



# SecureVantage

## TECHNOLOGIES

### ACS Noise Filter Guide

**Author:** Chance Folmar

**Published:** April 2007

**Last Modified:** August 2008

**Applies To:** System Center Operations Manager 2007

**Document Version:** v 2.02

**Acknowledgements:** Jeremiah Beckett, Joseph Chan, Eric Fitzgerald, Rory McCaw and Randy Franklin Smith

# Table of Contents

<b>OVERVIEW .....</b>	<b>3</b>
<b>MANAGING FILTERS .....</b>	<b>4</b>
REVIEW EXISTING FILTERS .....	4
FILTERING TIPS .....	4
APPLYING NEW FILTERS .....	5
EVENT LOAD ANALYSIS.....	5
<b>NOISE FILTER LIST.....</b>	<b>6</b>
<b>ADTSEVENT DETAILS .....</b>	<b>8</b>
CATEGORY ID .....	8
AUDIT RECORD FLAGS .....	9
<b>EVENT ATTRIBUTE MAPPING .....</b>	<b>9</b>
<b>WINDOWS SERVER FILTER EXAMPLES .....</b>	<b>10</b>
FS1001: WINDOWS SERVER ESSENTIAL FILTER.....	10
FS1002: WINDOWS SERVER REASONABLE FILTERS.....	11
FS1003: WINDOWS SERVER RATIONAL FILTERS .....	12
FS1004: WINDOWS SERVER AUTHENTICATION COMPUTER\$ FILTER.....	13
FS1005: SERVICE & SYSTEM ACCOUNT AUTHENTICATION FILTER .....	14
COMBINING DIFFERENT FILTERS.....	15
<b>SECURE VANTAGE STARTER FILTERS .....</b>	<b>16</b>

## OVERVIEW

In most cases it is unnecessary or impractical to collect and store all security events. While the Audit Collection Service (ACS) natively collects all security events from a target system, it includes a filtering mechanism which can be used to manage event insertion and storage to the SQL database. Filters can be implemented based on event ID or on the contents of the events themselves.

The Secure Vantage ACS Noise Filters Guide provides sample filter sets and guidance to optimize data collection, which improves both online and offline storage capabilities as well as reporting performance.

ACS Noise Filters are based on Microsoft recommended event filters defined in the Security Attack and Detection Planning Guide and best practices from Microsoft Security MVP Randy Franklin Smith.

### **Guide Considerations:**

- This is not an audit policy or data collection planning guide.
- Your corporate policy and/or regulatory requirements always dictate what you must collect.
- Currently the guide only covers Windows Server 2000 & 2003 events.
- This is a free community resource for administrators looking at ways to improve ACS collection performance and reduce overall load.
- This is a reference of what to consider filtering, why (based on MS) and how to go about it.
- Filter needs will vary based on audit policy, user activity and reporting requirements.
- Some filter examples include events that may not be relevant based on your audit policy.

### ***Additional Resources***

**Security Attack Detection and Planning Guide:** Appendix A Exclude Unnecessary Events

<http://www.microsoft.com/technet/security/guidance/auditingandmonitoring/securitymonitoring/default.aspx>

**Ultimate Windows Security:** <http://www.UltimateWindowsSecurity.com>

**Secure Vantage Windows Security Auditing Reference List:** Over 1300 Windows security events and settings with interactive links to Randy Franklin Smiths online security wiki.

<http://www.securevantage.com/Products/2007%20Solutions/Docs/Secure%20Vantage%20Windows%20Security%20Auditing%20Reference%20List.xls>

**Secure Vantage Team Blog:** <http://securevantage.spaces.live.com>

## MANAGING FILTERS

Managing filters is done through the adtAdmin command. The following information provides general guidelines for the command syntax and use with our noise filter template examples.

*Please Note:* Filter complexity and length can impact WMI performance. Order filters by most frequent event activity to optimize Collector processing of filter expression.

Managing filters is a bottom up approach starting at the Audit Policy level and targeted Systems, then Objects (if auditing Directory Services or Object Access), then specific Events IDs and finally Use Case scenarios.

### Review Existing Filters

You can use the adtAdmin command to list the ACS Collection filters. The following information shows the general syntax and a sample of using the command. This can be used to check existing filters or validate that new ones are loaded. More information on the adtAdmin command can be found in the Operations Manager Help libraries on your Management Server.

### Command Syntax

```
AdtAdmin.exe /getquery [/Collector:CollectorName]
```

### Filtering Tips

Consider the following items before applying ACS Noise Filters.

