Standalone Sentry 9.13.0 Installation Guide

for Core and Cloud

May 17, 2021

Contents

Overview for installing Standalone Sentry

This guide provides you with the information required to install Standalone Sentry. Standalone Sentry is a component of a Ivanti deployment. A Standalone Sentry deployment requires that you have already installed one of the Unified Endpoint Management (UEM) platforms, Core or Cloud. With input from Core or Cloud, Standalone Sentry does the following:

- Standalone Sentry configured for ActiveSync protects the ActiveSync server from wrongful access from devices.
- Standalone Sentry configured for AppTunnel provides authenticated apps secure access to the backend resource.

The installation instructions assume that you have already installed either Core or Cloud.

If your deployment uses Core, refer to the On-Premise Installation Guide for your Core version for information about setting up and installing Core. The On-Premise Installation Guide includes information about customer resources, deployment checklists, and firewall rules.

If your deployment uses Cloud, the Setup Wizard takes you through the initial setup. You can also refer to the *Cloud Getting Started: Basic Setup* document and the online help available with Cloud. Ensure that port 443 inbound is open. See Cloud Architecture and Port Requirements for more information.

Download Standalone Sentry ISO

For information about downloading the Standalone Sentry ISO see the *Standalone Sentry Release and Upgrade Notes* for your release.

Requirements for on-premise installation

You can set up Standalone Sentry on a virtual machine (VM) or a physical appliance. However, Standalone Sentry setup on a physical appliance is supported only for Core deployment. Standalone Sentry setup on a VM is supported for both Core and Cloud deployments.

The following provide the requirements for an on-premise Standalone Sentry installation and contains the following sections:

Virtual Standalone Sentry requirements

If you are installing Standalone Sentry on a virtual machine (VM), ensure that the minimum requirements are met.

ⓘ Standalone Sentry tunes its settings based on the available resources.

The following describe the minimum requirements for setting up Standalone Sentry on a VM:

- "Hard drive" below
- "Periodic backups for VMware" on the next page
- "VMware requirements (Core and Cloud)" on the next page
- "Hyper-V requirements (Core and Cloud)" on page 6
- "Minimum memory and CPU requirements for email (VMware and Hyper-V)" on page 6
- "Minimum requirements for tunneling (VMware and Hyper-V)" on page 6

Hard drive

Ivanti recommends the following:

- Configuring only one hard drive on the virtual machine.

  - Since system performance is directly related to hard disk drive performance, use only high-performance tier 1 storage products.

Periodic backups for VMware

Ivanti recommends the following:

- Take periodic .vmdk backups of your Virtual Appliance as part of your system maintenance.
  - Use VMware VCB or another VMware-supported backup system.
  - A backup of the full virtual disk is recommended; VMware snapshots are not sufficient.

VMware requirements (Core and Cloud)

Confirm the following requirements before setting up Standalone Sentry on VMware:

- Download link or package (ISO) from Support: [Support page]
- VMware

- ESXi 7.0
- ESXi 6.5
- ESXi 6
- ESXi 5.1/5.5

- 64-bit VM
- Network adapter:

- E1000
- VMXNET3

- VM OS Type:

- CentOS (64-bit)
- Other Linux (64-bit)
- Red Hat Enterprise Linux (64-bit)

This setting is intended to ensure successful installation; it does not imply that Ivanti distributes Red Hat.

- CPU Settings:

- Shares: Normal
- Reservation: 900MHz
- Limit: Unlimited (maximum assigned)

ⓘ Ivanti supports LSI logic SAS or Parallel SCSI controllers; para-virtualized controllers are not supported at this time. Only E1000 and VMXNET3 network adapters are supported.

Hyper-V requirements (Core and Cloud)

Confirm the following requirements before setting up Standalone Sentry on Hyper-V:

- Hyper-V version

- Microsoft Hyper-V Server 2012 R2
- Microsoft Hyper-V 2016

- 64-bit VM

- Network adapter

NOTE: Microsoft Hyper-V Server 2008 requires legacy network adapter.

Minimum memory and CPU requirements for email (VMware and Hyper-V)

The following table shows VM memory and CPU requirements depending on the number of devices your Standalone Sentry supports for email:

TABLE 1. MINIMUM MEMORY AND CPU REQUIREMENTS FOR EMAIL (VMWARE AND HYPER-V)

	Small configuration	**Medium configuration**	**Large configuration**
Maximum devices	< 2000 devices	< 8000 devices	< 20,000 devices
Memory	4 GB	6 GB	8 GB
Virtual CPUs **	1	2	4
Memory reservations	Reservations: 4 GB	Reservations: 6 GB	Reservations: 8 GB
Disk	20 GB	30 GB	40 GB

Minimum requirements for tunneling (VMware and Hyper-V)

To calculate the requirements for AppTunnel, see Sizing Calculator for the Access and AppTunnel Sentry.

Supported appliances

The following provide the appliances supported and the number of devices supported for emails and app tunnels for an appliance:

- "Supported number of devices for email" below.
    - "Supported number of devices for tunneling" below.

Supported number of devices for email

The following table summarizes capacity of supported devices (email only) for physical Standalone Sentry models:

TABLE 1. MAXIMUM NUMBER OF DEVICES SUPPORTED FOR EMAIL (HARDWARE)

Model	Max Number of Devices
M2600	40,000
M2500	40,000
M2250	20,000
M2200	20,000
M2100 (Gen 3)	20,000

Supported number of devices for tunneling

To calculate the requirements for AppTunnel, see Sizing Calculator for the Access and AppTunnel Sentry.

Installing the Standalone Sentry ISO on an appliance (Core only)

You can install a Standalone Sentry ISO on a appliance using a DVD or USB drive. The following describe the preparation and installation:

1. "Setting up access to the appliance" on the next page
2. "Preparing a USB drive for installation (M2600, M2250 only)" on the next page
3. "Installing Standalone Sentry ISO from DVD or USB" on page 9
   OR
   "Installing Standalone Sentry ISO using the IPMI feature " on page 10

Setting up access to the appliance

Standalone Sentry setup on an appliance is not supported for Cloud.

