NETCRAFT COMMUNICATIONS INC.

Versiera 3.2

Versiera User Guide

Versiera User Guide

© NetCraft Communications Inc.
312 Dolomite Drive • Suite 212
Toronto • ON • M3J 2N2
Phone 416-736-7474

Prepared by:
NetCraft Communications Inc.

Table of Contents

Introduction **4**

Features Overview **5**

Technical Support **7**

Getting Started **8**

VERSIERA ID 8
CONFIGURE VERSIERA MANAGEMENT CONSOLE 9
VERSIERA AGENT 11
AGENT INSTALLATION – WINDOWS 14
AGENT INSTALLATION - UNIX 16
AGENT INSTALLATION - PFSENSE FIREWALL 17
AGENT INSTALLATION – DD-WRT 19
AGENT INSTALLATION – OPENWRT 21

Versiera Management Console **23**

HOSTS 26
HOST GROUPS 28
SCHEDULES 31
JOBS 36
MONITORING 64
TICKETING 75
COMPLIANCE 81
DOCUMENTS 86
DASHBOARDS 90
SERVICE PROBES 93
STATE 102
NETWORK MAPS 124

Administration **126**

CONTACTS 127
ACCOUNTS 128
REGISTRATION USERS 130
TIME ZONE 131
SUBSCRIPTIONS 132
NOTIFICATION LOG 133
ACTIVITY LOG 134

Tips and Tricks **135**

HOW TO FORCE THE IP ADDRESS THAT THE VERSIERA AGENT LISTENS ON 135
AUTOMATE VERSIERA AGENT WINDOWS INSTALLATION 135
UNINSTALLING VERSIERA AGENTS 136
OS X *136*
Linux *136*
FreeBSD/NetBSD/OpenBSD *136*
Solaris *136*
Windows *137*

OpenWRT *137*
DD-WRT *137*

Introduction

Versiera is a web-based technology infrastructure management system used to visualize and operate large-scale computer networks. It also simplifies the common routine tasks performed by system administrators and enables a comprehensive view into the technology and its operation. Versiera offers a real-time view of all of your hardware, software and digital assets along with their operational health. Versiera is available as enterprise appliance or complete architectures for management of cloud data centers. Organizations looking to consolidate management platforms or those that need to incorporate the latest in management technologies, as well as, cut operational costs can take advantage of the free Internet accessible Versiera management service.

Versiera architecture enables Internet Service Providers, systems management organizations and consultants to broaden their services without having director access to customer technology or data and is accomplished without having to build dedicated management interconnects to end customers.

The Versiera Management Console (https://www.versiera.com/) is accessible using most popular web browsers over the Internet. Versiera collects and analyses information from your computer infrastructure describing the computer active and configuration states by means of resident host agents (agents are about 800KB) that push information to the central Versiera system over an authenticated and encrypted connection (SSL). During installation/registration every Versiera remote host agent is assigned a unique digital certificate to authenticate and encrypt all communications. Once the digital certificates have been assigned they are automatically managed by Versiera management system.

Broad operating system and platform support is offered including agents for Microsoft Windows*, Apple OS X (Intel/PowerPC), Linux (x86/amd64), FreeBSD (x86/amd64), NetBSD (x86), OpenBSD (x86) and Solaris (Sparc/x86). Embedded platform support includes DD-WRT (Broadcom/Atheros), and OpenWRT (Broadcom/Atheros). *

*
All Windows operating systems (except Win95, 98, and ME) are supported. Linux systems supported include but are not limited to: RedHat, Fedora, CentOS, Debian, Gentoo, Ubuntu, Mandriva, SuSE, Slackware, Xandros, PCLinus. Solaris 8 and higher supported.

Features Overview

Monitoring

- Monitoring host performance metrics
- Monitored host metrics include
  - CPU load average
  - Physical memory used and available
  - Virtual memory usage
  - Disk space available
  - Process name
  - Process count
  - Network port connections
  - Host uptime
  - Host time synchronization
  - Host check-in status
- Configurable monitoring thresholds
- Notification e-mails alerts
- Alert suppression through host maintenance status
- Monitoring event subscriptions
- Alert Queue for automating trouble tickets to address monitoring issues

Service Probes

- Service Probes are used for monitoring of enterprise or Internet services and digital assets
- Service Probes include
  - DNS – domain name service record monitoring
  - HTTP – website and URL monitoring
  - HTTPS – website and URL monitoring
  - SMTP – e-mail server monitoring
  - PING – host response monitoring
  - SSL – monitoring of digital certificates
  - DHCP – network address assignment monitoring
- Notification e-mail alerts for service probe monitoring

Network Maps

- Automatically visualize the corporate networks and all their nodes
- Automatically visualize the communications throughout the enterprise networks and to/from the Internet

Scheduling

- Versiera has its own general scheduling system which is used for all Versiera components including Monitoring, Jobs, Notifications and Service

Jobs

- Facility to create script tasks or use of built-in task models that can be assigned to one or more registered hosts for execution by remote agents
- Job types include:
    - User Management (Add/Delete/Disable/Change Password)
    - Process Management (Start/Kill)
    - Service/Daemon Control (Start/Stop/Restart)
    - Software Distribution
    - Software Removal
    - Host Shutdown/Reboot/User Logoff
- Job Chaining enables the execution of one job based on the successful completion of another
- Software Distribution is a built-in task model and includes support for distribution of pre-packaged software as executables, Microsoft System Installer (MSI), Install Shield, and Red Hat Package Manager (RPM), Debian Package Manager (DPKG) and FreeBSD Package Management (PKG) file formats
- Facility to assign a host a task of awakening, restarting, shutting down other hosts or forcing user logoff (Windows only)

Compliance

- Create and manage corporate host configuration standards using Versiera Management Console
- Apply corporate compliance standards for host active and configured states
- Report on host compliance deviations relative to configured corporate standards

Automated Documentation

- Infrastructure - ability to generate on demand formal documentation describing one or more hosts including their configuration details
- Monitoring Policy - ability to generate on demand formal documentation describing the configured monitoring policies applied to registered hosts
- Documentation may be generated as Rich Text Format (RTF) or Portable Document Format (PDF)
- Reports for host data in Versiera are available as Comma Separated Values (CSV) and Portable Document Format (PDF)

Report Host State

- Report host network listening ports, associated running applications and respective application user accounts – Application Dependency Mapping (ADM)
- Report on active host communications with remote hosts
- Report on running applications, their resource usage and associated user accounts
- Report on host user accounts details, user groups and group memberships
- Report on accuracy and functionality of time synchronizations across registered hosts and respective host time zones.
- Report on host network configuration including network interface name, speed duplex settings, MAC, manufacturer and packet counters
- Report on host operating system, hardware make, model and serial number, processor model, memory size, capacity of data storage devices, firmware version and date.

- Report on active user session across all managed hosts

Ticketing System

- Automated trouble ticket queue generated by Monitoring probes
- Ability to create trouble tickets, assign priority, and associate to hosts for documenting problem resolution workflow and delegation of work to operators

Contact Management System

- General contact management facility used for sending alert notifications

Dashboard

- A set of visual tools "gadgets" for displaying summary data
- Tools include: Host Performance, Bird's Eye View, Network List, Ticket Stats and Alert Stats

Historical Host State Tracking

- Ability to review host state changes over time

Audit

- Versiera generates an audit log of user administrative activity during Versiera use

Filters

- Filters provide the ability to reduce the quantity of presented host data to locate desired information
- Dynamic suggestions are available for locating the desired information

Custom Tables Presentation

- Versiera data presented in table format may be sorted by clicking on the respective column heading. Alternate clicks sort data based on ascending and descending values.
- Table columns may be rearranged by clicking and dragging the desired table column to the required location in the table.

Technical Support

Technical support is available via web based **forums** (http://forums.versiera.com/). To login, use your Versiera ID and password. In addition, technical support may be obtained by sending **Email** to support@versiera.com**.**

Getting Started

There are three (3) steps in getting started with Versiera:

1. Create your Versiera ID
2. Configure Versiera Management Console settings.
3. Download and install Versiera agents on managed hosts.

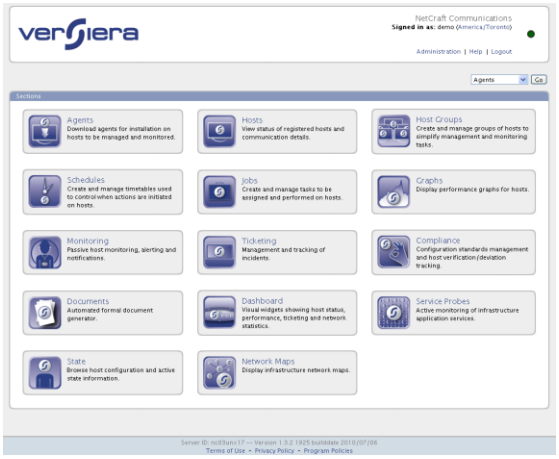
Versiera ID

Now that you've read a bit about what Versiera can be used for, let's get started using it! To use Versiera you will need to create your Versiera ID and password. To create a Versiera ID navigate your Internet browser to https://www.versiera.com and clicking on "**Create a Versiera ID**" link (as in the image below). This link will take you to a registration page, where you can create your Versiera ID. Once the Versiera ID has been successfully created, a confirmation email will be sent from Versiera to the email address you provide in the registration process, containing an embedded activation link for the new Versiera ID. Your Versiera ID will only become usable once you have clicked on the URL link contained in the email. .

Should you ever need to change your Versiera ID password, you may do so after signing into Versiera and using the **Administration** link (top right of page) and then the **Account** Section.

Configure Versiera Management Console

Once you have created your Versiera ID, you can sign into Versiera Management Console. The Versiera Management Console will be mostly empty until Versiera agents have been installed and registered on your managed hosts. Once the agents are installed, they will enable management capabilities for that host.



Before installing Versiera agents, it is recommended to first configure the following items to your requirements in the Administration Section:

Time Zone – follow the *Administration* link (top right) and select the *Time Zone* Section. Select your desired time zone to configure all time/date information to be displayed for your selected time zone.

Contacts - follow the *Administration* link (top right) and select the *Contacts* Section. In the *Contacts* Section you can add email address contact information for those individuals and groups that should receive automated alert notifications from Versiera for Monitoring, Service Probes, Jobs and Ticketing.

Accounts - follow the *Administration* link (top right) and select the *Accounts* Section. In the *Accounts* Section you can add additional Versiera IDs for other staff members that will be using the Versiera Management Console to manage the same hosts.

Registration Users - follow the *Administration* link (top right) and select the *Registration Users* Section. In the Registration Users Section you can create a restricted Versiera ID that can only install and register Versiera agents, but without access to the Versiera Management Console.

Activity Log - follow the *Administration* link (top right) and select the *Activity Log* Section. The *Activity Log* provides an audit trail of Versiera Management Console usage and should be reviewed regularly.

Versiera Agent

Once you have activated your Versiera ID, to make full use of Versiera you will need to sign-in to Versiera (Versiera ID and password), **download** and **install** a Versiera agent on one or more computer hosts you wish to manage using Versiera. At least one agent is necessary to populate Versiera with host information.

Standard Versiera Agents

Agents

Platform	Version	Build	
Mac OS X 10.4, 10.5 (x86/ppc)	1.3.2	1925	Download
FreeBSD 7 (amd64)	1.3.2	1925	Download
FreeBSD 8 (amd64)	1.3.2	1925	Download
FreeBSD 4 (x86)	1.3.2	1925	Download
FreeBSD 5 (x86)	1.3.2	1925	Download
FreeBSD 6 (x86)	1.3.2	1925	Download
FreeBSD 7 (x86)	1.3.2	1925	Download
FreeBSD 8 (x86)	1.3.2	1925	Download
Linux, glibc 2.2 or later (x86)	1.3.2	1925	Download
Linux, glibc 2.3 or later (x86_64)	1.3.2	1925	Download
NetBSD 5 (amd64)	1.3.2	1925	Download
NetBSD 3 (x86)	1.3.2	1925	Download
NetBSD 4 (x86)	1.3.2	1925	Download
NetBSD 5 (x86)	1.3.2	1925	Download
OpenBSD 4.5 (amd64)	1.3.2	1925	Download
OpenBSD 4.2 (x86)	1.3.2	1925	Download
OpenBSD 4.3 (x86)	1.3.2	1925	Download
OpenBSD 4.4 (x86)	1.3.2	1925	Download
OpenBSD 4.5 (x86)	1.3.2	1925	Download
Solaris 8, 9, or 10 (sparc)	1.3.2	1925	Download
Solaris 10 (x86)	1.3.2	1925	Download
Windows 2000 or later (x86)	1.3.2	1925	Download

Embedded Versiera Agents

Embedded Agents

Platform	Version	Build	
DD-WRT Linux 2.4 (brcm47xx)	1.3.2	1925	Download
DD-WRT Linux 2.6 (brcm47xx)	1.3.2	1925	Download
OpenWRT 8.09 (atheros)	1.3.2	1925	Download
OpenWRT 8.09 (brcm47xx)	1.3.2	1925	Download

There are two steps in installing an agent on a host; installing the agent and registering the agent with Versiera which will assign the Versiera agent with a digital certificate and map it to your Versiera account.

Versiera agents collect host information and send it encrypted to the central system inside secure socket layer tunnel (SSL). Versiera agents have, an AINA assigned, listening port 9050/tcp (listening port can be forced to listen on loopback interface only). The listening port is intended for on-demand agent requests from the Versiera Management Console in an Enterprise environment (initiated by the Versiera ID account holder).

Versiera agents operate on internal timers and communicate with the central system at regular intervals. The following are the default timers (the values may change in future releases).

Heart-beat check-in:	*1 minute interval*
Performance host data:	*5 minute interval*
Complete host state data:	*6 hour interval*

Further, agents detect host time changes such as those for time synchronization and adjust their timers accordingly.

Agent Installation – Windows

Versiera Agent Installation instructions for Win32 Platforms

Manual Installation

1. To install the Versiera agent you must have administrative access to the target computer where the agent will be installed.
2. Use your browser to navigate to https://www.versiera.com/
3. Sign-in using your Versiera ID and password corresponding to your Versiera account
4. In the Agent Section, review the list of the available Windows host agents for download and select the one matching your operating system and hardware platform.
5. Click on the "Download" link. Be sure to save the "versiera-agent-x.x.x.x.exe" to somewhere easy to find like your Desktop.
6. Run the "versiera-agent-x.x.x.x.exe" file and follow the on screen prompts.
    a. Note – when running the agent install on ***Windows Vista*** or ***Windows 7***, first right-click on the "versiera-agent-x.x.x.x.exe" and select "*Run as Administrator*".
7. When the introductory screen appears, click "Next" to continue.
8. On the next screen you can choose the installation path for the agent. It will automatically go to the default location which can be changed if necessary, click "Next" to continue.
9. The next screen will display a summary of the install. Click "Install" to proceed with the installation.
10. On the final screen, "Register as new host with server" is checked on by default. Leave checked for new host installations. Click on Finish.
11. A command prompt window will pop up prompting you for your Versiera ID and password to register the host. Use the Versiera account (Versiera ID and password) that you use to login to your Versiera web account.
12. If the Versiera account (ID and password) are accepted, the host will get registered with Versiera, receive an assigned digital certificate and the agent service will automatically restart.

Note - The rotating Versiera agent log file is located in *%SystemRoot%\vrsagent.log*

Unattended Installation

1. It is recommended that a Versiera Registration ID (Registration User) be created from the Versiera Management Console Administration section. The Registration ID can not be used to access the Versiera Management Console and protects the administrative Versiera ID.
2. Download the Versiera agent to the computer where it will be installed as outlined above.
3. To silently install the Versiera Agent use the following command line:
    a. versiera-agent-x.x.x.x.exe /user=*VersieraID* /pass=*password* /url=https://backend.versiera.com/versiera/backend/rpc.php /verysilent

Enterprise Automated and Unattended Deployment of Versiera Agents

The **PsExec** tool from Microsoft (Mark Russinovich) enables the ability for administrators to remotely copy and install Versiera Agents within an enterprise. The tool can remotely install Versiera Agent on one or multiple computers including registering the agents with the Versiera Management Console.

Detailed information regarding the **PsExec** (v1.97) tool and usage can be found at:
http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

1. Download **PsExec** tool from Microsoft and place in the executable path on a Windows computer
2. Download the Versiera Agent for Windows installation program and place in the same directory as the **PsExec** executable.
3. Use an enterprise administrative account on the machine from which **PsExec** will be used or supply **PsExec** with the appropriate administrative account and password for the remote host where the Versiera agent will be installed.
4. Execute **PsExec** to remotely copy the Versiera Agent, silently install and register the host with the Versiera Management Console:
    a. **psexec \\desktopA –u domain\user –p password –c versiera-agent-x.x.x.x.exe** /user=VersieraID /pass=password /url=https://backend.versiera.com/versiera/backend/rpc.php /verysilent

The Microsoft **PowerShell** (for Windows versions that support it) may also be used to remotely copy and install Versiera Agents to all computers in an enterprise.

Agent Installation - UNIX

Versiera Agent Installation instructions for POSIX (Unix) Platforms

1. To install the Versiera agent you must have administrative access to the target computer where the agent will be installed.
2. Use your browser to navigate to https://www.versiera.com/**.**
3. Sign-in using your Versiera account using your Versiera ID and password.
4. Review the list of available host agents for download and select the one matching your operating system and hardware platform.
5. To download the agent, right-click on the "Download" link and use SAVE LINK AS option. Be sure to save the "versiera-agent-x.x.x.x.sh" to somewhere easy to find like /tmp or your Desktop folder.
6. On your computer change directory to where the downloaded file was saved.
7. Set the execute permission on the "versiera-agent-x.x.x.x.sh" file by issuing the following command from the terminal "chmod 744 versiera-agent-x.x.x.x.sh".
8. Execute the "versiera-agent-x.x.x.x.sh" file with the command "./versiera-agent-x.x.x.x.sh" and follow the on screen prompts.
9. The installer informs you of the path it used to install the agent.
10. Once the agent is installed it will prompt you for your Versiera ID and password to register the host. Use the Versiera ID and password that you use to login to your Versiera web account.
11. If the Versiera ID and password were accepted, the host will get registered, receive a digital certificate and the agent will automatically restart.

Note – The rotating Versiera agent log file is located in /var/log/agentmond.log

Unattended Installation

1. It is recommended that a Versiera Registration ID (Registration User) be created from the Versiera Management Console Administration section. The Registration ID can not be used to access the Versiera Management Console and protects the administrative Versiera ID.
2. Download the Versiera agent to the computer where it will be installed as outlined above.
3. To silently install the Versiera Agent use the following command line:

    a. versiera-agent-x.x.x.x.sh -- --username=*VersieraID* --password=*password* --url=https://backend.versiera.com/versiera/backend/rpc.php

Agent Installation - pfSense Firewall

Versiera Agent Installation instructions for pfSense Firewall

1. To install the Versiera agent you must have administrative access to the target computer where the agent will be installed.
2. Use your browser to navigate to https://www.versiera.com/**.**
3. Sign-in using your Versiera account using your Versiera ID and password.
4. Check of the pfSense website the version of FreeBSD operating system used as the basis of the particular version of pfSense and download the appropriate Versiera FreeBSD agent to your desktop.
5. To download the agent, right-click on the "Download" link and use SAVE LINK AS option. Be sure to save the "versiera-agent-x.x.x.x.sh" to somewhere easy to find like your Desktop folder.
6. On your computer change directory to where the downloaded file was saved.
7. From the pfSense management web interface, go to Diagnostics and use the Command Prompt section. Use the Upload option to transfer the file from your desktop to pfSense. This will place the Versiera agent installer to the pfSense /tmp directory.
8. From the pfSense console, set the execute permission on the "versiera-agent-x.x.x.x.sh" file by issuing the following command from the terminal "chmod 744 versiera-agent-x.x.x.x.sh".
9. Execute the "versiera-agent-x.x.x.x.sh" file with the command "./versiera-agent-x.x.x.x.sh" and follow the on screen prompts.
10. The installer informs you of the path it used to install the agent.
11. Since pfSense uses different path for its startup scripts you will need to copy the /etc/rc.d/agentmond.sh startup script into /usr/local/etc/rc.d/agentmond.sh. This will be done automatically in a future release of the Versiera agent.
12. As a last step you will need to register the Versiera agent to your Versiera ID as follows:
    a. /usr/local/lib/vrsagent/agent/1.3.2/vrsagent -reghost -s https://backend.versiera.com --username=*VersieraID* --password=*password*
13. If the Versiera ID and password are accepted, the host will get registered, receive a digital certificate and the agent will automatically restart.

Note – The rotating Versiera agent log file is located in /var/log/agentmond.log

Note: It is recommended that a **Versiera Registration ID** (Registration User) be created from the Versiera Management Console Administration section. The Registration ID can not be used to access the Versiera Management Console and protects the administrative Versiera ID.

Agent Installation – DD-WRT

Versiera Agent Installation instructions for Embedded Platform

Prerequisite:

1. It is recommended the embedded network device should have a minimum of 8MB flash and 16MB DRAM memory.
2. **DD-WRT 2.4 SP1** (or newer) installed on the embedded device (Broadcom/Atheros). Note - the **Standard** and **Mega** DD-WRT distribution versions are known to work with Versiera agents.
3. Embedded device should be able to connect to the Internet. Required to register the device with Versiera Management Console.

Procedure:

1. Configure network the IP address, subnet mask and gateway on the embedded network device.
2. Configure DNS servers as the agent installation needs to be able to resolve "**https://backend.versiera.com/"**
    a. Example: **8.8.8.8** and **8.8.4.4** (Google DNS)
    b. Example: **208.67.222.222** and **208.67.220.220** (OpenDNS)
3. Configure the time zone using the DD-WRT management interface.
4. Configure the date/time on the embedded network device.
    a. Example: **date -s 2010.04.30-10:41**
5. Optionally configure the Network Time Protocol (NTP) to maintain the correct time.
6. Enable the "**jffs**" file system support using the DD-WRT management interface.
7. Use your browser to navigate to https://www.versiera.com/**.**
8. Sign-in using your Versiera ID and password.
9. Review the list of available host agents for download and select the one matching your embedded network device and firmware.
10. To download the agent, right-click on the "Download" link and use SAVE LINK AS option. Be sure to save the "versiera-agent-x.x.x.x.sh" to somewhere easy to find like your Desktop folder.
11. Secure copy the downloaded Versiera agent to the embedded device over the network using the command "**scp agent-install.tar.gz root@xxx.xxx.xxx.xxx:/tmp**" (agent may also be copied from USB if the port is available on the device).
12. Log into the embedded device console and change directory with the command "**cd /tmp**".
13. Extract the agent from the archive "**tar xzf agent-install.tar.gz –C /**".
14. Change directory with the command "**cd /jffs/opt/vrsagent/agent/1.3.2/**"
15. Manually register the host "**./vrsagent –reghost –s https://backend.versiera.com/versiera/backend/rpc.php**".

16. During the installation, when prompted, enter the Versiera ID and password that you use to sign-in to the Versiera Management Console.

Verification:

1. Versiera agent configuration settings are saved in "**/jffs/etc/versiera/**" directory.
2. Versiera agent startup script is "**/jffs/etc/config/agentmond.wanup**"**.**
3. Versiera agent is installed to "**/jffs/opt/vrsagent/**".
4. Verify that the agent is running by executing "**ps –ef | grep vrsagent**", if it is not reboot the embedded device.
5. Log into the Versiera website https://www.versiera.com/, after a couple of minutes the agent should start populating information for the embedded device.
6. Review firewall rules and ensure that the firewall rules on the embedded device are set to permit outbound communication on port *443/tcp (SSL).*

Agent Installation – OpenWRT

Versiera Agent Installation instructions for Embedded Platform

Prerequisite:

1. It is recommended the embedded network device should have a minimum of 8MB flash and 16MB DRAM memory.
2. **OpenWRT 8.09.1** (or newer) installed on the embedded device (Broadcom/Atheros).
3. Embedded device should be able to connect to the Internet. Required to register the device with Versiera Management Console.

Procedure:

1. Configure the IP address, subnet mask and gateway on the embedded device.
2. Configure DNS servers as the agent installation needs to be able to resolve "**https://backend.versiera.com/"**
    a. Example: **8.8.8.8** and **8.8.4.4** (Google DNS)
    b. Example: **208.67.222.222** and **208.67.220.220** (OpenDNS)
3. Configure the time zone and date/time on the embedded network device.
    c. Example: **date -s 2010.04.30-10:41**
4. Optionally configure the Network Time Protocol (NTP) to maintain the correct time.
5. From the OpenWRT console execute "**opkg update**"
6. From the OpenWRT console execute "**opkg install libopenssl**" to install required library.
7. From the OpenWRT console execute "**opkg install libpthread**" to install required library.
8. Use your browser to navigate to https://www.versiera.com/**.**
9. Sign-in using your Versiera ID and password.
10. Review the list of available host agents for download and select the one matching your embedded network device and firmware.
11. To download the agent, right-click on the "Download" link and use SAVE LINK AS option. Be sure to save the "versiera-agent-x.x.x.x.sh" to somewhere easy to find like your Desktop folder.
12. Copy Versiera agent "**versiera-agent-x.x.x.x.sh**" to the embedded device over the network using **scp** command**.**
13. Once the "**versiera-agent-x.x.x.x.sh**" is on the OpenWRT embedded device, set the execute permission on the file with the command "**chmod 744 versiera-agent-x.x.x.x.sh**".
14. Run the Versiera agent installer with the command "**./versiera-agent-x.x.x.x.sh**"
15. During the installation, when prompted, enter the **Versiera ID** and **password** that you use to sign-in to the Versiera Management Console.

16. A firewall rule may need to be set to permit outbound communication from the embedded device to Versiera Management Console. Please review firewall rules using "**iptables -L**".The following firewall rule can be added to the Versiera startup script "**/etc/init.d/agentmond**" by inserting a the following line at line 66.
    d. **iptables –A OUTPUT –p tcp –dport 443 –j ACCEPT**

Verification:

1. Versiera agent configuration settings are saved in **/etc/versiera** directory.
2. Versiera agent startup script is **/etc/init.d/agentmond** and a startup link is **/etc/rc.d/S99agentmond**.
3. Versiera agent is installed to **/opt/vrsagent**.
4. Verify the agent is running by executing "**ps –ef | grep vrsagent**"
5. Log into the Versiera website https://www.versiera.com/, after a couple of minutes the agent should start populating information for the embedded device.
6. The agent may be executed manually for debugging purposes by first stopping the agent "**/etc/init.d/agentmond stop**" and running the agent manually "**/opt/vrsagent/agent/1.3.2/vrsagent –C /etc/versiera/agent**".

Versiera Management Console

Now that you've successfully installed a Versiera agent on your host(s), we can introduce you to the information available in the Management Console as received from the Versiera agents. It is suggested that a minimum screen resolution of 1024x768 be used when using Versiera Management Console and for optimum results 1280x1024 or higher is recommended.

Web Browsers

The Versiera Management Console is the user web interface through which you are able to manage and monitor your infrastructure technology. To use the Versiera Management Console a web browser is required. Versiera Management Console has been tested successfully with the following browsers: Google Chrome, Apple Safari, Opera, Firefox, Konqueror and Microsoft Internet Explorer. Other browsers may also work, but have not been tested. For the best results Chrome, Safari, Opera and Firefox browsers are recommended.

Title Box

Once a user signs into Versiera, the main title box presents them with their registered Company Name, Versiera ID, and time zone information. Summary information is also provided on the number of registered hosts and the number that have not reporting in recently.

Main Screen - Sections

Versiera Management Console has been designed for quick and easy traversal. The main screen is divided into Sections. By clicking on a Section icon or title the user is taken to the information for the respective section. Sections are then subdivided by context tabs. Other interface traversal options are also available in the form of a section drop-down boxes and web page bread-crumb links.

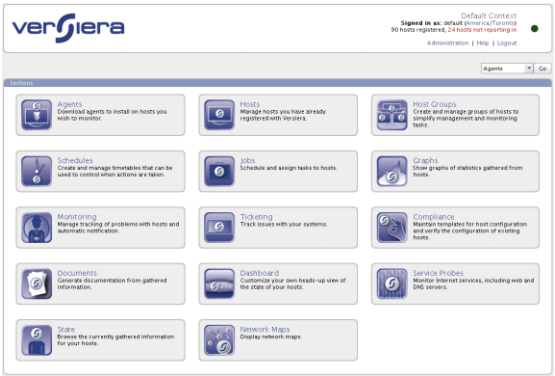
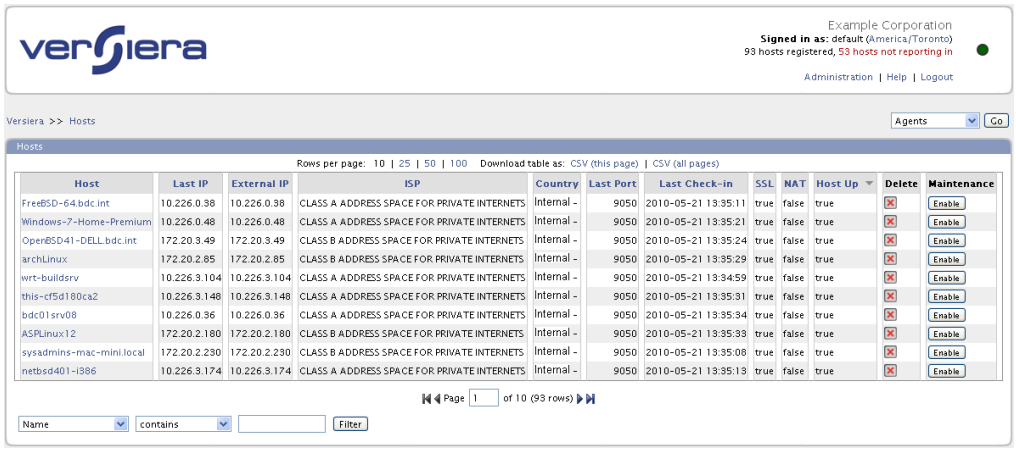


Table Data

Much of the information in Versiera Management Console is presented in table format. The number of rows per table may be controlled from 10, 25, 50, and 100 to suite user preferences. This preference is configurable from any of the tables using the selections above the table. Once selected the preference is saved and will be used throughout Versiera until changed by the user. The number of rows in a table is presented at the bottom of the table. When the total number of rows exceeds that of an individual table page, controls are provided below the table as direction arrows, to view the rest of the rows. All table data is available for download using comma separated values (CSV) or as a portable document format (PDF) file.



Sorting Table Rows

The table data is presented with default sort orders based on a particular column in the table. The table columns that have headings in blue colour can be used for sorting data rows. By clicking on the table column heading successively, that column will be used for sorting and alternate clicks will sort in ascending and descending order.

Arranging Table Columns

The default table column ordering in tables may be altered to suit preferences. By clicking on and dragging a table column heading to the desired position between columns in the table and releasing, the column ordering will be modified and saved as a preference.

Filters

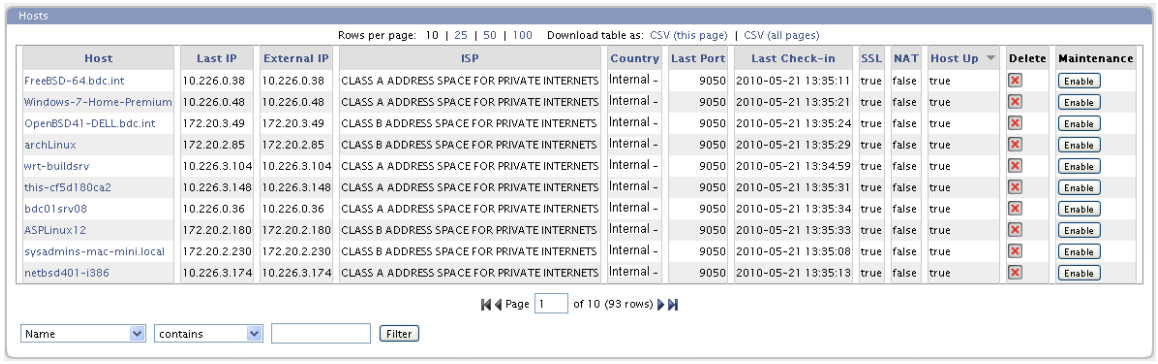
At the bottom of all tables there are three boxes and a "**Filter**" button that allow the selection of the desired data to be presented in the table. The left-most drop-down box (shown below) for building a filter expression allows the selection of the table column upon which the filter will be applied. The center drop-down box provides filter expression types. The right-most box provides user entered filtering criteria to be used in the expression for the target column.

By typing successive characters in the right-most box, Versiera Management Console automatically starts to suggest values from the table data which can be selected and applied. The user may prefer to only enter partial data for filtering, such as several characters of a name.

Versiera Management Console permits the use of multiple filters against a table to reduce the number of rows and present the optimum data set.

Hosts

The Host section provides an overview of host communication information. Table rows show host communication information and confirm the host is successfully reporting in. Table rows in yellow show hosts that have been successfully registered, but have not submitted any state information. Table rows highlighted in red, indicate hosts have not submitted any information to Versiera within the last five (5) minutes. In general the host installed Versiera agents submit quick "host up" status every sixty (60) seconds.



