Release Notes:

Web OS Switch Software

Release 9.0

Alteon WebSystems
Web Speed for e-Business

50 Great Oaks Boulevard
San Jose, California 95119
408-360-5500 Main
408-360-5501 Fax
www.alteonwebsystems.com

Part Number: 050160, Revision A, May 2001

Release Notes

The *Web OS 9.0 Release Notes* provide the latest information regarding your Alteon WebSystems switch with Web OS 9.0 software. This document modifies information found in the complete documentation:

- *Web OS 9.0 Command Reference* (part number 050158, Revision A)
- *Web OS 9.0 Application Guide* (part number 050159, Revision A)

Please keep this information with your Alteon WebSystems product manuals.

Supported Platforms

Web OS 9.0 is supported on the Alteon 180e, Alteon 184, Alteon AD3, and Alteon AD4 Web switches.

New Features

The following major features have been added for Web OS 9.0:

- Real Time Streaming Protocol (RTSP) load balancing
- Wireless Application Protocol (WAP) load balancing
- Intrusion Detection System (IDS) load balancing
- Delayed binding to prevent Denial-of-Service (DoS) SYN attacks
- Content intelligent Precedence Lookup
- Web switch Cookie Insertion for cookie-based persistence
- Regular expressions matching for content intelligent features
- Response Time and Bandwidth load balancing metrics
- Wide Area Network (WAN) link load balancing
- Free-metric Firewall Load Balancing (FWLB)

Details on these features can be found in the Web OS 9.0 manuals.

Additions and Improvements

- Concise display of configuration dump

  The switch now allows the display of configuration dump for only those parameters that are different from the default values.

- Allow ICMP in dynamic Network Address Translation (NAT)

  Web OS 9.0 allows internal servers to implement the ICMP function (`ping`, for example) to the Internet when the port is configured with dynamic NAT.

- Addition of Name to the IP Address

  In the Web OS 9.0 Browser-Based Interface (BBI), the user can add a name (for example, the name of the server) to the IP address on the dashboard of the switch.

- Increased Number of Characters in the Real Server Name

  The number of characters in the real server name has been increased from 15 characters to 31 characters.

- Increased Number of Filters

  The number of filters has increased from 224 to 2048 on the Alteon AD4 and Alteon 184 Web switches.

Installing Web OS 9.0

TFTP Software Installation

Because TFTP software downloads retain the switch configuration throughout the upgrade process, this method is preferred when upgrading switch software.

Use the following procedure when upgrading your Alteon WebSystems switch software.

1. **Be sure that your Web switch is currently running Web OS 8.3.**

NOTE – You can upgrade to Web OS 9.0 only from Web OS 8.3. If running Web OS software prior to version 8.3, obtain and follow the upgrade instructions found in the *Web OS 8.3 Release Notes* (part 050145A). The switch must be running Web OS 8.3 prior to continuing with the upgrade.

---

2. **Backup the current Web OS 8.3 configuration to a file (optional, but recommended).**

   You may obtain a configuration backup either though a TFTP configuration upload to a file or by copying the contents of the configuration dump to a file.

```
>> # /cfg/ptcfg
Enter hostname or IP address of TFTP server:
Enter name of file on TFTP server:
```

3. **Perform a TFTP download of the Web OS 9.0 software code onto the switch.**

```
>> # /boot/tftp
Enter name of switch software image to be replaced
  ["image1"|"image2"|"boot"]:
Enter hostname or IP address of TFTP server:
Enter name of file on TFTP server:
```

4. **Select the new Web OS 9.0 image for use upon reboot, and reset the switch.**

```
>> Boot Options# image
Currently set to use switch software "image1" on next boot.
Specify new image to use ["image1"/"image2"]:
>> Boot Options# reset
```

Direct Serial Upgrade

To upgrade to Web OS 9.0 directly from any different image, you can perform a serial download of the new switch software. However, serial download will reset the switch configuration back to its factory defaults.

