MITEL PERFORMANCE ANALYTICS

RELEASE 3.1

PROBE INSTALLATION AND CONFIGURATION GUIDE

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

Mitel Performance Analytics Probe Installation and Configuration Guide
Release 3.1 - May 12, 2020

INTRODUCTION

Mitel Performance Analytics is a fault and performance management system designed to provide users with fast actionable problem resolution so that optimal service quality levels are maintained for end customers.

Mitel Performance Analytics provides real-time alerts, detailed reporting and ubiquitous accessibility with secure remote access.

DOCUMENT PURPOSE AND INTENDED AUDIENCE

This document provides information required to install and configure a Mitel Performance Analytics (MPA) Probe.

The Probe enables communication between Mitel Performance Analytics and the customer network. It also acts as a data collector between Mitel Performance Analytics and the monitored devices. The monitored devices send their data to the Probe which then relays it to Mitel Performance Analytics.

For information required to administer and use a Mitel Performance Analytics monitoring system, refer to the Mitel Performance Analytics online help.

Note that screen captures in this document may not reflect the latest Mitel Performance Analytics User Interface updates.

REVISION HISTORY

DOCUMENT DATE	DESCRIPTION
November 20, 2015	Updated to reflect MarWatch R5.1.
December 6, 2016	Updated to reflect Mitel Performance Analytics R2.1.
November 2, 2017	Mitel Performance Analytics R2.2 General Availability
July 31, 2018	Mitel Performance Analytics R2.3 General Availability
January 16, 2019	Mitel Performance Analytics R3.0 General Availability
May 12, 2020	Mitel Performance Analytics R3.1 General Availability

PROBE INSTALLATION

The Probe is software that runs on a host in the customer LAN or on a dedicated server appliance, the Probe Appliance. The Probe monitors customer devices and reports to Mitel Performance Analytics, as well as providing Remote Access to a customer LAN, if this capability is enabled.

This chapter describes how to install various types of Probes.

For details on configuring Probes, see "Probe Settings Configuration" on page 24.

CAPACITY REQUIREMENTS

The Probe software is designed to be lightweight and to impose minimal host requirements. The Probe(s) are configured based on your Mitel Performance Analytics system requirements.

- For up to 10 monitored devices, you can use the pre-configured Martello Appliance
- If there are more than 10 monitored devices, a virtual appliance with a minimum of 2 GB of RAM is required. Contact Mitelfor engineering guidelines.

PROBE CAPACITY

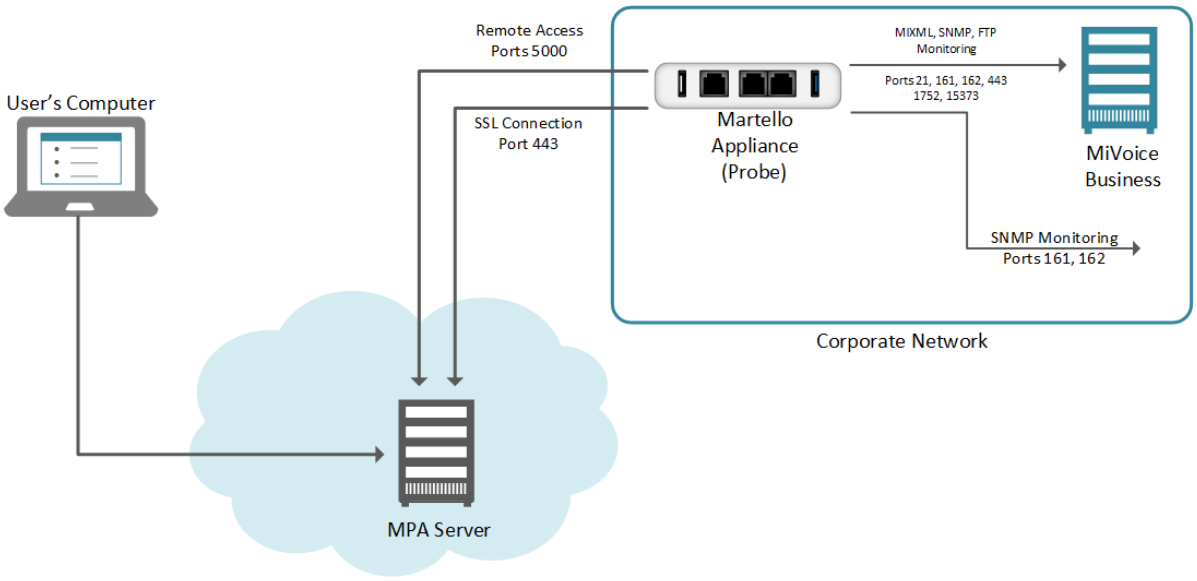
For users that have Mitel Performance Analytics installed on-site with their equipment, the Probe that is provided with your installation can monitor approximately 100 devices, assuming the monitored network consists of a variety of devices.

For service providers that have Mitel Performance Analytics installed in their data center, the system Probe that is provided with your installation can monitor approximately 100 devices, assuming the monitored network consists of a variety of devices.

For cloud based users, a single Probe can monitor a medium sized network consisting of five routers and 10 MiVoice Business devices with automatic backup and SMDR gathering enabled.

PROBE CONNECTIVITY OVERVIEW

The following figure shows the connectivity requirements between the Mitel Performance Analytics server, a Probe, and some monitored devices in a corporate network.



The connectivity requirements vary depending in the type of monitored device. Refer to the following sections for details.

LAN CONNECTIVITY REQUIREMENTS

To provide monitoring and remote access, the Probe must be able to connect to the LAN devices.