Viewing Hosts Table Information

The table data provides the following information:

Host – the hostname of the system registered with Versiera. Each name is also a link that when clicked on will take you to the host's summary page.

Last IP – the IP address of the host used by the agent to communicate to the Versiera management system.

External IP – the IP address seen by the central Versiera management system while communicating to the host agent (Internet public IP address). The IP address seen by Versiera may belong to another host device such as a firewall acting to perform network address translation (NAT).

Last Port – the listening port number of the Versiera agent running on the host

Last Check-in – the data and time of the last agent check-in, which in common usage should be updating once every minute

SSL – a Boolean value of true/false on whether the communications between the agent and central Versiera system is using secure socket layer (SSL)

NAT - a Boolean value of true/false on whether the network address as seen by Versiera Management Console during agent check-in matches one of the network interfaces of the particular host. If the value is TRUE, an intermediate device in the communication path is translating the network address of the host with the Versiera agent with one of its own.

Host Up – a Boolean value that shows whether the host agent is up and implies that the host must also be up

Delete – the button to unregister a host and remove its information from the Versiera Management Console. The Versiera agent on the host will no longer be authorized to check-in to the Versiera Management Console.

Maintenance – the button to enable/disable the maintenance state for a given host. When a host is placed in maintenance state any monitoring alerts are suppressed.

Host Groups

The Host Groups are used to simplify management and monitoring tasks. There are two types of groups static and dynamic. Static group members are explicitly defined by adding hosts to the group. Dynamic group members are automatically determined based on one or more rules regarding host properties. For example a Dynamic Groups may be based on hosts that reside on a particular network, hosts with similar operating systems, or hosts with similar running programs.

Viewing Host Groups Table Information

The table data provides the following information:

Name – the name of the host group.

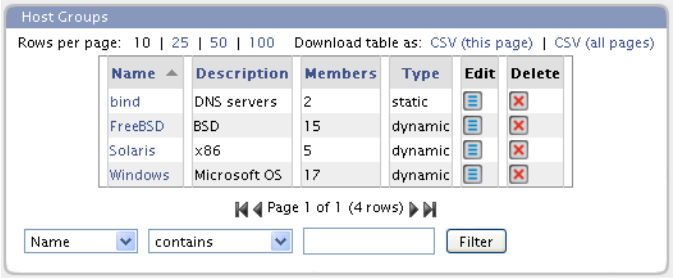
Description – additional information about the group

Members – the number of hosts in the host group

Type – the host group type (*static* or *dynamic)*

Edit – the button to edit the list of members of the host group

Delete – the button to delete a host group

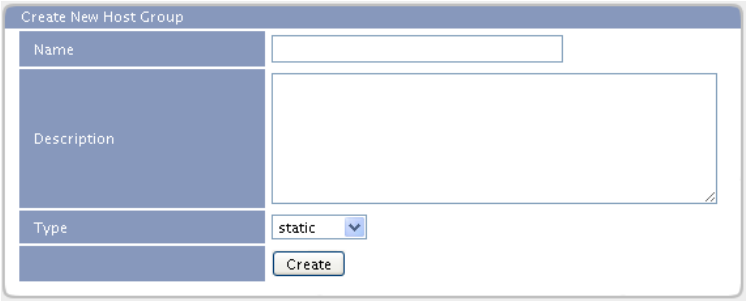


Create New Host Group Form

Name – the name of the host group

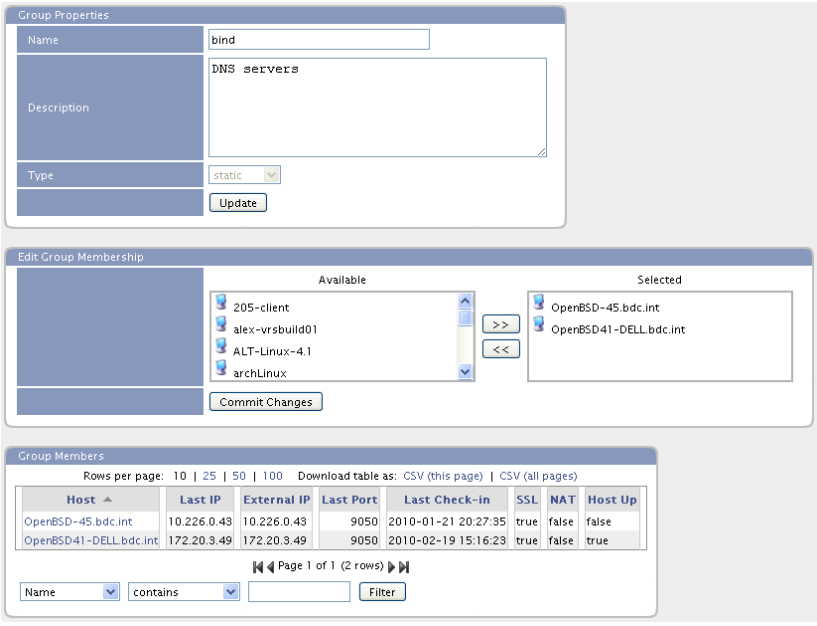
Description – additional information about the host group

Type – the host group type *static or dynamic*



Group Properties – Static Host Groups

To update the static groups, use the "Edit Group Memberships" form. Clicking on hosts or groups from ether the "Available" or "Selected" and then clicking on the ">>" or "<<" buttons to moves the hosts or groups in and out of the group's membership. Pressing the Commit Changes button applies the changes to the Host Group memberships.



Group Properties – Dynamic Host Groups

Op – logical operators (***and***, ***or***) for use with multiple rule sets

Invert – checkbox that applies the ***not*** logical operator to the Rule

Field – drop-down box that includes all possible host properties to be evaluated in the membership Rule

Rule – drop-down box of rule types to be used in the membership Rule

Value – the user supplied value for evaluation

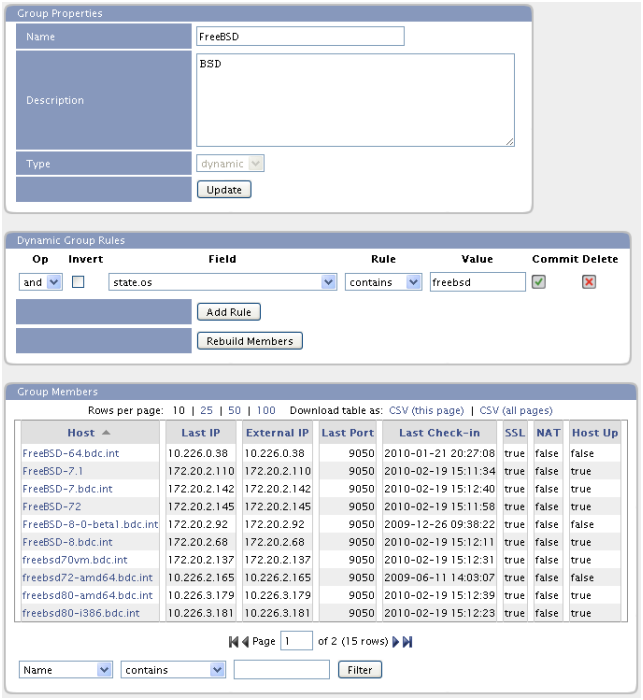
Commit – the button to apply a created Rule to the Host Group's memberships

Delete – the button used to delete a given Rule

Add Rule – the button for the addition of another dynamic group rule to a Rule Set

Rebuild Members – the button is used to generate or update table of a group's members

Group Properties – Dynamic Host Group



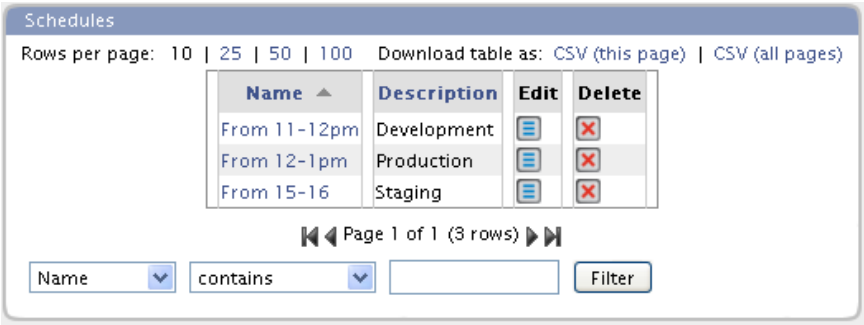
Schedules

Schedules are used for creating and managing timetables that can be used to control when actions are taken. Schedules can be used for Monitoring, Jobs, and for setting time intervals over which Notifications should be sent out. Schedules are evaluated by the Versiera central system. Since Versiera keeps data on the remote host's UTC offsets, the scheduled times are based on the local time of the remote hosts. That is to say that if a schedule to start a host backup job is scheduled to run at 22:00 on several servers located in different time zones, Versiera will offer the job to each servers based on when 22:00 is effective for them. This also applies for schedules used in user notifications. Each Versiera user configures their respective time zone, so any schedules for notifications apply to the users based on their respective time zone. The process of creating a schedule requires that at least one *Rule Set* be created to set a time zone. A *Rule Set* is itself comprised of one or more individual *Rules*. Schedules can be comprised of multiple Rule Sets to accommodate particular timing requirements. In general terms:

- A single *Rule Set* is a logical expression formed by individual *Rules* connected with the logical conjunction (logical AND)
- A *Schedule* is a logical expression formed by a group of *Rule Sets* connected with the logical disjunction (logical OR)

Viewing Schedules Table Information

The Schedules table data provides the following information:



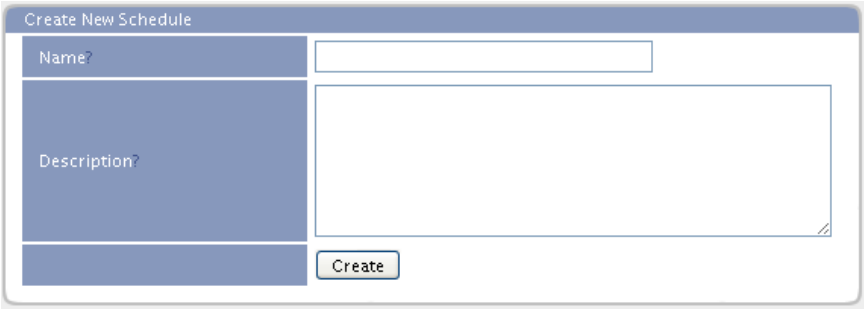
Name – the name of a particular schedule

Description – additional information about the particular schedule

Edit – the button allows the update of a particular schedule

Delete – the delete button removes a particular schedule

Create New Schedule Form

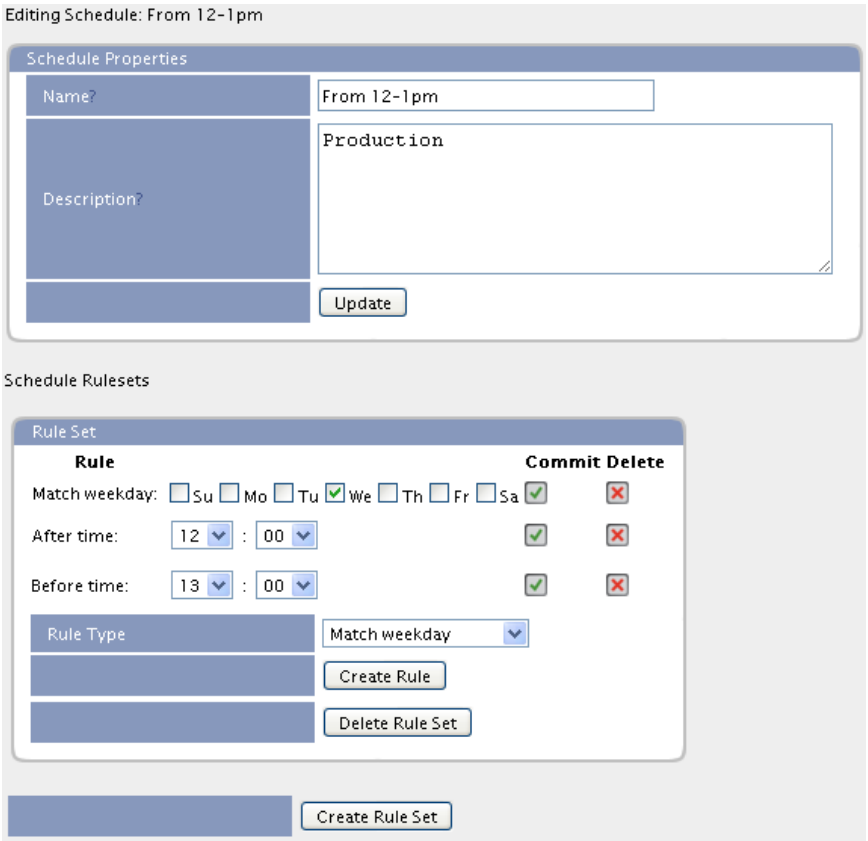


Name – the name of the schedule

Description – additional information about the schedule

Once a schedule has been created, one or more RULE SETS need to be associated with the schedules that define when actions should take place.

Create New Rule Set Form



Rule Type – a drop-down box to select a particular rule type

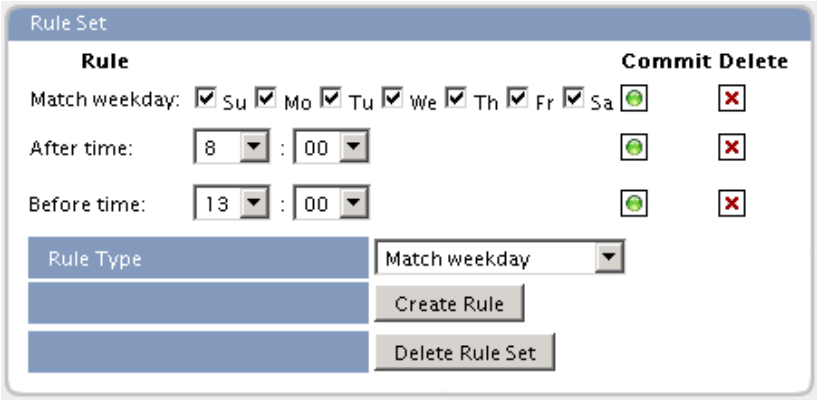
- Match weekday
- After day of month
- Before day of month
- After time
- Before time
- After date and time
- Before date and time

Create Rule – button to add a new Rule Type from the drop-down window to the Rule Set

Delete Rule Set – button to remove an entire Rule Set rather than individual rules in a set

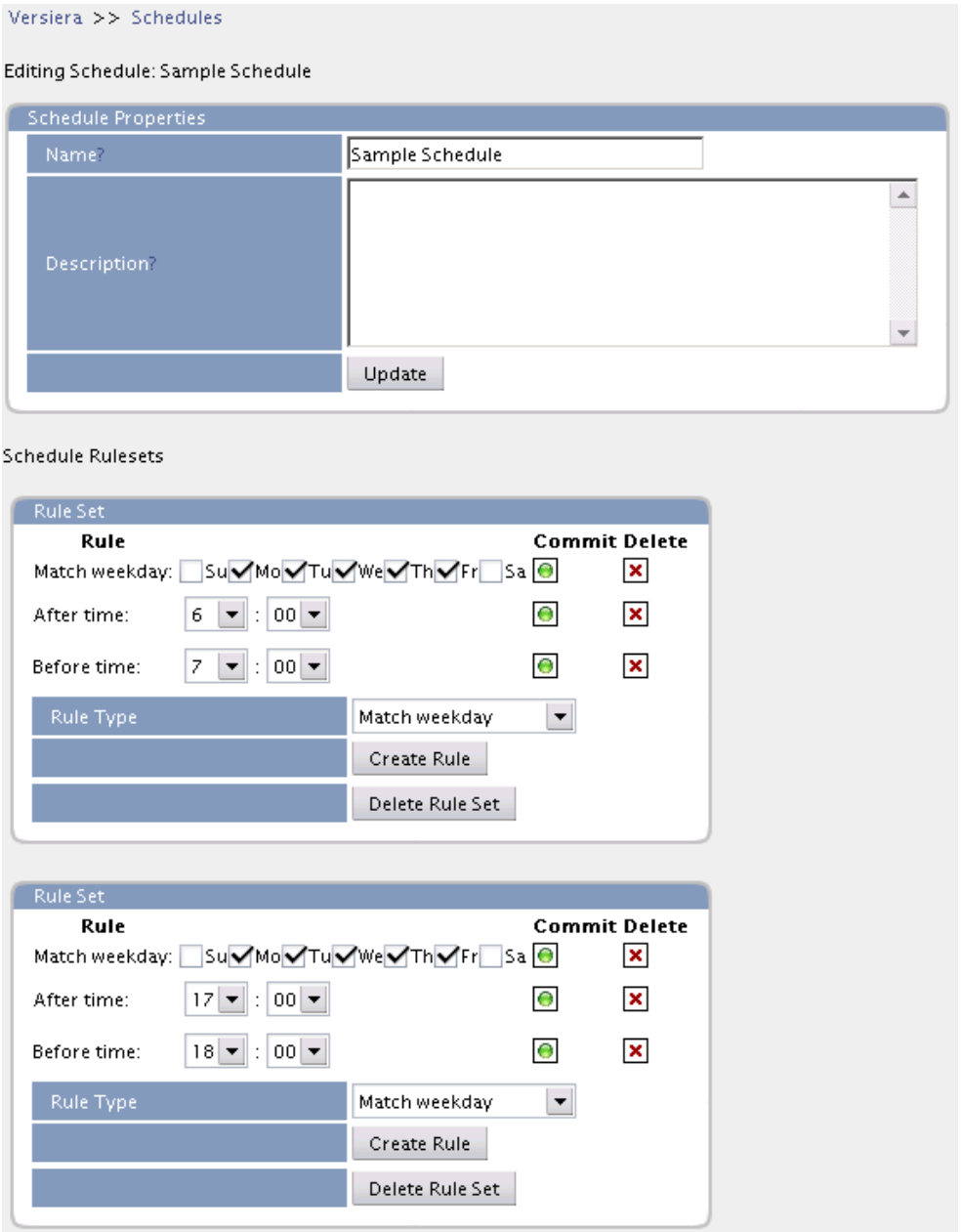
Sample Rule Set

The sample Rule Set is comprised of three separate Rules that form a logical expression having been connected with logical conjunction (logical AND). Given Rule Set can be used to run a particular job every day of the week between 8:00am and 1:00pm. If the Job must be repeated during the scheduled times, then an Interval time should be configured for the particular Job.



Sample Schedule

The following sample Schedule will perform the associated Job during weekdays between 6:00-7:00 and 17:00-18:00.



Jobs

Jobs are used to perform remote host operations. Jobs are comprised of Script operations, hosts to whom the jobs are assigned and optional schedules and prerequisites. Scripts include predefined operations such as User or Process Management or as user defined functions written in Bluescript language. In creating a Job, the first step is to select a Script that defines the desired operation required on a remote host(s). Next, a Job is configured, associated with the selected Script and assigned to one or more hosts. Once the Job has been configured and saved it is automatically published by the central Versiera for acceptance by remote hosts to whom the Job has been assigned. Jobs are accepted and initiated for execution by the remote host Versiera agents. During a check-in, the agents on remote hosts query the central Versiera system whether there are any scheduled Jobs for them to perform. If a Job has been assigned to a particular remote host it will be accepted by the remote host agent and executed.

Job Chaining

Job Chaining is used to specify an order between related Jobs and to establish a prerequisite for the successful completion of one Job before another is executed. This capability is useful for such operations as dumping the contents of a database before starting the backup of the database dump data.

There are two types of Versiera Scripts:

The first are predefined Script Models:

- User Management (Add/Delete/Disable/Change Password)
- Process Management (Start/Kill)
- Service/Daemon Control (Start/Stop/Restart)
- Software Distribution (exec, msi, installshield, rpm, dpkg, pkg)
- Software Removal (exec, msi, installshield, rpm, dpkg, pkg)
- Host Shutdown/Reboot/User Logoff

The second are Scripts written by Versiera users to perform custom tasks using BlueScript language (embedded agent language similar to TCL). Note – full Bluescript language documentation has not been officially released. Also the current implementation limits Bluescript script to 64KB.

User Management

The User Management Jobs are used for management of local host user accounts. The Jobs can perform account operations including adding, deleting, disabling accounts and changing passwords. For environments where a single sign-on directory service is not available or not practical, these Jobs may be useful in maintaining a set of synchronized host accounts and associated passwords.

Process Management

The Process Management Jobs include operations for starting and killing of application processes. Applications started by Versiera agents are started in the same security context as Versiera agents.

Service/Daemon Control

The Service/Daemon Control Jobs include operations for starting, stopping and restarting Services (Windows) and Daemons (Unix). As an example in using this Job type, it is possible to fail-over a production web server environment to for disaster recovery purposes or maintenance by enabling the services on a secondary site and shutting down services on a primary using scheduling.

Software Distribution

The Software Distribution Job type provides the ability to remotely install software packages located on web servers using the HTTP transfer protocol. This provides the ability to perform centralized software distribution to one or more remote systems.

> *Requirements* - Configuration of a Software Installation Job requires that the software to be delivered is placed on a web server accessible to the remote hosts. The software delivery transport mechanism uses HTTP protocol (port 80/tcp) to copy the file to the selected host(s).
>
> *Software Package Types*:
>
> > *Windows* - Microsoft Windows the Single Executable (such as Microsoft Hotfixes), Microsoft Installer Package (MSI) and InstallShield (ISS)
> >
> > *Linux* – Red Hat Package Management (RPM) and Debian Package (DPKG) Management Systems
> >
> > *FreeBSD/NetBSD/OpenBSD* – FreeBSD Ports collections (PKG)

Software Removal

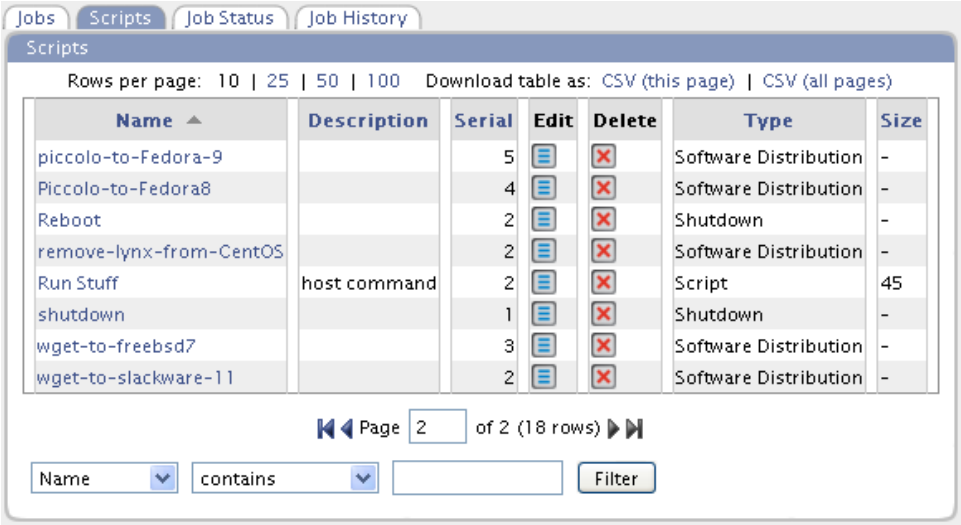
The Software Removal Job type provides the ability to remove software applications on remote hosts using the remote host's particular software management facilities (i.e. Windows Installer, etc.)

Host Shutdown/Reboot/User Logoff

The Shutdown script type provides a number of remote host operations including host shutdown, host reboot and the ability to force a user to logoff.

Scripts Tab

The Scripts table data provides the following information about configured scripts:



Name – the name of a particular script

Description – additional information about the particular script

Serial – a numeric value that automatically increments each time a script is modified

Edit – the button allows the update of a particular script

Delete – the button allows the removal of a particular script

Type – provides information whether the script is explicit or based on a predefined model

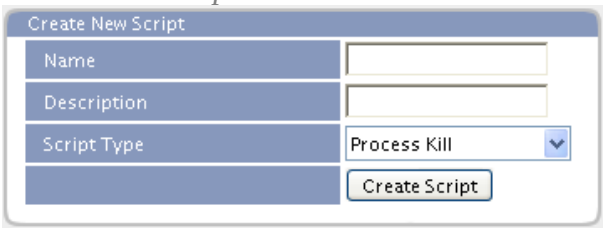
Size – provides the size of a script

Creating a Job

There are several steps in creating a basic Job:

1. Create a Script using the *Create New Script Form* and selecting one of the built-in Script Models.

Create New Script Form



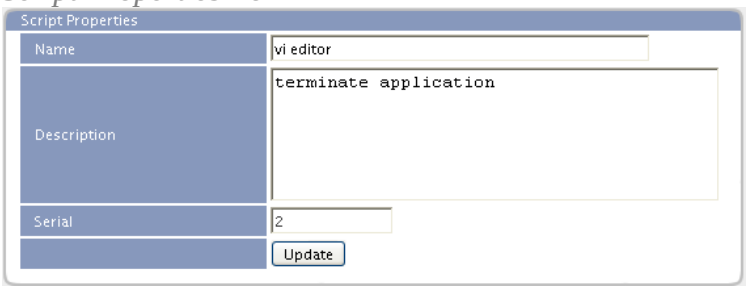
Name – the name assigned to the particular script

Description – information or details about the particular script

Script Type – script type (Process Kill, Process Start, Script, Service Control, Shutdown, Software Distribution, Software Removal, User Management)

2. Configure the Script Properties using the Script Properties Form.

Script Properties Form



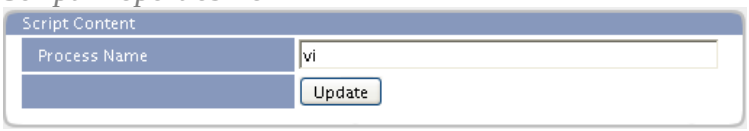
Name – the name the script

Description – information or details about the script

Serial – a numeric value that automatically increments each time a script is modified

3. Configure the *Script Content Form*

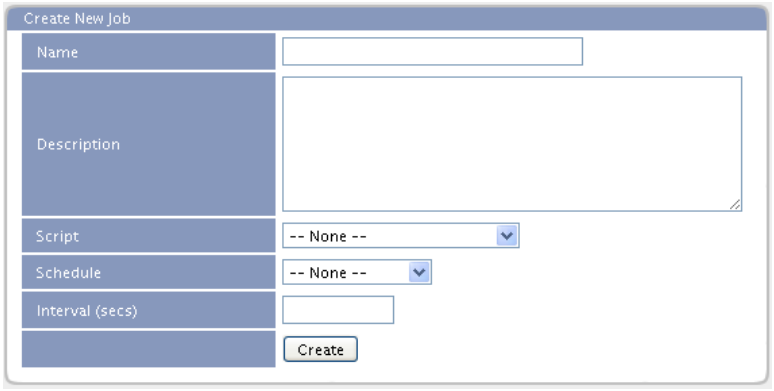
Script Properties Form



Process Name – the name of the application process to kill

4. Create a new Job using the *Create New Job Form.*

Create New Job Form



Name – the name assigned to the particular job

Description – (optional) information or details about the particular job

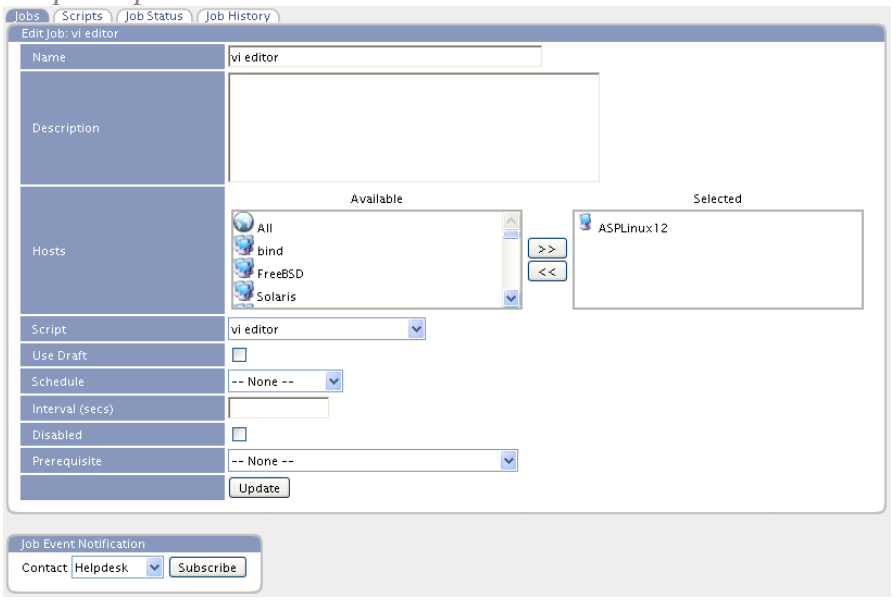
Script – drop-down windows allowing the selection of a script name to be assigned to the job, previously created in the Scripts tab

Schedule – (optional) drop-down window allowing the selection of a schedule name to be assigned to the job, previously created in the Schedule Section

Interval – (optional) the number of seconds between particular job repetitions for situations when a particular job must be performed continuously

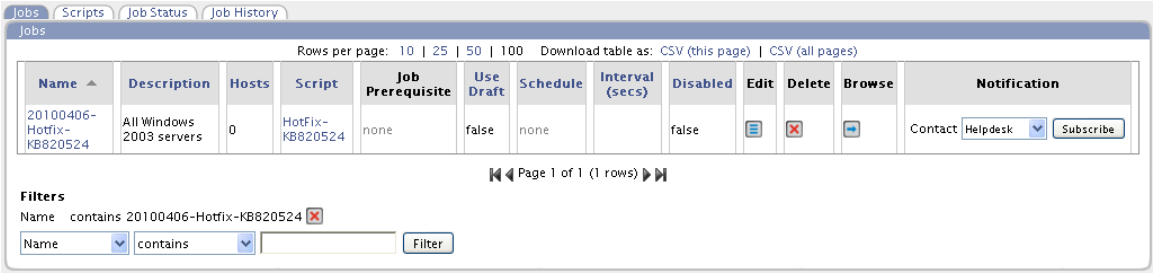
5. Select the hosts or groups of hosts where the created Jobs will be performed.
6. Associate the configured Script instance with the Job.
7. Save the created Job.

Script Properties Form



Jobs Table

The Jobs table data provides the following information about configured jobs:



Name – the name of a particular job

Description – additional information about the particular job

Hosts – the number of hosts assigned to a job

Script – the name of the script associated with the job

Use Draft – the Draft checkbox applies to only those jobs defined as Script type rather than Job Models (i.e. Software Distribution). By selecting the checkbox, the Draft version of a script will be used in place of the Body of a script. This is helpful for testing new versions of scripts.

Schedule – the name of the schedule associated with the job

Interval – the interval in seconds to repeat the job

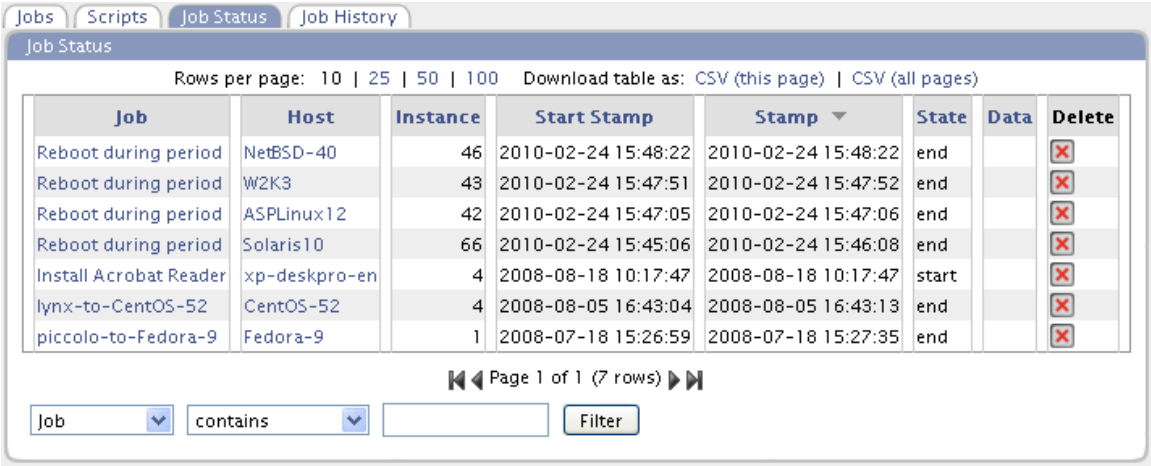
Disabled – Boolean value defining whether the script is disabled

Edit – the button for updating of a particular job

Delete – the button for removing of a particular job

Notification – the contact that should be notified of the job progress

Job Status Table



The Job Status table data provides the following information about the execution status of jobs:

Job – the name assigned to the job

Host – name of a host from list of hosts assigned to the job

Instance – the number of time the host attempted to complete the job

Start Stamp – the date and time for starting the job by the host

Stamp – the date and time the host Versiera agent updated Versiera Management Console on the Job status

State – the current state of a job (*queued, start, end/fail, wait*)

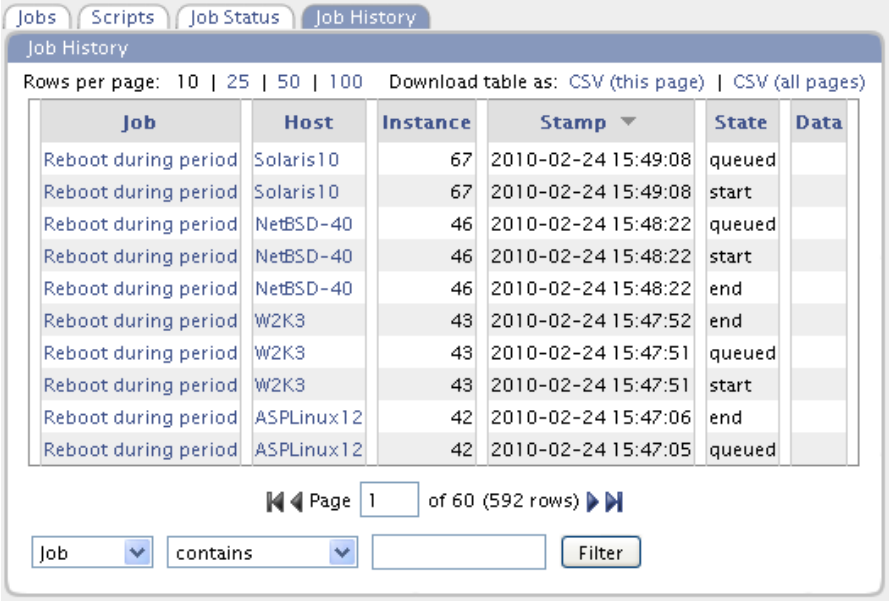
Data – any data returned from the job execution

Delete – the button for removing of the Job status table record

Rerunning Jobs

There may be situations where a particular *Job* needs to be run more than once on a particular host such as when it *failed* to complete. In that situation *Deleting* the particular job row for a given host from the *Job Status* table will enable the remote host to run the job again within the next five (5) minute interval.

