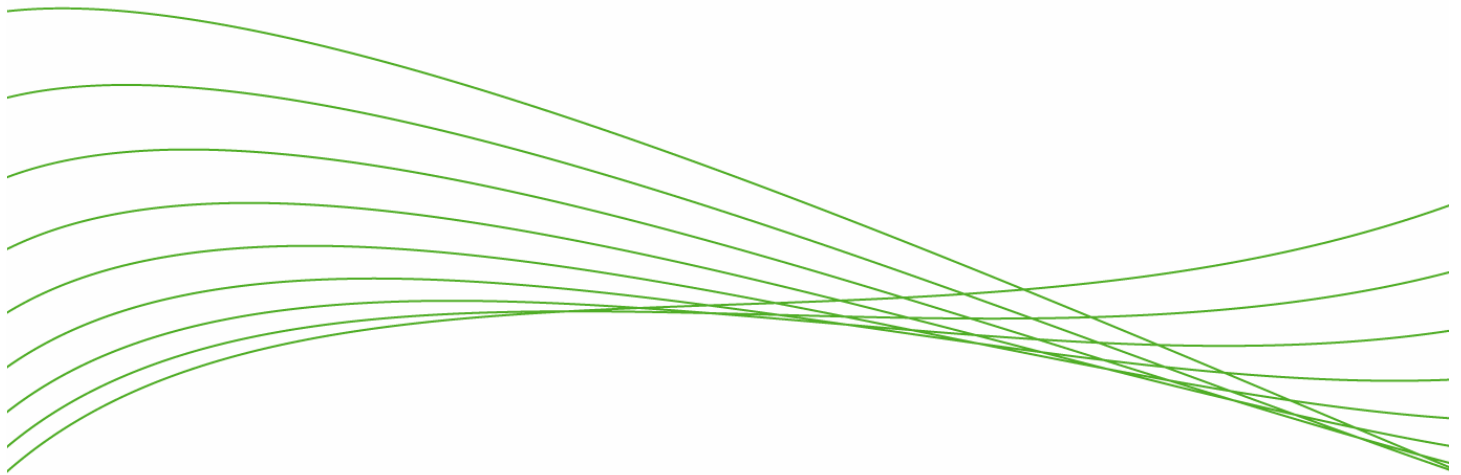


# ProCurve Secure Access 700wl Series Identity-based Access Control Technical Brief



Access Policy in the Wireless World .....	2
Determining User Identity .....	3
Who Is the User? .....	3
How Is the User Connected? .....	4
Determining the Access to be Granted to the User .....	4
Access Policy Example: ABC Company .....	5
Adding time and location restrictions .....	5
The Benefits of Access Policy Based on User Identity .....	8
For more information .....	10

## Access Policy in the Wireless World

As wireless access is added to wired networks in growing numbers of organizations, policy for controlling network access has become very important. Security is the driving factor, for more reasons than just encrypting the wireless data traffic. Most networks today implement some form of access and security policy; the challenge for wireless implementations is to work cooperatively within these policy structures.

One of the common methods for policy implementation in a wired network is through VLANs and ACLs. VLANs and ACLs, being port-based, work effectively in a switched network where we know a specific user is connected to a specific port. However, wireless is a shared medium rather than a switched medium, and one port does not map to one user. Therefore, a different policy method is needed for wireless users - a mechanism that is tied to the user identity, not to the port.

For example, in most wired organizations, each user has a network port at their desk. The network configuration takes advantage of this in setting access policies – it assumes that the user connected to the port at Mary's desk *is* user Mary and sets policies appropriate for the access Mary needs. The port at Joe's desk may allow different access rights based on Joe's needs. However, with the addition of a wireless access point, Joe and Mary now connect through the same network port, so setting access based on the port is no longer appropriate. The system needs to be able to differentiate between the traffic from Mary and the traffic from Joe, and enforce different access rules for each.

An additional challenge of wireless is that a user can appear anywhere in the network. By the very nature of wireless devices, they can easily move from one place to another. For example, now that Mary and Joe use laptops, they are no longer restricted to their desks, but may connect from conference rooms, the lobby, even the cafeteria. Again, in order to provide them with the appropriate access, this requires a policy implementation that is based not on the port, but on the identity of the user.