If you are installing the Standalone Sentry ISO on a physical appliance, you need to set up access to the console. You can use a PC or remote console system.

If using a PC, make sure it has a terminal program, such as Putty or HyperTerminal.

Procedure

1. Connect a console cable to the DB-9 port on the back of the appliance.
2. Connect a serial cable to a PC or remote console system.

Next steps

- If you are installing the Standalone Sentry ISO on a M2600 appliance using a USB drive, go to "Preparing a USB drive for installation (M2600, M2250 only)" below for instructions on how to prepare the USB drive.
    - If you are installing the Standalone Sentry ISO using a DVD go to "Installing Standalone Sentry ISO from DVD or USB" on the next page for the installation steps.
    - If you are installing the Standalone Sentry ISO using the IPMI feature, go to "Installing Standalone Sentry ISO using the IPMI feature " on page 10.

Related topics

For initial configuration for Standalone Sentry, go to "Using the setup wizard to complete Standalone Sentry installation" on page 15. Follow the steps to configure the Standalone Sentry.

Preparing a USB drive for installation (M2600, M2250 only)

The M2600 appliance does not come with a DVD-ROM drive. You will need to use a USB drive instead. The following describes how to prepare a bootable USB drive. Do these steps only if you are using a USB drive to install the Standalone Sentry ISO on an M2600 or M2250 appliance.

You also have the option to install the Standalone Sentry ISO using IPMI. Follow the steps in "Installing Standalone Sentry ISO using the IPMI feature " on page 10 to install the Standalone Sentry ISO on the M2600 appliance.

Before you begin

Ensure that the USB flash drive meets the following minimum requirements:

- USB Standard 2 or 3

- USB Connector Type-A
- Minimum size 2 GB

Procedure

1. Insert a USB drive into a Windows PC.
   Use a USB drive with a minimum of 2GB storage space.
2. Download the Standalone Sentry ISO image to the same PC from the Ivanti Support site.
3. Download a third-party bootable USB creation tool to the same PC to create a bootable USB drive.
   You can download one from https://rufus.akeo.ie/.
4. Run the tool and provide the following information when asked in the tool wizard:
   - Location of ISO.
   - Location of USB drive.
   - Volume label name for the USB drive.
     You must use **MOBILEIRON** as the volume label name.
5. Complete the wizard to create a bootable USB drive.

Next steps

See "Installing Standalone Sentry ISO from DVD or USB" below for the installation steps.

Select hw-usb-install when the installation program begins.

Installing Standalone Sentry ISO from DVD or USB

The following steps describe the installation of the Standalone Sentry ISO.

Before you begin

- Set up access to the appliance as described in "Setting up access to the appliance" on the previous page.
- Download the Standalone Sentry ISO from the software download site. See the release notes for links to the latest version.
- If you are installing on a M2600 appliance, do the steps described in "Preparing a USB drive for installation (M2600, M2250 only)" on the previous page.

Procedure

1. Insert the DVD or USB (containing the Standalone Sentry ISO image) into the appliance.
   USB installation is available only on the M2600 appliance.
2. Wait for the appliance to reboot for the installation program to begin after a few minutes.

Next steps

See "Using the setup wizard to complete Standalone Sentry installation" on page 15, for information on using the installation wizard.

Installing Standalone Sentry ISO using the IPMI feature

The appliance comes with the Intelligent Platform Management Interface (IPMI) module. Log in to the module remotely to install the Standalone Sentry ISO.

Before you begin

- Assign an IP address and user name and password to the IPMI module.
  - Download the Standalone Sentry ISO from the Ivanti software download site. See the release notes for links to the latest version.

Procedure

1. Log in to the IPMI module from a browser.
2. Go to **Remote Control > Console** Redirection.
3. Click **Launch Console**.
   A .jnlp file downloads.
4. Click on the downloaded .jnlp file.
   The JViewer console opens up.
5. On the JViewer console, go to **Device > Redirect ISO**.
6. Navigate to the location of the Standalone Sentry ISO.
7. Select the Standalone Sentry ISO and click **Open**.
8. On the IPMI module, go to **Remote Control > Virtual Front Panel**.
9. Click **Reset** to reboot the appliance with the Sentry ISO.
   After the image is installed, on the JViewer console, the Sentry installation welcome screen and prompts display.
   Select the appropriate installation option.

Next steps

Go to "Using the setup wizard to complete Standalone Sentry installation" on page 15. Follow the steps to do the initial configuration of Standalone Sentry.

Gather Standalone Sentry installation setup information

The Standalone Sentry installation uses a wizard for an easier process. Before using this wizard, it could be useful to gather the necessary information you will need to input into the wizard. Use the following worksheet to gather this information.

TABLE 1. GATHER STANDALONE SENTRY INSTALLATION INFORMATION

Wizard request	Value
Installation types: - *vm-install* for installing on a virtual machine - *hw-install* for installing on a physical appliance - *hw-usb-install* for installing on an appliance using USB	
Company name	
Contact person name	
Contact email	
Password (must be between 6 and 20 characters)	
Administrative user name (do not use *root*)	
Administrator password (must meet security criteria by including numerals and capital letters)	
Physical interface to connect to the management network. - a = for GigabitEthernet1 - b = for GigabitEthernet2	
IP address for the Sentry (associated with the physical interface)	
Netmask for use with the IP address (e.g., 255.255.255.0)	
Default gateway for the appliance	
Fully-qualified external domain name for the appliance	

Table 1. Gather Standalone Sentry installation information (Cont.)

Wizard request	Value
IP address of the primary name server to be used by the appliance	
(Optional) Secondary and tertiary name servers	
(Optional) IP address of the primary time source (NTP server) if you are configuring a time source	

Standalone Sentry installation on premise

The following describes how to install Standalone Sentry on premise:

Before installing Standalone Sentry

- Ensure that DNS is set up to direct Standalone Sentry to a valid internal IP address when it looks up the FQDN of UEM.

NOTE: If you did not set up the DNS before installing the Sentry, then after the initial Sentry setup, you must add a Host entry in the Sentry System Manager. To add a host, in the Sentry System Manager, go to **Settings > Static Hosts**.