Job History Table



The Job History tab provides the following information for review of older job records:

Job – the name assigned to the job

Host – name of a host from list of hosts assigned to the job

Instance – the number of times the job was executed by the host agent

Stamp – the date and time the historical data was saved

State – the data record on the job execution state (*queued, start, end/fail*)

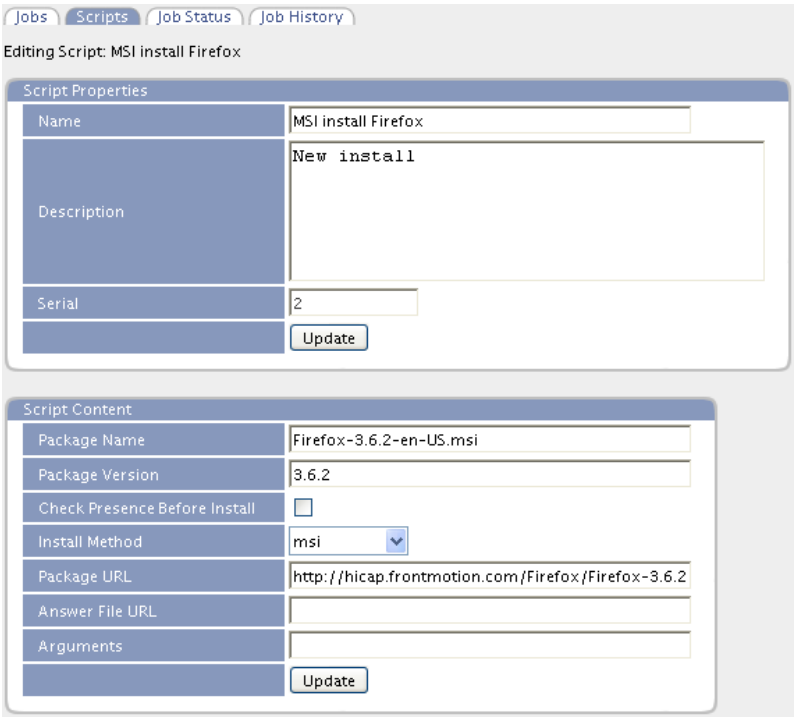
Data – any data returned from the job execution

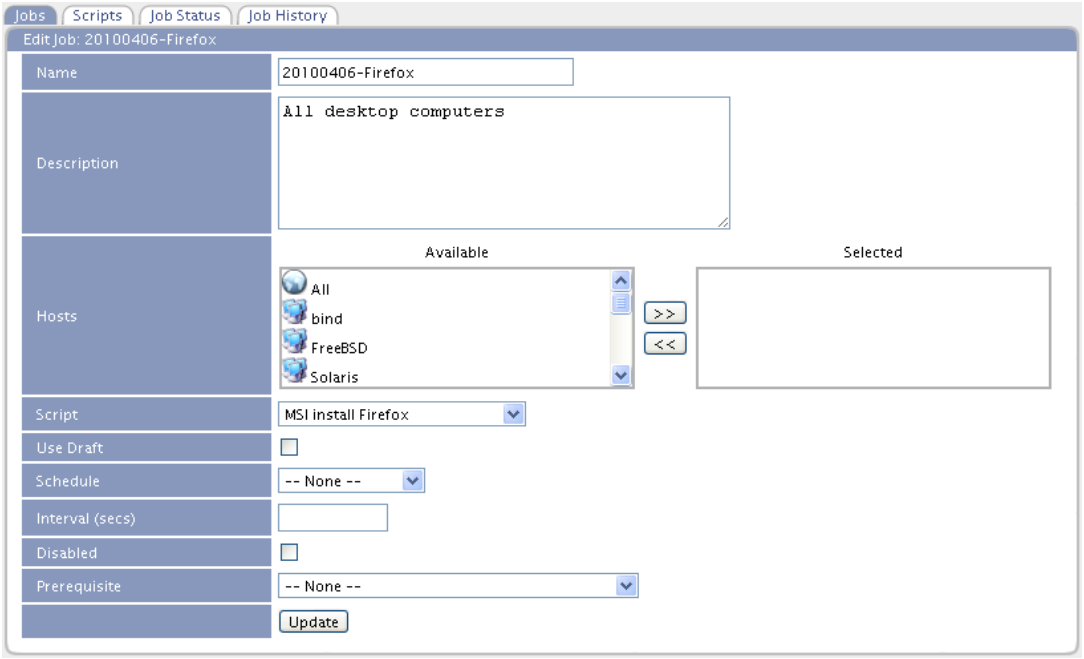
Example of a Job – Software Distribution

As an example we will demonstrate how it may be possible to distribute the popular Firefox web browser to one or more Windows computers. The following sample provides an overview of creating and executing a Software Distribution Job:

1. Obtain the Firefox Windows Installer package from http://www.frontmotion.com/Firefox/download_firefox.htm
2. From the "*Scripts*" tab, create a new software distribution script.
   - Name: **MSI install Firefox**
   - Description: **New install**
   - Script Type: **Software Distribution**
3. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
4. The next step is to complete the "*Script Content*" form and click the Update button once done:
   - Package Name: **Firefox-3.6.2-en-US.msi**
   - Package Version: **3.6.2**
   - Check Presence Before Install: (leave unchecked)
   - Install Method: **msi**
   - Package URL: **http://hicap.frontmotion.com/Firefox/Firefox-3.6.2-en-US.msi**
   - Answer File URL: -
   - Arguments: -
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100406-Firefox**
   - Description: **All desktop computers**
   - Script: **MSI install Firefox**
   - Schedule: -
   - Interval (secs): -
6. From the "*Edit Job*" form, assign to job **20100406-Firefox** to one or more hosts from the available list. Click on the Update button to save the form contents.
   - Use Draft – leave unchecked
   - Schedule – leave as "-- None --"
   - Internal (secs) – leave blank
   - Disabled – leave unchecked
   - Prerequisite – leave as "—None –"
7. Select the desired Contact for job notification and click on the Subscribe button.

Example – Microsoft Installer (MSI) Software Distribution Configuration



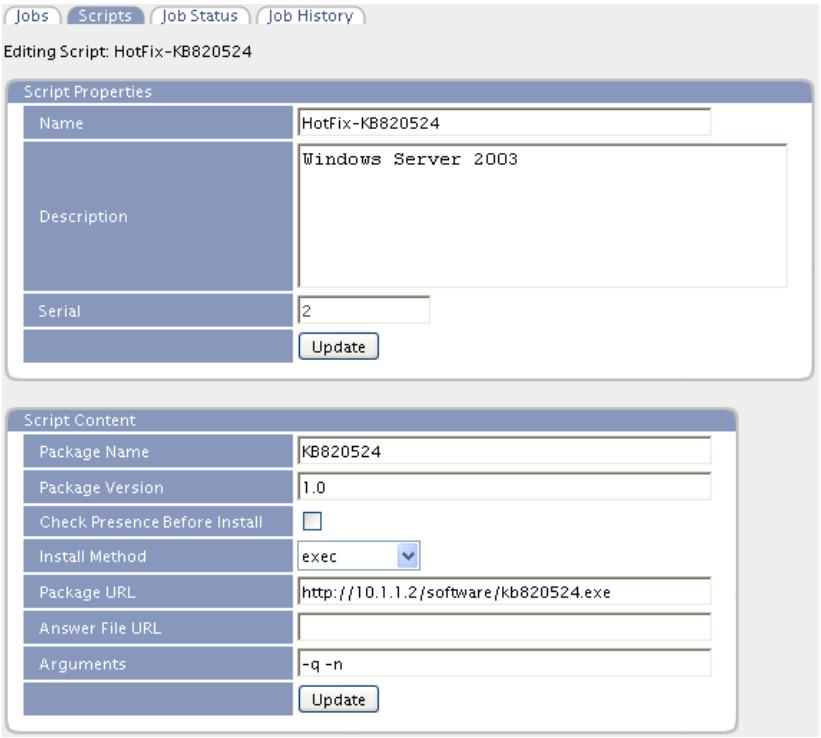


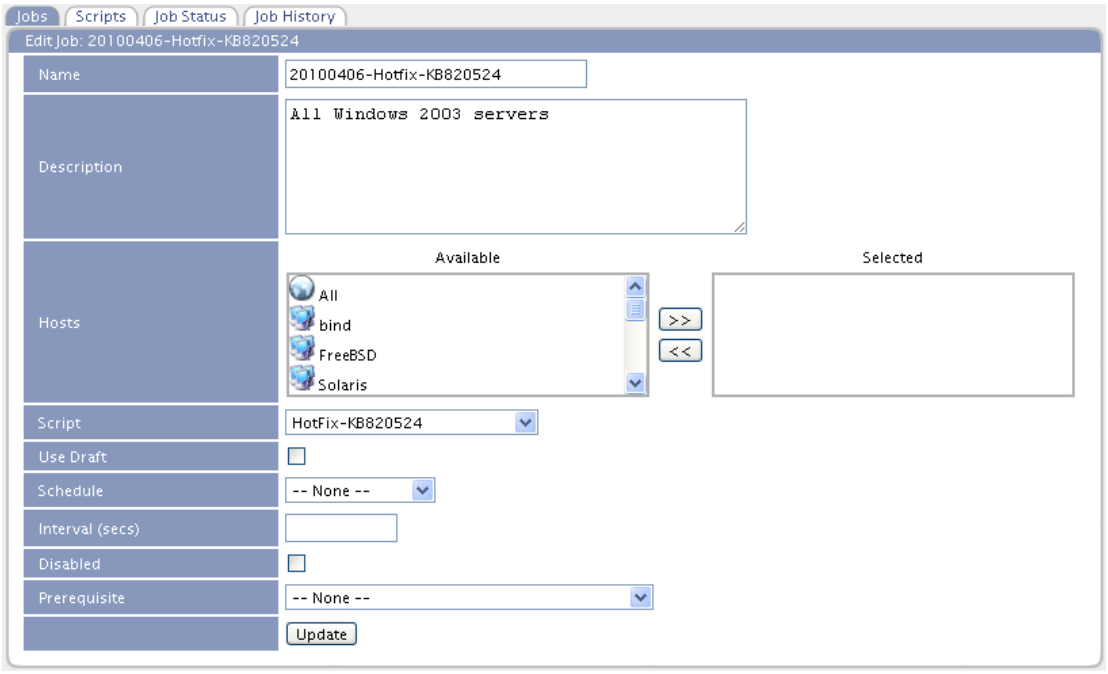
Example of a Job – Software Distribution

As an example we will demonstrate how to create a job to distribute a Microsoft Hotfix to one or more Windows computers.

1. Obtain the KB820524 Hotfix executable file from Microsoft and make it accessible on a web server via HTTP.
2. From the "*Scripts*" tab, create a new software distribution script.
   - Name: **HotFix-KB820524**
   - Description: **Windows Server 2003**
   - Script Type: **Software Distribution**
3. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
4. The next step is to complete the "*Script Content*" form and click the Update button once done:
   - Package Name: **KB820524**
   - Package Version: **1.0**
   - Check Presence Before Install: (leave unchecked)
   - Install Method: **exec**
   - Package URL: **http://10.1.1.2/software/kb820524.exe**
   - Answer File URL: -
   - Arguments: **-q -n**
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100406-Hotfix-KB820524**
   - Description: **All Windows 2003 servers**
   - Script: **HotFix-KB820524**
   - Schedule: -
   - Interval (secs): -
6. From the "*Edit Job*" form, assign the **20100406-Hotfix-KB820524** job to one or more hosts from the available list. Click on the Update button to save the form contents.
   - Use Draft – leave unchecked
   - Schedule – leave as "-- None --"
   - Internal (secs) – leave blank
   - Disabled – leave unchecked
   - Prerequisite – leave as "—None –"
7. Select the desired Contact for job notification and click on the Subscribe button.

Example – Microsoft Hotfix (EXEC) Software Distribution Configuration



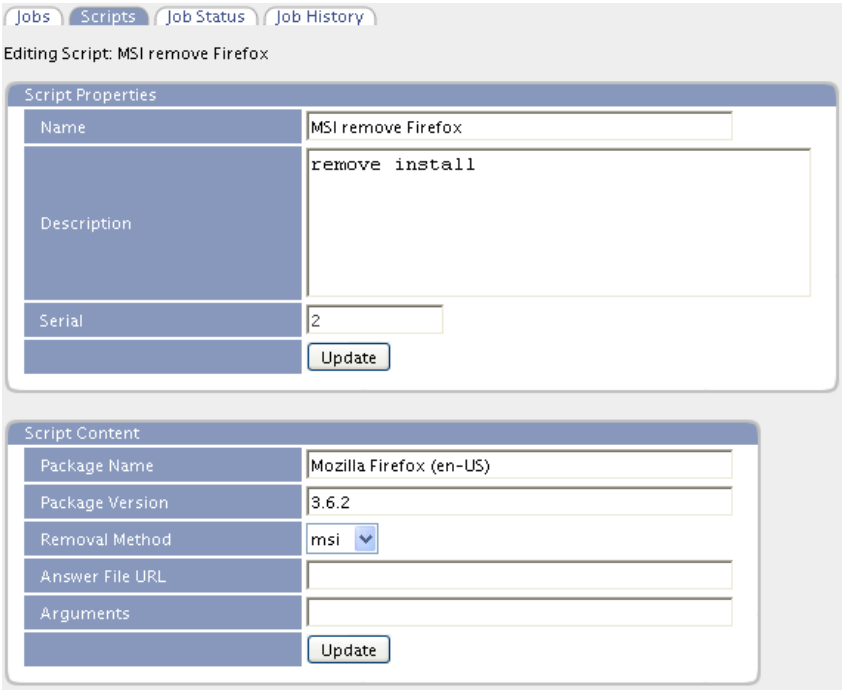


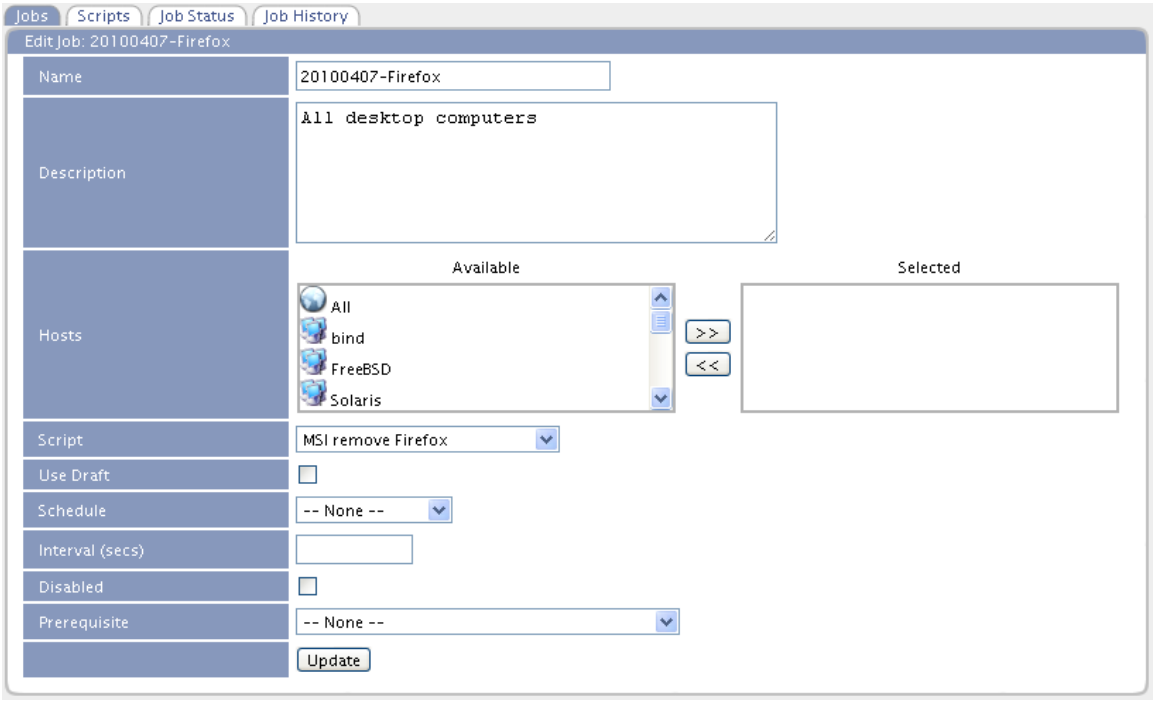
Example of a Job – Software Removal

As an example we will demonstrate how to create a job to remove Firefox web browser from one or more Windows computers.

1. From the "*Scripts*" tab, create a new software removal script.
   - Name: **MSI remove Firefox**
   - Description: **remove install**
   - Script Type: **Software Removal**
2. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
3. It is necessary to determine the application name of the software as it is recorded in "*Add or Remove Programs*" in the Windows Control Panel or as recorded by Versiera in "**Versiera >> State >> Software**". This name will be used below as the Package Name. For Firefox 3.6.2 the name is recorded as "*Mozilla Firefox (en-US)*"
4. The next step is to complete the "*Script Content*" form and click the Update button once done:
   - Package Name: **Mozilla Firefox (en-US)**
   - Package Version: **3.6.2**
   - Check Presence Before Install: (leave unchecked)
   - Install Method: **msi**
   - Package URL: **-**
   - Answer File URL: -
   - Arguments: **-**
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100407-Firefox**
   - Description: **All desktop computers**
   - Script: **MSI remove Firefox**
   - Schedule: -
   - Interval (secs): -
6. From the "*Edit Job*" form, assign the **20100407-Firefox** job to one or more hosts from the available list. Click on the Update button to save the form contents.
   - Use Draft – leave unchecked
   - Schedule – leave as "-- None --"
   - Internal (secs) – leave blank
   - Disabled – leave unchecked
   - Prerequisite – leave as "—None –"
7. Select the desired Contact for job notification and click on the Subscribe button.

Example – Microsoft Installer (MSI) Software Removal Configuration

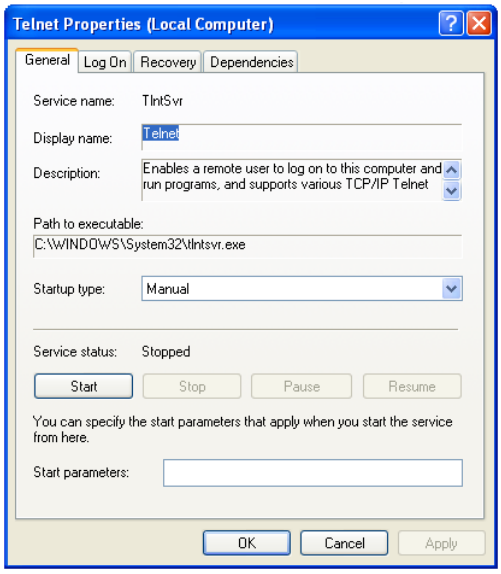




Example of a Job – Service Control (Windows)

As an example we will create a job to START the TELNET service on a Windows computer. The TELNET service is normally DISABLED and to start it, the service needs to be configured to MANUALLY start. The following sample provides an overview of creating and executing Service Control Job on Windows:

1. From the "*Scripts*" tab, create a new service control script.
   - Name: **Telnet service**
   - Description: **start service for remote connection testing**
   - Script Type: **Service Control**
2. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
3. It is necessary to determine *the Service Name* of the service to be controlled as it is recorded in Microsoft Management Console Service Snap-in below. The *Service Name* will be used below as the Service Name in the Script Content. For the Telnet service the name is recorded as "*TlntSrv*" (case sensitive).

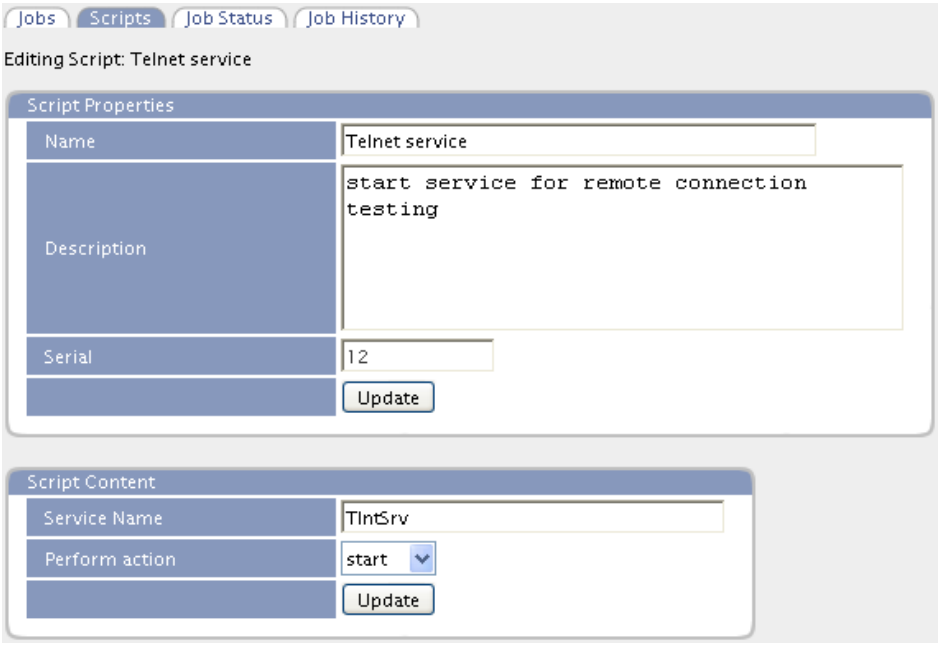


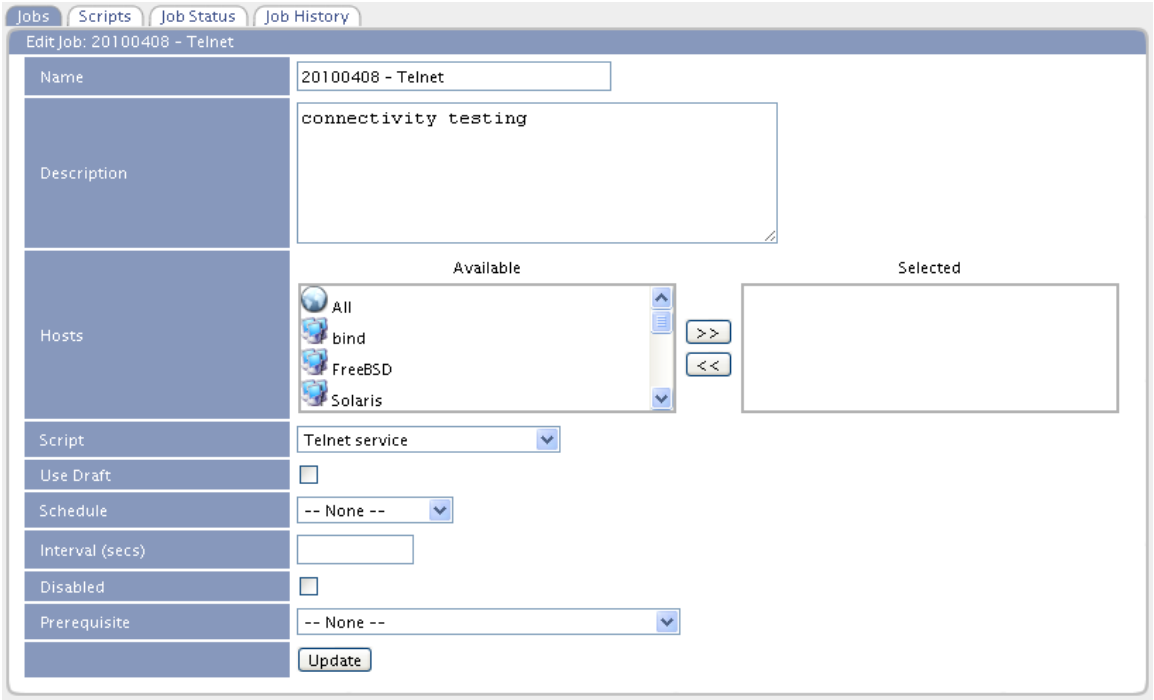
4. The next step is to complete the "*Script Content*" form and click the Update button once done:
   - Service Name: **TlntSrv**
   - Perform Action: **start**
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100408-Telnet**
   - Description: **connectivity testing**
   - Script: **Telnet service**
   - Schedule: -
   - Interval (secs): -
6. From the "*Edit Job*" form, assign the **20100408-Telnet** job to one or more hosts from the available list. Click on the Update button to save the form contents.

- Use Draft – leave unchecked
- Schedule – leave as “-- None --“
- Internal (secs) – leave blank
- Disabled – leave unchecked
- Prerequisite – leave as “—None –“

7. Select the desired Contact for job notification and click on the Subscribe button.

Example – Service Control (Windows)



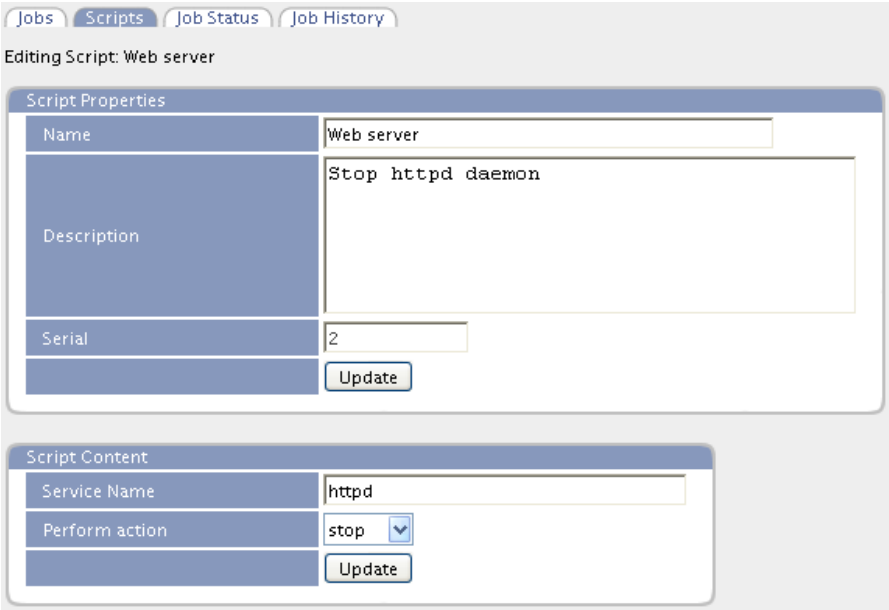


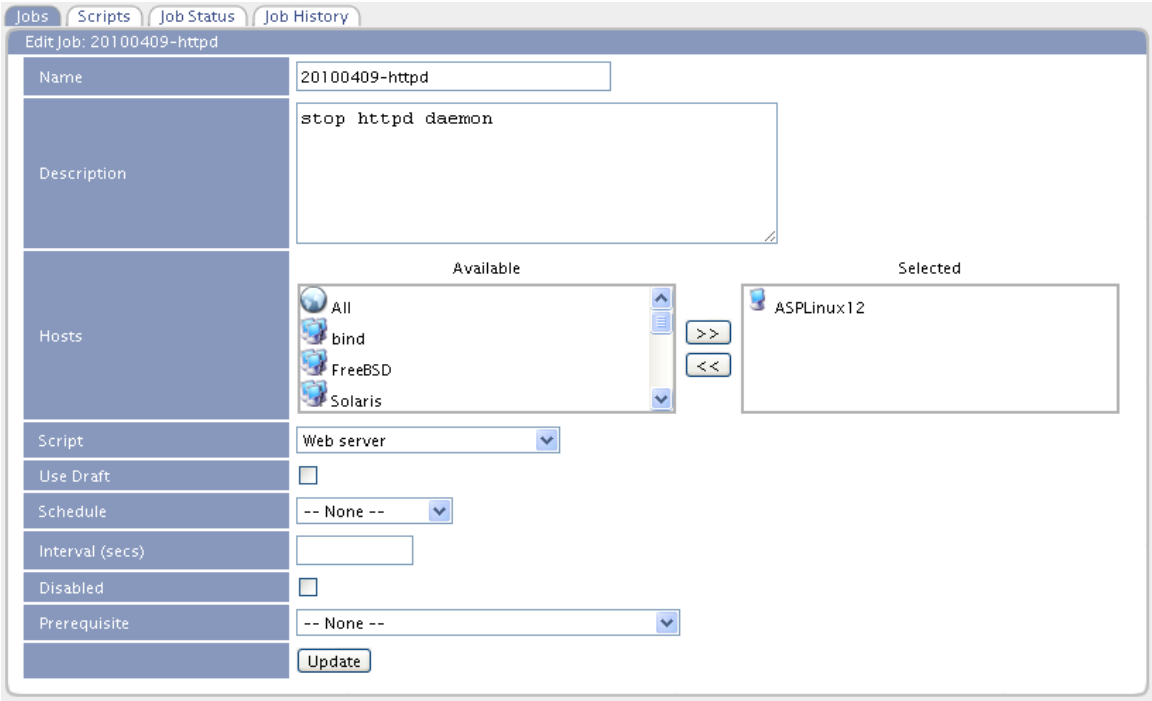
Example of a Job – Service Control (Linux)

As an example we will create a job to STOP a web server (HTTPD) on a Linux computer.

1. From the "*Scripts*" tab, create a new service control script.
   - Name: **Web server**
   - Description: **stop httpd**
   - Script Type: **Service Control**
2. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
3. The web server daemon name (init script) on the particular system used for the example is *httpd.*
4. The next step is to complete the "*Script Content*" form and click the Update button once done:
   - Service Name: **httpd**
   - Perform Action: **stop**
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100409-httpd**
   - Description: **stop httpd daemon**
   - Script: **Web server**
   - Schedule: -
   - Interval (secs): -
6. From the "*Edit Job*" form, assign the **20100409-httpd** job to one or more hosts from the available list. Click on the Update button to save the form contents.
   - Use Draft – leave unchecked
   - Schedule – leave as "-- None --"
   - Internal (secs) – leave blank
   - Disabled – leave unchecked
   - Prerequisite – leave as "—None –"
7. Select the desired Contact for job notification and click on the Subscribe button.