The Probe uses the following IP protocols to communicate to devices it is monitoring:

APPLICATION	IP PROTOCOL AND PORT	IP SESSION SOURCE	IP SESSION DESTINATION
SNMP / Performance	UDP, port 161	Probe	Device
SNMP	UPD, port 162	Device	Probe
HTTPS / Performance	TCP, port 443	Probe	Mitel Performance Analytics MarWatch
HTTP	TCP, port 80	Probe	MiVoice Office 250
MiXML	TCP, port 443	Probe	MiVoice Business and MiVoice Business EX

APPLICATION	IP PROTOCOL AND PORT	IP SESSION SOURCE	IP SESSION DESTINATION
SMDR	TCP, port 1752	Probe	MiVoice Business and MiVoice Business EX
SIP Endpoint Voice Quality	UDP, port 5060	SIP Endpoint	Probe
MiVoice Border Gateway Integration	UDP, port 26262	Device	MiVoice Border Gateway Integration
MiVoice Connect Remote Access	TCP, port 5478	Probe	MiVoice Connect Device
Network Testing	Outgoing, any port Incoming or Probe or SIP Device, port 5060	Probe	Probe or SIP Device
MiVoice Office 250 / Message Print	TCP, ports 4000, 44000	Probe	MiVoice Office 250
Avaya IP Office	TCP, port 50802 and ports in the range 50804 to 50813 (defaults, actual ports may range between 49152 and 65289 depending on IP Office services base port) UDP, ports 50794, 50798	Probe	Avaya IP Office
PathSolutions	TCP, port 8084 (default)	Probe	PathSolutions
FTP / Backup	TCP, port 21	Probe	MiVoice Business
SSH / Performance	TCP, port 22	Probe	Device
Ping / Availability	ICMP Echo	Probe	Device

Note: Some of the ports listed in this table are used by multiple devices. The device configuration determined the protocols and ports that are used. For example, if an MX-ONE device is configured to use SNMP, then UDP, port 161 is used. If MX-ONE is also configured for SSH, TCP port 22 is also used.

OTHER PROTOCOLS AND PORTS

If the Probe is used for Remote Access, the Probe must have network connectivity to the LAN devices for the appropriate TCP/IP protocol and port used by the Remote Application.

RECEIPT OF SNMP TRAPS

To receive SNMP traps, the Probe must receive the SNMP packets. These are sent by default on port 162.

The Probe attempts to bind to port 162. If it cannot, it binds to port 1162 instead.

The **Probe Status** panel shows the port that the Probe has bound to. To access the **Probe Status** panel, select **Status** under the **Network Tools** menu for the Probe dashboard.

Note: To view the Probe Status panel, ensure that the **Collect Probe Status** option is enable in the Probe Settings. See "Probe Settings Configuration" on page 24.

The following is a typical Probe Status panel:

Component	Message
ProbeConfig	Added: 8 Removed: 0 Updated: 0 LoadFail: 0
CheckForUpgrade	Last Modified: Mon Mar 30 21:33:10 UTC 2015
CollectorManager	Collecting 9 devices with 42 Collectors.
BufferingRemoteRrdUpdater	Buffer size: 0/2048, max age: -1, enqueued: 2552, sent: 2544, dropped: 0, errors: 0, permanent errors: 8, internal errors: 0, HWM: 38, retry later:0
MCDMiXMLCollector	Collecting for 4 MCDs
MBGCollector	Collecting VQ for 1 MBGs
ThreadPoolSNMPTaskRunner	Running 61 tasks, 0.15 Tasks/Second
SNMPTrapReceiver	Listening on port 162
FixedThreadPoolPingTaskRunner	Pinging 8 devices with 5 threads.

To ensure receipt of traps, configure the trap sender to send traps on the port the Probe has bound to.

INTERNET CONNECTIVITY REQUIREMENTS

For remote monitoring, the Probe must have continuous network access to the devices to be monitored and must have Internet access for HTTP/TLS on port 443 to the Mitel Performance Analytics server.

For other, optional services, the Probe connects to either customer specified servers (for file transfer) or to Mitel Performance Analytics servers for Mitel Performance Analytics cloud storage or Remote Access.

Note that the Probe always initiates IP connections; that is, all connections are outbound.

PROTOCOL OR APPLICATION	IP PROTOCOL AND PORT	IP SESSION INITIATOR	DESTINATION	COMMENT
HTTPS	TCP, port 443	Probe	Mitel Performance Analytics server(s)	Required for Remote Monitoring.
HTTPS	TCP, port 443	Probe	Mitel Performance Analytics Cloud File server(s)	Optional, Required for Mitel Performance Analytics Cloud File Storage.
FTP, FTPS Implicit	TCP, port 21	Probe	Customer-defined File server(s)	Optional, used for SMDR file transfer.
SFTP	TCP, port 22	Probe	Customer-defined File server	Optional, used for SMDR file transfer.
FTPS Explicit	TCP, port 990	Probe	Customer-defined File server	Optional, used for SMDR file transfer.
SSH	TCP, port 50000	Probe	Mitel Performance Analytics server(s)	Required for Remote Access.
DNS	TCP and UDP, port 53	Probe	DNS server	Required to resolve host names or URLs to IP addresses.
NTP	UDP, port 123	Probe	NTP server	Required to synchronize Probe system time.

OTHER REQUIREMENTS

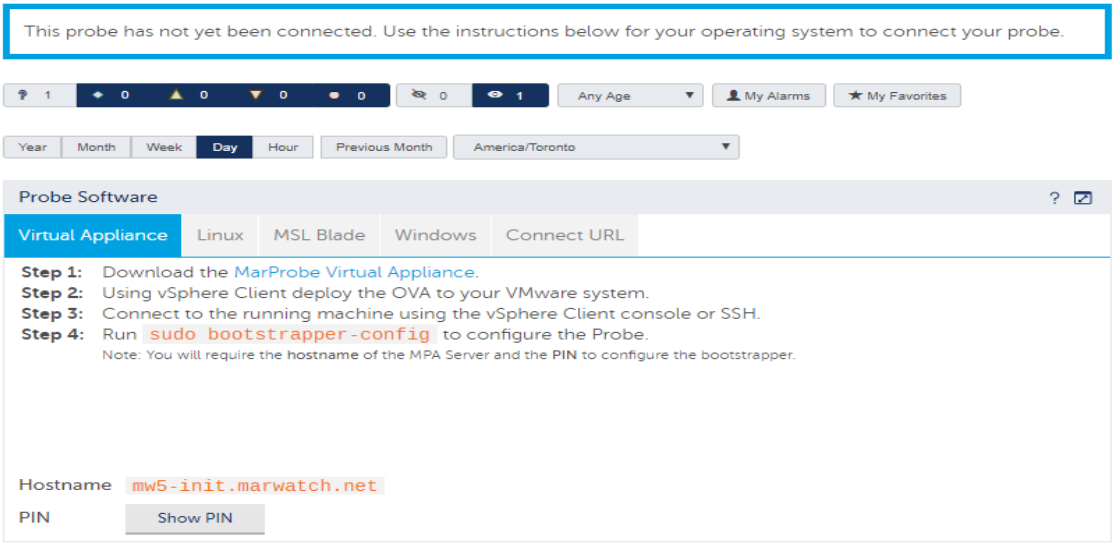
To install a Probe, you must have the **Probe Installer** administrative permission.

