

## Ryerson University



“At Ryerson we have found that the Avaya Identity Engines Ignition Server has simplified the management of our network access for wireless users and enhanced our level of security to the point where we have a very high level of confidence.”

“The product integrates seamlessly with whatever authentication clients are being used. It directly interfaces with our many Active Directories, which saves a great deal of time and money. It also has the flexibility and scalability to facilitate future technology needs.”

— Mourad Michael  
Network Engineering Manager

Ryerson is a distinctly urban university with a mission to serve societal needs, and a long-standing commitment to engaging its community. It is now the most applied-to university in Ontario relative to available spaces, and it has an outstanding reputation with business and community leaders.

Since 1948, Ryerson has built its reputation on the strength of its academic curriculum, offering close to 100 PhD, Master's, and undergraduate programs, with a total enrollment of 25,000 and more than 65,000 registrations annually in The G. Raymond Chang School of Continuing Education. In just a few years since the introduction of its first master's program, Ryerson has grown to host 2,000 graduate students in 34 programs, including nine at the doctoral level. The University now ranks third in Canada - and first in Ontario - in terms of research growth.

### Challenges and Goals

As a large university in Toronto, one of Canada's major cities, Ryerson University needs to take a very serious approach to the network security issues involved in offering wireless access for all students, faculty, and staff.

Mourad Michael, Network Engineering Manager, commented, “We had to consider many factors in choosing the best access control system for our network. We needed a solution that could handle the large volume of students, faculty, and staff who require access and authentication through our two separate active directories – one for academics (students and faculty), and the other for administration.”



*“We’ve seen the number of wireless users growing constantly,” Michael added. “We are now at approximately 5,000 authenticated users during a typical school day. Since installing and updating software clients on every staff work station is extremely time-consuming (and we’re not permitted to alter students’ personal computers), we needed a solution that wouldn’t require us to install new clients on users’ computers. Instead, we would have to work with the Active Directories for the authentication of both PC and Mac users.”*

According to Michael, universities are high-profile targets for malicious attacks, and Ryerson’s network must pass rigorous security audits. Michael explained, *“The encryption method for data over the wireless network is of great importance. WPA2 appeared to be the best authentication method for encryption, and we wanted a method that would facilitate and support that. Before we had LDAP as the only source for the directory service that we could use,*

*and for this we had to install clients on the users’ PCs. It was a limiting factor that we wanted to move beyond.”*

## Solution

Ryerson University chose the Avaya Identity Engines Ignition Server, which is an easy-to-deploy RADIUS and TACACS+ server that connects with existing directories and switch infrastructures, providing a central policy decision point. It enables network administrators to apply policies that evaluate user account details, switch details and/or any RADIUS or TACACS+ attributes to determine network access.

Authentication is performed directly against the enterprise’s user directories, so access policies operate on the latest user account information. This capability reduces latency and helps to ensure consistent security.

The University also uses the Avaya Ethernet Routing Switch 8600 portfolio in the network core, and the Avaya Ethernet Routing Switch 5500 series for access. Avaya Communication Server 1000 provides a VoIP telephony solution for the university.

## Value Created

### Adaptability to multiple directories saves time and money.

*“It is extremely important that Identity Engines utilizes our Active Directories, which are handled by the existing operating systems on both PCs and Macs,” Michael said. “We do not have to go to the enormous time and expense of installing and updating clients on individual computers, because policies are created from the Active Directory group membership.”*

The Ignition Server can integrate with multiple, heterogeneous directories, offering location-based and realm-based strategies to search multiple data repositories for the

**“It is extremely important that Identity Engines utilizes our Active Directories, which are handled by the existing operating systems on both PCs and Macs. We do not have to go to the enormous time and expense of installing and updating clients on individual computers, because policies are created from the Active Directory group membership.”**

— Mourad Michael  
Network Engineering Manager

user account. User attribute normalization features are provided to help obtain consistent user data from varied sources.