Example – Service Control (Linux)



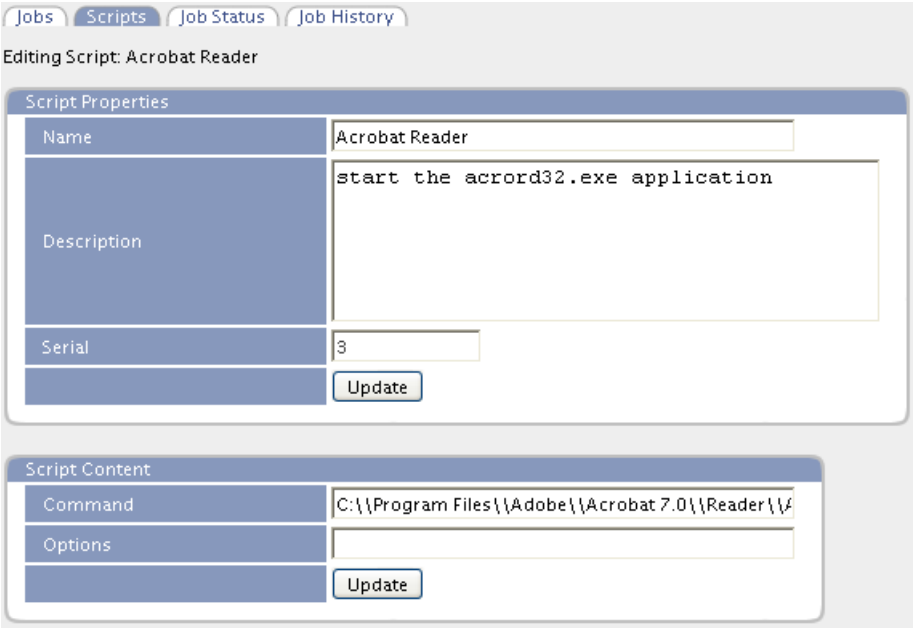


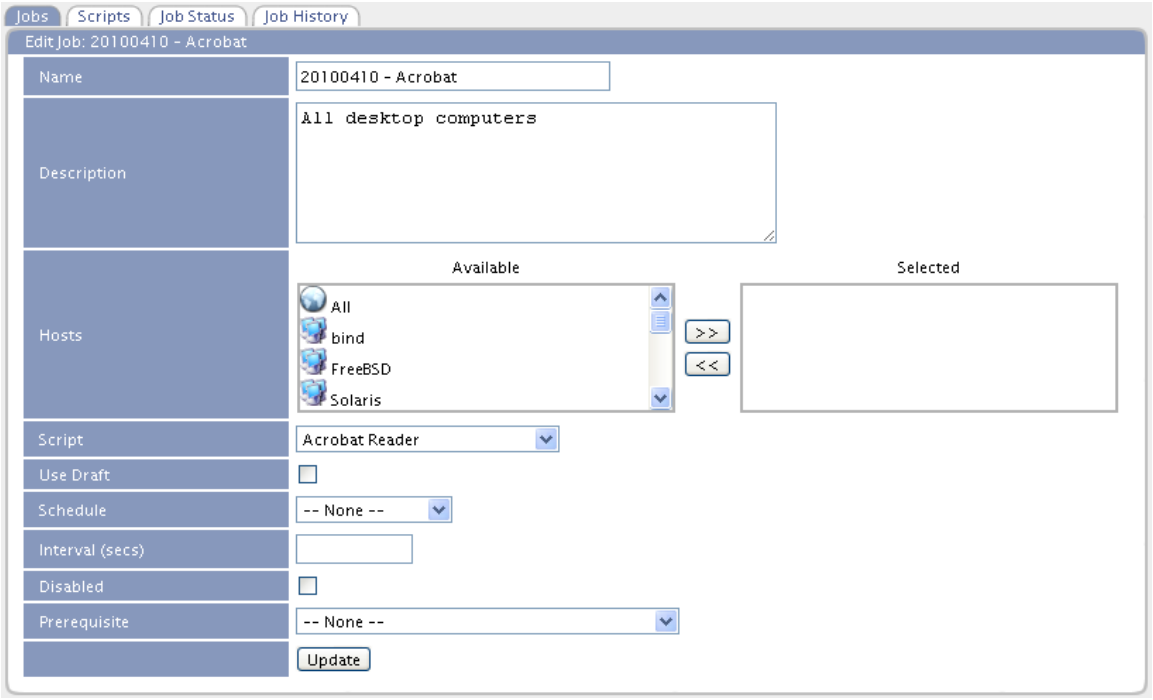
Example of a Job – Process Start (Windows)

As an example we will create a job to remotely *Start* a *Process* (application) on a Windows computer. In our simple example the job starts the Adobe Acrobat Reader Windows application on a remote Windows computer. It should be noted that the started "acroRd32.exe" process is visible in Task Manager, though it does not appear on the Desktop as it is running in the security context of the System and not the logged-in user. The following sample provides an overview of creating and executing a Process Start Job for Windows:

1. From the "*Scripts*" tab, create a new Process Start script.
   - Name: **Acrobat Reader**
   - Description: **start the acrord32.exe application**
   - Script Type: **Process Start**
2. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
3. The fully qualified path to the application must be known as it needs to be entered in *Script Content* form.
4. The next step is to complete the "*Script Content*" form and click the Update button once done:
   - Command: **c:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe**
   - Options: **-**
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100410-Acrobat**
   - Description: **All desktop computers**
   - Script: **Launch Notepad**
   - Schedule: -
   - Interval (secs): -
6. From the "*Edit Job*" form, assign the **20100410- Acrobat** job to one or more hosts from the available list. Click on the *Update* button to save the form contents.
   - Use Draft – leave unchecked
   - Schedule – leave as "-- None --"
   - Internal (secs) – leave blank
   - Disabled – leave unchecked
   - Prerequisite – leave as "—None –"
7. Select the desired Contact for job notification and click on the Subscribe button.

Example – Process Start (Windows)



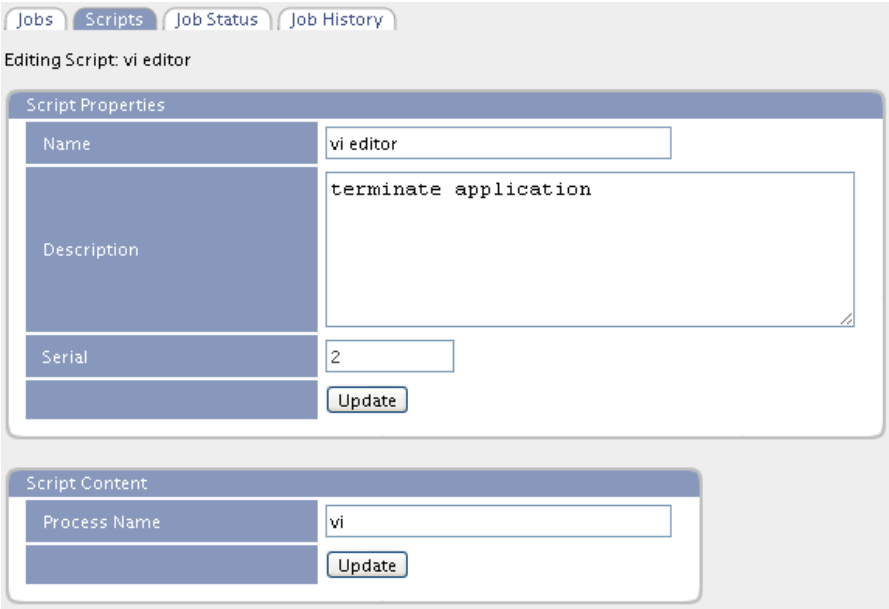


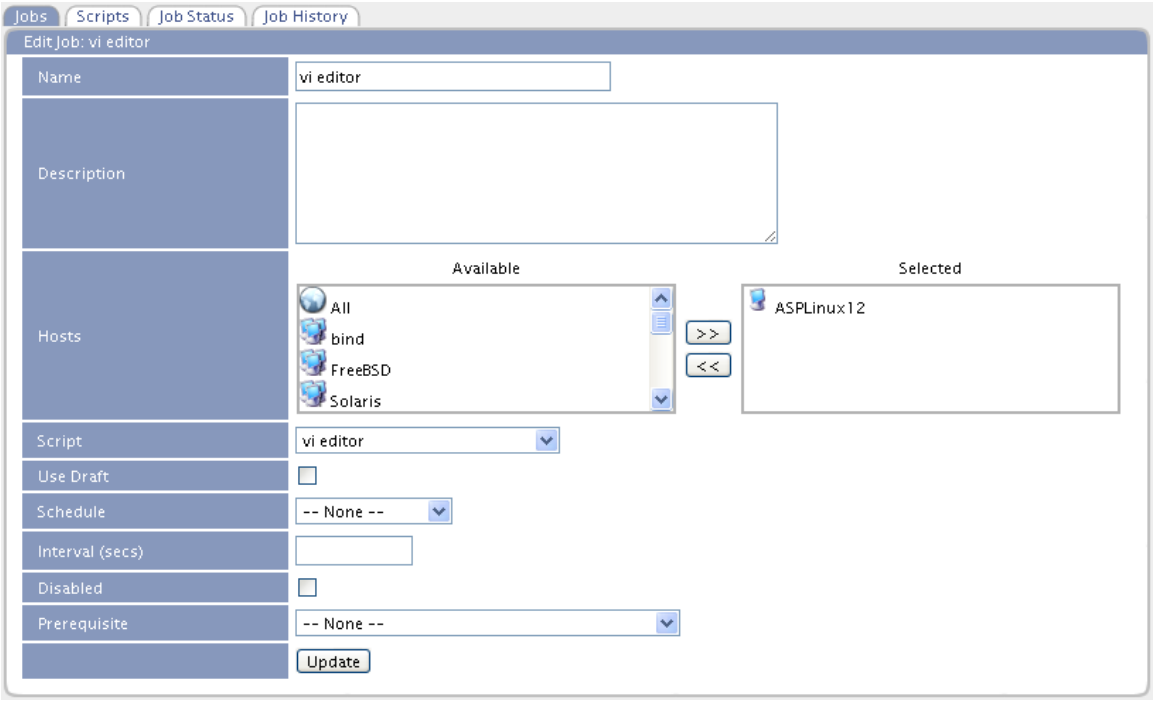
Example of a Job – Process Kill (Linux)

As an example we will create a job to remotely Kill a *Process* (application) on a Linux computer. In our simple example we terminate the "Vi" editor on a remote Linux computer. The following sample provides an overview of creating and executing a Process Kill Job for Linux:

1. From the "*Scripts*" tab, create a new Process Kill script.
   - Name: **Vi Editor**
   - Description: **kill the vi editor application**
   - Script Type: **Process Kill**
2. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
3. The application name to be terminated (killed) must be known as it needs to be entered in *Script Content* form.
4. The next step is to complete the "*Script Content*" form and click the Update button once done:
   - Process Name: **vi**
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100411-Vi**
   - Description: **All desktop computers**
   - Script: **Vi Editor**
   - Schedule: -
   - Interval (secs): -
6. From the "*Edit Job*" form, assign the **20100411- Vi** job to one or more hosts from the available list. Click on the *Update* button to save the form contents.
   - Use Draft – leave unchecked
   - Schedule – leave as "-- None --"
   - Internal (secs) – leave blank
   - Disabled – leave unchecked
   - Prerequisite – leave as "—None –"
7. Select the desired Contact for job notification and click on the Subscribe button.

Example – Process Kill (Linux)



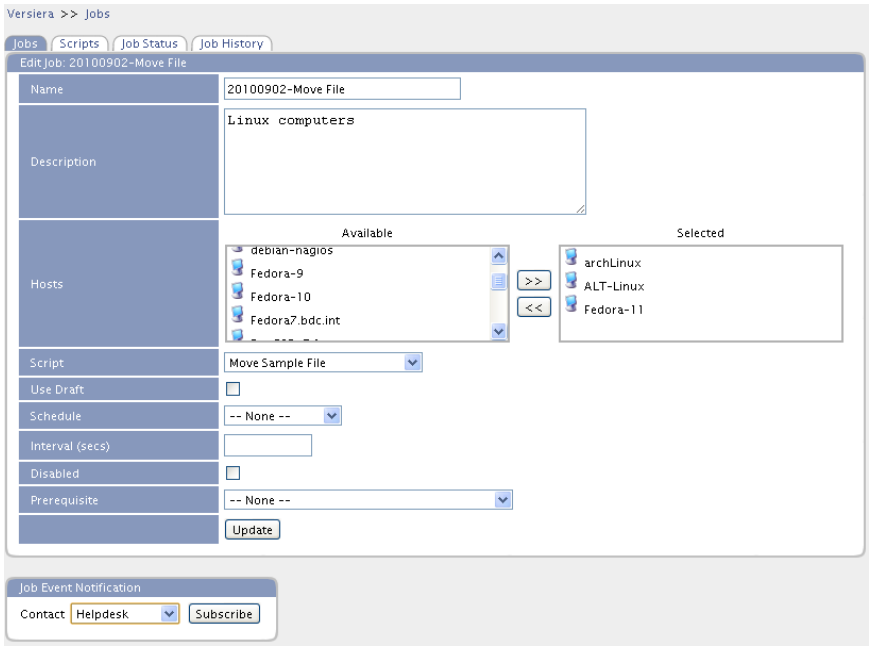


Example of a Job – Script - Remote Host Command (Linux)

As an example we will create a job to remotely execute a command on a Linux computer. In our simple example we move a file from one directory to another. The following sample provides an overview of creating and executing a Script Job for Linux:

1. From the "*Scripts*" tab, create a new Script.
   - Name: **Move Sample File**
   - Description: **Move the sample.txt file from user directory to /tmp**
   - Script Type: **Script**
2. The "*Script Properties*" form will be presented and include the above entered information. If the form needs to be revised, make the necessary changes and click on the *Update* button. The *Serial* number will increment by 1.
3. In the Body section of the Script Content enter the following command (note – directory paths must be absolute):
   - Body: **execl { /bin/mv /root/test.txt /tmp }**
4. Next click on the Update button in the Script Content form to save the script.
5. From the "*Jobs*" tab, create a new job:
   - Name: **20100902-Move File**
   - Description: **Linux computers**
   - Script: **Move Sample File**
   - Schedule: -
6. Interval (secs):
7. From the "*Edit Job*" form, assign the **20100902-Move File** job to one or more hosts from the available list. Click on the *Update* button to save the form contents.
   - Use Draft – leave unchecked
   - Schedule – leave as "-- None --"
   - Internal (secs) – leave blank
   - Disabled – leave unchecked
   - Prerequisite – leave as "—None –"
8. Select the desired Contact for job notification and click on the Subscribe button.

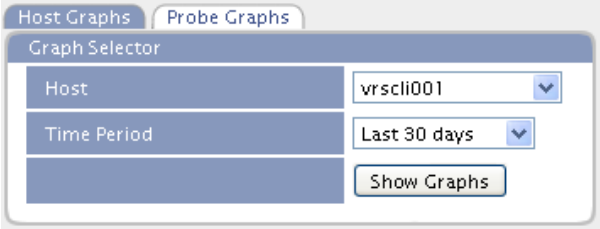
Example – Script - Remote Host Command (Linux)



Graphs

Graphs are used for visualization of host and service probe performance information over a period of time. Using the interface one can select a desired host and the time interval for display in the graphs. The respective host performance graphs will be drawn including information for load, memory, storage, and network statistics.

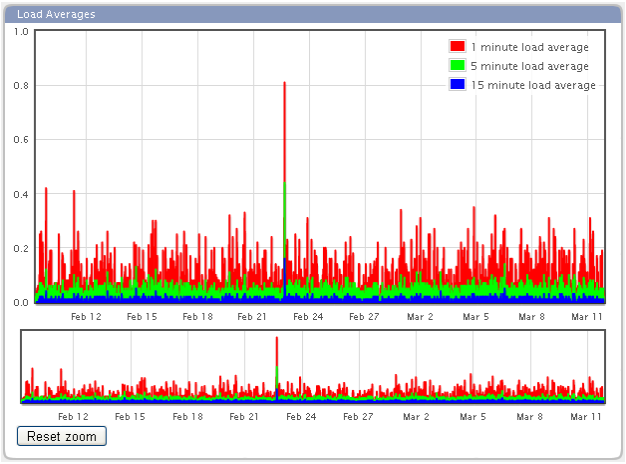
Host Graphs



Host: a drop-down box listing the available Service Probes that have been configured

Time Period: the button to generate the respective probe graph

Sample Host Graph

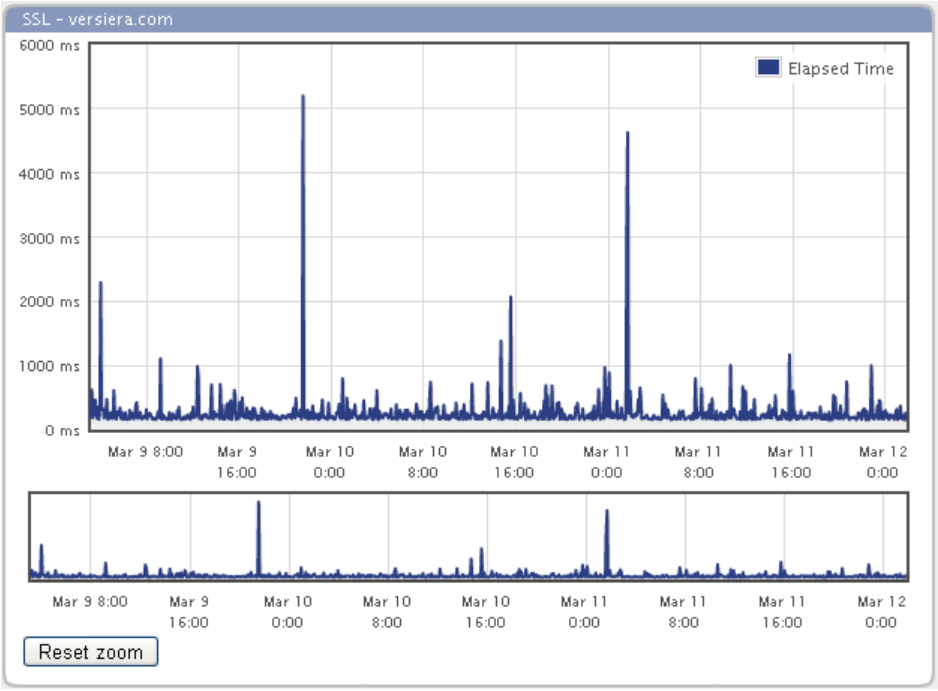


Probe Graphs

Select Probe: a drop-down box listing the available Service Probes that have been configured

Show Graphs: the button to generate the respective probe graph

Sample Probe Graph



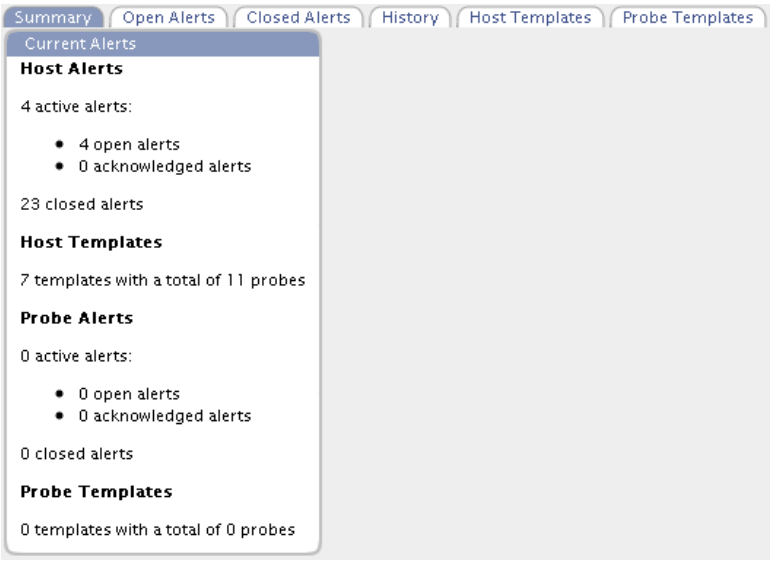
Note - Using the mouse to select an area from either of the graphs the user can zoom-in to values for a particular time interval.

Monitoring

Monitoring is used for real-time processing of data received from Versiera agents installed on the hosts or data obtained by monitoring probes. Templates are used to group one or more monitoring rules and to apply them to managed hosts or to probes monitoring application services. When one or more rules are matched, the monitoring system generates notification alerts to communicate operational levels and any degradation of services to operational staff.

Summary Tab

The "*Summary*" tab provides brief details on the number of alerts, templates and respective probes.



Monitoring Host Probes

Connections: rules for establishing the degraded and critical levels for the number of connections to a given server communication port (i.e. 22, 80, 443, 445, 3389, etc.). This enables the ability to trigger notification alerts and audit for load and remote administration. As an example, monitoring of one or more SSH or RDP connections or approaching a maximum connection load to a database.

Disk Space: rules for establishing the degraded and critical levels of available disk space remaining for storage of data.

Host Check-in: rules for establishing the degraded and critical time interval in seconds for a host that has not checked-in to Versiera Management Console. Monitoring in Versiera is passive and this rule enables alerting when Versiera Management Console has not received communications from the agent for a period of time.

Host Up: rules for establishing the degraded and critical time interval in seconds for the number of seconds a host has been up and running. The rule is useful to alert administrators when a host has recently restarted.

Load Average: rules for establishing the degraded and critical levels for the host processing load

Memory Free: rules for establishing the degraded and critical levels for the amount of available physical memory of a host.

Memory Usage: rules for establishing the degraded and critical levels for the amount of used physical memory of a host.

Process: rules for establishing the degraded and critical levels for whether processes are running or absent on hosts.

Process Count: rules for establishing the degraded and critical levels for the number of process instances on hosts. For example, monitoring the number of Apache web server processes.

Time Sync: rules for establishing the degraded and critical levels for the time interval in seconds the time (host's clock) on a host may be out of synchronization with the Versiera Management Console.

Uptime: rules for establishing the degraded and critical levels for the length of time a host has been operational. For example, to alert administrators when a host has restarted and has a low uptime.

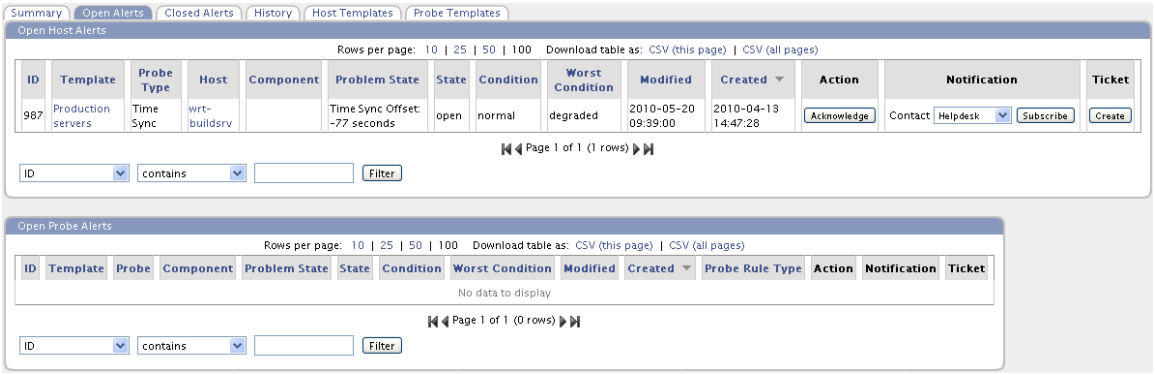
VM Usage: rules for establishing the degraded and critical levels for the amount of virtual memory used by a host.

Monitoring Service Probes

Elapsed Time: rules for establishing the degraded and critical time in milliseconds for a given service probe to complete

Open Alerts Tab

The entries in this table are automatically generated by the monitoring probes checking state information as it is received from host agents against probe rule sets. The Open Alerts table data provides the following information about issues that occurred during monitoring period:



ID – the alert identifier assigned by the system

Template – the name of the template which contains the probe and associated rules

Probe Type – the type of probe which signaled the alert

Host – the name of the host associated with the open alert

Component – the components are associated with certain probe types such as *Disk Space* and represent specific storage drive paths or mount points

Problem State – the details of the probe value which triggered the alert and its current value

State – the state of the alert as either Open, Acknowledged or Closed

Condition – the current state of the monitoring probe as one of Normal, Warning or Critical

Worst Condition – the worst monitoring probe condition as one of Warning or Critical

Modified – the date/time the open alert was last modified

Created – the date/time the open alert was created in the system

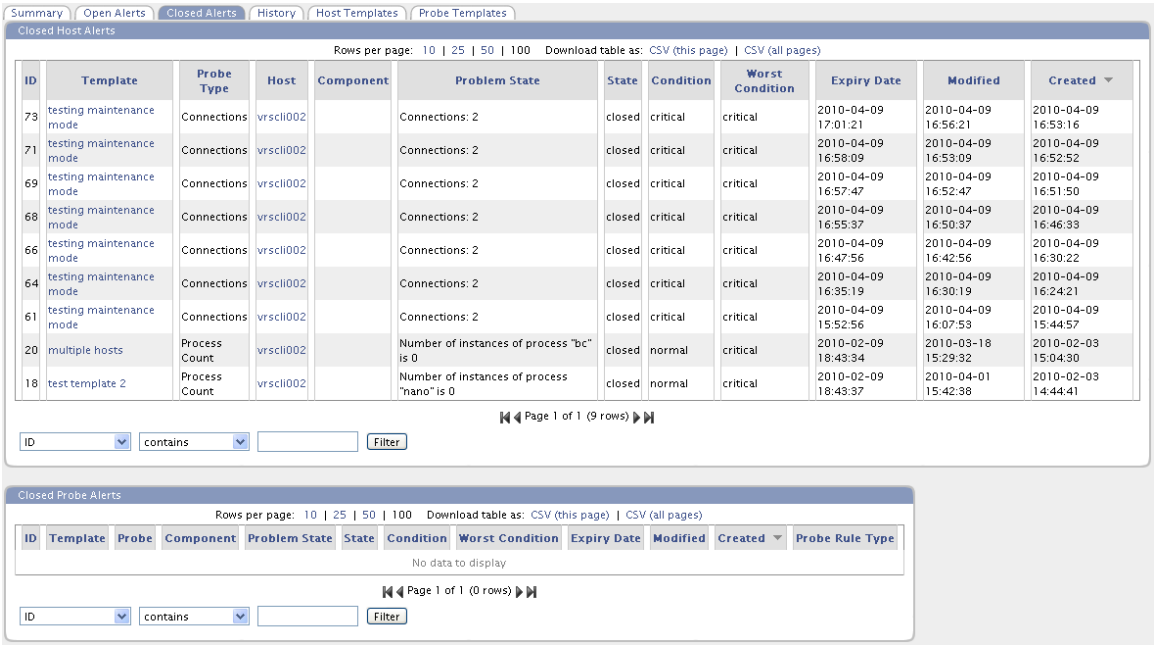
Action – the buttons for Acknowledging and Closing the alert

Notification – the button allowing either the subscription or unsubscription of email notifications for the open alert. The Subscription rules, found in the Administrative Settings, may automatically enroll the Versiera ID associated email address for receipt of host open alert notifications.

Ticket – the button for creating a ticket based on the open alert details for the purpose of documenting the problem and/or its resolution.

Closed Alerts Tab

A table row associated with an open alert that is acknowledged and subsequently closed. The table row is subsequently moved to the Closed Alerts table and is automatically removed from that section after a 5 minute window. The open alerts table data provides the following information about host and service probe monitoring issues:



ID – the alert identifier assigned by the system

Template – the template which contains the probe and associated rules

Probe Type – the type of probe which signaled the alert

Host – the name of the host associated with the open alert

Component – the components are associated with certain probe types such as *Disk Space* and represent specific storage drives or mount points

Problem State – the details of the probe value triggering the alert and its present state

State – the state of the alert as either Open, Acknowledged or Closed

Condition – the current state of the monitoring probe as one of Normal, Warning or Critical

Worst Condition – the worst monitoring probe condition as one of Warning or Critical

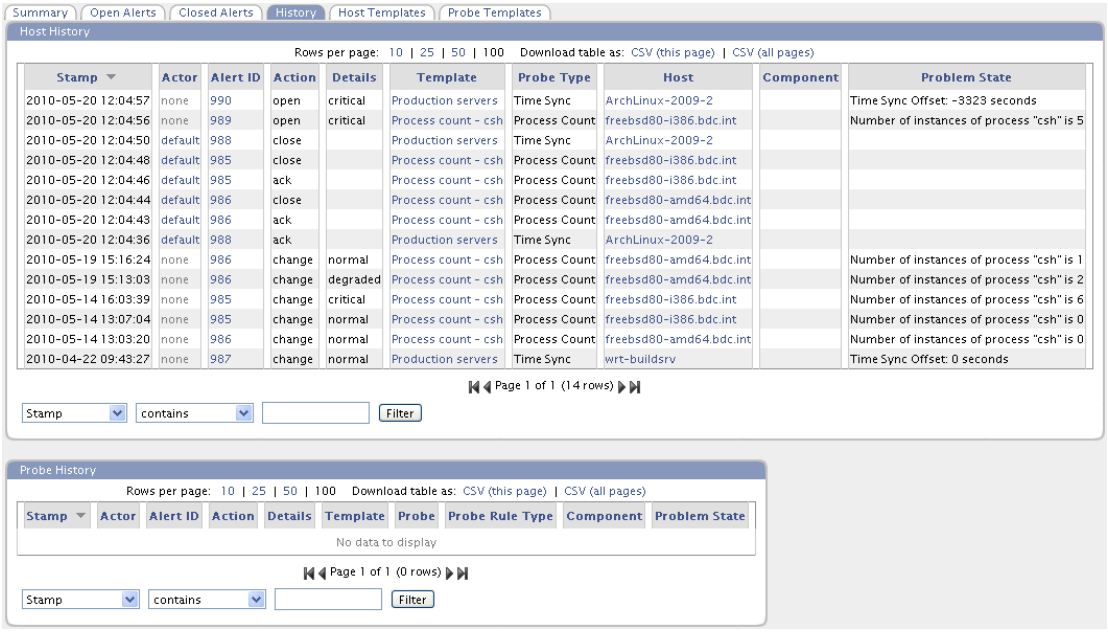
Expiry Date – the date/time when the closed alert will be removed from the table

Modified – the date/time the open alert was last modified

Created – the date/time the open alert was created in the system

History Tab

The alert history table data provides the following information about host alerts:



Stamp – the date/time of a particular entry

Actor – the Versiera ID, if any, associated with the alert action or event

Alert ID – the alert identifier assigned by the system

Action – the action by Versiera or a user (Open, Change, Acknowledge, Close, Expire)

Details – the alert level (normal, degraded, critical)

Template – the name of the template which contains the probe and associated rules

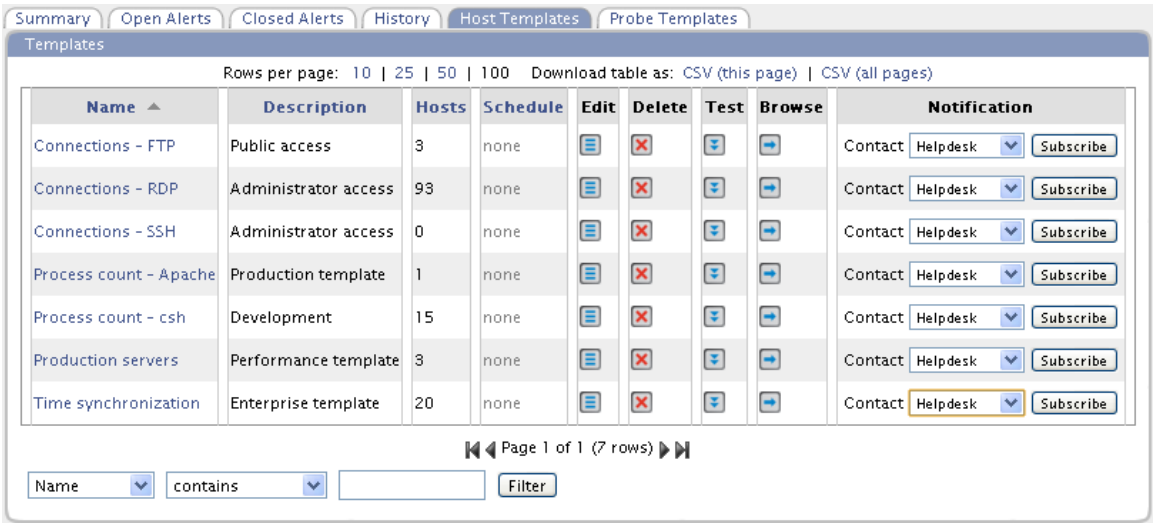
Probe Type – the type of probe which signaled the alert

Host – the name of the host associated with the open alert

Component – the components are associated with certain probe types such as Storage and represent specific storage drives or mount points

Problem State – the details of the probe value triggering the alert and its present state

Host Templates Tab



The Templates Tab provides the facility for creating or editing monitoring template models:

Name – name assigned to a particular template

Description – template description or its intended purpose

Hosts – the number of hosts that are monitored with the use of a given template

Schedule – (option) any monitoring schedule; if none is assigned then the template is always used

Edit – the button for editing existing templates

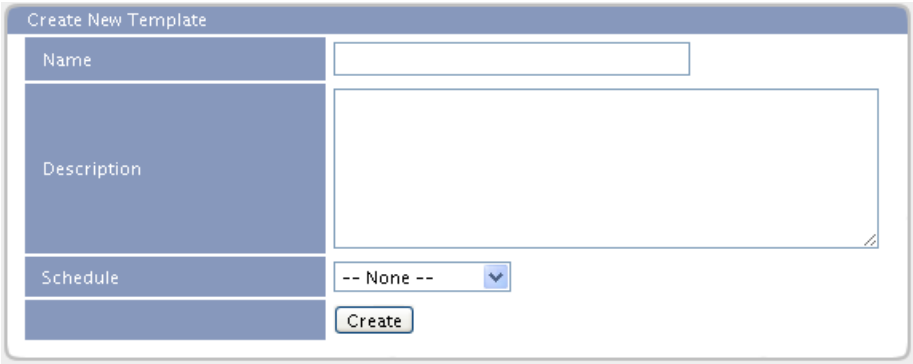
Delete – the button for removal of a monitoring template

Test – the button for performing a test of a template against particular hosts

Browse – the button for viewing the status of a particular template using existing host data

Notification – (optional) the button to subscribe a recipient to whom subscription notifications are sent

Create New Template Form

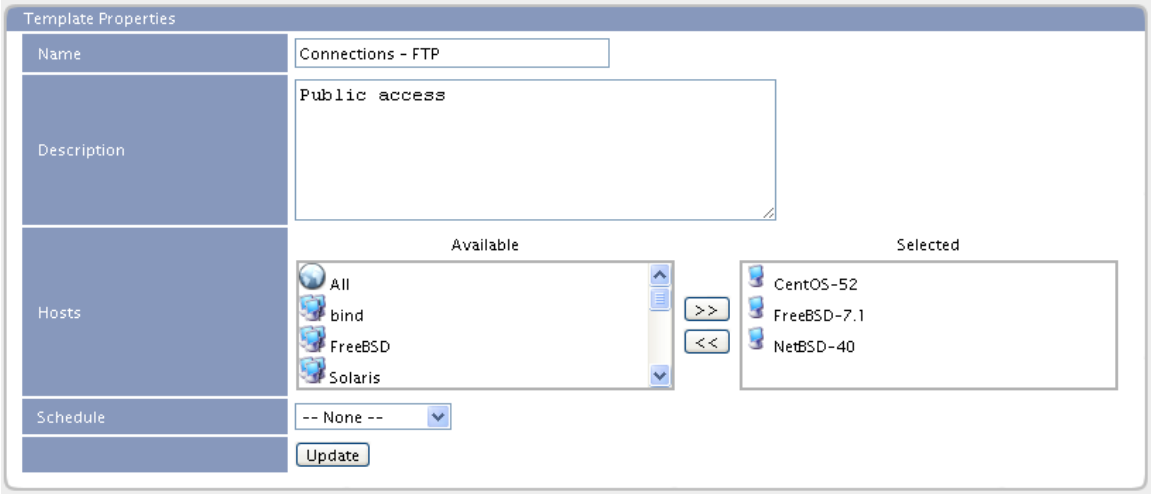


Name – the name to be assigned to the template

Description – information or details about the template or its purpose

Schedule – an optional schedule to be used with the template. In the absence of a schedule "--None--", the template will be used all the time

Template Properties Form



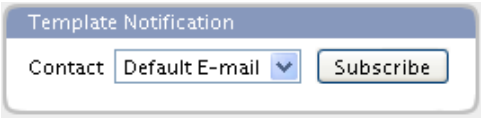
Name – the name assigned to the template

Description – information or details about the template or its purpose

Hosts – any hosts or host groups that have been selected for monitoring with the template

Schedule – an optional schedule to be used with the template. In the absence of a schedule "--None--", the template will be used all the time

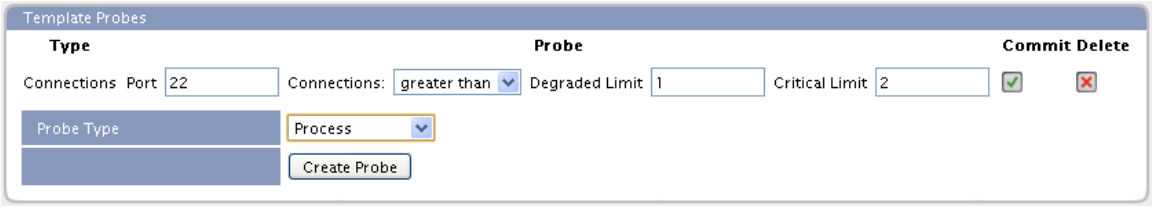
Template Notification Form



Contact – drop-down box to select a Contact for email notification subscription

Subscribe – the button to activate the subscription

Template Probes Form



Type – one or more probe types assigned to the template

Probe – probes that have been created and assigned to the template. Each probe may have respective values that need to be entered and committed.

