Preparing a Site - Hosted

https://campus.barracuda.com/doc/89620617/

Configuring SNMP Devices

SNMP devices are polled using case-sensitive community strings that must be provided by the monitoring agent, in this case Onsite Manager, to access data about the device's performance.

The default community string set for most devices is public, and this is automatically populated in the Onsite Manager network scan, so you may find that no additional configuration of the SNMP devices is required. If you have SNMP devices not showing as SNMP-enabled in Onsite Manager, confirm that the networking requirements are satisfied. If there are no networking issues, refer to the vendor documentation on how to configure the SNMP community string.

Each device that generates SNMP Traps must be given the host name or IP address of the Onsite Manager server to use as the receiver. Consult the vendor documentation on how to configure the receiver for each supported device at the customer site.

Configuring Syslog Devices

Some network infrastructure and most Unix/Linux devices will generate syslog messages sent out to syslog receivers, in this case the OnsiteManager, regarding the device status. The Onsite Manager will accept Syslog messages from all devices.

Each syslog-generating device must be given the host name or IP address of the Onsite Manager server to use as the syslog receiver. Consult the vendor documentation on how to configure the syslog receiver for each supported device at the customer site.

Configuring WMI Devices

Unless configured to use another account, the Onsite Manager Windows services will use the default logon account named MWService, created during installation, to scan the network. Depending on the type of network, this will require different actions to be taken.

Domain Networks

On Domain networks, the account is created as a Domain Administrator, so that it can access all

Windows devices attached to the Domain. If installing in a Domain, then the Windows service account is created within Active Directory for Windows-based monitoring and management. Domain Policy settings, which help enable monitoring within a Domain environment, can be found in the Site Management section of Service Center.

To access the Domain Configuration Guide, click the Documentation tab in the Partner Portal.

Workgroup Networks

On Workgroup networks, the account is created locally on the Onsite Manager server, and also needs to exist as a Local Administrator on each Windows device in the Workgroup. This user must have exactly the same logon and password as that on the Onsite Manager server, and the password must be set to never expire.

If installing in a Workgroup, then the Windows service account is created locally on the Onsite Manager, but you must run the Workgroup Preparation Utility on all the devices you want managed.

The Workgroup Preparation Utility can be run from the Site Management section of Service Center, which creates the user (and makes other changes required for monitoring) with a single click, minimizing setup time for Workgroup devices.

Mixed Domain-Workgroup Networks

Barracuda Managed Workplace requires a service account (administrative user) to authenticate against and monitor the devices in your network. Depending on your network configuration, configure Barracuda Managed Workplace as follows:

- If installing in a hybrid (mixed) environment, and you install on a computer that has access to the Domain, then the Windows service account is created within Active Directory for Domain-based Windows devices. You only have to run the Workgroup Preparation Utility on all Workgroup-based devices.
- If installing in a hybrid (mixed) environment, and you install on a computer that does not have access to the Domain, then you must run the Workgroup Preparation Utility on all managed devices (because the Windows service account cannot be created if Active Directory cannot be accessed).

Caution: This configuration limits monitoring of Domain Controllers to availability and SNMP because Windows does not allow the required local User account to be created. Note: For ease of use, it is recommended that you install the Onsite Manager on a server that is a member of the domain and not a domain controller.

Creating a Workgroup Prep Utility

1. In Service Center, click **Configuration** > **Site Management**.

2. Click the site for which you want to run the utility.
3. Click the **Resources** tab.
4. In the Workgroup Resources section, click **Download Workgroup Prep Utility**.
5. Click **Save** and select the location to which you want to save the Workgroup Prep Utility.

Running a Workgroup Prep Utility

1. Extract the following file on each Workgroup device that needs to be configured.
   LPIWorkgroupPrep_<om site name>_yyyy-mm-ddThh:mm:ss.zip
   For example: LPIWorkgroupPrep_myOmsitename_2009-05-28T13:01:01.zip
2. From the extracted location, double click the **omsiteprep.exe** file.
   When complete, a dialog box opens stating if the site preparation was successful.
3. Click **OK**.

The utility generates a log file in the current working directory named OASiteprep.log, which contains a detailed report of all changes and errors.

The site preparation process:

1. Checks if Barracuda Managed Workplace site preparation has been run before.
2. Checks the type of platform (Window OS) since some site preparation tasks are dependent upon the OS version.
3. Creates a Barracuda Managed Workplace service account. Updates the password if the account already exits.
4. Starts and configures dependent system services, if required.
5. Configures and enables WS-MAN and WMI, if required.
6. Configures UAC options on Vista and later versions of Windows Operating Systems.
7. Configures all firewall profiles regardless of whether the firewall is enabled. This includes allowing ICMP echo; remote administration, file and print sharing, and remote desktop services; and ports required for WMI and Barracuda Managed Workplace applications.
8. Logs all changes to file and update registry with record of execution.

Configuring Intel® AMT Devices

To prepare Intel® AMT devices for discovery, you must do the following:

- Configure the device in Small Business Mode (SMB) mode. AMT devices configured to run in Enterprise mode are not compatible with Barracuda Managed Workplace.
- Configure the user for the Intel® AMT device. It is recommended that you use the same account on all Intel® AMT devices in the environment so that when you scan the network you can provide a single credential for the Onsite Manager to use for discovery.
- Configure the Intel® AMT device for SMB.
- For devices that are prior to version 4.0, ensure the host name is the same as the host name

that is set in the operating system and configure the device for DHCP mode.

AMT Firmware	DHCP Mode	Static Mode
<4.0	Supported when both AMT and operating system are set to DHCP mode and use the same hostname	Not supported
>=4.0	Supported when both AMT and operating system are set to DHCP mode and use the same hostname	Supported when both AMT and operating system are set to the same static IP address