What is Simplified Deployment?

https://campus.barracuda.com/doc/98216873/

The Onsite Manager requires the 3 following key items for simplified deployment:

- Onsite Manager must be able to ping the device.
- It must be able to access the admin share to transfer the scripts used for configuration. If file and printer sharing is disabled in the OS or Firewall this will not work.
- It must have valid credentials configured for the Device that grant administrative access to make the necessary configuration changes.

In order to achieve this, the Windows Prep Utility (Formerly the Workgroup Prep Utility) has been updated in order to add more flexibility. When the Windows Prep Utility is run on a device, it will perform the following:

- The utility will create local MWService account when running on a Workgroup machine. If the utility is run on a domain computer, it will not create a local MWService account.
- The Windows firewall, if enabled, will be configured to allow access to the required ports for Onsite Manager to fully monitor the device. These ports are described in the Setup Guide.
- Remote Desktop will be enabled.
- WMI access using DCOM will be enabled.
- The utility will also configure the Windows Management Framework to allow WMI access using the newer WSMan protocol. The device must have the Windows Management Framework version 2.0 or newer.
- If no Management Framework version is found, or an unsupported version of the Management Framework, the latest Framework version for the target operating system will be installed. The Windows Management Framework installation requires a reboot however, a reboot will not be forced upon installation, and instead will be allowed to finalize upon the next system reboot.

The domain configuration guide is available on the partner portal.

How does the Simplified Deployment work?

If Onsite Manager cannot access WMI on a device after 2 consecutive attempts or if it cannot access Remote Desktop after 1 failure, the Onsite Manager will attempt to run the Windows Prep Utility silently against the device. This deployment will be performed remotely against the target device using PAExec. A maximum of 5 simultaneous instances can run at any time.

- If the Windows Prep Utility has been run but the device is still not WMI enabled, the Onsite Manager will attempt to re-run the Windows Prep Utility once a day until the issue is resolved.
- If the Windows Prep Utility fails to run altogether, the Onsite Manager will try up to 3 additional times to resolve the issue.

When the Windows Prep Utility is run against a device, the Onsite Manager will collect the logs and store them in the following default location:
`C:\Program Files (x86)\Level Platforms\Onsite Manager\Logs\SitePrep`

In addition to this new functionality, the Onboarding Overview page will only report WMI issues on a device after 3 consecutive failed attempts to access WMI, or 2 consecutive failed attempts to query Remote Desktop.

How Can I Disable Simplified Deployment?

Simplified Deployment can be disabled for a site by performing the following steps:

1. Navigate to the **Status** > **Onboarding Overview** > page.
2. Select the Site name you which to manage.
3. Click the **More Actions** button.
4. Select **Modify Advanced Settings**.
5. Uncheck the box labeled **Automatically resolve onboarding issues related to Windows devices**.

How Can I Disable Simplified Deployment on a Per-Device Basis?

Advanced Users Only! Advanced Users Only: Simplified Deployment can also be disabled on a per-device basis by performing the following steps on the Onsite Manager:

1. Log into the **Onsite Manager**.
2. Open the following file in **Notepad** as Administrator:
   C:\Program Files (x86)\Level Platforms\Onsite Manager\Bin\MWExpertSystem.exe.config

- It is recommended you create a backup before making modifications.

1. Locate the following section provided as an example:
```
<AutoResolveExclusions>
   <!--<add DeviceGuid="25E50C4B-3DE3-4D4A-898A-C588E98E6E01"></add>
   <add IPAddress="10.0.0.1">–>
</AutoResolveExclusions>
```
2. Add the IP Address you wish to exclude (Example: 192.168.1.124):
```
<AutoResolveExclusions>
   <!--<add DeviceGuid="25E50C4B-3DE3-4D4A-898A-C588E98E6E01"></add>
   <add IPAddress="10.0.0.1">–>
   <add IPAddress="192.168.1.124">
```

```
    </AutoResolveExclusions>
```

3. Save the file and restart the MWExpertSystem service.

© Barracuda Networks Inc., 2024 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.