1. **Query Syntax is WQL** not SQL - some minor syntactical differences. In particular, advanced string manipulations are not supported in WQL (example: Right, Left, Substring, etc.).  
*Microsoft WQL Reference:* [http://msdn2.microsoft.com/en-us/library/aa394606\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/aa394606(VS.85).aspx)
2. **Default WQL Query** – The default query is “SELECT \* FROM AdtsEvent” and allows all events to be inserted in the Collector database
3. **Query Length Max** - 100 tokens W2K3 SP1 or 500 tokens W2K3 SP2 (token is one set of objects, i.e. SELECT is 1 Token, SELECT \* FROM is 3 Tokens)
4. **Use WHERE NOT statements** – The WQL Query tells the stream what to allow through to the Collector and into the ACS database. Using a NOT statement will allow all items through except those in the string.
5. **Query Length and Complexity** can impact ACS Performance
6. **Test the Query** – Test the query before applying it to production. Queries can become complex quite quickly, and it is difficult to foresee all impacts by simply looking at the query. Testing the noise filter before placing it in production will help alleviate unintentional data loss.

## Applying New Filters

You can use the `adtAdmin` command to update the ACS Collection filters. The following information shows the general syntax and a sample of using the command with one of the filters described in this guide.

### Command Syntax

```
AdtAdmin.exe /SetQuery [/Collector:CollectorName] /Query:QuerySyntax
```

### Sample: Loading Filter

```
adtadmin /setquery /collector:"Collector Name" /query:"SELECT *  
FROM AdtsEvent WHERE NOT(EventId=551 Or EventId=562 OR EventId=573 OR  
EventId=577 OR EventId=578 OR EventId=697 OR (EventId>=594 AND  
EventId<=597)OR (EventId>=768 AND EventId<=771) OR (EventId>=532 AND  
EventId<=841))"
```

## Event Load Analysis

Before and after you implement ACS filters it is important to understand the current event stream to validate your filters are working and also help identify other opportunities for performance tuning. Customers can leverage both reports and performance counters to assist with this analysis.

Secure Vantage provides an 'Event Load Analysis' report which identifies the count of unique events and primary objects plus a range of other analytics about your event stream. Customers can also leverage the canned event analysis reports from Microsoft and the sample query below.

### Sample: Query Active ACS Partition for Event Count

```
declare @activepartition nvarchar(max)  
declare @schemaname nvarchar(255)  
declare @executesql nvarchar(max)  
  
SELECT @activepartition = [PartitionId]  
FROM [OperationsManagerAC].[dbo].[dtPartition]  
where [Status] = 0  
  
Select @schemaname = schema_name(schema_id)  
from sys.objects  
where name = 'dtEvent_' + @activepartition  
  
set @executesql = 'SELECT [EventNo],count(*) FROM [' + @schemaname +  
'].[dtEvent_' + @activepartition + '] Group by [EventNo] order by 2  
desc'  
  
EXECUTE sp_executesql @executesql
```

## NOISE FILTER LIST

This list is a consolidation of Events referenced in this guide.

Flag	Name	Description
538	User logoff	This event only indicates the time a user initiates logoff or the when the system initiates logoff. This does not mean the user actually stopped using the system.
528 & 540	Where User Name contains \$ or = X	Some Service and System accounts generate excessive activity while doing normal approved activities. Filtering these accounts can greatly reduce load when collecting successful logon events. Consider adding Event 538 and 680 if not already filtering those events.
538 & 540	Where Logon Type = 3 and User Name contains \$	Windows Computers generate many logon/logoff events on DCs as they frequently check for group policy updates and query other information in AD.
551	User initiates logoff	Event 538 confirms logoff, use instead if you want to collect logoffs.
562	A handle to an object closed	Always records a success
571	Client Context deleted by Authorization Manager.	Normal activity where Authorization Manager is active and in use
573	Process generates nonsystem audit	MS defined Typical Behavior
577 & 578	Privilege service called, privileged object operation	Very high volume events that provide little information to act upon or understand in most
594	A handle to an object was duplicated	MS defined Typical Behavior
595	Indirect access to an object was obtained	MS defined Typical Behavior
596	Backup of data protection master key	Occurs every 90 days automatically with default settings
597	Recovery of data protection master	MS defined Typical Behavior
624	User Account Created where New Account Name ends with '\$'	A domain user has created or connected a new computer account to the domain. This may be normal activity if users have this right.
627	Change Password Attempt where User equals 'System' and Target Account Name equals 'TslnternetUser' and Caller User Name ends with '\$'	This is normal behavior of a computer that runs Terminal Services.
672	Kerberos AS Ticket request	If you collect logon events 528 and 540 from all computers, this event only adds data that a Kerberos TGT was granted. As there must still be a service ticket granted (event 673) for any access to occur, this event may be redundant. Please note this event can be associated with smart card logons if applicable
672 - 677	Where User Name contains \$	Windows Computers generate many Kerberos events as they frequently check for group policy updates and query other information in AD.