- Create a VM that meets the specifications recommended by Ivanti.

See "Virtual Standalone Sentry requirements" on page 4 for specifications. The Standalone Sentry installation will complete the installation based on the resources you have configured; the installation script does not provide an opportunity to select a deployment size (i.e., small, medium, etc.).

NOTE: Failing to size the VM according to the minimum specification results in a daily error message in the System log.

- Standalone Sentry installation uses a wizard for an easier process. Before using this wizard, Ivanti recommends gathering the necessary information needed to input into the wizard. See "Gather Standalone Sentry installation setup information" on page 10.

- You must have already deployed either Core or Cloud. Standalone Sentry installation on premise is supported for Core and Cloud.

Installing Standalone Sentry ISO on a VM

The following provide the steps for installing the Standalone Sentry ISO on a virtual machine (VM):

- "Installing Standalone Sentry ISO on VMware" on the next page

- "Installing Standalone Sentry ISO on Hyper-V" on the next page

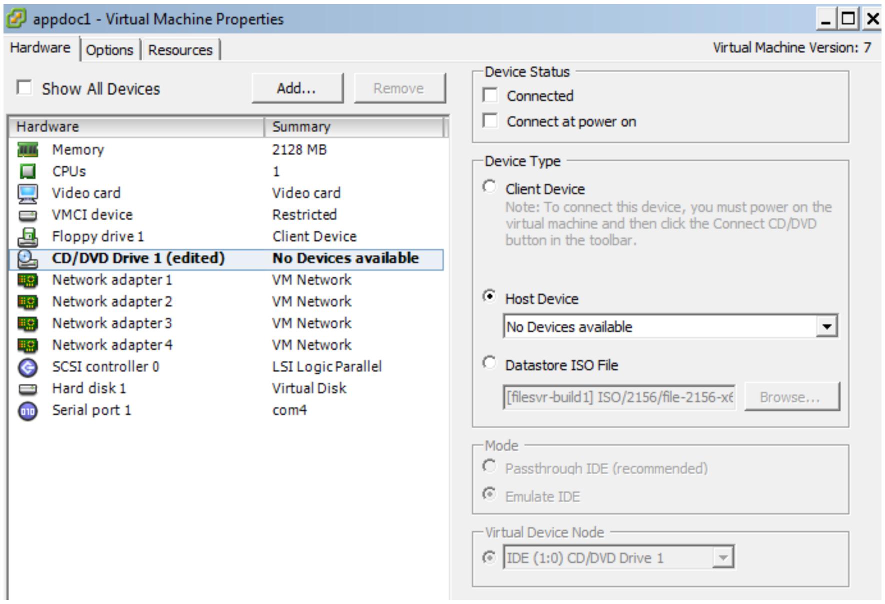
Installing Standalone Sentry ISO on VMware

This section provides instructions on how to download the Standalone Sentry ISO to VMware.

Procedure

1. Place the ISO distribution in an existing vSphere datastore.
2. In the vSphere Client, select the **Edit Settings** option for the VM you created.

FIGURE 1. VIRTUAL MACHINE IN VMWARE



appdoc1 - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 7

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	2128 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Floppy drive 1	Client Device
CD/DVD Drive 1 (edited)	**No Devices available**
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Serial port 1	com4

Device Status
□ Connected
□ Connect at power on

Device Type
○ Client Device
Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar.
● Host Device
No Devices available
○ Datastore ISO File
[filesvr-build1] ISO/2156/file-2156-x€ — Browse...

Mode
○ Passthrough IDE (recommended)
● Emulate IDE

Virtual Device Node
● IDE (1:0) CD/DVD Drive 1

3. Select **Datastore ISO File**.
4. Click **Browse** to select the Sentry ISO distribution.
5. Make sure the "Connected" and "Connect at power on" options in the Virtual Machine Properties screen **are selected.**
6. Select **Host Device**.
7. Click **OK**.
8. Power on the VM.
   The VM automatically installs and reloads after a few minutes, and the installation program starts. See "Using the setup wizard to complete Standalone Sentry installation" on the next page for the next steps.

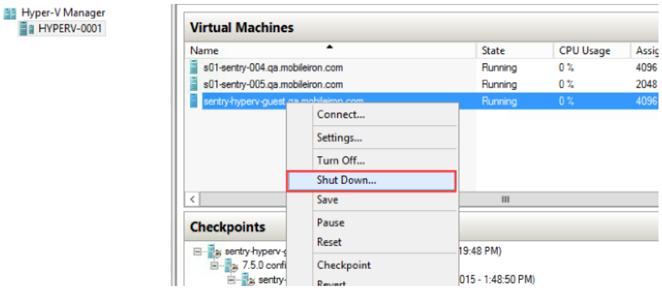
Installing Standalone Sentry ISO on Hyper-V

This section provides instructions on how to download the Standalone Sentry ISO to Hyper-V.

Procedure

1. Log into your Windows server.
2. From a web browser, download the ISO to the VM datastore.

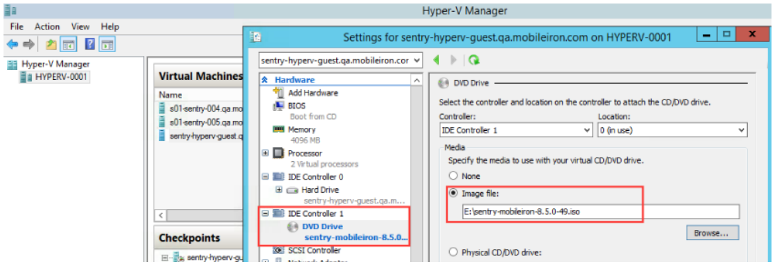
Figure 2. Virtual machine in Hyper-V manager



Name	State	CPU Usage	Assig
s01-sentry-004.qa.mobileiron.com	Running	0 %	4096
s01-sentry-005.qa.mobileiron.com	Running	0 %	2048
sentry-hyperv-guest.qa.mobileiron.com	Running	0 %	4096

3. In the Hyper-V Manager, select the Virtual Machine (VM) and shut it down by right clicking on the VM and clicking **Shutdown**.
4. Right-click on the VM and click on Settings.

