

Splunk Cloud

Splunk App for Windows Infrastructure – MS Windows AD Objects

Quick Start Guide

This guide is for either *Current Splunk Cloud Customers* or for performing a *Splunk Cloud Trial* leveraging the **Splunk® App for Windows Infrastructure, MS Windows AD Objects**, and **Splunk Windows TA(s)** applications to analyze Microsoft Windows data with Splunk. After performing each of the 4 steps outlined in this document you will be able to take full advantage of the built-in intelligence and in-depth analysis of your Windows.

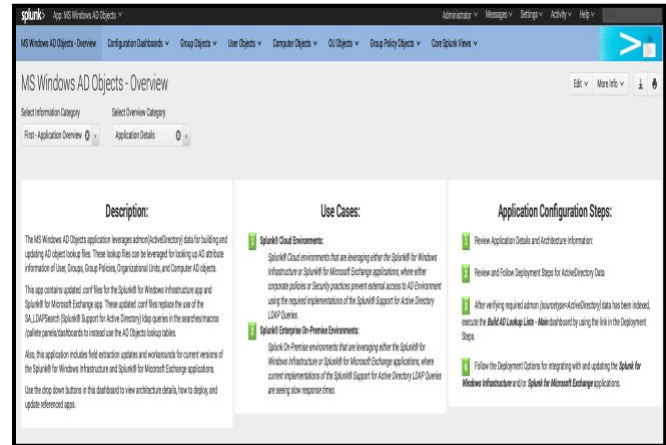
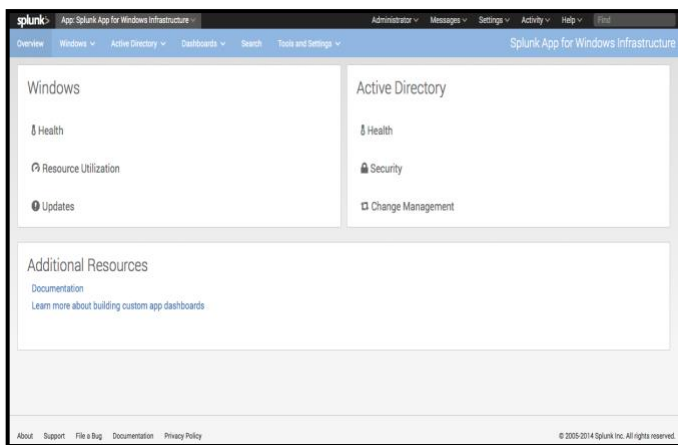


Table of Contents

| | |
|--|-----------|
| Splunk App for Windows Infrastructure and MS Windows AD Objects application Overview | 2 |
| Splunk App for Windows Infrastructure and MS Windows AD Objects Architecture..... | 2 |
| Installation Steps Overview..... | 3 |
| Collected and used Windows Data Details..... | 3 |
| Permission Requirements..... | 3 |
| Step 1: Splunk Cloud Environment Configuration | 4 |
| Step 2: Download Splunk Technical Add-Ons and Update Data Inputs..... | 4 |
| Application Details and Download links..... | 4 |
| Configure and Update the Data Inputs | 6 |
| Step 3: Splunk Universal Forwarder Installation on Target Windows Systems and AD DC's | 7 |
| Required Pre-Installation Step: Set PowerShell Execution Policy | 7 |
| Installing the Splunk Universal Forwarder, Splunk Cloud App for Universal Forwarder and Splunk TA(s) | 7 |
| Step 4: Complete Setup of Splunk App for Windows Infrastructure and MS Windows AD Objects..... | 9 |
| Splunk App for Windows Infrastructure: <i>Start the Initial Setup Wizard</i> | 9 |
| MS Windows AD Objects: <i>Build the initial AD Objects lookup files</i> | 10 |
| Appendix A – Splunk Current Cloud Customers – Support Case Steps..... | 11 |
| Appendix B – Troubleshooting missing admon baseline or AD MSAD Health data..... | 12 |
| Appendix C – Troubleshooting Splunk Communication Issues..... | 13 |
| Appendix D – Enable Auditing in the Active Directory Environment..... | 16 |

Splunk App for Windows Infrastructure and MS Windows AD Objects application Overview

The **Splunk® App for Windows Infrastructure** application gives you insight into your Microsoft Windows and Active Directory deployment with pre-built, in-depth, content that provides enterprise-wide analysis of configuration, health and security.

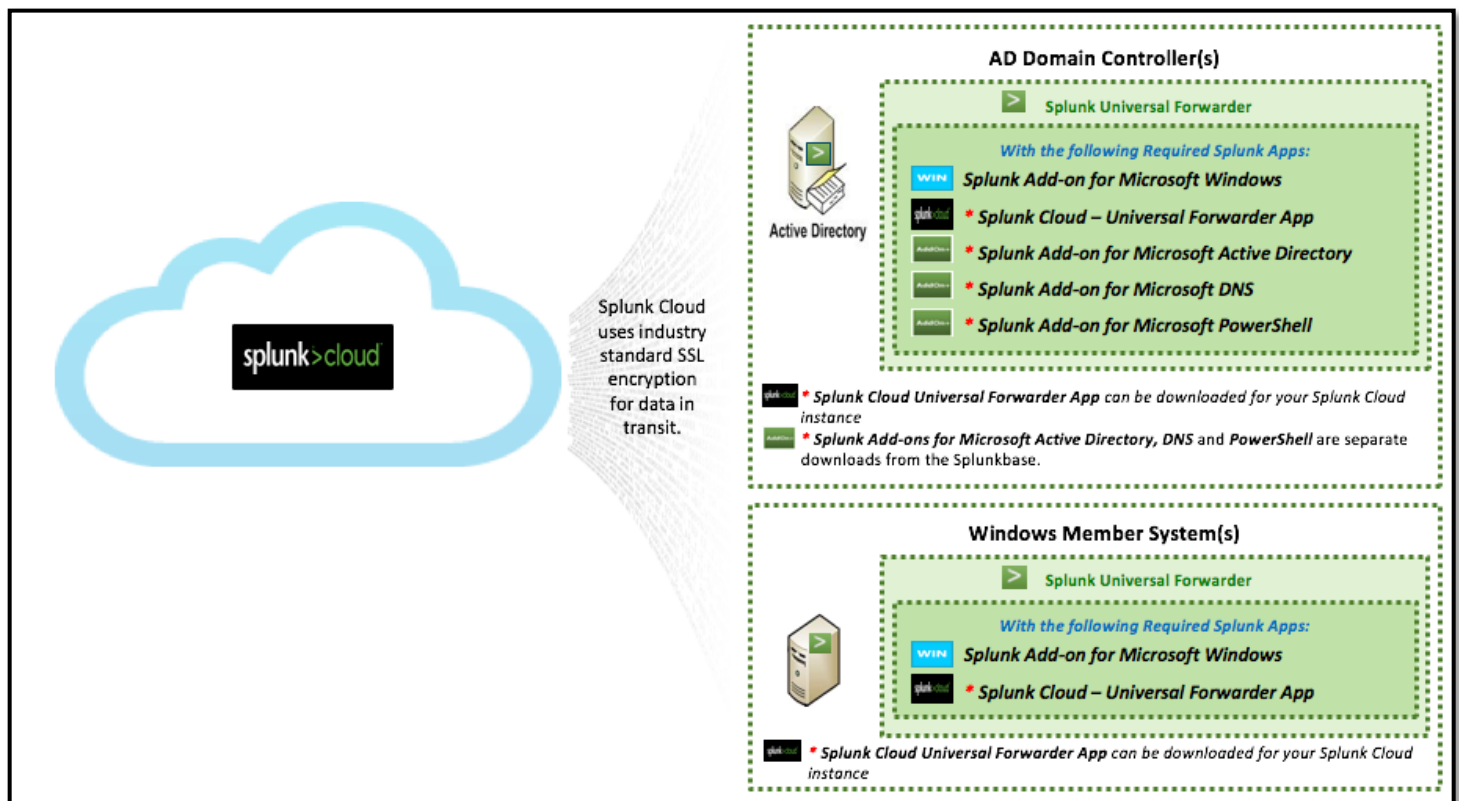
The **Splunk® Add-on for Windows** provides data inputs for Windows management. The add-on comes with a set of file, event log, performance monitoring, and other inputs for collecting CPU, disk, I/O, memory, log, configuration, and user data.

