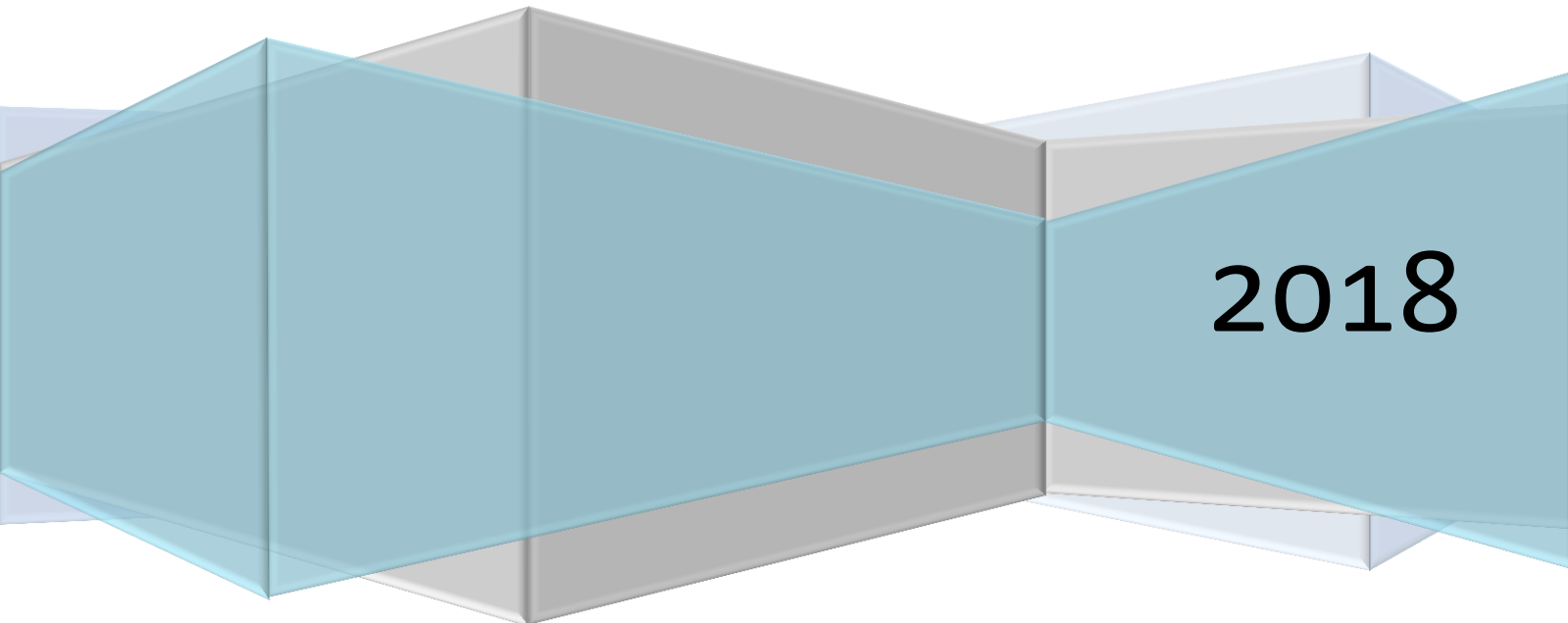


# Applications Manager Architecture Document

[www.manageengine.com/apm](http://www.manageengine.com/apm)



2018

# Table of Contents

Introduction .....	2
Monitoring Capabilities.....	3
How does Applications Manager work? .....	5
System Requirements .....	6
Architecture Overview .....	8
Presentation tier .....	8
Database tier.....	9
Application tier (Business logic).....	9
Applications Manager Editions .....	10
Monitoring Terminology .....	12
Database Tables .....	14
Enterprise Edition Architecture .....	15
Other Monitoring Capabilities .....	16
End User Monitoring.....	16
APM Insight.....	16
Real Browser Monitoring.....	16
Application Discovery and Dependency Mapping (ADDM) .....	17
Rest API Functionality .....	17
Security/Firewall Requirements .....	18
Reports.....	25
Useful Resources.....	26

# Introduction

---

## Overview

ManageEngine® Applications Manager is an on-premise application performance monitoring software that monitors heterogeneous business applications and their underlying infrastructure components. The product supports multiple application types such as web applications, application servers, web servers, databases, network services, servers, middleware and messaging components, ERP software, virtual systems, and cloud resources. It provides remote business management to the applications or resources in the network. It is a powerful tool for system and network administrators, helping them monitor any number of applications or services running in the network without much manual effort.

Applications Manager offers out-of-the-box discovery, availability, health, performance and fault management, and reporting of multi-vendor applications.

Alarms are generated to notify the faults in the application and are configured to trigger actions, such as notifying the user through e-mail, SMS, trap, executing a command and invoking an MBean operation. Through alarms, you can identify the root cause of any problem in the network with just a few clicks. Additionally, the flexible architecture of the Applications Manager allows you to manage any application (J2EE or J2SE) that exposes management information via JMX or SNMP through custom applications.

## Key Features

- Gain deep visibility into the way your business applications perform. Detect slow transactions and resolve performance degradation issues regardless of the cause.
- Get the exact invocation pattern and details related to a transaction. Zoom in on bottlenecks, right down to the minutest detail.
- Monitor the JVM and analyze thread dump of your apps in production. Detect and troubleshoot memory leaks as and when it happens
- Track the before and after effects of your optimization efforts. Ensure your app delivers a fabulous experience to end users.
- Out-of-the-box support for over 80 application servers, servers, databases, ERP, middleware, web servers, Exchange servers, virtual systems, public cloud resources, etc. - all from a single, integrated monitoring console.

