Securing Campus Network Access for an Improved User Experience

Chris Ford
Network Administrator
Brescia University
chris.ford@brescia.edu

Jack Wilson
Director of Information Technology
Brescia University
jack.wilson@brescia.edu

About Brescia University

Brescia University was founded in Owensboro, KY in 1950 as a college by the Ursuline Sisters of Mount Saint Joseph. Brescia began as a junior college at Mount Saint Joseph in 1925 but as many GI's returned from war, the need to offer education in town became the catalyst to move the college. It became a four-year institution and was made a University in 1998. Brescia University has more than 5,000 alumni across the United States and the world. In 2003, Brescia University inaugurated its first non-Ursuline president, Fr. Larry Hostetter, who is now on his second term as President.

- Offerings of three master's degrees, 39 bachelor's degrees, five associate degrees, and eleven pre-professional programs.
- One of three accredited institutions in the U.S. to offer an online degree completion program in Social Work.
- Increased enrollment for at least the past three years.
- All freshman participate in two service projects a year.
- Ranked by the *U.S.News & World Report* in the top 35 colleges in our region for the past five years.
- Offers 15 different coed athletic teams, in which two teams won their conference titles last spring.
- Students in pre-professional programs see 100% placement into graduate schools.

Session Overview

- Discusses path of deployment
  - Differentiated network access
  - Various levels of security
  - Meet bandwidth concerns
  - Protect the network from unwanted applications
  - Improve the user connectivity experience
- Highlights resolution of common network hurdles
  - Bandwidth usage
  - Network usage information
  - Meet compliance requirements

Original Configuration

- Traditional Network Access
  - Manual VLAN changes
  - Manual wireless provisioning
  - Lack of bandwidth prioritization
  - Low level of logging
  - Basic packet shaping

Problems

- Time consuming
- No ease of change
- No ease of lockdown
- Low quality of tracking
- Lack of ownership of individual actions
- Lack of control over non-university devices

Goals

- Higher level of network monitoring
- Pre-emptive authorization or lockout
- Automatic remediation
- Post-authorization monitoring
- Accountability
- Automated network management and VLAN distribution

Overview of Deployment Success

- Replaced traditional network access and monitoring
  - Removed manual VLAN changes, manual wireless setup, and lack of prioritization
  - Added or enhanced differentiated network access for various user levels, application checking, health remediation, continuous logging, and monitoring for post authentication P2P activity
- Added flexible network assignments
  - Now able to assign users to VLAN and policies dependent upon location and group membership
- Added bandwidth prioritization
  - VLAN members are either given access priority or access restrictions for network access and internet connectivity
- Assists in HEOA compliance
  - P2P checking and continuous logging after authentication

Equipment

- Entry point to the network
  - Switches
  - Wireless Controllers and Access Points

- Access Control
  - Captive Portal or Radius Authentication

- Logging
  - Syslog, packet capture logging
- Bandwidth Monitoring/Limiting
  - Packet Shaping Device, Router Policies

Technologies Used

- Wired and Wireless MAC Authentication (Pre-Authentication and Authentication)
- Wired and Wireless web portal logon (Authentication)
- Health Check and Remediation (Authentication)
- Distribution to Proper VLAN (Pre-Authentication and Authentication)
- Packet Shaping (Post-Authentication)
- Priority Queuing (Post-Authentication)
- Logging (Post-Authentication)