This procedure requires the following:

- A computer running terminal emulation software
- A standard serial cable with a male DB9 connector (see your switch hardware installation guide for specifics)
- A *binary* switch firmware image (*not* the `tfpt` file used for TFTP download)

Use the following procedure to perform a serial upgrade.

1. **Using the serial cable, connect the computer to the switch Console port.**
2. **Make sure that the new binary firmware file is available on the computer.**
3. **Start your terminal emulation software and set the communication parameters:**

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1

4. **Turn on the switch power and press <Shift-F> while the switch is first attempting to boot.**

   When performed correctly, the following message appears:

```
Xmodem flash download 1.0.5
To download to flash use xmodem at 57600 baud
Power cycle to end xmodem.
```

5. **Reconfigure your terminal emulation software for the following parameters:**

Parameter	Value
Baud Rate	57,800
Data Bits	8
Parity	None
Stop Bits	1

6. **Set the file transfer mode to Xmodem.**

7. **Transfer the binary firmware image file to the switch.**

   This process can take three or four minutes to complete. When finished, the message “done” will appear on your terminal.

8. **Disconnect the terminal emulation session and reconfigure your terminal emulation software for normal switch connection parameters:**

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1

9. **Reconnect the terminal session to the switch.**

10. **Turn the switch power off, and then back on again.**

    The switch should now boot normally.

Retrograde Procedure

NOTE – Retrograding from Web OS 9.0 to earlier versions without following this procedure will result in configuration loss.

1. **Backup the current Web OS 9.0 configuration to a file.**

2. **Perform a TFTP download of the Web OS 8.3 software code onto the switch.**

3. **Reset the switch to its factory defaults.**

4. **Select the new Web OS 8.3 image for use upon reboot, and reset the switch.**

5. **Get the desired switch configuration.**

   - To restore the Web OS 8.3 configuration to the original settings prior to the upgrade, you can use the configuration backup created during the upgrade procedure.
   - To use the configuration for Web OS 9.0, get the configuration file created in Step 1 above. Any Web OS 9.0-specific configurations will be lost when you retrograde the software. An error message may appear on your display.

NOTE – If you have saved the switch configuration to a TFTP server, temporarily add one IP interface to reach the TFTP server. If the TFTP server is on the same subnet, use `ping` to test the connection. If the TFTP server is on another subnet, add a default gateway to the other network. These settings will be overwritten once you have loaded the configuration file.

Feature Configuration Notes

Telnet

Telnet access is disabled by default. To enable Telnet access to the switch, connect to the switch via the console port and enter the following command:

```
>> # /cfg/sys/tnet ena
```

NOTE – Remember to configure an IP interface on the switch so that you can access the switch via Telnet.

SNMP

Simple Network Management Protocol (SNMP) is disabled by default. To enable SNMP access, enter one of the following commands:

```
>> # /cfg/sys/snmp write     (for read-write access)
>> # /cfg/sys/snmp read      (for read-only access)
```

Browser-Based Interface

The BBI is supported only on the Alteon AD4 and Alteon 184 Web switches. By default, the BBI is disabled. To enable this feature on the supported platforms, enter the following command:

```
>> # /cfg/sys/http ena
```

NOTE – Remember to configure an IP interface on the switch so that you can access the switch via your Web browser.

Configuration Dump

The output file from the `ptcfg` command is formatted with line breaks but no carriage returns, and thus cannot be viewed with editors that require carriage returns (such as MS Notepad).

SecurID

There is no SNMP or BBI support for SecurID because the SecurID server, ACE, is a one-time password authentication and requires an interactive session.