Figure 3. Location of the image file



Settings for sentry-hyperv-guest.qa.mobileiron.com on HYPERV-0001

DVD Drive

Select the controller and location on the controller to attach the CD/DVD drive.

Controller: IDE Controller 1

Location: 0 (in use)

Media

Specify the media to use with your virtual CD/DVD drive.

○ None

● Image file:

E:\sentry-mobileiron-8.5.0-49.iso

○ Physical CD/DVD drive:

5. Click on DVD Drive and select **Image file**.
6. Enter the location of the image file you downloaded in "From a web browser, download the ISO to the VM datastore." on the previous page
7. Right-click on the VM and click on **Start** to start the installation.

   See "Using the setup wizard to complete Standalone Sentry installation" below for the next steps.

Using the setup wizard to complete Standalone Sentry installation

When you first boot the Standalone Sentry you automatically open the installation setup wizard. The Welcome screen is shown. Use the information gathered in the worksheet ("Gather Standalone Sentry installation setup information" on page 10) to complete the Standalone Sentry installation steps.

Procedure

TABLE 1. STANDALONE SENTRY INSTALLATION STEPS

Step	Prompt	Enter

1.	`Welcome to Sentry Installation`
	`- For virtual machine installation, type:`
	`vm-install<ENTER>`
	`- For standard physical appliance installation, type:`
	`hw-install<ENTER>`
	`- For standard physical appliance installation from USB, type:`
	`hw-usb-install<ENTER>`
	`- To boot from your local hard disk, type: <ENTER>`
	`Note: System will boot from the local hard disk in 30 seconds if no key is pressed.`
		One of the following installation types:
		• **vm-install**: for installing on a virtual machine.
		• **hw-install**: for installing on standard physical appliances.
		• **hw-usb-install**: for installing on standard physical appliances from a USB.
		The options for physical appliances are applicable only if your deployment uses Core. Cloud does not support the options for physical appliances.

2.		Press **Enter**. The CentOS installation begins and might take several minutes. The Configuration Wizard starts. Use the Configuration Wizard to set the following: • system properties/admin accounts • network settings
System properties and admin accounts setup		

3.	`Welcome to the MobileIron Configuration Wizard`
	`Use the “-“ character to move back to a previous field.`
	`Continue with configuration dialog? (yes/no):`
		yes

4.	`Do you accept the End User License Agreement?:`	**yes** Enter **yes** to accept the End User License Agreement.
5.	`Company name`	A *name* that identifies your organization.

Table 1. Standalone Sentry installation steps (Cont.)

Step	Prompt	Enter
6.	`Contact person name`	The *name* of the responsible person in your organization.
7.	`Contact person email`	The *email addres*s for the responsible person.
8.	`Enter enable secret:`	A *password* for privileged access. The password must be alphanumeric and contain 6-20 characters.
9.	`Enter enable secret (confirm):`	Re-enter the *password* you just set.
10.	`Administrator User Name:`	*User name* for the Sentry administrator.
11.	`Administrator Password`	*Password* for the Sentry administrator.
12.	`Administrator Password (confirm)`	Re-enter the *password* you just set.
Network setup		

13.	`Available network interfaces:`
	`a) GigabitEthernet1`
	`b) GigabitEthernet2`
	`Select the interface that will be used to connect to`
	`the management network:`
		The *letter* for the physical interface you want to use.

14.	`IP address:`	The *IP address* for this system. The IP address will be associated with the physical interface you selected.
15.	`Netmask:`	The *subnet mask* associated with the IP address you just entered.
16.	`Default Gateway:`	The *default gateway address* for this system.
17.	`External Hostname (Fully-Qualified Domain Name):`	The f*ully-qualified domain name* for this system.
18.	`Default domain:`	The *default domain* for this system.
19.	`Name server 1:`	The *IP address* for the primary DNS name server to be used by the appliance.
20.	`Name server 2:`	(Optional) The *IP address* of a secondary name server, or press Enter if you have finished entering name servers.

TABLE 1. STANDALONE SENTRY INSTALLATION STEPS (CONT.)

Step	Prompt	Enter
21.	`Name server 3:`	(Optional) The *IP address* of a tertiary name server, or press **Enter** if you have finished entering name servers.
22.	`Enable remote shell access via SSH (yes/NO):`	**yes** to enable remote access via SSH.
23.	`Configure NTP? (yes/no):`	**yes** to enable an NTP service and specify time sources. Ivanti recommends that you configure at least one time source to ensure proper synchronization of time-based tasks. Enter **no**, if you do not want to set up an NTP server. You will be prompted to set the system clock.
a.	`NTP server 1 hostname or address:`	the *hostname or IP address* of a time source if you entered yes for configuring NTP. If you entered **no** for configuring NTP, you are prompted to set the system clock. • Use HH:MM:SS as the format for the time you enter. • Use DD MM YYYY as the format for the date you enter.
b.	`NTP server 2 hostname or address:`	the hostname or IP address of a secondary NTP server, or press **Enter** if you are finished entering NTP servers.
c.	`NTP server 3 hostname or address:`	the hostname or IP address of a tertiary NTP server, or press **Enter** if you are finished entering NTP servers.

TABLE 1. STANDALONE SENTRY INSTALLATION STEPS (CONT.)

Step	Prompt	Enter
24.	`Commit this config?`	review the output. Enter **yes** to save the changes.
Reload		
25.	`Standalone Sentry command line interface (CLI) command prompt`	reload to complete the installation. Enter **yes** and **yes** again. The installation script continues, displaying status on the console. This may take several minutes. Ignore the following message unless the installation fails to complete: `Unable to connect to MICS service...`

Next steps

- (Optional) If needed, once the installation is complete, install the VMware tools. See "Installing the VMware tools" below.
- Standalone Sentry configuration is done in the UEM platform you have deployed. Depending on whether you have deployed Core or Cloud, you will either add or register Standalone Sentry.

