

MITEL PERFORMANCE ANALYTICS

RELEASE 2.1

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.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2016, Martello Technologies Corporation

All rights reserved

Mitel Performance Analytics Probe Installation and Configuration Guide
Release 2.1 - December 6, 2016

Introduction	4
Document Purpose and Intended Audience	4
Revision History	4
Probe Installation	5
Host Requirements	5
Probe Capacity	5
LAN Connectivity Requirements	6
Other Protocols and Ports	7
Receipt of SNMP Traps	7
Internet Connectivity Requirements	8
Other Requirements	9
Probe Software Installation Procedures	9
Probe Windows installation	11
Probe Linux installation	15
Probe MSL Blade installation	16
Probe MiCollab Blade installation	18
Probe Virtual Application installation	22
Probe Appliance Installation	24
Probe Appliance Configuration with SSH	25
Probe Appliance Configuration with USB Drive	26
Static IP Addressing	27
Log collection	27
SSH Log Access	27
USB Drive Log Access	27
Probe Device Connectivity Check	27
Probe Configuration	30
Remote Access Control Configuration	30

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 a information required to administer and use a Mitel Performance Analytics monitoring system, refer to the *Mitel Performance Analytics System Guide*.

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. Ongoing updates and improvements.

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.

Mitel Performance Analytics provides Probe installers for Windows, Red Hat Linux (and distributions based on this, such as CentOS and Mitel Standard Linux), installation as a blade on a Mitel MSL or MiCollab server, and installation as a virtual appliance.

This chapter describes how to install various types of Probes. For details on configuring Probes, see "Probe Configuration" on page 30.

HOST REQUIREMENTS

The Probe is designed to be lightweight and to impose minimal host requirements. Recommended host configurations are listed in the following table. The Probe is a Java application and requires the Oracle JRE or OpenJDK JRE Release 1.8, or later. Mitel recommends Java Release 1.8 release 40 or later. For MiVoice MX-ONE support, ensure the host uses Java Release 1.8, release 25 only.

NO. OF DEVICES TO MONITOR	CPU	RAM	DISK	JAVA ENVIRONMENT
< 10 monitored devices per Probe Appliance	ARM5, 1GHz	512 MB total	512 MB total	OpenJDK 1.8 or later.
< 10 monitored devices per host	Core2 Duo / i3 1 GHz or faster	256 MB Service, 512 MB Host	5 GB free space	Oracle Java Runtime Environment (JRE) 1.8 or OpenJDK 1.8 or later.
< 80 monitored devices per host	Dual Core i5, 2 GHz or faster	1 GB Service, 2 GB Host	20 GB free space	Oracle Java Runtime Environment (JRE) 1.8 or OpenJDK 1.8 or later.
≥ 80 monitored devices per host	Contact Mitel for engineering guidelines.			

PROBE CAPACITY

For users that have Mitel Performance Analytics installed on premise 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. Every additional installed Probe can monitor a

medium sized network consisting of five routers and 10 MiVoice Business devices with automatic backup and SMDR gathering enabled.

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.

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
HTTP	TCP, port 80	Probe	MiVoice Office 250
MiXML	TCP, port 443	Probe	MiVoice Business
SMDR	TCP, port 1752	Probe	MiVoice Business
SIP Endpoint Voice Quality	UDP, port 5060	SIP Endpoint	Probe
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

APPLICATION	IP PROTOCOL AND PORT	IP SESSION SOURCE	IP SESSION DESTINATION
FTP / Backup	TCP, port 21	Probe	MIVoice Business
SSH / Performance	TCP, port 22	Probe	Device
Ping / Availability	ICMP Echo	Probe	Device

OTHER PROTOCOLS AND PORTS

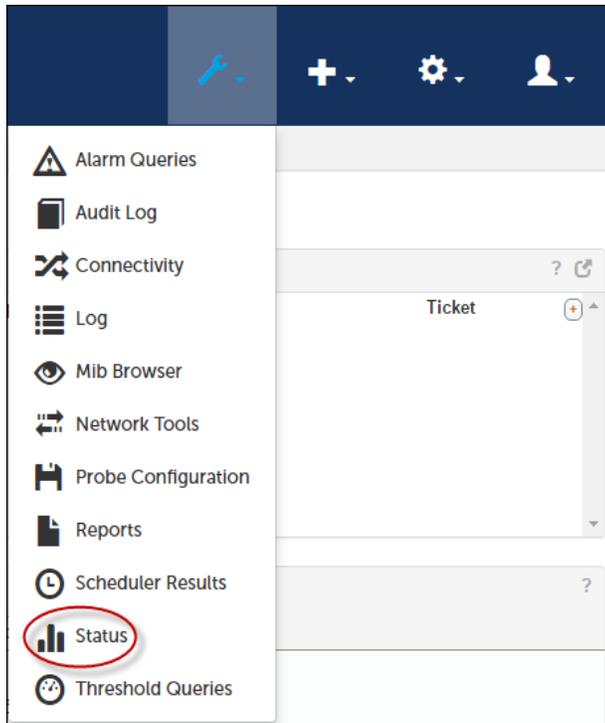
If the Probe is used for Remote Access, the Probe must have network connectivity to the LAN devices for the appropriate TCP/IP protocol and port used by the Remote Application.

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. The **Probe Status** panel is available under the **Tools** icon of the Probe dashboard:



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/SSL 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.

PROTOCOL OR APPLICATION	IP PROTOCOL AND PORT	IP SESSION INITIATOR	DESTINATION	COMMENT
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

All installers are available from the **Probe Configuration** panel.

