Managed Services
Security

365 ManagedIT

To take care of your IT environment, 365 Managed IT uses sophisticated, feature-rich software that handles many security concerns in its architecture. This document describes how it works, and suggests ways that you can establish a solid overall security strategy for your business.

The monitoring software that we use consists of three main components: *Onsite Manager*, *Device Manager*, and *Service Center*.

What is Onsite Manager?

Onsite Manager is a light-weight piece of software that is installed on a server attached to your network. It automatically performs comprehensive scans of your environment, gathering up-to-date information that 365 Managed IT needs to manage your IT assets with unparalleled efficiency. It does this using standard management protocols already in place. It doesn't collect private data.

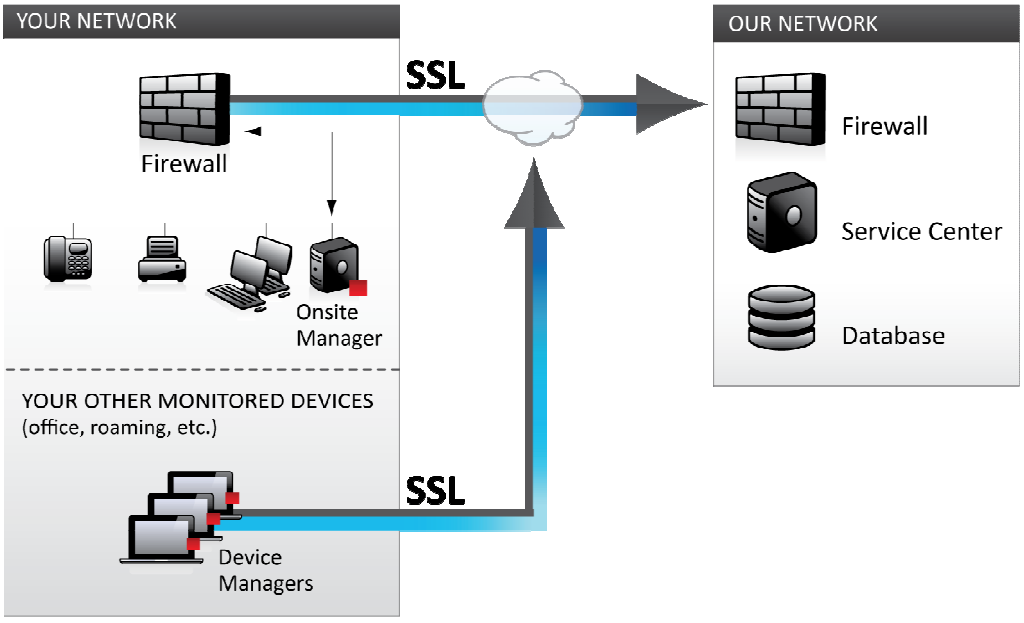
What is Device Manager?

Device Manager is installed on equipment that can't be directly monitored by the Onsite Manager, such as roaming laptops, servers in remote offices or data centers, home offices, or if your business doesn't have a server. Like the Onsite Manager, it doesn't collect private data.

What is Service Center?

Service Center is a powerful, web-based, centralized dashboard that allows your Managed Services Provider to view the asset health and performance data sent by the Onsite Manager, drill down to details as required, perform rapid remote remediation, configure advanced services and produce a range of useful reports to manage your network.

Your Network and Our Network



Onsite Manager and Device Manager Security – Your Network

How is Your Data Collected?

WMI and SNMP
Onsite Manager and Device Manager use standard Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP) and other industry standard protocols to provide management data describing the system configuration and status.

Intel® vPro™ [If installed]
Onsite Manager collects active management data made available by devices with Intel® vPro™ using credentials you provide. This secures the collection of the out-of-band and low-level hardware statuses of these devices. The information is collected over a secure network.

No Inbound Ports Required
There are absolutely no inbound connections to Onsite Manager. Onsite Manager makes outbound connections on standard communications ports, port 80 and port 443 for secure connections through Secure Sockets Layer (SSL) and establishes a connection with Service Center. This means that the monitoring provided by Managed Workplace does not require any external access to your networks, and no external source can gain access.

