Performing Initial Setup for the Dashboard

Performing Initial Setup for the Dashboard

There are a few configuration tasks that should be performed to ensure that the Dashboard meets your requirements.

Configuring Basic System Settings

To configure basic system settings such as IP addressing and time settings for the Dashboard, follow the steps below:

1. Connect to the console of the Dashboard using the appropriate tools for your hypervisor if using a virtual machine, or by connecting to your AWS or Azure instance using SSH
2. If using a virtual machine, log in using the default username and password set to: `cisco`. For an AWS instance, use the key pair you specified when the instance was created, and the username: `cisco`. For an Azure instance, use the administrator username and password or key you specified when creating the instance.

   You will be required to change the password for the cisco account immediately after logging in. The new password should be a complex, non-dictionary word using a mixture of character types.
3. Enter the command `sudo config_vm` to perform the initial configuration. When prompted, enter the password for the cisco account. The `config_vm` utility will prompt you with a series of steps to change the platform settings.
4. First you will be prompted to change the hostname for the Dashboard. The hostname is used to identify the Dashboard on the network. Choose a meaningful name here, or you can skip this step to keep the default hostname.
5. Next you will be prompted to change the web server ports. If these ports are changed from the default values, it may also be necessary to change firewall settings in your network, or security group settings in AWS or Azure.
6. Next you will be prompted to configure the network interface. The options here are static and dhcp (the default). If you select static, you will be prompted for IP address information, default gateway, and DNS server addresses. The network interface will be reset if you make changes here.

Note This step is not available with Cisco Business Dashboard for AWS or Azure. To modify the network configuration, use the EC2 console in AWS for an AWS instance. Use the Azure Portal for an Azure instance.

7. Next, you will be prompted to configure the time settings for the Dashboard. You can opt to configure one or more NTP servers for time synchronization (recommended), and you will be asked to select the timezone.

Note If the hypervisor in use is VirtualBox and the VirtualBox Guest Additions are installed in the VM, the NTP service - timesyncd - will not operate.

8. Finally, you will be asked if you wish to change the bootloader password. The bootloader username and password can be used on the console at system startup to change the system boot process or recover lost operating system passwords. The default bootloader credentials are username: **root** and password: **cisco**.

You can change these settings at any time by re-running the script, or through the web interface at **System**>**Platform Settings**.

Launching the Dashboard User Interface

1. Launch a web browser such as **Google Chrome** or **Microsoft Edge**.
2. In the **Address** field, enter the IP address or hostname of the Dashboard and press **Enter**
3. Enter the default user name: `cisco` and password: `cisco`. If you are using Cisco Business Dashboard for AWS, the default password is the instance ID. You can view the instance ID in the AWS EC2 console.
4. Click **Login**. You will be prompted to change the username and password for the cisco account. Ensure that the new password is at least 8 characters in length contains at least 3 different character classes.
5. Click **Next**. You will be presented with information about how Cisco Business Dashboard uses your data and what information is shared with Cisco. Make any changes appropriate for your organization's requirements before proceeding.
6. Click **Next**. At this point you are given the option to run the System Setup Wizard which walks you though the key configuration elements that should be considered when installing a new dashboard. You may choose to continue with the wizard by clicking **Next**, or you may click **Finish** to exit to the dashboard UI.

If you choose to proceed with the System Setup Wizard, it will guide you through each of the following areas:

- Platform Settings, including network setup, webserver and security configuration.
- Software licensing requirements. This section is generally only required for systems that will manage more than 25 network devices
- Email forwarding setup for notifications and alerts.
- Creating additional organizations to help manage complex networks or to deliver managed services.
- Create additional users who can manage the dashboard.

- Choose whether to enable or disable Local Probe.

For more information on any of the configuration covered by the wizard, consult the corresponding section of the Cisco Business Dashboard Administration Guide.

Disabling the Embedded Probe on the VM Image

Note This does not apply to Cisco Business Dashboard for AWS or Azure.

The virtual machine image for the Dashboard includes the Probe software for managing devices on the network local to the Dashboard. If you do not wish to manage the local network, you can disable the embedded Probe using the following steps:

1. Navigate to **System**>**Local Probe**.
2. Click the toggle switch to disable the embedded Probe.
3. Click **Save**.

Create Networks (Optional)

You can pre-define network records in the Dashboard for Probes that you will associate later. Typically, each network represents a separate site, but you can have multiple networks in the same location. To create a new network, follow the steps below:

1. Navigate to **Network**.
2. Click **Add Network** in the **Map View** or **+**(plus) icon in the **List View**.
3. Specific a name, organization and default device group for the network.

   If the dashboard version is 2.6.0 or higher, you must also choose the management method for the network - Probe Managed if you will be using a software or embedded probe to manage the network, or Direct Managed if you will be enabling the CBD agent on each device. If you choose Direct Managed, you may also choose to have the dashboard automatically enable the agent on any newly discovered devices in the network.
4. Enter the address of the network into the appropriate fields. If you enter a partial address, a list of potential matches will be displayed, and you can select the location from the list. Alternatively, you can click on the location in the map.
5. Click **Save**.
6. Repeat steps 1 to 5 for each network you wish to create.

Performing Initial Setup for the Dashboard