Commit – button to apply the entered values to the respective probe

Delete – button to delete the particular probe form the template

Probe Type – adding one or more probe type to a template

Create Probe – button to add the selected probe and its associated values to the monitoring template.

Ticketing

Ticketing is used for creating and managing workflow of operational tickets, problem resolution and documentation of host systems. Tickets are manually generated or created from a queue of monitoring alerts that automatically fill-in ticket fields with the alert information.

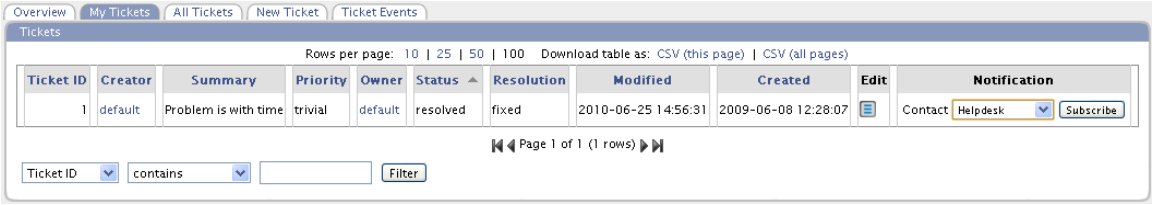
Overview Tab

The Overview tab provides brief detail statistics showing the number of open and resolved tickets.

Sample Ticket

My Tickets Tab

The My Tickets table data provides details for the tickets assigned to the currently signed-on Versiera ID and include the following information:



Ticket ID – ticket identification number. Each new ticket may not have a sequential numeric value from the previous

Creator – the Versiera ID that generated the particular ticket

Summary – a brief description of the ticket subject matter

Priority – priority assigned to the ticket (Critical, Major, Minor, Trivial)

Owner – the Versiera ID to whom the ticket has been assigned

Status – the current ticket status; assigned or resolved

Resolution – the ticket resolution state (Fixed, Invalid, Will Not Fix, and Not Found)

Modified – the date/time the ticket was last updated

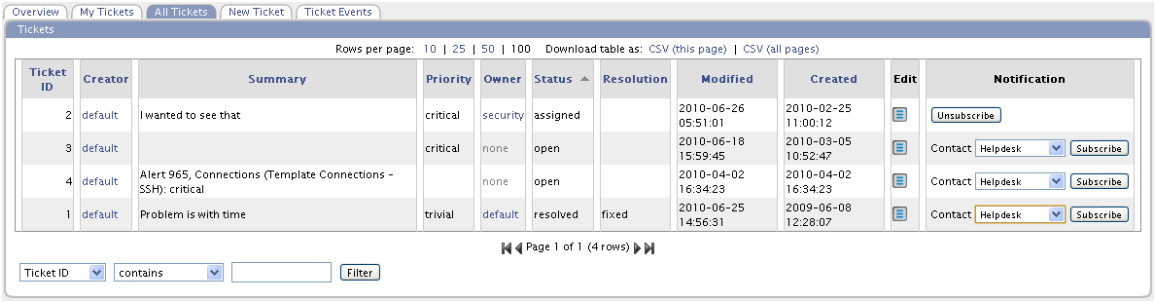
Created – the date/time the ticket was created

Edit – button allowing the review and update of respective tickets

Notification – drop-down box to select contact for email notifications when subscribed to ticket updates

All Tickets Tab

The All Tickets table data provides details for all tickets and their respective Versiera IDs (creator/owner):



ID – ticket identification number, each new ticket may not have a sequential numeric value from the previous

Creator – the Versiera ID that generated the particular ticket

Summary – a brief description of the ticket subject matter

Priority – priority assigned to the ticket (Critical, Major, Minor, Trivial)

Owner – the Versiera ID to whom the ticket has been assigned

Status – the current ticket status; assigned or resolved

Resolution – the ticket resolution is one of; Fixed, Invalid, Will Not Fix, and Not Found

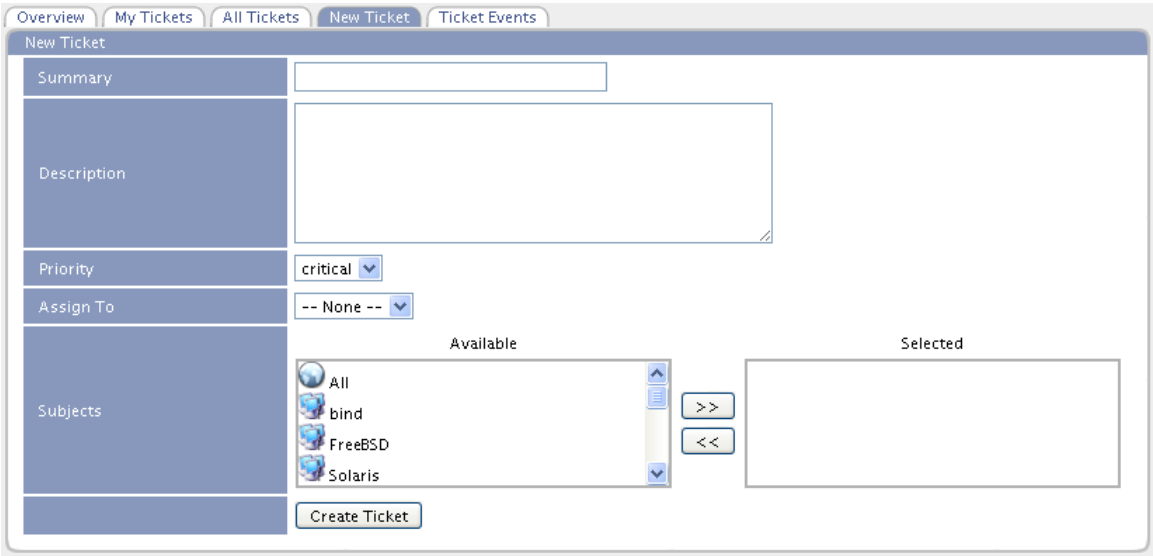
Modified – the date/time the ticket was last updated

Created – the date/time the ticket was created

Edit – button allowing the review and update of respective tickets

Notification – drop-down box to select contact for email notifications when subscribed to ticket updates

New Ticket Form



Summary – brief title or summary for ticket

Description – additional information and details of issue to be addressed

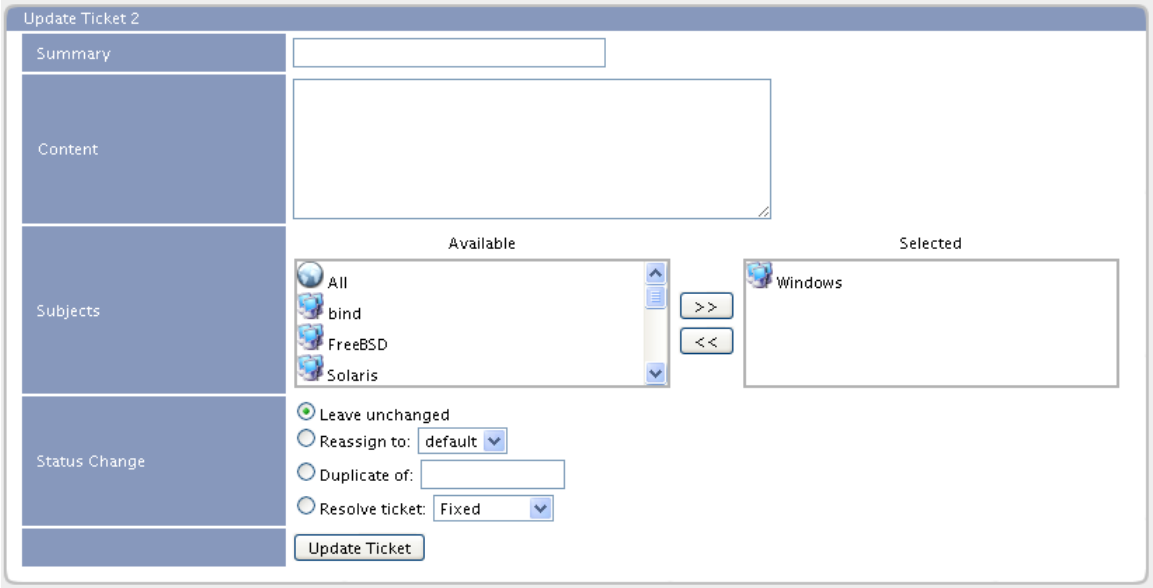
Priority – priority assigned to the ticket (Critical, Major, Minor, Trivial)

Assigned To – the Versiera ID assigned the task of working on the ticket

Subjects– one or more host systems (including groups and All Hosts group) can be associated with a given ticket.

Note – once a ticket is created, to receive emails concerning ticket status updates, editing the ticket and ***enable*** Subscription to the ticket.

Update Ticket Form



Summary – make changes to the ticket summary

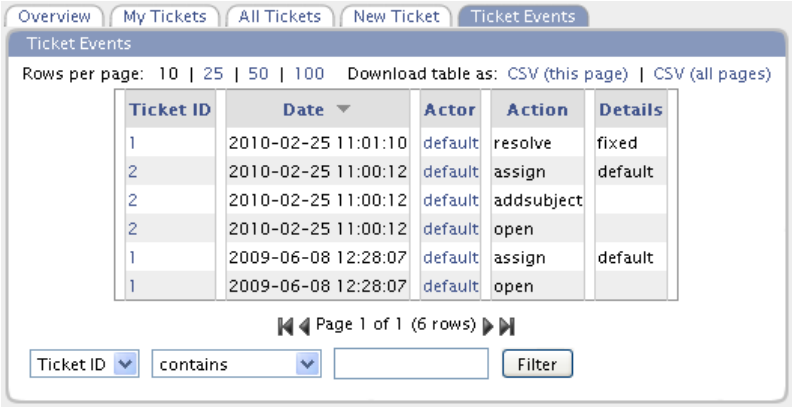
Content – information to be entered detailing ticket resolution procedure, updates, status, and other relevant information

Subjects– add or remove hosts and groups to the ticket.

Status Change – update ticket information, reassign to other operators and update ticket status

Ticket Events Tab

The Ticket Events tab provides the following information:



Ticket ID – ticket identification number

Date – the date of the respective ticket event

Actor – the Versiera ID associated with the ticket event

Action – the change in the ticket

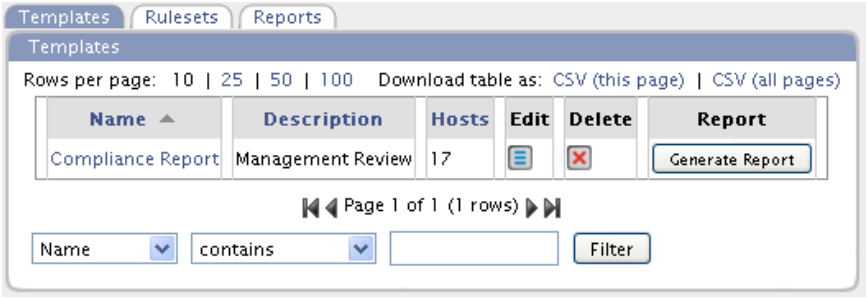
Details – any additional information associated with the ticket event

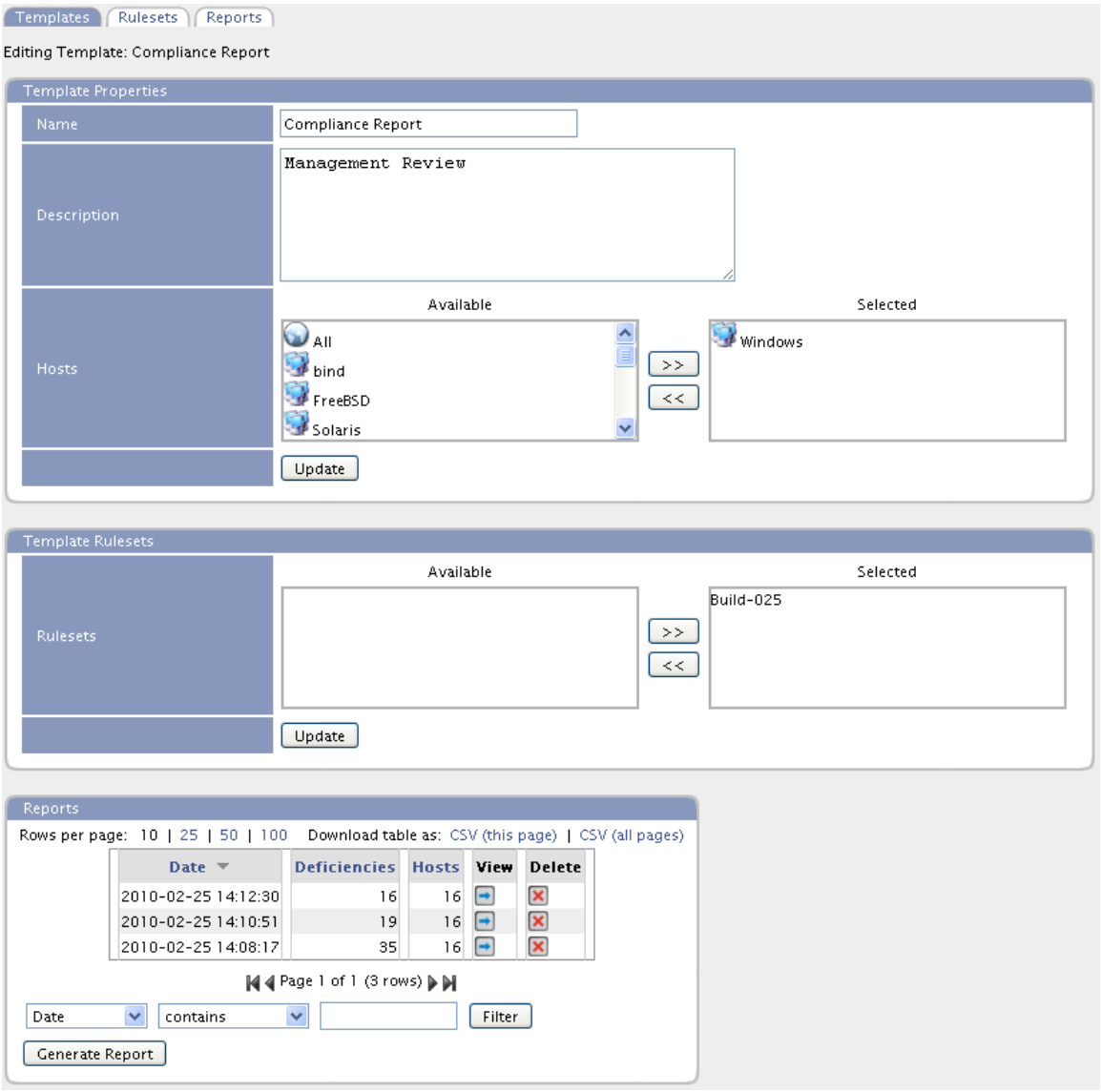
Compliance

The Compliance section enables administrators to generate a template, based on one or more rule sets, which describe or model a corporate configuration standard for host systems. The templates can then be applied to one or more hosts and the tracking of deviations from the corporate standards.

Templates Tab

A Compliance Template represents one or more rule sets that model a configuration standard for an enterprise. One such rule set may represent a corporate standard for installed software. Once one or more rule sets have been generated, they can then be applied to a template to represent a corporate standard for workstations or servers. A template must be applied to one or more computers in order to generate reports that show deviations from the corporate standards.



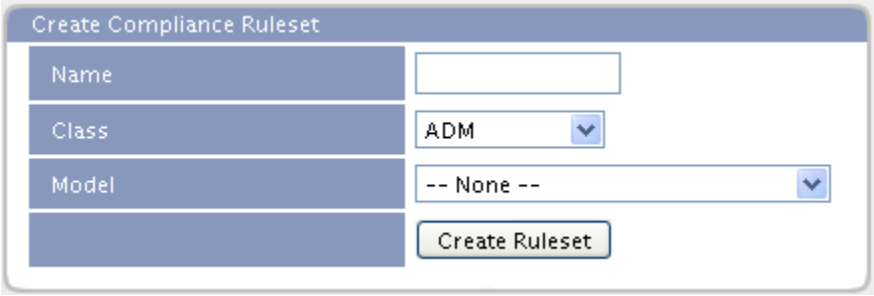

Templates
Rulesets
Reports
Editing Template: Compliance Report
Template Properties
Name
Compliance Report
Description
Management Review
Hosts
Available
Selected
All
bind
FreeBSD
Solaris
Windows
>>
<<
Update
Template Rulesets
Rulesets
Available
Selected
Build-025
>>
<<
Update
Reports
Rows per page: 10 | 25 | 50 | 100 Download table as: CSV (this page) | CSV (all pages)
Date
Deficiencies
Hosts
View
Delete
2010-02-25 14:12:30 16 16
2010-02-25 14:10:51 19 16
2010-02-25 14:08:17 35 16
Page 1 of 1 (3 rows)
Date
contains
Filter
Generate Report

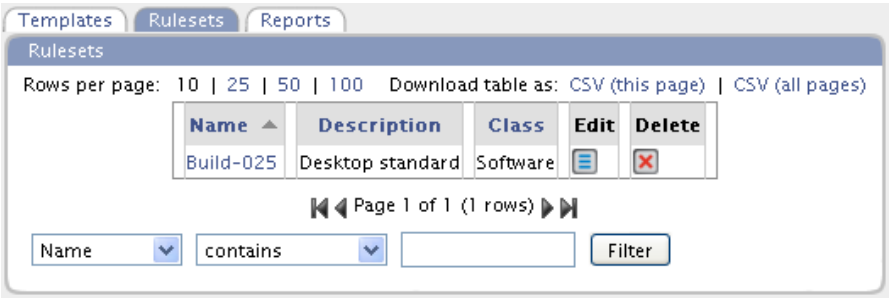
Rulesets Tab

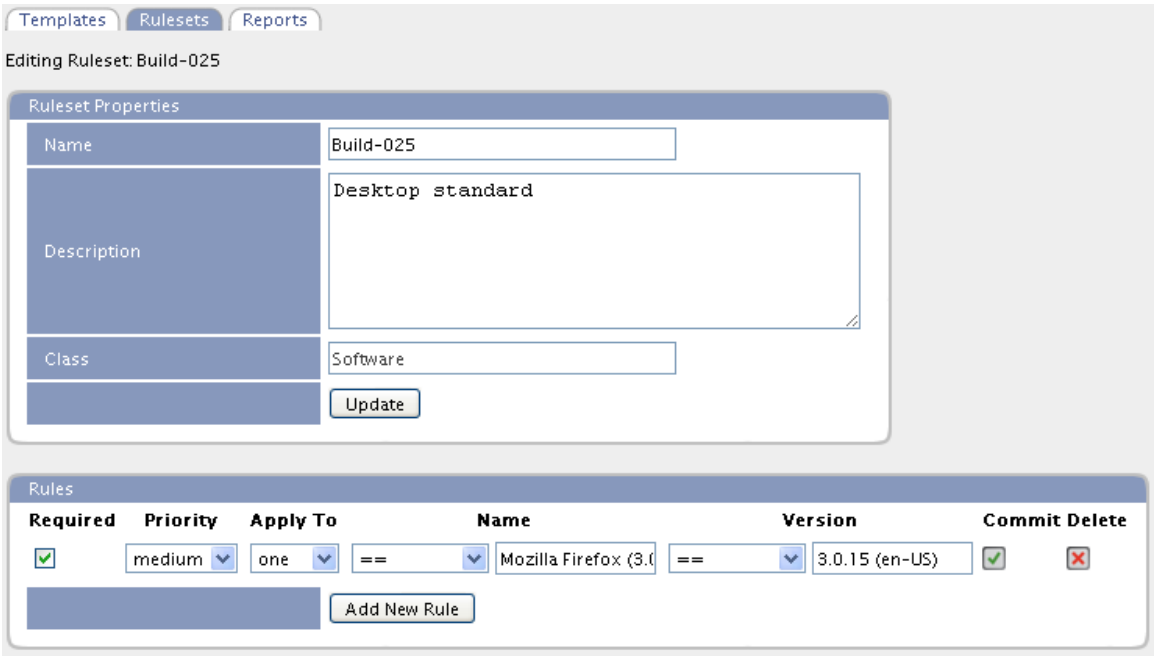
The process of generating rules to model/describe corporate standards can be made easier by modeling a set of given properties of an existing host already registered with Versiera. By selecting a compliance class and a registered host, Versiera will generate a set of rules that may be edited as required to publish a rule set.

Compliance Classes include:

ADM:	ability to model service programs, their listening ports/addresses and users
Agent:	ability to model Versiera agent properties
Connections:	ability to model host communications with other hosts
Groups:	ability to model host user groups
Host:	ability to model host hardware, operating system and firmware details
Software:	ability to model installed software
Users:	ability to model host account details

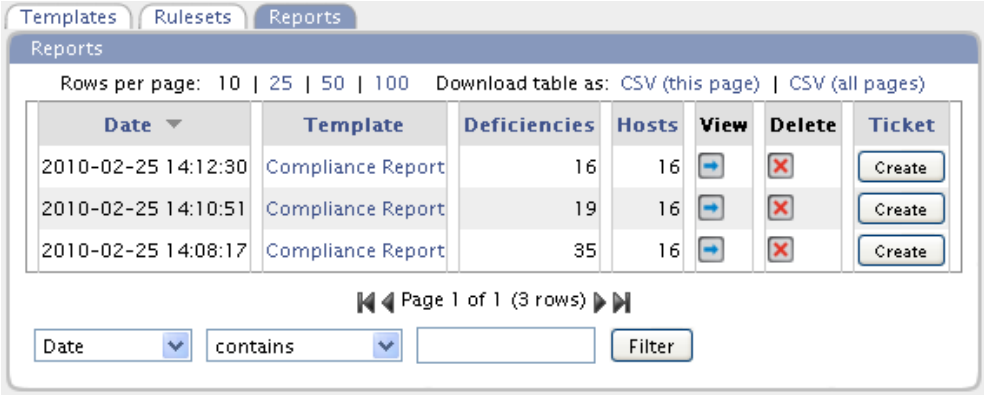


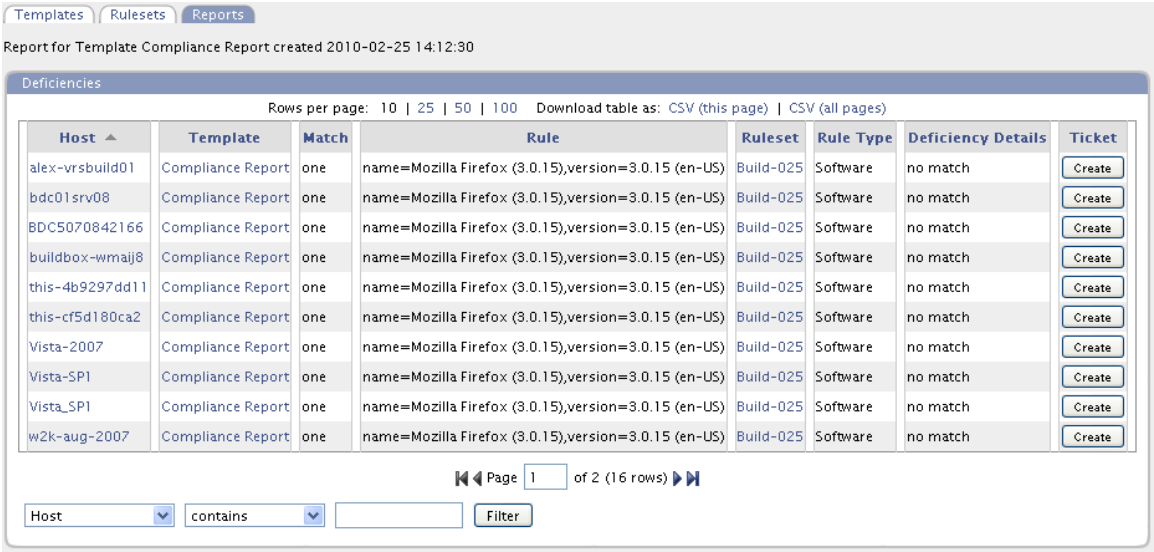



Templates
Rulesets
Reports
Editing Ruleset: Build-025
Ruleset Properties
Name
Build-025
Description
Desktop standard
Class
Software
Update
Rules
Required
Priority
Apply To
Name
Version
Commit
Delete
medium
one
==
Mozilla Firefox (3.(
==
3.0.15 (en-US)
Add New Rule

Reports Tab

The compliance reports are generated on demand and show deviations from corporate standards.

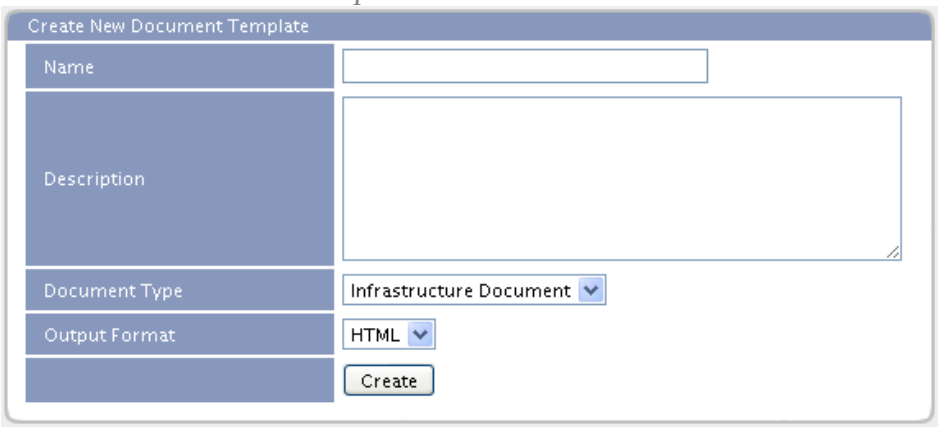




Documents

The Documents section enables administrators to generate a formal library of documents to describe their technology infrastructure. The documents can be generated in various formats to accommodate documentation requirements. In addition tools are included to document digital assets such as domain records.

Create New Document Template Form



Name - the name of the document describing what hosts it will reference

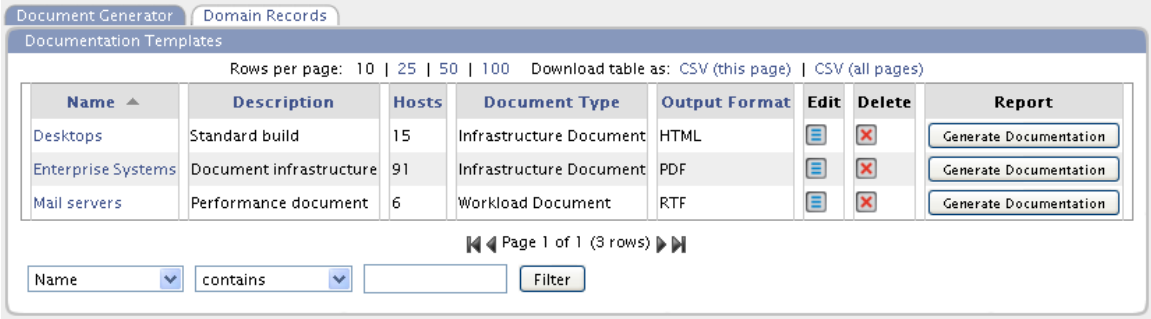
Description - the description of the document

Document Type - the type of information the document will contain referencing the hosts (Infrastructure Document, Workload Document)

Output Format - the format of the document (PDF, RTF, HTML)

Document Generator

The Document Generator tab enables Administrators to create formal documents that describe their technology, configuration and used operations. The following document types are generated:



Name – the name of the document

Description – the user entered description of the documentation template

Hosts – the number of hosts to be include in the document

Document Type – – the type of the document selected from the library of available formal documents and related information

Output Format – the format the document will be generated in

Edit – the button to update of a particular template

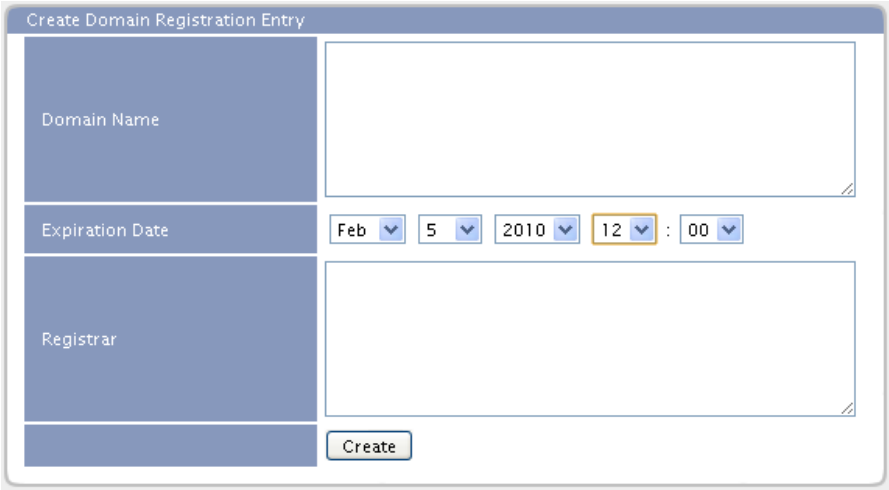
Delete – the button to remove of a particular template

Report– the button to generate a document from a template and download to the browser

Domain Records

The Domain Records tab lets administrators to manually keep records of domain name virtual asset information, their expiration dates and the associated registrars. The intention is to help administrators in documenting their digital assets and their records keeping.