### Open standards flexibility.

The Ignition Server handles multiple EAP types and supports network hardware from all major vendors. *“For us, it is a huge benefit that Identity Engines uses an open standard. It adapts easily to our Aruba® wireless system, and we know it will fit with changes that may occur as our network evolves,”* Michael stated.

### Ease/speed of installation and management.

The Ryerson IT team installed Identity Engines, tested it, and moved it into production within 10 days. *“We were amazed at the speed of installation and how quickly our team was able to become comfortable with this solution,”* Michael said. *“The GUI is very straightforward, requiring only minimal training. We find it surprisingly easy to implement policies and configure them, to add rules and to remove rules—making it all as granular as we want.”*

### Comprehensive logging and reporting capabilities.

The Ignition Server provides an accurate account of which users and devices have logged in and offers simple report generation for compliance. Michael has found that the reporting features for Identity Engines are very robust and comprehensive, providing all the information that is needed to facilitate quick troubleshooting when users report access issues.

Heightened security that meets strict requirements for organizational governance/regulations/compliance. Policy-based access control governs which users can log in and what areas of the network they can access. The Ignition Server sets session parameters at log-in time, allowing VLAN provisioning and the activation of switch-based security features.

Michael commented, *“We feel very confident going into both internal and external audits now because, with Identity Engines, we can use WPA2, which is recognized as the best encryption method for data over the wireless network.”*

Identity Engines provides an EAP (Extensible Authentication Protocol) framework, which is required for WPA2 (Wi-Fi Protected Access 2). WPA2 provides network administrators with a high level of assurance that only authorized users can access the network.

### High capacity and scalability.

*“At first we were concerned about sending thousands of users through this one authentication engine, but we find that the system has no problems with our huge, constant volume, and we’ve seen no capacity limitation issues. There have been no ‘hiccups’ and no downtime at all.”*

The Identity Engines Ignition Server has enabled the University to implement a Guest Access procedure that coordinates seamlessly with their existing processes. It has also allowed for the retention of legacy authentication processes which can utilize the ignition server as a single point of entry.

**“We were amazed at the speed of installation and how quickly our team was able to become comfortable with this solution. The GUI is very straightforward, requiring only minimal training. We find it surprisingly easy to implement policies and configure them, to add rules and to remove rules—making it all as granular as we want.”**

— Mourad Michael  
Network Engineering Manager



The IT team is also creating user groups within the University. Michael explained, *“We are starting to group users and assign the policies and rules according to the membership. This process is very straightforward and easy to apply. We have good visibility into the system to ensure*

*that the grouping system makes sense and that things are flowing well. This feature is beneficial because, no matter where the users are located, they will get the same access rights and firewall rules that apply to them."*

In the future, the University will consider expanding use of Identity Engines to the wired population as well. They also plan to integrate the Identity Engines solution with Microsoft® Network Access Protection (with the Identity Engines 7.0 release) to provide health checking on administrative users' PCs, using the native Windows client.

*"Again, Identity Engines will simplify a situation that could have been very difficult for us before,"* Michael concluded.

## Learn More

For more information on how Avaya Intelligent Communications can take your enterprise from where it is to where it needs to be, contact your Avaya Account Manager or a member of the Avaya Connect channel partner program, or access other collaterals by clicking on

**Resource Library** at [www.avaya.com](http://www.avaya.com).

---

All statements in this case study were made by Mourad Michael, Network Engineering Manager, Ryerson University.

“**At first we were concerned about sending thousands of users through this one authentication engine, but we find that the system has no problems with our huge, constant volume, and we've seen no capacity limitation issues. There have been no 'hiccups' and no downtime at all.**”

— Mourad Michael  
Network Engineering Manager

## ABOUT AVAYA

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, data solutions and related services to companies of all sizes around the world. For more information please visit [www.avaya.com](http://www.avaya.com).

© 2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries.

All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc.

All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein.

References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.

07/11 • DN4645-01

**AVAYA**  
The Power of We™