Service Center System Requirements

https://campus.barracuda.com/doc/85492992/

Service Center

Service Center is resource-intensive. This means production systems should be dedicated to Barracuda Managed Workplace. Sharing a server with other applications results in contention for resources, particularly memory and disk throughput, which can significantly impact the performance of all applications on the server.

Memory and disk space requirements listed in this section must be dedicated to Service Center, so additional resources are required for the server operating system and any other roles performed.

Best Practices

•For easier scaling as you grow your usage of Barracuda Managed Workplace, it is recommended that you implement a two-server deployment.

• To reduce the possibility of data loss, store database backups on another

system or device in addition to the SQL server.

•It is not recommended to install Service Center on Exchange servers or Hyper-V hosts, as these systems are typically extremely busy, and an installation could result in resource contention.

•Additionally, it is not recommended that you install Service Center on domain controllers, which can pose a security risk.

Note: The storage space required for the database, database backups, and transaction logs will vary based on product usage, including the number of sites and devices monitored, monitoring configurations, and data retention settings.

Single Server Deployment

A single server deployment consists of the Service Center application and SQL server residing on the same server.

Occupancy	Hardware Minimums

1 - 5 sites (1 - 150 devices)	• 4 logical CPUs • 8 GB RAM • 2 volumes with the following roles: ◦ Volume 1 (500 GB) plus size of physical RAM for OS Page File - install OS, SQL databases, and transaction log. Recommended RAID: 10 or 1. ◦ Volume 2 (500 GB) - Separate volume to store database backups and isolate the backup files in case of hardware failure. Recommended RAID: 10, 5, or 1.
5 - 25 sites (150 - 650 devices)	• 4 CPUs • 8 GB RAM • 2 volumes with the following roles: ◦ Volume 1 (500 GB) plus size of physical RAM for OS Page File- install OS, SQL databases, and transaction log. Recommended RAID: 10 or 1. ◦ Volume 2 (500 GB) - Separate volume to store database backups and isolate the backup files in case of hardware failure. Recommended RAID: 10, 5, or 1.

Two Server Deployment

A two server deployment consists of the Service Center application and SQL server hosted on separate servers.

Occupancy	Hardware Minimums
25 - 50 sites (650 - 1300 devices)	• Application server: 8 logical CPUs with 8 GB RAM and 120 GB disk space for storage • Database server: 8 logical CPUs with 12 GB RAM and 2 volumes with the following roles: ◦ Volume 1 (500 GB) plus size of physical RAM for the OS Page File- install OS, SQL databases, and transaction log. Recommended RAID: 10 or 1. ◦ Volume 2 (500 GB) - Separate volume to store database backups and isolate the backup files in case of hardware failure. Recommended RAID: 10, 5, or 1.

50 - 100 sites (1300 - 3000 devices)	• Application server: 8 logical CPUs with 8 GB RAM, and 120 GB disk space for storage • Database server: 8 logical CPUs with 16 GB RAM, and 4 volumes with the following roles: ◦ Volume 1 (120 GB) plus size of physical RAM for the OS Page File- install OS and application files. Do not install database files, transaction logs, or SQL backups. Recommended RAID: 1. ◦ Volume 2 (200 GB) - Location of database data files, including TempDB. Recommended RAID: 10 or 5. ◦ Volume 3 (100 GB) - Location of transaction logs for all databases. If you are using Full Recovery model, a larger capacity is recommended. Recommended RAID: 10 or 1. ◦ Volume 4 (500 GB) - Storage of SQL Database backups. If you are using Simple Recovery model, you can use a combination of full database backups and differentials. Recommended RAID: 10, 5, or 1.
3,000 - 10,000 devices	• Application server: 8 logical CPUs with 8 GB RAM, and 120 GB disk space for storage • Database server: 8 logical CPUs, 32 GB RAM and 4 volumes with the following roles: ◦ Volume 1 (120GB) plus size of physical RAM for the OS Page File- install OS and application files. Do not install database files, transaction logs, or SQL backups. Recommended RAID: 1. ◦ Volume 2 (200 GB) - Location of database data files, including TempDB. Recommended RAID: 10 or 5. ◦ Volume 3 (100 GB) - Location of transaction logs for all databases. If you are using Full Recovery model, a larger capacity is recommended. Recommended RAID: 10 or 1. ◦ Volume 4 (500 GB) - Storage of SQL Database backups. If you are using Simple Recovery model, you can use a combination of full database backups and differentials. Recommended RAID: 10, 5, or 1.