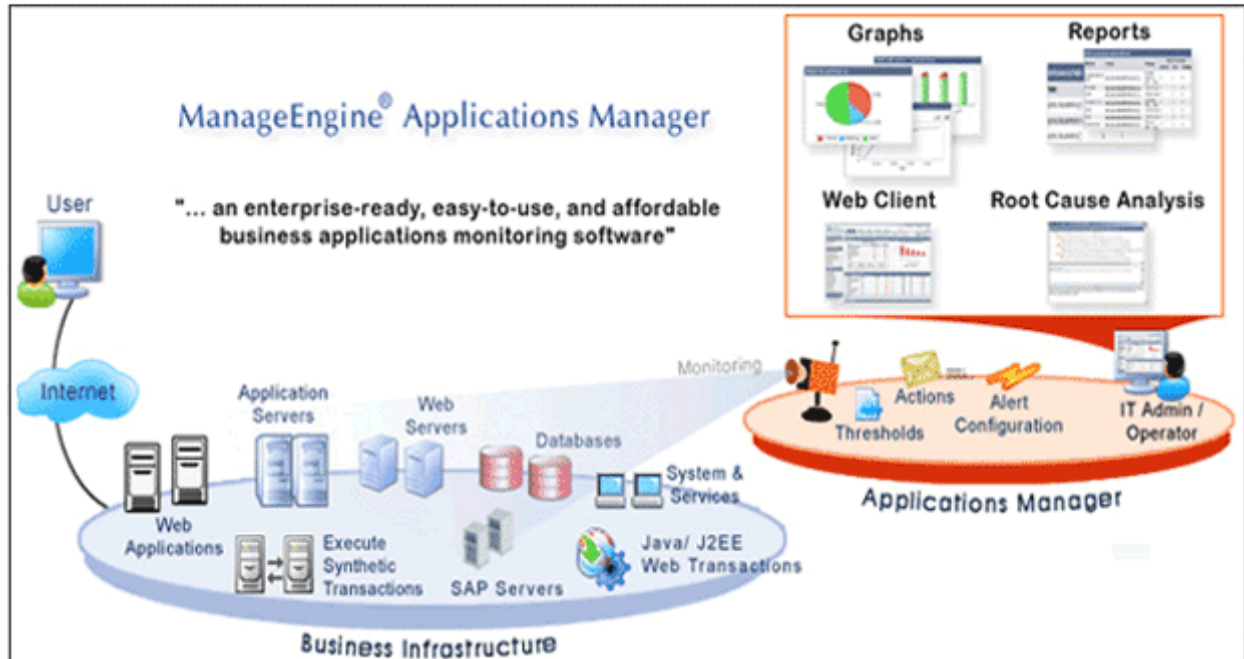
# Monitoring Capabilities

The following are some of the key features of Applications Manager. Apart from the following applications, you can also monitor your own custom applications via scripts.

Feature	Description
<b>Application Server Monitoring</b>	Microsoft .NET, GlassFish, JBoss and Wildfly, Jetty Servers, Oracle Application Servers, Resin Server, SilverStream, Tomcat Servers, VMware vFabric tc Servers, WebLogic Servers, WebSphere Servers, Apache Geronimo and also web-based applications such as Servlets, JSP and EJB of the application servers.
<b>Middleware / Portal Monitoring</b>	Monitors WebLogic Integration, IBM WebSphere MQ, Microsoft Office Sharepoint, Microsoft Message Queue (MSMQ) servers, Microsoft BizTalk, Microsoft Lync Server, Oracle Tuxedo, Azure Service Bus, Apache HBase and Apache Kafka.
<b>SAP Monitoring</b>	Monitors the performance of SAP Servers and SAP CCMS servers.
<b>Oracle EBS Monitoring</b>	Monitors the modules of Oracle E-Business Suite.
<b>APM Insight Monitoring</b>	Comprehensive end-to-end monitoring of Java, Ruby on Rails and .NET web transactions. Provides an indepth view into the performance metrics of all components starting from URLs to SQLs and transaction trace histories.
<b>Virtualization Monitoring</b>	Monitor VMware ESX/ESXi servers, Microsoft Hyper-V servers and their guest virtual machine instances. Support for monitoring Citrix XenServer, XenApp, Docker and virtual infrastructure components such as data center and cluster through vCenter.
<b>Cloud Apps Monitoring</b>	Support for monitoring Amazon EC2 & RDS instances, attached EBS volumes and Amazon S3 buckets. Windows Azure monitor enables users to collect diagnostic data for the applications deployed in Windows Azure platform. Monitor Office 365 applications, including Exchange Online, SharePoint Online and Skype for Business.
<b>Database Monitoring</b>	Supports monitoring of MySQL, MariaDB, Oracle, IBM DB2, DB2 for i, Sybase, MS SQL, CouchBase, PostgreSQL and NoSQL database monitoring for Memcached, Cassandra, MongoDB, IBM Informix, Redis servers.
<b>Host Resource Monitoring</b>	Monitors the performance of Windows, Linux, Solaris, HP Unix, Tru64, Mac OS, Unix, IBM AIX, IBM AS400 / iSeries, Novell and FreeBSD servers. Also monitors Event Logs for Windows and Windows Server Clusters.
<b>Java Runtime Monitor</b>	Provides out-of-the-box remote monitoring and management on the Java platform and of applications that run on it.
<b>File System Monitor</b>	Monitors changes in the selected files and directories.
<b>Windows Performance Counters</b>	Monitors windows performance counter values through WMI.
<b>Ping Monitor</b>	Checks for availability of a device, server or network device.
<b>Script Monitoring</b>	Ad-hoc Windows/Linux custom scripts, used in-house can be managed from the same web console.
<b>Services Monitoring</b>	Monitors Services such as FTP, DNS, SFTP, Hadoop, Telnet, RMI adaptor, TCP port, JMX Applications, Ping, SNMP, Active Directory, LDAP, Apache Solr and Ceph Storage.
<b>Mail Servers Monitoring</b>	Monitors Mail servers (including SMTP servers and POP servers) and Microsoft Exchange Server.
<b>WebServices Monitoring</b>	Monitors Apache, IIS, PHP, SSL Certificate, Web Services (SOAP), nginx and other webservers.
<b>End User Experience Monitoring</b>	Provides the ability to measure the experience of your end users. Includes support for Real Browser Monitor, DNS, Ping, LDAP and Mail Server monitors.

<b>HTTP URL Monitoring</b>	Monitors any HTTP or HTTPS -based URL of web pages.
<b>Custom Application Management</b>	Groups data sources from multiple resources and displays them in a common place. The data sources can be JMX MBeans and SNMP agents.
<b>Root Cause Analysis</b>	Provides details on the different severity levels by identifying its reason/cause.
<b>Fault Management</b>	Sends 'Alarms' based on the monitored attributes. These can be escalated through e-mail / SMS /trap/ MBean Operation/ execute a program.
<b>Performance Reports</b>	The performance of the monitored application is depicted in the form of graphs and charts for easy analysis. Its powerful reporting mechanism enables you to analyze the trends over a period. Scheduling of reports is also possible.
<b>Graphical Representation of Attribute Statistics</b>	The attribute details are represented through graphs that provides an easy approach to understand the "attribute vs time" statistics for one hour. Also the icons and provided in the graphs represent details about the statistics for 7 days and 30 days respectively.
<b>Intuitive Web Client</b>	Allows you to perform admin activities through Web browser interface. You can also monitor and view attributes such as the health and availability of the monitors.
<b>Holistic view to Monitor Group</b>	Manages a wide range of business applications and network services. It provides you the flexibility to group the application and its related services to be monitored as a single unit.
<b>Mobile Web/ iPhone App</b>	An optimized view of applications being monitored for all types of smart phones available in the market.
<b>Business Service Management</b>	Helps the Manager to have an integrated high-level view of the Business Infrastructure. Location intelligence is added via World Map Business View.
<b>Scalable Architecture</b>	Our scalable architecture provides you the ability to monitor a variety of Monitors. It uses a blend of both agent-based monitoring and agent-less monitoring depending on the need.
<b>Product Integration</b>	Integration with ManageEngine ServiceDesk Plus and Site24x7.
<b>Website Content Monitoring</b>	Monitor your websites for defacement, modification and malicious insertions and be notified promptly during a hack detection. Manage six basic HTML elements - Text, Script, Image, Anchor, Iframe and Link.

