
About Installation - Hosting Provider

<https://campus.barracuda.com/doc/86544978/>

Review all documentation prior to performing an installation so that you are familiar with the procedures involved.

Resources will be assigned to you to assist with the installation and configuration of the hosted Service Center environment.

Access to Software

Barracuda Managed Workplace installation packages are available on the Partner Portal. You will be provided with a login and password so that you can download the installers.

Service Center installer A download that does not contain any redistributables. If a component is missing from the computer you are installing to, you can use a download link to fetch it.

Onsite Manager installer Does not contain any redistributables, but will check for any missing components and will provide a link to download the product on Microsoft's website.

Note: The Onsite Manager installer can also be downloaded from within Service Center, in the Site Management page.

Onsite Manager appliance installer Used with Microsoft's System Preparation utility to create an image to clone Onsite Managers. It is otherwise identical to the Onsite Manager installer.

Installing Service Center

Before proceeding, ensure that:

- the server meets Service Center system requirements for the expected monitoring load.
- the user account performing the installation must have Domain or Local Administration privileges, as applicable.
- ensure the FQDN has been registered with the DNS.
- all Microsoft installation source files are available.
- all Barracuda Managed Workplace installation source files are available locally.
- you have your VAR code so you can complete the registration. Your Senior Account Manager provides this, and it is the same as your account number.

The Hosted Service Center installer creates the Application Servers that receive incoming information from solution providers' customers' sites, and also provide the interface for users and PSA applications to interact with the system.

As the resource demand increases over time as VARs are added to the environment you will want to install multiple Application Servers.

Reboot After Install

Barracuda Managed Workplace 10 SP3 and higher requires Microsoft .NET 4.6.0, which is included in the installer unless .NET 4.6.0 or higher is already installed on the target machine. For example, Microsoft Windows 10 includes .NET 4.6.0 or higher, so does not require an additional installation.

.NET 4.6.0 requires a reboot after installation on certain Operating Systems. The following table shows which Operating Systems will reboot after the install.

Operating System	Reboot
Windows 10	No
Windows 8.1	Yes
Windows 8	Yes
Windows 7 SP 1	Yes
Windows Vista 7 SP2	Yes
Windows Server 2016	No
Windows Server 2012 R2	Yes
Windows Server 2012	Yes
Windows Server 2008 R2 SP1	Yes

Virtual Directories and New Websites

Barracuda Managed Workplace creates three URLs for deployment. You can choose to create virtual directories or new websites.

The install creates the path the following way, based on the FQDN that you provide:

- Virtual directories - The component identifier is added to the end of the site path. See the Example 1 column in the table below.
- Separate sites - The component identifier is added to the beginning of the site URL. See the Example 2 column in the table below.

Component	Example 1 Virtual Directories	Example 2 New Sites
-----------	----------------------------------	------------------------

Public Service Center URL	http://www.mycompany.com/SC	http://sc.mycompany.com
Public SC Messaging URL	http://www.mycompany.com/SCMessaging/ScWebservices.asmx	http://SCMessaging.mycompany.com/ScWebservices.asmx
Public Update Service URL	http://www.mycompany.com/MWUS	http://MWUS.mycompany.com

Important: Microsoft Windows Server 2008 SP2 is no longer a supported operating system.

1. Double-click **SetupSC.exe** to launch the Service Center installer.
2. Click **Verify Required Components** to confirm software requirements. Install any missing components by clicking the links presented, if any.
3. Under the **Options** section, select the **Install Service Center** check box.
4. Click **Install Service Center**.
5. Click **Next**.
If any required Windows services are not running, you will be prompted to start them at this point. Also, if you are presented with the option, click Configure to update IIS and ASP.NET to work with Barracuda Managed Workplace.
6. Indicate where you want to create the Service Center databases by selecting **Local machine** or **Remote machine**. Click **Next**.
7. The **SQL Server Login** dialog box opens. Choose the target SQL server from the list or manually type the server name or IP address. Enter the SQL authentication login and password. Click **Next**.
8. Click Browse to review the installation path and, if required, select a different location. Click **Next**.
9. Choose whether a proxy will be used.
If using a proxy server, do the following:
 1. Enter the **Address**, Port, **Username** and **Password**.
 2. Define the authentication type by selecting either **Basic**, **Digest** or **Negotiate**.
 3. Click **Next**.
10. Indicate how you want the Service Center websites to be created by choosing either Virtual Directory or New Website. Click **Next**.
Note: If the computer is a Domain Controller, the only option you will have is to create virtual directories.
 - If using a virtual directory, select the parent website and enter Virtual Directory Name. Click **Next**.
 - If using a new website, enter the URL for Service Center. A corresponding DNS entry is required to view the site. Click **Next**.**Note:** Ensure the FQDN has been registered with the DNS.
The **Public Service Center Communication Settings** dialog box opens.
11. Enter the following information:
 1. Public facing Service Center URL, which is the URL for Service Center, that must also be accessible from the Internet in order for Device Managers to obtain configuration information.