For both Windows and Linux installations, the general procedure is:

1. Install the Probe software.
2. Start the Probe application (as a Windows service or Linux daemon).
3. Provide the Probe software with the appropriate Mitel Performance Analytics configuration URL to enable the Probe to connect to the correct Mitel Performance Analytics server and to uniquely identify itself to Mitel Performance Analytics.

Note: To perform Step 3, you have the **Probe Installer** administrative permission.

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.

Mitel Performance Analytics Probe Installation and Configuration Guide

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

This Probe has not yet connected to CloudNOC.

Probe Software

Windows Linux MSL Blade Virtual Appliance

Step 1: Download the [MarProbe Windows Installer](#).

Step 2: Run the provided MSI to install the MarProbe software.
Note: Ensure you have administrative rights on your current user (under User Accounts).

Step 3: Provide the following URL to the installer:

```
https://Probe-6f41fb88-f2ea-4517-b85c-e47fb0104e34:W3AjC4GCu1qI7xw@marketing-demo.marwatch.net/central/rest/devices/6f41fb88-f2ea-4517-b85c-e47fb0104e34/
```

Copy URL

Device Information

Probe Versions Licensing

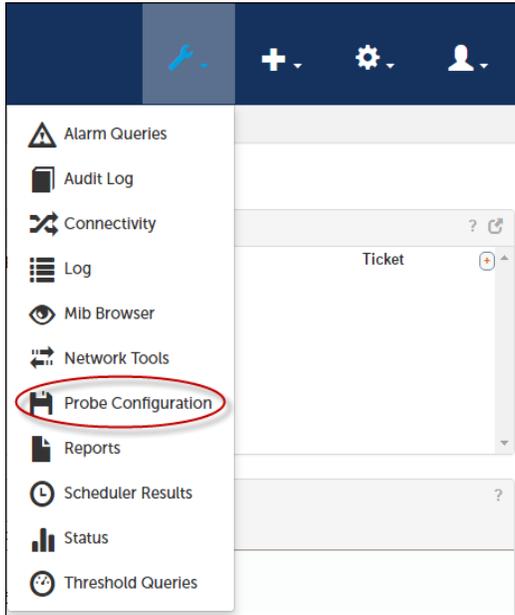
Local IP:

Public IP:

Check In:

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.

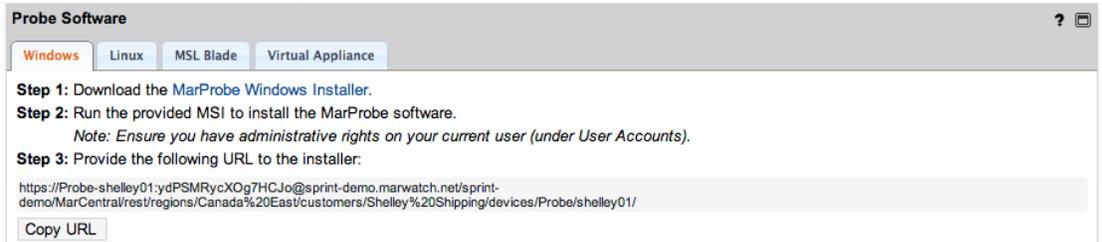
If a Probe is already connected to Mitel Performance Analytics, the **Probe Configuration** panel is available under the **Tools** icon of the Probe dashboard:



PROBE WINDOWS INSTALLATION

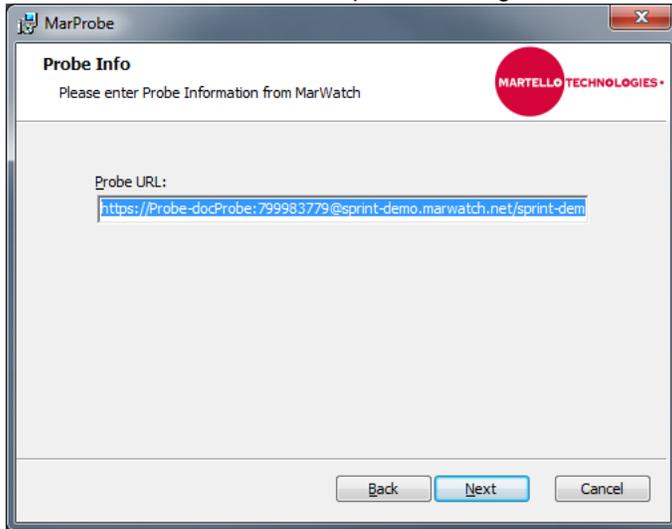
The Windows Installer runs on Windows (XP, Vista, 7) and Windows Server (2003 and Server 2008). To install the software on Windows:

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. Copy the Probe URL, either manually or by clicking the **Copy URL** button.
Note: To do this step, you must have the **Probe Installer** administrative permission.
5. Run the Probe Windows installer.

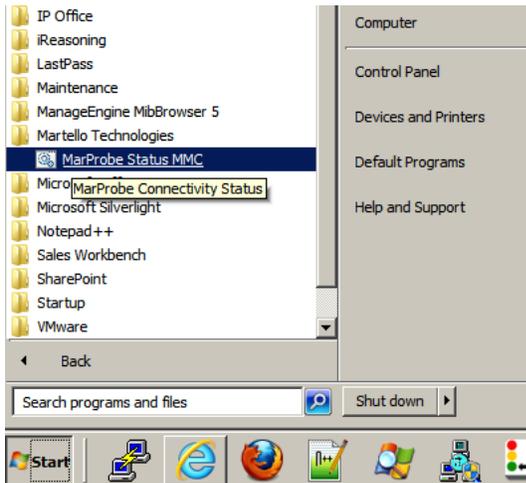
6. Paste the Probe URL when requested during the installation process.