# How does Applications Manager work?



- Download and Install ManageEngine® Applications Manager in your system.
- Configure the desired monitors (using the web client) via Telnet, SSH or SNMP. To configure, you will need to specify only the host name, credentials and mode of monitoring.
- The performance stats get stored in a MySQL/MS SQL database and you can view the data in the webclient in the form of graphs and reports.
- You can configure alarms (Email, SMS, Execute Program, etc.) when any attribute crosses the configured threshold level. For example, if the CPU utilization of Linux servers cross 90%, you can configure an email alarm to be generated and delivered to along with the root cause analysis of the problem.
- So, you are ready to monitor the various applications and servers in your environment in a matter of few minutes.

# System Requirements

This section lists the system requirements for installing and working with Applications Manager.

- Hardware Requirements
- Real Browser Monitor System requirements
- Software Requirements
- Supported Database Backends
- Supported Browsers

## Hardware Requirements:

The performance of Applications Manager depends considerably on the CPU and memory of the system. The following table describes the recommended configuration of the system running the product.

Up to 250 monitors (with medium load on the monitored servers)			
Operating Platform	Processor Speed	Memory*	Hard Disk Space Required
Windows / Linux	2.4 GHz and above	4 GB RAM	60 GB

250 - 1000 monitors - Enterprise Edition Setup (One Admin & 2-3 Managed Servers)			
Per Managed Server/Admin Server			
Operating Platform	Processor Speed	Memory*	Hard Disk Space Required
Windows / Linux	Dual Core, 2.4 GHz and above	8 GB RAM	80 GB

1000 monitors and above - Enterprise Edition Setup (One Admin & 4 Managed Servers and above)			
Per Managed Server/Admin Server			
Operating Platform	Processor Speed	Memory*	Hard Disk Space Required
Windows / Linux	Quad Core, 2.4 GHz and above	16 GB RAM - Managed Server	100 GB or higher based on monitors

### Note

- The above mentioned memory does not include memory used by OS which should account for another 4 GB
- If the number of Managed Servers is high, 16 GB RAM for the Admin Server is recommended.

## Real Browser Monitor System requirement

**Requirements for the machine where RBM Agent is to be deployed:** RBM Firefox Agents have to be installed on a dedicated Windows / Mac machine - 8 GB RAM, 40 GB HD. RBM Internet Explorer agent (deprecated) have to be installed on a dedicated Windows machine - 4 GB RAM, 40 GB HD with Internet Explorer 6, 7 or 8 (32 bit). However, Applications Manager can be installed on Windows or Linux. This works with the Professional Edition and Enterprise Edition (with Managed Server).

### Software Requirements:

- Supported Operating Systems
  - Windows 7, Windows 8, Windows 10, Windows Server 2008, 2012, 2012 R2, 2016 both 32 and 64 bit.
  - Enterprise Linux 2.1 and above, Debian, Suse, Ubuntu, Mandriva, CentOS, Oracle Enterprise Linux, RHEL 6 and above, Fedora Core both 32 and 64 bit.
- Supported Monitor Resolution
  - Applications Manager is optimized for 1024 x 768 resolutions and above.

**Note:** Do take a look at the [Windows Vs Linux comparison page](#). Compare the capabilities of Windows and Linux variations before proceeding to download the product.

### Supported Database Back-ends

Applications Manager supports PostgreSQL and MS SQL database backends for storing all the configuration information and data collected.

- PostgreSQL comes bundled with your download of Applications Manager from Build 11000. We support PostgreSQL Versions upto 9.3.5 for backend.
- The supported MS SQL database versions that you may use are: MS SQL Servers 2005 / 2008 / 2012 / 2016 / 2017 ( SQL Standard / Enterprise Edition )

**SQL Server Collation:** Any case-insensitive collation. For Chinese Installation use Chinese\_PRC\_CI\_AS

**Note:** Support for existing customers with MySQL database has been deprecated from March 31, 2017.

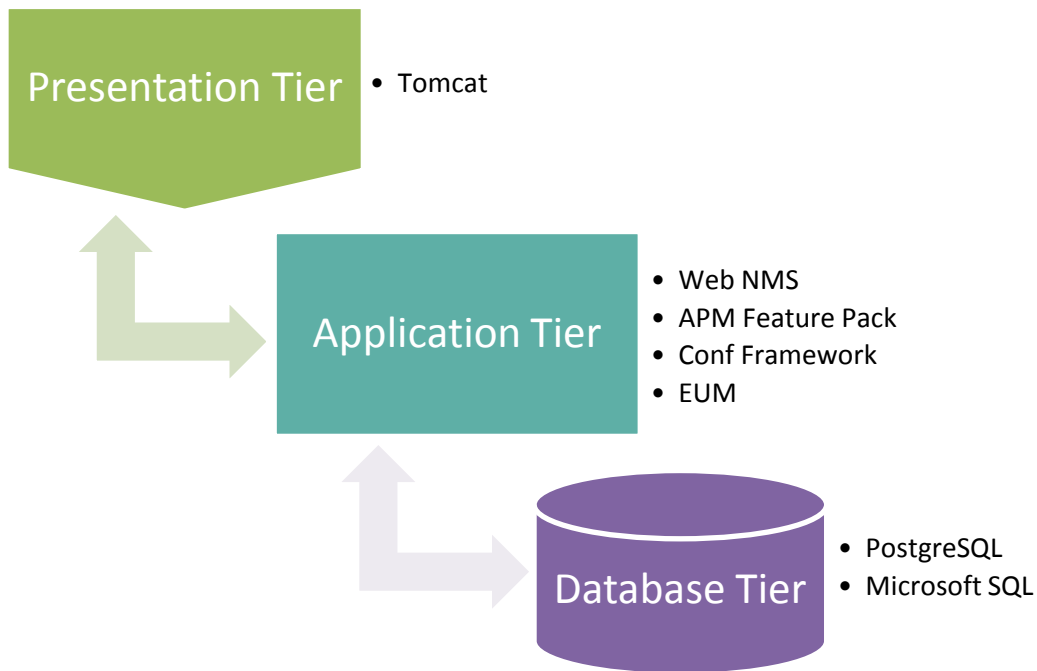
### Supported Browsers

- Internet Explorer 10, 11 and Edge
- Mozilla Firefox
- Google Chrome

# Architecture Overview

---

- Overview
- Presentation Tier
- Application Tier
- Database Tier



## Overview

- Web based Application
- Built using Java (JRE 1.7.0\_71 bundled with product. JRE 1.6.0\_18 used for customers before 12000)
- Installable in Windows (exe) / Linux (bin).
- Both 32-bit and 64-bit installers of Applications Manager installers available.