PROBE SOFTWARE INSTALLATION PROCEDURES

The Probe software is available from the **Probe Configuration** panel available on the Probe dashboard. That means that you must have previously added the Probe device to a container.

Before the Probe has connected to Mitel Performance Analytics, the Probe dashboard shows only two panels: the **Probe Configuration** panel and the **Probe Device Information** panel.

The following is a typical Probe dashboard before it has connected to Mitel Performance Analytics:



If a Probe is already connected to Mitel Performance Analytics, the **Probe Configuration** panel is accessed by selecting **Probe Software** from the **System Administration** menu from the Probe dashboard.

The Probe Dashboard shows only these two panels to highlight the fact that the Probe has not yet connected to Mitel Performance Analytics. Use the **Probe Configuration** panel to install the Probe software.

Each tab contains instructions to download the installation files for a Probe for that platform. The Connect URL tab is used primarily to regenerate a Probe URL for Mitel Flex K8s device implementations.

Warning: Do not generate a new Probe URL unless absolutely necessary. Doing so renders the existing URL invalid and the current probe will cease to function, even if this probe was not configured as part of a Flex K8s implementation. The newly generated URL must be implemented in order for the Probe to function again.

PROBE VIRTUAL APPLICATION INSTALLATION

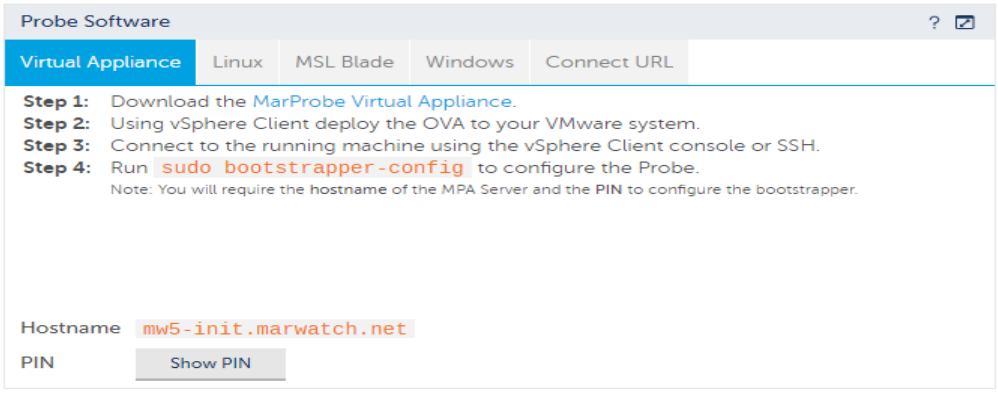
The Probe can also be downloaded as a Virtual Appliance. The system provides a VMware OVA that can be installed as Virtual Machine. The Virtual Machine contains an Ubuntu 18.04 Linux installation with the Probe software preinstalled.

Before installing the Virtual Appliance, configure the memory and resource allocation for the VM so that it meets the RAM requirements shown in "Capacity Requirements" on page 5.

Note: The system uses systemd-networkd to manage network interfaces and Netplan to configure them. The system is configured for DHCP network configuration by default. You can find instructions to configure a static IP address and custom DNS server at https://netplan.io/examples.

To install and configure the Virtual Appliance:

1. Go to the dashboard for the Probe that you wish to install.
2. Go to the **Probe Configuration** panel, select the **Virtual Appliance** tab and download the OVA file.