Finally, wireless signals are not bounded by physical barriers such as the walls of buildings or locked doors, so network security that relies on physical constraints such as cardkeys or other controlled, restricted access is no longer effective. For example, although the accounting department where Joe and Mary work has restricted access via cardkey control, it happens to be located physically next to the building lobby. This means that, due to the range of the wireless access point signal, any one in the lobby can attempt to access the network through the accounting department's wireless LAN. In fact, even though cardkey access to the department is restricted even further (to a few key people) after normal business hours, anyone parked on the street in front of the lobby can access the accounting wireless LAN 24 hours a day.

Figure 1 illustrates how access policies can be used to limit and control network access despite the lack of physical barriers inherent in a wireless deployment.



The 700wl series uses the concept of an “Identity Profile” to group like users together to simplify the application of access policies. Identity Profiles can be set up in the 700wl system to map to the group structure of the organization, and the 700wl series can directly map the group label received from an authentication service to an Identity Profile. A user’s access rights are determined, in part, by the Identity Profile with which he is associated.

## How Is the User Connected?

The other factor the 700wl series uses to decide what policy should apply is based upon *how* the user is connected to the network, which is a combination of where he or she appears (i.e. through which access point) and the time at which the user makes the connection.

The 700wl series uses the concept of a “Location” to distinguish between different points of entry to the wireless network. Locations can be used to identify the wireless access points installed at different physical locations – the building lobby, the manufacturing floor, the accounting department, and the cafeteria – and thus identify the user’s point of connection to the network. This in turn affects the access policy that applies to the user – for example, a different access policy might apply in a corporate lobby, even for known users, than would apply in an engineering lab, or a given employee might have different levels of access in different buildings in a corporate campus.

The time (time of day, day of the week) at which the individual is connected also may affect the access policy that applies. For example, a policy for contract employees may allow access only during working hours on weekdays. The 700wl series uses the concept of a “Time Window” to define time periods that have significance for access control. For example, a Time Window might be set up to define the work week as Monday-Friday, 8am – 5pm. Another example would be a Time Window set up to define a few consecutive days (for example, June 8-10) during which visiting customers should be given access to specific intranet sites relevant to their visit.

The 700wl series uses the concept of a “Connection Profile” to indicate how a user is connected to the network. A Connection Profile is defined primarily by Location and Time Window elements; the 700wl series can be configured to define these as needed for effective access control. The combination of the Location (access point) at which a user is detected, and the Time Window during which the connection occurs, determines the Connection Profile that applies to the individual user.

## Determining the Access to be Granted to the User

Once the user has been associated with an Identity Profile (based on who the user is) and a Connection Profile (based on how they are connected to the network) the 700wl series can determine the access policy for this user. The combination of the Identity Profile and Connection Profile determines the Access Policy that will be enforced for that user.

The 700wl system enables the creation of Access Policies that permit or deny access to a combination of applications, such as Internet or intranet web access, FTP, telnet, specialized application servers, or other network elements that can be identified by port and IP address. The ProCurve Switch xl Access Controller Module’s packet inspection engine enforces these policies by looking at the packets entering the system and determining how to handle them. The Access Policy in place for a specific user tells the packet inspection engine how to handle packets from that user.

For example, an access policy for network administrators would probably permit sending packets to network devices such as switches and routers for management and configuration of these devices, while the policy for regular company employees might deny this ability. Given the level of virus activity today, an Access Policy of this nature could enhance network availability by preventing non-administrator users from unwittingly causing damage to the network.

The 700wl series uses a Rights Assignment Table to associate Identity Profiles and Connection Profiles with Access Policies. Within this table, the combination of a specific Identity Profile and a specific Connection Profile gets associated with a specific Access Policy.

Once the 700wl series has determined a user’s Identity Profile (based on who the user is) and Connection Profile (based on how they are connected to the network), the system searches the Rights Assignment Table for a matching combination of profiles to determine the Access Policy it should apply to the user.



## Access Policy Example: ABC Company

The following example illustrates how the 700wl series rights management might be implemented within a hypothetical company, ABC Company, to control access to their corporate network.