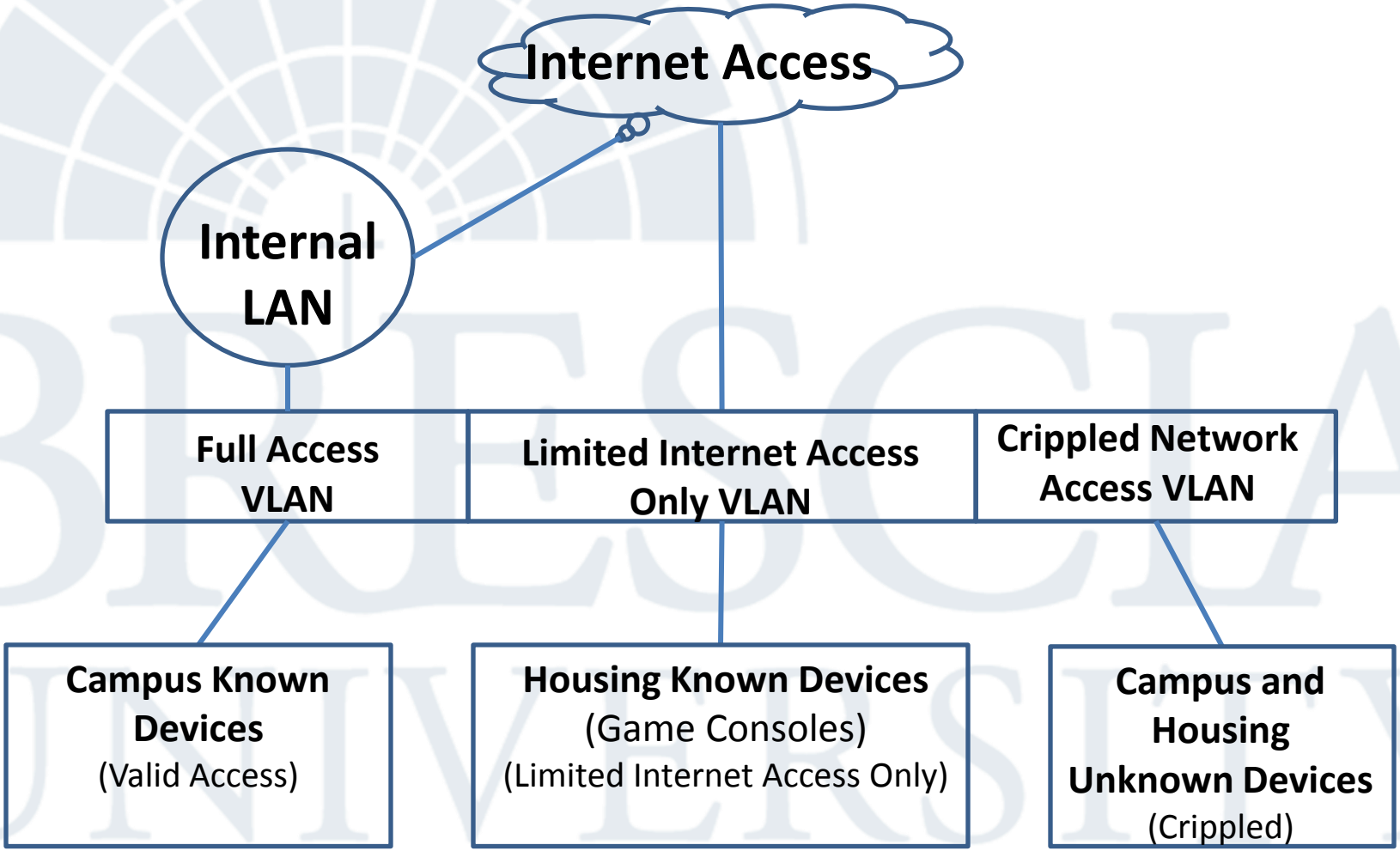
Pre-Authentication

(802.1x/MAC authentication, VLAN Placement)

- Devices are placed into a VLAN when initially connected to the network
  - Campus known devices are automatically put into the proper VLAN by hardware MAC address
  - Housing known devices are automatically put into the proper VLAN by MAC address
  - Unknown devices are placed into a crippled VLAN, requiring a more in-depth authentication process

Pre-Authentication

(802.1x/MAC authentication, VLAN Placement)



Authentication

(802.1x/user authentication, Web Portal authentication, Health Check, VLAN Placement)

