

Architecture Overview - Hosted

<https://campus.barracuda.com/doc/89620611/>

Barracuda Managed Workplace is made up of four components:

- [Service Center](#)
- [Onsite Manager](#) or [Device Manager](#)
- [Support Assistant](#)
- Barracuda Managed Workplace Update Service

Service Center is installed on servers in your hosting provider's data center. Service Center is the web-based management application where users perform their work and also the database where all the client information resides.

Onsite Manager and Device Managers collect client data and send it to Service Center over the Internet. Use Onsite Manager to collect data and manage many devices. Use Device Manager to collect data and manage a single device.

The Onsite Manager performs agentless monitoring, collecting information from all types of IP-based devices, including computers running any operating systems as well as routers, printers and other infrastructure devices.

The Device Manager is an agent, monitoring information only from the device upon which it is installed.

Both Onsite Managers and Device Managers regularly initiate outbound communications to Service Center to receive new instructions and upload the data that has been collected.

Note: Barracuda Managed Workplace doesn't support the monitoring of clusters.

Service Center

Service Center is installed in your hosting provider's data center and has been provided with adequate resources to accommodate your needs. The application is designed to scale with high-demand occupancy, so you can be confident you are always operating at optimal efficiency.

This means there is no administration to the actual environment required on your part, with the exception of managing integration with any Professional Services Automation (PSA) application you use.

Other Applications

Service Center can optionally integrate with other applications to extend workflow capabilities:

PSA applications Provides integration with third-party professional services automation (PSA) systems for comprehensive ticket tracking and issue management. Most partners use a PSA system to assist them with project and resource management. Service Center integrates with the most popular, powerful applications available today, and can also be integrated with custom solutions.

See Also: [Professional Services Automation \(PSA\) Integration Guide](#)

Onsite Manager

Onsite Manager uses Microsoft SQL Server 2014 Express edition and .NET Windows Services. It is capable of handling up to 1000 devices, in healthy environments with basic monitoring requirements. As such the database engine and the application reside on the same physical server. Dedicating a server to Onsite Manager is recommended for larger networks and when more thorough or frequent monitoring is required. For an average SMB client, you can typically install Onsite Manager onto a shared server.

Best Practice: When deploying a single Onsite Manager to monitor more than 500 devices, start with a basic monitoring service policy set, and layer in other monitoring, automated tasks, and patch management activity one configuration at a time, keeping track of any changes to the performance of the server at each stage (CPU, RAM, and disk activity).

Important: When installing onto a shared server, you must ensure that the resources specified as the system requirements are available during the client's production hours. (For information about the Onsite Manager system requirements, see [Onsite Manager](#).) Otherwise you are introducing contention for the server's resources, which can cause both Onsite Manager and its other roles to be performed less than optimally.

Best Practice: When there is another option available, you should avoid installing Onsite Manager on Domain Controllers or other mission-critical servers. Web or file servers are favorable when available.

Database Component

The Onsite Manager uses Microsoft SQL Server 2014 Express, included in the installation package, to house the Barracuda Managed Workplace database:

MWData Stores the monitoring rules that have been defined in Service Center, which direct the activities of the Onsite Manager application. It also contains the information about IP addresses and their associated devices. During periods where Internet connectivity is interrupted, monitoring data is queued in the database to be sent to Service Center once the connection has been restored.

Best Practice: Install Microsoft SQL 2014 Management Studio Express when you install Onsite Manager so that you have a tool to back up your database, and are ready to receive technical support should it be required.

Application

The Onsite Manager application makes use of three Windows services:

MWExpertSystem Handles all the querying of managed devices for data, and also listens for data being sent to it, such as SNMP traps or Syslog messages. To function correctly, it must run with Administrator privileges to ensure it can gather all the information you are requesting from the devices.

MWExpertSystemHelper Uses Microsoft Background Intelligent Transfer Service (BITS) to download large automated task files from Service Center.

OMNetworkService Controls all the remote sessions users launch.

Device Manager

Device Manager is the functional equivalent of the Onsite Manager but monitors and manages a single device only. Device Manager can be deployed to a Windows or Mac OS X device. There is a lightweight database that is bundled with the application for data storage.

For information about the Device Manager system requirements, see Device Manager and Support Assistant.

On Windows devices, the Device Manager makes use of a single Windows service:

MWExpertSystem Runs under the security context of the Local System account unlike that for the Onsite Managers. Also, because only a single device is being managed, the transfers normally handled by the MWExpertSystemHelper and remoting normally handled by the OMNetworkService are included in this service.

Support Assistant

Support Assistant is your company's brandable presence on managed Windows and MAC OS X devices and includes a context menu and an icon which is delivered in one of two ways:

- as a recommended feature of the Device Manager when the profile used is configured to display an icon in the notification area
- independently by configuring an automated task

The brandable icon can be a 16 x 16 pixel image of your corporate logo, or any other icon that you choose. You can also add another icon to indicate a fault state so the user knows when something is not working properly with the Device Manager.

You can determine what additional functionality is offered on the context menu, which end users will access by clicking the icon. For example, you can include text-based messages for the end user, shortcuts to email and web addresses, allow them to request live chat or remote assistance, and offer the ability to send trouble tickets to Service Center.

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.