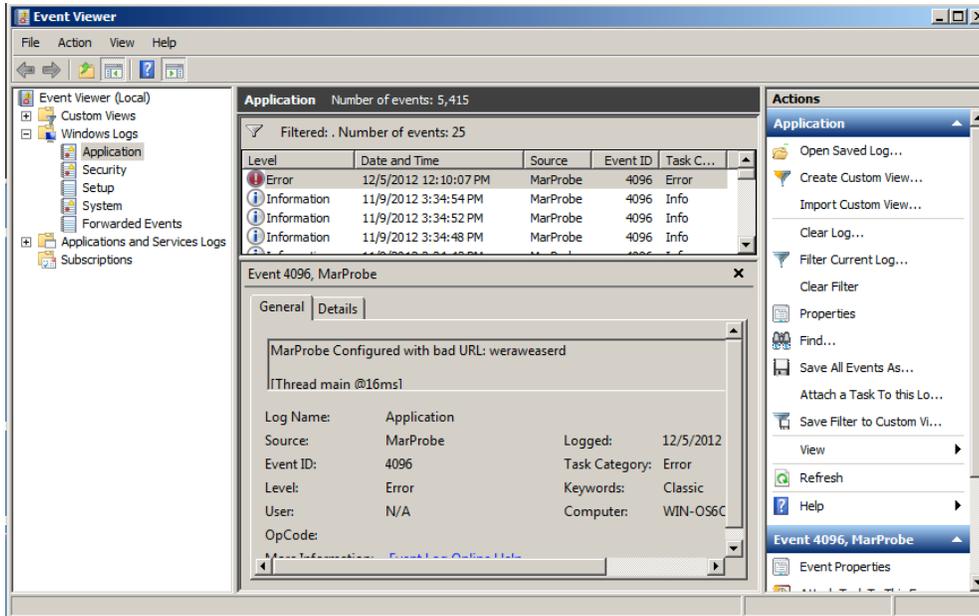
When the installer has finished, the Probe software is configured to run as a Windows service.

Confirm Installation

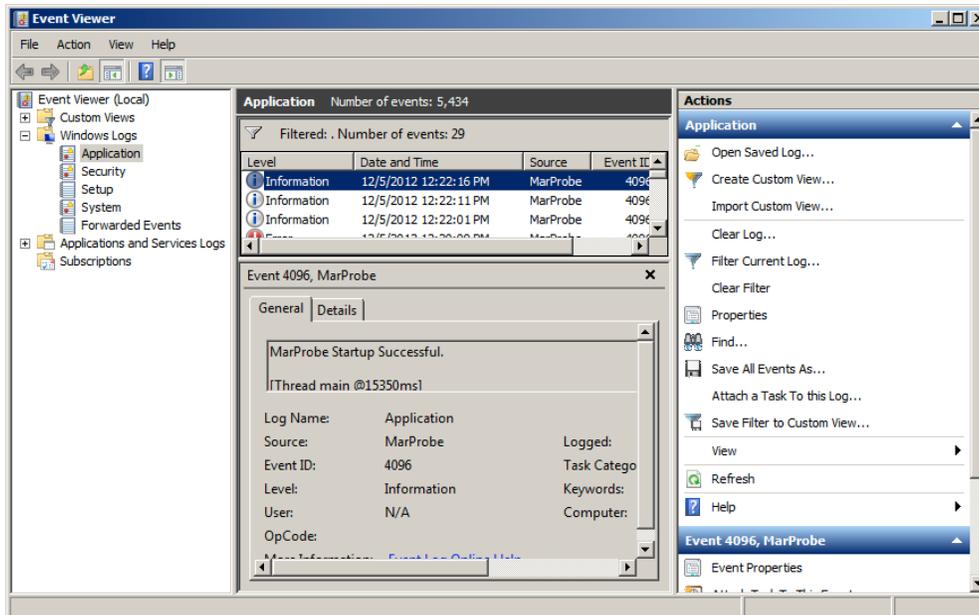
To confirm that the software is running, go to the Martello Technologies folder in the Start Menu, and click on the MarProbe Status MMC link.



This action opens the Microsoft Management Console and shows recent Windows events related to the Probe. In the following example, the Probe has been misconfigured with a bad URL. This condition is shown in the MMC Console.



To correct the URL, uninstall and reinstall the Probe software with the correct URL. This time, the MarProbe Status MMC command shows that the Probe startup has been successful.



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:

Mitel Performance Analytics Probe Installation and Configuration Guide

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]

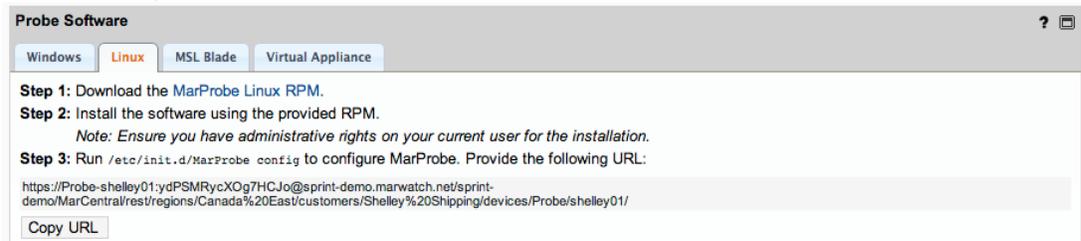
Type: information
Event: 4096
Date Time: 12/05/2012 13:37:33
Source: MarProbe
ComputerName: MRTCOMP-11
Category: Info

```
User: N/A
Description: Remote Access Connected. [Thread RemoteAccess Client
Initializing
Thread @51797656ms]
```

PROBE LINUX INSTALLATION

The Probe is supported on Red Hat Enterprise Linux or a derivative platform such as Fedora, CentOS or Mitel Standard Linux.

