



Guide for System Center Management Pack for Advanced Threat Analytics

Microsoft Corporation

Published: April 20, 2018

Send feedback or suggestions about this document to mpgfeed@microsoft.com. Please include the management pack guide name with your feedback.

The Operations Manager team encourages you to provide feedback on the management pack by providing a review on the management pack's page in the [Management Pack Catalog](http://go.microsoft.com/fwlink/?LinkID=82105) (<http://go.microsoft.com/fwlink/?LinkID=82105>).

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2013 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Bing, BizTalk, Forefront, Hyper-V, Internet Explorer, JScript, SharePoint, Silverlight, SQL Database, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows Azure, Windows Intune, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

Guide for System Center Management Pack for Advanced Threat Analytics (ATA)	4
Management Pack Purpose	5
Monitoring Scenarios	5
How Health Rolls Up.....	6
.....	7
Links	7
Appendix: Management Pack Contents.....	8

Guide for System Center Management Pack for Advanced Threat Analytics (ATA)

This guide was written based on version 1.9.0.0 of the Management Pack for Advanced Threat Analytics (ATA).

Guide History

Release Date	Changes
September 5, 2017	Original release of this guide
April 20, 2018	Updates for ATA 1.9

Supported Configurations

This management pack requires System Center Operations Manager 2012 R2 or later. A dedicated Operations Manager management group is not required.

The following table details the supported configurations for the Management Pack for ATA:

Configuration	Support
Advanced Threat Analytics	1.7 1.7 Update 1 1.7 Update 2 1.8 1.8 Update 1 1.9
Clustered servers	Not Tested
Agentless monitoring	Not Tested
Virtual environment	Yes

Prerequisites

The following requirements must be met to run this management pack:

- System Center Operations Manager 2012 R2 and later must be installed prior to running the management pack.
- The Windows Server 2008, 2008 R2, 2012, 2012 R2 or 2016 Operating System Discovery management pack must be installed. Use the respective pack to the operating system that ATA Center and Gateways are installed on.
- The ATA Center and Gateway application must be installed prior to the management pack discovering the ATA application components.
 - The ATA Configuration must have 1 directory synchronization candidate enabled. If not the discovery will fail to map the Center and gateways to the correct forest.

Files in this Management Pack

List all downloadable files that are part of the management pack .msi and indicate whether they are optional or required.

The Management Pack for ATA includes the following files:

- Microsoft.AdvancedThreatAnalytics.1.7.mpb
- Microsoft.AdvancedThreatAnalytics.1.7.Overrides.mpb
- Microsoft.AdvancedThreatAnalytics.1.8.mpb
- Microsoft.AdvancedThreatAnalytics.1.8.Overrides.mpb
- Microsoft.AdvancedThreatAnalytics.1.9.mpb
- Microsoft.AdvancedThreatAnalytics.1.9.Overrides.mpb
- Microsoft.AdvancedThreatAnalytics.Library.mpb

Management Pack Purpose

This Management pack defines and monitors the objects for the ATA .


In this section:

- [Monitoring Scenarios](#)
- [How Health Rolls Up](#)

For details on the discoveries, rules, monitors, views, and reports contained in this Management pack, see [Appendix: Management Pack Contents](#).

