

Dynatrace Managed provides all the monitoring capabilities on-premise within your own data center. All monitoring data remains on your infrastructure, ensuring full compliance with legal and other regulatory requirements.

Dynatrace Managed is pro-actively monitored and managed remotely from the Dynatrace Mission Control team.

### Contractual obligations for customers and for Dynatrace

Since Dynatrace Managed is running inside a customer's data center, the customer has to provide the necessary hardware including Operating System according to the specifications of the Dynatrace Managed offering: <https://help.dynatrace.com/managed/install-and-configure/what-arehardware-and-software-requirements/>.

Upon purchasing Dynatrace Managed the customer will receive an email with the license information and all instructions to download and install a Dynatrace Managed cluster. After installation Dynatrace Managed has to be integrated with other existing services, such as user authentication/IDM, email servers, etc. A user can install custom certificates for added security.

The customer has to ensure outbound access of the Dynatrace Managed cluster nodes to the Internet for remote management and consumption tracking to a specific set of fixed IP addresses.

The Dynatrace Managed cluster is automatically upgraded whenever a new version is released. The upgrade is performed at a user specified time, at least once a week Dynatrace Managed must be allowed to update itself. If a new version of Dynatrace Managed is released, the actual upgrade is announced via email at least 24 hours before it is executed. An upgrade can be rescheduled after it has been announced, or it can be executed immediately instead of waiting for the next scheduled update time. The Dynatrace Managed cluster installation updates itself automatically at the user specified time without further manual interaction. During upgrades or other maintenance work the Dynatrace Managed User interface may not be available for up to one hour, collection of metrics is typically uninterrupted.

Dynatrace Managed clusters maintain compatibility with Dynatrace agents for at least 6 months. The update of Dynatrace agents is fully under the control of the Dynatrace Managed users and different policies can be applied to different environments.

Bugfixes and security patches for both Dynatrace agent and cluster are only available for the latest available versions.

### Mission Control and Service Quality

The Dynatrace Mission Control team monitors the service quality and hardware utilization of Dynatrace Managed and alerts if additional hardware is needed to monitor a customer's environments. The Dynatrace Mission Control team can also tune the configuration of Dynatrace Managed to ensure highest service quality and best utilization of the provided hardware. All configuration changes are fully audit-logged.

Dynatrace Managed cluster automatically sends self-monitoring and consumption metrics to Dynatrace Mission Control. Based on this the Mission Control proactively detects and analyzes any misconfigurations or potential incompatibilities with your technologies and applications. For this purpose, the team can retrieve log files from the Dynatrace Managed cluster, Dynatrace agents or crash dumps that may be related to Dynatrace Managed.

To resolve specific problems, the Dynatrace Mission Control team can also release special hotfixes or security patches, which are applied as regular updates at a user specified time.

The Dynatrace Mission Control may reach out to a customer via email or phone in case a specific problem requires local interaction.

Dynatrace Mission Control ensures overall availability of Dynatrace Managed cluster at 99% or more for the UI and 99.5% or more for the collection of monitoring data. Any hardware, network or other infrastructure-related outages that are in the responsibility of the Dynatrace customer have to be excluded from these availability metrics.