SIEM COLLECTOR WINDOWS INSTALLATION GUIDE

Summary

This will provide documentation on the installation process of the SIEM collector on Microsoft Windows. It documents both the installation using the graphical user interface as well as a console install process.

Terms

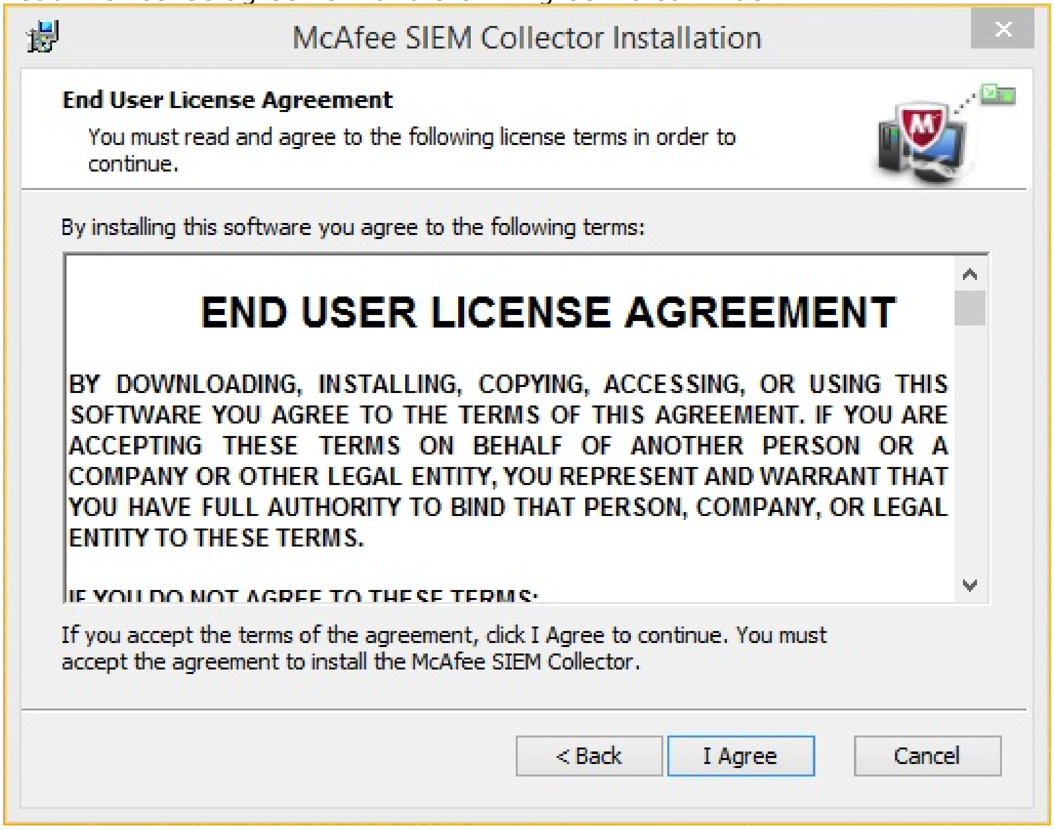
- SIEM - Security Information Event Management

GRAPHICAL USER INTERFACE INSTALLATION METHOD

```
This installation method is for use with the "SiemCollector11.exe" executable.  The SIEMCollect
orInstaller.msi installation file should NOT be used for manual installation, but console insta
llation only.  Console installation is described below.
```

1. Double-click the installer executable to begin installation.

    1. Please read the installation overview and click “Next” to continue.
    2. Read the license agreement and click “I Agree” to continue.



End User License Agreement

You must read and agree to the following license terms in order to continue.

By installing this software you agree to the following terms:

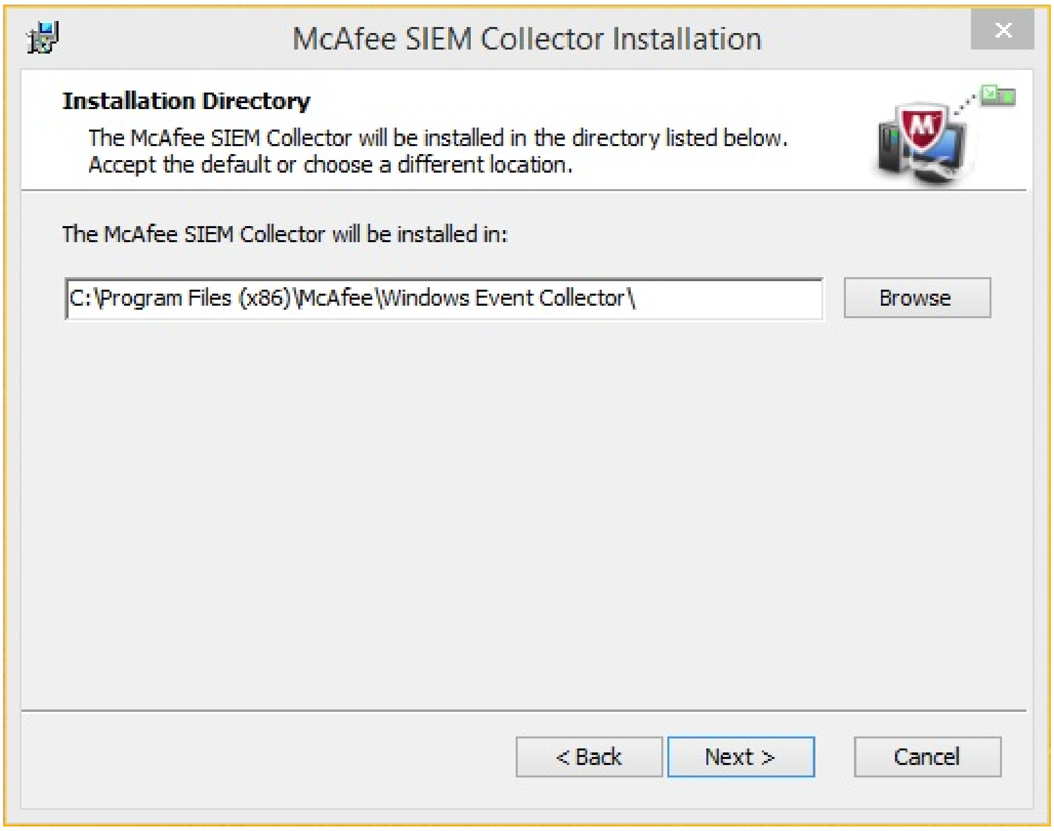
END USER LICENSE AGREEMENT

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THIS SOFTWARE YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS.

IF YOU DO NOT AGREE TO THESE TERMS:

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install the McAfee SIEM Collector.

    3. Confirm your installation directory and click “Next” to continue..


McAfee SIEM Collector Installation

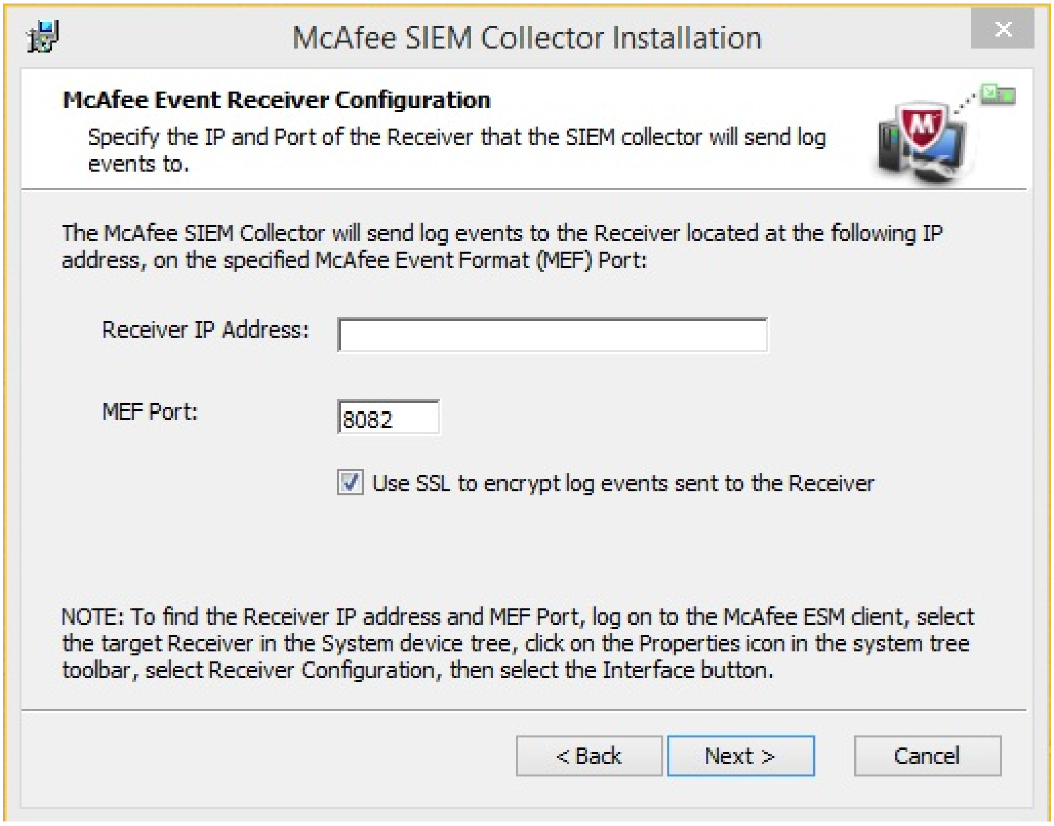
Installation Directory

The McAfee SIEM Collector will be installed in the directory listed below. Accept the default or choose a different location.