- The device is given an authentication opportunity
  - 802.1x/user authentication for PCs or some mobile devices
    - Domain PCs logged in with student credentials are placed in a specific VLAN with limited access to campus resources
    - Domain PCs logged in with faculty/staff credentials are placed in a specific VLAN with a broader access to campus resources
  - MAC authentication for game consoles
    - Game consoles are authenticated via MAC address and placed in a specific VLAN with only internet access. All other local access is denied on these devices

Authentication

(802.1x/user authentication, Web Portal authentication, Health Check, VLAN Placement)

- All unknown devices are given the opportunity to authenticate via Web Portal
  - As authentication takes place the following are checked
    - Location
      - Campus or housing
    - User group and ID
      - Faculty, Staff, Student, Guest
    - Health
      - Healthy, unhealthy, transitional, quarantine

Captive Portal Web Access

Brescia University

Computer Use Policy

PLEASE NOTE: You must read and agree to the Guidelines for use of Brescia Computer Resources below in order to use Brescia computer resources. Violators of these guidelines will be referred for appropriate disciplinary action. The computer resources have been installed to support the educational mission of the University. Consequently they are to be used in accordance with U.S. and International law. Refer to the computer use guidelines in the handbook.

- University facilities are available to faculty, staff, and currently enrolled students during regular