TABLE 2. CONFIGURE STANDALONE SENTRY

UEM	Next Steps
Core	For Core deployments, configure Standalone Sentry in the Core Admin Portal. See "Adding Standalone Sentry in Core" below.
Cloud	For Cloud deployments, register Standalone Sentry. See "Registering Standalone Sentry to Cloud" on the next page.

Installing the VMware tools

The open-vm-tools rpm is now installed by default when Sentry runs on VMware platform and is not required to install the VMware tools manually.

Adding Standalone Sentry in Core

This procedure only applies to Core deployments.

Add Standalone Sentry in Core and then configure the ActiveSync or AppTunnel settings for the Standalone Sentry.

Procedure

1. Log into the Admin Portal.
2. Go to **Services > Sentry** in the Admin Portal.
3. Select **Add New > Standalone Sentry**.
4. Edit the settings to configure Standalone Sentry as necessary.
5. Click **Save > OK**.

Related topics

- For information about how to configure Standalone Sentry for ActiveSync, AppTunnel, and Kerberos Key Distribution Center Proxy (KKDCP), see the Sentry Guide for Core.
- "Accessing the Standalone Sentry System Manager" on the next page.
- "Software updates " on page 22.

Registering Standalone Sentry to Cloud

This procedure only applies to Cloud deployments.

After installing Standalone Sentry, register the Standalone Sentry with Cloud. You register Standalone Sentry from the Standalone Sentry command line interface.

Procedure

1. At the Standalone Sentry command line prompt, enter `enable`.
2. Enter the enable privileged password.
3. Enter `configure terminal`.
4. Enter `registration` <*user*>.
   <*user*> is the username (name@email_server.com) of the Cloud tenant admin.
5. Enter the tenant admin password when prompted.
6. Enter `end`.
7. Enter `show registration status`.
8. Confirm that the registration was successful.
   The output of `show registration status` provides information whether or not the registration was successful.
   Example:
   ```
   sentry# show registration status
   Sentry registration has been completed.
   Registered successfully on Thu Feb 16 02:07:06 UTC 2017
   User name used for registration: admin@sentry.yourcompany.com
   sentry#
   ```

Next steps

Create a profile for Standalone Sentry in Cloud.

Related topics

- For information on how to create a profile for Standalone Sentry and configure Standalone Sentry for ActiveSync and AppTunnel, see the Sentry Guide for Cloud.
  - "Accessing the Standalone Sentry System Manager" below.
  - "Software updates " on the next page.

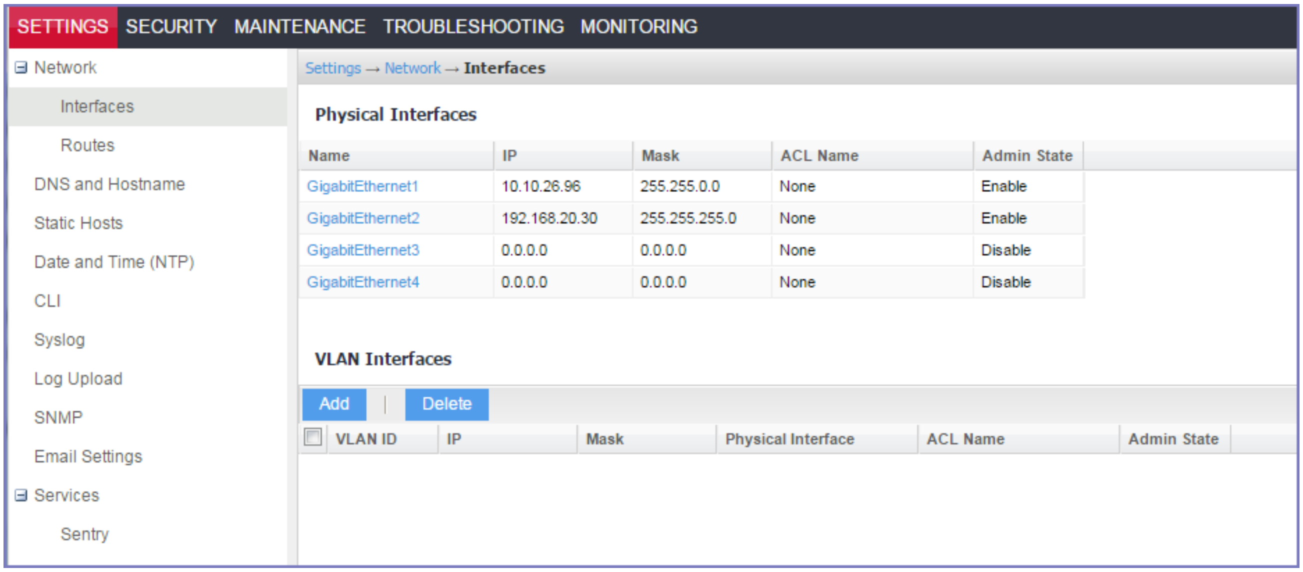
Accessing the Standalone Sentry System Manager

You use the Standalone Sentry System Manager to configure and update the Standalone Sentry network settings such as, host name, network address, interfaces, and routes. You also use the Standalone Sentry System Manager to manage portal certificates and access logs for troubleshooting.

Procedure

1. Open a supported browser.
2. Enter the URL and port number for the Sentry:
   https:<sentry_hostname>:8443/mics
3. Enter the credentials set during installation of the Sentry.
4. Click **LOGIN** to open the Standalone Sentry System Manager home screen.

FIGURE 1. STANDALONE SENTRY SYSTEM MANAGER HOME SCREEN



Physical Interfaces

Name	IP	Mask	ACL Name	Admin State
GigabitEthernet1	10.10.26.96	255.255.0.0	None	Enable
GigabitEthernet2	192.168.20.30	255.255.255.0	None	Enable
GigabitEthernet3	0.0.0.0	0.0.0.0	None	Disable
GigabitEthernet4	0.0.0.0	0.0.0.0	None	Disable

VLAN Interfaces

□	VLAN ID	IP	Mask	Physical Interface	ACL Name	Admin State

Software updates

See the *Standalone Sentry Release and Upgrade Notes*, for the specific release, for information on supported upgraded paths and other upgrade related information specific to that release. The *Standalone Sentry Release and Upgrade Notes* also provides references for upgrade instructions. For the software upgrade procedure, see the *Sentry Guide*.