The McAfee SIEM Collector will be installed in:

C:\Program Files (x86)\McAfee\Windows Event Collector\

4. Now you will see the McAfee Event Receiver Configuration screen. In this window you configure the SIEM Collector to communicate with a specific Receiver. Type the IP address of the Receiver to which you would like the SIEM Collector to forward events. You can also change the port and specify whether or not the SIEM Collector will use SSL to communicate with the Receiver.


McAfee SIEM Collector Installation

McAfee Event Receiver Configuration

Specify the IP and Port of the Receiver that the SIEM collector will send log events to.

The McAfee SIEM Collector will send log events to the Receiver located at the following IP address, on the specified McAfee Event Format (MEF) Port:

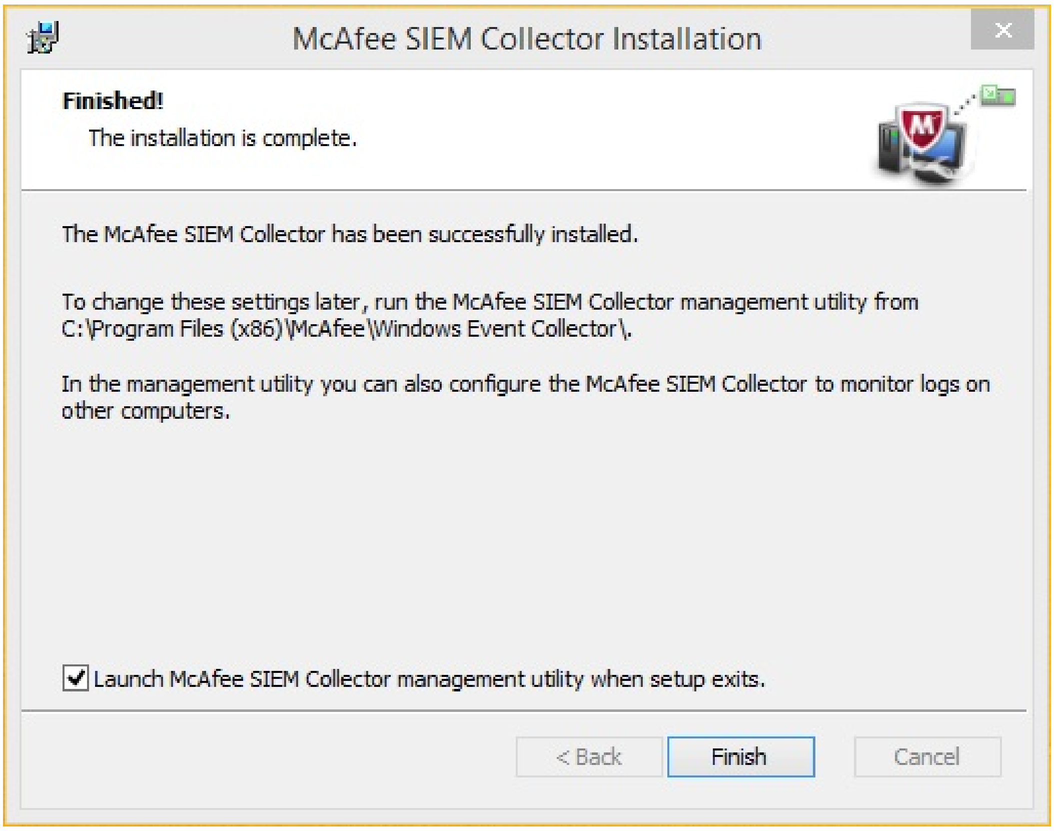
Receiver IP Address:

MEF Port: 8082

☑ Use SSL to encrypt log events sent to the Receiver

NOTE: To find the Receiver IP address and MEF Port, log on to the McAfee ESM client, select the target Receiver in the System device tree, click on the Properties icon in the system tree toolbar, select Receiver Configuration, then select the Interface button.

5. When you click “Next”, the SIEM Collector will be installed.



McAfee SIEM Collector Installation

Finished!

The installation is complete.

The McAfee SIEM Collector has been successfully installed.