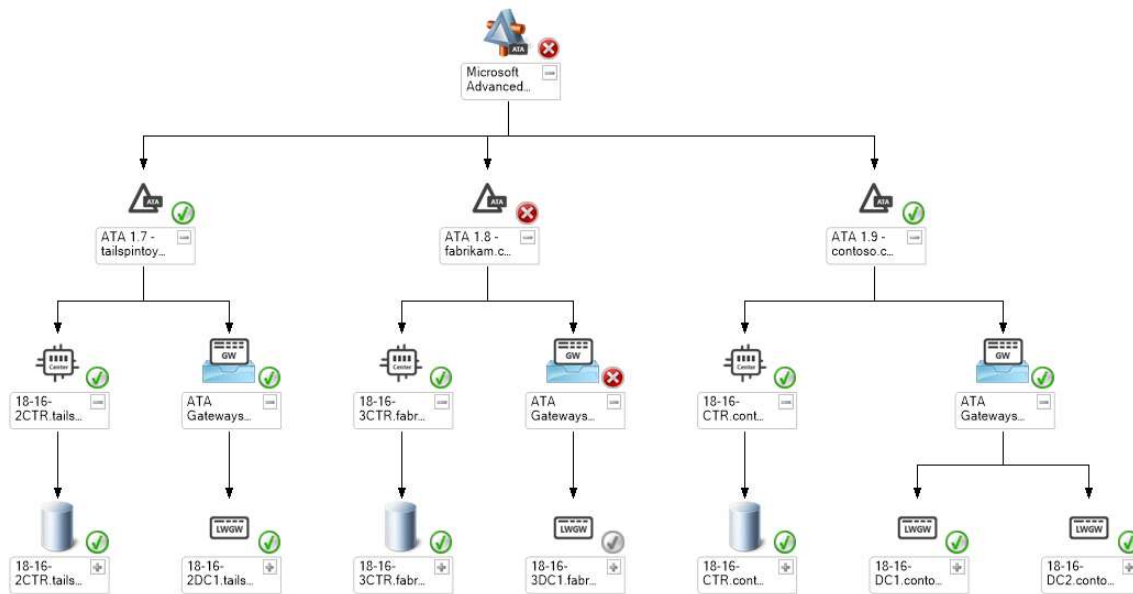
Monitoring Scenarios

The following table describes the key monitoring scenarios that the management pack for Advanced Threat Analytics (ATA) enables.

Monitoring scenario	Description
ATA Center Service Status	Monitors whether the ATACenter service has stopped.
ATA Database Service Status	Monitors whether the MongoDB service has stopped.
ATA Gateway Service Status	Monitors whether the ATAGateway service has stopped.
ATA Gateway Updater Service Status	Monitors whether the ATAGatewayUpdater service has stopped.
ATA Center Performance Monitor	Monitors key performance counters on the ATA Center for indicators of issues. See https://docs.microsoft.com/en-us/advanced-threat-analytics/troubleshoot/troubleshooting-ata-using-perf-counters
ATA Gateway Performance Monitor	Monitors key performance counters on the ATA Gateway for indicators of issues. See https://docs.microsoft.com/en-us/advanced-threat-analytics/troubleshoot/troubleshooting-ata-using-perf-counters
ATA Health Alerts	Monitors ATA Health issues from the ATA Health Center
ATA Suspicious Activity Alerts	Monitors ATA Suspicious Activities from the ATA Suspicious Activity Timeline  Note By Default these rules are disabled. Included are some override packs to enable these.

How Health Rolls Up

The following diagram shows how the health states of objects roll up in this management pack.



Links

The following links connect you to information about common tasks that are associated with System Center management packs:

System Center 2012 - Operations Manager

- [Management Pack Life Cycle](#)
- [How to Import a Management Pack](#)
- [Tuning Monitoring by Using Targeting and Overrides](#)
- [How to Create a Run As Account](#)
- [How to Export a Management Pack](#)
- [How to Remove a Management Pack](#)

Operations Manager 2007 R2

- [Administering the Management Pack Life Cycle](#)
- [How to Import a Management Pack in Operations Manager 2007](#)
- [How to Monitor Using Overrides](#)
- [How to Create a Run As Account in Operations Manager 2007](#)
- [How to Modify an Existing Run As Profile](#)
- [How to Export Management Pack Customizations](#)
- [How to Remove a Management Pack](#)

For questions about Operations Manager and management packs, see the [System Center Operations Manager community forum](#).

A useful resource is the [System Center Operations Manager Unleashed blog](#), which contains “By Example” posts for specific management packs.

For additional information about Operations Manager, see the [System Center 2012 - Operations Manager Survival Guide](#) and [Operations Manager 2007 Management Pack and Report Authoring Resources](#)

 **Important**

All information and content on non-Microsoft sites is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied, or statutory, as to the information at this website.

Appendix: Management Pack Contents

The Management Pack for ATA discovers the object types described in the following sections. Not all of the objects are automatically discovered. Use overrides to discover those objects that are not discovered automatically.

Microsoft.AdvancedThreatAnalytics.Seed.Discovery

Discovery Information

Interval	Enabled	When to Enable
21600 Seconds	True	Not applicable

Microsoft.AdvancedThreatAnalytics.Center.Discovery

Discovery Information

Interval	Enabled	When to Enable
21600 Seconds	True	Not applicable

Related Monitors

Monitor	Data source
Service Status	Checks the status of ATACenter This monitor checks the start and stop status of the ATACenter Service. It does not check the Windows Application log.