3. Install the OVA file according to VMware instructions.
4. Start the VM and connect to it using SSH or the VMware console.
5. Log in as `config` with password `changeme`.
   For the first log in, you are prompted to change passwords.
6. By default, the VM is configured to use DHCP. You can optionally change this setting to use static IP addressing. To do so, do the following steps:
   - Set a static IP address by running the following command and providing the following fields:
     - Copy the static configuration template to the configuration directory using the following command:
       `sudo cp /etc/netplan/eth0-static.yaml-template /etc/netplan/eth0-static.yaml`
     - Rename the dynamic configuration file to disable it. For example:
       `sudo mv /etc/netplan/eth0-dynamic.yaml /etc/netplan/eth0-dynamic.yaml.disabled`
     - Edit the static template with your specific configuration: `sudo vi /etc/netplan/eth0-static.yaml`. For example:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: false
      addresses:
      - 192.168.0.2/24 # ip address/netmask
      gateway4:
        192.168.0.1
      nameservers:
        addresses:
        - 1.1.1.1
```

     - Press `Esc` and enter `:wq` to write and exit from the file.
   - Validate the configuration using the following command: `sudo netplan try`

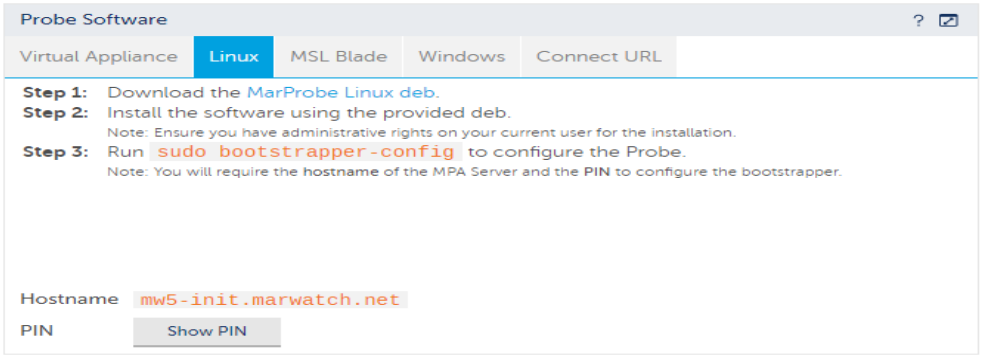
If it passes validation, press Enter to accept the configuration.

7. Generate the PIN by clicking the **Generate PIN** button.
   IMPORTANT: Make note of the Hostname and PIN displayed on the page.
8. Run `sudo bootstrapper-config` to configure the Probe.
9. Enter the hostname when prompted and press Enter.
   The utility runs and checks to see of the TLS certificate is trusted. If it is untrusted, it prompts you trust the certificate. If you choose not to trust it, the utility exits and the probe is not configured.
10. Enter the PIN when prompted and press Enter.
    The configuration process runs. This may take a few minutes. Upon successful completion a confirmation message is displayed indicating that the marprobe service is restarting. If the configuration was unsuccessful, a message is displayed requesting that you confirm the probe setup.

PROBE LINUX INSTALLATION

The Probe is supported on the Ubuntu Linux platform.

1. Log into the Linux system using an account with administration privilege (root).
2. Go to the dashboard for the Probe that you want to install.
3. Go to the **Probe Configuration** panel, select the **Linux** tab and download the MarProbe DEB to the Linux system.



4. Open a terminal window.
5. **Type `dpkg -i <path/MarProbe-Installer_file_name>.deb` to install the Probe, where <*path/MarProbe-Installer_file_name*> is the path to and the file name of the MarProbe DEB file downloaded in the step above.**
6. Generate the PIN by clicking the **Generate PIN** button on the **Probe Configuration** panel.
   IMPORTANT: Make note of the Hostname and PIN displayed on the page.