2. Public SCMessaging URL, which is the URL used by the Onsite Managers, Device Managers and other components of Barracuda Managed Workplace to report and send data to Service Center.
3. Public Update Service URL, which is the URL used by the Service Center application and by device managers under patch management to update Microsoft and Windows applications on devices.

Note: If you use an https schema, before starting Service Center, use IIS to select a certificate for the website.

12. Write the URL down because you will need it later when you install the Onsite Manager. Click **Next**.
13. Click **Install**.
14. Once the wizard completes, click **Continue** to run Reporting Services Configuration utility.
15. From the Barracuda Managed Workplace Service Center - Reporting Service Configuration, select **Remote Machine** and enter the host name or IP address of the SQL Server in the **Machine Name** box. Under **User Credentials with Access to Server**, select either **Local Administrator Account** or **Domain User Account** (specifying the User Name, including Domain, and Password) and click **OK**. Whichever account is selected, it must have access rights to create a local user on the remote machine.
16. Click **OK** when a dialog box shows your choices, and again when you are advised that the configuration succeeded.
17. The **Register Service Center** dialog box opens. Enter identifying information in the Company Information and Contact Information sections.
18. Type your Installation Key into the **Key** box and then click **Register**.

Adding Application Servers

When starting out hosting Barracuda Managed Workplace, it is customary to begin with two application servers at a minimum. This allows you to balance the load between the servers as you on-board more VARs with Service Centers.

Adding application servers after the first one is installed is very simple. Perform the install following the exact same procedure you followed for the first one. Then, make sure the IP address of the new application server is added to the load-balancer.

Important: The MW Remote Desktop service, which manages legacy remote control connections, must only be running on a single application server. On all others, disable the service. If you originally installed Barracuda Managed Workplace 2011 or later, you can safely ignore this requirement as the service will never be accessed.

Important: Each application server must be able to contact each other application server locally in order for mobile device management to function correctly in environments with multiple application servers.

Firewall rules required for multiple application servers

The MW installer doesn't create the firewall rules that are required for multiple application server configurations. As a result, the creation of a new VAR may fail when installed on multiple application servers with certain firewall rules in place.

To ensure successful VAR creation, add the following rules to Windows Firewall on each application server you want to use:

- %SystemRoot%\System32\inetsrv\w3wp.exe
- %ProgramFiles% (x86)\Level Platforms\Service Center\Bin\SCMonitor.exe
- %ProgramFiles% (x86)\Level Platforms\Service Center\Bin\SCWorker.exe

To Add Rules to Windows Firewall

1. In Windows, click **Start > Control Panel**.
2. Click **Windows Firewall**.
3. Click **Advanced Settings**.
4. Click **Inbound Rules**.
5. Click **New Rule**.
6. Click **Program**.
7. Click the **This Program Path** button and type the following:
 - %SystemRoot%\System32\inetsrv\w3wp.exe
8. Click **Next**.
9. In the **Action** step, click **Next**.
10. In the **Profile** step, click **Next**.
11. In the **Name** step, type a name for the rule, then click **Finish**.
12. Repeat steps 3 to 13 twice, typing the following paths in step 7:
 - %ProgramFiles% (x86)\Level Platforms\Service Center\Bin\SCMonitor.exe
 - %ProgramFiles% (x86)\Level Platforms\Service Center\Bin\SCWorker.exe
13. Repeat this procedure for each application server you want to use in your installation.

Defining an Application Server for Mobile Device Management

The mobile device management service is controlled by a single application server, even when multiple application servers are available. A single web service connection is accepted from all Android and Blackberry mobile devices enrolled for Service Centers hosted by the system, as are transient connections from the Service Centers when users send immediate commands to these devices.

1. Using SQL Management Studio, connect to the Service Center database server.
2. Open the SCMaster database and open the Configuration table. Enter the IP address of the application server to host mobile device management in the **TunnelServerHost** record. This IP address must be accessible to all of the application servers in the environment.

3. On the selected application server, open \Level Platforms\Service Center\SCMdmWindowsServices\TunnelServer\TunnelServer.exe.config and edit <Add Port="7778" Address="127.0.0.1"> to read <Add Port="7778" Address="0.0.0.0">.
4. Confirm that all application servers have access to port 7778 on the selected application server.
5. Using the **Windows Service Control Manager**, locate the TunnelService service. Right-click it and choose **Restart**.
6. On each application server, restart the MWPool application pool from within IIS.

© Barracuda Networks Inc., 2019 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.