## Presentation tier

- Tomcat 7.0.21 bundled with product
- Default HTTP port 9090
- HTTPS with self signed certificate enabled by default (port 8443)
- Uses Tomcat Form authentication (j\_security\_check)
- Web content displayed using JSP, Struts 1.1, Jstl 1.x (will be replaced by Ember.js from APM 14)

## Database tier

- Supports PostgreSQL / Microsoft SQL / MySQL as backend database
- PostgreSQL 9.2.4 bundled by default with product since Applications Manager 11000 (older versions bundled with MySQL 5.5)
- Use local database or customer's remote database
- MySQL supported for Old customers / OpManager plugin (steps available for migrating from MySQL to PostgreSQL)

## Application tier (Business logic)

- Web NMS 4.5 with Applications Feature pack used as framework for some monitor types (Servers, MySQL, MsSQL, SAP etc) and alerting.
- New CONF framework used for easily developing new Monitor types. This is a XML driven framework (all monitors will be moved to this framework slowly)
- Standard protocols like SNMP, WMI, JMX, HTTP / HTTPS, SOAP, Rest API, CLI and some custom proprietary protocols used for monitoring

# Applications Manager Editions

## *Free, Professional and Enterprise Editions*

You can meet your specific monitoring needs and unique business objectives by choosing the right edition of ManageEngine Applications Manager. Applications Manager is available in these editions - Free, Professional and Enterprise.

Features	Free	Professional	Enterprise
<b>Out-of-the-box support for 80+ applications</b>	Supports monitoring up to 5 apps or servers. There is no time limit on the free edition - you can use it forever.	Supports integrated performance monitoring for a heterogeneous set of applications. Ideal for small to medium enterprises.	Supports large deployments with its distributed monitoring capability. Ideal for large enterprises.
Server Monitoring	✓	✓	✓
Monitor open source apps & servers	✓	✓	✓
Monitor commercial apps & servers	✓	✓	✓
Application Server Monitoring	✓	✓	✓
Database Monitoring	✓	✓	✓
Website / Web Services Monitoring	✓	✓	✓
SLA Management	✓	✓	✓
Exchange Server Monitoring	✓	✓	✓
Virtualization monitoring	✓	✓	✓
Cloud monitoring	✓	✓	✓
WebSphere MQ Series monitoring	✗	Add-On	Add-On
MS Office SharePoint monitoring	✗	Add-On	Add-On
AS400 monitoring	✗	Add-On	Add-On
ERP monitoring	✗	Add-On	Add-On
Web transactions monitoring for J2EE and .Net (APM Insight)	✗	Add-On	Add-On
Web transactions monitoring for Ruby on Rails (APM Insight)	✓	✓	✓
Integration with Site 24x7	✓	✓	✓
End user monitoring (EUM)	✗	Add-On	Add-On
URL monitoring/multi-step URL sequence monitoring	✗	✓	✓
User administration, network discovery, custom dashboards	✗	✓	✓
ManageEngine OpManager Connector	✗	✓	✓
ManageEngine OpStor Connector	✗	✓	✓

<b>ServiceDesk Plus Integration</b>	<b>✘</b>	<b>✓</b>	<b>✓</b>
<b>Anomaly detection</b>	<b>✘</b>	<b>✓</b>	<b>✓</b>
<b>Admin tools: Downtime scheduler, Trap Listener, Scheduling, enabling, disabling reports.</b>	<b>✘</b>	<b>✓</b>	<b>✓</b>
<b>Updates and patches</b>	<b>✘</b>	<b>✓</b>	<b>✓</b>
<b>Technical support</b>	E-mail Support (30 days)	<b>✓</b>	<b>✓</b>
<b>Failover support</b>	<b>✘</b>	<b>✘</b>	<b>✓</b>
<b>High scalability</b>	<b>✘</b>	<b>✘</b>	<b>✓</b>
<b>Distributed architecture</b>	<b>✘</b>	<b>✘</b>	<b>✓</b>
<b>Supported Operating Systems for Installation</b>	Windows, Linux	Windows, Linux	Windows, Linux

# Monitoring Terminology

---

- Monitors
- Monitor groups and Sub-Groups
- Attributes
- Alarms
- Thresholds
- Actions

## Monitors

A monitor, in Applications Manager terms, is a means of defining an Application, Server, Service or Web URL for monitoring performance, health and availability on the basis of metrics like CPU Usage, Response Time and more. Applications Manager's Monitors keep track of attributes, processes and events on devices they are deployed to, and raise an alert when the device is not operating within specified parameters.

Examples of monitors supported are Windows server monitor, WebLogic monitor, Oracle database monitor, service monitor, URL Sequence monitor, Apache monitor etc. For eg., If you want to monitor 100 SQL Server installations in your network, the 100 SQL Servers will be considered as 100 monitors.

## Monitor groups and Sub-Groups

You can create a logical view of your heterogeneous IT infrastructure by grouping resources, such as applications, servers, and systems in your network. We call the logical view a '**Monitor Group**' and the applications and servers are '**Monitor Types**'.

A monitor Group is particularly useful for grouping the resources of a location say the resources available in sales office or for grouping the resources used by a business application. Applications Manager provides two types of monitor groups - Monitor Group and Web Application Group.

You can also create Sub-Groups within a Monitor Group. Sub-Groups help better organization of your resources. With Sub-Groups, you can capture advanced dependencies in your infrastructure. You can group clustered databases or servers and create complex groups.





## Attributes

Applications Manager collects and explores performance data of the resources that you have set up to monitor. The data collected includes metrics and often times log data which shows major issues in application availability or health. You can define the attributes you want to monitor. Attributes monitored are Numeric and String. You can configure alarms for respective attributes and associate thresholds or actions (or both) to them.

## Alarms

Alarms are notifications generated based on some condition or criteria, helping to detect problems when any of the servers running in the network is experiencing it. This improves the fault management ensuring productive application monitoring

There are four severity levels for the Alarms (denoted by different colors):

- Critical - 
- Warning - 
- Clear - 
- Unknown - 

## Thresholds

Thresholds let you define the status of an attribute based on specific conditions. For example, you can define a threshold to show the status of the web server as critical, if the response time exceeds 100 seconds. Likewise, you can define a threshold to show the status as clear, if the MBean's attribute - Active is equal to true.

The thresholds defined can be associated with the attributes for determining the status of the attributes of the Monitor Group.

## Actions

Applications Manager provides the flexibility in fault management by triggering actions, such as sending e-mail, SMS, trap, and executing a command, to notify you of the alarms generated while monitoring the applications. These corrective actions make fault detection easier and faster enhancing Monitor Group management.

To trigger such corrective actions, you should have defined the action, which can then be associated with an attribute.