Standalone Sentry Installation on Amazon Web Services

The following describe how to install Standalone Sentry on Amazon Web Services (AWS):

Before you begin Standalone Sentry installation on Amazon Web Services (AWS)

Before you install Standalone Sentry on Amazon Web Services (AWS), ensure the following:

- You have a UEM deployed.
- You have an AWS account.
- Ports 22 and 443 inbound are open.
- The following minimum memory and CPU requirements are available for Standalone Sentry. The table lists t2.medium type configuration offered by AWS that maps to the Standalone Sentry small configuration size.

TABLE 1. MINIMUM MEMORY AND CPU REQUIREMENTS

Parameters	Medium configuration
Maximum devices	< 8000 devices
Minimum memory	4 GB
Virtual CPUs**	2
Disk	32 GB

- The Standalone Sentry medium configuration size maps to the t2.large type offered by AWS.
- To access the Standalone Sentry System Manager, you have enabled port 8443 or TCP port on AWS security group.

- Site-to-site VPN is enabled between Core and AWS.

Working with RSA Keys for SSH Access

The RSA keys are a pair of public and private keys known as a key pair. You can generate RSA keys or use the existing RSA keys for SSH Access. The following procedure provides steps to create and use the key pairs. If you already have a key pair generated, then skip steps a, b, and c.

> To create new key pair using Amazon EC2, see Creating a Key Pair in http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html.

Procedure

1. Run the following commands in PowerShell to generate the RSA keys.
   a. Generate the private.pem file.
   `#openssl genrsa -des3 -out private.pem 2048`
   b. Change the permission of the private.pem file.
   `#chmod 400 private.pem`
   c. Generate the public.pem file using the private.pem file.
   `#openssl rsa -in private.pem -outform PEM -pubout -out public.pem`
   d. Open the public.pem file and delete the following lines if present and save the file:
   -----BEGIN PUBLIC KEY-----
   -----END PUBLIC KEY-----
2. In AWS, on the left pane, click **Key Pairs** > **Import Key Pair**.
3. Click **Browse** and upload the public.pem file.

Related topics

For more information on key pairs, see http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html.

Overview of tasks for installing Standalone Sentry on AWS

The following provides an overview of the tasks for installing Standalone Sentry on AWS:

1. "Creating an instance of Standalone Sentry on AWS" below.
2. "Setting the initial configuration of Standalone Sentry on AWS" on the next page.
3. "Configuring DNS for Standalone Sentry" on page 26

Creating an instance of Standalone Sentry on AWS

Standalone Sentry is packaged as an Amazon Machine Image (AMI) and is available in multiple AWS regions. It is available on AWS community as a public AMI.

Before you begin

- Verify that you have a valid AWS account.
- Verify that the system and memory requirements are met as mentioned in the "Standalone Sentry Installation on Amazon Web Services" on page 23 section.
- Verify that port 22 is open when the instance is created. SSH is enabled by default in the instance.
- The source IP must be decided by the administrator.

Procedure

1. Log in to **AWS** with admin credentials.
2. On the **AWS services** page, click **EC2** under **Compute**.
3. Expand **Images** and select **AMIs** in the left pane.
4. Select **Public Images** from the drop-down list in the right pane.
5. Search for Sentry using **Sentry-MobileIron** as the keyword. Select the latest version of Sentry from the list and click **Launch**.
6. On **Step 2: Choose Instance Type** page, select **General purpose - t2.medium** as the instance type and click **Next: Configure Instance Details.**
7. On **Step 3: Configure Instance Details** page, retain the default values, and click **Next: Add Storage.** **Note**: Verify that the Auto Assigned Public IP is enabled.
8. On **Step 4: Add Storage** page, retain the default values and click **Next: Add Tags**.
9. On **Step 5: Add tags** page, retain the default values and click **Next: Configure Security Group**.
10. On **Step 6: Configure Security Group** page, select **Select an existing security group** and select **launch-wizard-1**. Click **Review and Launch**.
11. Select the existing key pair for SSH and the acknowledgment. After a successful launch, the launch status is displayed.

Related topics

For more information RSA keys, see "Working with RSA Keys for SSH Access" on the previous page.

Next steps

Go to "Setting the initial configuration of Standalone Sentry on AWS" below.

Setting the initial configuration of Standalone Sentry on AWS

After creating an instance, do the initial configuration of Standalone Sentry on AWS.

Before you begin

- Verify that you have created an instance of Standalone Sentry on AWS. See "Creating an instance of Standalone Sentry on AWS" on the previous page.

Procedure

1. Run the following command from shell on your machine:
   `#ssh -i private.pem aws-user@<hostname>`
2. Use the Configuration Wizard to set up Standalone Sentry.
3. Enter **reload** to complete the installation.
   Ignore the Hostname warning.

Related topics

For a description of the configuration wizard prompts and actions, see "Standalone Sentry configuration wizard prompts and options" on the next page.

Next steps

Standalone Sentry configuration is done in the UEM platform you have deployed. Depending on whether you have deployed Core or Cloud, you will either add or register Standalone Sentry.

IMPORTANT: Secure the communication from your UEM to Standalone Sentry through an IPSec tunnel.

TABLE 1. NEXT STEPS

UEM	Next Steps
Core	For Core deployments, you must configure Standalone Sentry in the Core Admin Portal. See "Adding Standalone Sentry in Core" on page 19.
Cloud	For Cloud deployments, you must register Standalone Sentry. See "Registering Standalone Sentry to Cloud" on page 20.

Configuring DNS for Standalone Sentry

Configure DNS so that the Standalone Sentry instance on AWS uses DNS on the other side of the AWS tunnel by default. Configuring the DNS for Standalone Sentry is optional. You may need to configure the DNS for Standalone Sentry in some cases, such as, the backend resources that Standalone Sentry connect to are on premise.