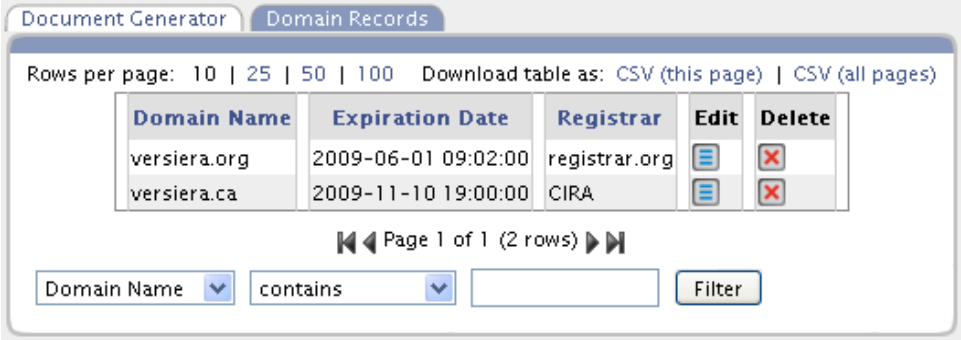
Create Domain Registration Entry Form



Domain Name – the fully qualified domain name

Expiration Date – the expiration date of the domain

Registrar – the name of the registrar with whom the domain is registered



Domain Name – the fully qualified domain name

Expiration Date – the expiration date of the domain

Registrar – the name of the registrar with whom the domain is registered

Edit – the button to update of a particular entry

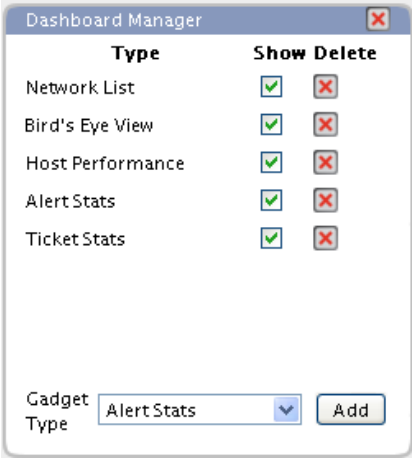
Delete – the button to remove of a particular entry

Dashboards

The Dashboard provides a set of visual aids for reviewing summary information relating to managed hosts. Versiera refers to these visual aids as gadgets, and presents each in a pseudo window. To view a large number of gadgets at once, it is suggested to use a large wide-screen display. The Dashboard screen periodically refreshes and conveniently does not timeout on user inactivity so that periodic sign-on is not required when the Dashboard is open.

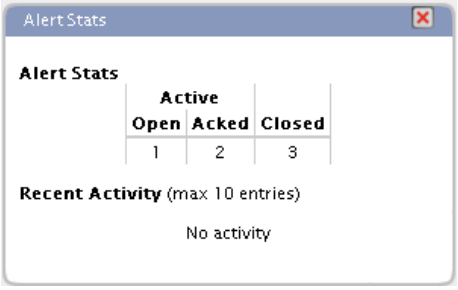
Dashboard Manager

A Dashboard Manager gadget is used to add, identify and remove available gadgets on the Dashboard.



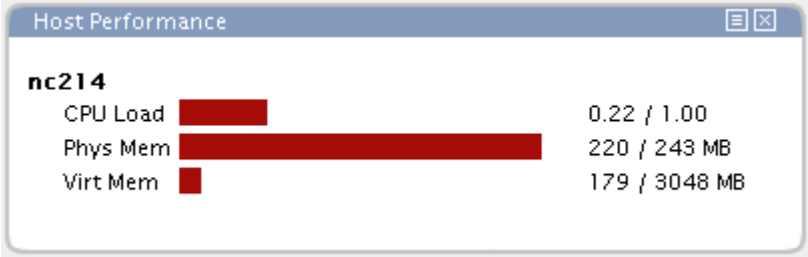
Alerts Stats Gadget

The gadget provides a statistics summary table of the alerts and alert management activity by operators.



Host Performance Gadget

The gadget provides basic host performance metrics including host CPU load, physical and virtual memory utilization. A control in the gadget title allows the selection of the particular host for which performance information should be displayed in the gadget window. Multiple Host Performance gadget windows may be displayed, each in its own window. The Dashboard Manager provides a Show checkbox that will hide/display a particular Host Performance windows when more than one are in use.

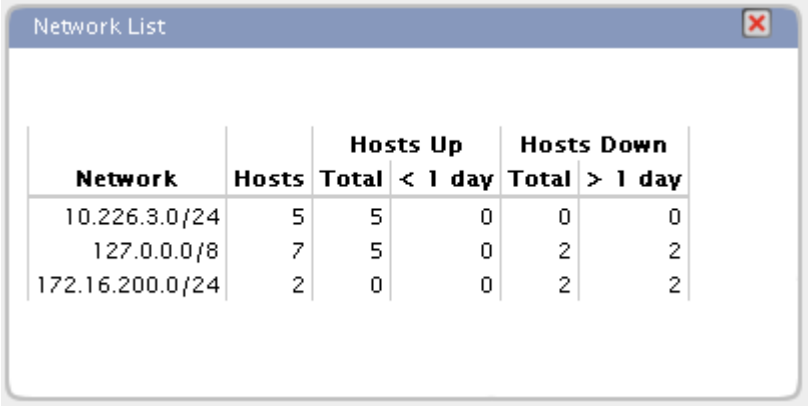


Bird's Eye View Gadget

The gadget provides a status view of selected host groups, by displaying the operating system icon for each host in a grid pattern with a different color background to illustrate the state of each as either up (green) or down (red). A control in the gadget title allows the selection of the host group to be displayed and the size of the host icons. Moving the mouse over each icon provides the hostname and IP address of the respective host.

Network List Gadget

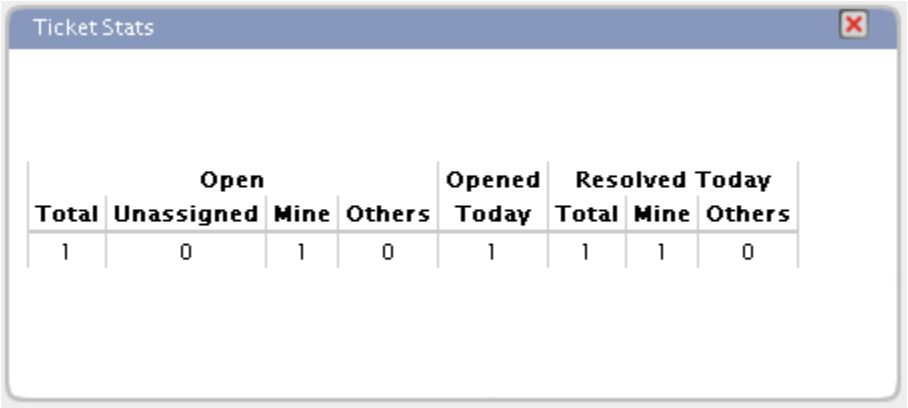
The gadget lists all networks where a registered host has an assigned IP address. In the Host column of the table, a host is deemed to be on a network if one of its interfaces has a respective IP address. Therefore the number of hosts in the table is if fact the number of network interfaces and may not match the total number of physical hosts if one or more hosts are multi-homed. Additionally the table shows the total number of hosts that are up or down and the number of hosts up less than one day (recent reboot) and those down for longer than one day.



Network	Hosts	Hosts Up		Hosts Down	
		Total	< 1 day	Total	> 1 day
10.226.3.0/24	5	5	0	0	0
127.0.0.0/8	7	5	0	2	2
172.16.200.0/24	2	0	0	2	2

Ticket Stats Gadget

The gadget provides a summary statistics table for Ticketing.



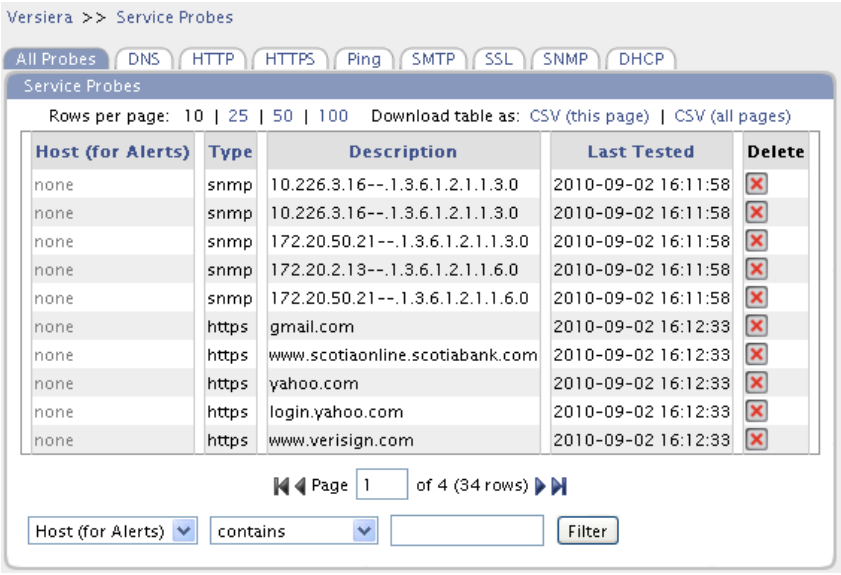
Open				Opened	Resolved Today		
Total	Unassigned	Mine	Others	Today	Total	Mine	Others
1	0	1	0	1	1	1	0

Service Probes

Service probes are used to monitor application services hosted and virtual assets such as digital certificates on your hosts. Service probes comprise a set of methods and protocols for active monitoring of your host application services from Versiera. With active monitoring the probe traffic originates from Versiera servers as opposed to Versiera passive host monitoring which accepts data from Versiera host agents and compares the data against monitoring rules you have configured for your hosts (traffic originates from your hosts.

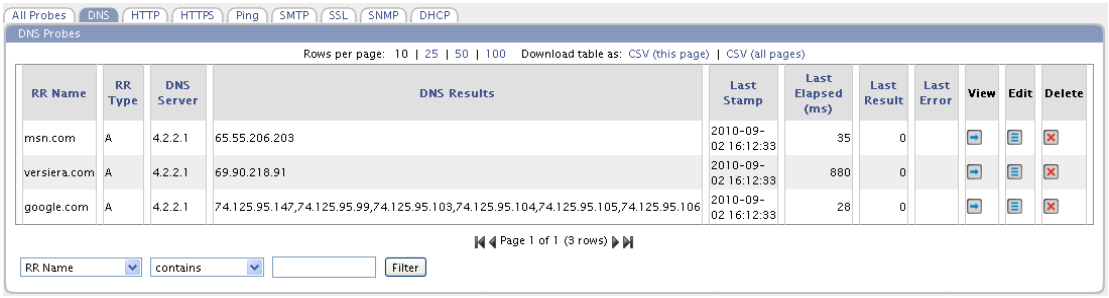
All Probes

The All Probes tab provides a summary of the service probes that have been configured, their type and when they were last tested.

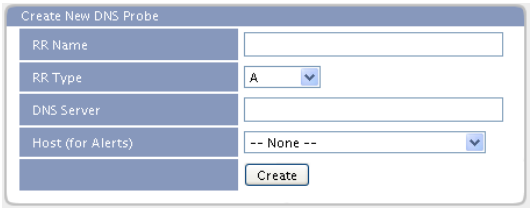


DNS

Domain Name Service (port 53/udp, 53/tcp) probes are used to actively monitor domain name records. Optionally a specific DNS server may be specified for queries In order to configure an active probe the following information must be provided:



Create New DNS Probe Form



RR Name – the DNS resource record name to be tested, example *www.google.com*

RR Type – the drop-down box to select the type of DNS resource record to be returned

A – network IP address record

PTR – pointer to a canonical name, used in reverse DNS lookups

CNAME – canonical name for one alias host name to another

NS – authoritative name server record(s)

MX – mail exchanger server records(s)

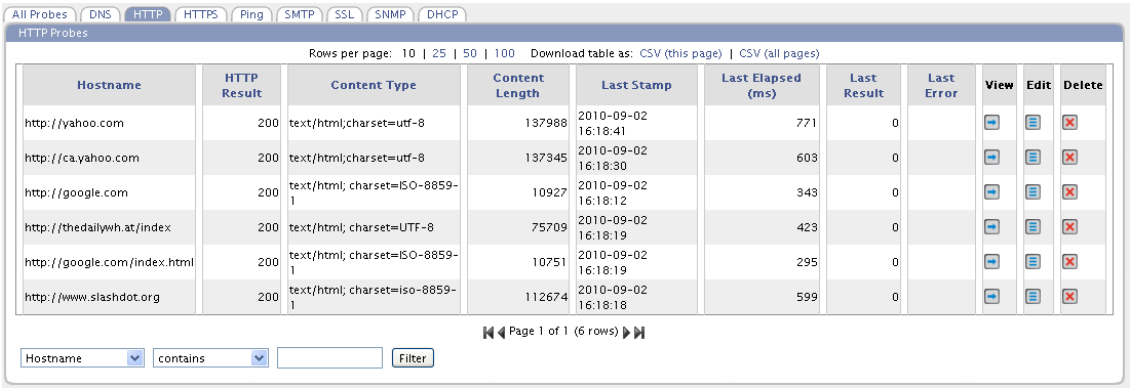
TXT – text string

DNS Server – (optional) the fully qualified domain name (FQDN) or network IP Address of the DNS server to be queried, otherwise Versiera probes use a preconfigured DNS server.

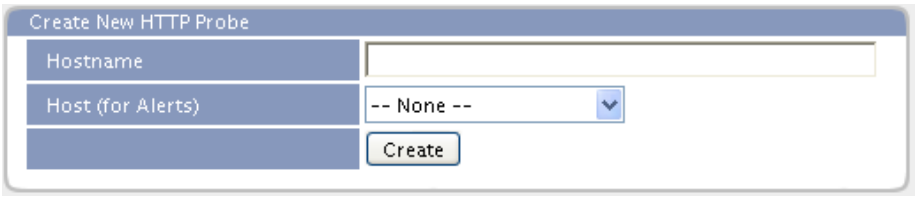
Host (for Alerts) – (optional) if the host address to be monitored is a host already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

HTTP

Hypertext Transfer Protocol (port 80/tcp) probes are used to actively monitor communication with web servers you specify in the probe configuration. In order to configure an active HTTP probe the following information must be provided:



Create New HTTP Probe Form

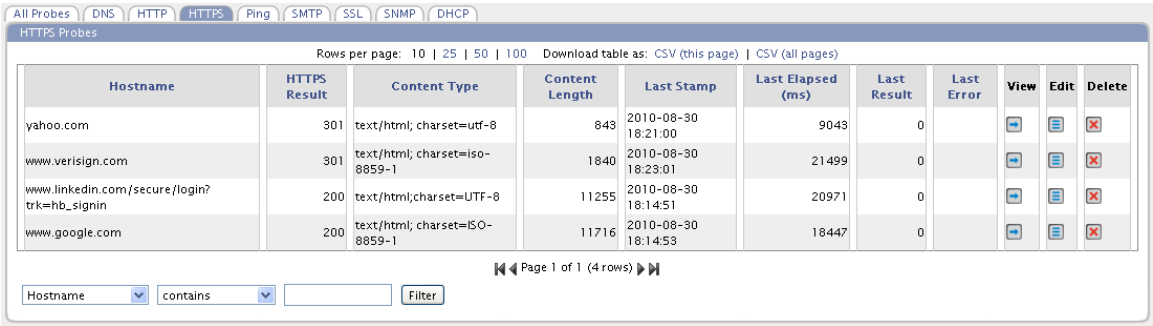


URL –the uniform resource locator (URL) for the web server and /or web server page to be monitored, example *http://www.wikipedia.com*

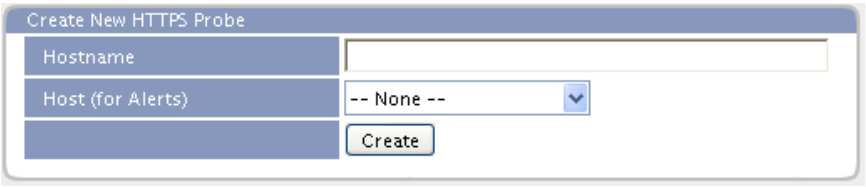
Host (for Alerts) – (optional) if a host address to be monitored is already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

HTTPS

Hypertext Transfer Protocol Secure (port 443/tcp) probes are used to actively monitor communication with web servers you specify in the probe configuration. In order to configure an active HTTPS probe the following information must be provided:



Create New HTTPS Probe Form

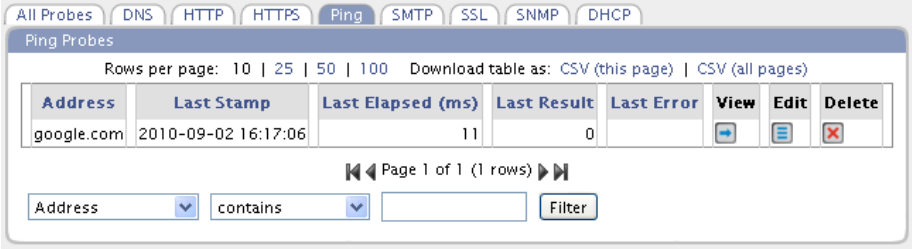


URL –the uniform resource locator (URL) for the web server and /or web server page to be monitored, example *https://www.google.com*

Host (for Alerts) – (optional) if a host address to be monitored is already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

PING

Ping probes (ICMP echo request/reply) are used to actively monitor communication to hosts or devices responding to PING. In order to configure an active probe the following information must be provided:



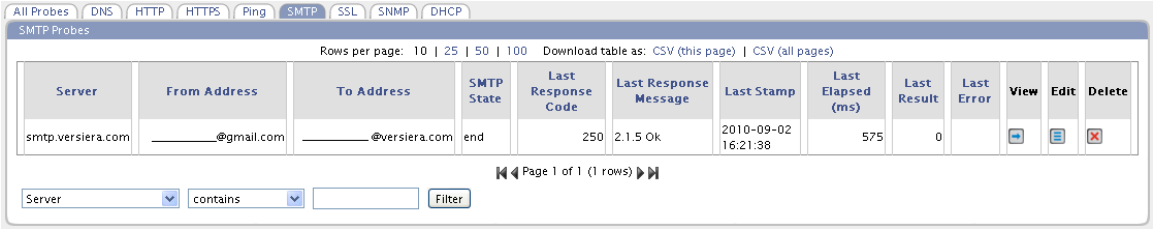
Create New Ping Probe Form

Address – the fully qualified domain name (FQDN) or network IP Address of the host to be monitored

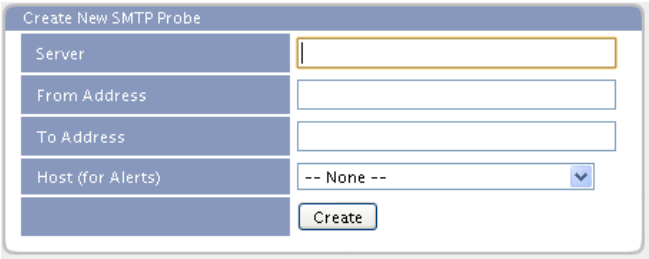
Host (for Alerts) – (optional) if the host address to be monitored is a host already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

SMTP

SMTP service (port 25/tcp) probes are used to actively monitor communication with mail servers. In order to configure an active probe the following information must be provided:



Create New SMTP Probe Form



Server – the fully qualified domain name (FQDN) or network IP Address of the mail server to be monitored

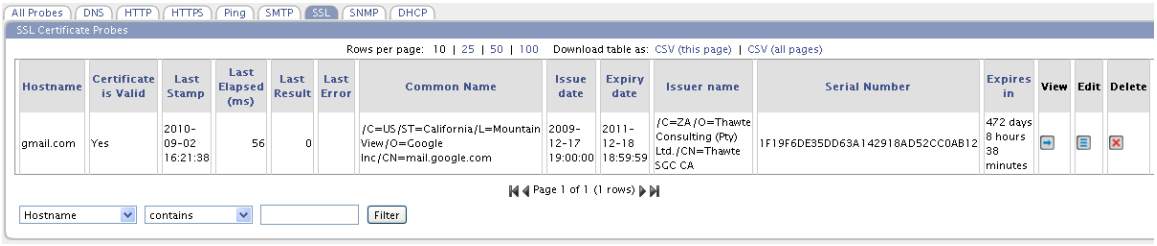
From Address – the e-mail address of the sender

To Address – the e-mail address of the recipient

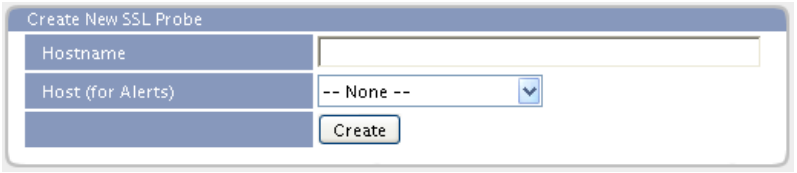
Host (for Alerts) – (optional) if the host address to be monitored is a host already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

SSL

The SSL probes are used to establish a secure connection to a web server or a network device running an embedded website and obtain a digital certificate from a website. The tab then displays the relevant information from the digital certificate including its expiration. In order to configure an active probe the following information must be provided:



Create New SSL Probe Form

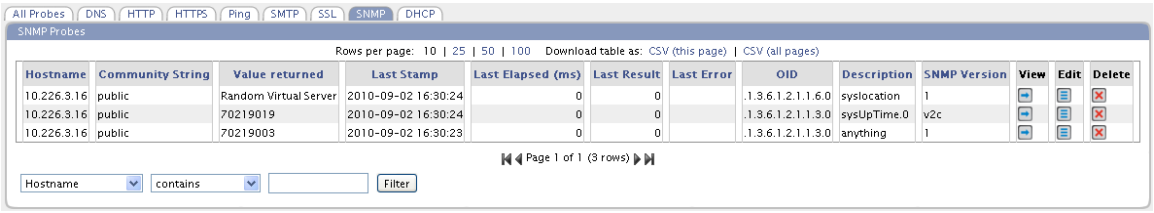


Hostname – the fully qualified domain name of a host

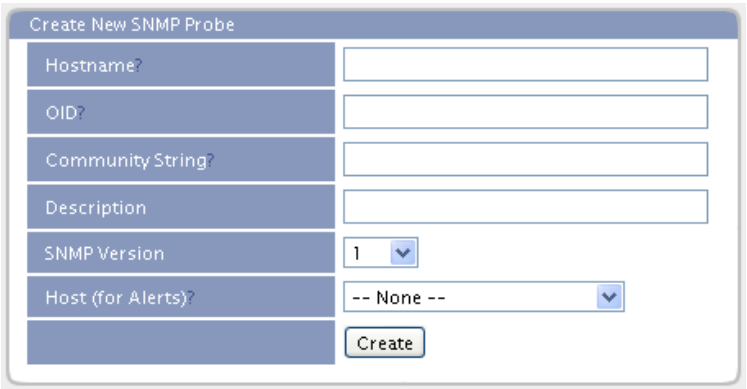
Host (for Alerts) – (optional) if the host address to be monitored is a host already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

SNMP (Enterprise only)

The SNMP service probes (ports 161/udp) are used to actively monitor servers and network devices, as well as, collect the required values from SNMP MIBs. Support for SNMP includes v1 and v2c. In order to configure an active probe the following information must be provided:



Create New SNMP Probe Form



Hostname – the fully qualified domain name of a host or its IP address

OID – a particular object identifier from a given SNMP MIB (e.g. .1.3.6.1.2.1.1.6.0 for System Location)

Community String – the password used to secure SNMP on the monitored host or device

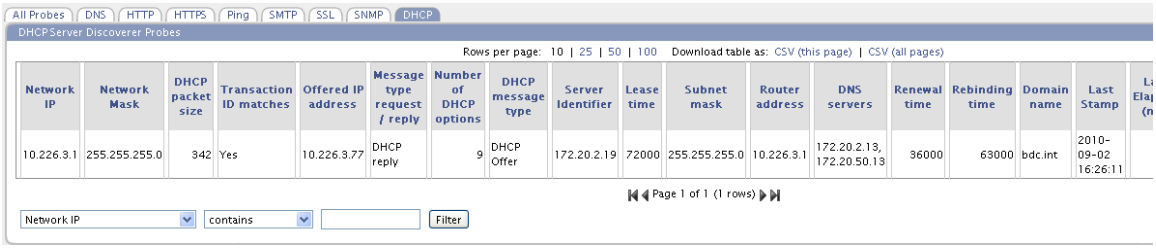
Description – information about the value returned for the particular object identifier (OID)

SNMP Version – the supported versions of SNMP are v1 and v2c

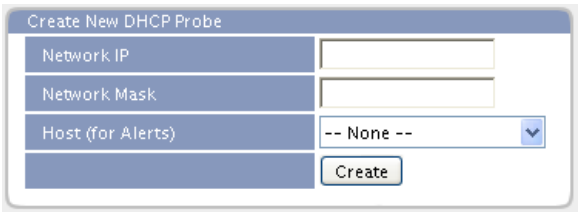
Host (for Alerts) – (optional) if the host address to be monitored is a host already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

DHCP (Enterprise only)

The DHCP service probes (ports 67/udp and 68/udp) are used to actively monitor servers configured to provide network address assignment using the Dynamic Host Configuration Protocol by requesting network address assignments from these servers and analyzing the results. In order to configure an active probe the following information must be provided:



Create New DHCP Probe Form



Network IP – the IPv4 network address

Network Mask – the network mask for the respective IPv4 network address

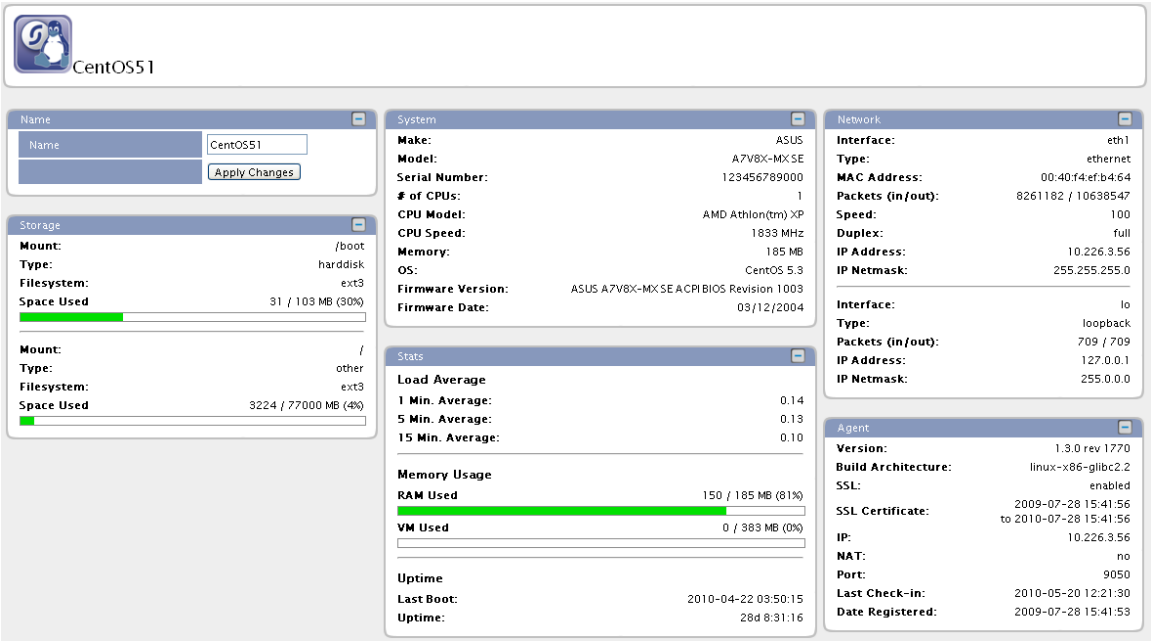
Host (for Alerts) – (optional) if the host address to be monitored is a host already registered with Versiera, then any service probe alerts for the probe will be associated with the registered host

State

The State section is used to view information on the configuration and active state for registered hosts. The section has been divided into three subsections to group relevant information. The sections are State Activity, State Configuration and History (State Changes over time).

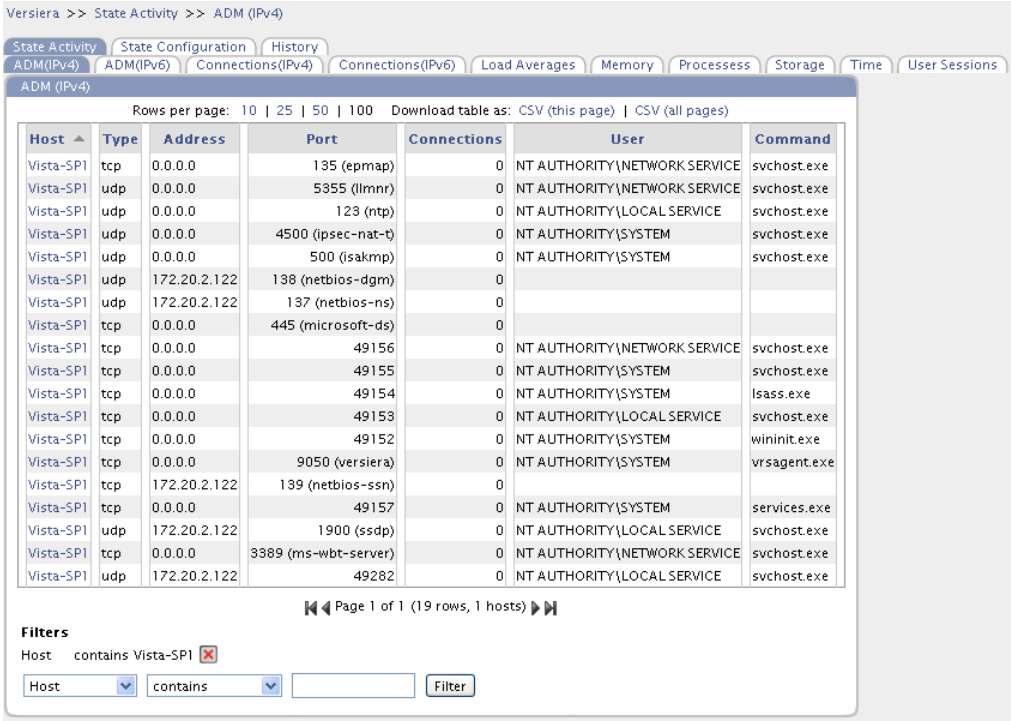
Host Summary

By clicking on a host link (host name in blue text) from any of the tables in Versiera will display the summary information page for the host.



ADM tabs, IPv4 and IPv6

Application Dependency Mapping tabs, IP4 and IP6, provide information useful in understanding what network applications are available on a particular host and their specific details.



Host	Type	Address	Port	Connections	User	Command
Vista-SP1	tcp	0.0.0.0	135 (epmap)	0	NT AUTHORITY\NETWORK SERVICE	svchost.exe
Vista-SP1	udp	0.0.0.0	5355 (llmnr)	0	NT AUTHORITY\NETWORK SERVICE	svchost.exe
Vista-SP1	udp	0.0.0.0	123 (ntp)	0	NT AUTHORITY\LOCAL SERVICE	svchost.exe
Vista-SP1	udp	0.0.0.0	4500 (ipsec-nat-t)	0	NT AUTHORITY\SYSTEM	svchost.exe
Vista-SP1	udp	0.0.0.0	500 (isakmp)	0	NT AUTHORITY\SYSTEM	svchost.exe
Vista-SP1	udp	172.20.2.122	138 (netbios-dgm)	0		
Vista-SP1	udp	172.20.2.122	137 (netbios-ns)	0		
Vista-SP1	tcp	0.0.0.0	445 (microsoft-ds)	0		
Vista-SP1	tcp	0.0.0.0	49156	0	NT AUTHORITY\NETWORK SERVICE	svchost.exe
Vista-SP1	tcp	0.0.0.0	49155	0	NT AUTHORITY\SYSTEM	svchost.exe
Vista-SP1	tcp	0.0.0.0	49154	0	NT AUTHORITY\SYSTEM	lsass.exe
Vista-SP1	tcp	0.0.0.0	49153	0	NT AUTHORITY\LOCAL SERVICE	svchost.exe
Vista-SP1	tcp	0.0.0.0	49152	0	NT AUTHORITY\SYSTEM	wininit.exe
Vista-SP1	tcp	0.0.0.0	9050 (versiera)	0	NT AUTHORITY\SYSTEM	vrsagent.exe
Vista-SP1	tcp	172.20.2.122	139 (netbios-ssn)	0		
Vista-SP1	tcp	0.0.0.0	49157	0	NT AUTHORITY\SYSTEM	services.exe
Vista-SP1	udp	172.20.2.122	1900 (ssdp)	0	NT AUTHORITY\LOCAL SERVICE	svchost.exe
Vista-SP1	tcp	0.0.0.0	3389 (ms-wbt-server)	0	NT AUTHORITY\NETWORK SERVICE	svchost.exe
Vista-SP1	udp	172.20.2.122	49282	0	NT AUTHORITY\LOCAL SERVICE	svchost.exe

Host – the hostname of the host registered with Versiera

Type – type of the transport layer protocol (*tcp* connection oriented, *udp* connectionless)

Address – IP address the host is listening on for connections, an address *0.0.0.0* implies any of the host's IP addresses

Port – network port number and port description

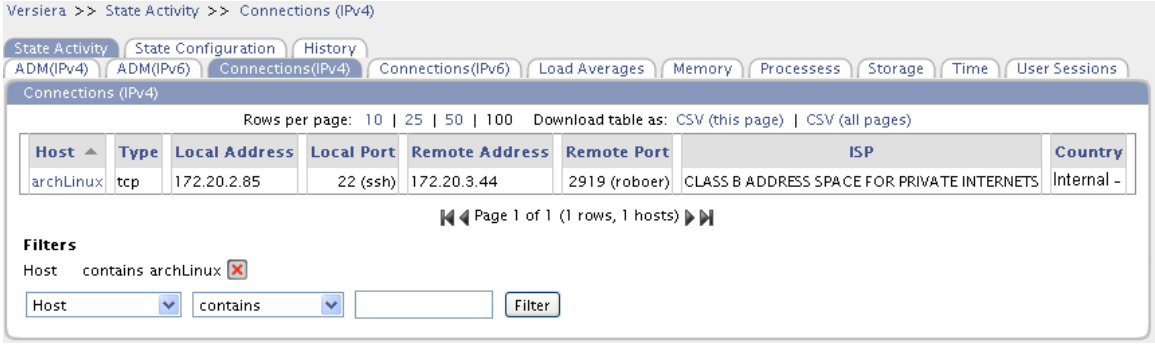
Connections – number of network connections to the application

User – user account running the application on the host

Command – application name

Connections tabs, IPv4 and IPv6

The Connections tabs provide information showing the current application socket connections that exist on a host.



