



Devicescape Enterprise- Managed AP Release Notes

**Release 1.1
23 March 2005**

Devicescape Enterprise-Managed AP Release Notes

Release 1.1

Copyright © 2005 **Devicescape Software, Inc.**, 1000 Marina Blvd., Brisbane, CA 94005. All rights reserved.

This product and documentation are protected by copyright and distributed under licenses and/or non-disclosure agreements restricting their use, copying distribution, and decompilation. No part of this product or document may be reproduced in any form by any means, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) for any purpose, without prior written authorization of **Devicescape Software, Inc.** ("Devicescape") and its licensors, if any.

Devicescape may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Devicescape, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED INTO NEW EDITIONS OF THE PUBLICATION. DEVICESCAPE MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

The Devicescape Enterprise-Managed AP product from **Devicescape Software, Inc.** incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, **Devicescape Software, Inc.** will make available, upon written request, a complete machine-readable copy of the source code components, and only those source code components, that are covered by the GNU GPL. Written requests for this source code distribution should be directed via email to support@devicescape.com. For further information on the GNU GPL, please see <http://www.opensource.org/licenses/gpl-license.php>.

Ver. 23 March 2005-1.1

Trademarks

Devicescape Networks and the Devicescape Networks logo are trademarks of **Devicescape Software, Inc.** and/or its affiliates in the US and other countries.

All other registered and unregistered trademarks in this document are the sole property of their respective owners.

You must accept the enclosed License Agreement before you can use this product. If you do not accept the terms of the License Agreement, you should promptly return the product.

Release	Date	Description
1.1	23 March 2005	Devicescape Enterprise-Managed AP Release Notes

Contents

Release Notes for Instant802™ Self-Managed AP	1
Release Contents	1
Supported Platforms.	1
Documentation and Online Help.	2
What's New in Release 1.1?	2
Known Problems	3
Cluster Recovery	7
Resolved Problems.	7

Release Notes for Devicescape Enterprise-Managed AP

Release	Date	Description
1.1	February 22, 2006	Devicescape Enterprise-Managed AP

The following topics are included in these release notes:

- Release Contents
- Reference Platforms
- Documentation and Online Help
- What's New in Release 1.1?
- Known Problems
- Resolved Problems

Release Contents

The Devicescape Enterprise-Managed AP 1.1 release contains the following components:

- Devicescape Enterprise-Managed AP software binary executables for each supported target systems as described below. Please contact your Devicescape Sales Representative for information on how to get the AP software binaries for a specific target platform.
- Web-based AP Administration User Interface (UI) for configuring and monitoring one or more stand-alone or clustered APs

Reference Platforms

The following table shows the hardware platforms used by Devicescape for quality assurance testing. Many other platforms are supported. Please contact your Devicescape Sales Representative for a complete list.

Target System	Description
Gateway GW7001AP	CPU: Intel IXP-422 RAM: 32MB Flash Memory: 8MB Console Speed: 115200

Target System	Description
Netgear® WGT624	CPU: Atheros AR2312 System-on-a-Chip (SoC) RAM: 16MB Flash Memory: 4MB Console Speed: 115200
Coyote	CPU: Intel IXP-425 RAM: 32MB Flash Memory: 8MB Console Speed: 115200
x86 PC	CPU: Standard PC RAM: 32MB Flash Memory: Console Speed: 115200

Documentation and Online Help

To view the full set of documentation for the Instant802™ Self-Managed AP as HTML or PDF documents, please visit the online documentation site for this product at <http://www.devicescape.com/docs/smap/index.php>. You will need a client password to view the documentation. If you do not have one, please contact your sales representative.

The documentation set includes these Release Notes, an Evaluation Guide, a Manufacturers Guide, and an Administrators Guide.

Online Help for the Web-based AP Administration UI is integrated into the UI.

Documentation source files and templates for the Administrators Guide, Glossary, and Online Help are available to all Instant802 customers. For more information, please see the section Documentation Re-use Kit for Devicescape Customers in the Administrators Guide introduction.

What's New in Release 1.1?

Cluster Neighborhood - Shows all access points within range of every member of the cluster, shows which access points are within range of which cluster members, and distinguishes between cluster members and non-members. By showing which APs are visible at what signal strength from other APs, the Cluster Neighbors view can help you detect rogue APs, verify coverage expectations, and detect faults.

Channel Management - Automatically assigns radio channels used by clustered access points to reduce mutual interference (or interterference with other access points outside of its cluster). Channel Management maximizes WiFi bandwidth and helps maintain efficiency of communication over your wireless network.

