CLOUD MANAGEMENT SUITE

COMMUNICATION

Requirements & Prerequisites

Please ensure that all prerequisites have been met before using Cloud Management Suite.

DISCOVERY & INVENTORY

1. Install a vRep
2. Add administrator account(s)
3. The vRep will need to be able to connect to devices over TCP ports 135 and 445 (Administrative /C$ Shares). These are the typical Windows SMB ports used for remote administration. If you use the Windows Firewall, you can enable File and Printer Sharing to open these ports. For Workgroup devices, please enable Remote Connections or simply install the MicroAgent software (easier method).

OPERATING SYSTEMS

WINDOWS DEVICES

Windows devices support all features of Cloud Management Suite. Devices below are supported for vRep, MicroAgent, standard discovery, and agentless installations.

- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Wndows Server 2019

OS Requirements for Windows Devices

- .Net Framework 2.0
- .Net Framework 4.0 Full Version (not Client Profile)

LINUX DEVICES

Linux devices support discovery, inventory, and patching with Cloud Management Suite. Devices below are supported over SSH from vRep client (requires at least 1 Windows device for vRep).

- CentOS 5
- CentOS 6
- CentOS 7
- Oracle Enterprise Linux 5
- Oracle Enterprise Linux 6
- Oracle Enterprise Linux 7
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- SUSE Enterprise 11
- SUSE Enterprise 12
- Ubuntu 12
- Ubuntu 14
- Ubuntu 16
- Ubuntu 18

MAC DEVICES

Mac devices support discovery, inventory, patching, and remote control with Cloud Management Suite. Devices below are supported for Mac Agent installations and over SSH (with Remote Management enabled).

- OS X 10.11
- OS X 10.12
- OS X 10.13
- OS X 10.14

WHITELISTED LOCATIONS

The following locations must be whitelisted by the firewall (or refer to vRep Relay functionality):

LOCATION	REASON
***.cloudmanagementsuite.com**	To ensure devices can reach cloud console and for console email notifications
***.verismic.com**	Console email notifications and support emails
verismic.blob.core.windows.net	Clustered content repository within Microsoft Azure

EXCEPTIONS THIRD-PARTY ENDPOINT MANAGEMENT

Before any installation occurs, please ensure that all existing solutions have exceptions for Cloud Management Suite communication.

The following directories must be excluded from any endpoint protection software:

DIRECTORY LOCATION	REASON
C:\$VCMSTEMP$	Standard installation directory for vRep and MicroAgent
C:\Program Files (x86)\Verismic	Standard installation directory for vRep
C:\Windows\System32\config\systemprofile \Appdata\Roaming\Verismic CMS	Standard installation directory for vRep and MicroAgent certificates and task logs

NETWORK PORT REQUIREMENTS

Standard ports to open:

PORT	DIRECTION	RECOMMENDATION	REASON
TCP Port 443 (HTTPS)	Internal/External	**Required**	All communication to the cloud console
TCP Port 135	Internal	Recommended; **Required for Discovery**	Discovery: vRep to Windows devices
TCP Port 445	Internal	Recommended; **Required for Discovery**	Discovery: vRep to Windows devices
TCP Port 22	Internal	Optional; **Required for Discovery and Linux/Mac**	Discovery: vRep to Linux/Mac devices

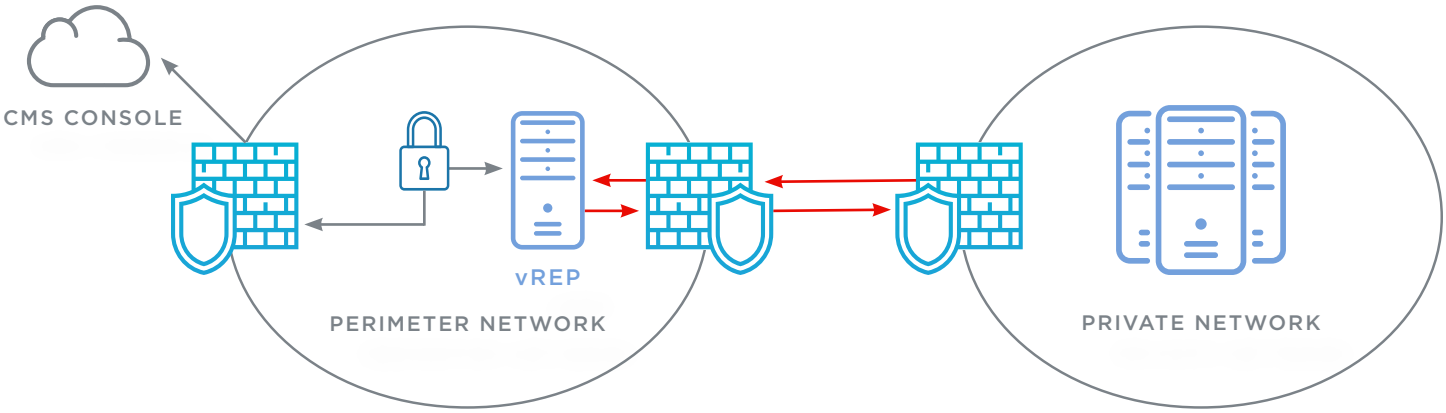
Custom service ports to open internally:

PORT	DIRECTION	RECOMMENDATION	REASON
TCP Port 51339	Internal	Recommended	Remote Control
TCP Port 51340	Internal	Recommended	Remote Control
TCP Port 51341	Internal	Recommended	CMS Management
TCP Port 51342	Internal	**Required**	vRep to Managed Device
TCP Port 51343	Internal	Recommended	Software Deployment
TCP/UDP Port 51344	Internal	Recommended	Software Deployment
TCP/UDP Port 51345	Internal	Recommended; **Required for vRep Relay**	vRep Relay Functionality

VREP PROXY RELAY CONFIGURATION (IF REQUIRED)

For private network devices without Internet access, Cloud Management Suite can manage these devices using our vRep. The vRep acts as a centralized proxy and discovery agent, relaying data to/from the private network to the perimeter and back to the cloud services.

Sample environment diagram:



HOW TO IMPLEMENT

1. Install a vRep in the perimeter (or subnet where it will have Internet access)
2. In the Cloud Management Suite console, create a Site to represent the private network/subnet
3. Assign the intended vRep device to the site (right-click the Site and choose Config > vReps)
4. Before leaving the Site Config, place all required IP Address Ranges in the IP Address Ranges section
5. Run a Discovery Task on the new Site and all ranges applicable. During the Discovery Task Wizard, administrative/service account details will be required.
6. Repeat the process for each private network

During the discovery process, the vRep will automatically assign itself as the proxy to manage these devices. These devices will send traffic through the vRep, so that Internet access is not required on the private network.

ABOUT US

Cloud Management Suite allows you to get the complete picture of your entire IT environment from the cloud. Automatically discover network devices, remotely deploy software applications and automate patch management. A single web-based console allows access to any device from anywhere.

Headquartered in Aliso Viejo, California, Cloud Management Suite is a growing and dynamic organization with offices in four countries and 12 partners in nine countries. For more information about Cloud Management Suite and how we've revolutionized IT systems management, visit **www.cloudmanagementsuite.com**.

CALL
US: +1 (949) 270-1903
UK: +44 (0) 1256-806567

CONNECT
www.cloudmanagementsuite.com
info@cloudmanagementsuite.com