safe connect
network access control

Safe•Connect | Access Requests Guide

Safe•Connect can be configured to allow end users to request temporary access by adding an exemption for a pre-determined period of time. Access Requests are useful in situations where a user does not meet policy criteria, but has a legitimate reason for requiring temporary network access or the solution to a quarantine requires network access that would otherwise be blocked. Access Requests can be pre-configured to allow instant access, instant access with administrative notification or require validation prior to activation.

Impulse Point
6810 New Tampa Highway
Lakeland, FL 33815
863-802-3738
www.Impulse.com

August 2012

Contents

Overview

Beginning with version 5.4, Safe•Connect provides the ability for users to request temporary access when they are blocked for not meeting policy. Access Requests allow a user to gain temporary access when they are not able to remedy a situation to meet policy, or in situations where they have a legitimate need to gain network access and are not immediately able to meet policy requirements. There are situations, such as updating antivirus definitions, where a user will need network access to remediate an issue. Prior to access requests, a user would have to call the help desk, where they would then be placed in Open Access by a help desk representative. With Access Requests, this process can be automated, therefore, reducing help desk calls.

The purpose of this document is to introduce you to the configuration and operation of the Access Request module of Safe•Connect. This document provides all the information needed to fully configure the Access Request module. This document will also step you through how a user will request access and receive subsequent notification when they are able to access the network. This document assumes that standard URLs will be used. If a branded deployment is in use, please refer to the appendix for information on branded URLs.

Safe•Connect Access Requests provides a portal style system to allow end users to temporarily gain access to the network when they do not meet policy requirements. The default notification requirements and access "Time to Live" durations are completely configurable. All user information is viewable and editable by an administrator through the Open Access management page of the Safe•Connect Dashboard. Administrators have the ability to choose from one of three approval methods, depending on the level of control required:

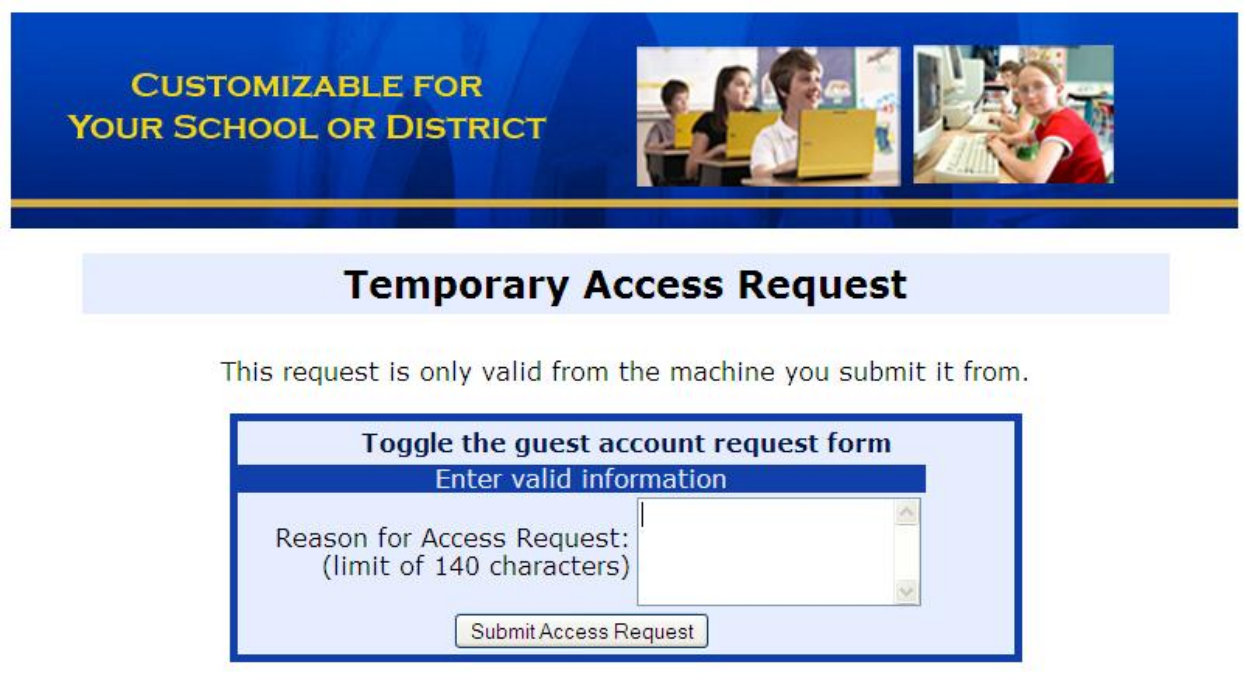
- Automatic Approval with no notification
- Automatic Approval with a notification sent to administrators
- Notification sent to administrators with administrative approval required