The **Splunk® Add-on for Microsoft Active Directory** provides the necessary Active Directory knowledge objects for a Splunk App for Microsoft Exchange or Splunk App for Windows Infrastructure deployment.

The **Splunk® Add-on for Microsoft DNS** provides the necessary Windows DNS Server knowledge objects for a Splunk App for Microsoft Exchange or Splunk App for Windows Infrastructure deployment.

The **MS Windows AD Objects** application leverages **admon** data for building and updating local AD Objects Splunk lookup files. These lookup files can be leveraged for looking up the latest (< 10 Minutes) AD attribute information of User, Groups, Group Policies, Organizational Units, and Computer AD objects. Also, this app contains updated .conf files for the **Splunk® App for Windows Infrastructure** for replacing the use of the **Splunk® Support for Active Directory** ldap queries in the searches/macros/palette panels/dashboards to instead use the local Splunk AD Objects lookup files.

Splunk App for Windows Infrastructure and MS Windows AD Objects Architecture



NOTE: A Splunk Universal Forwarder is recommended on each AD Domain Controller targeted for analyzing AD data with Splunk.

Installation Steps Overview

Below is an overview and order of steps for installing and configuring the *Splunk® App for Windows Infrastructure* and *MS Windows AD Objects* applications.

- 1) **Work with Splunk Cloud Ops or your Splunk Sales team to prepare Splunk Cloud Environment**
 - a) **Splunk Cloud Trials:** Contact Splunk Sales Contact for getting the Splunk Cloud Trial instances configured.
 - b) **Current Splunk Cloud Customers:** Open a Splunk Support Ticket to add the required *Splunk Windows Apps* and *Add-Ons* to Splunk Cloud systems (See [Appendix B](#)).
- 2) **Download Splunk Technical Add-Ons and Update Data Inputs:**
 - a) Download Splunk Applications, and perform initial configuration of data inputs.
- 3) **Splunk Universal Forwarder Installation on Target Windows Systems and AD DC's:**
 - a) Install *Splunk Universal Forwarder* on the target Windows Member and Domain Controllers.
 - b) Add the Technical Add-Ons to target Windows Member Servers and Domain Controllers.
- 4) **Complete application setup:**
 - a) Update and complete setup of the *Splunk App for Windows Infrastructure* application.
 - b) Complete Setup, and Configure the *MS Windows AD Objects* application

Collected and used Windows Data Details

Windows and Active Directory data the [Splunk App for Windows Infrastructure](#) collects using the Splunk TA(s):

- Windows event logs:
 - Security, Application, System
 - Distributed File System Replication (DFSR)
 - NT File Replication Services (FRS)
 - DNS Server
- Active Directory schema baseline and changes (through Splunk's Active Directory monitoring input)
- PowerShell Scripts:
 - Active Directory forest-wide health, information and replication statistics
 - DNS server health and information
- Domain controller health and performance metrics
 - Memory, CPU, disk, network, and NTDS operations and connectivity performance counters
- General Windows host, printer, and network information

Active Directory data the [MS Windows AD Objects](#) Uses:

- This App leverages the ActiveDirectory (admon) data collected by the [Splunk Add-On for Microsoft Active Directory](#) deployed to the Active Directory Domain Controller's with the Splunk Universal Forwarder

Permission Requirements

Below are the permission requirements for the [Splunk App for Windows Infrastructure](#), leveraged [Technical Add-ons](#), and [MS Windows AD Objects](#):

- **Technical Add-Ons: (Splunk TA windows, Splunk TA microsoft ad, and Splunk TA microsoft dns)**
 - To run these Splunk Technical Add-On's on either a Windows member server or an AD Domain Controller, it is recommended to run the Splunk Service Account as **Local System**.
 - If corporate policy requires that you run application services as a Domain Account, then make sure the specified account has "Full Permissions" to the `/Program Files/SplunkUniversalForwarder/..` directory and also make sure the specified account is set as the "Owner" for the complete directory.
 - The `Splunk_TA_microsoft_ad` Technical Add-On leverages Powershell Scripts to collect AD Topology, and other key AD Health data; so the **Powershell Execution-Policy** needs to be set to atleast RemoteSigned on the AD Domain Controllers using these TA's.
- **No extra permissions required for the MS Windows AD Objects application.**

Step 1: Splunk Cloud Environment Configuration

The **Splunk® App for Windows Infrastructure** and **MS Windows AD Objects** applications require some configuration on the Splunk Cloud instances. This installation and configuration needs to be completed by the Splunk Cloud's Operations team or through your Splunk Sales technical team, depending on if it is a Splunk Cloud Trial or a current Splunk Cloud customer environment.

- **Splunk Cloud Trials:** Contact Splunk Sales Contact for getting the Splunk Cloud Trial instances configured.
- **Current Splunk Cloud Customers:** Open a Splunk Support Ticket to add the *Required Splunk Applications* to Splunk Cloud systems (Follow Steps outlined in [Appendix A](#)).

Step 2: Download Splunk Technical Add-Ons and Update Data Inputs

Below are preparation steps for installing the Splunk Universal Forwarder on the targeted Windows Systems and AD Domain Controllers.