All of the following monitors are alerts logged by ATA in the Microsoft ATA log.

Monitor	Data source
Center Database Data Drive Free Space Monitoring Alert	Event ID 1001
Center Overloaded Monitoring Alert	Event ID 1003
Certificate Expiry Monitoring Alert	Event ID 1004
Database Disconnected Monitoring Alert	Event ID 1005
Directory Services Client Account Password Expiry Monitoring Alert	Event ID 1006
Domain Synchronizer Not Assigned Monitoring Alert	Event ID 1007
Gateway Capture Network Adapter Faulted Monitoring Alert	Event ID 1008
Gateway Capture Network Adapter Missing Monitoring Alert	Event ID 1009
Gateway Directory Services Client Connectivity Monitoring Alert	Event ID 1010
Gateway Disconnected Monitoring Alert	Event ID 1011
Gateway Overloaded Event Activities Monitoring Alert	Event ID 1012
Gateway Overloaded Network Activities Monitoring Alert	Event ID 1013
Mail Monitoring Alert	Event ID 1014
Syslog Monitoring Alert	Event ID 1015
Gateways Outdated Monitoring Alert	Event ID 1016
Gateway Not Receiving Traffic Monitoring Alert	Event ID 1017
Gateway Start Failure Monitoring Alert	Event ID 1018
Gateway Low Memory Monitoring Alert	Event ID 1019
Gateway Radius Event Listener Monitoring Alert	Event ID 1020 (1.8 & 1.9 Only)
Gateway Syslog Event Listener Monitoring Alert	Event ID 1021 (1.8 & 1.9 Only)
Center External Ip Address Resolution Failure Monitoring Alert	Event ID 1022 (1.8 & 1.9 Only)

Monitor	Data source
These Monitors are disabled by default.	
Abnormal Behavior Suspicious Activity	Event ID 2001
Abnormal SMB Suspicious Activity	Event ID 2002
Account Enumeration Suspicious Activity	Event ID 2003
Brute Force Suspicious Activity	Event ID 2004
Computer Preauthentication Failed Suspicious Activity	Event ID 2005 (1.7 & 1.8 Only)
Directory Services Replication Suspicious Activity	Event ID 2006
DNS Reconnaissance Suspicious Activity	Event ID 2007
Encryption Downgrade Suspicious Activity	Event ID 2008
Encryption Downgrade Suspicious Activity (Golden Ticket)	Event ID 2009
Encryption Downgrade Suspicious Activity (Overpass the Hash)	Event ID 2010
Encryption Downgrade Suspicious Activity (Skeleton Key)	Event ID 2011
Enumerate Sessions Suspicious Activity	Event ID 2012
Forged Pac Suspicious Activity	Event ID 2013
Honeytoken Activity Suspicious Activity	Event ID 2014
LDAP Simple Bind Cleartext Password Suspicious Activity	Event ID 2015
Massive Object Deletion Suspicious Activity	Event ID 2016
Pass the Hash Suspicious Activity	Event ID 2017
Pass the Ticket Suspicious Activity	Event ID 2018
Remote Execution Suspicious Activity	Event ID 2019
Retrieve Data Protection Backup Key Suspicious Activity	Event ID 2020
SAMR Reconnaissance Suspicious Activity	Event ID 2021
Encryption Downgrade Suspicious Activity (Skeleton Key)	Event ID 2022

Monitor	Data source
Brute Force Suspicious Activity	Event ID 2023 (1.8 &1.9 Only)
Abnormal Sensitive Group Membership Change Suspicious Activity	Event ID 2024 (1.8 &1.9 Only)
Abnormal Vpn Suspicious Activity	Event ID 2025 (1.8 &1.9 Only)
Malicious Service Creation Suspicious Activity	Event ID 2026 (1.9 Only)