Procedure

1. In the AWS VPC console, go to **DHCP Options Sets**.
2. Create a new DHCP Options Set.
   - Add the internal domain name for Standalone Sentry.
   - Add the on-premise DNS server address.

   The Standalone Sentry AWS instance in the VPC now defaults to using the DNS on the other side of the AWS tunnel by default.

Related topics

For more information, see the AWS documentation at Changing the Set of DHCP Options a VPC Uses.

Standalone Sentry configuration wizard prompts and options

The following table provides sequence of prompts and actions in the configuration wizard for Standalone Sentry.

TABLE 1. CONFIGURATION WIZARD PROMPTS AND ACTIONS

Prompt	Enter
System properties, Admin accounts setup	

`Welcome to the MobileIron Configuration Wizard`
`Use the “-“ character to move back to a previous field.`
`Continue with configuration dialog? (yes/no):`
	yes

`Do you accept the End User License Agreement?:`	yes Enter yes to accept the End User License Agreement.
`Company name`	A name that identifies your organization.
`Contact person name`	The name of the responsible person in your organization.
`Contact person email`	The email address for the responsible person.
`Enter enable secret:`	A password for privileged access. The password must be alphanumeric and contain 6-20 characters.
`Enter enable secret (confirm):`	Re-enter the password you just set.
`Administrator User Name:`	User name for the Sentry administrator.
`Administrator Password`	Password for the Sentry administrator.
`Administrator Password (confirm)`	Re-enter the password.
Network setup ⓘ DHCP and SSH are enabled by default. SSH can be disabled after doing the initial setup.	
`Hostname`	A valid FQDN. ⓘ Ivanti recommends that you use the Public DNS name provided by AWS.

TABLE 1. CONFIGURATION WIZARD PROMPTS AND ACTIONS (CONT.)

Prompt	Enter
`Configure NTP? (yes/no):`	yes Enter yes to specify the time source. If you decide not to set up NTP access, then you will be prompted to set the system clock.
`NTP server 1 hostname or address:`	The hostname or IP address of the NTP server. The NTP server address should be a public IP address reachable by Standalone Sentry. Example: time.apple.com
`NTP server 2 hostname or address:`	The hostname or IP address of another time source, or press **Enter** if you have finished entering time sources. The NTP server address should be a public IP address reachable by Standalone Sentry. Example: time.apple.com
`NTP server 3 hostname or address:`	The hostname or IP address of another NTP server, or press **Enter** if you have finished entering time sources. The NTP server address should be a public IP address reachable by Standalone Sentry. Example: time.apple.com
`Commit this config?`	yes

Standalone Sentry installation on Microsoft Azure

The following describe how to install Standalone Sentry on Microsoft Azure:

Before you begin Standalone Sentry installation on Microsoft Azure

Before you install Standalone Sentry on Microsoft Azure, ensure the following:

- You have a UEM deployed.
- Port 443 inbound is open.
- You have a Microsoft Azure account.
- You have made a note of the VHD location. You will need this when you are "Installing Standalone Sentry on Microsoft Azure" on page 31.

VHD-Location: See the *Standalone Sentry Release and Upgrade Notes* for your release.

- You have downloaded the following json files:

- the parameter file, which includes information such as the initial azure user, vhd to be used, the storage account. You will update this file during installation.
- the deployment file with default values required for installation, such as the inbound and outbound rules to allow or disallow incoming and outgoing IP addresses. Do not make any changes to this file.

See the *Standalone Sentry Release and Upgrade Notes* for the location of these files.

- The installation instructions provided use the Microsoft Azure Cloud Shell bash CLI 2.7 and *azcopy* commands. If you are using a Mac or PC, the Microsoft Azure command line plugin is downloaded and installed to your Mac or Linux machine.
- Execute the following Azure CLI commands :

-
  ```
  az login -u <username@domain.com> -p <password>
  ```

-
  ```
  az group create -n "groupname" -l <location>
  ```

-
  ```
  az storage account create --resource-group <groupname>  --location
  <location>  --sku Standard_LRS --kind Storage --name <storagename>
  ```

-
  ```
  az storage container create -n copiedvhds --account-name <storagename>
  ```

-
  ```
  az storage account keys list -g <groupname> -n <storagename>
  ```

-
  ```
  az copy --blob-type page --source <Sentry VHD File Source Location>  --
  destination <https://storagename.blob.core.windows.net/copiedvhds/sentry-
  mobileiron.vhd> --dest-key <account keys from previous command>
  ```

-
  ```
  az deployment group create --resource-group <groupname>  --template-file
  <path-to-template>  --parameters <path-to-parameter>
  ```

Note The Following:

- "location" - It is the Azure location where the group is created.
- The "Sentry VHD File Source Location" is available in the *Standalone Sentry Release and Upgrade Notes*.
- If you are using an installer, an understanding of creating a VM on Microsoft Azure. You will be creating a VM for Standalone Sentry in Microsoft Azure using the Azure Resource Manager deployment model using CLI only.

For Microsoft Azure command line interface (CLI) commands, see https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-command-line-tools/

- Minimum memory and CPU requirements for Standalone Sentry:

TABLE 1. MINIMUM MEMORY AND CPU REQUIREMENTS

Item	**Requirement**
Configuration size	Medium configuration
Maximum devices	< 8000 devices
Memory	6 GB
Virtual CPUs**	2
Memory reservations	6 GB
Disk	32 GB

The Standalone Sentry medium configuration size maps to Standard_D2_v2 VM type offered by Microsoft Azure.

- Site-to-site VPN is enabled between Core and Microsoft Azure.

Overview of tasks for installing Standalone Sentry on Microsoft Azure

Installing Standalone Sentry on Microsoft Azures requires the following:

1. "Installing Standalone Sentry on Microsoft Azure" below
2. "Setting the initial configuration of Standalone Sentry installed on Microsoft Azure" on the next page

Installing Standalone Sentry on Microsoft Azure

> The following instructions are specific to an installation using Microsoft Azure Cloud Shell bash commands. If you are working from a Mac, Linux, or Windows machine see the Microsoft Azure documentation for creating a VM Instance from a VHD using Azure CLI.