Application Details and Download links

Below is a list of the Splunk required technical addons for each role of the targeted Windows systems. Use the below "blue" hyperlinks to download the required **Splunk Universal Forwarder**, **Splunk Cloud Universal Forwarder App**, **Splunk Add-On for Windows**, **Splunk Add-On for Microsoft Active Directory**, **Splunk Add-On for Microsoft DNS**, and **Splunk Add-On for Microsoft PowerShell**.

It is recommended to download, extract, and copy the below **Splunk Universal Forwarder** and **Splunk TA's** into a created Windows directory that is accessible by the targeted Windows/AD Systems. For this document this will be referred to as the **target_share_folder**. This way you can make the configuration changes outlined below in a central place before placing them on the Splunk Universal Forwarder.

- **Note:** : If downloading these TA's to a Windows System, then you can use 7-zip([7-Zip installation site](#)), or another tar extracting application, to extract the below applications.
- **Splunk Universal Forwarder**
 - From your Splunk Cloud UI, navigate into **Splunk Cloud UI → Apps → Universal Forwarder** application.
 - Click the **Download the Splunk Universal Forwarder** button and then copy the downloaded **splunkforwarder...msi** file into the **target_share_folder**.
 - Or you can download it from [Splunk Universal Forwarder](#).
- **Splunk Cloud Universal Forwarder App**
 - From your Splunk Cloud UI, navigate into **Splunk Cloud UI → Apps → Universal Forwarder** application
 - Click the **Download your Splunk Cloud Universal Forwarder app** and then copy the downloaded **splunkclouduf.sp** file into the **target_share_folder**.
 - This app contains custom secure certificates and outputs settings to connect specifically to your Splunk Cloud.
- **Splunk TA for other Windows Targeted Systems (Non-Active Directory Domain Controllers):**
 - First, in your **target_share_folder** create a sub-folder called **Base_Windows**.
 - **Note:** The creation of the **Base_Windows** folder is just to separate out what TA's get deployed to which system type. Make sure that you **do not** copy the **Base_Windows** folder, but just the contents, to the Splunk Universal Forwarders **C:/Program Files/SplunkUniversalForwarder/apps/** directory.
 - **Splunk Technical Add-ons for core Windows data:**
 - [Splunk Add-On For Windows](#) (*Splunk_TA_windows*)
 - Click the above link to download the TA, then extract the **splunk-add-on-for-microsoft-windows_.....tgz** and copy the **Splunk_TA_windows** to the **target_share_folder/Base_Windows**.
- **Splunk TA's for AD Domain Controllers:**
 - First, in your **target_share_folder** create a sub-folder called **AD_DomainControllers**.
 - **Note:** The creation of the **AD_DomainControllers** is just to separate out what TA's get deployed to which system type. Make sure that you **do not** copy the **AD_DomainControllers** folder, but just the contents, to the Splunk Universal Forwarders **C:/Program Files/SplunkUniversalForwarder/apps/** directory.
 - **Splunk Technical Add-ons for core Windows data:**
 - ****Note:** Copy the **Splunk_TA_Windows** folder from the **target_share_folder/Base_Windows** directory and place it into the **target_share_folder/AD_DomainControllers** directory.
 - **Splunk Technical Add-ons for Active Directory and DNS Data:**
 - [Splunk Add-On for Microsoft Active Directory](#) (*Splunk_TA_microsoft_ad*)

- Click the above link to download the TA, then extract the **splunk-add-on-for-microsoft-active-directory_....tgz** and copy the **Splunk_TA_microsoft_ad** to the **target_share_folder/AD_DomainControllers** directory.
- **Splunk Add-On for Microsoft DNS** (*Splunk_TA_microsoft_dns*)
 - Click the above link to download the TA, then extract the **splunk-add-on-for-microsoft-windows_dns_....tgz** and copy the **Splunk_TA_microsoft_dns** to the **target_share_folder/AD_DomainControllers** directory.
- **Splunk Add-On for Microsoft PowerShell** (*SA-ModularInput-PowerShell*)
 - Click the above link to download the TA, then extract the **SA-ModularInput-PowerShell...tgz** and copy the **SA-ModularInput-PowerShell** to the **target_share_folder/AD_DomainControllers** directory.

Configure and Update the Data Inputs

Below are the steps for configuring the data inputs for the Splunk Add-Ons downloaded in the previous step.

Base Windows Inputs:

- 1) Navigate to the **target_share_folder/Base_Windows/Splunk_TA_Windows/default** directory.
- 2) Copy the **inputs.conf** file.
- 3) Navigate up to the **target_share_folder/Base_Windows/Splunk_TA_Windows** directory.
- 4) Create a new folder, named **local**.
- 5) Navigate into the **local** directory
- 6) Paste the **inputs.conf** previously copied into the **target_share_folder/Base_Windows/Splunk_TA_Windows/local** directory.
- 7) Using a text editor, ie Wordpad/Notepad++/etc, open the pasted **inputs.conf** file.
- 8) Scroll through each of the stanzas, ie the square brackets [...], and change the text **disabled = 1** to **disabled = 0** for each of the data inputs you want to enable.
 - a) **Optional Notes:**
 - i) **Performance Monitoring Interval:** As a recommendation, it is suggested to up the interval setting for the perfmom data inputs from **interval = 10**, which is every 10 seconds, to something like **interval=60** or some other greater interval depending on your specific needs.
 - ii) **Minimum Enabled Inputs:** It is recommended to enable the following inputs, as a minimum, for the *Splunk App for Windows Infrastructure* application.
 - (1) [WinEventLog://Application]
 - (2) [WinEventLog://Security]
 - (3) [WinEventLog://System]
- 9) **Save** the updated information to the **inputs.conf**.

AD Domain Controllers Inputs:

- 1) Navigate to the **target_share_folder/Base_Windows/Splunk_TA_Windows/local** directory.
- 2) **Copy** the previously configured **inputs.conf** file and place into the **target_share_folder/AD_DomainControllers/Splunk_TA_Windows/local**.
 - i) **Optional Note:** After you copy the **inputs.conf** file from the *Splunk_TA_windows* directory, you can optionally adjust it to enable/disable/update different data input settings for your Active Directory Domain Controllers.
- 3) Enable admon "baseline" data collection that is **required** and leveraged by the **MS Windows AD Objects** application.
- 4) Navigate to the **target_share_folder/AD_DomainControllers/Splunk_TA_microsoft_ad** directory and create a new folder, named **local**
- 5) Navigate into the **local** directory.
 - a) Create a new file named **inputs.conf** and open it with a text editor.
 - b) Add the following text into the **inputs.conf** file to update the default admon (Active Directory) data input to collect and index **baseline** data along with the already configured **update/delete** data.

```
[admon://NearestDC]
baseline = 1
disabled = 0
```
 - c) Save the updated information to the **inputs.conf**.
 - d) Create a new file named **admon.conf** in the same **local** directory and open it with a text editor.
 - e) Add the following text into the **admon.conf** file.

```
[NearestDC]
disabled = 0
monitorSubtree = 1
baseline = 1
```
 - f) Save the updated information to the **admon.conf**.