10,000 - 25,000 devices	• Application server: 8 logical CPUs, 16 GB RAM, and 120 GB disk space for storage. • Database server: 8 logical CPUs, 64 GB RAM, and 6 volumes with the following roles: ◦ Volume 1 - 120 GB plus size of physical RAM for the OS Page File and SQL application. Recommended RAID: 1. ◦ Volume 2 (200 GB) - SQL database data files, exclusing TempDB. Recommended RAID: 10 or 5. ◦ Volume 3 (100 GB) - SQL database transaction log files, except TempDB. If using Full Recovery model, a larger capacity is recommended. Recommended RAID: 10 or 1. ◦ Volume 4 (200 GB) - SQL TempDB data files, which are placed in this volume to be isolated for performance reasons. Recommended RAID: 10 or 1. ◦ Volume 5 (200 GB) - SQL TempDB transaction log file, which is placed on this volume to be isolated for performance reasons. If you choose not to create this volume, put the TempDB transaction log file where the other transactions logs are located. Recommended RAID: 10 or 1. ◦ Volume 6 (500 GB) - Storage of SQL Database backups. A combination of full database backups and differentials can be used if using Simple Recovery model. Recommended RAID: 1.

Software

All the software listed in this section has passed performance testing with Barracuda Managed Workplace 2013. While it may be possible to install on other flavors of Windows or other required applications, it is not recommended because support may be limited for any products not explicitly listed.

Installation

The following installer is required:

- Windows Installer 4.5

Operating System

A 64-bit server operating system is recommended, and Barracuda Managed Workplace will install natively for either 32- or 64-bit operating systems. When installing on a 64-bit operating system, all required software components must be 64-bit. The following operating systems are supported:

- Microsoft Windows Server 2016 (Standard and Datacenter)
- Microsoft Windows Server 2012 (Essentials, Standard, and Datacenter)
- Windows Server 2008 R2 (Web, Standard, Enterprise and Datacenter)
- Windows Server 2012 R2 (Essentials, Standard, and Datacenter)

Application Frameworks

The following application frameworks are required:

- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 4.6.0 or higher (4.6.1 or higher is recommended)

Web Server

The following web servers are supported:

- Microsoft Internet Information Services 7.5, 8, and 8.5

Notes:

- When using SSL with IIS 7.x, the web server must be configured to Ignore client certificates. This is the default setting.

Database Server

Several versions of Microsoft SQL Server are supported, but the recommended version is Microsoft SQL Server 2016. Microsoft SQL Server 2016 provides functionality not available with other versions. For more information, see https://blogs.msdn.microsoft.com/sqlreleaseservices/sql-server-2016-service-pack-1-sp1-released/.
The following database servers are supported:

- Microsoft SQL 2016 (Recommended)
- Microsoft SQL 2014
- Microsoft SQL Server 2012 with Reporting Services (Standard or Enterprise)
- Microsoft SQL Server 2008 SP1 or R2 with Reporting Services (Enterprise Edition) with
  - Microsoft SQL Server 2008 Management Objects
  - Microsoft SQL Server 2008 Native Client
  - Microsoft .Net 3.5 SP1

Important: Virtualization of SQL Server with Barracuda Managed Workplace is not supported because of performance concerns for CPU and disk performance. Barracuda Managed Workplace heavily relies on SQL Server for data loading, reporting, and high speed transactions, therefore it is recommended that you do not virtualize the SQL Server to ensure that the system is responsive, performs well, and to reduce complexity in deployment and troubleshooting. Data Centers typically encourage real hardware except where databases serve light applications such as blogs.

Important: For performance and management reasons, the Service Center databases should be housed in its own database instance on a dedicated system.

Mail Server

Barracuda Managed Workplace will work with any SMTP server. Authentication and port options are configurable.

Web Browser

- Microsoft Internet Explorer 10 and 11
- Google Chrome current version
- Mozilla Firefox current version
- Safari (Mac OS and iOS - partial)

Network Requirements

The following lists the networking requirements for Service Center:

80 TCP inbound Access to the SCMessaging and SC websites over HTTP. This is not required if using SSL.

80 TCP outbound Access to the license server and WSUS meta data server. This is not required if using SSL.

443 TCP inbound Access to the SCMessaging and SC websites over HTTPS. This is only required if using SSL.

1433 TCP outbound from the application to the database server Access to the database server.

2195 TCP outbound Access to Apple web service (gateway.push.apple.com) for mobile device management feature.

2196 TCP outbound Access to Apple web service (feedback.push.apple.com) for mobile device management feature.

The following lists the networking requirements for Service Center:

80 TCP inbound Access to the VARAdmin, SCMessaging and SC websites over HTTP.

80 TCP outbound Access to the license server and WSUS meta data server.

443 TCP inbound Access to the VARAdmin, SCMessaging and SC websites over HTTPS.

2195 TCP outbound Access to Apple web service (gateway.push.apple.com) for mobile device

management feature.