# Database Tables

---

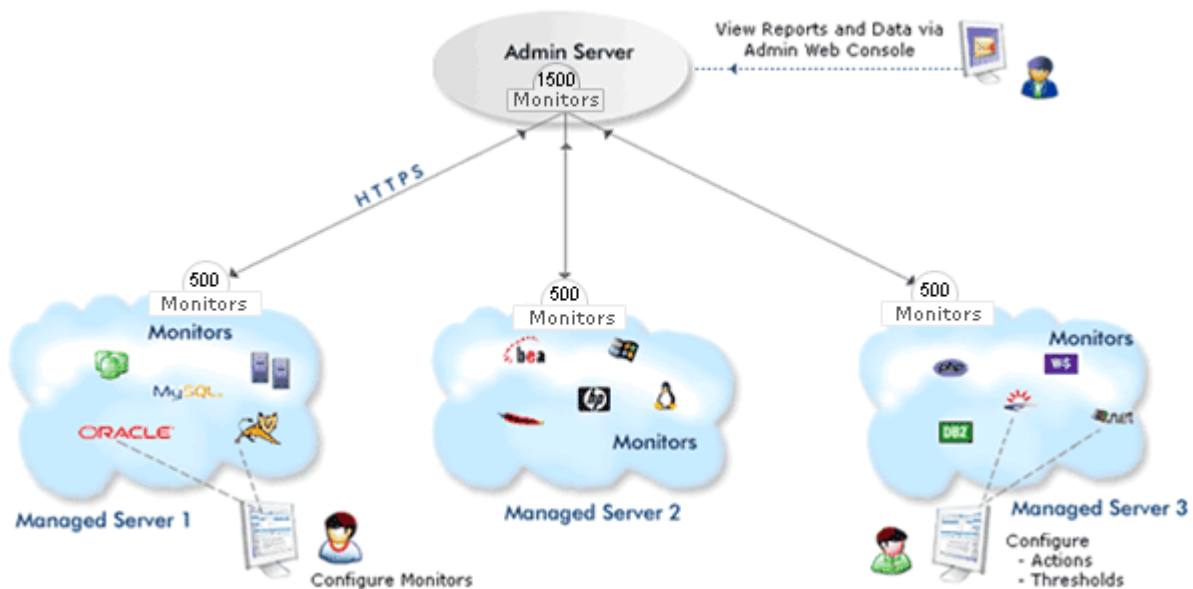
- **AM\_ManagedObject** - The base table used to represent any Application/device/monitor element (also known as MOs). This table extends WebNMS's ManagedObject table
- **AM\_PARENTCHILDMAPPER** - Mapping table for storing relationship between a Parent MO and Child MO
- **AM\_ManagedResourceType** - Base table to store all the first level type of monitors which will be shown in GUI and which will be taken licensed
- **AM\_MONITOR\_TYPES - CONF** table to store TYPEID and other details about CONF monitors
- **AM\_ATTRIBUTES** - Base table to store details about all default Attributes used in APM and their corresponding TYPE
- **AM\_ATTRIBUTES\_EXT** - Table to store Raw data and Archived data table information for all Attributes
- **AM\_ATTRIBUTESDEPENDENCY** - Mapping Table for storing relationship between a Parent ATTRIBUTE and Child ATTRIBUTE
- **AM\_CAM\_DC\_ATTRIBUTES, AM\_CAM\_DC\_RESOURCE\_ATTRIBUTES\_MAPPER** - Table to store custom attributes details and their mapping information
- **AM\_RCAMAPPER** - Mapping table for storing relationship between RESOURCEID and ATTRIBUTEIDs
- **AM\_ResourceConfig** - Contains Username and Encrypted Password for all Non-CONF monitors
- **am\_args\_[TYPEID]** - Contains Username, Encrypted Password and other information provided while adding monitor for all CONF monitors
- **Event** - Contains history of all the alarms generated in Applications Manager. Will be stored for 30 days
- **Alert** - Contains details of the latest Alarm for all attributes (Availability / Health / Attribute for which Threshold associated)
- **AM\_MO\_DowntimeData** - Contains details about the Downtime / Unmanaged time / Scheduled Maintenance time for all monitors in APM
- **AM\_DataCleanupInfo** - Contains details about Data cleanup interval for all tables in Applications Manager

# Enterprise Edition Architecture

Our Enterprise Edition provides an affordable, scalable solution for medium and large enterprises to monitor their applications and underlying infrastructure elements. The Enterprise Edition supports a distributed monitoring architecture and can scale up to 50,000 applications and servers.

The Enterprise Edition comes with all the features offered by Professional Edition. However, Enterprise Edition's ability to scale for larger number of monitors, provide consolidated view from various restricted networks and performance comparisons and failover support are some of its key abilities. The Enterprise Edition comprises of distributed data collectors (Managed Servers) setup. It also provides a single console (Admin Server) for consolidated reports and viewing alarms. The Admin Server facilitates a single view to all data and reports from the various distributed data collectors (Managed Servers).

Applications Manager Enterprise Edition - Architecture



## Highlights

- One Admin with Multiple Managed Servers (MAS)
- Admin - Consolidated view of all monitors, monitor groups, alarms, reports
- MAS - Datacollection for monitors, notifications (actions)
- Additional Features : Failover, Single Sign on, Easy Upgrade

# Other Monitoring Capabilities

---

## End User Monitoring

ManageEngine Applications Manager offers capabilities for measuring the end-user experience of business-critical services from both local and remote locations. Our approach is based on synthetic agent-based monitoring which enables businesses to monitor the response time of these services from branch offices or actual customer locations. Applications Manager's end user monitoring capabilities allow IT teams to

- Ensure business-critical network services such as DNS, LDAP, Ping and mail server as well as web transactions perform well from the end user perspective.
- Categorize performance issues as global or local problems.
- Gain accurate response time information from all critical locations.
- Plan capacity, meet promised SLAs and improve quality of services delivered to the end-users and the business.

## APM Insight

Applications Manager's **APM Insight** provides you with unmatched visibility into the way your business applications behave for your end users. Applications Manager uses Java / Dotnet instrumentation to perform End-to-End realtime monitoring of any Java / Microsoft .Net application with agents manually deployed into the customer's application

## Real Browser Monitoring

With Applications Manager's Real Browser Monitoring recorder, you can easily record web transactions, and then replay the sequence in EUM agents. The recorded sequence is played back in a browser to mimic user behavior and collect the necessary metrics, which are sent to Applications Manager, providing a consolidated view of the data collected across all the agents for easy perusal. With Applications Manager running in your data center you can:

- Gain better visibility into synthetic web transactions with proactive monitoring of availability, response times and page loading time of the recorded web transactions and the individual URLs
- Also have EUM agents deployed in other geographical locations and have them report web application performance data to the central site.
- Get the actual response times of the website transactions dynamically. It waits for the entire page to load inclusive of the media content, along with the text.
- Monitor your website's performance and detect the components (images, javascript, css, etc.) that increase the website's loading time.
- Customize alerts to receive proactive notifications.