Host – the hostname of the hosts registered with Versiera

Type – type of the transport layer protocol

Local Address – host network IP Address used in the communication session

Local Port – the application network port

Remote Address – remote host network IP Address used in the communication session

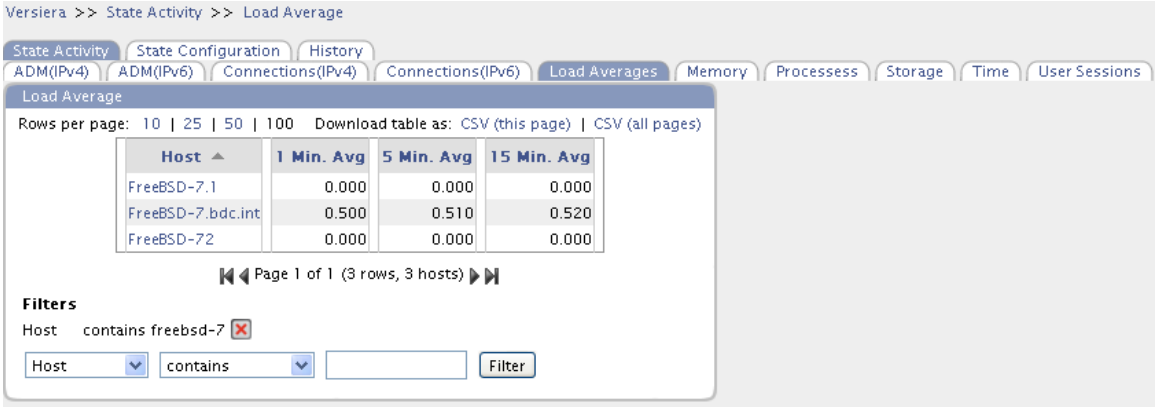
Remote Port – the remote application network port

ISP – the name of the Internet Service Provider that owns the Remote Address

Country – the country where the Internet Service Provider has registered the Remote Addresses

Load Average tab

The Load Average tab provides host performance measurement of work that a host is doing over a period of time. An idle host has a load number of 0 and each process using or waiting for CPU adds to the load number by 1. One can think of load average as a percentage of system utilization during a respective time period.



Host – the hostname of the host registered with Versiera

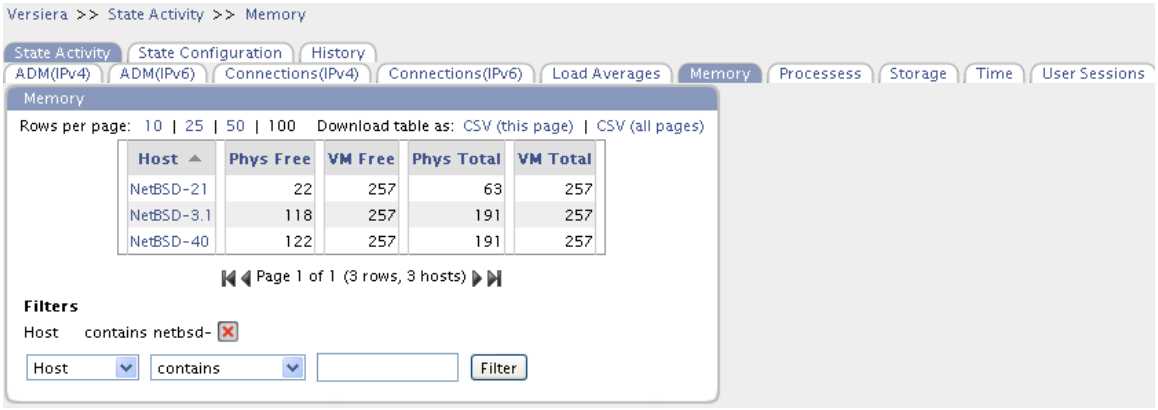
1 Min. Avg. – host load average over the last minute

5 Min. Avg. – host load average over the last 5 minutes

15 Min. Avg. – host load average over the last 15 minutes

Memory tab

The Memory tab provides host performance information for physical and virtual memory utilization.



Host – the hostname of the host registered with Versiera

Phys Free – the amount of unused physical memory

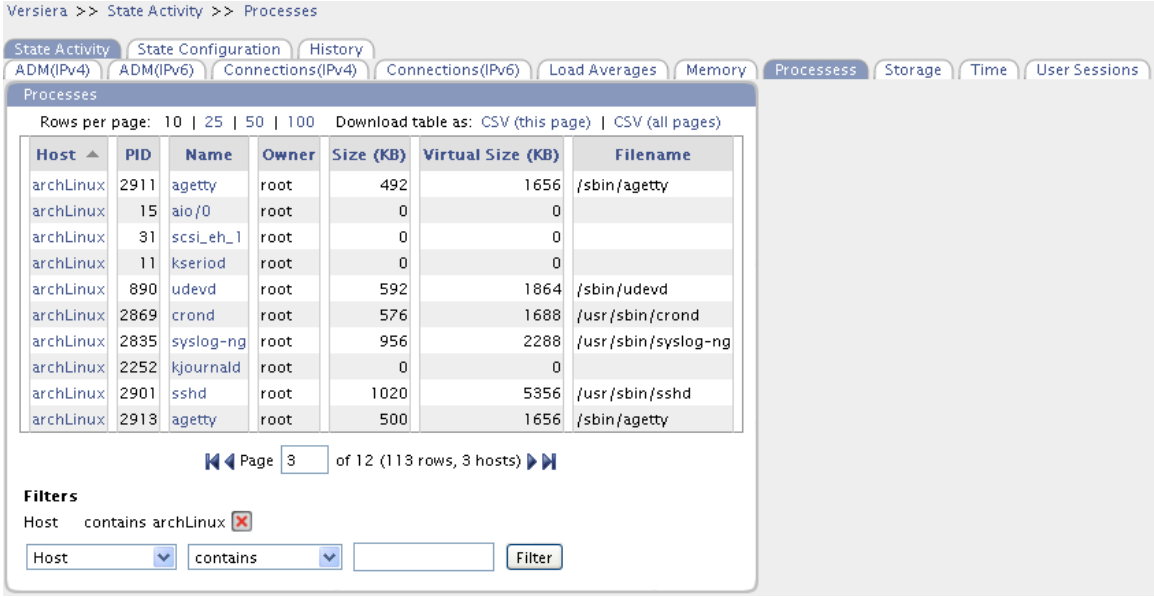
VM Free – the amount of unused virtual memory

Phys Total – the total amount of physical memory as seen by the operating system

VM Total – the total amount of configured virtual memory

Processes tab

The Processes tab provides details of host running applications.



Host – the hostname of the host registered with Versiera

PID – the application process identifier number on the respective host

Name – the application name

Owner – the user account running the application on the host

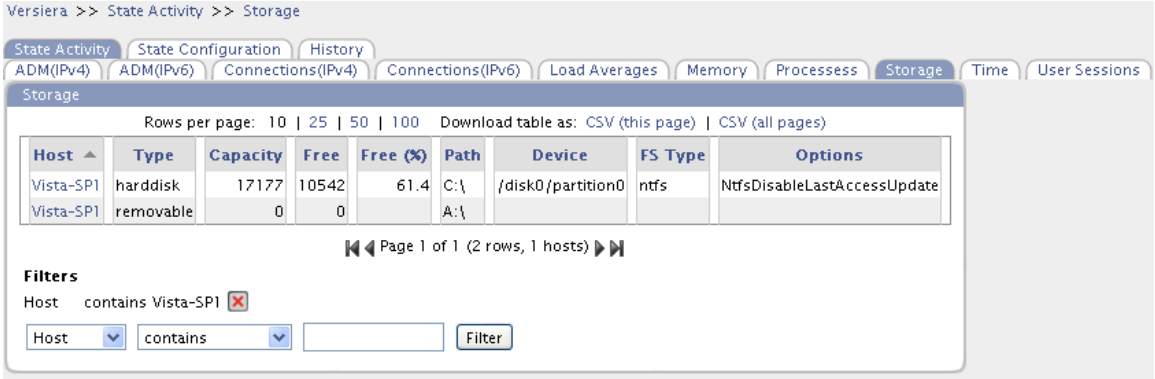
Size (KB) – the amount of physical memory used by the application

Virtual Size (KB) – the amount of virtual memory used by the application

Filename – the name of a process or a full path of an application that generated the process

Storage tab

The Storage tab provides details of the host storage capacity and space availability.



Host – the hostname of the host registered with Versiera

Type – the type of storage device as identified by the operating system

Capacity – the total amount of memory the storage device holds, in MB

Free – the amount of available storage on the device, in MB

Free (%) – the percentage of available storage on the device

Path – the name or the path to the mount point of the storage device

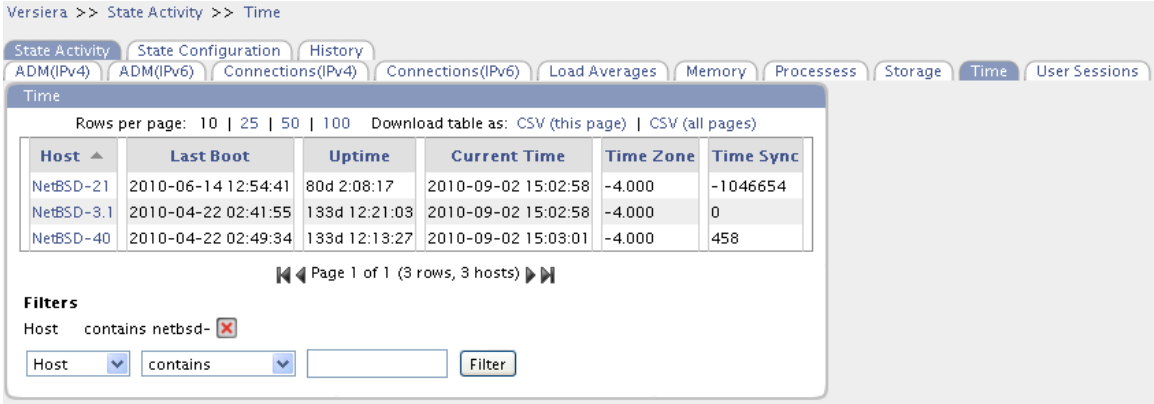
Device – the file system location on the storage device

FS Type – the type of file system used on the storage device

Options – the file system options in use

Time tab

The Time tab provides information related to the time information for a host. A useful item included is the Time Sync field which shows whether the registered host's time is accurate relative to time kept by Versiera (Versiera time servers are Stratum 3 servers).



Host – the hostname of the host registered with Versiera

Last Boot – the date and time when the host was last started

Uptime – the amount of time a host has been running continuously

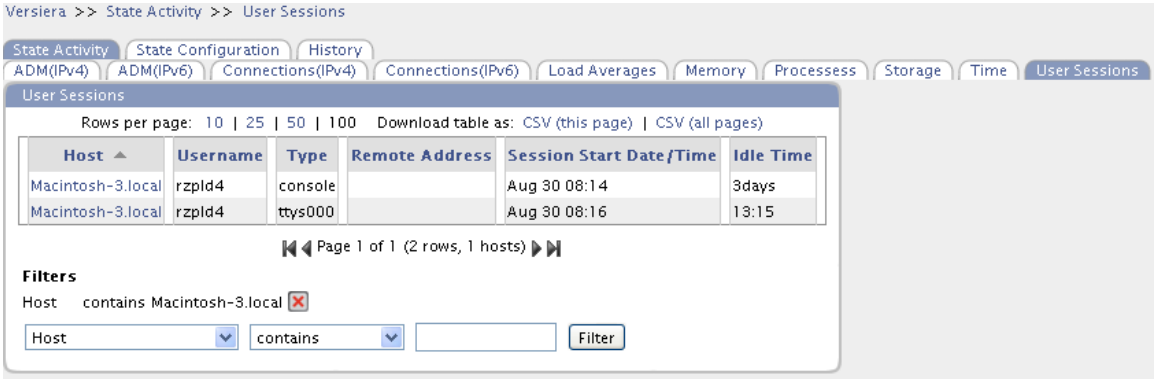
Current Time – the current date and time configured on the host

Time Zone – the time zone configured on the host as an offset in hours from UTC/GMT

Time Sync – the difference in seconds between the host's and Versiera server's clocks

User Sessions tab

The User Sessions tab provides details of the active user sessions across the managed hosts.



Host – the hostname of the host registered with Versiera

Username – the username used to sign on to the host

Type – the host device type the user used to sign on to the host

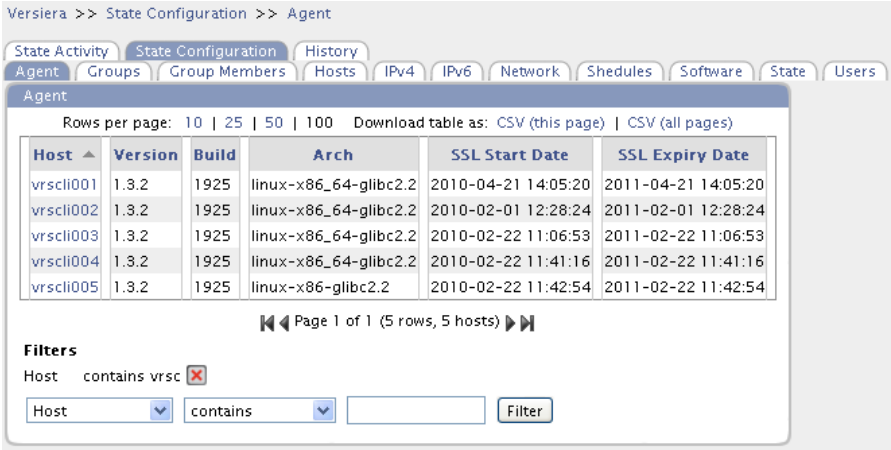
Remote Address – the remote IP Address from where the user initiated their remote session

Session Start Date/Time – the date and time when the user logged in to their remote session

Idle Time – the amount of time a remote user session has been idle

Agent tab

The Agent tab provides information concerning the Versiera agent running on the host systems.



Host – the hostname of the host registered with Versiera

Version – agent version number, version numbers are incremented with each new agent release

Build – agent build number, useful in communicating with the Versiera Support Department

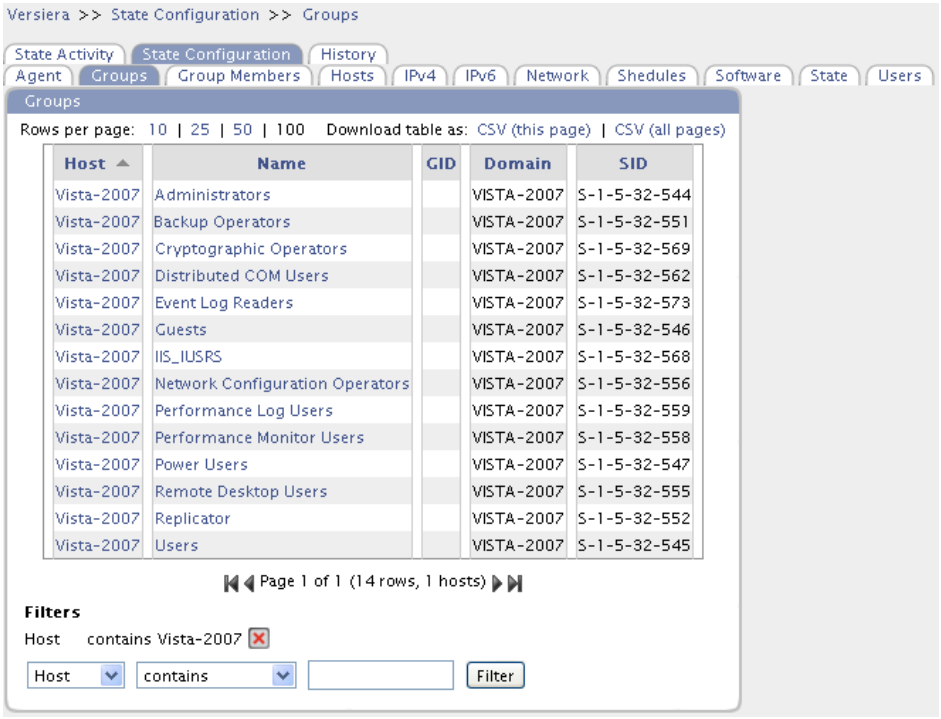
Arch – the agent operating platform

SSL Start Date – the date and time when the digital certificate was assigned to the registered host

SSL Expiry Date – the date and time when the host's digital certificate will expire, Versiera agents automatically renew their digital certificates

Groups tab

The Groups tab provides a listing of the host's security groups.



Host – the hostname of the host registered with Versiera

Name – the name of the user group on the host

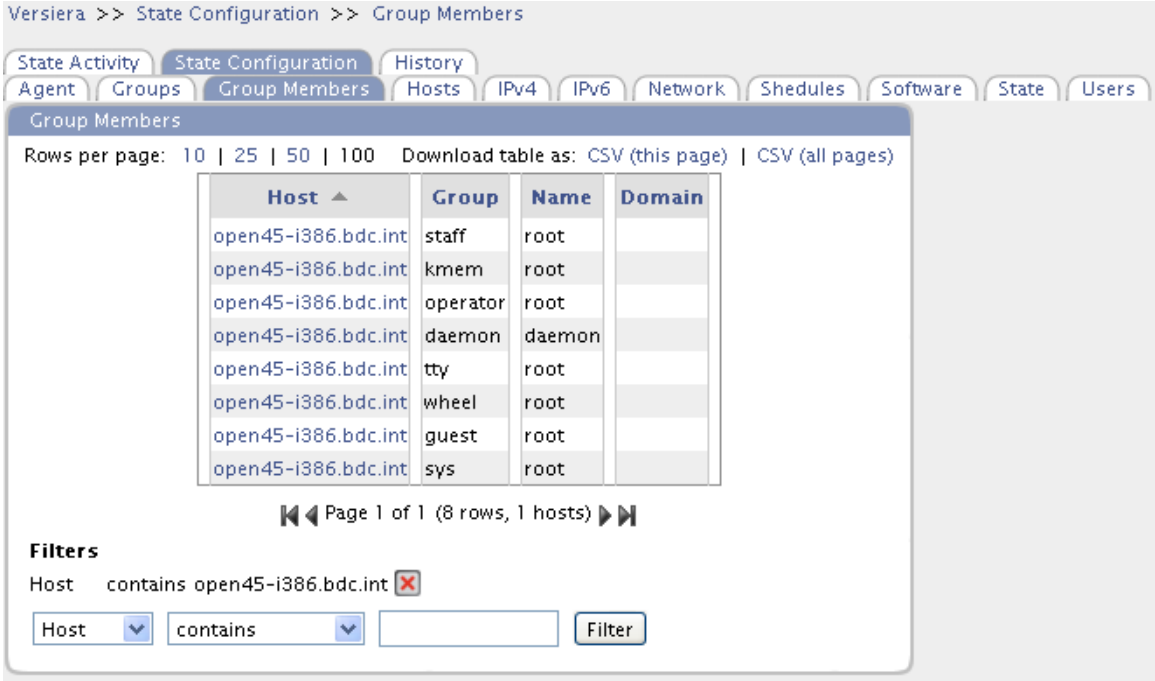
GID – (Unix) – the numeric value used to represent particular groups

Domain –name of the Windows Domain or hostname if not a member of a Windows domain

SID – (Windows) – security identifier that uniquely identifies a particular group

Group Members tab

The Group Members tab provides a listing of the host security groups and their respective group members.



Host – the hostname of the host registered with Versiera

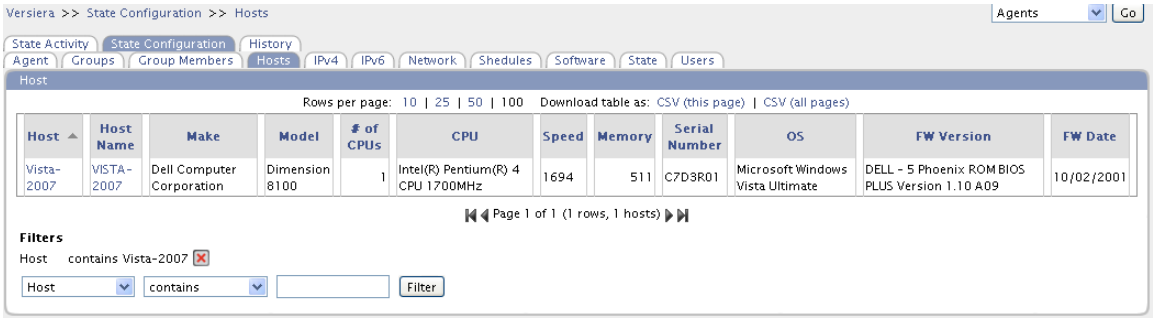
Group – the user group name on the host

Name – the user account name which is a member of the respective user group

Domain –name of the Windows Domain or hostname if not a member of a Windows domain

Host tab

The Host tab provides hardware and operating system details for the each registered host.



Host – the hostname of the host registered with Versiera

Host Name – the current hostname of the host computer (if the hostname has changed since registration)

Make – name of the manufacturer

Model – the manufacturer model number

# of CPUs – the number of processors

CPU – processor name

Speed – processor speed in megahertz (MHz)

Memory – the host memory size as seen by the operating system

Serial Number – the host hardware serial number

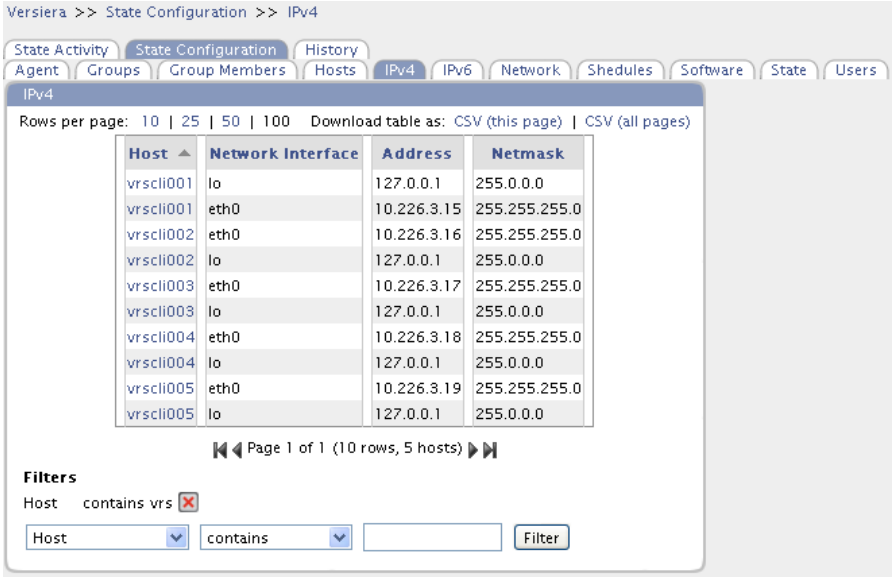
OS – the name of the host operating system

FW Version – the version number of the host firmware (BIOS)

FW Date – the date of the host firmware (BIOS)

IPv4 tab

The IPv4 tab provides detail for the host network interface configuration with respect to 32 bit network addresses.



Host – the hostname of the host registered with Versiera

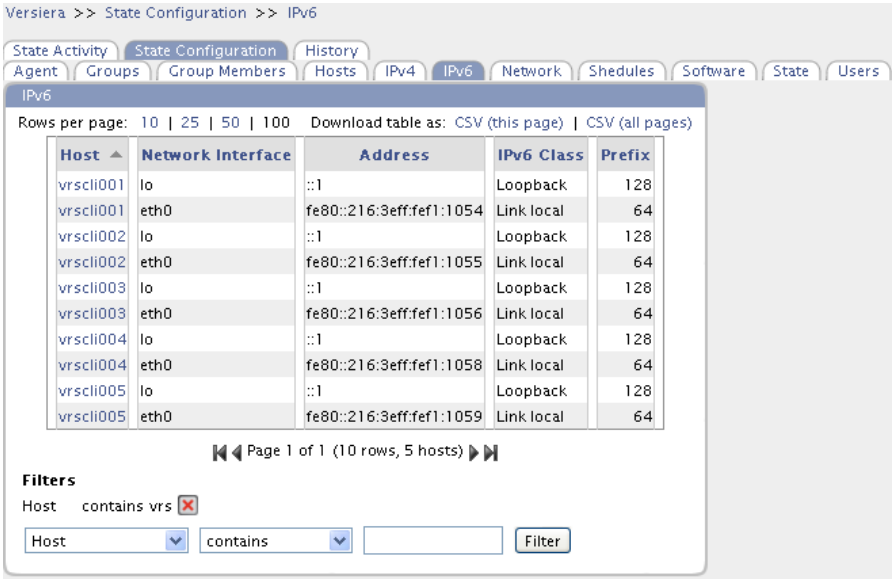
Net IF – the name of the network interface

Address – network IP address

Netmask – subnet network mask

IPv6 tab

The IPv6 tab provides detail for the host network interface configuration with respect to 128 bit network addresses.



Host – the hostname of the host registered with Versiera

Net IF – the name of the network interface

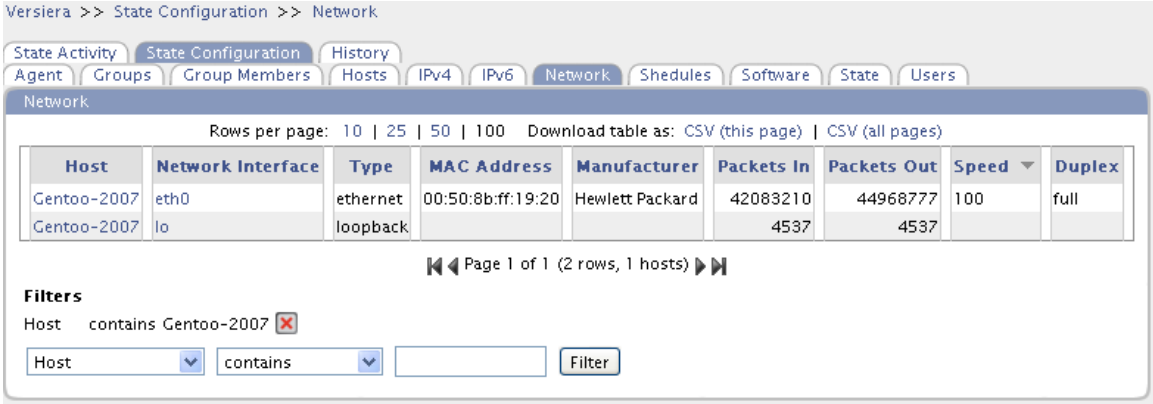
Address – network IP address

IPv6 Class – the type of IPv6 address

Prefix – the number of address bits associated with the network portion of the network IP address

Network tab

The Network tab provides host network interface details.



Host – the hostname of the host registered with Versiera

Name – the name of the network interface

Type – the type of network interface (Ethernet/Loopback/Other)

MAC Address – the media access control address of the network interface

Manufacturer – the name of the manufacturer of the network interface

Packets In – counter for the number of packets arriving to the network interface

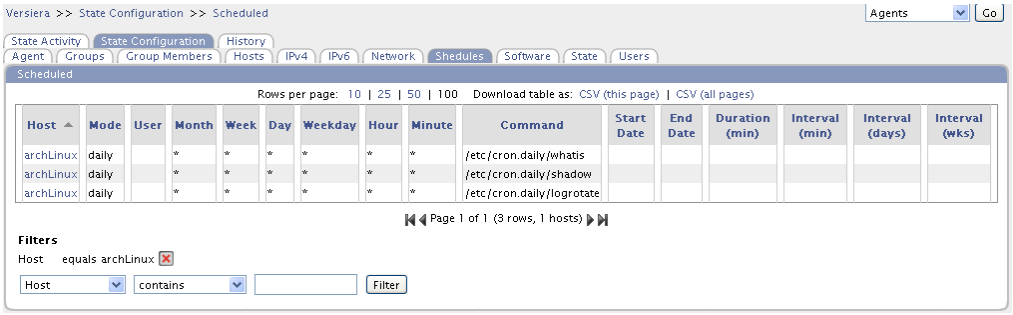
Packets Out – counter for the number of packets leaving the network interface

Speed – the network interface speed

Duplex – the network interface duplex information (half/full)

Scheduled tab

The Schedule tab provides details of the jobs that have been scheduled to execute on hosts.



Host – the hostname of the host registered with Versiera

Mode – job execution frequency

User – the security context the job will execute as

Month – the month(s) the job will execute

Week – the week(s) the job will execute

Day – the day(s) the job will execute

Weekday – the weekdays the job will execute

Hour – the hour the job will execute

Minute – the minute the job will execute

Command – the command used to execute the application or script

Start Date – the start date when the job will execute

End Date – the end date when the job will stop execute

Duration (min) – time interval in minutes the job will execute

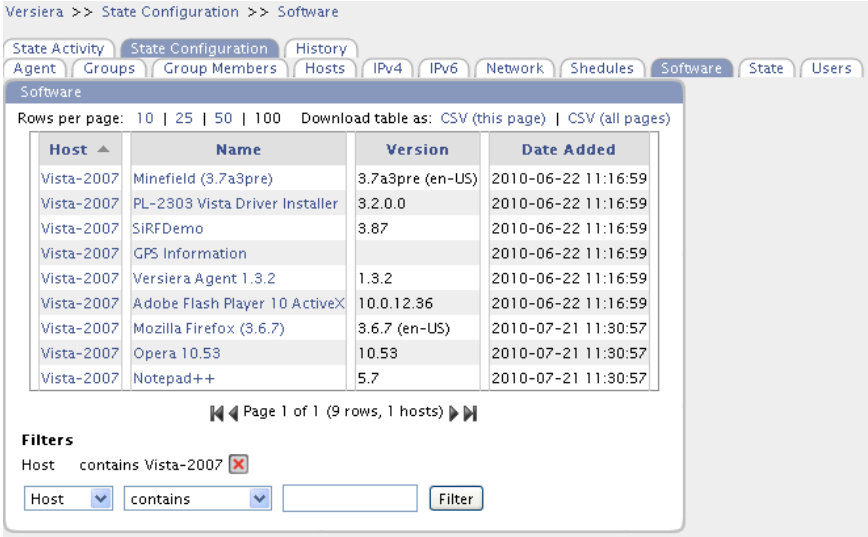
Interval (min) – time interval in minutes between successive job executions

Interval (days) – the number of days between successive job executions

Interval (wks) – the number of weeks between successive job executions

Software tab

The Software tab provides details of host installed applications.



Host – the hostname of the host registered with Versiera

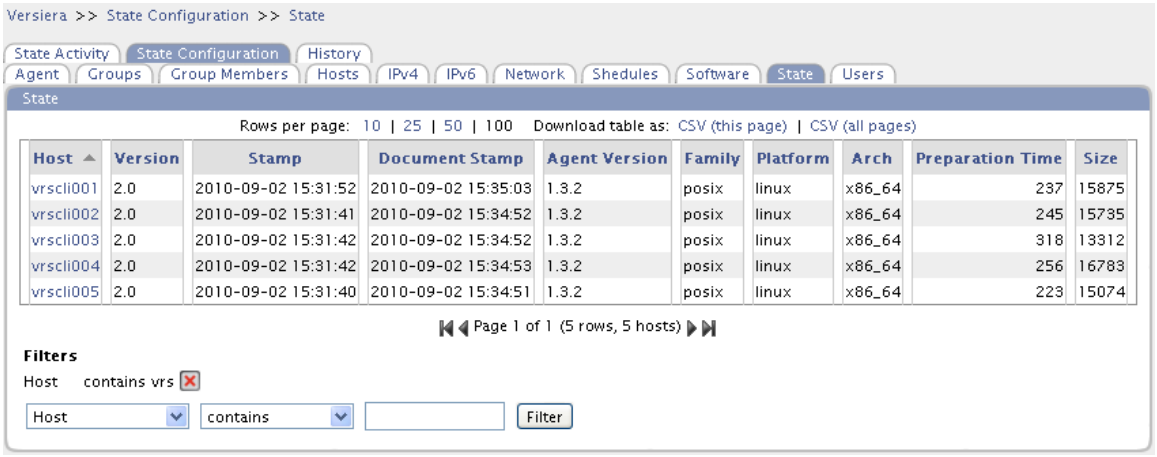
Name – the application name

Version – the version number of the application

Date Added – the date stamp the application was first catalogued by Versiera

State tab

The State tab provides general host details pertaining to the state documents the host submits to Versiera.