7. Run `sudo bootstrapper-config` to configure the Probe.
8. Enter the hostname when prompted and press Enter.
   The utility runs and checks to see of the TLS certificate is trusted. If it is untrusted, it prompts you trust the certificate. If you choose not to trust it, the utility exits and the probe is not configured.
9. Enter the PIN when prompted and press Enter.
   The configuration process runs. This may take a few minutes. Upon successful completion a confirmation message is displayed indicating that the marprobe service is restarting. If the

configuration was unsuccessful, a message is displayed requesting that you confirm the probe setup.

PROBE MSL BLADE INSTALLATION

The Probe software can be installed on an MSL server as an MSL blade.

Note: Mitel does not provide support or warranty for the Probe blade installation on an MSL server.

MSL Version Requirement

The Probe MSL blade is supported on MSL R10.3 and later.

Blade Packaging

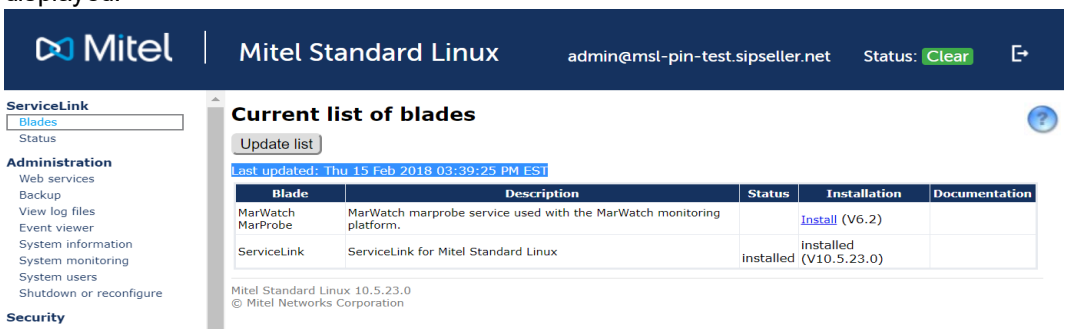
The blade is distributed as an ISO CD image file. The image file can be either burned to a CD or installed using a VMWare CD image mounting utility for Virtual MSL installation.

Installation

To install the Probe MSL blade:

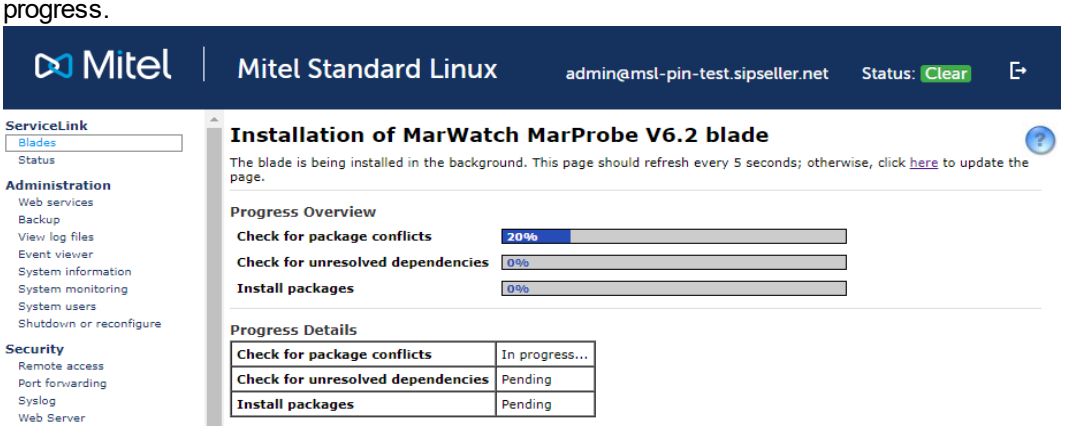
1. Go to the dashboard for the Probe that you wish to install.
2. Go to the **Probe Software** panel, select the **MSL Blade** tab and download the MSL blade ISO image.
3. Generate the PIN by clicking the **Generate PIN** button on the **Probe Software** panel. **IMPORTANT:** Make note of both the Hostname and PIN displayed on the page.

   Note: To do this step, you must have the **Probe Installer** administrative permission.
4. Open a Web browser and navigate to the MSL server manager URL (for example, http://<MSL_server_FQDN>/server-manager).
5. Log in to the MSL Server Manager interface.
6. If you are installing the blade from CD, insert the CD in the server CD ROM drive.
7. In the left navigation pane under **ServiceLink**, click **Blades**. The available list of blades is displayed.

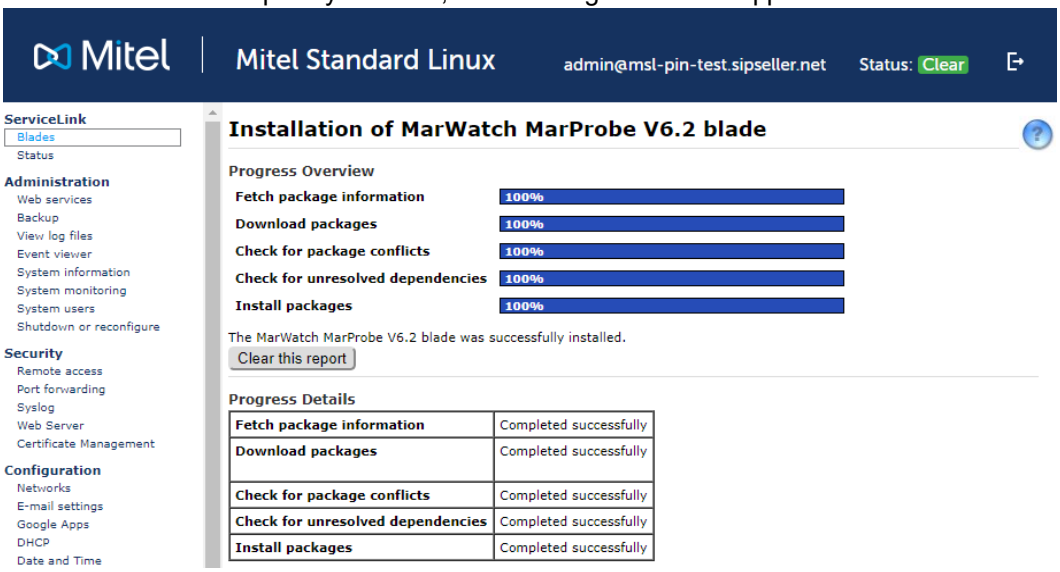


8. Click the **Install** link for the probe.
9. Review and accept the software license terms by clicking **Accept All Licenses**.

10. The installation process for the Probe blade begins. The installation screen shows installation progress.



11. When the blade is completely installed, the following information appears on the screen:



12. Click **Clear this report**.

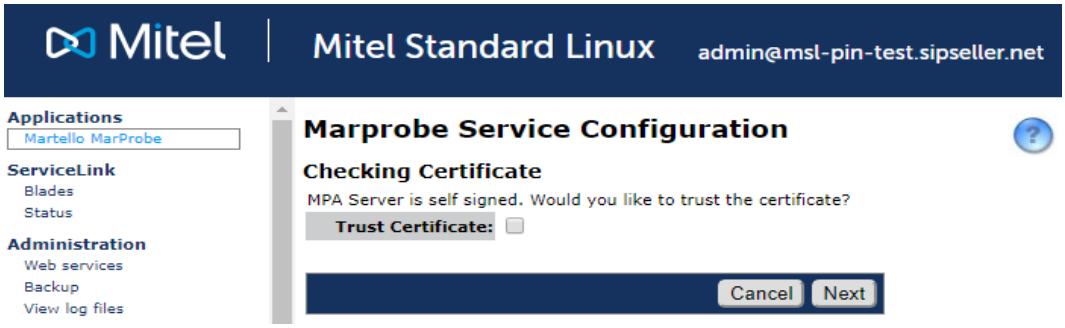
This completes the Probe blade installation.

After the Probe blade installation is complete, the Probe service starts and is available for configuration.

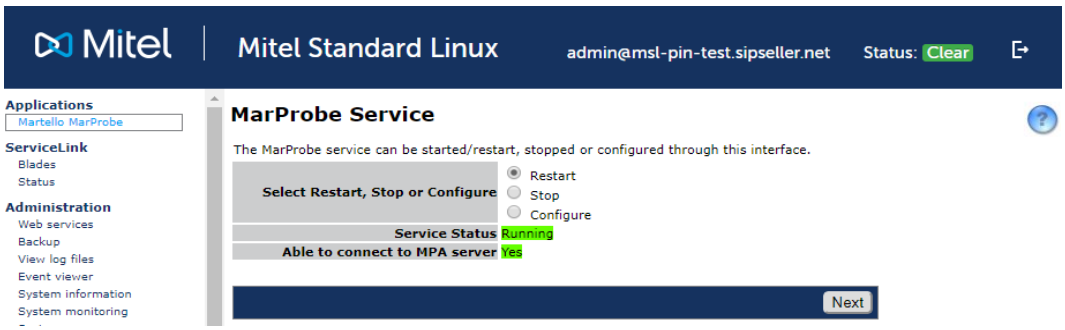
Configuration

1. From the MSL Server Manager interface select **Martello MarProbe** from the **Application** menu.
2. On the MarProbe Service page, click the **Configure** option, then click **Next**.