2196 TCP outbound Access to Apple web service (feedback.push.apple.com) for mobile device management feature.

Firewall exceptions for the SCMonitor.exe and SCworker.exe applications must be made on each application server to allow for communications on all TCP ports where the source IP Addresses are those of the other application servers.

Required External Sites for Barracuda Managed Workplace

The following table outlines the external sites that must be allowed by security products for Barracuda Managed Workplaceto function properly.

Note: In addition to these sites, the URL where Service Center is installed must be accessible for communication between Onsite Manager, Device Managers, and managed devices.

Site	Service Center	Onsite Manager	Device Manager	Technician's Computer
https://www.avg.com Links to various product pages	X			
https://support.avg.com Links to Knowledge Base articles	X			
https://wl.msp1services.com/lookup.php Warranty lookup service	X			
https://www.update.microsoft.com Patch metadata, wuident.cab	X	X		
http://ds.download.windowsupdate.com Windows self update URL		X		
http://download.mwrmm. barracudamsp.com/ Update Center components, initial patch metadata, Service Center online help	X	X	X	
https://ss01.ccrmm.avg.com Network Assessment	X			
https://whatsmyip.ccrmm.avg.com Whats My IP service		X		
https://lplic.levelplatforms.com License service, telemetry service, Service Center locator	X	X	X	
https://www.levelplatforms.com Update center metadata	X			

https://sso.avg.com Centrify SSO	X			
https://www.islonline.net/ download PRC Viewer and Server	X		X	X
https://download.microsoft.com Used by setup to download required components (prerequisites)	X	X	X	
https://sws.update.microsoft.com Used to connect to Microsoft patch management	X	X		

Required External Sites for Avast Business Antivirus Pro Plus

If you're using Avast Business Antivirus Pro Plus, the following external sites must be allowed by security products:

- *.avast.com
- *.avcdn.net

Required External Sites for Service Modules

If you're using a service module, consult the documentation for the integrated program for any external sites that are required for communication.

Technician's Computer

A technician's computer requires the following:

- Web browser (recommend Internet Explorer)

Browser and Operating System Support for Remote Control and Remote Tools

This table identifies what feature works in which browser:

Browser	Remote Control	Remote Tools	Premium Remote Control
Internet Explorer	Yes	Yes	Yes
Mozilla Firefox	Yes (plugin)	Yes	Yes
Google Chrome	Yes (plugin)	Yes	Yes
Apple Safari	No	Yes	Yes
Opera	No	Yes	Yes

Note: Remote control will fail if you are prompted for a plugin and choose not to install it. If you also select the Don't Show this Message Again check box, you will not be offered the choice to install the required plugin on subsequent attempts, and the connection will fail without further messages. To be prompted for plugin installation again, you must remove the cookies for the Service Center site and then install the plugin when prompted.

This table identifies what feature works in which operating system:

Operating System	Remote Control	Remote Tools	Premium Remote Control
Windows	Yes	Yes	Yes
macOS	Yes (requires the server software for the selected protocol)	No	Yes
Linux	Yes (requires the server software for the selected protocol)	No	No

Note: The remote tools are not supported on Windows 2000 computers because .NET 3.5 is required on the target device. Windows 2000 does not support .NET 3.5.

SQL Server

SQL Server Hardware and Operating System Configuration

Note: Several versions of Microsoft SQL Server are supported, but the recommended version is Microsoft SQL Server 2016.

The information in this section is intended for advanced users or users with Database Administrator experience.

If you are using a dedicated SQL server (that is separate from the system where Service Center will be installed), it is recommended that:

- other database applications are not using the SQL instance or system;
- you do not install other SQL instances on the same machine.