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 RPM to the Linux system.



4. Copy the Probe URL, either manually or by clicking on the **Copy URL** button.
Note: To do this step, you must have the **Probe Installer** administrative permission.
5. Open a terminal window.
6. Type `rpm -ivh <path_to_Probe_file/Probe_file_name>.rpm` to install the Probe, resulting in the following output:

```
[root@localhost ~]# rpm -ivh MarProbe-MarWatch-3.5.0.i386.rpm
Preparing... ##### [100%]
java version "1.6.0_22"
OpenJDK Runtime Environment (IcedTea6 1.10.4) (fedora-61.1.10.4.fc16-
i386)
OpenJDK Client VM (build 20.0-b11, mixed mode)
1:MarProbe ##### [100%]
=====
```

7. Type `/etc/init.d/MarProbe config` to configure the Probe and provide it with the Probe URL from the **Probe Configuration** panel:

```
[root@localhost ~]# /etc/init.d/MarProbe config

===== Martello Technologies MarProbe Configuration =====

Enter Probe URL from MarWatch []:
https://Probe-shelley01:ydPSMRycXOg7HCJo@sprint-
demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
Writing config to /usr/local/martello/marProbe.conf... OK
```

8. Type `/etc/init.d/MarProbe start` to start the Probe.

```
[root@localhost ~]# /etc/init.d/MarProbe start
Starting MarProbe (via systemctl): [ OK ]
```

9. To confirm that the software is running, type `ps -Af | grep MarProbe` to display the running Probe processes.

```
[root@localhost ~]# ps -Af | grep MarProbe
root 1873 1 0 10:18 ? 00:00:00 /usr/local/martello/bin/marProbe -debug
-pidfile /var/run/marProbe.pid -DmarProbe.logfile.prefix=/var/log/ -cp
/usr/local/martello/MarProbe-Fat.jar
com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
root 1874 1873 25 10:18 ? 00:00:00 /usr/local/martello/bin/marProbe -
debug -pidfile /var/run/marProbe.pid -
DmarProbe.logfile.prefix=/var/log/ -cp /usr/local/martello/MarProbe-
Fat.jar com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
```

Note: You can also download the Probe using the `wget` command from a terminal window:

```
[root@localhost ~]# wget
https://d3lno0et4zhxmw.cloudfront.net/MarProbe-MarWatch-3.5.0.i386.rpm
--2012-01-16 10:29:51-- https://d3lno0et4zhxmw.cloudfront.net/MarProbe-
MarWatch-3.5.0.i386.rpm
Resolving d3lno0et4zhxmw.cloudfront.net... 204.246.169.166,
204.246.169.191, 204.246.169.186, ...
Connecting to d3lno0et4zhxmw.cloudfront.net|204.246.169.166|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 898566 (878K) [application/x-rpm]
Saving to: "MarProbe-MarWatch-3.5.0.i386.rpm"

100%
[=====
=====>] 898,566 3.07M/s
in 0.3s

2012-01-16 10:29:51 (3.07 MB/s) - "MarProbe-MarWatch-3.5.0.i386.rpm"
saved [898566/898566]
```

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 Support

The Probe MSL blade is supported on MSL R9.3 and later.

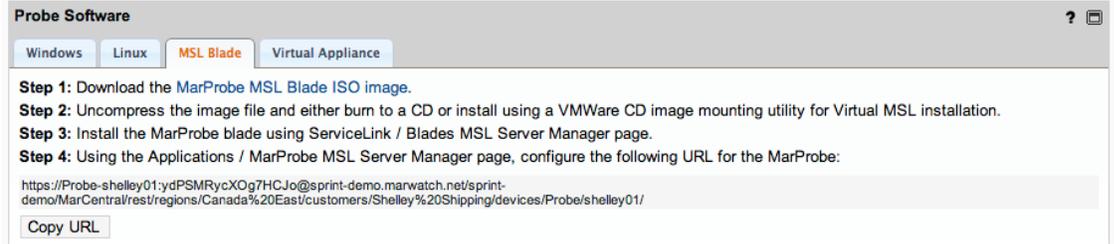
Blade Packaging

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 Configuration** panel, select the **MSL Blade** tab and download the MSL blade ISO image.