<b>Flag</b>	<b>Name</b>	<b>Description</b>
<b>680</b>	Account Logon	If you collect logon events 528 and 540 from all computers, this event only records validation of the account credentials. Separate logon events record what the user accessed; this event may be redundant.
<b>697</b>	Password policy checking API called	MS defined Typical Behavior
<b>768</b>	Forest namespace collision	MS defined Not Security Related
<b>769, 770, 771</b>	Trusted forest information added, deleted or modified	Normal operations of inter-forest trusts. Do not confuse these with addition, deletion, or modification of the trust itself.
<b>832 - 841</b>	Various Active Directory replication	MS defined No Security Implications

## ADTSEVENT DETAILS

The list below represents the available fields from AdtsEvent for Noise Filter statements.

Field Name	Type	Description	Sample
EventID	uint32		636
SequenceNo	uint32	Dynamic Value, do not filter on this field	7060303
Flags	uint32	See AuditRecordFlags enumeration below	0x01
Type	uint32	8=success, 16=failure, all ACS Events 4=info	8
Category	uint32	Category ID	7
CreationTime	uint64	FILETIME, UTC, time audit was created	8/5/2008 9:14:56 PM
CollectionTime	uint64	FILETIME, UTC, time audit arrived at AdtServer	8/5/2008 9:14:58 PM
AgentMachine	String	Name of machine that sent the event	MMS2008\SQL2005\$
EventMachine	String	Name of machine in event header	SQL2005
Log	String	Log where Event originated	Security
Source	String	Log Source where Event originated	Security
HeaderSid	String	User SID in Header of Event	S-1-5-21-3936682612-
HeaderUser	String	User Name in Header of Event	Administrator
HeaderDomain	String	User Domain in Header of Event	MMS2008
PrimarySid	String	Primary User SID in Event Details	S-1-5-21-1468679-39309
PrimaryUser	String	Primary User Name in Header of Event	test41
PrimaryDomain	String	Primary User Domain in Header of Event	SQL2005
PrimaryLogonId	uint64	Primary User LogonID in Event Details	0
ClientSid	String	Client User SID in Event Details	S-1-5-21-3936682612-
ClientUser	String	Client User Name in Header of Event	Administrator
ClientDomain	String	Client User Domain in Header of Event	MMS2008
ClientLogonId	uint64	Client User LogonID in Event Details	541879972
TargetSid	String	Target SID in details of Event	S-1-5-32-547
TargetUser	String	Target Name in details of Event	Power User
TargetDomain	String	Target Domain in details of Event	Builtin
String01 through String22	String	Event detail attributes	

\*Note: Based on how ACS processes event User Data, the string attributes (String01-22) in ACS will not be in the same position as shown in the event viewer on a local machine.