Enhanced VLAN Capabilities. Now configure Virtual Wireless Networks as needed. You can still set up Guest and Internal networks on physically separate networks or Virtual LANs (VLANs), just as before, but now you can also set up multiple Internal networks on VLANs as needed.

Backup and Restore of AP Configuration. Save a copy of the current settings on the Devicescape Enterprise-Managed AP to a backup configuration file. The backup file can be used at a later date to restore the access point to the previously saved configuration.

Backup and Restore of User Database. User management and authentication on the access point is available for use with Security modes IEEE 802.1x and WPA with RADIUS security modes. Now, save a copy of the current set of user accounts on the AP to a backup configuration file. The backup file can be used at a later date to restore the user accounts on the AP to the previously saved configuration.



Command Line Interface (CLI) for Configuring the AP. In addition to the Web based user interface, the Devicescape Enterprise-Managed AP now includes a command line interface (CLI) for administering the access point and wireless networks. The CLI lets you view and modify status and configuration information, and offers some advanced configuration options not available from the Web UI.

SNMP MIBs. The 1.1 release of the Devicescape Enterprise-Managed AP ships with the following standard Simple Network Protocol (SNMP) Management Information Bases (MIBs):

- SNMP v1 and v2 MIBs
- IEEE802.11 MIB
- An Instant802 proprietary MIB, based on the upcoming IEEE 802.11k MIB

Known Problems

The following table summarizes problems that have been identified in the Devicescape Enterprise-Managed AP software.

Bug Numbers	Description	Workaround
2735, 2737, 2662, 2705	<p>Various events or actions such as shutdown (power outage) or removal of an access point may cause problems with joining or removing an access point from the cluster, or with other aspects of a configuration sharing.</p> <p>Some of these problems may be indicated by a red status message at the bottom of the Administration Web page. (For example, activator timed out.)</p>	<p>Reset the access point.</p> <p>Navigate to Advanced > Reset Configuration on the access point and click the "Reset" button.</p> <p>(See "Cluster Recovery" on page 8 for more information.)</p>
2896	<p>MAC Address Filtering supports up to 200 addresses. However; while the Administrator is entering MAC addresses in Advanced > MAC Filtering, the Web Administration pages may become unreachable. This will not result in loss of data already entered, nor will it prevent users from accessing the access point or transmitting / receiving data.</p>	<p>Reboot the access point and continue adding MAC addresses up to the 200 address limit.</p>
2894	<p>If there are more than 50 clients associated to the access point, information on client sessions will be unavailable (Cluster > Sessions on the Administration Web pages) and in such cases Administrators should avoid clicking on this tab.</p> <p>Clicking on the Cluster > Sessions tab when (a) there are more than 50 clients associated and (b) the access point is set to use the built-in authentication server (with either IEEE 802.1x or WPA with RADIUS security modes) will cause clients to temporarily lose connectivity to the access point. (If the built-in authentication server is not used, clients will retain connectivity.)</p>	<p>If you know there are more than 50 clients associated to the access point, do not click on the Session Monitoring tab.</p> <p>If you do access the Session Monitoring tab, the page will not display accurate session information. Also, be prepared for a potential brief break in network service for clients using the built-in authentication server.</p>
3001	<p>Wireless clients will fail to associate when trying to connect to an AP using WPA with RADIUS security mode with the option "Allow non-WPA IEEE 802.1x clients" enabled.</p>	<p>Do not enable the option "Allow non-WPA IEEE 802.1x clients" when using WPA with RADIUS security mode.</p>
3155	<p>Putting an access point in standalone mode too quickly can cause the clustering subsystem to get stuck in the "seeking" stage.</p> <p>On the Basic Settings tab, there is an option under "Set Configuration Policy for New Access Points ..." to change how new access points are configured. If you reset this from "are configured automatically" to "are ignored" before clustering has initialized, the access point will continue to look for the cluster indefinitely.</p> <p>To determine when clustering has initialized, monitor the cluster icons on the Basic Settings tab. When the top "not Clustered" icon changes to "Clustered" and the icon below it changes from "0 Access Points" to "1 Access Point" showing in the cluster, this means clustering is on and you can make policy configuration changes.</p>	<p>Do not reset the configuration policy until the access point has clustered with itself.</p> <div style="border: 1px solid red; padding: 5px; margin-bottom: 5px;"> <p>Wait:</p> <p>While AP shows as "Not Clustered", do not attempt to reset its configuration policy.</p>  </div> <div style="border: 1px solid green; padding: 5px;"> <p>Okay to Reset:</p> <p>When AP shows as "Clustered", you can proceed with resetting the configuration policy.</p>  </div>