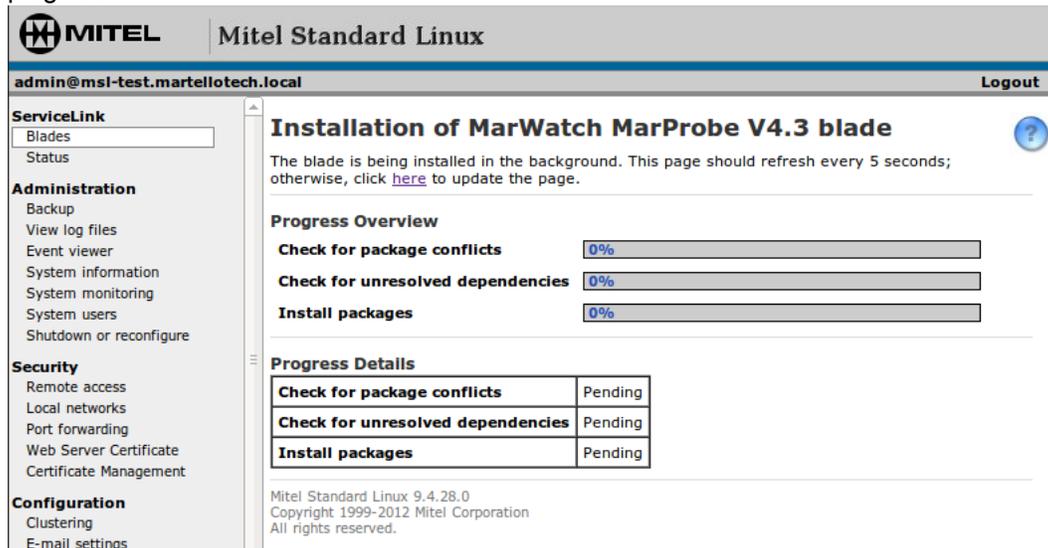


3. Copy the Probe URL, either manually or by clicking on the **Copy URL** button.
Note: To do this step, you must have the **Probe Installer** administrative permission.
4. Open a Web browser and navigate to the MSL server manager URL (for example, `http://<MSL_server_FQDN>/server-manager`).
5. Log in 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.

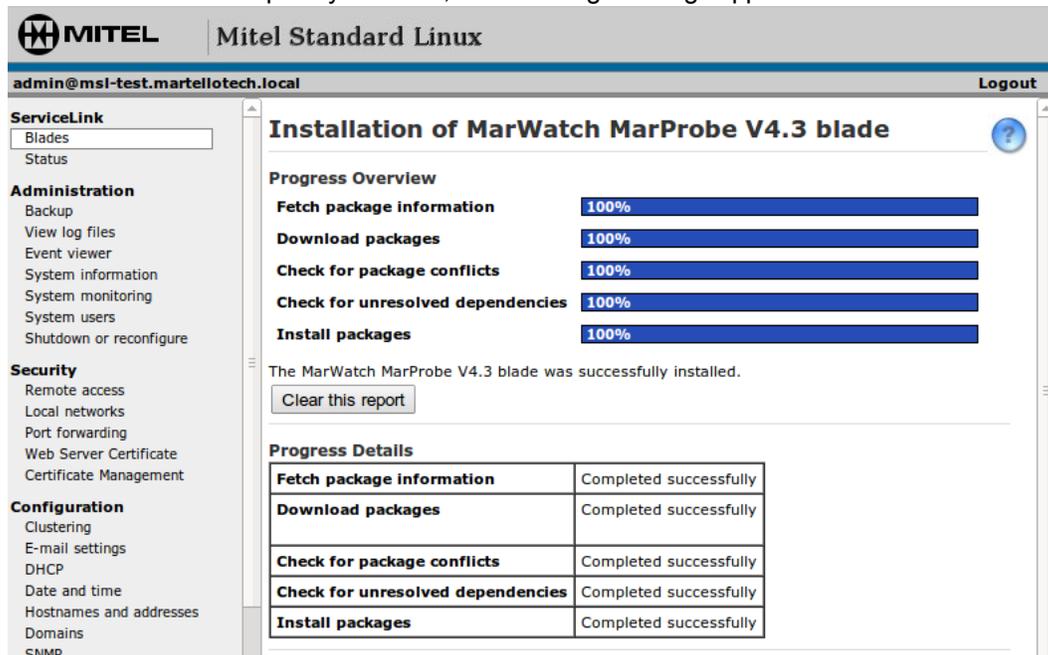


8. Click **Install**.
9. Review and accept the software license terms by clicking **Accept All Licenses**.

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



- When the blade is completely installed, the following message appears on the screen:



- 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.

PROBE MICOLLAB BLADE INSTALLATION

The Probe software can be installed on a MiCollab server as a blade.

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

To manually install the Probe software downloaded from the Probe dashboard as a blade on a MiCollab server:

1. Start an SSH session to the MiCollab system. Log in as `root` with the admin password.
2. Put the ISO image from the Probe dashboard onto the `/root` directory of the MiCollab server using one of the following methods:
 - Download the ISO image to your local computer and then use SSH to copy the file to the MiCollab server.
 - Download the ISO image to your local computer and then put it on a USB memory stick.
 - Download the ISO image directly from the Mitel Performance Analytics server to the MiCollab server.
3. Mount the ISO image to the Linux system using the `mount -o loop` command.
4. Install the blade using the `install_blade -cdrom` command.
5. If your MiCollab is running MSL 10.3.31 or later, run the following command:
`signal-event app-post-install`

Example – Copying a local ISO image using scp

This assumes the following:

- You have already downloaded the ISO image to your local computer.
- The ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso`.
- The IP address of the MiCollab server is `10.10.5.10`.

The `scp` command to copy from your local system to the MiCollab `/root` directory is:

```
scp Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso  
root@10.10.5.10:/root/
```

Example – Copying a local ISO image using WinSCP

This assumes the following:

- You have already downloaded the ISO image to your local computer.
- The ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso`.
- The IP address of the MiCollab server is `10.10.5.10`.

The procedure to copy from your local Windows machine to the MiCollab `/root` directory is:

1. Start the WinSCP application.
2. Connect to the MiCollab server.
3. Using the WinSCP GUI, drag the `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso` file to the target MiCollab `/root` directory.