The first thing the ABC company does in implementing the 700wl series rights management is set up Identity Profiles for the types of users they want to identify. The following Identity Profiles are created.

**Guest:** these are users who would not be recognized by ABC's authentication database, but for whom ABC want to allow Internet access. The 700wl series provides a guest logon feature that allows individuals to be associated with this Identity Profile without requiring authentication.

**Employees:** authenticated employee users will be associated with this Identity Profile.

**Finance:** specific authenticated users who require access to restricted financial data would be associated with this Identity Profile

**Any:** this is a default Identity Profile (pre-defined by the 700wl series) for users who do not match to any of the established Identity Profiles. The Identity Profile **Any** is usually restricted to allow only access to the logon process, and no other access.

These Identity Profiles allow the company to apply different Access Policies for Guests, Employees, and members of the Finance department.

If ABC Company uses the default Connection Profile **Any** provided by the 700wl series (which includes all locations – i.e. all access points – and has no time restrictions), then these Access Policies will be effective regardless of how the employee accesses the network. For example, an employee will have the same access rights whether he accesses the network from his desk, from the cafeteria during lunch, from the lobby on the weekend, or even from the parking lot at night, if there is a wireless access point within range.

### Adding time and location restrictions

Now suppose that ABC Company decides it wants to restrict access in the lobby and the cafeteria, even for employees, to safeguard confidential information, and to allow guest access only from the lobby, cafeteria, and conference rooms, and only during business hours. This requires creating an additional Connection Profile to allow this level of restriction.

The network administrator first creates a Location to identify the access points in the lobby, the cafeteria, and the conference rooms, and creates a Time Window that defines working hours (example: M-F, 7am-6pm). The administrator can then create a new Connection Profile, **Public**. ABC's system now has two Connection Profiles:

**Public:** defined as the locations for the lobby, cafeteria, and conference rooms, and constrained by the time window that defines working hours. Now, a user who connects from the lobby, cafeteria or a visitor conference room during working hours will match the **Public** Connection Profile. Note, however, that a user connecting outside of working hours will *not* match this Connection Profile, even though they connect through an access point in one of these public locations.

**Any:** still defined as access from anywhere with no time restrictions.

The administrator's goal is to allow network access as follows:

Guests should be granted Guest access only from the lobby, cafeteria and conference rooms, and only during weekday working hours.

Employees accessing the network from the lobby, cafeteria, or conference areas should not be able to access certain sensitive resources.

Employees in other parts of the plant should have normal employee access based on their Identity Profile (*Finance* or *Employee*)

To enforce these restrictions, the administrator adds to the 700wl's Rights Assignment Table new rows that map combinations of Identity Profiles and Connection Profiles to the Access Policies that define the appropriate access rights.

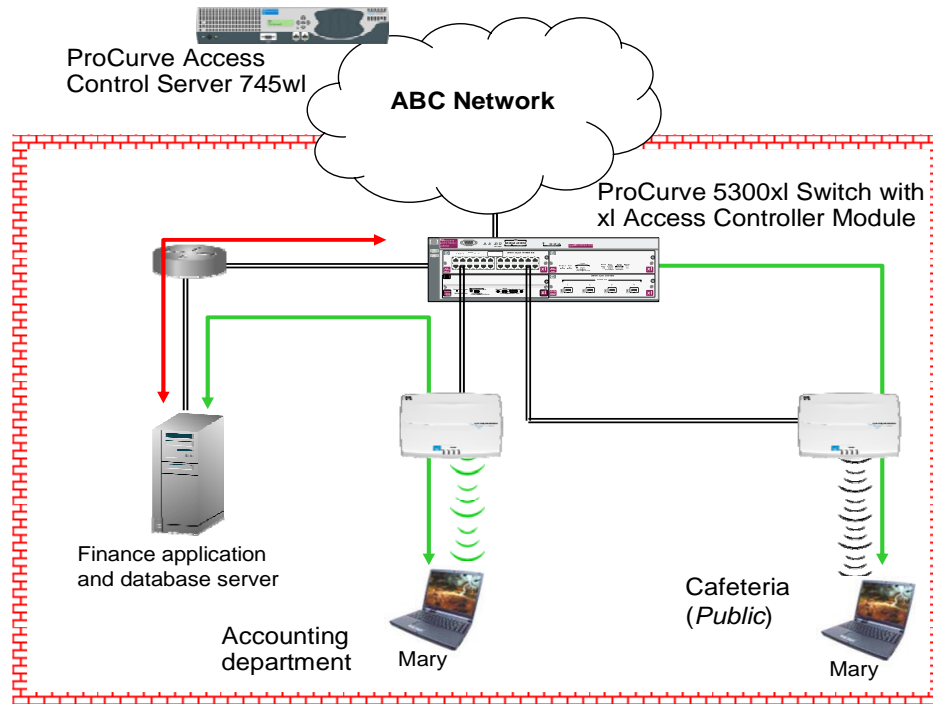
Identity Profile	Connection Profile	Access Policy
Guest	Public	Guest Access
Guest	Any	No Access
Finance	Public	Employee Restricted
Finance	Any	Finance
Employees	Public	Employee Restricted
Employees	Any	Employees