### Category ID

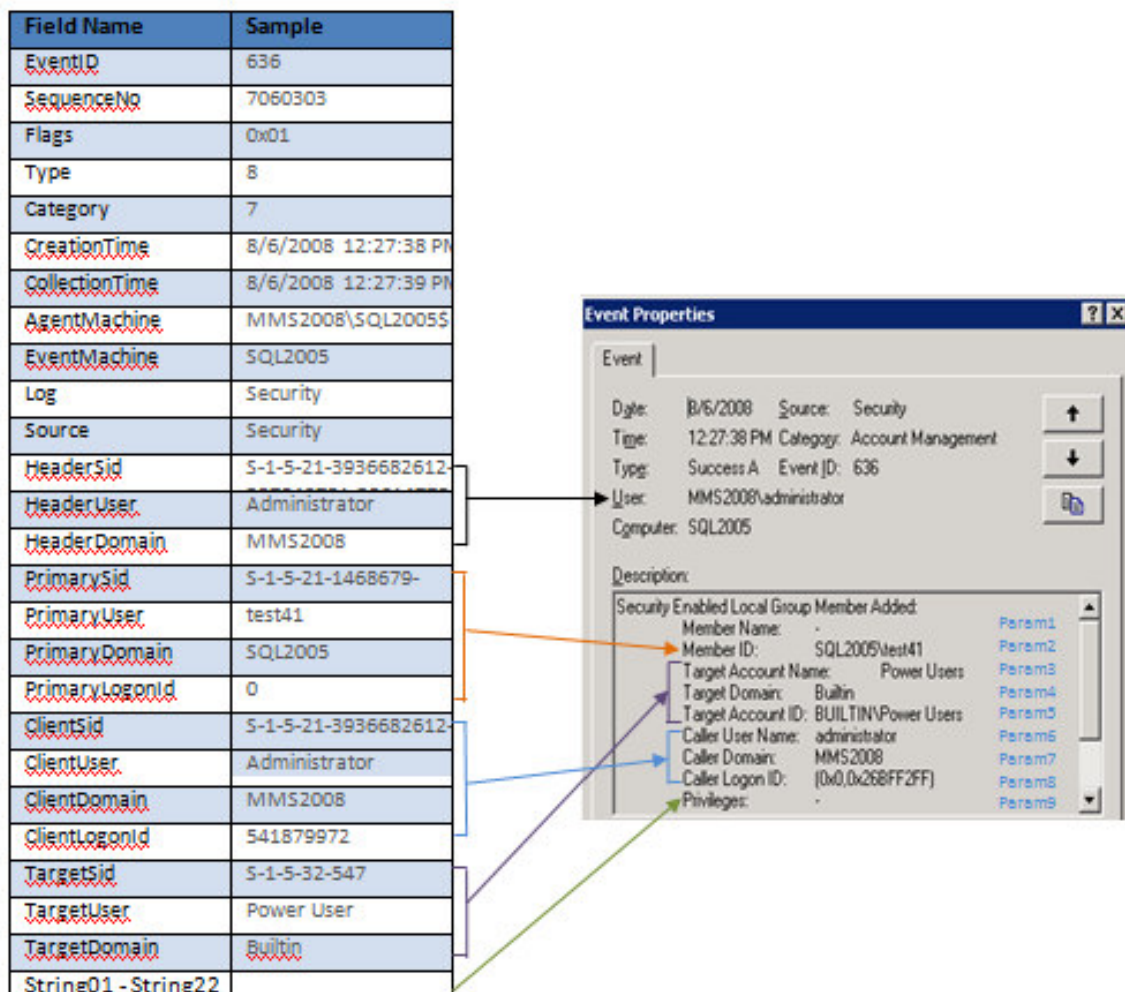
ID	Name
0	n/a
1	System Events
2	Logon/Logoff
3	Object Access
4	Privilege Use
5	Detailed Tracking
6	Policy Change
7	Account Management
8	Directory Service Access
9	Account Logon

## Audit Record Flags

Flag	Name	Description
0x00	arfNone	
0x01	arfRealTime	Event was collected in real time, not from backlog at forwarder connect
0x02	arfTruncated	Event strings truncated
0x04	arfPseudo	Event is an ACS intrinsic event (e.g. gap detected), not an event log event
0x08	arfUnknown	No transformation information available for this event
0x10	arfCorrupt	Event is corrupt

## EVENT ATTRIBUTE MAPPING

This information shows how the sample event user and string details have been mapped to an ACS event. Note when comparing events in a local Security Event Viewer and those in ACS it's important to understand both sources contain the same raw data but store and display the information slightly differently. The Events Details from the Event Viewer and ACS Strings will almost never match in ordering. The EventSchema.xml provides the mappings and conversions for all Events.



## WINDOWS SERVER FILTER EXAMPLES

The Windows Server Base Filters include lists of common events customers filter depending on overall auditing scope and reporting needs. Samples can be modified as needed to support your collection policy, environmental or activity needs. Some events while identified as noise may not occur frequently and should only be included in your filter as applicable.

**Important:** *Cut-n-paste from PDF to CMD can drop parentheses '(' and ')', check syntax after copy*

### FS1001: Windows Server Essential Filter

The Windows Server Essentials filter provides a basic filter set that should be considered in any Audit Collection environment if applicable based on audit policy. Some events may not need to be filtered.