To change these settings later, run the McAfee SIEM Collector management utility from C:\Program Files (x86)\McAfee\Windows Event Collector\.

In the management utility you can also configure the McAfee SIEM Collector to monitor logs on other computers.

☑ Launch McAfee SIEM Collector management utility when setup exits.

CONSOLE INSTALLATION METHOD

```
This installation method utilizes the SIEMCollectorInstaller.msi installer file.
```

1. The following parameters are optional but will minimize any configurations that need to occur post installation. * INSTALLOCATION – Input: Directory path, the directory to install the SIEM collector software to. * CONFIGFILE - Input: properly formatted XML or .txt file, a path to a configuration file defining the collector installation parameters.

1. Console install example:

```
msiexec /i WindowsAgentInstaller.msi /quiet INSTALLLOCATION=”C:\Program Files (x86)”  CONFIGFILE=”c:\temp\config.txt”
```

2. The above example command can be ran with 3rd party applications to install the SIEM Collector on several nodes within your network.

CONFIGURATION FILE OVERVIEW

```
<EventCollectorConfig log_level="diag|debug|warn|info|err" log_size="">
  <credentials user="" pass="" b64pass="" domain="" />
  <receiver ip="" port="" use_ssl="yes|no" />
  <group name="" use_parent_logging="yes|no" log_level="diag|debug|warn|info|err" use_parent_credentials="yes|no">
    <credentials user="" pass="" b64pass="" domain="" />
    <host name="" ip="" use_parent_logging="yes|no" log_level="diag|debug|warn|info|err" use_parent_credentials="yes|no">
      <credentials user="" pass="" domain="" />
      <plugin hostid="" name="" type="win_evt|file_evt|file|c2">
        <config key="" value="" />
      </plugin>
    </host>
  </group>
</EventCollectorConfig>
```

TROUBLESHOOTING

If you are experiencing issues with installations these are some common troubleshooting tips:

1. Make sure you install the SIEM Collector with root privileges.
2. Refer to the Configuration File Overview if Receiver, group, and plugin configurations are not loading properly.

Upgrading

The SIEM Collector version 11 installations described above will automatically attempt to upgrade a previous version 10 installation in the same installation directory. The SIEM Collector version 11 will only upgrade from the an existing installation having version 10.02 or later. If you are not running at least 10.02, please upgrade to at least 10.02 before attempting the upgrade.

The upgrade will reuse your existing configuration and bookmarks. If you "Apply" configuration changes in the SIEM Collector version 11 UI, it will also read external SQL configuration files and add them to the newly written config.xml. SIEM Collector version 11 no longer references external .xml files for SQL configurations. All new SQL configurations will also be written to the config.xml file.

If you are planning to downgrade from version 11 back to version 10, make certain to make a copy of the "Plugins" directory and the "config.xml" located in the SIEM Collector installation directory before upgrading. Bookmark formats have not changed between version 10 and 11, but the config.xml formatting has changed and may no longer be readable by the previous version.

Downgrading

It is possible to uninstall version 11 and return to version 10. Doing so, however, will lose configuration changes added in version 11.

To downgrade, perform the following steps:

1. Copy the config.xml and Plugins directory from the installation directory to a safe location. This should not be the same backup location used for the backups you may have made before upgrading.
2. Uninstall the SIEM Collector version 11 using Window's uninstallation process.
3. Confirm that the installation directory is empty.
4. Install the SIEM Collector version 10.
5. Make certain that the none of the SIEM Collector applications are running. Stop the service.
6. Copy the Plugins directory from step 1 into the installation directory. Do not delete the existing Plugins directory before copying. This will make certain that your bookmarks will be available to the new installation.
7. If you have a copy of your original version 10 config.xml that you saved before upgrading, copy that into the installation directory. Your downgrade has been completed.
8. If you do not have a copy of your original version 10 config.xml, remake your configuration using the SIEM Collector management utility.
9. Now that you have your config.xml from step 1 and your new configuration, contact support to associate your new configuration with your existing bookmarks.

Known Issues

- You must be running the latest version of SIEM Collector version 10 to be able to upgrade to version 11.
- The SIEM Collector will not warn you if you have issues with configuration file formatting.
- If installing SIEM Collector 11 on Windows 2003 (x64) or Windows XP (x64) there are two required packages:
  - Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)
  - Microsoft Visual C++ 2008 Redistributable Package (x86)
- If the SIEM Collector is installed on a machine running Windows 2003 or Windows XP and assigned a configuration to collect Windows events from a client running Windows 10 or Windows Server 2012 may lead to a service crash. To mitigate this issue, install the SIEM Collector on 2008/Vista or newer if you need to collect logs from Windows 10 or Server 2012.

Download PDF