Table 1: Rights Assignment Table

The order of the rows in the table is important, because the 700wl series searches this table top down for a match to a combination of Identity Profile and Connection Profile, and stops at the first match it finds.

The following are examples of how the 700wl system determines the access policy that should apply to a user under different circumstances, based on the Rights Assignment Table the administrator had created.

1. Mary, a member of the finance department, logs into the network from her laptop at her desk:  
After authenticating successfully, Mary matches the Identity Profile Finance. She is not in one of the public areas, so she does not match the Public Connection Profile. Therefore, she matches the default Connection Profile Any and receives access rights based on the Access Policy defined for finance users. She can now access the finance department systems.
2. Mary goes to lunch in the cafeteria, taking her laptop with her:  
When Mary roams to a different access point, the 700wl series re-evaluates her rights. From the cafeteria, Mary now matches the Connection Profile Public, so the 700wl series gives her the restricted set of access rights that applies to employees when they are in public areas of the company during working hours. For confidentiality reasons, she cannot access confidential finance or company data when she is in a public area, even though she would otherwise have that access (see Figure 2).



When user Mary connects from her desk in Accounting, she can access Finance department services. When she connects from the cafeteria, she cannot access those restricted services.

Figure 3: Restricted Access for user Mary when she connects from the cafeteria

1. Jack, a visitor, arrives in the lobby at 8AM, and fires up his laptop to check email while he waits for his host:  
Jack does not have a user ID on ABC's network, but he is able to log on as a guest. Because he is connected through the access point in the lobby, and it is within working hours, he gets associated with Connection Profile Public, so the 700wl series gives him Guest access. This allows him to access the Internet and get his email, but does not provide him any other access.
2. Jack's host takes his visitor (with laptop) into his office in the engineering area:  
Jack still matches the Identity Profile Guest, but is no longer associated with Connection Profile Public. Therefore, when the 700wl re-evaluates Jack's rights after the roam, because Guest access is allowed only from the public areas, Jack does not get any access.
3. Later that night Jack happens to drive by Company ABC's headquarters on his way to the airport, and decides to try using Guest access to ABC's network to check his email. From the parking lot in front of the lobby, he gets a signal from the lobby access point, and attempts to log on. Jack tries to log on as a guest. However, as it is after 6 PM, he is outside the Time Window defined for the Connection Profile Public. Since Jack is a guest but does not match Connection Profile Public, he does not get any network access.