Enter Login Credentials

Username

Password

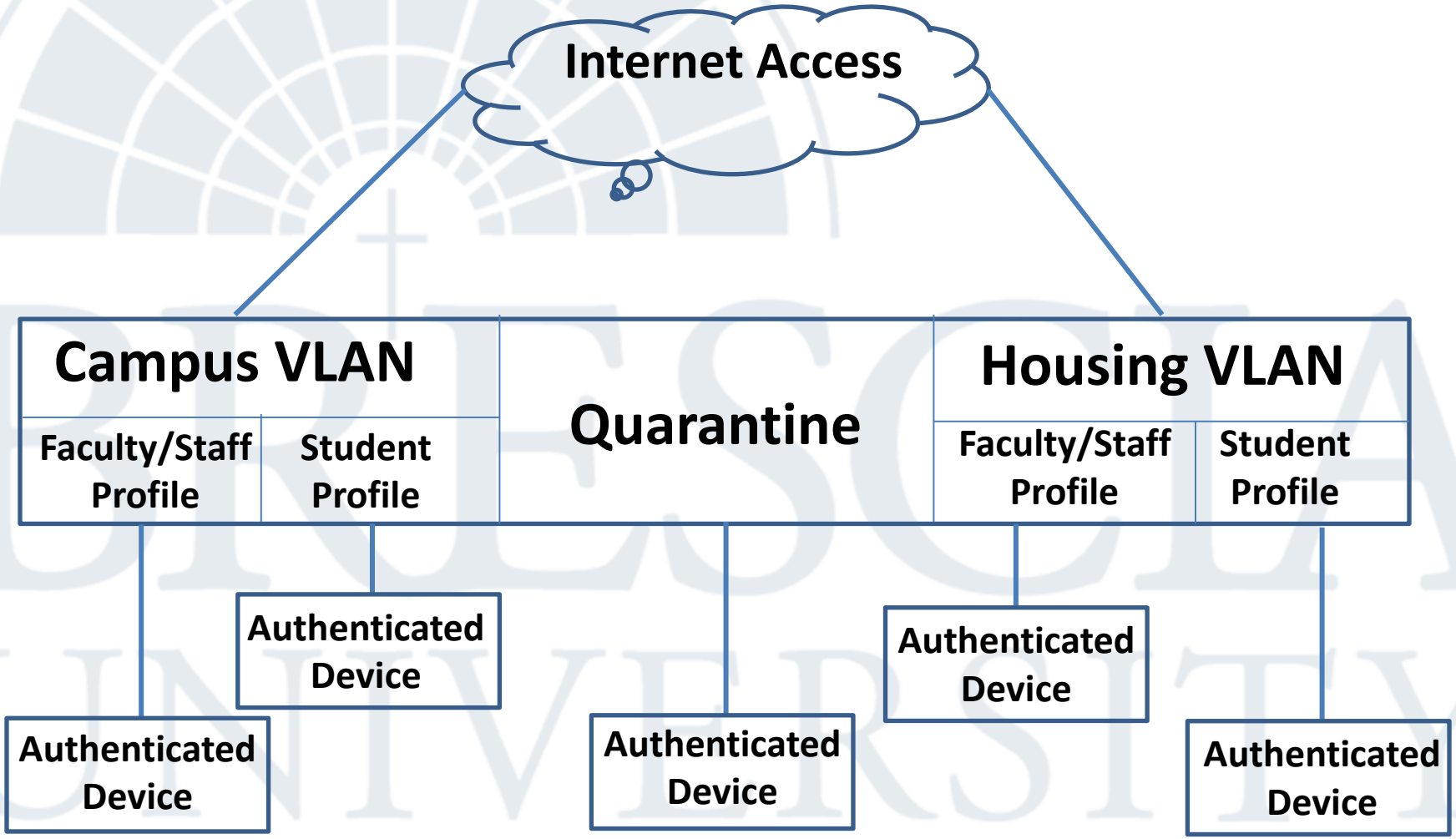
Submit

Note: If you cannot access the network, your device may be in quarantine. Please visit the Brescia University Helpdesk for assistance.

