Webmin How To Guide

Contents

Overview

Webmin is a third party package present on Version 2 and Version 3 Swivel Appliances. It has many administrative functions which are of particular use during a support incident, rather than day-to-day administration:

- Retrieving files from the Swivel appliance (we recommend ?WinSCP? as an alternative);
- Inspecting the MariaDB Swivel database;
- Stopping or Starting services (Most of these can be managed from the appliance console).

Webmin is often useful when it is not possible to get a connection using PuTTY or WinSCP over SSH, such as when access is restricted. For more information on using PuTTY and WinSCP, see the PuTTY How To Guide and WinSCP How To Guide.

This article describes how to login to Webmin on an appliance. To discover more about how Webmin can be used to support Swivel, see the Common Uses for Webmin section below.

Prerequisites

- Swivel version 2 or 3 appliance (hardware or virtual machine) with Webmin installed;
- Web browser to connect to the Swivel server;
- Webmin login credentials.

Accessing Webmin

WARNING: Webmin does NOT start automatically by default on Version 3 Appliances. You can enable Webmin from the CMI menu, under Appliance > Default Running Services > Webmin. Note that this does NOT start Webmin immediately - it just causes it to start automatically when the appliance starts. To start it immediately, use Appliance > Start or Stop Services.

The default URL for Webmin is:

https://192.168.0.35:10000/

(where 192.168.0.35 is replaced by your Swivel appliance IP. By default a single appliance is 192.168.0.35 and primary and secondary appliances are by default 192.168.0.36 and 192.168.0.37 respectively).

The default credentials are:

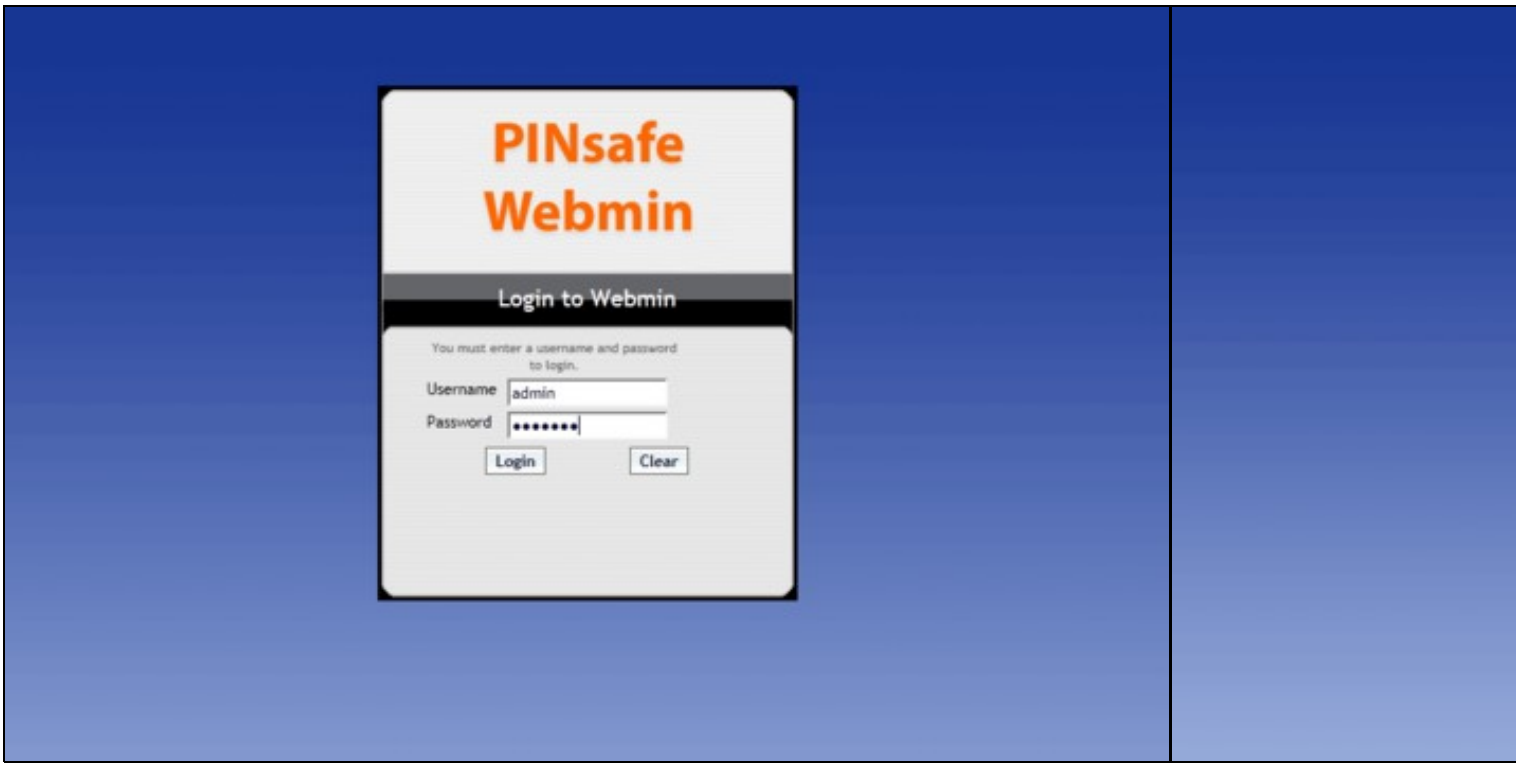
- Username: admin
- Password: lockbox

Note that the Webmin password is not changed when you change the appliance console password. You must change the Webmin password within Webmin itself.

