Data Collection

Customer Data Collection Spreadsheet

Pre-populating the Customer Data Collection workbook before adding a new customer will assist you with the onboarding process.

Right click the link below to download the workbook.

Customer Data Collection.xlsx

The following items in this section will guide you on what is required within each sheet of the workbook.

Customer Details

The following information is required to add a customer into the web portal.

Item	Setting
Display name	
Customer Service Desk Email	
Partner Account Number	
Partner Customer Number	
Partner Service Desk Email	
Billing address Country	
Billing address Time Zone	
Billing address Address 1	
Billing address Address 2	
Billing address City/Suburb	
Billing address Zip Code/Post Code	
Shipping address same as Billing Address	Yes or No (If 'No' complete the next 6 lines)
Shipping address Country	
Shipping address Time Zone	
Shipping address Line 1	
Shipping address Line 2	
Shipping address City/Suburb	
Shipping address Zip Code/Post Code	

Customer Security Policies

A number of security policies can be enforced within VSM and are administered at the time of creating the customer in the portal.

Policy	Value
Enable Password Aging	Yes or No (If 'Yes' complete the next line)
Maximum Password Age (Days)	
Enable Password History	Yes or No (If 'Yes' complete the next line)
Number of Unique Password Before Re-use	
Enable Idle Timeout	Yes or No (If 'Yes' complete the next line)
Number of Minutes Before Timeout	
Suspend Account on Inactivity	Yes or No (If 'Yes' complete the next line)
Number of Days Before Suspension	
Role (Used for Role Based Access)	

Customer Features

The following features are available within VSM.

Assignment of these features in the web portal creates a billing contract and the Business Partner will begin to be invoiced for the service by Virsae in accordance with the financial relationship.

Each VSM feature is priced separately. See your Virsae Account Manager for more details.

ITIL Feature	Subscribed
API	Yes
Service Desk	Yes
Availability Manager	Yes or No
Capacity Manager	Yes or No
Configuration Manager	Yes or No
Continuity Manager	Yes or No
Release Manager	Yes or No
Change Manager	Yes or No
Security Manager	Yes or No

API and Service Desk are automatically subscribed to, as part of the VSM service

IP Network and Firewall Settings (Legacy Hardware Appliance Only)

The Legacy Hardware Appliance is comprised of a Virtual Machine host and a Virtual Machine, therefore it requires two IP addresses to be administered.

Capture the IP Addresses and additional network details required.

VSM Appliance Network Settings	
Item	**Setting**
TCP Port 443 to Virsae cloud computing service	Yes or No
Proxy in use	Yes or No (If 'Yes' complete next 4 lines)
Proxy IP address	
Proxy Port	
Proxy Username	
Proxy Password	
DHCP	Yes or No (If 'No' complete next 4 lines)
IP Address (V4)	
Subnet Mask	
Default Gateway	
Primary DNS	

VSM Probe Network Settings	
Item	**Setting**
TCP Port 443 enabled outbound to Azure	Yes or No
DHCP	Yes or No (If 'No' complete next 4 lines)
IP Address (V4)	
Subnet Mask	
Default Gateway	
Primary DNS	

Only the Legacy Hardware Appliance requires two IP addresses (**the table above applies only to the Legacy Hardware Appliance**).

The Windows Software Client, Linux Virtual Machines and Raspberry Pi only require one IP Address.

IP addresses are recommended to be static or reserved via DHCP

UC Platform Settings

VSM requires access to various interfaces on UC Application Servers to enable the collection of data.

In is most basic form these are normally an SSH Connection on TCP Port 22 and SNMP Traps and SNMP Access on UDP Ports 161/162, however on some applications VSM uses other specific interfaces to collect data such as SFTP

With this in mind it is wise to capture (or have available) at minimum the following information for each UC Application you wish to monitor with VSM:

Item	Description
Name	The name you wish to be displayed in VSM for this server
IP Address	The IP Address of the administrative interface for this server, this will be used for SSH connections
Username	The name of the user account you wish VSM to access this server with, bear in mind this may need elevated permissions
Password	The password for the user account you with VSM to use.
SNMP Trap details	The Version of SNMP (1,2,3c) you wish the Application to use when sending SNMP Traps to VSM. E.g. the Username and Community string and any Authentication/Privacy protocols and passwords required.
SNMP Access details	The Version of SNMP (1,2,3c) you wish VSM to use when querying information from the Application. e.g. the Username and Community string and any Authentication/Privacy protocols and passwords required.

Each of the specific interfaces and steps to configure them are found within the guides below.

- AudioCodes

- Avaya
- Cisco Systems
- Generic Devices
- Genesys
- Linux Server
- Microsoft
- Ribbon
- VMware
- VSM Everywhere

Equipment can also be bulk imported into VSM by using the template below:

Equipment Import Template