After completing the above steps you are now ready for **Step 3**, installing the Splunk Universal Forwarders and adding the updated Splunk TA's to your target Windows Systems and Windows AD Domain Controllers.

Step 3: Splunk Universal Forwarder Installation on Target Windows Systems and AD DC's

Below are the steps for setting up the **Splunk Universal Forwarder**, **Splunk Cloud App for Universal Forwarders**, **Splunk Technical Add-on** apps, and **PowerShell** execution policy on the target Windows Servers and AD Domain Controllers.

Required Pre-Installation Step: Set PowerShell Execution Policy

We need to verify and possibly update **PowerShell's Execution Policy** so that the Splunk TA's for Active Directory and Exchange can execute their PowerShell scripts to collect topology, health, etc data from those environments. (Click [here](#) for more details)

- **NOTE:** This Pre-Step is only required for **Active Directory Domain Controllers ONLY**
- 1) Log into the targeted AD Domain Controller(s) using a *Domain Account* with software installation permissions.
- 2) Go to **Start-->Programs-->Accessories-->Powershell** and **right-click** on the PowerShell icon to select **Run As Administrator**.
- 3) Type **get-executionpolicy** in the powershell command window to check the current setting.
 - a) If it states **RemoteSigned** or **Unrestricted**, then it is currently at the minimum required level and you can exit the Powershell command window by typing **exit** and proceed to step 3).
 - b) Otherwise type **set-executionpolicy RemoteSigned** and enter **y** to accept.
- 4) Then exit the powershell command by typing **exit**.

Installing the Splunk Universal Forwarder, Splunk Cloud App for Universal Forwarder and Splunk TA(s)

Perform the following steps for each of the targeted AD Domain Controllers, and other Windows Systems

Splunk Universal Forwarder Installation Steps:

- 1) Log into the targeted Windows system using a *Domain Account* with software installation permissions.
- 2) Navigate in **Windows File Explorer** to the UNC path of the **target_share_folder** where you placed the **splunkforwarder...msi** file in [Step 2](#), or download it directly from [here](#).
- 3) Click on the **splunkforwarder...msi** to launch the *Splunk Universal Forwarder* Installation Wizard and follow the below steps:
 - a) **First Window:**
 - i) **Check** the **Check this box to accept the License Agreement** checkbox.
 - ii) **Uncheck** the **Use this UniversalForwarder with on-premises Splunk Enterprise...** checkbox.
 - iii) **Customize Options:**
 - (1) **NOTE:** To change any of the default installation settings, click the **Customize Options** button and browse [here](#) to proceed to the *Customize options* documentations for a cloud installation procedure.
 - iv) Click **Next**.
 - b) **Second Window: (Deployment Server** pane)
 - i) **Recommended:** Leave the Hostname or IP and Port fields **blank**.
 - (1) **Or** if you have installed an **On-Premise** Splunk instance that will be the Splunk Deployment Server, then enter the host name or IP address and management port for the deployment server that you want the universal forwarder to connect to and click **Next**.
 - c) **Third Window:**
 - (1) Click **Install**. The installer runs and displays the *Installation Completed* dialog and start the service.
 - d) **Fourth Window:**
 - i) Click **Finish**

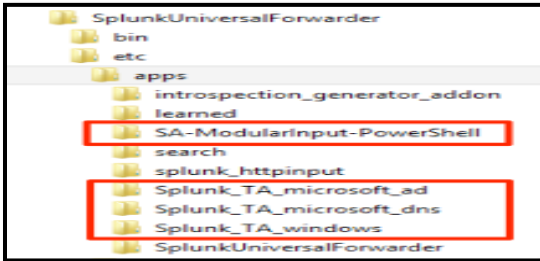
Splunk Cloud App for Universal Forwarder Installation Steps:

- 1) After the *Splunk Universal Forwarder* has been installed, copy the **splunkclouduf.spl** application from the **target_share_folder** to a **local folder** on the targeted system.
- 2) Open the **Command Prompt** program by **right clicking** on the **Command Prompt** icon and selecting **Run-As-Administrator**.
- 3) Run the following commands to install the **splunkclouduf.spl** application.
 - a) **Execute:** `cd "c:\program files\SplunkUniversalForwarder\bin"`
 - i) **NOTE:** If you installed the Splunk Universal Forwarder in a non-default directory, then replace "c:\program files\SplunkUniversalForwarder\bin" with the correct location.
 - b) **Execute:** `splunk install app c:\ Splunk_UF_Apps\splunkclouduf.spl -auth admin:changeme`
 - i) **NOTE:** Replace **c:\ Splunk_UF_Apps** with the **local folder** where you copied the **splunkclouduf.spl** application to.
 - ii) **Successful response:** `App 'c:\Splunk_UF_Apps\splunkclouduf.spl' installed`
 - c) **Execute:** `splunk restart`

- 4) After completing the above steps you can run the following search in the Splunk UI to verify the Splunk Universal Forwarder is sending data to the Splunk Cloud instance: `index=_internal | stats count by host`
 - a) If you **do not** see your forwarder listed in the above search results, then review the troubleshooting steps in [Appendix C](#)

Splunk TAs for Universal Forwarder Installation Steps:

- 1) Copy the Splunk TA folders ([Base_Windows](#), or [AD_DomainControllers](#)) from the [target_share_folder](#) folders configured in [Step 2](#) into the `$SPLUNK_HOME\etc\apps` (Ex `C:\program files\SplunkUniversalForwarder\etc\apps`) directory.
 - a) **Critical Note:** Make sure that you only copy the **contents** of the [Base_Windows](#)/[AD_DomainControllers](#) folders and not the folders themselves. See below screenshot of what the directory should look like.
 - i) **Domain Controller – Example:**



- ii)
- 2) **Restart** the `SplunkForwarder` service again to pick up the new Splunk TA's and their data inputs.
- 3) After restarting the `SplunkForwarder` Service, you can run the below search from the Splunk Cloud UI to verify that you are receiving configured input data.
 - a) Login to the *Splunk Cloud UI* and navigate to **Apps → Search and Reporting**
 - b) In the *Search* box run the below search.
 - i) `sourcetype=WinEventLog:* OR sourcetype=perfmon* earliest=-5m | stats values(source) AS sources, count by sourcetype`
 - c) If you are seeing results the the above search, then you can proceed to [Step 4 Complete Setup of Splunk App for Windows Infrastructure and MS Windows AD Objects](#).
 - d) If you do not see any or all of the results for a specific host, or data input, then follow some of the troubleshooting steps outlined in [Appendix C: No Splunk Data Input Data section](#).