Related Rules

Rule	Data source (Performance counter)
All of the rules in this table are enabled.	
Microsoft ATA Center EntityReceiver Entity Batch Block Size	Center\EntityReceiver Entity Batch Block Size
Microsoft ATA Center NetworkActivityProcessor Network Activity Block Size	Center\NetworkActivityProcessor Network Activity Block Size
Microsoft ATA Center EntityProfiler Network Activity Block Size	Center\EntityProfiler Network Activity Block Size
Microsoft ATA Center Database AtSvc Block Size	Center\Database AtSvc Block Size
Microsoft ATA Center Database DirectoryServicesActivity Block Size	Center\Database DirectoryServicesActivity Block Size
Microsoft ATA Center Database Dns Block Size	Center\Database Dns Block Size
Microsoft ATA Center Database Drsr Block Size	Center\Database Drsr Block Size
Microsoft ATA Center Database KerberosAp Block Size	Center\Database KerberosAp Block Size
Microsoft ATA Center Database KerberosAs Block Size	Center\Database KerberosAs Block Size
Microsoft ATA Center Database KerberosTgs Block Size	Center\Database KerberosTgs Block Size
Microsoft ATA Center Database Ldap Block Size	Center\Database Ldap Block Size

Rule	Data source (Performance counter)
Microsoft ATA Center Database LsaRpc Block Size	Center\Database LsaRpc Block Size
Microsoft ATA Center Database Netlogon Block Size	Center\Database Netlogon Block Size
Microsoft ATA Center Database Ntlm Block Size	Center\Database Ntlm Block Size
Microsoft ATA Center Database NtlmEvent Block Size	Center\Database NtlmEvent Block Size
Microsoft ATA Center Database ServiceControl Block Size	Center\Database ServiceControl Block Size
Microsoft ATA Center Database Smb Block Size	Center\Database Smb Block Size
Microsoft ATA Center Database SrvSvc Block Size	Center\Database SrvSvc Block Size
Microsoft ATA Center Database TaskScheduler Block Size	Center\Database TaskScheduler Block Size

Related Views

View	Description	Rules and Monitors that Populate the View
Microsoft Advanced Threat Analytics Alerts	Shows all alerts for the ATA Center and Gateways	All

Microsoft.AdvancedThreatAnalytics.Gateway.Discovery

Discovery Information

Interval	Enabled	When to Enable
21600 Seconds	True	Not applicable

Related Monitors

Monitor	Data source
Service Status	Check the status of ATAGateway and ATAGatewayUpdater

Monitor	Data source
	This monitor checks the start and stop status of the ATAGateway and ATAGatewayUpdater Service. It does not check the Windows Application log.

Related Rules

Rule	Data source (Performance counter)
All of the rules in this table are enabled.	
Microsoft ATA Center Database AtSVC Block Size	Center\Database AtSVC Block Size
Microsoft ATA Center Database DirectoryServicesActivity Block Size	Center\Database DirectoryServicesActivity Block Size (1.7 and 1.8 Only)
Microsoft ATA Center Database DNS Block Size	Center\Database DNS Block Size
Microsoft ATA Center Database DRSR Block Size	Center\Database DRSR Block Size
Microsoft ATA Center Database GroupMembershipChangeEvent Block Size	Center\Database GroupMembershipChangeEvent Block Size (1.8 & 1.9 Only)
Microsoft ATA Center Database KerberosAP Block Size	Center\Database KerberosAP Block Size
Microsoft ATA Center Database KerberosAS Block Size	Center\Database KerberosAS Block Size
Microsoft ATA Center Database KerberosTGS Block Size	Center\Database KerberosTGS Block Size
Microsoft ATA Center Database LDAP Block Size	Center\Database LDAP Block Size
Microsoft ATA Center Database LogicalActivity Block Size	Center\Database LogicalActivity Block Size (1.9 Only)
Microsoft ATA Center Database LogonEvent Block Size	Center\Database LogonEvent Block Size (1.8 & 1.9 Only)
Microsoft ATA Center Database LsaRPC Block Size	Center\Database LsaRPC Block Size