IMPORTANT: The .vhd filenames are examples. For the correct .vhd filename for this release, see the Standalone Sentry release notes for this release.

Before you begin

1. See "Before you begin Standalone Sentry installation on Microsoft Azure" on page 29.
2. Modify the json parameter file:
   a. Change the value of "adminPassword".
   b. Change the value of "storageAccountName". You will use this value in the installation steps.
      Example: daredevil78
   c. Change the value of "vhdName". You will use this value in the installation steps.
      Example: sentryblobV920.vhd
3. For installation using Cloud Shell, upload the template file and parameters file as described in: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-template-deploy-cli#deploy-template-from-cloud-shell

Procedure

	Task	Enter Azure CLI command
1.	Login	az login -u <username@domain.com> -p <password>
2.	Create resource group	az group create -n "groupname" -l <location> Example: `az group create -n "daredevil" -l "westus"`
3.	Create storage account	az storage account create --resource-group <groupname> --location <location> --sku Standard_LRS --kind Storage --name <storagename>

	Task	Enter Azure CLI command
		Example: `az storage account create --resource-group daredevil --location "westus" --sku Standard_LRS --kind Storage --name daredevil78`
4.	Create container inside storage account	az storage container create -n copiedvhds --account-name <storagename> Example: `az storage container create –n copiedvhds --account-name daredevil78`
5.	List the storage account keys	az storage account keys list -g <groupname> -n <storagename> Example: `az storage account keys list -g daredevil -n daredevil78`
6.	Copy vhd to	az copy --blob -type page --source <Sentry VHD File Source Location> --destination <https://storagename.blob.core.windows.net/copiedvhds/sentry-mobileiron.vhd> --dest-key <account keys from previous command>
7.	Installing the vhd	az deployment group create --resource-group <groupname> --template-file <path-to-template> --parameters <path-to-parameter> Example `az deployment group create --resource-group daredevil --template-file <clouddrive/templates/singleInstanceVMv2_d.json> --parameters <clouddrive/templates/singleInstanceVM.parametersV2d.json>`

Next steps

Go to "Setting the initial configuration of Standalone Sentry installed on Microsoft Azure" below.

Setting the initial configuration of Standalone Sentry installed on Microsoft Azure

You do the initial configuration of Standalone Sentry in the configuration wizard, which is presented after the VM instance for Standalone Sentry is created and running. You configure system properties, administrator accounts, and network settings during initial installation.

Procedure

1. SSH to the Standalone Sentry FQDN.
   The FQDN for Standalone Sentry is *resource_group_name*_sentry_*location*_cloudapp.azure.com.
   Example of the Standalone Sentry FQDN: daredevilsentry.westus.cloudapp.azure.com

TIP: To check the DNS value given by Microsoft Azure, login to the Microsoft Azure portal, go to the resource group and click on the Sentry VM.

2. For username, enter **azureuser**.
   For the first ssh access to Standalone Sentry, you must use **azureuser** for the username. For subsequent ssh access use the username you created in “Create the VM image and VM instance.”
3. For password, enter the value of the adminPassword you created when you installed Standalone Sentry on Microsoft Azure.
   The Configuration Wizard starts.
4. Use the Configuration Wizard to set up Standalone Sentry.
5. Enter **reload** to complete the installation.
   Ignore the Hostname warning. Microsoft Azure sets the hostname. Proceed with the reload and save the configuration.

Related topics

- The value of the adminPassword was created in "Installing Standalone Sentry on Microsoft Azure" on page 31.
- For a description of the configuration wizard prompts and actions, see "Standalone Sentry configuration wizard prompts and options" below.

Next steps

Standalone Sentry configuration is done in the UEM platform you have deployed. Depending on whether you have deployed Core or Cloud, you will either add or register Standalone Sentry.

IMPORTANT: Secure the communication from your UEM to Standalone Sentry through an IPSec tunnel.

TABLE 1. NEXT STEPS

UEM	Next Steps
Core	For Core deployments, configure Standalone Sentry in the Core Admin Portal. See "Adding Standalone Sentry in Core" on page 19.
Cloud	For Cloud deployments, register Standalone Sentry to Cloud. See "Registering Standalone Sentry to Cloud" on page 20

Standalone Sentry configuration wizard prompts and options

The following table provides sequence of prompts and actions in the configuration wizard for Standalone Sentry.

Table 1. Configuration wizard prompts and actions

Prompt	Enter
System properties, Admin accounts setup	
Welcome to the MobileIron Configuration Wizard Use the “-“ character to move back to a previous field. Continue with configuration dialog? (yes/no):	yes
Do you accept the End User License Agreement?:	yes Enter yes to accept the End User License Agreement.
Company name	A name that identifies your organization.
Contact person name	The name of the responsible person in your organization.
Contact person email	The email address for the responsible person.
Enter enable secret:	A password for privileged access. The password must be alphanumeric and contain 6-20 characters.
Enter enable secret (confirm):	Re-enter the password you just set.
Administrator User Name:	User name for the Sentry administrator.
Administrator Password	Password for the Sentry administrator.
Administrator Password (confirm)	Re-enter the password.
Network setup ℹ DHCP and SSH are enabled by default. SSH can be disabled after doing the initial setup. You can disable SSH for Standalone Sentry in Cloud.	
Configure NTP? (yes/no):	yes Enter yes to specify the time source. If you decide not to set up NTP access, then you will be prompted to set the system clock.
NTP server 1 hostname or address:	The hostname or IP address of the NTP server. The NTP server address should be a public IP address reachable by Standalone Sentry.

TABLE 1. CONFIGURATION WIZARD PROMPTS AND ACTIONS (CONT.)

Prompt	Enter
	Example: time.apple.com
`NTP server 2 hostname or address:`	The hostname or IP address of another time source, or press **Enter** if you are finished entering time sources. The NTP server address should be a public IP address reachable by Standalone Sentry. Example: time.apple.com
`NTP server 3 hostname or address:`	The hostname or IP address of another NTP server, or press **Enter** if you are finished entering time sources. The NTP server address should be a public IP address reachable by Standalone Sentry. Example: time.apple.com
`Commit this config?`	yes