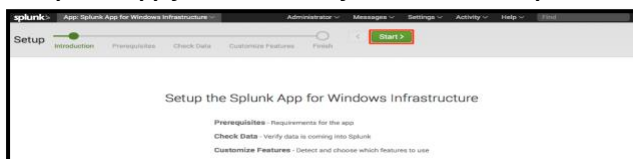
Step 4: Complete Setup of Splunk App for Windows Infrastructure and MS Windows AD Objects


This section covers the final steps for setting up and configuring the **Splunk® App for Windows Infrastructure** and **MS Windows AD Objects** applications. It is recommended to complete and verify each of the following steps in order.

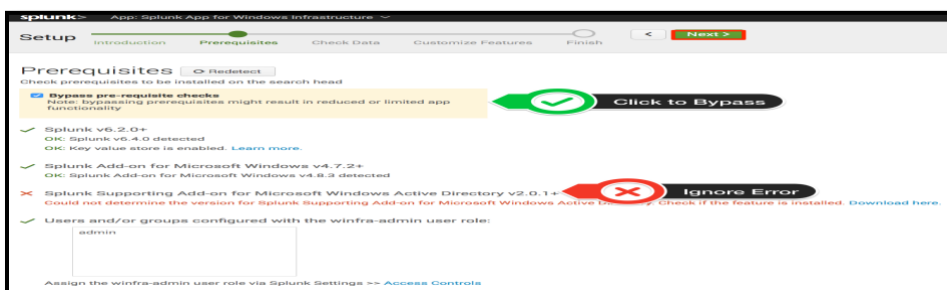
Splunk App for Windows Infrastructure: Start the Initial Setup Wizard



Complete the setup of the **Splunk App for Windows Infrastructure** application by walking through the *Initial Setup Wizard*

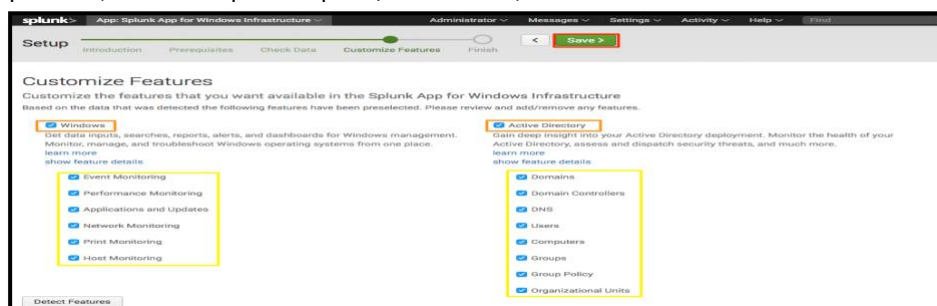
- 1) **First**, Add the Splunk Windows Roles to a Splunk Role you are in:
 - a) In the Splunk UI, navigate to **Settings** → **Access Controls** → **Roles**
 - b) Click on the **admin** role, or any other role that you want to give access to the Windows data being indexed by Splunk.
 - c) Scroll down to the **Inheritance** section, and click on the **windows-admon** and **winfra-admin** roles to add them to the **Selected roles** box.
 - d) Click the **Save** button.
- 2) Open the **Splunk App for Windows Infrastructure** application
 - a) In the **Splunk User Interface** navigate to **Apps** → **Splunk App for Windows Infrastructure**
- 3) The **Guided Setup App for Windows Infrastructure Setup Wizard** will start, as shown below.



- a) **Ex.**
- 4) Click **Start**
 - 5) Next is the **Prerequisites** window. If each of the sections have a , **except** for the **Splunk Supporting Add-On for Microsoft Windows Active Directory**, then click the **Bypass pre-requisite checks** option, as shown in the below example, and click the **Next** button.



- a) **Ex.**
 - b) **Note:** If there isn't a  in any of the other sections, then use the below list to navigate to and then verify the steps were completed in this guide.
 - i) **Note:** After re-verifying the data/steps then click the  button to redetect.
- 6) Next is the **Customize Features** window, which will run some searches against collected Windows data to recommend which menu drop downs, and subsequent Reports/Dashboards, will be available based on collected data.



- a) **Ex.**
 - b) **Note:** This will kick off the initial building of lookup tables that are leveraged by the dashboard Dropdowns and reports.
 - c) **Note:** After the build process completed, you can optionally enable/disable the applications menu listed dashboards.
- 7) Click the **Save** button.

MS Windows AD Objects: *Build the initial AD Objects lookup files*

- 1) In the Splunk UI, navigate to **Apps** → **MS Windows AD Objects**
 - a. This will bring you to the landing view that contains information about this application, deployment steps, etc.
- 2) Select the **Build AD Lookup Lists – Main** view from **Configuration Dashboards** menu dropdown.
 - a. This view is used for initially building the AD Object lookup files.
 - i. **NOTE – Auto Search Verification Information:**
 1. If you see the following message in your dashboard, then go to [Appendix B – Troubleshooting for missing admon baseline data or AD MSAD Health data](#) for troubleshooting steps.
 - a. **WARNING!! - No (eventtype=msad-dc-health) data found. Make sure you have deployed the Splunk Addon for Active Directory to your domain controllers. Click the 'msad verify search' link to the right to see the search used.**
 2. If you see the following message in your dashboard, then go to the [Appendix B – Troubleshooting for missing admon baseline data or AD MSAD Health data](#) for troubleshooting steps.
 - a. **Auto Search Results - WARNING!! - No ActiveDirectory baseline (Sync) data found. Rerun through through Deployment Steps to verify admonEventType=Sync data has been collected from the Domain Controller.**
- 3) Select how you would like to build the lookups, either **All at once**, or **by walking through each object type building it in steps**.
 - a. **Option A: Build All**
 - i. **Description:** When this option is selected and executed it will open a separate view and build/update all of the Lookups at once, versus stepping through each object manually.
 - ii. Click the **radio** button for **Option A**.
 1. A new button labeled “**Click Here to Build All Lookups Automatically**”, will appear.
 - iii. Click the new button to start the automatic build process. After it completes you can click the Finish and Go Back button to come back to this view.
 - b. **Option B: Build Individually**
 - i. **Description:** This option allows for you to build the lookups by stepping through each AD Object.
 - ii. Select **Users** from the **Step 1: Select AD Object** dropdown.
 - iii. Select **Yes** from the **Step 2: Build User Lookup** dropdown that appeared when you selected **Users** in the previous step.
 1. This will run the searches against the `sourcetype=ActiveDirectory` data to build the Users AD Object lookup files.
 2. **Note:** For **Users**, **Groups**, and **Computers**, there will be a **Step 3: Sync ... Group Membership**. Select **Yes** to ensure the selected AD Object's lookup table has the latest Group Membership.
 - iv. Repeat **Step 3** and **Step 4** for the following AD Object Types using the **Step 1: Select AD Object Target To Build Lookup for** dropdown:
 1. **Computers, Groups, Distribution Lists, Organizational Units, Group Policies**
 - v. Use the **Building Status for AD Object Lookups** table to view and track the progress of building the AD Object Lookups.
- 4) After you complete either of the above building option, your now ready to start using the MS Windows AD Objects application. If you are planning on integrating with the **Splunk App for Windows Infrastructure** application, then complete the integration steps outlined in the next section.