How is Your Data Protected?

Data Access
The data collected from Onsite Manager is only temporarily held in the database in compressed and encrypted packages until it is sent to Service Center. The Service Center database is not accessible on the Internet.

No Web Interface
Onsite Manager does not have a web interface. This means that only a user who has direct logon access to the server where it is installed can access it.

Service Account
Onsite Manager uses standard access control, requiring a service account that is like any other domain Administrator user and is subject to all the domain-enforced security rules. Administrators can manage service accounts individually to determine the level of access for each account. Service Center also uses Microsoft domain credentials to authenticate access to the database and Web resources it displays.

Device Managers use the Local System account to manage and monitor devices. This is a special, highly secure account that is used by Windows to handle processes launched by the operating system.

Proprietary Communications to Service Center
All communications between Onsite Manager, Device Manager, and Service Center employ a proprietary communications scheme that is compressed, SSL-encrypted and protected by a secret key that only the deployed Onsite Manager, Device Managers and Service Center know. Even users of Managed Workplace do not know what this key is since it is generated and stored internally to the Managed Workplace application.

SSL (Secure Sockets Layer)
SSL (Secure Sockets Layer) is used to encrypt communication between Onsite Manager, Device Managers and Service Center to provide an additional security layer for communications. It further confirms the identity of the servers to which the communications are being sent.

Security Monitoring
By default and based on Microsoft best practices, Microsoft Baseline Security Analyzer (MBSA) will run once a week to scan and assess the security of all Windows devices.

Service Center Security - Our Network

Access Control

Authenticated Access to Web – Encrypted in Database
Access to the web console is authenticated and encrypted in the database. Credentials, in the form of a user name and password, are always requested. The resulting string is then encrypted and sent to the database.

Physical Access to Servers
As an extra security measure, physical access to the servers is monitored and controlled.

Remote Access

For the remote control tools to work, the domain account on the server where Onsite Manager is installed requires Administrator access. This is a secure account and our staff does not need to know these credentials; only Managed Workplace needs to know.

While communications are bi-directional, only Onsite Manager and Device Manager establish connections to Service Center. And although remote control may imply a two-way connection, it is an outbound request that establishes the remote connection. Requests are generated from your site through Onsite Manager. There is NO inbound communication or open port requirements to be configured on customer firewall devices.

The following describes the remote control workflow:

An authenticated Service Center user must be logged into Service Center to make a remote control request. At the time of the request, the Managed Workplace remote control client software is installed on the operator's computer and the Service Center identifies that a remote session is trying to be established. This client software must be present for the Service Center to accept the request and for remote access to function, and cannot be used unless authenticated through the Service Center.

Onsite Manager and Device Managers establish regular connections to Service Center to determine if any remote control sessions are requested. After recognizing and validating that a request has been made, a TCP tunnel between Onsite Manager or Device Manager and Service Center is established, and Onsite Manager or Device Manager acts as a software router to direct secure communications between the technician and the remote client workstation. If it determines for some reason that the remote control session is either unattended, or if the remote control session ended abruptly, it will closes the outbound session automatically.

Secure Communications

Authenticated Web Services
Service Center only makes limited functionality available publicly through a secured web service (authenticated with a trusted key that only Managed Workplace knows about), which limits what requests can be made of the system.

The monitoring provided by Managed Workplace does not require any external access to your networks and no external source can gain access.

Encrypted Service Center User Names and Passwords

User names and passwords are encrypted using MD5 encryption in the database. MD5 is a one-way only encryption method that calculates a hash (a hexadecimal number) unique to a set of data. It is a widely used Internet standard.

Network Protection

Firewall and Network Configuration
Device Manager uses a compact database that is not publicly accessible when protected by a firewall. The database that stores Onsite Manager data is not publicly accessible if it is behind a firewall.

Security Software
By applying security software, you protect your information and business assets.

Backup
Backups are useful to restore information after a disaster or after files have been accidentally deleted or corrupted.

Contact Us for More Information

365 Managed IT
602-490-0990
Phoenix, AZ
info@365ManagedIT.com
www.365ManagedIT.com