

Splunk® App for Microsoft® Exchange

Real-time Monitoring and Auditing for Microsoft Exchange

HIGHLIGHTS

- Monitor key Exchange Server metrics
- Identify issues, reduce the mean time to repair and maintain maximum uptime
- Deliver integrated, centralized view of entire Exchange infrastructure from one place

Today's Exchange environments are critical to business success and customer satisfaction. A disruption in email services can mean losing orders, missing out on important customer communications and damaging your organization's reputation. Add to this the increasing volume of cyber-security attacks along with the need to support mobile devices, and your IT organization's ability to provide support can quickly reach a breaking point. IT departments need to deliver email services that are constantly available and so having deep operational insight to the inner workings of their Exchange infrastructure is mission critical.

Splunk App for Microsoft Exchange

The Splunk App for Microsoft® Exchange answers the call of IT departments globally. Traditional email management tools only notify you of an "up or down" status or are incapable of tracking email messages beyond the Exchange boundary. By contrast, the Splunk App for Microsoft Exchange delivers a data-rich and easy-to-use platform to make your Exchange Infrastructure visible and simple to manage. The Splunk App for Microsoft Exchange collects metrics and logs from Microsoft Exchange Server and its underlying infrastructure (including Internet, servers, Windows event logs from security, Exchange audits and application events and add-ons like Blackberry Enterprise Server). Now Exchange IT professionals can view real-time and trending dashboards and reports to reduce mean time to repair problems. IT organizations can view service availability, usage patterns and traffic flow, while also drilling into details on performance and security.

With Splunk App for Microsoft Exchange you can:

- Identify infrastructure problems, such as non-running services and load issues
- Monitor the performance of all servers throughout your messaging environment
- Track messages throughout your messaging environment
- Monitor client usage, including mobility usage via ActiveSync or Blackberry Enterprise Server
- Monitor security events, such as virus outbreaks and anomalous logons

- Track administrative changes to the environment
- Analyze long-term mail operations trends
- Plan for capacity expansion
- Monitor your organization's outbound email sender reputation

Splunk App for Microsoft Exchange Features

The Splunk App for Microsoft Exchange provides several specialized features to monitor Exchange data, including:

Health Dashboards

Provides up-to-the-minute information on the health of your Exchange environment, including service availability, message throughput and organizational reputation.

Dashboard views include:

- Senderbase Reputation – Detailed review of your organizations external reputation
- Services Availability – List of servers that are not running services that should be running
- Non-Reporting Servers – Microsoft Exchange Servers that have not reported status updates

Message Tracking

Provides a break-down of the flow of messages through the system. IT administrators will appreciate the fact that they can segment internal from Internet traffic. Messages can be tracked at any granularity necessary. Also, messages can be tracked beyond the boundaries of the Exchange system, allowing the administrator to view activity by anti-spam, anti-virus and archiving services.

Dashboard views include:

- Inbound Message Tracking – View messages entering the email system
- Outbound Message Tracking – View messages leaving the email system



Analyze and report dynamically and iteratively.

- Internal Message Tracking – View messages flowing within the email system
- Track a Message – Track messages with the email system
- Message Activity for Username – Track email activity by user
- Message Activity for an IP Address – Track what an IP address is sending or receiving
- Message Activity for a Domain – Track what messages have been sent or received from a domain

Client Behavior

Provides in-depth visibility into how the users are utilizing the email service. This includes the methods of access and mailbox usage statistics. By allowing the user to identify user trends, the Exchange administrator can identify issues before users notice and take remedial action

Dashboard views include:

- Mailbox Store Overview – Top users in a mailbox store
- Microsoft Outlook Overview – OWA access data internally and externally
- Outlook Web Access Overview – OWA usage over a given time and by operating system
- Microsoft ActiveSync Overview – ActiveSync connections by user, device and connection time
- Outlook Anywhere Overview – Outlook Anywhere usage data by user or IP address
- Exchange Web Services Overview – Exchange Web Service usage data
- POP3 and IMAP4 Overview – Clients using POP3 or IMAP4 connectivity
- Blackberry Enterprise Server Overview – Information on users and load for BES
- Client Activity for a Username – How users are connecting and their location
- External Logins Map – Google Map™ showing user log in location

Operations

Displays views of the performance of your Exchange infrastructure from an operations perspective.

Dashboard views include:

- Client Access – Performance details broken down by the client type selected protocol
- Mailbox Store – Views about the use and capacity of your Mailbox Store servers.
- Forefront Security – Views into the health and status of Forefront Security for Exchange
- Exchange 2010 Administrator Audit – Search for change events initiated by administrators

- Anomalous Logins Report – Failed logins by IP address and username

Capacity Planning

Displays information about the volume of email and number of users your system is handling over time to help you to plan for future expansion.

Dashboard views include

- Sizing – Message Volume - Displays number of messages an organization receives
- User Population – How many users use the Exchange Server resources.
- Environment Report – Overview of all of the information on your Exchange Server

Product Requirements

Supported Exchange Server Versions

Splunk App for Microsoft Exchange supports Microsoft Exchange 2007 and 2010 with Microsoft Forefront Security running on Windows Server 2003 or later.

Splunk Requirements

Splunk App for Microsoft Exchange requires Splunk® Enterprise™ on Windows v4.2 for deployment to the Exchange Servers. Splunk App for Microsoft Exchange UI requires Splunk Enterprise v4.3 or later, Sideview Utils v1.2.5 or later and Google Maps™. Sideview Utils™ and Google Maps are available as a free download on Splunkbase.

Free Download

[Download Splunk](#) You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. You can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

Try Out the App, it's Free!

Go to www.splunk.com/microsoft to learn more.