#### Event Filter Scope

Event	Description	Filter Rationale
551	User initiates logoff	Event 538 confirms logoff, use instead if you want to collect logoffs.
562	A handle to an object closed	Always records a success
573	Process generates nonsystem audit event with Authorization Application Programming Interface (AuthZ API)	MS defined Typical Behavior
577 & 578	Privilege service called, privileged object operation	Very high volume events that provide little information to act upon or understand in most cases.
594	A handle to an object was duplicated	MS defined Typical Behavior
595	Indirect access to an object was obtained	MS defined Typical Behavior
596	Backup of data protection master key	Occurs every 90 days automatically with default settings
597	Recovery of data protection master key	MS defined Typical Behavior
697	Password policy checking API called	MS defined Typical Behavior
768	Forest namespace collision	MS defined Not Security Related
769, 770, 771	Trusted forest information added, deleted or modified	Normal operations of inter-forest trusts. Do not confuse these with addition, deletion, or modification of the trust itself.
832 - 841	Various Active Directory replication issues	MS defined No Security Implications

---

## Event Filter Syntax

```
--FS1001: Windows Server Essential Filters
SELECT *
FROM AdtsEvent WHERE NOT
(EventId=551
Or EventId=562
OR EventId=573
OR EventId=577
OR EventId=578
OR EventId=697
OR (EventId>=594 AND EventId<=597)
OR (EventId>=768 AND EventId<=771)
OR (EventId>=832 AND EventId<=841)
)
```

## FS1002: Windows Server Reasonable Filters

The Windows Server Reasonable filters provide an extension to the essentials that is acceptable to most environments and reduces considerable noise.

---

## Event Filter Scope

Event	Description	Filter Rationale
538	User logoff	This event only indicates the time a user initiates logoff or the when the system initiates logoff. This does not mean the user actually stopped using the system.
672	Kerberos AS Ticket request	If you collect logon events 528 and 540 from all computers, this event only adds data that a Kerberos TGT was granted. As there must still be a service ticket granted (event 673) for any access to occur, this event may be redundant. Please note this event can be associated with smart card logons if applicable.
680	Account Logon	If you collect logon events 528 and 540 from all computers, this event only records validation of the account credentials. Separate logon events record what the user accessed; this event may be redundant.

---

## Event Filter Syntax

```
--FS1002: Windows Server Reasonable Filters
SELECT *
FROM AdtsEvent WHERE NOT
(EventId=538
Or EventId=672
OR EventId=680
)
```

## FS1003: Windows Server Rational Filters

The Windows Server Rational filters go beyond raw event ID filtering to provide target filtering. These can be used when applicable. Note the Account Management events, and more specifically the 627 event, do not occur as frequently as other event types like Logon/Logoff. Therefore, filtering event 627 may simply add complexity to your filter without reducing much 'Noise' in the scheme of things.

---

## Event Filter Scope

Event	Description	Filter Rationale
571	Client Context deleted by Authorization Manager.	Normal activity where Authorization Manager is active and in use
624	User Account Created where New Account Name ends with '\$'	A domain user has created or connected a new computer account to the domain. This may be normal activity if users have this right.
627	Change Password Attempt where User equals 'System' and Target Account Name equals 'TsInternetUser' and Caller User Name ends with '\$'	This is normal behavior of a computer that runs Terminal Services.

---

## Event Filter Syntax

```
--FS1003: Windows Server Rational Filters
SELECT *
FROM AdtsEvent WHERE NOT
(EventId=571
Or (EventId=624 And TargetUser LIKE '%$%')
OR (EventId=627 AND HeaderUser='System' AND ClientUser like '%$%' And
TargetUser = 'TsInternetUser'))
```

## FS1004: Windows Server Authentication Computer\$ Filter

The Windows Server Authentication Computer\$ filter is for common computer account logon traffic.

### Event Filter Scope

Event	Description	Filter Rationale
<b>538 &amp; 540</b>	Where Logon Type = 3 and User Name contains \$	Windows Computers generate many logon/logoff events on DCs as they frequently check for group policy updates and query other information in AD. Please note Filter Set 1002 already excludes event 538.
<b>672 - 677</b>	Where User Name contains \$	Windows Computers generate many Kerberos events as they frequently check for group policy updates and query other information in AD. Please note Filter Set 1002 already excludes event 672.

### Event Filter Syntax

```
--FS1004: Windows Server Authentication Computer$ Filter
Select * from AdtsEvent where NOT (((EventId = 538 or EventId = 540)
AND (String01 = '3') AND HeaderUser like '%$%')) OR ((EventId > 671 and
EventId < 678) and ClientUser LIKE '%$%')
```

## FS1005: Service & System Account Authentication Filter

The Service Account Authentication Success filter provides an example of how to filter specific user accounts or patterns within a user account name like admin or sys on logon. These are commonly used to filter service and system accounts that run on all systems frequently, such as antivirus or backup programs. Please note this is for 'Success' activity only; all Logon failure activity should be collected.

