the following under **Group Policy > Local Policies > Audit Policy**:
   **Policy = Audit object access**
   **Security Setting = Success or Failure**

## Configure File Auditing Policy

Configure this policy to see user meta data in file auditing events.

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.

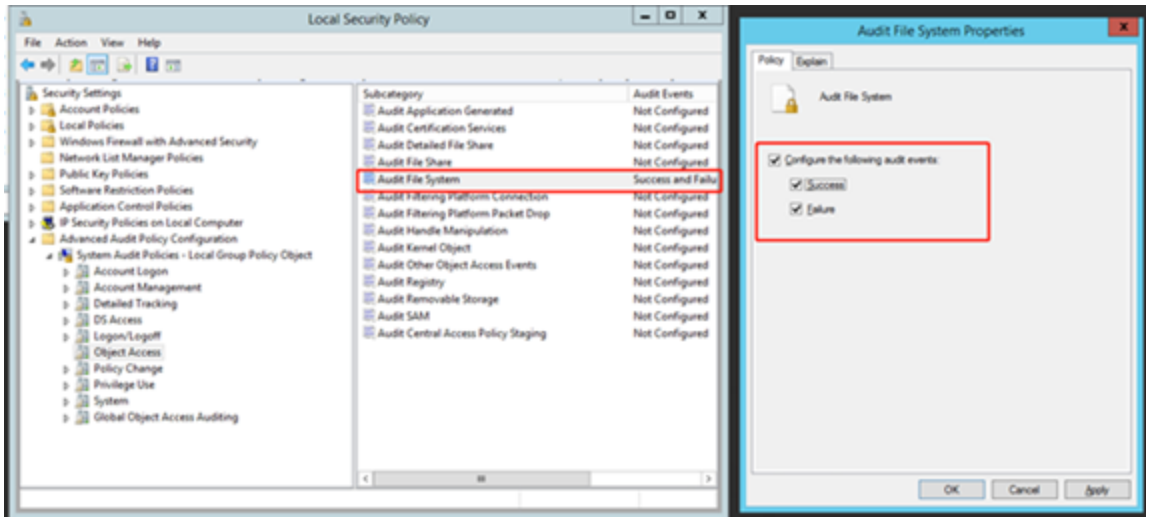
## Configure Audit File System Policy

Configure this policy to enable change events for permission and/or ownership changes to files and/or directories. The policy will also upload the monitored files to FortiSIEM. This feature is available in FortiSIEM Windows Agent 4.x.x.

Complete these steps to enable Audit File System policy:

1. Log in, with administrator privileges, to the machine where you want to set the policy.
   On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand the **Advanced Audit Policy Configuration** node.
4. Expand **System Audit Policies-Local Group Policy Object** node.
   You will see the current security audit settings.
5. Select **Object Access**.
6. Select **Audit File System** on the left side of the window.
7. Double-click **Audit File System**. In the pop-up window, select both **Success** and **Failure** under **Configure the following audit events**.

8. Click **Apply**, then **OK**.




The Audit File System Policy is now enabled. Reboot your system to apply the changes.

## 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**.

# Configuring Monitoring Policies in FortiSIEM

After you have configured Windows Servers in the previous step (Configuring Windows Servers for FortiSIEM Agents), you must create monitoring policies in FortiSIEM. For more information, see Define the Windows Agent Monitor Templates and Associate Windows Agents to Templates in the FortiSIEM User's Guide.

# Verifying Events in FortiSIEM

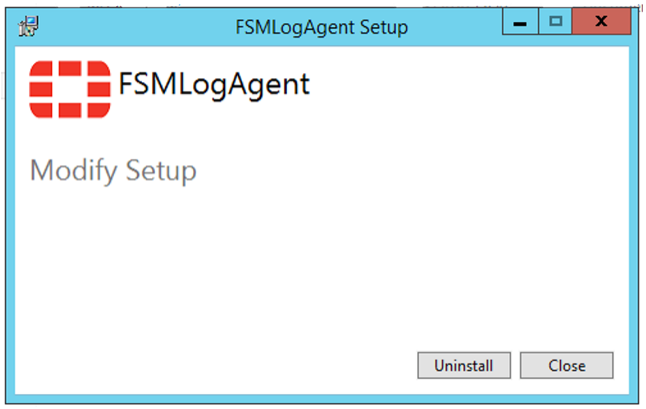
Follow the steps below to verify the events in FortiSIEM:

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

To uninstall FortiSIEM Windows Agent, run the FortiSIEM Installer. When prompted, click **Uninstall**.




# 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

For sample Windows Agent logs, see Sample Windows Agent Logs in the FortiSIEM User's Guide.