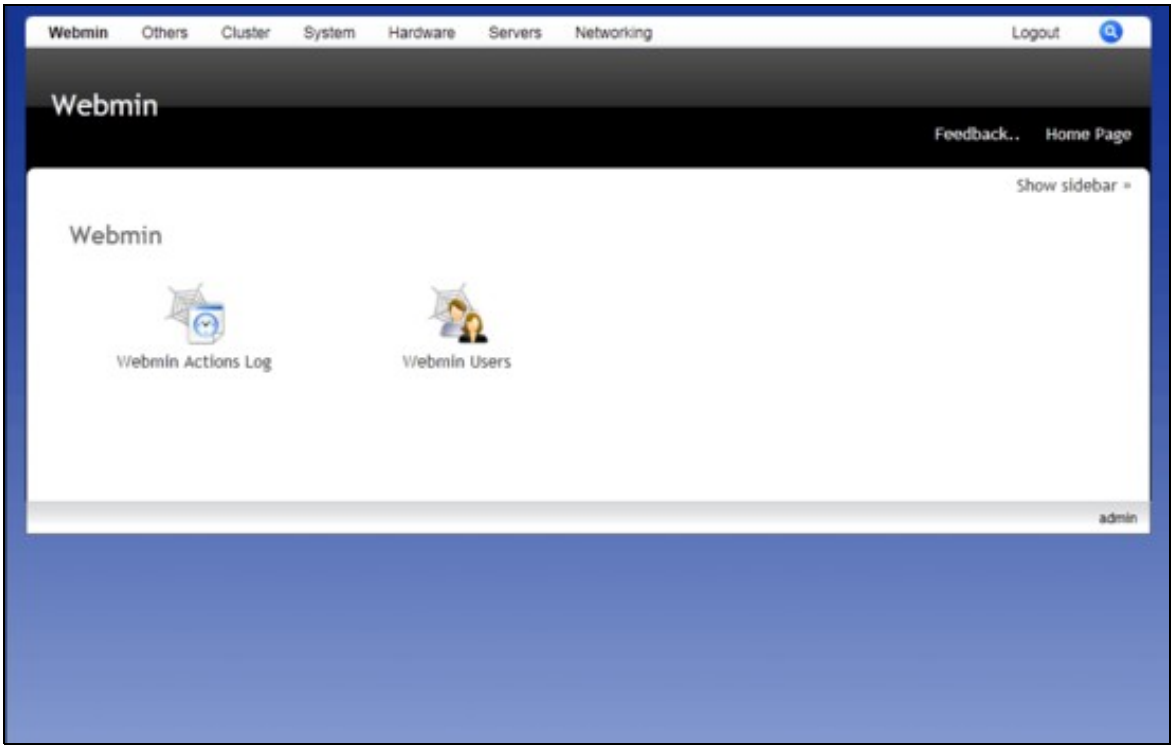
Logging in

Using a Web browser, visit the URL given above (https://192.168.0.35:10000/) using the IP address or hostname you have assigned to your Swivel appliance.

You should reach the following page, where you can enter the default credentials given above, to login (the former on v2 and the latter on v3):



Once logged in, you should see the following screen:



If for some reason you cannot establish a connection to the web page, then consult the Troubleshooting section below.

Webmin guides

128-bit encryption enforcement How to Guide

Troubleshooting

Changing the Web Certificate

Generate a New Certificate

The instructions below describe how to install a 2048-bit certificate for Webmin (original source: http://blog.rimuhosting.com/2014/11/18/webmin-sec-err-invalid-key/).

- Log into the appliance console.
- Go to Advanced Menu, Command Line. If you do not know the command line password, please contact support@swivelsecure.com
- Enter the following commands:

```
file=/etc/webmin/miniserv.pem

openssl req -x509 -newkey rsa:2048 -keyout $file  -out $file -days 3650 -nodes -subj \
 "/C=GB/ST=West Yorkshire/L=Wetherby/O=Swivel Secure/CN=pinsafe.swivelsecure.com"

openssl x509 -x509toreq -in $file -signkey $file >> $file

service webmin restart
```

In the above commands, replace the subject with values appropriate to your own country, state, city, company and server name.

Using an Existing Certificate

If you already have a certificate that is suitable for use - for example, if you want to re-use the same certificate as Tomcat uses, you can convert it to the correct format using Keystore Explorer.