### Event Filter Scope

Event	Description	Filter Rationale
528 & 540	Where User Name contains or = X	Some Service and System accounts generate excessive activity while doing normal approved activities. Filtering these accounts can greatly reduce load when collecting successful logon events. Consider adding Event 538 and 680 if not already filtering those events.

### Event Filter Syntax

```
--FS1005: Service Account Authentication Success Filter
Select * from AdtsEvent where NOT ((HEADERUSER LIKE '%ADM_%' OR
HEADERUSER LIKE '%SYS_%') AND(EventID = 528 OR EventID = 540 OR EventID
= 680))
```

### Computer Accounts Extension

```
--Filter on HEADERSID vs HEADERUser
(HeaderUser like '%$%')
```

### System Accounts Extension

```
--Filter on HEADERSID vs HEADERUser
(HeaderSid = 'S-1-5-18' OR HeaderSid = 'S-1-5-19' OR HeaderSid = 'S-1-5-20')
```

- S-1-5-18 : SYSTEM
- S-1-5-19 : LOCAL SERVICE
- S-1-5-20 : NETWORK SERVICE

## Combining Different Filters

You can consolidate different filters in the document by combining the WQL syntax to a single query

### Sample: Combining Filter FS1001 & FS1002

--FS1001: Windows Server Essential Filters

```
SELECT * FROM AdtsEvent WHERE NOT (EventId=551 OR EventId=562 OR
EventId=573 OR EventId=577 OR EventId=578 OR EventId=697 OR
(EventId>=594 AND EventId<=597) OR (EventId>=768 AND EventId<=771) OR
(EventId>=832 AND EventId<=841))
```

--FS1002: Windows Server Reasonable Filters

```
SELECT * FROM AdtsEvent WHERE NOT(EventId=538 OR EventId=672 OR
EventId=680)
```

--Combined Custom Filter

```
SELECT * FROM AdtsEvent WHERE NOT (EventId=551 OR EventId=562 OR
EventId=573 OR EventId=577 OR EventId=578 OR EventId=697 OR EventId=538
OR EventId=672 OR EventId=680 OR (EventId>=594 AND EventId<=597) OR
(EventId>=768 AND EventId<=771) OR (EventId>=832 AND EventId<=841))
```

## SECURE VANTAGE STARTER FILTERS

The Secure Vantage Starter Filters are intended to be used instead of the default filter when deploying ACS to avoid unwanted event collection and optimize the initial reporting experience. These filters are progressive based on the type of reporting you are trying to implement and assuming Audit Policies are already enabled for all event types. These filters are great for Proof of Concepts or to start building your own corporate noise filter policy.

*Download the Secure Vantage Noise Filter Kit to and automate your configuration today.*

### Secure Vantage ACS Noise Filter Management v1.0

<h4>Usage Guidelines</h4> <p><i>Note - Filters are guidance ONLY, production usage should be reviewed by IT Security Risk.</i></p> <p>Secure Vantage ACS Noise filters allow you to select a filtering scheme for ACS to ensure you collect the required Security Events to help support Compliance Requirements.</p> <p>Selecting a filter below will set the default ACS filter to the predefined template on your ACS collector.</p>	<h4>Noise Filter Guide</h4>
<h4>ACS Audit Scenarios Noise Filters</h4> <p><i>*Note - All filters are progressive. Default Domain Audit Policies must be defined.</i></p> <ol style="list-style-type: none"><li><b>1. Base Reporting</b> - Provides the ability to Report on Windows Security Events for Account Management, System, Domain Policy Changes, Privilege Use, and Logon Failure.</li><li><b>2. Base Reporting (File Auditing)</b> - Provides the ability to Report on Windows Security Events for Account Management, System, Domain Policy Changes, Privilege Use, Logon Failure, and Object Access (File\Folder).</li><li><b>3. Base Reporting (File Auditing + Directory Services)</b> - Provides the ability to Report on Windows Security Events for Account Management, System, Domain Policy Changes, Privilege Use, Logon Failure, Object Access (File\Folder), and Directory Services.</li><li><b>4. Base Reporting (File Auditing + Directory Services + Logon Success)</b> - Provides the ability to Report on Windows Security Events for Account Management, System, Domain Policy Changes, Privilege Use, Object Access (File\Folder), Directory Services, All Logon\Logoff, and Account Logon.</li></ol>	<h4>Append Current Filter</h4>

**SecureVantage**  
System Center Based Security Solutions

Exit