Appendix A – Splunk Current Cloud Customers – Support Case Steps

The following steps are for **current** Splunk Cloud customers who want to add the **Splunk App for Windows Infrastructure**, **Splunk Add-On for Windows** and **MS Windows AD Objects** applications to their Splunk Cloud instance(s). These steps outline and provide input values you can use for submitting a Splunk Support Case to have Splunk Cloud's Support team perform the appropriate steps to install and configure these applications.

Note: You will need to use an authorized contact to file a Splunk Support case.

Filling out the case submission form

- 1) Navigate and login in to the [Splunk Support Portal](#).
- 2) Click the **Submit Case** link on the left side, under the **Cases** section, or the **Submit a New Case** button.
- 3) Fill in the below values in the *Submit a Case* form.
 - **Special Notes:**
 - o Select or replace the values in **red** with your specific Splunk Cloud instance information.
 - o Values in **green** should be copied and pasted into the appropriate fields.
 - **Select Entitlement: (Required)**
 - o Select the **right entitlement** for your Splunk Cloud instance.
 - This is the entitlement that corresponds with the license installed. If you have more than one entitlement, you can check My Licenses to which entitlement is paired with the license.
 - **Select Deployment: (Optional)**
 - o Select the **right Deployment**.
 - Deployments allow you to represent the various instances of Splunk in your environment, their functions to your business and their ancillary resources (a license, primary administrator etc.). This is an optional selection.
 - **Splunk Installation is?**
 - o Select the following from the drop down:
 - All configuration issues and any other case where a feature is not operating as documented.
 - **Subject:**
 - o Enter in the following text:
 - Request for Splunk Cloud Application Installation and Configuration. Apps: Splunk for Windows Infrastructure, Splunk Add-On for Windows, Splunk Add-On for Microsoft Active Directory, Splunk Add-On for Microsoft DNS, and MS Windows AD Objects.
 - **What Product are you having trouble with?**
 - o First Drop Down
 - Select **Splunk Cloud**
 - o Second Drop Down
 - This should automatically get populated with **Cloud**.
 - **What OS are you using?**
 - o Leave the default of **None**.
 - **What OS Version are you using?**
 - o Leave the field blank
 - **I need help with ...**
 - o Select the following from the drop down:
 - **Apps**.
 - **Feature / Component / App**
 - o Select the following from the drop down:
 - **Splunk App for Windows Infrastructure**
 - **Deployment Type**
 - o Select the following from the drop down:
 - Select **Cloud**
 - **What is the impact...**
 - o Enter the following text:
 - **Splunk Applications required for Windows data management.**

Appendix B – Troubleshooting missing admon baseline or AD MSAD Health data

Not seeing **admon baseline**, “Sync”, data

Perform the following steps on the **Splunk Universal Forwarder** on the **Domain Controller** if you are not seeing results from the following search:

- `sourcetype=ActiveDirectory admonEventType=Sync`

1. On the Domain Controller with the Splunk Universal Forwarder **Stop** the **SplunkForwarder** Service
2. Using Windows File Explorer to navigate to the `$SPLUNK_HOME\SplunkUniversalForwarder\var\lib\splunk\persistentstorage\ADMon` directory.
3. Delete the **NearestDC.ini** file, and the **ADMonitoring.ini** file if it exists.
4. Restart the **SplunkForwarder** Service.
5. Rerun the following search from the Splunk UI to verify admon baseline data is being indexed.
 - o `sourcetype=ActiveDirectory admonEventType=Sync`
6. If you are now seeing data from verification search, then go back to Step 4a and complete the AD Objects Splunk Lookup file building steps in the **Build AD Lookup Lists – Main** view.

Not seeing **AD MSAD data** - Verify and update PowerShell’s Execution Policy

Like most Applications that integrate and specifically monitor Active Directory, Splunk leverages PowerShell to collect detailed information from the Active Directory Domain and Domain Controller. In order for the Splunk Forwarder to initiate the pre-built PowerShell scripts, the Execution Policy of PowerShell must be at least RemoteSigned.

Perform the following steps on the **Splunk Universal Forwarder** on the **Domain Controller** if you are not seeing results from the following search:

- `eventtype=ms_ad_obj_msad-dc-health`

- 1) Run **Powershell** console as an **Administrator**:
 - a) Go to **Start-->Programs-->Accessories-->PowerShell** and right-click then select **Run As Administrator**.
- 2) Check/Update the current **Powershell ExecutionPolicy** Setting:
 - a) Type `get-executionpolicy` in the powershell command window.
 - b) If it states **RemoteSigned**, then exit the PowerShell command window by typing `exit`.
 - c) Otherwise type `set-executionpolicy RemoteSigned` and enter `y` to accept.

Then exit the powershell command by typing `exit`.

Appendix C – Troubleshooting Splunk Communication Issues

Below are several troubleshooting steps you can perform to find the root cause, and a resolution to common Splunk UF → Splunk Cloud communication issues.

First - Check Splunk Cloud instance if it is receiving Splunk UF internal logs:

First, check to see if the *Splunk Universal Forwarder* is sending its internal logs to the Splunk Cloud instance. This is done by default with all Splunk Forwarder installations, and will determine if the communication issue is, or is not, being caused by a firewall inbetween the Splunk Forwarder and the Splunk Cloud Indexers.

- 1) Login to the your Splunk Cloud UI, then navigate to the **Apps → Searching and Reporting**
- 2) In the Splunk Search bar type in the following search, to see if the Splunk Universal Forwarder(s) are listed in the results:
 - a) `index=_internal | stats count by host`
- 3) If **do** see results for the *Splunk Universal Forwarder*(s), then the *Splunk Universal Forwarder* is able to communicate with the indexer. You can then skip to the view the **No Splunk Data Input Data** sections below for troubleshooting steps on why there is no Splunk data being received by the *Splunk Cloud Indexer*(s).
- 4) If you **do not** see the *Splunk Universal Forwarder*(s) listed in the results, then proceed to the next section **Check and Create Inbound/Outbound Rules for Windows Firewall**.

No Splunk UF Internal Log Data: Troubleshooting Steps for Internal Logs Not being received by Indexer:

- *Splunk Universal Forwarder IS NOT listed when executing the `index=_internal | stats count by host` search*

Check and Create Inbound/Outbound Rules for Windows Firewall

Below are the steps for adding Windows Firewall Rules to allow communication between the Splunk Universal Forwarder and the Splunk Cloud Indexer.