- Open the certificate (PFX or Java Keystore) in Keystore Explorer.
- Right-click on the certificate, click Export then Export Key Pair.
- Select PEM as the format and don?t enter a password. Save the file.
- Upload the resulting file to the appliance.
- From the appliance command line, take a backup of /etc/webmin/miniserv.pem
- Copy your new PEM certificate and overwrite /etc/webmin/miniserv.pem.
- Restart webmin as above.

Cannot Access Webmin

NOTE On a Version 3 Appliance, the Webmin service is now disabled by default and must be enabled via the CMI menu (Main Menu -> Appliance -> Start or Stop Services -> Start webmin).

- Is port 10000 being specified in the browser address bar?
- Is network access to the appliance available, can you ping the appliance?
- Is port 10000 blocked by an intermediary firewall? Can you telnet to port 10000 from your workstation?
- Is SSL specified in the request using https?

IE / Firefox will not login to Webmin

This affects appliance versions up to 2.0.14 and is due to Internet Explorer preventing login to websites with key lengths of less than 1024 bits. Recent versions of Firefox also exhibit the same behaviour. Use another web browser to access the appliance or upgrade to a more recent version of appliance.

If you do not wish to use an alternative browser, then you can enable the "Continue to this website" button in IE, by running the following command on the **Windows Command Line**:

```
certutil -setreg chain\minRSAPubKeyBitLength 512
```

This is mentioned in the article:

http://support.microsoft.com/kb/2661254

If you want to revert this change, run:

```
certutil -delreg chain\MinRsaPubKeyBitLength
```

If you prefer to update your certificate to 2048 bits, use the routine detailed above to change the certificate.

Webmin not running?

NOTE On a Version 3 Appliance, the Webmin service is now disabled by default and must be enabled via the CMI menu (Main Menu -> Appliance -> Start or Stop Services -> Start webmin).

If you find that you cannot obtain Webmin access, check to see that Webmin is listening for connections. Login to the appliance via SSH using PuTTY (see the PuTTY How To Guide) and get to the command line:

Enter the following netstat command. If you return a result similar to this then you know that Webmin is installed and running.

```
[admin@appliance ~]# netstat -anp | grep 10000
tcp        0      0 0.0.0.0:10000               0.0.0.0:*                   LISTEN      3594/perl
udp        0      0 0.0.0.0:10000               0.0.0.0:*                               3594/perl
[admin@appliance ~]#
```

If this returns nothing then it could indicate that Webmin is not installed. If this is the case try running the following commands to see if the package exists on the appliance:

```
[admin@appliance ~]# find /etc/ -iname webmin
/etc/sysconfig/daemons/webmin
/etc/pam.d/webmin
/etc/webmin
/etc/webmin/webmin
/etc/rc.d/init.d/webmin
[admin@appliance ~]#
```

Also:

```
[admin@appliance ~]# whereis webmin
```

```
webmin: /etc/webmin /usr/libexec/webmin
[admin@appliance ~]#
```

If you don't return a result, then it's likely that your appliance is too old to have Webmin installed. If you do return a result then you can use the following stop and start commands to get Webmin stopped and started:

```
[admin@appliance ~]# service webmin stop
Stopping Webmin server in /usr/libexec/webmin
[admin@appliance ~]# service webmin start
```

A further check of the listener will confirm if Webmin is now started:

```
[admin@appliance ~]# netstat -anp | grep 10000
tcp        0      0 0.0.0.0:10000               0.0.0.0:*                   LISTEN      3185/perl
udp        0      0 0.0.0.0:10000               0.0.0.0:*                               3185/perl
[admin@appliance ~]#
```

If you're not bringing up anything via a Web Browser check that there are no firewalls between you and the Swivel appliance which could be obstructing access. Try the following command to reveal the Swivel firewall entries, to ensure that the Swivel appliance is allowing access to the Webmin listener:

```
[admin@appliance ~]# cat /etc/sysconfig/iptables
```

This will produce the following output.

```
[admin@appliance ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 694 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 1311 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
[admin@appliance ~]#
```

Ensure that the following ACCEPT line (highlighted in the output above) exists, to be sure that Swivel is allowing access to the Webmin listener:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
```

Webmin inaccessible after patch upgrade

Edit the file /etc/webmin/miniserv.conf locate the line ssl_version=10 line and remove it. Restart webmin with;

```
service webmin restart
```

Locked out of Webmin?

Using the PuTTY How To Guide SSH to the appliance, goto the Command Line and enter the following command:

```
/usr/libexec/webmin/changepass.pl /etc/webmin/ admin lockbox
```

This will reset the password for the admin user to lockbox.

Common Uses for Webmin

Below are articles which describe common use cases for Webmin:

- Timezone
- SQL commands in Webmin
- Password change for Webmin How to Guide
- Retrieving PINsafe backup files using Webmin
- MON Service Monitor How to guide
- How to run PINsafe on non-default ports
- ResetPIN How To Guide
- ChangePIN How to Guide