Secure Shell and Secure Copy

The following tips and restrictions apply for the Secure Shell (SSH) and Secure Copy (SCP) features:

- These features have been tested with the following SSH clients:
  - SSH client version SSH 1.2.27 and 1.2.23 for Linux (freeware)
  - SecureCRT 3.0.2 and 3.0.3 for Win NT
  - F-Secure SSH 1.1 for Windows from Data Fellow. (It will accept all clients which have version identification “SSH-1.5-1.X.”)
- The Web switch SSH daemon uses TCP port 22 only and is not configurable.
- The configuration of SSH/SCP parameters can only be performed using the console port.
- The maximum number of simultaneous Telnet/SSH/SCP connections is four.
- The Web switch will perform only one session of key/cipher generation at a time. Thus, an SSH/SCP client will not be able to log in if the switch is performing key generation at that time or if another client has logged in immediately before. Also, key generation will fail if an SSH/SCP client is logging in at that time.
- The `/cfg/sys/radius/telnet` command also applies to SSH/SCP connections.
- The `scpadmin` login is only useful when the `scp` command is to be used with RADIUS and SecurID authentication.
- The `scpadmin` login should not be given the same password as any other user, administrator, or operator. Logins using a password that is the same as the `scpadmin` password will be logged in as `scpadmin`.

Delayed Binding

When enabling delayed binding to protect against DoS SYN attacks, either Direct Access Mode (DAM) must be enabled or a proxy IP address must be configured for client ports.

FTP Parsing Servers

The following tips and restrictions apply when using the enhancements for passive FTP:

- You must use either DAM or a proxy IP address.
- This feature does not support different FTP modes within a single session; that is, the user cannot switch from active to passive or vice versa in the same FTP session.
- FTPP with port mapping is not supported.
- Performance may be impacted when URL parsing is used.

RTSP and GSLB

Global Server Load Balancing (GSLB) cannot be used for RTSP traffic.

WAP Load Balancing

When using WAP load balancing in RADIUS snooping mode, IDS load balancing must be disabled.

IDS Load Balancing

The following tips and restrictions apply for the IDS load balancing feature:

- A default `allow` filter must be configured for all ports where IDS load balancing is enabled.
- Only one IDS load balancing group is supported on each Web switch.
- The link health check applies only to the IDS load balancing group. It will not function with other types of load balancing. Also, the link health check will declare the IDS servers up or down based on the status of the link rather than the status of the service.
- The round-robin (`roundrobin`) metric is not supported with FTP load balancing solutions in combination with IDS load balancing. Use `hash` or `minmisses` instead.

WAN Link Load Balancing

The following tips and restrictions apply for the WAN link load balancing feature:

- Gateways configured as real servers must be on different subnets.
- Proxy IP addresses on ports connected to gateways must also be on different subnets.

TOS Rewrite

Type-of-Service (TOS) rewrite is only applicable when defining a filter with the `allow` action.

VMA with Single Proxy IP Address

Web OS 9.0 supports configuration using a single proxy IP address on all ports with Virtual Matrix Architecture (VMA) enabled under special cases. To do so, the following limitations must be observed:

- Proxy must be disabled on real servers.
- One-armed SLB configuration is not supported.
- NAT is not supported on the client ports.

Script-Based Health Check

Health check scripts can only be configured through the Command Line Interface (CLI), but once entered can be assigned as the health check method using SNMP or the BBI.

WTLS Health Checks

WTLS health checks are performed only for connection-oriented port 9203. Health for connectionless port 9202 is not independently checked. Servers on ports 9202 and 9203 are both marked as up or down based on the result of the port 9203 health check.

WSP Health Checks

The following tips and restrictions apply when using the WSP health check feature:

- The WSP health check feature is only available on the Alteon 184 and Alteon AD4 platforms.
- The buffer size of WSP health check content is limited to 255 bytes.
- This feature supports only Nokia WAP application gateways.

Stateful Failover

The following tips and restrictions apply when using Stateful failover:

- New sessions created after the last update between active and standby switches will be lost if the active switch fails.
- Stateful failover requires VMA to be enabled.
- Ensure that the switches are using the same version of Web OS software.