3. When prompted, enter the hostname that you recorded in the procedure above in the **MPA Server** field, click **Next**.
4. If the Mitel Performance Analytics server is using a self signed certificate, you must trust the certificate. Check the **Trust Certificate** checkbox and click **Next**.



5. Type the PIN you generated and recorded in the **PIN** field, then click **Next**.
6. The MarProbe Service page is displayed, and if successfully configured, the service status indicates that the probe is running. The "Able to connect to MPA server" statuses are:
   - Red - unable to connect
   - Yellow - connected but certificate not trusted
   - Green - connected

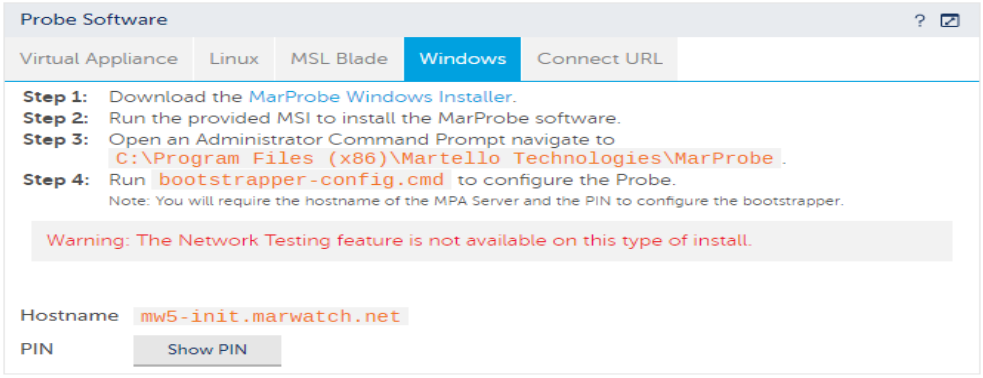


PROBE WINDOWS INSTALLATION

The Windows Installer runs on Windows 7 and 10 and Windows Server 2016. To install the software on Windows:

1. Log into the Windows system using an account with administration privileges.
2. Go to the dashboard for the Probe you want to install.

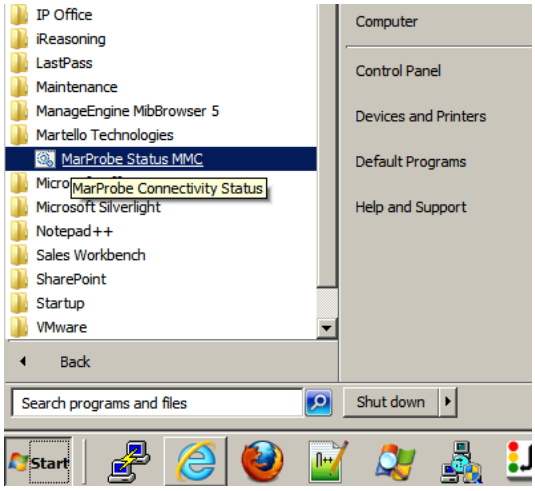
3. Go to the **Probe Configuration** panel, select on the **Windows** tab and download the Probe installer to the Windows system.



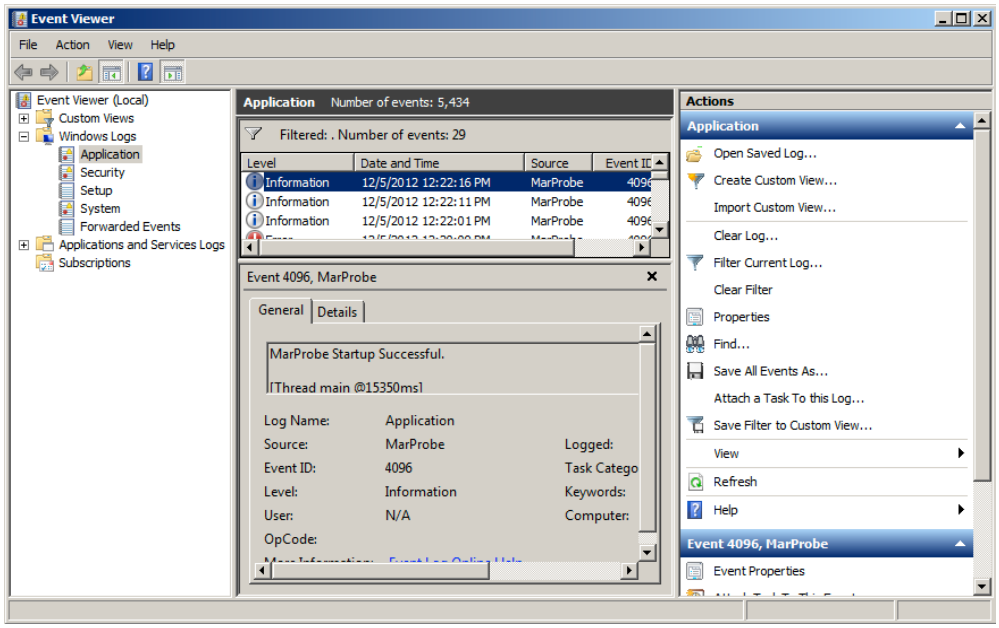
4. Run the Probe Windows installer (MarProbe-Installer.msi).
5. Follow the instructions in the Setup Wizard.
6. Generate the PIN by clicking the **Generate PIN** button on the **Probe Configuration** panel. **IMPORTANT:** Make note of the Hostname and PIN displayed on the page.
7. From the Start menu on the Windows machine, run the Command Prompt as an administrator.
8. In the command prompt window, navigate to the directory where the Probe is installed. For example:
   `cd C:\Program Files (x86)\Martello Technologies\MarProbe`
9. Run `bootstrapper-config.cmd`to configure the Probe.
10. Enter the hostname when prompted and press Enter.
    The utility runs and checks to see of the TLS certificate is trusted. If it is untrusted, it prompts you trust the certificate. If you choose not to trust it, the utility exits and the probe is not configured.
11. Enter the PIN when prompted and press Enter.
    The configuration process runs. This may take a few minutes. Upon successful completion a confirmation message is displayed indicating that the marprobe service is restarting. If the configuration was unsuccessful, a message is displayed requesting that you confirm the probe setup.

Confirm Installation

To confirm that the software is running, go to the Martello Technologies folder in the Start Menu, and click on the MarProbe Status MMC link.



This action opens the Microsoft Management Console and shows recent Windows events related to the Probe.



In Windows XP, the MarProbe Status MMC Start menu item is replaced by MarProbe Status CMD. This option opens a Windows command line interface which shows the five most recent entries in the Windows System Log for the Probe.

For example, the results from the MarProbe Status CMD on a Windows XP computer with a system name of MRTCOMP-11:

```
The default script host is now set to "cscript.exe".
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
-------------------------------------------------------------------------
-------
Listing the events in 'application' log of host 'MRTCOMP-11'
-------------------------------------------------------------------------
-------
Type:         information

Event:        4096
Date Time:    12/05/2012 15:44:59
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
User:         N/A
Description:  Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @59443625ms]

Type:         information
Event:        4096
Date Time:    12/05/2012 14:31:43
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
User:         N/A
Description:  Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @55047297ms]

Type:         information
Event:        4096
Date Time:    12/05/2012 14:00:23
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
User:         N/A
Description:  Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @53167797ms]

Type:         information
Event:        4096
Date Time:    12/05/2012 13:37:33
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
User:         N/A
Description:  Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @51797656ms]
```

MARTELLO APPLIANCE INSTALLATION

Note: In releases previous to Mitel Performance Analytics 3.1, the Martello Appliance was referred to as the Probe Appliance

The Martello Appliance is a small form-factor server with pre-installed Probe software. The Martello Appliance uses Ubuntu Linux as its operating system.

The Martello Appliance must be configured for use with Mitel Performance Analytics. The configuration details for a Martello Appliance are entered in the property page for that Probe device and are visible on the device dashboard page for that Probe.

You must have the Probe configuration URL to configure a Martello Appliance.

MARTELLO APPLIANCE

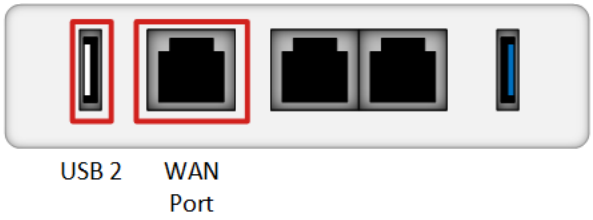
This Martello Appliance has connectors for:

- Power, 12V DC jack
- 3 Gb Ethernet LAN
- USB 2.0 type A,
- USB 3.0
- micro USB serial console

The Martello Appliance is shipped with:

- Standard USB cord
- Two-pin US power connector
- Ethernet cable

For the purposes of configuring a Martello Appliance for Mitel Performance Analytics, you are only concerned with the USB 2 and WAN Port connectors, as highlighted in the image below.



MARTELLO APPLIANCE CONFIGURATION WITH SSH

Do the following steps:

1. Connect power and Ethernet to the Martello Appliance. The Martello Appliance uses DHCP to obtain its Ethernet address. To configure a Martello Appliance, you need to know its IP address.
2. The IP address can be obtained by scanning the network in which the Martello Appliance has been installed, and looking for devices with a MAC address that starts with `F0-AD-4E` or `00-50-43`.
3. Connect to the Probe using SSH to its IP address.
4. Login to the system as user `config` with password `changeme`. The first time you login to the system, it prompts you to change the shipped default password. The `config` user has sudo privileges.
5. The system now terminates the SSH session. You need to reconnect and login as the user `config` with the password you have chosen.
6. Generate the PIN by clicking the **Generate PIN** button on the **Probe Configuration** panel. **IMPORTANT:** Make note of the Hostname and PIN displayed on the page.
7. Run `sudo bootstrapper-config` to configure the Probe.
8. Enter the hostname when prompted and press Enter.
   The utility runs and checks to see of the TLS certificate is trusted. If it is untrusted, it prompts you trust the certificate. If you choose not to trust it, the utility exits and the probe is not configured.
9. Enter the PIN when prompted and press Enter.
   The configuration process runs. This may take a few minutes. Upon successful completion a confirmation message is displayed indicating that the marprobe service is restarting. If the configuration was unsuccessful, a message is displayed requesting that you confirm the probe setup.

MARTELLO APPLIANCE CONFIGURATION WITH USB DRIVE

The Martello Appliance can also be configured using a USB drive. To configure the Martello Appliance, you need a USB drive formatted as FAT32 and the configuration URL supplied by the Mitel Performance Analytics Probe Status page.

Do the following steps:

1. Create a file called `marprobe.config`. on the root directory of the USB drive.
2. Edit the file to contain the following lines:
   ```
   pin=
   mpa_server=
   trust_cert=
   ```

The values for these options are case sensitive and must not contain quotation marks. After the `pin=` option, enter the PIN generated by on the **Probe Configuration** panel by clicking the **Generate PIN** button. After the `mpa_server=` option, provide the hostname displayed on the **Probe Configuration** panel . For the `trust_cert=` option, the certificate is trusted by default. Provide the value 'no' or 'NO' if you do not want to trust the certificate. If this option is left blank, or contains any value other than no or NO, the certificate will be trusted.

Note: The value 'No' also results in the certificate being trusted.

3. Save the file in the root directory of the USB drive and eject it.
4. Insert the drive into the USB port of the Martello Appliance. The indicator LED on the top of the appliance starts to blink as data is being read from, and written to the USB drive. When the LED stops blinking, it is safe to remove the drive from the appliance.
   Note: If the LED does not blink, the USB drive is not being read properly.

STATIC IP ADDRESSING

The Probe Appliance can be optionally configured with a static IP address using the USB drive configuration method. The following additional configuration variables are supported in the marprobe.config file:

```
address_assignment={static|dynamic}
address={dotted quad ip address}
netmask={dotted quad mask}
gateway={dotted quad ip address}
dns1={dotted quad ip address}
dns2={dotted quad ip address}
```

If `address_assignment` is set to `static`, the rest of the variables are used to define the network interface configuration.

If `address_assignment` is set to `dynamic`, the default DHCP configuration is used.

The following is an example marprobe.config file:

```
address_assignment=static
address=10.0.10.25
netmask=255.255.255.0
gateway=10.0.10.1
dns1=10.0.10.2
dns2=10.0.10.3
```

It assigns IP address 10.0.10.25/24 with default gateway 10.0.10.1 and DNS server addresses 10.0.10.2 and 10.0.10.3 to the Probe Ethernet interface.

LOG COLLECTION

To assist in troubleshooting, the Probe collects log information. Mitel support may ask for these logs to assist in problem resolution. The logs can be accessed through SSH or using a FAT-formatted USB drive.

SSH LOG ACCESS

The logs are stored in the `/var/log/marprobe/` directory. This is accessible from the `config` user account.

USB DRIVE LOG ACCESS

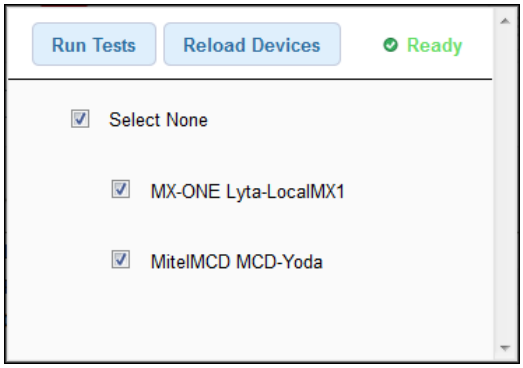
When a FAT formatted USB drive is connected to the Probe Appliance, the system automatically copies logs and configuration data to the USB drive.

PROBE DEVICE CONNECTIVITY CHECK

The device connectivity check is used to verify that the Probe can establish connections to the devices it is configured to monitor.

The connectivity check is accessed by selecting **Connectivity** under the **Network Tools** menu for the Probe dashboard:

The following is a typical connectivity check panel:

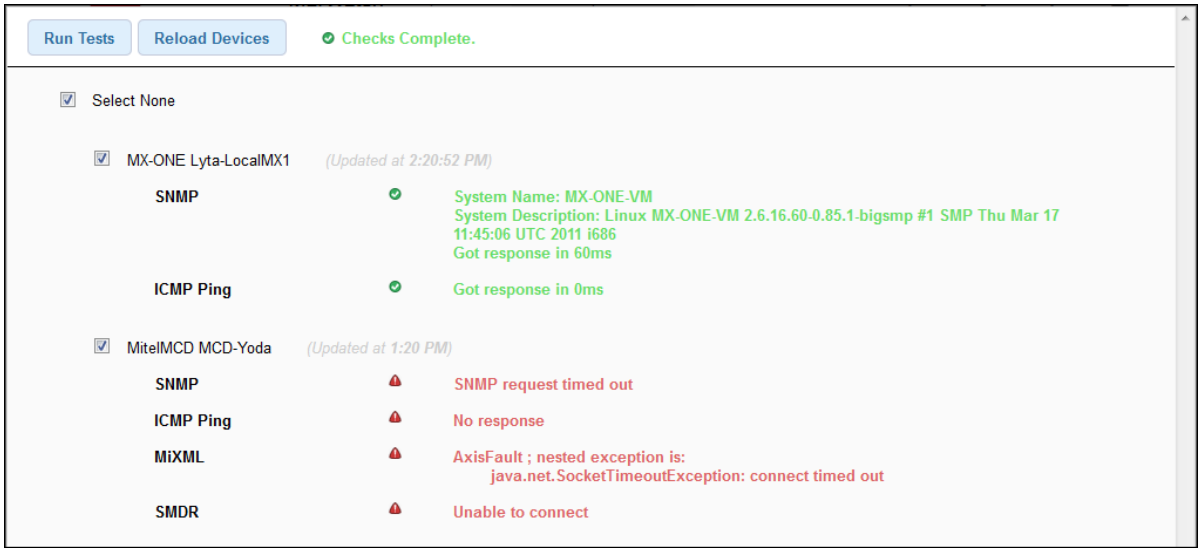


The checks verify both the IP network connectivity and the access credentials that have been configured for the device. The system runs this check for all of the connection protocols used by the device.

This capability can be used during installation to verify that local devices are properly configured and reachable from the Probe.

When a Device is created or edited, it can take up to 15 minutes for the configuration changes to propagate to the Probe. To check sooner, press the Reload Devices button to cause the Probe to request its configuration data from Mitel Performance Analytics.

The following is an example of the device connectivity check output.



PROBE SETTINGS CONFIGURATION

A single Probe enables monitoring of multiple devices on the same IP network. If the container in which the Probe is added contains subcontainers, the Probe can monitor the devices in the subcontainers also.

Do the following steps:

1. Access the Probe's dashboard.
2. From the Probe's dashboard, select **Probe Settings** under the **System Administration** menu.
   The Probe properties sheet is displayed.
3. Edit and change property settings as required. In addition to general settings available to all Mitel Performance Analytics devices, Probe settings include:

SETTING	DESCRIPTION
General Settings	Configure the following settings: • **Name**—If necessary, change the name of the Probe. • **Container**—If necessary, change the Container where the device is located. • **Description**—Enter a description for the Probe.
IP SLA Monitoring	Select the **Enabled** check box to enable IP SLA monitoring. Enter up to four IP SLA targets, specifying either the target IP address or the FQDN. For each target, you can specify Differentiated Services Code Point (DSCP) settings. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
Probe Software Override	Select the **JAR URL**check box for troubleshooting purposes. It allows for installation of special software. It is used only with assistance from Mitel support.
Probe Diagnostics	Select the **Collect JVM Stats** and **Collect Probe Status** check boxes to display additional diagnostic tools. The tools should be used and interpreted with assistance from Mitel support.

SETTING	DESCRIPTION
Network Testing	Select the **Enable** check box to indicate that the probe can be used as a test agent for Network Testing. For details see "Network Testing Setup" on page 1. Select the **Shared** check box to make the test agent shareable to other test agents for SIP Call tests within the container hierarchy. **Notes:** • Network Testing is not supported for MiCloud Flex on Google Cloud environments. • MSL Blade and Windows probes do not support the Network Testing functionality.
Maintenance Mode	While in maintenance mode, Mitel Performance Analytics provides only minimal monitoring of the device. This setting is useful to isolate a device with known issues so its alarms do not clutter the monitoring data of the rest of the network.
Device Message	Settings for a message banner that appears on the device dashboard. Users can specify the message importance level, message title, and message text.
Remote Access	See "Remote Access Control Configuration" on page 26.
Remote Access	Mitel Performance Analytics allows remote access controls to the Probe settings. Select one of: • Never–Never allow port forwarding, thereby blocking all remote access capabilities • Always–Allow port forwarding only to those devices monitored by the Probe • To Monitored Devices Only–Allow port forwarding for all devices on the subnet the Probe is connected to, thereby allow remote access to devices not monitored by the Probe

4. Click the **Save** button when done.

REMOTE ACCESS CONTROL CONFIGURATION

Mitel Performance Analytics allows remote access controls on the Probe settings sheet. The following is a typical settings sheet area for interface filtering configuration:

Users can configure the Probe to:

- Never allow port forwarding, thereby blocking all remote access capabilities
- Allow port forwarding only to those devices monitored by the Probe
- Allow port forwarding for all devices on the subnet the Probe is connected to, thereby allow remote access to devices not monitored by the Probe

Permissive Port Forwarding

By default, users can remotely access a device only if they have Remote Access permission for both the device and the Probe monitoring it. The **Permissive Port Forwarding** option allows a user to remotely access a device if they have Remote Access permission for the device, but not for the Probe monitoring it.

Before enabling this option, consider carefully why you denied the user Remote Access for Probe. By enabling this option, the user can access the Probe's network environment and could harm it.

Disabling this option does not terminate existing Remote Access sessions. To terminate existing Remote Access sessions, use the Probe's **Port Forwards** panel.

PROBE UPDATE

At a minimum of every six months, you should check for and run updates on all of the Probes that exist in your system.

To run these updates, the installed Mitel Performance Analytics server must have:

- An Internet connection
- Access to the `packages.martellotech.com` website

Run the `sudo update-mpa` command to download and install the Probe software updates (OVA or Martello Appliance probes only) to the server where the Probe software is installed.

Note: To update MSL and Windows Probes, you must download and re-install the Probe software.