Bug Numbers	Description	Workaround
3264	<p>Guest clients are not disassociated per load balancing settings.</p> <p>Load balancing settings are designed to distribute the amount of wireless traffic across multiple access points so that no single AP is handling a disproportionate share of the traffic. When load balancing is enabled, an AP identified as having too much traffic should be automatically relieved of some of its clients.</p> <p>For example, an AP set to a Station Threshold for Disassociation of "4", should never have more than four (4) clients associated. However, load balancing is not properly extending to the Guest Network. So a client set to a Station Threshold of 4 will maintain 4 clients on the Internal network, and any number of clients on the Guest Network since the Guest Network is not being taken into account.</p>	<p>In all cases, leave Load Balancing enabled on the access point so that the load on Internal Network is automatically regulated. Workarounds for the Guest Network problem are as follows:</p> <p>Disable the Guest Network on the access point that is experiencing the overload.</p> <p>Or</p> <p>Manually load balance the guest clients on the access point that is experiencing the overload as follows:</p> <ul style="list-style-type: none"> • View the Status > Client Associations tab to determine which clients are on the Guest Network. (You might want to monitor this over a period of time first.) Note their MAC Addresses. • Click Cluster > Sessions tab, choose "Utilization" from the drop-down menu, and click "Go". Note which guest clients (based on your list of MAC addresses) have high utilization percentages. You might also compare other measurements like "Idle Time" for guest clients to get a picture of utilization patterns. • Click Advanced > MAC Filtering and set up MAC Filtering to disallow those guest clients that are overloading the AP. This will have the affect of forcing those clients to disassociate and reconnect to a different AP.
3438	<p>The "Station Isolation" Security feature does not work over a Wireless Distribution System (WDS) link.</p>	<p>Keep in mind that you cannot rely on Station Isolation on a WDS link.</p>

Bug Numbers	Description	Workaround
3467	<p>If an access point is not in a cluster (either because it is stand-alone AP or in the process of joining a cluster):</p> <ul style="list-style-type: none"> Clicking Cluster > Channel Management tab on the Web UI shows "initializing . . ." phase and error for that feature Clicking Cluster > Wireless Neighborhood tab on the Web UI results in an error for that feature 	<p>Cluster tabs such as Channel Management and Wireless Neighborhood apply only to clustered APs. These features should not be accessible for stand-alone APs.</p> <ul style="list-style-type: none"> If you want to use the AP in stand-alone mode, do not expect to access Cluster features. The Channel Management and Wireless Neighborhood pages will show error messages instead of the "Join Cluster" option, which should be showing. If you encounter these errors while your AP is in the process of joining a cluster, refresh the Web page to make the Cluster features accessible (including Channel Management and Wireless Neighborhood.) If you want to add a stand-alone AP to a cluster, click Cluster > Access Points and then click "Join Cluster".
3478	See problem 3596.	
3555	<p>Clicking the "Back" button on Kickstart to attempt a re-scan for access points on the subnet gives unreliable results. All access points may not be found.</p> <p>Although it is reliable on the initial search for access points, Kickstart may not find all access points on the subnet on a re-scan.</p>	<p>If you need to re-run Kickstart, close the Kickstart application and then re-start it.</p> <p>Do not attempt a re-scan by using the "Back" button in Kickstart as it may not find all the APs this way.</p>
3580	When a WDS link is configured between the Guest interfaces of two access points, client stations connected to those APs are required to click through two, consecutive Guest Welcome screens (instead of one).	If you are using WDS linking for Guest networks, notify Guest users that they must click through two Welcome screens to log onto the Guest network.
3581	<p>When a WDS link is configured between the Guest interfaces of two access points, client stations connected to those APs cannot communicate with each other across these networks.</p> <p>Therefore, Guest client stations of APs on a WDS link cannot ping or telnet to one another, or exchange FTP traffic.</p>	<p>If Guest clients require communication with one another (such as for telnet or FTP), then do not route them through WDS-linked Guest networks.</p> <p>Instead, have these guests use the same Guest network.</p>