Example – Direct download of the ISO image

This assumes the following:

- The URL of the Mitel Performance Analytics server is `https://mycompany.com`.
- You have not already downloaded the ISO image to your local computer.

The `wget` command to download the ISO image from the Mitel Performance Analytics server to the `MiCollab /root` directory is:

```
wget https://mycompany.com/ProbeSoftware/MarProbe-Installer.noarch.iso
```

Example – Mounting and Installing ISO Image When Using SSH

In this example, the ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso`. The `MiCollab` is running `MSL 10.3.31` or later.

The Linux commands to mount the ISO image and install the blade are:

```
mkdir /mnt/cdrom
mount -o loop Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso
/mnt/cdrom
install_blade -cdrom Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386
signal-event app-post-install
```

Example – Mounting and Installing ISO Image When Using USB Stick

In this example, the USB stick's storage name is `sdd1` and the ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso`. The `MiCollab` is running `MSL 10.3.31` or later.

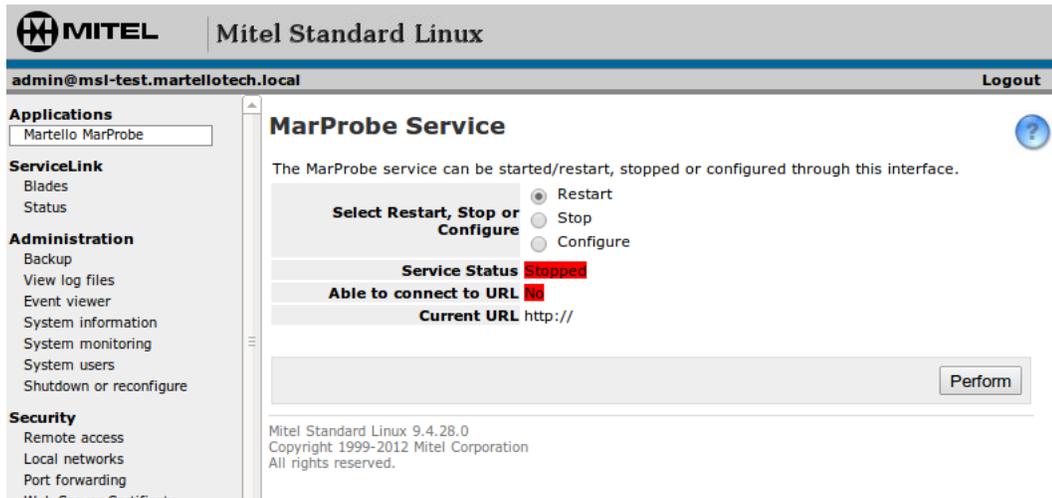
The Linux commands to mount the ISO image and install the blade are:

```
mkdir /mnt/usbflash
mount /dev/sdd1 /mnt/usbflash
cp /mnt/usbflash/Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso /root/
mkdir /mnt/cdrom
mount -o loop Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso
/mnt/cdrom
install_blade -cdrom Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386
signal-event app-post-install
```

Post Blade Installation Configuration

After installing the Probe blade, you must configure the Probe. You are presented with a new link in the Applications menu: `Martello MarProbe`.

Click the **Martello MarProbe** link to open the **MarProbe Application Menu**.



The web interface for the Probe service has three options; **Restart**, **Stop** and **Configure**. To perform an action, select an option and click the **Perform** button.

By default **Restart** is selected. It performs a restart of the Probe service. The **Stop** option forces the Probe service to stop. The **Configure** option is used to apply a Probe URL from the Mitel Performance Analytics device page for the Probe.

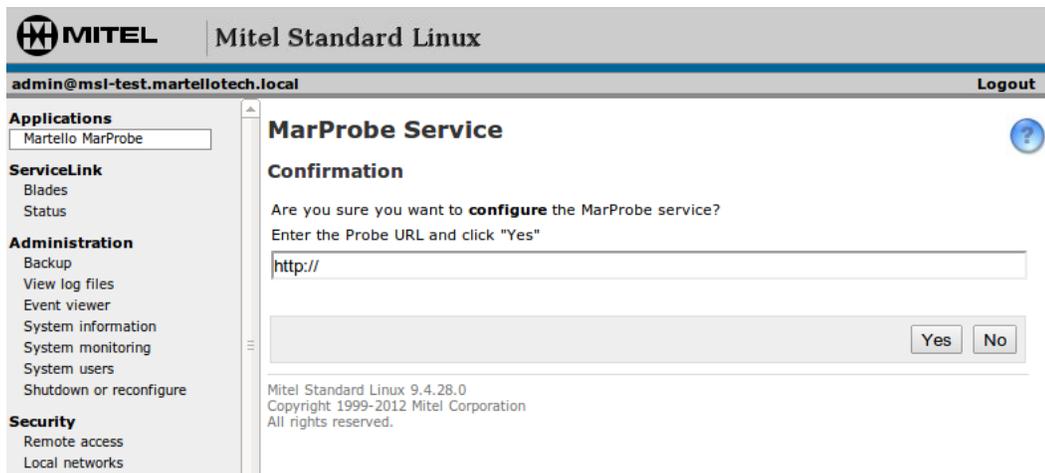
When the Probe service is initially installed, there is no Probe URL configured and the service is stopped.

Note: After installation or upgrade of the Probe blade, you may be unable to **Restart**, **Stop** or **Configure** the Probe service. This is a known MSL issue. The workaround is to quit the web browser, wait 15 minutes for all session timers to expire and try again.