Host – the hostname of the host registered with Versiera

Version – state document version

Stamp – time stamp the state document was received

Document Stamp – time stamp of the state document generated by the agent

Agent Version – version number of the Versiera agent

Family – operating system family type

Platform – operating system kernel

Arch – the host processor architecture as identified the operating system

Preparation Time – time interval in seconds required generate the host's state document

Size – the size of the state document is based on a character count

Users tab

The Users tab provides details of the host user accounts.

Host – the hostname of the host registered with Versiera

Name – the name of the user account

Domain – the name of the Windows Domain

SID – (Windows) – security identifier that uniquely identifies the user account

Disabled – indicates whether the account is disabled (true/false)

UID – (Unix) the number identifying the user account, the user ID number

GID – (Unix) the number identifying the user account's primary group account, the group ID number

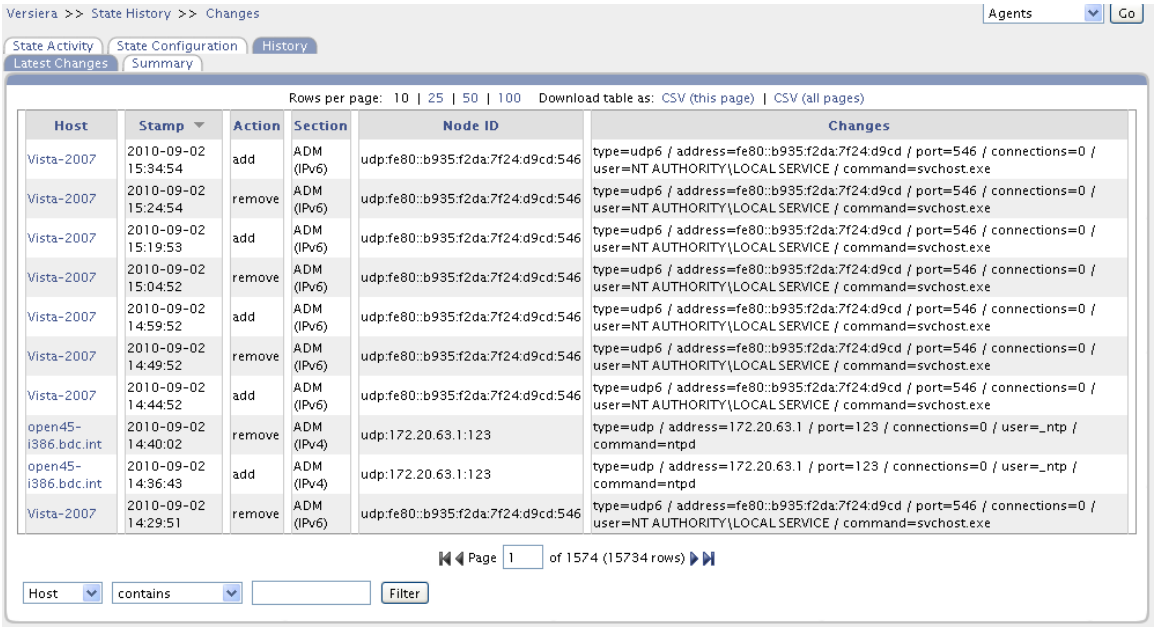
Full Name – the account owner's first and last name

Home – the path of the account home directory

Shell – the default user shell command interpreter

History Latest Changes tab

The History Latest Changes tab provides details of the latest changes to host information as tracked over a period of time.



Host – the hostname of the host registered with Versiera

Stamp – the date and time when the change was found

Action – describes the type of host historical information (initial, additional, change or removal)

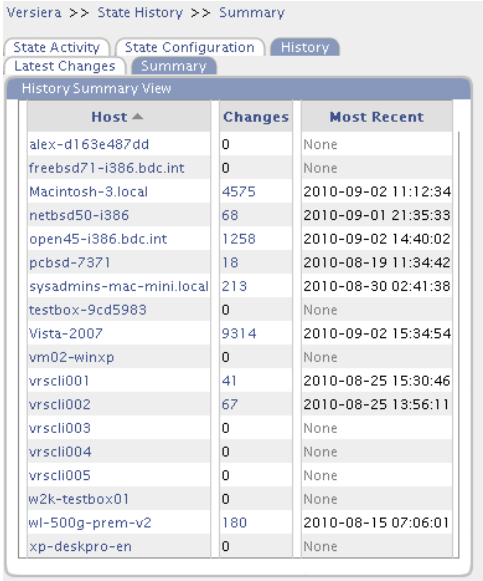
Section – the particular section of the state document where the change was found

Node ID – type or change records

Changes – the details describing the records change

History Summary tab

The History Summary tab provides a report showing the host and the number of state changes that have occurred.



Host	Changes	Most Recent
alex-d163e487dd	0	None
freebsd71-i386.bdc.int	0	None
Macintosh-3.local	4575	2010-09-02 11:12:34
netbsd50-i386	68	2010-09-01 21:35:33
open45-i386.bdc.int	1258	2010-09-02 14:40:02
pcbsd-7371	18	2010-08-19 11:34:42
sysadmins-mac-mini.local	213	2010-08-30 02:41:38
testbox-9cd5983	0	None
Vista-2007	9314	2010-09-02 15:34:54
vm02-winxp	0	None
vrscli001	41	2010-08-25 15:30:46
vrscli002	67	2010-08-25 13:56:11
vrscli003	0	None
vrscli004	0	None
vrscli005	0	None
w2k-testbox01	0	None
wl-500g-prem-v2	180	2010-08-15 07:06:01
xp-deskpro-en	0	None

Host – the hostname of the host registered with Versiera

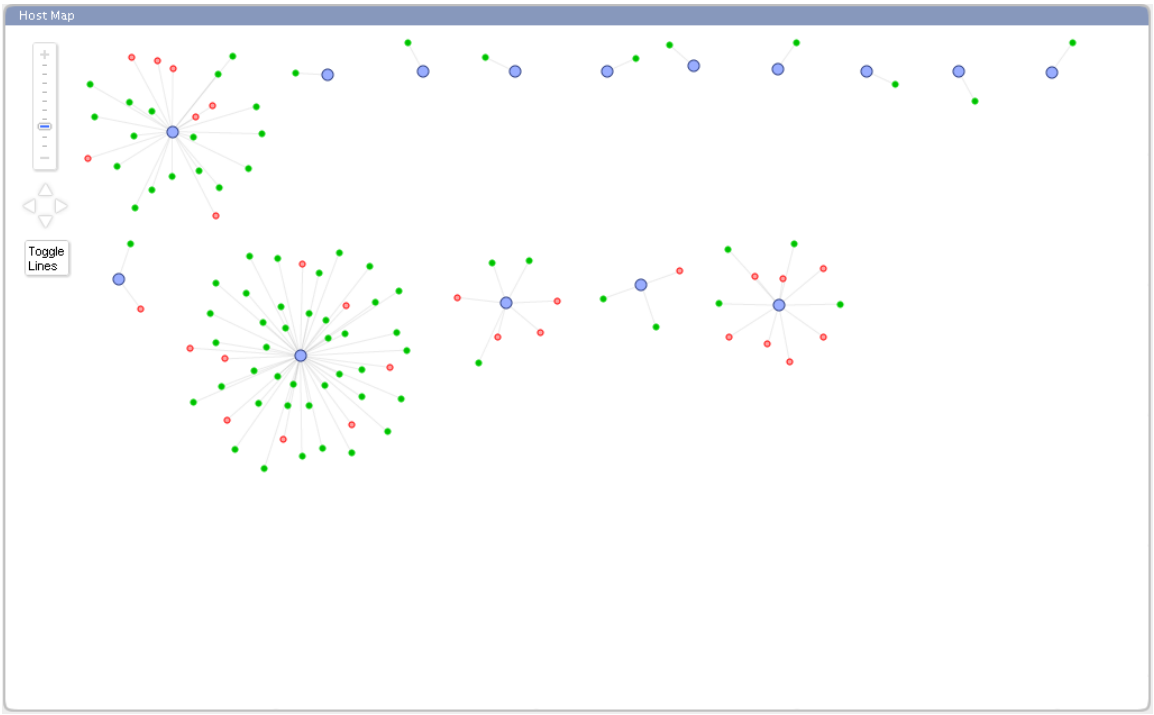
Changes – the number of changes recorded for a host

Most Recent – the date and time of the most recent change in state

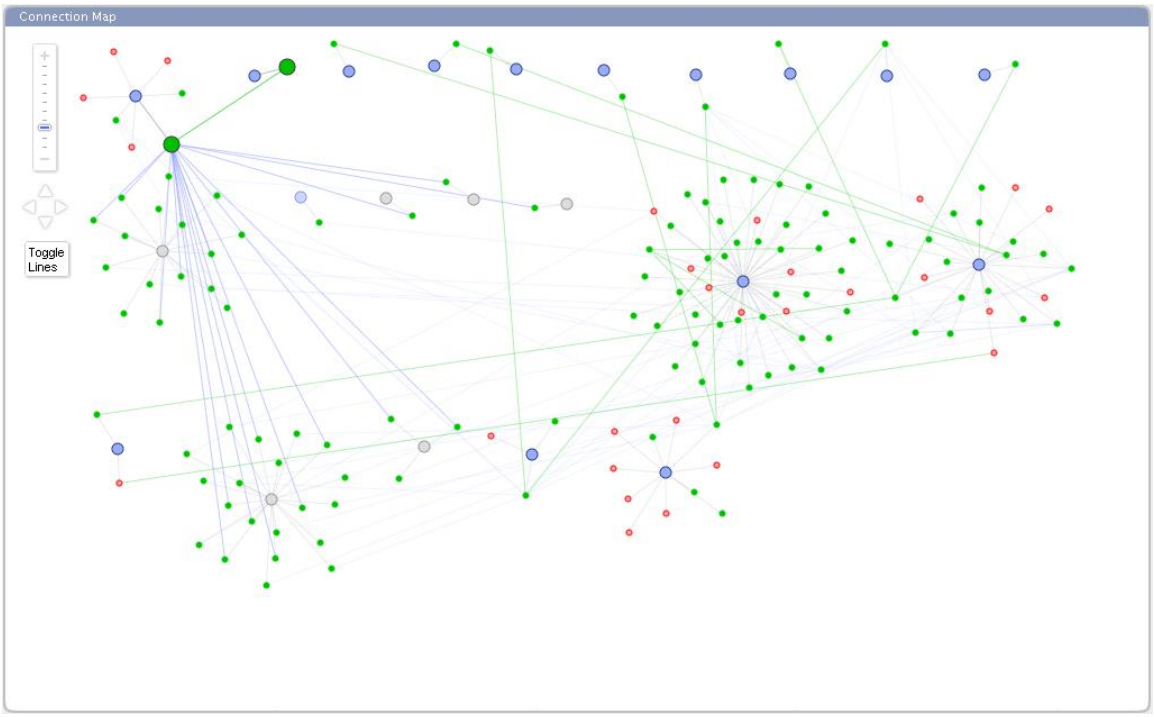
Network Maps

Versiera Network Maps are auto generated, fully user interactive and offer the ability to perform host inspection, drag/drop the network map and zoom in/out. Network Maps are available for showing corporate host status, host communications and other network views of systems and data flows.

Sample Host Map



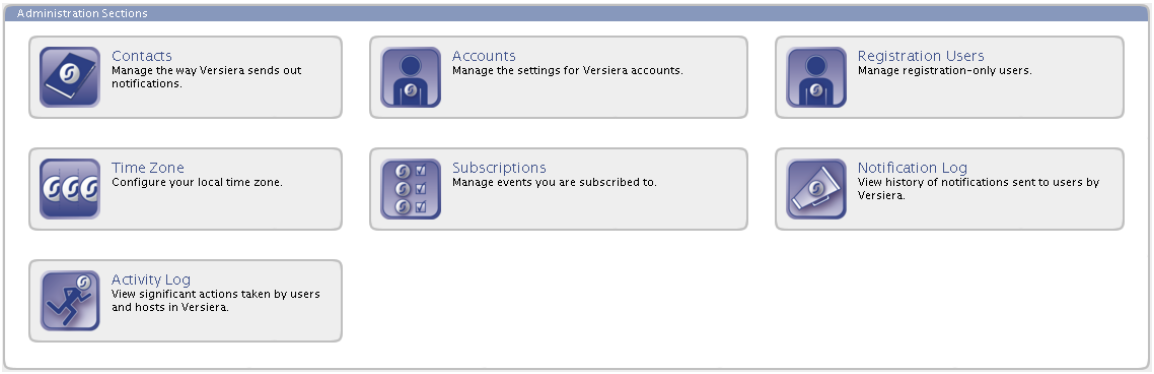
Sample Enterprise Connections Map



Administration

The Versiera Administration Sections are used for managing various Versiera settings, customizations, adding multiple Versiera IDs and review/audit of Versiera activity logs in using the Versiera Management Console.

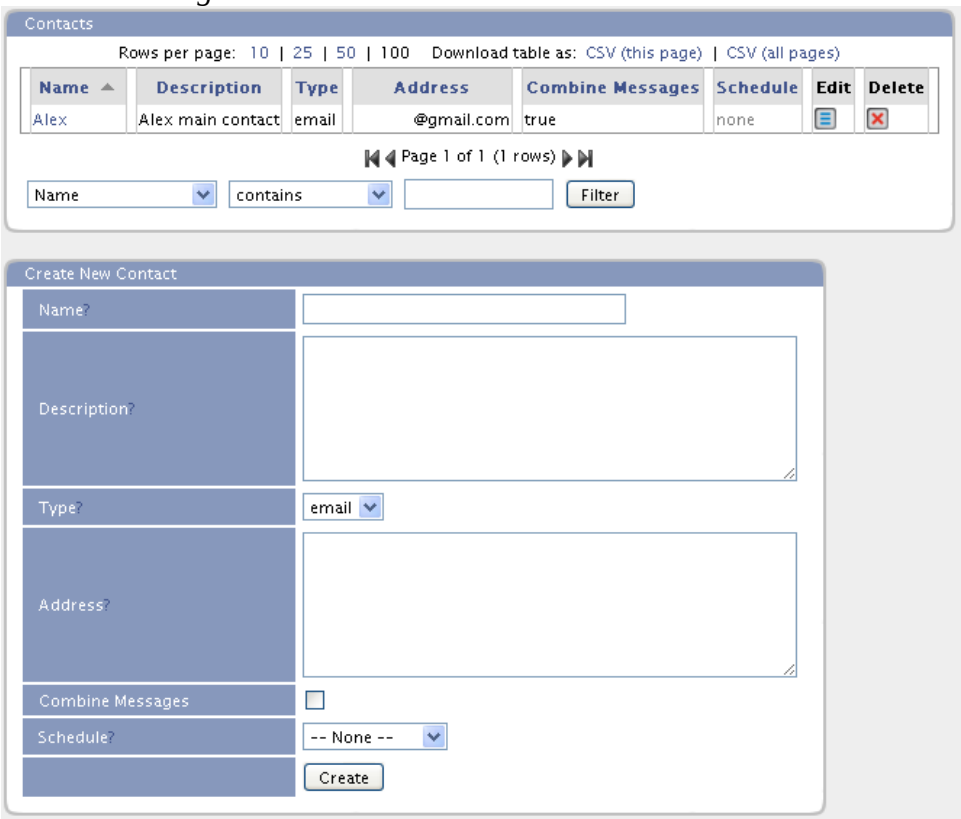
Administration Sections



Contacts

The Contacts section is used for adding and managing contact information used in sending Versiera alert notifications. The contact email addresses may be used to "subscribe" to event alert notifications for communicating with external users. Contacts would typically be corporate administrators of hosts that are managed using Versiera Management Console. Note - Contacts are not involved in accessing the Versiera Management Console.

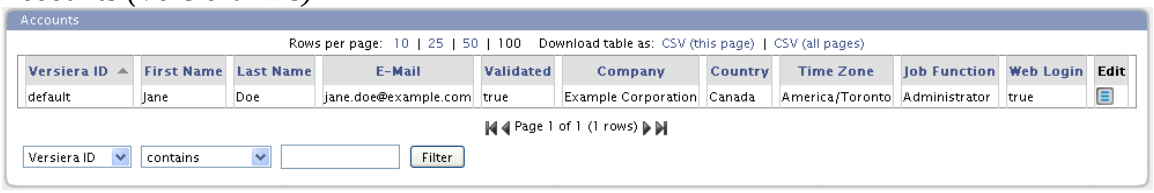
Contacts Management



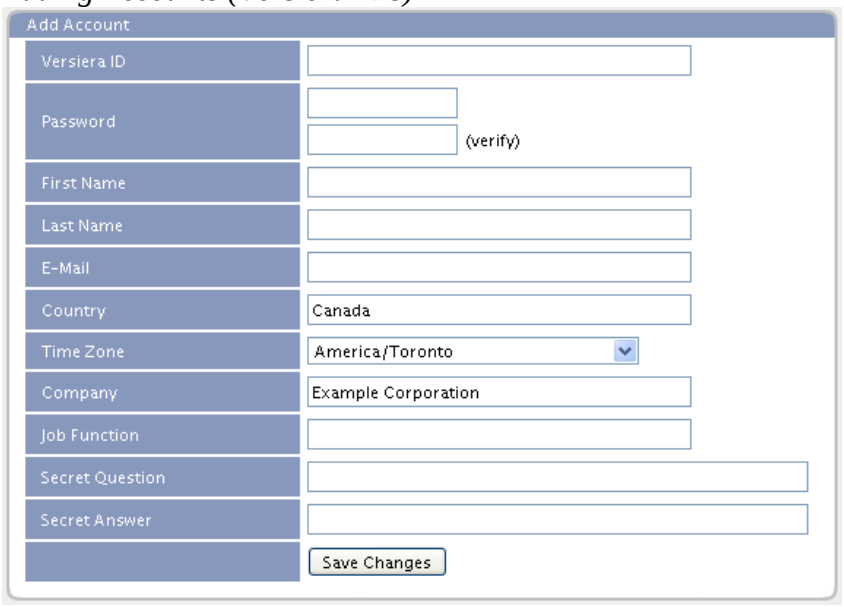
Accounts

The Accounts section is used for adding and managing Versiera IDs. A Versiera ID is used to sign-in to the Versiera Management Console. The first Versiera ID created, during the initial registration, is considered the master Versiera ID. The master Versiera ID can create, edit and disable additional Versiera IDs which can be created to facilitate multiple persons using the Versiera Management Console to manage hosts for an enterprise. Activity for each Versiera ID is audited and the master Versiera ID has access to the complete audit of all subordinate Versiera IDs.

Accounts (Versiera IDs)

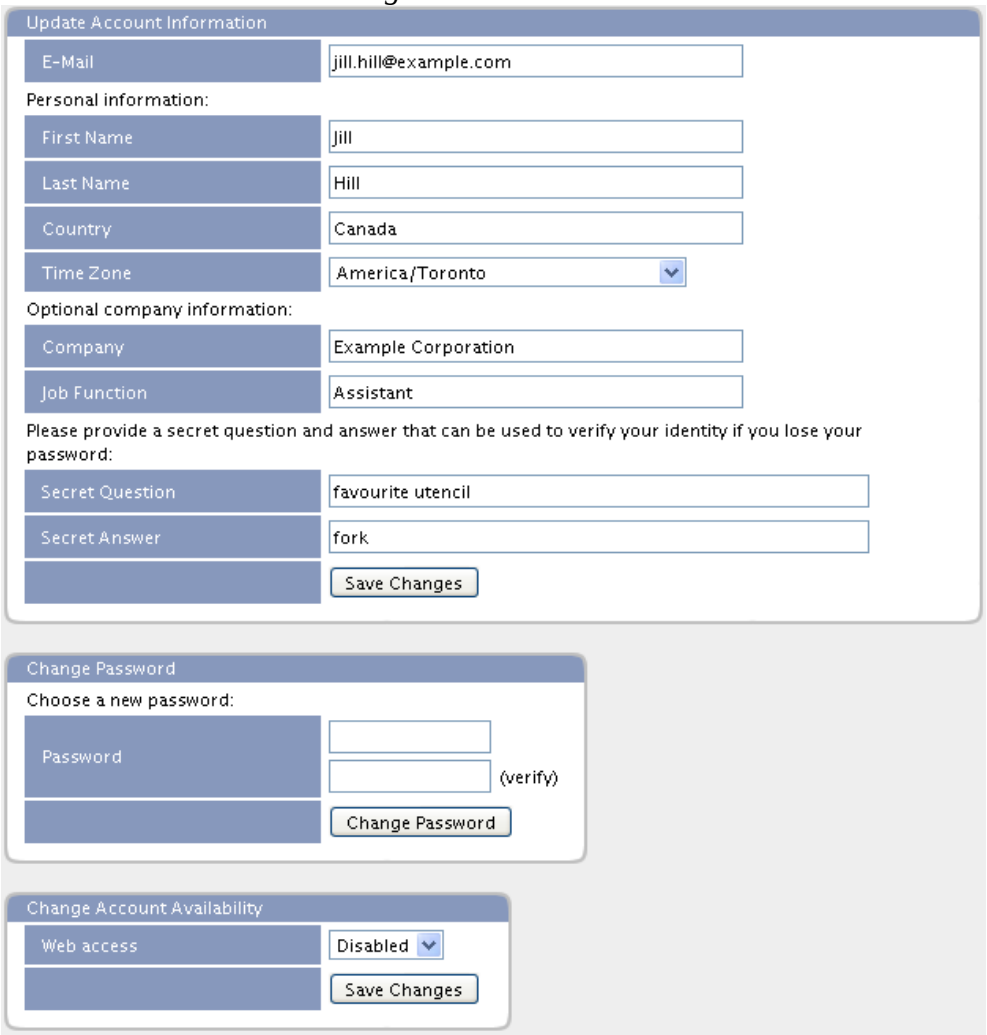


Adding Accounts (Versiera IDs)



When additional Versiera IDs are added, they can not be deleted and a trail of their activity is preserved for auditing purposes. In the Versiera Management Console the non-primary Versiera IDs may be updated, have their password changed and be enabled or disabled.

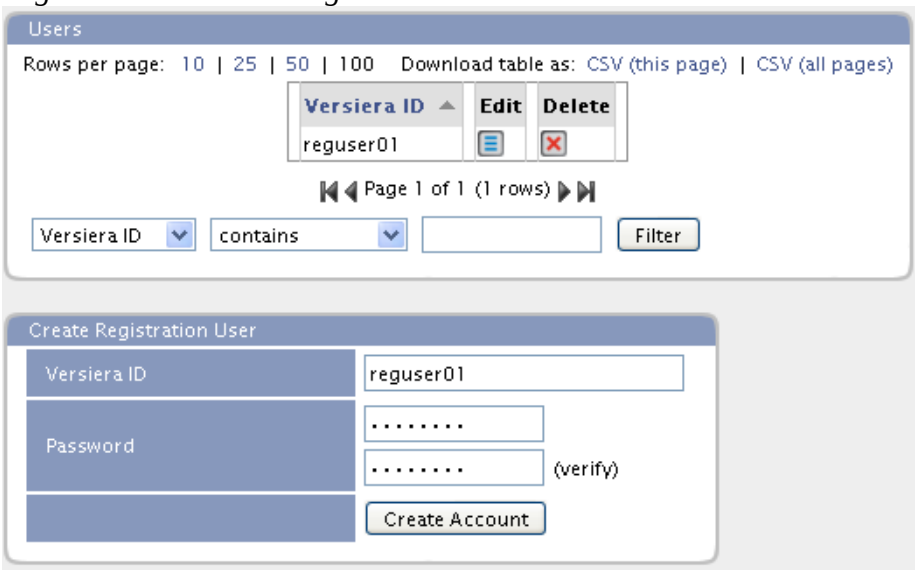
Administrative Account Management Form



Registration Users

The Registration Users section is used for adding and managing accounts with limited access to Versiera. These accounts may be used to register new hosts with Versiera. These registration accounts are not able to access the Versiera Management Console.

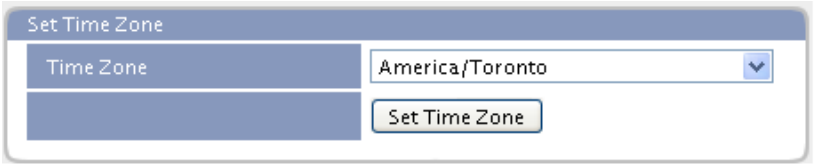
Registration Users Management



Time Zone

The Time Zone section is used for the configuration of the time zone setting for the currently logged in account. By modifying the time zone, all information in Versiera showing date and time will be adjusted based on the configured time zone.

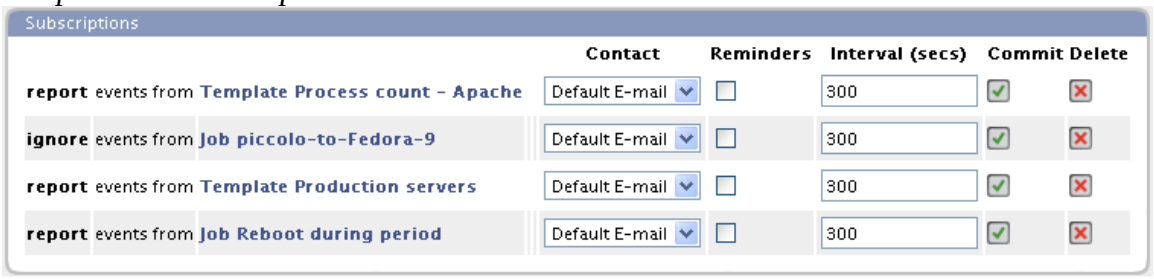
Time Zone Configuration



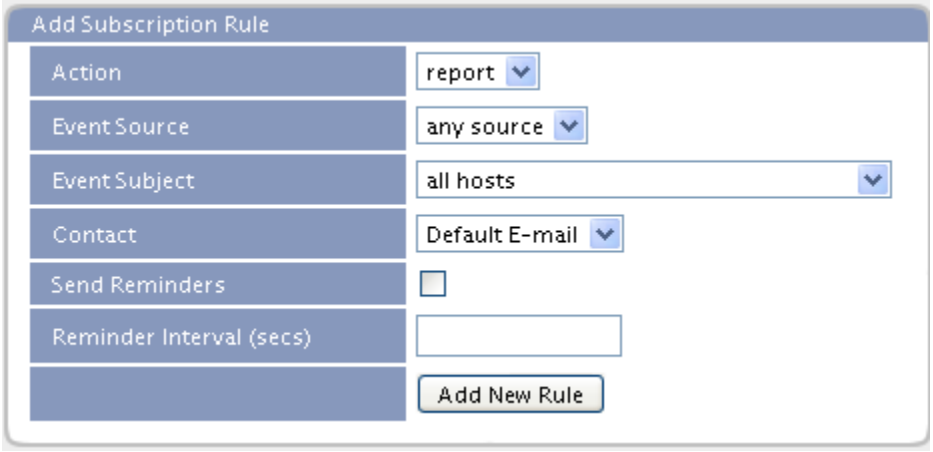
Subscriptions

The Subscriptions section is used for the review and management of event alert notification subscriptions. The Contact email addresses are obtained from the Contacts section of the Versiera Management Console.

Sample Event Subscriptions



Add Subscription Rule



Notification Log

The Notification Log section is used for the review and audit of all alert notifications sent from Versiera to alert notification subscribers.

Sample Notification Log

Activity Log

The Activity Log section is used for the review and audit of Versiera account actions performed while using Versiera Management Console. The primary Versiera ID can see in the Activity Log both its own audit trail and that of the subordinate Versiera IDs, while the subordinate Versiera IDs can only review their only Activity Log.

Sample Activity Log

Tips and Tricks

How to force the IP address that the Versiera agent listens on.

By default the Versiera agent listens on IP address 0.0.0.0 (all host IP addresses) and port 9050/tcp. To force listening on a particular IP address:

1. In the directory where Versiera agent is installed create a *local.cfg* file (same directory as *init.cfg* file)
2. Add the following text without quotes to the local.cfg file substituting your IP address at the end: **"bind_address = x.x.x.x"**

Note: To accept only loopback connections, add the following text without quotes to the local.cfg file: **"bind_address = 127.0.0.1"**

Automate Versiera Agent Windows Installation

There are two steps in getting Versiera agents operational. The first is installing the agent on the host and the second is to register the agent against the Versiera Management Center in order to obtain a digital certificate and map the agent to the respective Versiera Account.

1. To automate the agent install from the command line (in silent mode) use the following code:

versiera-agent.exe /url https://backend.versiera.com /user *Versiera ID*/pass *password* /sp- /verysilent /suppressmsdboxes /nocancel /norestart

Note:

It is recommended to create a **Registration** Versiera ID in the Administration Section for use in scripting/automation.

Uninstalling Versiera Agents

OS X

1. Stop Versiera agent: "**sudo launchctl stop com.netcraftinc.versiera.agentmond**"
2. Verify agent is no longer running: "**ps aux | grep vrsagent**"
3. Delete the **versiera** directory and its contents (agent configuration files): "**rm –r /etc/versiera**"
4. Delete the **VersieraAgent** directory and its contents (agent binary files)**:**"**rm –r /Library/VersieraAgent**"
5. Delete the **com.netcraftinc.versiera.agentmond.plist** file, if it exists: "**rm –r /Library/com.netcraftinc.versiera.agentmond.plist**"
6. Delete the **agentmond.log** file, if it exists: "**rm –r /var/log/agentmond.log**"
7. Reboot the system

Linux

1. Stop Versiera agent, depending on Linux distribution: "**/etc/init.d/agentmond stop** " or "**/etc/rc.d/agentmond stop**"
2. Verify agent is no longer running: "**ps -ef | grep vrsagent**"
3. Delete the **versiera** directory and itscontents (agent configuration files): "**rm –r /etc/versiera**"
4. Delete the **vrsagent** directory and its contents (agent binary files): "**rm –r /opt/vrsagent**"
5. Delete the **agentmond.log** file, if exists: "**rm –r /var/log/agentmond.log**"
6. Reboot the system

FreeBSD/NetBSD/OpenBSD

1. Stop Versiera agent: "**/etc/rc.d/agentmond stop**"
2. Verify agent is no longer running: "**ps aux | grep vrsagent**"
3. Delete the **versiera** directory and its contents (agent configuration files): "**rm –r /etc/versiera**"
4. Delete the **vrsagent** directory and its contents (agent binary files): "**rm –r /usr/local/lib/vrsagent**"
5. Delete the **agentmond.log** file, if exists: "**rm –r /var/log/agentmond.log**"
6. Reboot the system

Solaris

1. Stop Versiera agent: "**/etc/init.d/agentmond stop**"
2. Verify agent is no longer running: "**ps -ef | grep vrsagent**"
3. Delete the **versiera** directory and its contents (agent configuration files): "**rm –r /etc/versiera**"

4. Delete the **vrsagent** directory and its contents (agent binary): "**rm –r /opt/vrsagent**"
5. Delete the **agentmond.log** file "**rm –r /var/log/agentmond.log**" (if exists)
6. Reboot the system

Windows

1. Use Services Management Console to stop "**Versiera Agent Monitor**" or use the command line interface to issue the command: "**net stop "Versiera Agent Monitor"**"
2. Using Windows Task Manager verify that "**vrsagent**" process is no longer running
3. Use Add/Remove Programs tool in the Windows Control Panel to Uninstall "**Versiera Agent x.x.x**"
4. Delete the "**Versiera Agent**" directory and its contents (agent binary and configurations files) using Windows Explore or the command line interface with the command: "**rmdir /S /Q C:\Program Files\NetCraft Communications\Versiera Agent**"
5. Delete the **vrsagent.log** file, if exists: "**del C:\Windows\vrsagent.log**"
6. Reboot the system

OpenWRT

1. Stop Versiera agent: "**/etc/init.d/agentmond stop** "
2. Verify agent is no longer running: "**ps -ef | grep vrsagent**"
3. Delete the **versiera** directory and its contents (agent configuration files): "**rm –r /etc/versiera**"
4. Delete the **vrsagent** directory and its contents (agent binary files): "**rm –r /opt/vrsagent**"
5. Reboot the network device

DD-WRT

1. Use the "**ps | grep vrsagent**" command to determine the **"agentmond**" process ID
2. Use the "**kill xxxx**", where *xxxx* is the "**agentmond"** process ID
3. Verify that the agent is no longer running: "**ps | grep vrsagent**"
4. Delete the **versiera** directory and its contents (agent configuration files): "**rm –r /jffs/etc/versiera**"
5. Delete the **vrsagent** directory and its contents (agent binary files): "**rm –r /jffs/opt/vrsagent**"
6. Delete the **agentmond.wanup** file (agent startup file) "**rm /jffs/etc/config/agentmond.wanup**"
7. Reboot the network device