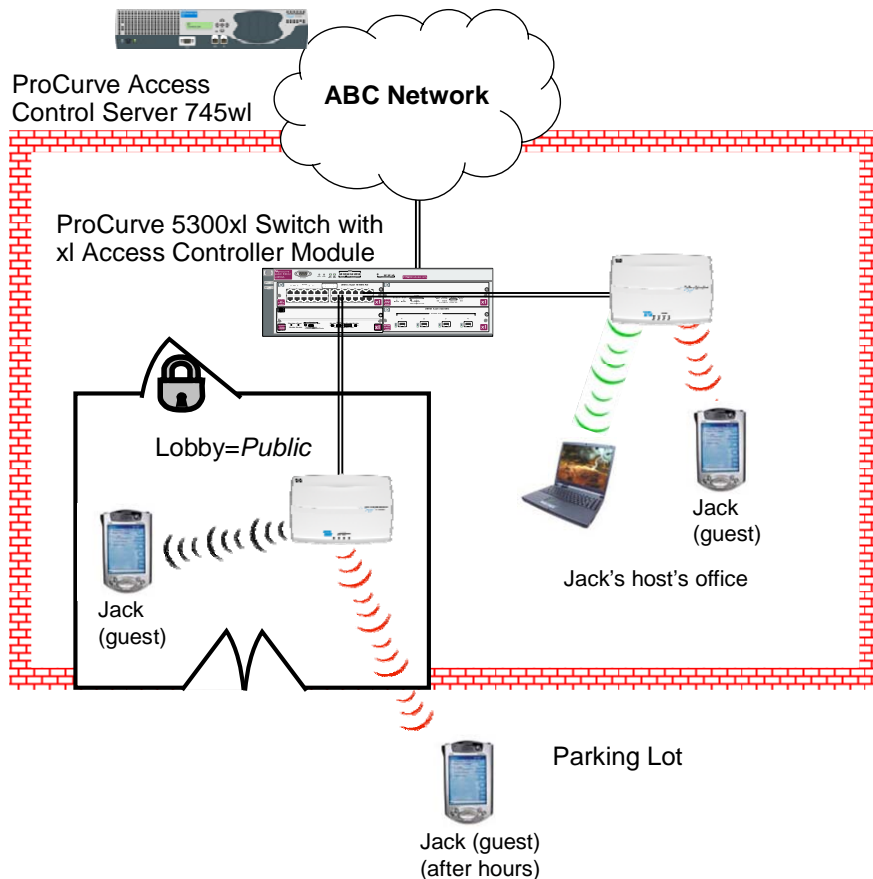


Figure 4: Access for Guest Jack depends on where and when he connects

## The Benefits of Access Policy Based on User Identity

As this paper has demonstrated, in the wireless world, effective access policies need to be user-based rather than port-based. In a shared environment, physical location can provide useful information (such as whether the user is in the building lobby or on a restricted floor) but does not allow any assumptions to be made about the identity of the user. Therefore, access policy must be based primarily on the actual identity of the user, and the appropriate policy must be enforced for a given user wherever they are when they access the network.

Conversely, the 700wl series' knowledge about how the user has accessed the network allows Access Policies to be defined and enforced with much finer granularity than would otherwise be possible. Given the mobility of wireless devices, users may roam between access points (thus moving between network ports) while they are connected to the system, and will expect to have continued access to the same resources after they roam as they did before. However, there may be situations, when a user is connected in a public area such as the lobby or the cafeteria, where access to certain resources may not be appropriate. The ability to refine Access Policies based on the location of the access point and the time of day provides a powerful mechanism for protecting sensitive resources.

The 700wl series identity-based rights model also allows mobile users to roam – from desk to conference room, for example - without losing network connectivity or access to the resources they need. From the network administrator's perspective, the 700wl series identity-based policy enables this level of mobility without administrator intervention.

The 700wl series' multi-dimensional, policy mechanism overcomes many of the shortcomings of port-based access policies. Identity-based access allows access policies tailored to an individual user's needs to be enforced even when multiple users share a single network connection.

Identity-based access also means that, regardless of where or when an individual appears on the network, policy appropriate for that individual can be enforced. In addition, policy based on the individual means that non-trusted users (the hacker in the company parking lot, for example) can be prevented from accessing the network even though they connect through a seemingly legitimate connection point. Identity-based access control makes it possible to allow mobile users to roam throughout the network, and yet continue to have the appropriate access to the resources based on business need.

## For more information

For more information on ProCurve Networking products and solutions, please visit <http://www.procurve.com>.

To find out more about  
ProCurve Networking  
products and solutions,  
visit our web site at

[www.procurve.com](http://www.procurve.com)



© 2005,6 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

5982-8269EN Rev. 1, 06/2006