To configure a URL for the Probe service, select the **Configure** option and click **Perform**.

Enter the URL from the **Probe Configuration** panel in Mitel Performance Analytics into the Probe URL text box, and click **Yes**. This applies the URL to the system and the restarts the Probe service.

Note: To do this step, you must have the **Probe Installer** administrative permission.



After the service is restarted, the MarProbe Application interface shows the Probe service status and whether or not Mitel Performance Analytics is reachable from the Probe (that is, that the Probe can resolve the hostname in the URL and establish a connection to the Mitel Performance Analytics server identified by that hostname).



The Service Status shows the status of the Probe, either Running or Stopped.

If the MSL server can connect to the URL specified, the **Able to connect to URL** field shows Yes. If not, it shows No.

This feature facilitates troubleshooting connectivity issues by allowing arbitrary URLs to be tested, similar to pinging a server. For example, if <http://www.google.com> is entered as the configured URL, the MSL server attempts to retrieve the contents of <http://www.google.com> and report the result of that action.

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 14.04 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 "Host Requirements" on page 5.

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 `config`.
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:
Command: `sudo vi /etc/network/interfaces.d/eth0`
Fields:

```
auto eth0
iface eth0 inet static
address <IP address>
netmask <network mask>
gateway <Gateway IP Address>
```

- Press `Esc` and enter `:wq` to write and exit from the file.
- Configure DNS server by running the following command and providing the following fields:
Command: `sudo vi /etc/resolv.conf`
Fields:

```
nameserver <DNS server IP Address 1>
nameserver <DNS server IP Address 2>
```

Enter as many DNS server IP addresses as required.

- Press `Esc` and enter `:wq` to write and exit from the file.
- Bring up the network interface by running the following command:
Command: `sudo ifdown eth0 && sudo ifup eth0`

7. Type `sudo /etc/init.d/marprobe config` to configure the Probe and provide it with the Probe URL from the **Probe Configuration** panel:

Note: To do this step, you must have the **Probe Installer** administrative permission.

```
[root@localhost ~]# sudo /etc/init.d/marprobe config
```

```
===== Martello Technologies MarProbe Configuration =====
```

```
Enter Probe URL from MarWatch []:
https://Probe-shelley01.ydPSMRycXOg7HCJo@sprint-
```

```
demo.marwatch.net/sprint-  
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping  
/devices/Probe/shelley01/
```

Writing config to /usr/local/martello/marprobe.conf... OK

8. Type `sudo /etc/init.d/marprobe start` to start the Probe.

```
[root@localhost ~]# sudo /etc/init.d/marprobe start  
Starting marprobe (via systemctl): [ OK ]
```

9. To confirm that the software is running, type `sudo ps -Af | grep marprobe` to display the running Probe processes.

```
[root@localhost ~]# sudo ps -Af | grep marprobe  
root 1873 1 0 10:18 ? 00:00:00 /usr/local/martello/bin/marprobe -debug  
-pidfile /var/run/marprobe.pid -Dmarprobe.logfile.prefix=/var/log/ -cp  
/usr/local/martello/marprobe-Fat.jar  
com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-  
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-  
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping  
/devices/Probe/shelley01/  
root 1874 1873 25 10:18 ? 00:00:00 /usr/local/martello/bin/marprobe -  
debug -pidfile /var/run/marprobe.pid -  
Dmarprobe.logfile.prefix=/var/log/ -cp /usr/local/martello/marprobe-  
Fat.jar com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-  
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-  
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping  
/devices/Probe/shelley01/
```

10. If you need to configure the Linux system (IP address DNS, system name etc.), use standard Red Hat or CentOS instructions.
These are available at: <http://wiki.centos.org/FAQ/CentOS6>

PROBE APPLIANCE INSTALLATION

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



The Probe Appliance has connectors for:

- Power, 110/240 VAC, 50/60 Hz
- Ethernet (10, 100, 1000 BASE-T)
- USB 2.0 type A

The Probe Appliance is shipped with:

- Standard US Power Cord
- Two-pin US Power Connector
- Ethernet Cable

The Probe Appliance must be configured for use with Mitel Performance Analytics. The configuration details for a Probe 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 Probe.

PROBE APPLIANCE CONFIGURATION WITH SSH

Do the following steps:

1. Connect power and Ethernet to the Probe Appliance. The Probe Appliance uses DHCP to obtain its Ethernet address. To configure a Probe Appliance, you need to know its IP address.
2. The IP address can be obtained by scanning the network in which the Probe 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 `config`. The first time you login to the system, it prompts you to change the shipped default password. The `config` user has `sudo` privileges.
The following is an example of the password change dialog. (Note that IP addresses and Linux version numbers may be different. This is not significant).

```
Using username "config".
```

```
config@10.4.50.8's password:
```

```
You are required to change your password immediately (root enforced)
```

```
Linux marProbe 2.6.32-5-kirkwood #1 Sat Dec 11 05:09:52 UTC 2010
```

```
armv5tel
```

```
The programs included with the Debian GNU/Linux system are free software;
```

```
the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
```

```
Last login: Wed Jul 6 14:37:29 2011 from 10.4.50.7
```

```
WARNING: Your password has expired.
```

```
You must change your password now and login again!
```

```
Changing password for config.
```

```
(current) UNIX password:
```

```
Enter new UNIX password:
```

```
Retype new UNIX password:  
passwd: password updated successfully
```