Additionally, you should ensure the following:

- Because SQL Server relies heavily on RAM for efficiency, it is recommended to provide as much RAM as possible.
- At a minimum, use a gigabit Ethernet LAN connection between the SQL Server and the application server and SQL Report server.
- The Windows Page file should be enabled, located on a storage system that is separate from the SQL data and transaction volumes, and explicitly set to at least the same size as the system's physical memory.
- To maximize performance and reduce potential configuration complexities, install SQL server on a physical machine and not in a virtual environment. An example of a performance issue that can occur is if you are running on hardware-based NUMA and the virtualization technology is not configured properly.
- RAID 10 is recommended for all data volumes to maximize performance and minimize downtime. In particular, it is not recommended to use RAID 5 for transaction logs. For example, if there is a hard drive failure and you have to rebuild the array, you might be prevented from doing so due to reduced performance and incomplete parity data or data damage. Additionally, Barracuda Managed Workplace is a write-intensive application, and RAID 5 is less efficient at performing writes.
- For large deployments, it is recommended to have an Active/Passive SQL Failover Cluster to minimize outages should hardware issues occur.

SQL Server Configuration

The following SQL Server configuration settings are recommended:

- Use the Simple Recovery model for the databases, which includes changing the system model database to SIMPLE. Set the model database data file to 2 GB, the model log file to 2 GB, and set the growth in increments of 1 GB for both data and log files.
- Pre-allocate the TempDB data files and TempDB transaction log file to at least 2 GB.
- System with high speed IO and multiple CPUs may benefit from multiple TempDB data files. For more information, see Microsoft's guidelines for multiple TempDB files.
  Note: Do not exceed a ratio of 1:4 or 1:2 TempDB data files to CPUs. Typically, 1 file is used. If multiple data files are required you should set them to identical file sizes. It is not advised to exceed 8 files.
- When setting the maximum memory that SQL Server can use, leave at least 2 to 10 GB of RAM for the operating system.

SQL Server Operational Maintenance

Barracuda Managed Workplace has a built-in database maintenance feature that includes all the necessary procedures to ensure the database is optimized and cleans up the old data which includes index maintenance and defragmentation, statistics updating, and data cleanup based on retention

settings. You are not required to configure maintenance plans in SQL Management Studio or to

implement your own maintenance for the MW SQL databases.

Additionally, do not shrink database data files unless there is critically low space situation. Shrinking data files causes high index fragmentation, requires a lot of CPU and IO, and generates a lot of transaction log activity.

SQL Server Back Ups

When backing up SQL databases, use either native SQL Server backups, which are configurable through SQL Management Studio using maintenance plans, or use a third party back up solution that interacts with the SQL database engine, causing a checkpoint. Back up technologies that freeze or lock the database files from SQL Server are not supported.

The following database backup practices are recommended:

- File system snapshots cause IO stalls, therefore it is not recommended that file system snapshots be used. IO stalls can cause user latency in Service Center, and can cause expected internal operations run by Service Center to encounter an unexpected error if it times out, which could leave the application in a degraded state.
- For quick recovery, store a copy of the SQL database backups locally on the SQL server. It is also recommended to store copies of the SQL database backups on another storage device (such as another computer or an external hard drive) that is separate from the SQL server's main storage. This ensures that backup files can be recovered if there is a hardware failure on the SQL Server.
- It is not recommended that you back up the databases by making copies of the MDF or LDF files.
- Run back ups outside of business hours.

SMTP Server

If you are using IIS SMTP, you should have a cleanup routine to delete "badmail" email files from the file system, which can accumulate if Barracuda Managed Workplace alert emails are configured to be sent to invalid email addresses.

TLS 1.2

By default, new installs of Managed Workplace use TLS 1.2.

Enabling TLS 1.2 requires:

- Previous versions of TLS and SSL are disabled.
- The device you are installing Service Center on is up to date with all Microsoft Security Updates. Below is a table of the required hotfixes and updates as of Sept 2018.

Operating system	Hotfixes
Windows 7 SP1 Windows 2008 R2 SP1	• Support for TLS System Default Versions included in the .NET Framework 3.5.1 on Windows 7 SP1 and Server 2008 R2 SP1 • Update for Windows (Select from list)
Windows 8.1 and Windows Server 2012 R2	• Support for TLS System Default Versions included in the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 • Update for Windows (Select from list)
Windows 10 Version 1607 and Windows Server 2016	• Cumulative Update for Windows 10 Version 1607

- The SQL server for Service Center is hotfixed to the latest updates.

Server	Hotfix
SQL server	• FIX: You cannot use the Transport Layer Security protocol version 1.2 to connect to a server that is running SQL Server 2014 or SQL Server 2012