GSLB Static Client Proximity

The following tips and restrictions apply for the GSLB Static Client Proximity feature:

- The switch supports only a single domain.
- No health checks or `pings` are supported for virtual servers.
- The switch replies with only one virtual server IP address, based on response time and minimum connection (`mincon`) value.

GSLB with VRRP

When using both GSLB and Virtual Router Redundancy Protocol (VRRP), you must change the `/cfg/sys/wport` (BBI port) value of the target switch (the switch that is being synchronized) to a port other than port 80 before VRRP synchronization begins.

Firewall Load Balancing with VMA

The VMA feature must be enabled in certain Firewall Load Balancing (FWLB) situations. When setting up FWLB with clean-side switches performing Server Load Balancing (SLB) or URL-based SLB, if DAM is enabled, then VMA must be also be enabled.

VPN Load Balancing

The following tips and restrictions apply when using Virtual Private Network (VPN) load balancing:

- VPN load balancing and generic NAT cannot be configured on the same switch at the same time.
- VPN load balancing requires VMA to be enabled.
- The VPN load balancing feature is supported only for VPN vendors with cluster IP addressing capability.
- VPN load balancing requires the `hash` metric.
- Six-subnet VPN load balancing is not supported because all VPN devices must be on the same subnet. In six-subnet VPN load balancing, the VPN devices are on different subnets.
- Ports configured for VPN load balancing may *not* have filtering enabled.

Layer 7 Statistics

Statistics for Layer 7 header matching has been removed from the virtual server statistics. However, these statistics are still available in the Layer 7 string statistics. Only Layer 7 cookie header matching statistics are still available in the virtual server statistics.

URL Parsing with Content Intelligent Persistence

Tips and Limitations

The following tips and restrictions apply when using URL-based SLB or Web Cache Redirection (WCR) with cookie-based or Secure Sockets Layer (SSL) session ID persistence:

- VMA is recommended when using any content intelligent switching feature.
- You must use either DAM or a proxy IP address.
- Precedence for load balancing/persistence algorithms are:
  - Persistence-based load balancing (Cookie, SSL Session ID, or Client IP-based persistence)
  - HTTP Header or URL-based load balancing (cookie-based preferential service, or host header-based load balancing for virtual hosting, or load balancing based on the URLs)

Capacity Summary

- Supports up a maximum of 4500 bytes in a single request
- Cookie information

  Cookie name of up to 20 bytes with support of wildcard “*”

  Cookie value for hashing of up to 64 bytes
- URL-based and HTTP Header-based SLB

  Up to 128 substrings

  Maximum length of 40 bytes per substring
- URL-based WCR

  Up to 32 expressions

  Maximum length of 8 bytes per expression
- Hashing based on URL

  Maximum of 255 bytes to hash

URL Parsing with VRRP Active/Active Setup

When URL-based SLB is used in a VRRP active/active redundant setup, do not use DAM. Instead, use a proxy IP address.

Content Precedence Lookup

When using the content precedence lookup to combine Layer 7 load balancing features, some combinations can be redundant or nonsensical and are not supported. For example, when cookie-based persistence is used with Layer 7 URL SLB and URL Hashing, no resolution is possible and the condition will never be matched.

Bandwidth Management

The following tips and restrictions apply for the Bandwidth Management (BWM) feature:

- VMA is recommended when BWM is enabled.
- When both Filter TOS and BWM TOS are applied, the BWM TOS has precedence.
- BWM configurations will not be synchronized during VRRP synchronization.
- The maximum hard limit for a bandwidth policy is 1 Gbps, even when multiple Gigabit ports are trunked.
- When using cookie-based BWM, it is recommended that it be used with Preferential Cookie or any other URL application that can be assigned with string ID.

Late-Breaking News and Support

Web access: http://www.alteonwebsystems.com

Questions? Check the URL for Alteon WebSystems Online Information. This web site includes product information, software updates, release notes, and white papers. The web site also includes access to Alteon WebSystems Customer Support for accounts under warranty or that are covered by a maintenance contract.