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. Type `sudo /etc/init.d/marprobe config` to configure the Probe and provide it with the Probe URL from the **Probe Configuration** panel:
Note: To do this step, you must have the **Probe Installer** administrative permission.

```
[root@localhost ~]# sudo /etc/init.d/marprobe config
```

```
===== Martello Technologies MarProbe Configuration =====
```

```
Enter Probe URL from MarWatch []:  
https://Probe-shelley01:ydPSMRycXOg7HCJo@sprint-  
demo.marwatch.net/sprint-  
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping  
/devices/Probe/shelley01/
```

```
Writing config to /home/marProbe/etc/marProbe.conf...  
OK  
MarProbe service is now restarting  
Stopping MarProbe stopped PID=###  
Starting MarProbe started PID=###
```

PROBE APPLIANCE CONFIGURATION WITH USB DRIVE

The Probe Appliance can also be configured using a USB drive. To configure the Probe 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:

```
url=  
force=
```

Note: These options are case sensitive and must not contain quotation marks. After the `url=` option, enter the Probe configuration URL supplied by Mitel Performance Analytics. The file dates are used to determine if the configuration URL should be applied. This can be overridden by placing `YES` after the `force=` option. Any other value in the force option field is ignored. Also note that only the first `url` and `force` options are read.

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 Probe 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.

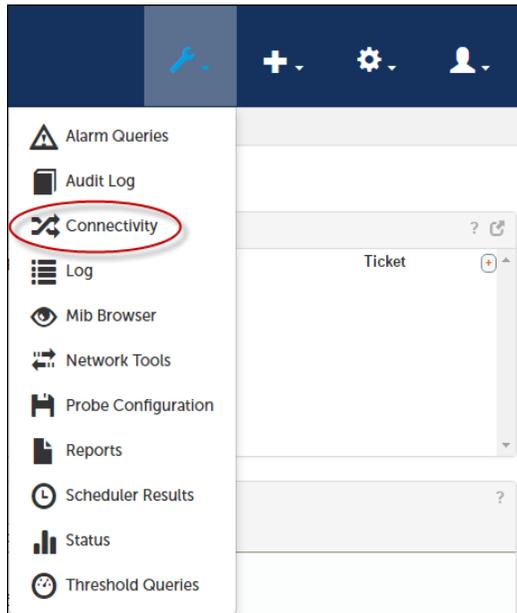
USB DRIVE LOG ACCESS

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

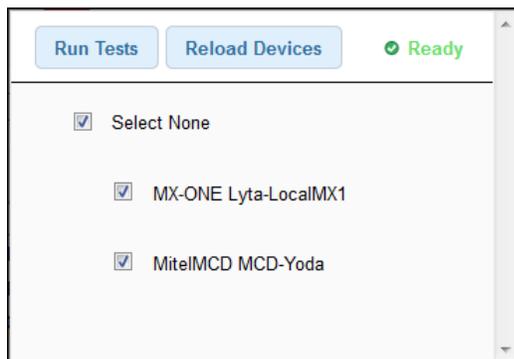
PROBE DEVICE CONNECTIVITY CHECK

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 available under the **Tools** icon of 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.

✔ Checks Complete.

Select None

MX-ONE Lyta-LocalMX1 (Updated at 2:20:52 PM)

SNMP	✔	System Name: MX-ONE-VM System Description: Linux MX-ONE-VM 2.6.16.60-0.85.1-bigsmg #1 SMP Thu Mar 17 11:45:06 UTC 2011 i686 Got response in 60ms
ICMP Ping	✔	Got response in 0ms

MitelMCD MCD-Yoda (Updated at 1:20 PM)

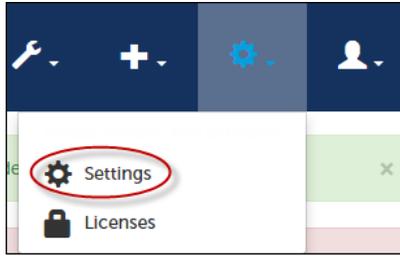
SNMP	⚠	SNMP request timed out
ICMP Ping	⚠	No response
MiXML	⚠	AxisFault ; nested exception is: java.net.SocketTimeoutException: connect timed out
SMDR	⚠	Unable to connect

PROBE 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 **Settings** under the **Settings** icon.



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 device, Probe settings include:
 - **IP SLA Monitoring:** Enable the checkbox and enter up to four IP SLA targets, specifying either the target IP address or their 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 Diagnostics:** Enabling these settings displays additional diagnostic tools. The tools should be used and interpreted with assistance from Mitel support.
 - **Probe Software Override JAR URL** field: This field is used for troubleshooting purposes. It allows for installation of special software. It is used only with assistance from Mitel support.
 - **Probe Password:** This setting appears only when you have the **Probe Installer** administrative permission. When a Probe is first added to Mitel Performance Analytics, Mitel Performance Analytics generates a random security password for Server to Probe communications. Afterwards, when the Probe is installed, it is automatically configured to use this password. At this stage, when first adding a Probe but before it is installed, users may choose to replace the random password with their own. The security password can contain only alphanumeric characters. Spaces or other special characters cannot be used. Changing the password after the Probe is installed and configured is not recommended because it disables Server to Probe communications.
 - **Remote Access Control:** See "Remote Access Control Configuration" on page 30.
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:



The screenshot shows a configuration window titled "Remote Access". Inside, there is a label "Allow Port Forwards:" followed by a dropdown menu. The dropdown menu is open, showing four options: "Always", "Never", "Always", and "To Monitored Devices Only". The second "Always" option is highlighted with a blue background.

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.