## Application Discovery and Dependency Mapping (ADDM)

With Applications Manager's ADDM capability, you discover all the resources (storage, network, applications, servers, and databases) in your IT environment. The vCenter server allows you to discover resources in your entire VMware virtual infrastructure, or you can specify an IP range to discover all resources within that range. You can also schedule periodic re-discoveries to stay updated about new resources. Create business service groups, and let the ADDM feature automatically associate all discovered resources to the desired group. Your CMDB integration and updates are also made effortless.

## Rest API Functionality

---

We provide REST APIs for fetching data and integrating Applications Manager's data with any internal portal or 3rd party System Management software. The data can be represented in a single dashboard itself. By using any XML parser in a scripting language, Java, C, Perl or Python, etc. you can make HTTPs requests in the format recommended in the API. This data can then be inserted into your own database or put in any format that you need.

### How do APIs work?

In order to use the API, each user should obtain an API key - which is a long text and is unique to their Applications Manager Account. The API key has to be passed as parameter in every API request made.

### Generating an API Key

The User can register for the API key from within Applications Manager product using the "REST API" option in the Admin tab.

Here are some examples of Rest APIs:

REST Commands	Description
<b>ListMonitor</b>	This API allows the user to know the availability, health status of monitors, type, state - managed/unmanaged, etc.
<b>ListServer</b>	This API allows the user to know the details of servers like IP Address, status, services running in them, etc.
<b>ListAlarms</b>	This API allows the user to know the details like alarm state - critical/warning/clear, type, top N alarms, time bound alarms, etc.
<b>ListDashboards</b>	This API allows the user to list all the dashboards configured in the Applications Manager.
<b>ListMonitorGroups</b>	This API allows the user to list all the monitor groups and their basic details.
<b>AddMonitor</b>	This API allows the user to the user to add monitors in Applications Manager.

# Security/Firewall Requirements

Firewalls act as barriers preventing unauthorized access to a network. They act as entrance through which authorized people may pass and others not. You must configure the firewall so that the host on which Applications Manager runs, can access the monitor at the relevant port. Ports to be opened when Monitors are behind the firewall:

Monitors	Port Details
<b>APPLICATION SERVERS</b>	
<b>Glassfish</b>	Glassfish JMX port (default : 8686)
<b>JBoss</b>	Two-way communication between JBoss web server port (default : 8080) and Applications Manager web server port (default : 9090). Applications Manager hostname should be accessible from JBoss server. JBoss RMI object port (default : 4444).
<b>Microsoft .Net</b>	Windows Management Instrumentation (WMI) -- Port: 445 Remote Procedure Call (RPC) (default : 135) <a href="#">Know more about the ports required for WMI Mode of monitoring.</a>
<b>Oracle Application Server</b>	Oracle Application Server port (default : 7200)
<b>Tomcat</b>	Tomcat web server port (default : 8080)
<b>VMware vFabric tc Server</b>	JMX port of VMware vFabric tc Server (default : 6969)
<b>WebLogic</b>	Two-way communication between WebLogic listening port (default : 7001) and Applications Manager web server port (default : 9090)
<b>WebSphere</b>	WebSphere application port (default : 9080)
<b>Jetty</b>	Enable JMX for monitoring. The JMX Port for default installations of Jetty is 9999.
<b>CUSTOM MONITORS</b>	
<b>Database Query monitor</b>	Corresponding database server port
<b>File/Directory, Script (Telnet/SSH mode)</b>	Telnet Port: 23 (if mode of monitoring is Telnet) SSH Port: 22 (if mode of monitoring is SSH)
<b>File/Directory, WMI Performance counter (WMI mode)</b>	Windows Management Instrumentation (WMI) -- Port: 445 Remote Procedure Call (RPC) -- Port: 135 <a href="#">Know more about the ports required for WMI Mode of monitoring.</a>
<b>DATABASE SERVERS</b>	
<b>DB2</b>	The port in which DB2 is running (default: 50000)
<b>Memcached</b>	The port in which Memcached server is running (default : 11211)
<b>MySQL</b>	The port in which MySQL is running (default : 3306)
<b>Oracle</b>	The port in which Oracle is running (default : 1521)
<b>PostgreSQL</b>	The port in which PostgreSQL is running (default : 5432)
<b>Microsoft SQL Server</b>	The port in which SQL Server is running (default : 1433). UDP port 1434 might be required for the SQL Server Browser Service when you are using named instances.
<b>Sybase</b>	The port in which Sybase is running (default : 5000)

<b>SAP HANA</b>	SAP HANA's IndexServer port (default: 30015)
<b>Apache HBase</b>	The port in which Hbase is running. For default installations of HBase, the JMX port number is 10101 for Master and 10102 for RegionServer.
<b>NoSQL</b>	
<b>Cassandra</b>	Enable JMX for monitoring. The JMX Port for default installations of Cassandra is 7199.
<b>ERP</b>	
<b>Oracle EBS</b>	Oracle EBS webserver port (default:7200)
<b>Microsoft Dynamic CRM</b>	To monitor a Microsoft Dynamics CRM application, use Administrator user account which has the permission to execute WMI queries on 'root\CIMV2' namespace of the CRM Server. <b>Firewall access for monitoring:</b> Ports required for monitoring via WMI. Windows Management Instrumentation (WMI) (default : TCP 445) Remote Procedure Call (RPC) (default :TCP 135) Target server uses random port above 1024 by default to respond back for remote communication (DCOM) (default : TCP 1025 to 1030)
<b>MAIL SERVERS</b>	
<b>Exchange Server</b>	The port in which Exchange Server is running (default : 25) Windows Management Instrumentation (WMI) (default : 445) Remote Procedure Call (RPC) (default : 135) <a href="#">Know more about the ports required for WMI Mode of monitoring.</a>
<b>Mail Server</b>	SMTP server port (default : 25) to send mails from Applications Manager. POP port (default : 110 ) to fetch mails using the POP server.
<b>MIDDLEWARE/PORTAL</b>	
<b>IBM WebSphere MQ</b>	The MQ Listener Port (default:1414)
<b>Microsoft MSMQ/SharePoint Server</b>	Windows Management Instrumentation (WMI) -- Port: 445 Remote Procedure Call (RPC) -- Port: 135 <a href="#">Know more about the ports required for WMI Mode of monitoring.</a>
<b>VMware vFabric RabbitMQ Server</b>	The Port ID where the management plugin is configured (default : 55672)
<b>WebLogic Integration Server</b>	WebLogic Integration port (default : 7001)
<b>Oracle Tuxedo</b>	The SNMP port number , on which the Tuxedo SNMP agent is running. The default port number is 161.
<b>Apache ActiveMQ</b>	The port in which ActiveMQ is running.
<b>Apache Kafka</b>	The default JMX port: 9999. <a href="#">Reference link.</a>
<b>SERVERS</b>	
<b>AS400/iSeries</b>	To connect AS400/iSeries server from Applications Manager it uses JTOpen package. The JTOpen package uses the following Non-SSL ports 449, 446, 8470, 8471, 8472, 8473, 8474, 8475, 8476. Ensure that the ports mentioned under "Port Non-SSL" column in the link are not blocked in firewall. <a href="http://www-01.ibm.com/support/docview.wss?uid=nas1acc12fda96496e4b8625668f007ab75f">http://www-01.ibm.com/support/docview.wss?uid=nas1acc12fda96496e4b8625668f007ab75f</a>
<b>Linux / Solaris / AIX / HPUnix /Tru64 Unix</b>	Telnet Port (default : 23), if mode of monitoring is Telnet. SSH Port (default : 22), if mode of monitoring is SSH SNMP Agent Port (default : 161), if mode of monitoring is SNMP