If **Windows Firewall** is *disabled*, or the below steps don't fix the communication issue, then check with your network administrator for allowing TCP Ports –9997 to any firewalls inbetween the Splunk Systems.

If **Windows Firewall** is *enabled*, then follow the below steps to add **Inbound** and **Outbound** rules for *Splunk Universal Forwarder* TCP communication to the *Splunk Cloud Indexer/Deployment Server*.

- 1) Login to the Splunk Universal Forwarder System
- 2) Open **Windows Firewall** and Click on the **Inbound Rules**:
- 3) Click on the **Outbound Rules** link:
- 4) Create a **New Outbound Rule** with the following settings:
 - a) Select **Port**, then Click **Next**
 - b) Enter in 9997 for the Port value, then Click **Next**
 - c) Click **Allow the Connection**, then Click **Next**
 - d) Select **Domain**, **Private**, and **Public**, then Click **Next**
 - e) Enter the following values and then Click **Finish**
 - i) **Name:**
 - (1) **Splunk – Outbound Rule**
 - f) Restart **Splunk Forwarder** Service

Check for the existence of outputs.conf in the system directory, and that the Splunk Cloud Universal Forwarder App has been installed:

The **outputs.conf** file contains the list of Splunk Indexer(s) the Splunk Universal Forwarder sends its data to. For Splunk Cloud installations this is already created and configured for you in the *Splunk Cloud Universal Forwarder Application*. However, if an indexer was accidentally manually entered during the *Splunk Universal Forwarder* installation, then it also will create an **outputs.conf** file, and will override the values in the *Splunk Cloud Universal Forwarder Application* version.

Below are the steps for ensuring that you don't have **outputs.conf** file in the **\$SPLUNK_HOME/etc/system/local** directory, and also show you how to verify that the *Splunk Cloud Universal Application* has been installed on the Splunk Forwarder.

On the *Splunk Universal Forwarder* System:

- 1) Check for the existence of the **outputs.conf** file in the System directory:
 - a) Open Windows File Explorer and navigate to **\$SPLUNK_HOME/etc/system/local** directory (Ex. C:\program files\SplunkUniversalForwarder\etc\system\local).
 - b) Check to see if there is an **outputs.conf** file there:
 - i) If there is not an **outputs.conf** file there, then skip to step 3).
 - ii) If there is an **outputs.conf** file there:

- (1) Delete the **outputs.conf**
- (2) **Restart the Splunk Forwarder Service.**
- (3) Rerun the following Splunk search in the Splunk Cloud UI to see if the Splunk Forwarder is now listed in the results:
 - (a) `index=_internal | stats count by host`
- 2) Check that the Splunk Cloud Universal Forwarder Application has been installed.
 - a) Open Windows File Explorer and navigate to **\$SPLUNK_HOME/apps** directory (Ex. `C:\program files\SplunkUniversalForwarder\etc\apps`).
 - i) Check to see if the **splunkclouduf** directory is there. If not then run the following steps to install the Splunk Cloud Universal Forwarder Application:
 - (1) From your Splunk Cloud UI, navigate into **Splunk Cloud UI → Apps → Universal Forwarder** application
 - (2) Click the **Download your Splunk Cloud Universal Forwarder app** and then copy the downloaded **splunkclouduf.spl** file into the **local folder** on the Splunk Universal Forwarder system.
 - (a) This app contains custom secure certificates and outputs settings to connect specifically to your Splunk Cloud.
 - (3) Open the **Command Prompt** program by **right clicking** on the **Command Prompt** icon and selecting **Run-As-Administrator**.
 - (4) Run the following commands to install the **splunkclouduf.spl** application.
 - (a) **Execute:** `cd "c:\program files\SplunkUniversalForwarder\bin"`
 - (i) **Note:** If you installed the Splunk Universal Forwarder in a non-default directory, then replace `"c:\program files\SplunkUniversalForwarder\bin"` with the correct location.
 - (5) **Execute:** `splunk install app c:\ Splunk_UF_Apps\splunkclouduf.spl -auth admin:changeme`
 - (a) **Note:** Replace `c:\ Splunk_UF_Apps` with the **local folder** where you copied the **splunkclouduf.spl** application in step 6).
 - (b) **Successful response:** `App 'c:\Splunk_UF_Apps\splunkclouduf.spl' installed`
 - (6) **Execute:** `splunk restart`
 - ii) Recheck to see if the **splunkclouduf** directory is now in the **\$SPLUNK_HOME/etc/apps** directory.

No Splunk Data Input Data: Troubleshooting Steps for no Splunk Universal Forwarder Data Input data being received by Indexer:

- **Splunk Universal Forwarder Is listed when executing the `index=_internal | stats count by host` search**

This section covers some of the common troubleshooting and resolution steps for when a Splunk UF has data inputs enabled, but it is not showing up in the Splunk UI.

Note: Only do this if you ran the previous search, `index=_internal | stats count by host`, and the target Splunk UF is able to send/index its internal log data.

First, Verify that the Windows data is not being indexed by Splunk:

- 1) In the Splunk UI, navigate to **Apps → Search and Reporting**.
- 2) In the Search box, enter and execute the following search with the Time Period of **Last 60 Minutes**.
 - a) `index=* host="your_forwarder_host_name" | stats count by sourcetype`
 - b) **Note:** Replace `"your_forwarder_host_name"` with the **hostname** of your forwarder.
- 3) If you do not see the any results from the previous search, then proceed to the next troubleshooting sections.

Verify and Update Splunk Access Control Settings

The below steps are for verifying that the Splunk User being leveraged has the proper Splunk permissions to view the collected Windows Data.

- 1) Add Windows Roles to a Splunk Role you are in.
 - a) In the Splunk UI, navigate to **Settings → Access Controls → Roles**
 - b) Click on the **admin** role, or any other role that you want to give access to the Windows data being indexed by Splunk.
 - c) Scroll down to the **Inheritance** section, and click on the **windows-admon** and **winfra-admin** roles to add them to the **Selected roles** box.
 - d) Click the **Save** button.

Verify the Splunk TA's have been configured and added to the Splunk Universal Forwarder

The below steps are for verifying that the Splunk Universal Forwarder data

- 1) On the Splunk Universal Forwarder, navigate to the **\$SPLUNK_HOME/etc/apps** directory (Ex. C:\Program Files\SplunkUniversalForwarder\etc\apps)
- 2) You should see the *Splunk_TA_windows* folder, and if it is an AD Domain Controller, you should also see the *Splunk_TA_microsoft_ad* and *Splunk_TA_microsoft_dns* folders.
- 3) If you **do** see those folders, then doublecheck that you followed the **inputs.conf** configuration steps outlined [here](#), and have copied them to the Splunk Universal Forwarder as outlined in [this section](#).
- 4) If you **do not** see those folders, then rewalk through the configuration steps outlined in [this section](#).