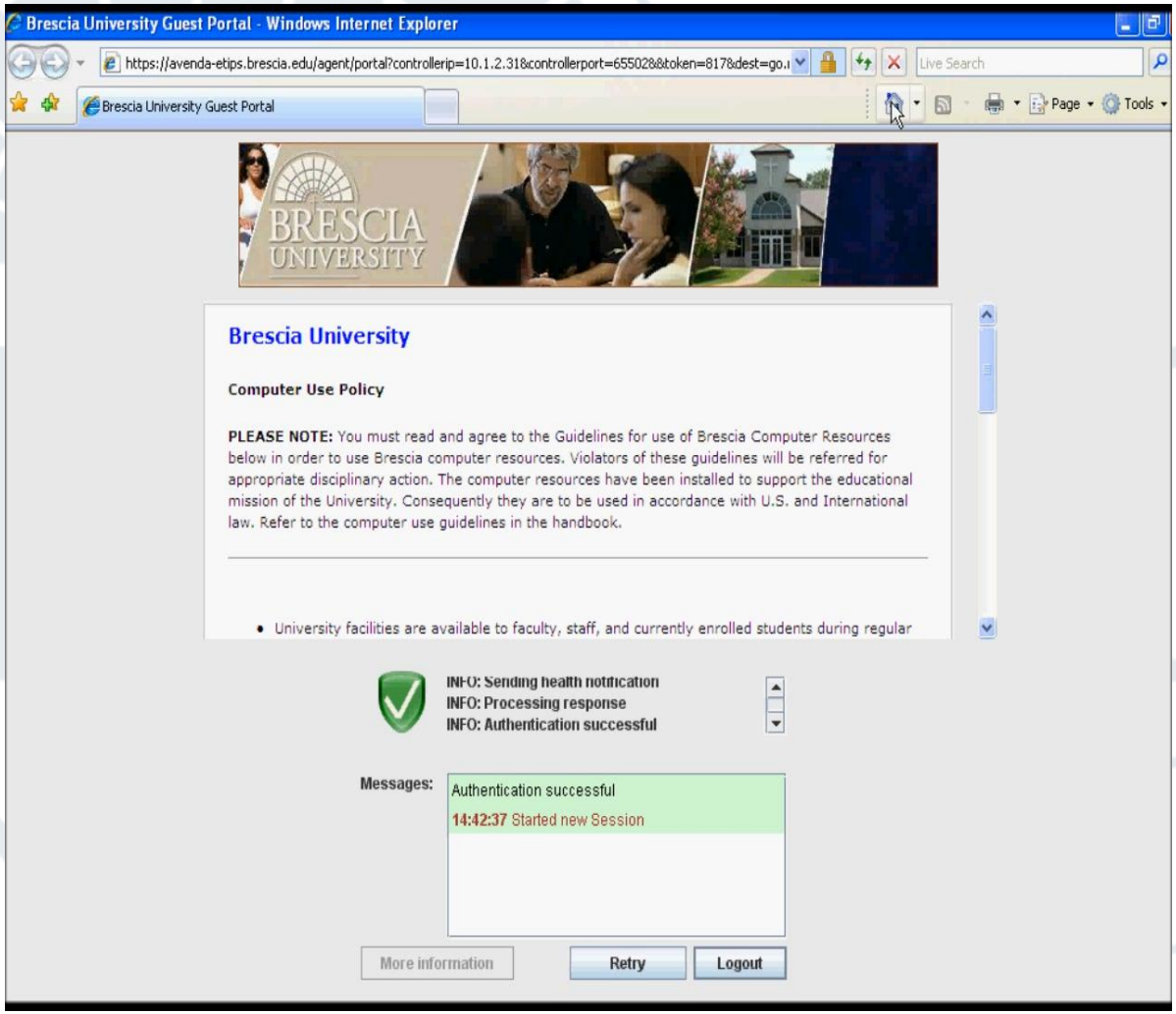
Health Check

- Unhealthy – Moved to remediation or quarantine VLAN
  - Checks for specific malware or other threats
  - If P2P apps are running, they must be removed
- Intermediate – Moved to transitional VLAN
  - If no anti-virus is present, anti-virus must be installed
  - If anti-virus is not updated, anti-virus must be updated
- Healthy
  - Students from Housing location
    - Housing VLAN
  - Faculty/Staff from Housing location
    - Faculty/Staff Housing VLAN
  - Students or Faculty/Staff from Campus location
    - Campus VLAN, but are given various access levels, depending on group membership