<p><b>Windows</b></p>	<p><b>For WMI Mode of Monitoring:</b></p> <p>To monitor a Windows Server the user must have "Administrator" privileges. Ports required -</p> <p>Windows Management Instrumentation (WMI) (default : 445) Remote Procedure Call (RPC) (default : 135)</p> <p>WMI uses DCOM for remote communication. The server to be monitored by applications manager uses a random port number above 1024 by default to respond back. You have to connect to this target server and configure it to use a port within a specified range of ports. You can follow the steps mentioned in this link : <a href="http://support.microsoft.com/kb/300083">http://support.microsoft.com/kb/300083</a> for restricting the ports in the target server. Note that you must specify at least 5 ports in this range for target server ( you are normally recommended to open at least a 100 ports - <a href="http://support.microsoft.com/kb/217351/EN-US/">http://support.microsoft.com/kb/217351/EN-US/</a> ). This same range of ports must also be opened in the firewall.</p> <p>In Windows Server 2008 and later versions, and in Windows Vista and later versions, use the following dynamic port range:</p> <p>Start port: 49152 End port: 65535</p> <p>If your computer network environment uses only Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows 8, Windows 7, or Windows Vista, you must enable connectivity over the high port range of 49152 through 65535.</p> <p>Windows 2000, Windows XP, and Windows Server 2003 use the following dynamic port range:</p> <p>Start port: 1025 End port: 5000</p> <p>If your computer network environment uses Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows 8, Windows 7, or Windows Vista together with versions of Windows earlier than Windows Server 2008 and Windows Vista, you must enable connectivity over both the following port ranges:</p> <p>High port range 49152 through 65535 Low port range 1025 through 5000 SNMP Mode of monitoring: Ports required - SNMP Agent Port: 161</p>
<p><b>SERVICES</b></p>	
<p><b>Active Directory</b></p>	<p>Windows Management Instrumentation (WMI) -- Port: 445</p> <p>Remote Procedure Call (RPC) -- Port: 135 Also refer to ports required for WMI Mode of monitoring under Servers</p>
<p><b>FTP/SFTP</b></p>	<p>Port in which FTP or SFTP is running (default:21 for FTP, 22 for SFTP)</p>

<b>JMX [ MX4J / JDK 1.5]</b>	<p>Port of JMX agent (default:1099)</p> <p>To monitor JMX behind firewall the following changes have to be done.</p> <p>Edit startApplicationsManager.bat/sh file. Add -Dmonitor.jmx.rmi.port=&lt;port number for RMI socket communication&gt; to the Java runtime options.</p> <p>Restart Applications Manager server</p> <p>Ensure that you have the RMI Socket port (step1) and JNDI Port (step4) are opened up in the firewall</p> <p>Add the JMX Applications monitor after providing the relevant details.</p> <p>The monitor should be added successfully</p>
<b>LDAP</b>	LDAP server port
<b>Service Monitoring</b>	The service port that you need to monitor
<b>SNMP</b>	SNMP Agent port (default:161)
<b>Telnet</b>	Port which you need to telnet
<b>Apache Zookeeper</b>	<p>Port of JMX agent (default:1099)</p> <p>If Authentication is enabled, enter the Username and password for connecting to the JMX agent. To know more about monitoring a <a href="#">JMX Application if your application is behind a firewall, check out this blog post.</a></p>
<b>Oracle Coherence</b>	Enable JMX for monitoring. The JMX Port for default installations of Coherence is 1099.
<b>Hadoop</b>	Enable JMX for monitoring. The JMX port of the NameNode.
<b>TRANSACTION</b>	
<b>APM Insight</b>	Applications Manager's Web Server port should be accessible from the APM Insight agent server (default:9090).
<b>VIRTUALIZATION</b>	
<b>Hyper-V</b>	<p>Windows Management Instrumentation (WMI) -- Port: 445</p> <p>Remote Procedure Call (RPC) -- Port: 135</p> <p>Also refer to the ports required for WMI Mode of monitoring under Servers</p>
<b>VMWare ESX/ESXi</b>	VMWare Web Service port (default:443)
<b>Citrix XenServer</b>	The https Port where the XenServer web service runs. The default port is 443.
<b>Docker</b>	The Docker socket port. (default port: 4243).
<b>WEB SERVER/SERVICES</b>	
<b>Real Browser Monitor (Qengine port)</b>	The qeport (default:5001) mentioned in the AppManager_Homeworkingconfqeruntime.properties file should be accessible from the machine where you want to Record RBM webscripts
<b>SSL Certificate Monitor</b>	SSL port in which the web server is running (default:443).
<b>Web Server - Apache / IIS / PHP</b>	HTTP Port of Web Server (default:80).
<b>Elasticsearch</b>	The port on which the ElasticSearch is running (default: 9200).
<b>Apache Solr</b>	The port on which the ApacheSolr is running (default: 8983)

Miscellaneous	
<b>Trap Listeners</b>	Trap Listener port (default:1620) in Applications Manager server should be accessible from the server where you want to send traps. More on receiving SNMP Traps.
<b>Web User Experience Monitoring</b>	Make sure you are connected to the internet and can access Site 24X7.

Applications Manager makes sure that data is secure. The internal PGSQL database allows only the localhost to access the database through authenticated users. User Names and Passwords are stored in the PGSQL database that is bundled along with the product. The passwords are encrypted to maintain security.