Appendix D – Enable Auditing in the Active Directory Environment

Auditing overview

By default, Active Directory does not automatically audit certain security events. You must enable auditing of these events so that your domain controllers log them into the Security event log channel.

Refer to the table below to learn about which policy settings generate which event types, and how the *Splunk App for Windows Infrastructure* uses those events to populate its dashboards, reports and lookups.

If you choose to disable certain policy settings in an effort to curb indexing volume, you directly affect how much data gets sent to the *Splunk App for Active Directory*. The table below lists what data you do not collect if you decide not to enable a particular policy setting. This is not an all-inclusive list - the app correlates some lookups across various policy settings, as multiple events often derive a single knowledge object. Failure to enable all of the policy settings might cause the *Splunk App for Windows Infrastructure* to display incomplete or incorrect knowledge objects in its dashboards and reports.

| Policy setting: | Required? | What the Splunk App for Windows Infrastructure uses it for: |
|----------------------------|-----------|--|
| Audit Account Logon Events | Yes | Administrator Audit dashboards Security->Logon dashboards Security->Reports->New (Computer or Domain) Accounts Session ID-to-User (tSessions) lookup Computer-to-IP Address (tHostinfo) lookup |
| Audit Account Management | No | Administrator Audit dashboards Change Management dashboards |
| Audit Logon Events | No | Administrator Audit dashboards Logon and access information |
| Audit Object Access | No | Administrator Audit dashboards Information on who changed a GPO and when |
| Audit Policy Change | No | Security->Reports->Group Policy Reports GPO Change Management dashboard |
| Audit System Events | No | Directory Services replication events |

Enable Auditing on Windows Server 2008, Server 2008 R2, Server 2012, and Server 2012 R2

- 1) Create a new GPO:
 - a) Click **Start > Administrative Tools > Group Policy Management**.
 - b) In the left pane, under "Group Policy Management," expand the forest and domain for which you want to set group policy.
 - c) Right-click **Group Policy objects** and select **New**.
 - i) In the dialog window that opens, enter a unique name for your new GPO that you will remember in the **Name** field, and select **None** for the **Source Starter GPO** field.
 - ii) Open the GPO for editing by right-clicking the newly created GPO in the Group Policy Objects window and selecting **Edit**.
 - iii) In the GPO editor, select **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policy > Audit Policy**.
 - iv) Enable both **Success** and **Failure** auditing of the following policy settings:
 - (1) Audit account logon events
 - (2) Audit account management
 - (3) Audit directory service access
 - (4) Audit logon events
 - (5) Audit object access
 - (6) Audit policy change
 - (7) Audit privilege use
 - (8) Audit system events
 - v) Close the Group Policy Object Editor window to save your changes.
- 2) Deploy the GPO:

- a) In Group Policy Management, in the left pane of the window, right-click on the **Domain Controllers** item and click **Link an existing GPO...**
- b) In the window that appears, select the GPO you created in **Step 1**.
- c) Click **OK**. The GPMC will refresh to show that your GPO is now linked to the **Domain Controllers** organizational unit.

Advance Auditing Settings:

Creating and verifying an advanced audit policy

The nine basic audit policies under **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy** allow you to configure security audit policy settings for broad sets of behaviors, some of which generate many more audit events than others. An administrator has to review all events that are generated, whether they are of interest or not.

Starting in Windows Server 2008 R2 and Windows 7, administrators can audit more specific aspects of client behavior on the computer or network, thus making it easier to identify the behaviors that are of greatest interest. For example, in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy**, there is only one policy setting for logon events, **Audit logon events**. In **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies**, you can instead choose from eight different policy settings in the **Logon/Logoff** category. This provides you with more detailed control of what aspects of logon and logoff you can track.

A default domain policy is automatically generated when a new domain is created. In this section, you will see the steps for creating a group policy to add an advanced security audit policy setting that audits when a user either successfully or unsuccessfully logs on to a computer in the your domain.

To configure, apply, and validate an advanced domain logon audit policy setting, you must:

- 1) Configure an advanced domain logon policy setting.
- 2) Ensure that Advanced Audit Policy Configuration settings are **not overwritten**.
- 3) Update Group Policy settings.
- 4) Verify that the advanced logon security audit policy settings were applied correctly.

To configure an advanced domain logon audit policy setting

- 1) Log on to the domain's Domain Controller as a member of the local **Domain Admins** group.
- 2) Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
- 3) In the console tree, double-click **Forest: your fqdn**, double-click **Domains**, and then double-click **your domain**.
- 4) Right-click on the **Group Policy Objects** folder, and then click **New**.
- 5) Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
- 6) Double-click **Security Settings**, double-click **Advanced Audit Policy Configuration**, and then double-click **System Audit Policies**.
- 7) Double-click **Logon/Logoff**, and then double-click **Logon**.
- 8) Select the **Configure the following audit events** check box, select the **Success** check box, select the **Failure** check box, and then click **OK**.
- 9) Repeat **Step 7** and **Step 8** for other Auditing Settings you would like to generate Security Audit events for, like **Account Management**, etc.
- 10) In Group Policy Management console, in the left pane of the window, right-click on an Organizational Unit you would like to test this setting against. item and click **Link an existing GPO...**
- 11) In the window that appears, select the GPO you created in **Step 1**.
- 12) Click **OK**. The GPMC will refresh to show that your GPO is now linked to the specified organizational unit.

Important Note: When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. The following procedure shows how to prevent conflicts by blocking the application of any basic audit policy settings.

To ensure that Advanced Audit Policy Configuration settings are not overwritten

- 1) On domain's Domain Controller, click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
- 2) In the console tree, double-click **Forest: your fqdn**, double-click **Domains**, and then double-click **your domain**.
- 3) Right-click on the Group Policy created in the previous section, and then click **Edit**.
- 4) Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
- 5) Double-click **Security Settings**, and then click **Security Options**.

- 6) Double-click **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings**, and then click **Define this policy setting**.
- 7) Click **Enabled**, and then click **OK**.

Before you can verify the functionality of advanced security audit policy settings in your domain, you will log on as the domain administrator of your domain to a user machine that has the previously create GPO applied to it and ensure that the Group Policy settings have been applied.

To update Group Policy settings

- 1) Log on to a user machine that has the previously create GPO applied to it.
- 2) Click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- 3) If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
- 4) Type **gpupdate**, and then press ENTER.

After the Group Policy settings have been applied, you can verify that the audit policy settings were applied correctly.

To verify that the advanced logon security audit policy settings were applied correctly

- 1) Log on to a client system and using a domain account that has the previously created GPO applied to it.
- 2) Click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- 3) If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
- 4) Type **auditpol.exe /get /category:***, and then press ENTER.
- 5) Verify that **Success**, **Failure**, or **Success and Failure** are shown to the right of **Logon**.