Rule	Data source (Performance counter)
Microsoft ATA Center Database Netlogon Block Size	Center\Database Netlogon Block Size
Microsoft ATA Center Database NTLM Block Size	Center\Database NTLM Block Size
Microsoft ATA Center Database NTLMEvent Block Size	Center\Database NTLMEvent Block Size
Microsoft ATA Center Database SAMR Block Size	Center\Database SAMR Block Size
Microsoft ATA Center Database ServiceControl Block Size	Center\Database ServiceControl Block Size
Microsoft ATA Center Database ServiceInstalledEvent Block Size	Center\Database ServiceInstalledEvent Block Size (1.9 Only)
Microsoft ATA Center Database SMB Block Size	Center\Database SMB Block Size
Microsoft ATA Center Database SrvSVC Block Size	Center\Database SrvSVC Block Size
Microsoft ATA Center Database TaskScheduler Block Size	Center\Database TaskScheduler Block Size
Microsoft ATA Center Database VpnAuthenticationEvent Block Size	Center\Database VpnAuthenticationEvent Block Size (1.8 & 1.9 Only)
Microsoft ATA Center Database Wmi Block Size	Center\Database Wmi Block Size (1.8 & 1.9 Only)
Microsoft ATA Center EntityProfiler Event Activity Block Size	Center\EntityProfiler Event Activity Block Size (1.9 Only)
Microsoft ATA Center EntityProfiler Logical Activity Block Size	Center\EntityProfiler Logical Activity Block Size (1.9 Only)
Microsoft ATA Center EntityProfiler Network Activity Block Size	Center\EntityProfiler Network Activity Block Size
Microsoft ATA Center EntityReceiver Entity Batch Block Size	Center\EntityReceiver Entity Batch Block Size

Rule	Data source (Performance counter)
Microsoft ATA Center EventActivityProcessor Event Activity Block Size	Center\EventActivityProcessor Event Activity Block Size (1.9 Only)
Microsoft ATA Center EventActivityProcessor Postponed Event Activity Block Size	Center\EventActivityProcessor Postponed Event Activity Block Size (1.9 Only)
Microsoft ATA Center LogicalActivityTranslator Event Activity Block Size	Center\LogicalActivityTranslator Event Activity Block Size (1.9 Only)
Microsoft ATA Center LogicalActivityTranslator Network Activity Block Size	Center\LogicalActivityTranslator Network Activity Block Size (1.9 Only)
Microsoft ATA Center LogicalActivityTranslator Unique Activity Block Size	Center\LogicalActivityTranslator Unique Activity Block Size (1.9 Only)
Microsoft ATA Center NetworkActivityProcessor Network Activity Block Size	Center\NetworkActivityProcessor Network Activity Block Size
Microsoft ATA Center NetworkActivityProcessor Postponed Network Activity Block Size	Center\NetworkActivityProcessor Postponed Network Activity Block Size (1.9 Only)
Microsoft ATA Center UniqueEntityProcessor Unique Entity Block Size	Center\UniqueEntityProcessor Unique Entity Block Size (1.9 Only)
Microsoft ATA Gateway NetworkListener PEF Dropped Events/Sec	Gateway\NetworkListener PEF Dropped Events/Sec
Microsoft ATA Gateway NetworkListener ETW Dropped Events/Sec	Gateway\NetworkListener ETW Dropped Events/Sec
Microsoft ATA Gateway NetworkActivityTranslator Message Data # Block Size	Gateway\NetworkActivityTranslator Message Data # Block Size
Microsoft ATA Gateway EntityResolver Activity Block Size	Gateway\EntityResolver Activity Block Size

Rule	Data source (Performance counter)
Microsoft ATA Gateway EntitySender Entity Batch Block Size	Gateway\EntitySender Entity Batch Block Size
Microsoft ATA Gateway EntitySender Entity Batch Batch Send Time	Gateway\EntitySender Entity Batch Batch Send Time
Microsoft ATA Gateway RadiusEventActivityTranslator Radius Packet Block Size	Gateway\RadiusEventActivityTranslator Radius Packet Block Size (1.9 Only)
Microsoft ATA Gateway SyslogEventActivityTranslator String Block Size	Gateway\SyslogEventActivityTranslator String Block Size (1.9 Only)
Microsoft ATA Gateway WefEventActivityTranslator String Block Size	Gateway\WefEventActivityTranslator String Block Size (1.9 Only)

Related Views

View	Description	Rules and Monitors that Populate the View
Microsoft Advanced Threat Analytics Health Alerts	Shows all alerts for the ATA Center and Gateways	All Health Alerts
Microsoft Advanced Threat Analytics Health State	Shows all alerts for the ATA Center and Gateways	Health Rollup
Microsoft Advanced Threat Analytics Performance Alerts	Shows all alerts for the ATA Center and Gateways	All Performance Alerts
Microsoft Advanced Threat Analytics Security Alerts	Shows all alerts for the ATA Center and Gateways	All Security Alerts