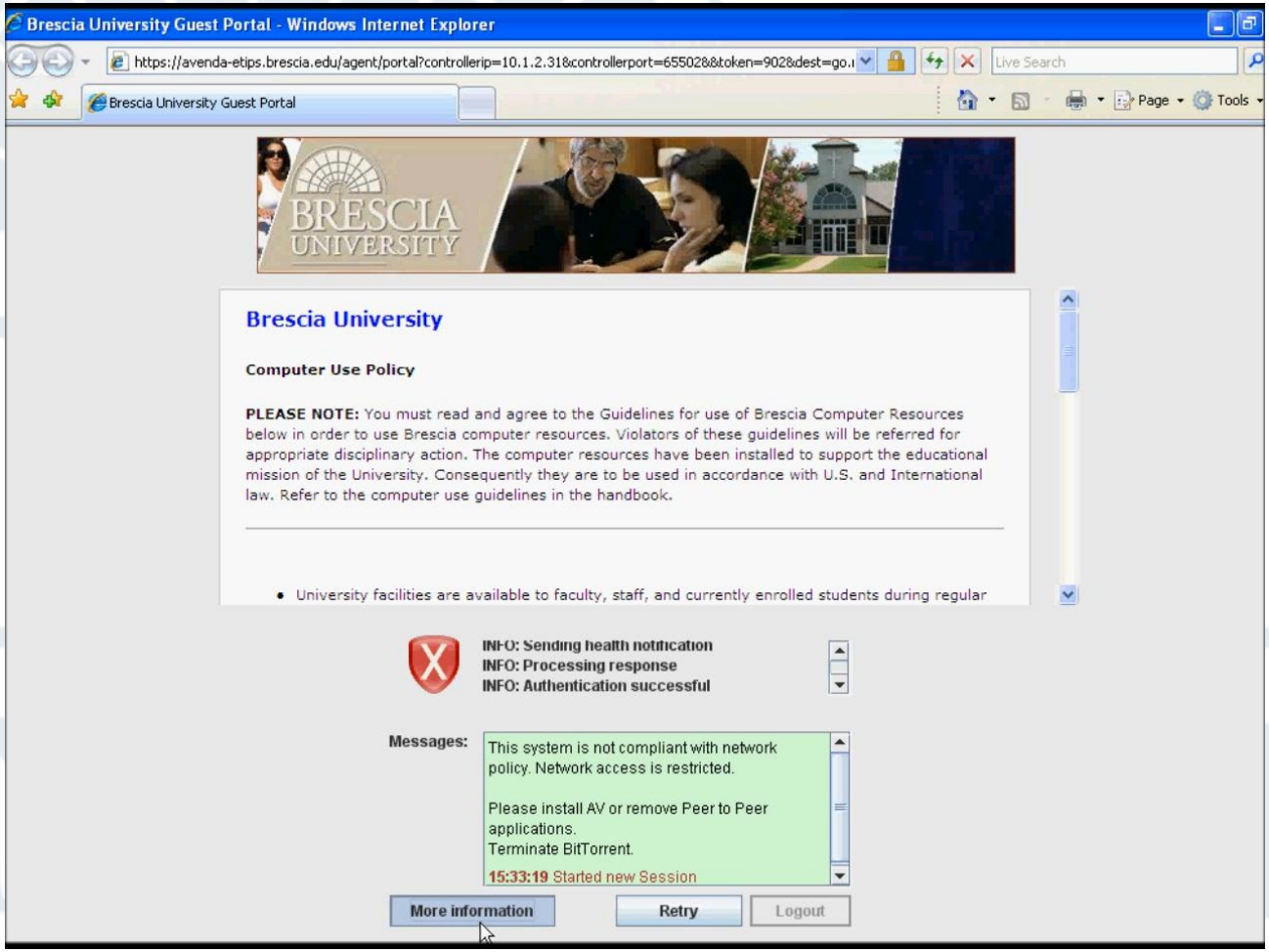
Authentication



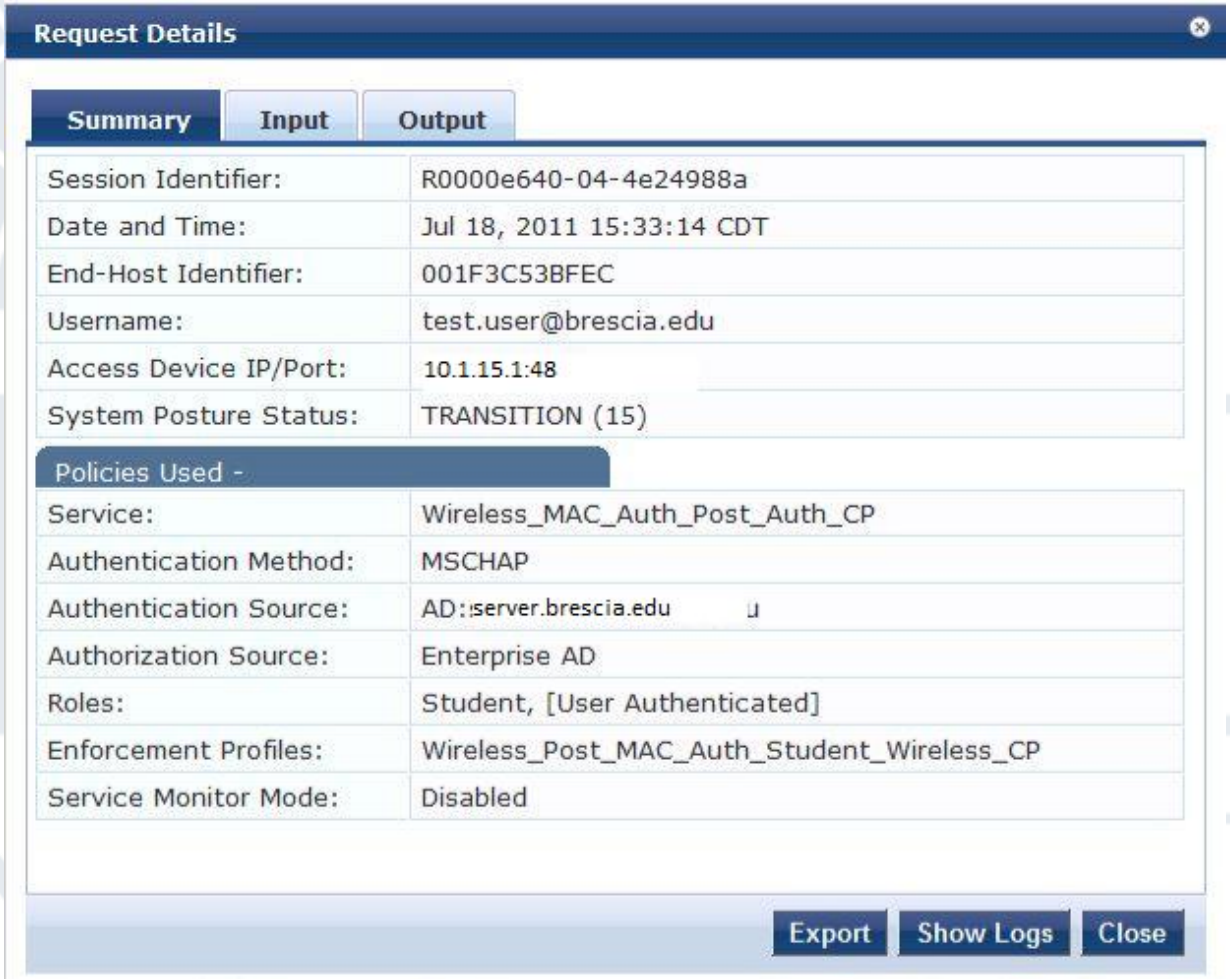
Healthy Authentication



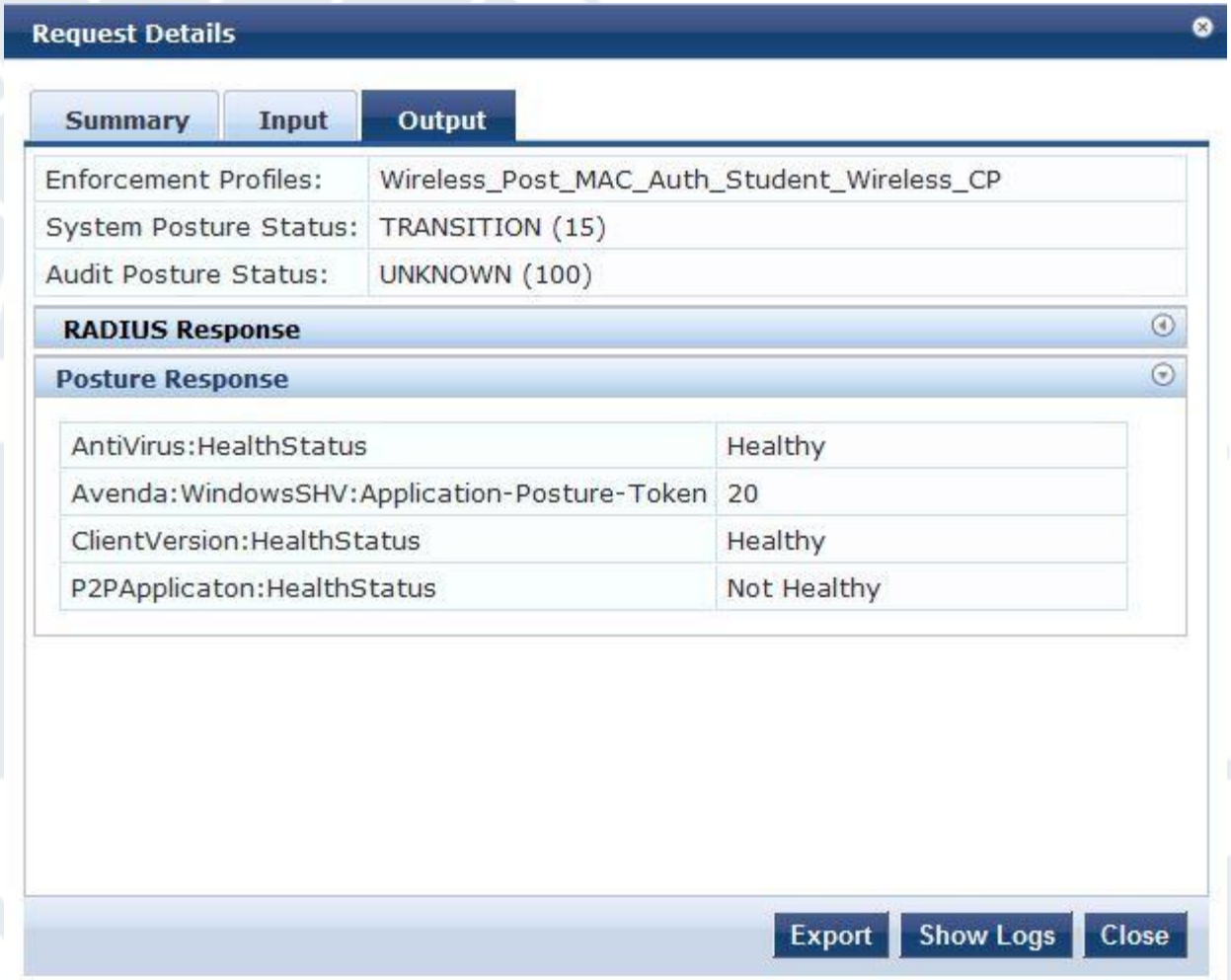
Unhealthy Authentication



Authentication Summary



Authentication Posture Response



Peer to Peer Application Information

P2PApplication:BitTorrent:Status	Running
P2PApplication:BitTorrent:Vendor	BitTorrent, Inc.
P2PApplication:Name	BitTorrent

Post-Authentication

- Queuing Priority based on
  - Campus Users
  - Faculty/Staff Housing Users
  - Student Housing Users
  - Game Consoles
- Packet Shaping
  - Shape P2P or unwanted traffic
- Logging
  - SNORT used to log data (network captured data)
  - Syslog used to log data (firewalls, routers, switches, wireless controllers)

Advantages

- Centralized control over connectivity of users
  - Individualized authentication process
- Pre-emptive remediation of devices
  - Health checking
    - Active and updated anti-virus
    - Active viruses and malware
    - Active P2P software
- More detailed logging
  - User ID information
  - MAC address information
  - IP address information
  - Individual activity and amount of bandwidth used
- Helps with HEOA compliance
  - A plan to "effectively combat" copyright abuse on the campus network using "one or more technology-based deterrents"
  - Bandwidth shaping
  - Traffic monitoring to identify the largest bandwidth users
  - A variety of commercial products designed to reduce or block illegal file sharing

Observations

- Fewer network management issues
- P2P usage decrease
- More usable network data
- Users are more aware of their actions
- Fewer credible bandwidth complaints
- Higher level of network security

Thank you.

Chris Ford
Network Administrator
Brescia University
chris.ford@brescia.edu

Jack Wilson
Director of Information Technology
Brescia University
jack.wilson@brescia.edu