### Privileges required for different monitor types:

Monitors	Privileges
<b>Active Directory</b>	Administrator username/password [WMI mode]
<b>Amazon</b>	The AWS Access Key Id for accessing the AWS through the API. The access key has 20 alpha-numeric characters. The Secret Access Key of the AWS. The secret key should be 40 alpha-numeric characters long.
<b>Apache Server</b>	Credentials for accessing the server status url for Apache
<b>AS400/iSeries</b>	To retrieve data for all modules in AS400/iSeries monitor except 'Disk', an user with *USER user profile is required. To retrieve data for 'Disk' and to perform Admin actions from Applications Manager, an user with *SECOFR user profile is required. If using the *SECOFR user profile is not possible, then for retrieving disk data and to perform the admin actions such as viewing spooled file, job log and performing actions in JOBS, SPOOL, SUBSYSTEM a user profile with special authorities such as *ALLOBJ, *SAVSYS, *JOBCTL, *SPLCTL is required. The user should have permission to access QMPGDATA/QPFRDATA library because Applications Manager uses performance collection service for retrieving disk details from AS400/iSeries server. Note: If the performance data collection is not enabled in AS400/iSeries, you need to start it by using the command STRPFCOL or GO PERFORM-->COLLECT PERFORMANCE DATA-->START PERFORMANCE COLLECTION. You will also be able to execute the STRPFCOL command from AS400/iSeries server monitor page in Admin-->Non-Interactive command option.
<b>Database Query Monitor</b>	User with privileges for accessing a particular database and execute the query
<b>DB2</b>	User with atleast SYSMON instance level authority
<b>Exchange Server</b>	Administrator username/password [WMI mode]
<b>File/Directory</b>	User with privileges for accessing the File or Directory to monitor

<b>FTP/SFTP</b>	If Authentication is enabled, enter the Username and Password for connecting to the FTP/SFTP server & move to required directory
<b>Glassfish</b>	Username and password for connecting to Glassfish Admin console
<b>HP-UX</b>	Guest user privilege
<b>HTTP URL</b>	If basic authentication is required enter the same in monitor
<b>Hyper-V</b>	Administrator privileges to the root OS (Windows 2008 R2 and other supported Hyper-V versions)
<b>IBM AIX</b>	Guest user privileges are sufficient but "root" privileges are required for collecting Memory related details. Hence, it is preferable to use a "root" account to view all the details
<b>IBM WebSphere MQ</b>	A Channel name with type of "Server Connection Channel"
<b>JBoss</b>	Use the JBoss username/password (if Jboss is authenticated). User should be able to access the JBoss JMX console. If not, no username/password is required
<b>JMX/Java Runtime</b>	<a href="#">If Authentication is enabled, enter the Username and password for connecting to the JMX agent. To know more about monitoring a JMX Application if your application is behind a firewall, check out this blog post.</a>
<b>LDAP</b>	If Authentication is enabled, enter the Username and Password. If no username and password is provided, then it will connect to LDAP server as an anonymous login.
<b>Linux</b>	Guest user privilege
<b>Mail Server</b>	If Authentication is enabled, enter the Username and password for connecting to the SMTP and POP
<b>Microsoft .Net</b>	Administrator username/password [WMI mode]
<b>Microsoft Office SharePoint Server</b>	Administrator username/password [WMI mode]
<b>MS SQL</b>	System Administrator/Owner for the "master" database
<b>MSMQ</b>	Administrator username/password [WMI mode]
<b>MySQL</b>	The User-name specified should have access to the databases to be monitored. MySQL should also be configured. This allows the host on which App Manager is running to access the MySQL database.
<b>Oracle</b>	User with CONNECT and SELECT_CATALOG_ROLE roles
<b>SAP/SAP CCMS</b>	You need a SAP user profile with the following authorization objects: S_RFC, S_XMI_LOG and S_XMI_PROD which are the minimum prerequisites for adding a SAP monitor. We use the SAP Java Connector to connect to the SAP ABAP server. The SAP JCo will communicate from APM to SAP using the SAP Dispatcher. The SAP Dispatcher port to be used is 3200 with the SAP System number.
<b>Script monitor</b>	User with privileges for executing the script and accessing the output file.
<b>Server with SNMP mode</b>	SNMP Community string with read privileges.

<b>SNMP/Network device</b>	<p><b>For SNMP Version V1/V2c:</b> SNMP Community string with read only privileges.</p> <p><b>For SNMP Version V3:</b> Select one of the three Security Levels in the drop-down list:</p> <ul style="list-style-type: none"> <li>• NoAuthNoPriv - Messages can be sent unauthenticated and unencrypted. Enter a UserName and Context Name.</li> <li>• AuthNoPriv - Messages can be sent authenticated but unencrypted. Enter a UserName, Context Name and an Authentication Password. You can select an Authentication Protocol like MD5 or SHA from the drop-down list.</li> <li>• AuthPriv - Messages can be sent authenticated and encrypted. Enter a UserName, Context Name, an Authentication Password and a Privacy Password. You can select an Authentication Protocol like MD5 or SHA from the drop-down list. By default 'DES' encryption technique will be used.</li> </ul>
<b>Solaris</b>	Guest user privilege.
<b>Sybase</b>	The user should have admin privileges or the DB owner for master database.
<b>Tomcat</b>	<p>For 5.x and above, a username and password is required to connect to Tomcat Manager Application. If not, no username/password is required.</p> <p>For 5.x the user specified should have a 'manager' role.</p> <p>For 6.x and above, the user specified should have "manager-gui", "manager-script", "manager-jmx" and "manager-status" roles.</p>
<b>VMWare ESX/ESXi</b>	<p>When adding VMWare ESX/ESXi servers for monitoring, we recommend that you use the root account. However, if you are unable to use the root account, you can use a 'view-only' profile to add the servers. This profile has all the privileges required for monitoring. The user you create must be:</p> <ul style="list-style-type: none"> <li>• a member of the group user.</li> <li>• based on the profile 'read only'.</li> </ul>
<b>VMware vFabric RabbitMQ Server</b>	User Name and Password of RabbitMQ server.
<b>WebLogic</b>	Use the WebLogic username/password, if WebLogic is authenticated. The user should be an administrator. Otherwise, no username/password is required.
<b>WebLogic Integration Server</b>	Use the WebLogic username/password, if WebLogic is authenticated. User should be an administrator. Else no username/password is required.
<b>Webservices</b>	Give the User Name and Password, if it is required to invoke the webservice operation.
<b>WebSphere</b>	If Global Security is enabled, use the same username/password . If not, no username/password is required.
<b>Windows</b>	Administrator username/password [WMI mode].

**Enterprise Edition**

Path	Ports
Admin to Managed Server	SSL Port (default 8443) - for database syncing Webserver (default 9090).
Managed Server to Admin	SSL Port (default 8443).

## Reports

---

Perform trend analysis, identify bottlenecks, and plan for your IT environment requirements from the real-time graphs and comprehensive performance reports that are generated. The graphs and reports can be viewed on a custom-defined hour, daily, weekly, and monthly basis and can be generated quickly. They also provide visibility into Mean Time To Repair (MTTR) and Mean Time Between Failures (MTBF) for each application/service. Downtime & Summary reports are also provided. All the reports can be scheduled according to your preference (for eg., you can schedule the delivery of summary reports every monday at 10.a.m). You have the added ability to compare the reports. You can generate different reports based on the resource type: Business Application report, Application Server report, Database Server report, Service report, Server report, and Custom Application report. The reports generated can be exported to CSV or PDF formats.

# Useful Resources

---

**Online Help Documentation:**

<http://help.appmanager.com>

**Contact Support:**

appmanager-support@manageengine.com