Bug Numbers	Description	Workaround
3586, 3625	<p>On Netgear WGT624 access points, and any other APs that have an outdated Atheros MAC revision for Wi-Fi Protected Access (WPA) and Wi-Fi Multimedia (WMM), the following problem will occur:</p> <p>If the Access Point is set to either of these Security modes:</p> <ul style="list-style-type: none"> • WPA/WPA2 Personal (PSK) • WPA/WPA2 Enterprise (RADIUS) <p>. . . and if Wi-Fi Multimedia (WMM) is enabled on the AP (it is enabled by default on the AP)</p> <p>. . . then clients set to WPA security mode with TKIP and to WMM at the same time will fail to associate or authenticate.</p>	<p>If you have Netgear WGT624 access points on your network, disable WMM on the access point and the clients when you want to use WPA security mode.</p> <p>(For other security modes, you can have WMM enabled.)</p>
(3478), 3596	<p>Radio mode, channel, internal and guest SSID may fail to synch on clustered APs.</p> <p>Case 3596: Changing the radio mode can kill kaffe and you can loose your config</p> <p>Case 3478: kaffe is restarted when security mode is modified on AP (Can't set security on clustered APs?)</p>	<p>Keep in mind that these settings may fail to cluster and reset manually on each AP as required.</p>
3622	<p>After enabling Virtual Wireless Networks on an access point in a cluster, you cannot make any more configuration changes on the AP.</p> <p>Note: This problem relates to the Instant802™ Enterprise-Managed AP only. These problems do not affect the Instant802™ Self-Managed AP.</p>	<p>On the Instant802™ Enterprise-Managed AP, avoid using Virtual Wireless Networks on a clustered AP.</p>
3647, 3649, 3650	<p>Errors in the Instant802™ Enterprise-Managed AP Web UI prevent users from configuring security modes other than plain text on VLANs through Web UI. Problems are detailed in several related cases:</p> <ul style="list-style-type: none"> • 3647: Static WEP security mode for VLAN 2 is not configurable from Advanced > Ethernet (Wired) settings Web page on Netscape and Mozilla browsers. • 3649: WPA-PSK security mode for VLANs is not configurable from the Web UI (Advanced > Ethernet and Advanced > Virtual Wireless Networks pages). • 3650: Web UI displays duplicate instances of fields for WPA/WPA2 Personal (PSK) and WPA/WPA2 Enterprise (RADIUS) security modes. <p>Note: These problems relate to the Instant802™ Enterprise-Managed AP only. These problems do not affect the Instant802™ Self-Managed AP.</p>	<p>On the Instant802™ Enterprise-Managed AP, use the CLI to configure security on VLANs after configuring VLAN IDs on Administrator UI:</p> <p>(1) Use the Administrator UI to set up the Virtual Networks VLAN IDs.</p> <p>(2) Use the command line interface (CLI) to configure security on the VLANs.</p> <p>For more information on using CLI to configure security, see Appendix C. Command Line Interface (CLI) for AP Configuration in the Administrators Guide.</p>
3662	<p>Static WEP security mode is not configurable for WDS links.</p>	<p>Do not use Static WEP security mode on a WDS link.</p>

Cluster Recovery

In cases where the access points in a cluster become out of sync or an access point cannot join or be removed from a cluster, the specific cluster recovery are recommended. For complete information, see Appendix B. Troubleshooting in the Administrators Guide (https://www.devicescape.com/docs/smap/AdminGuide/App_Troubleshoot.html).

Resolved Problems

The following table summarizes problems identified in previous releases of Devicescape Enterprise-Managed AP software that are fixed in this release.

Bug Numbers	Description	Workaround
2811, 2987	<p>IP address for access point may change when any of the following are changed on the Advanced > Ethernet (Wired) tab:</p> <ul style="list-style-type: none"> • When Guest Access is enabled • When the DNS name is changed • When the DNS Nameservers settings (Manual, Dynamic) are changed 	<p>Resolved in Release 1.1</p> <p>Use Kickstart or check DHCP logs to determine new IP address for access point.</p>
(2830) 3489	<p>A maximum number of 253 characters is allowed for a user name on the built-in authentication server. However, the User Name field on the Cluster > User Management tab incorrectly allows a user to enter up to 256 characters for a user name. The Online Help also incorrectly indicates that 256 characters (not 253) is the accepted maximum length.</p>	<p>Resolved in Release 1.1</p> <p>The access point allows a maximum of 253 characters for a user name on the built-in authentication server.</p> <p>When adding users on the Cluster > User Management tab, do not create user names longer than 253 characters.</p>
3002	<p>Enabling <i>Virtual LAN</i> (VLAN) mode (for Guest Access) on a clustered AP with a static IP address will cause the AP to behave unpredictably.</p>	<p>Resolved in Release 1.1</p> <p>Do not use these three settings (VLANs, static IP, and clustering) together. For example, you can do any one of the following:</p> <ul style="list-style-type: none"> • Use dual Ethernet mode to physically separate Guest and Internal networks (no VLANs). • Use DHCP (no static IP) and Guest Access on VLANs. • Set the AP to stand-alone mode. (In this mode you can use VLANs and a static IP with no problems.)