End User Experience

Access Request Overview

The end user is quarantined for not meeting policy. The remediation page has a link to request temporary access.

After the user clicks on the link, they fill in a form to request temporary access.



If approval is required, there will be fields for an email address, cell phone number and cell phone carrier.

Temporary Access Request

This request is only valid from the machine you submit it from.

Toggle the guest account request form

Enter valid information

Reason for Access Request:
(limit of 140 characters)

This request requires approval.

Notification Options

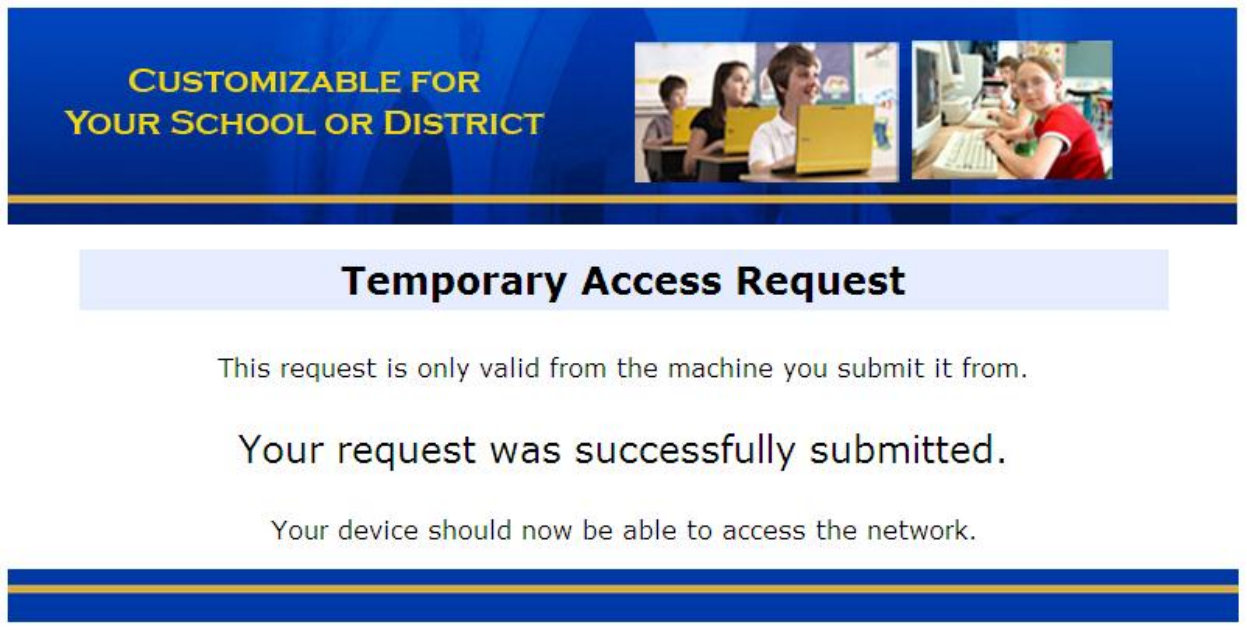
Valid Email Address:

Valid Phone Number:

Pick your Carrier: Select a Phone Service Provider

Submit Access Request

After submitting the request, the user will see the following message if no approval is required:



If administrator approval is required, a slightly different screen will appear. The user will be notified via text message or email when their request is approved or denied. The notification will be sent to the email address or phone number specified when the access request was submitted.

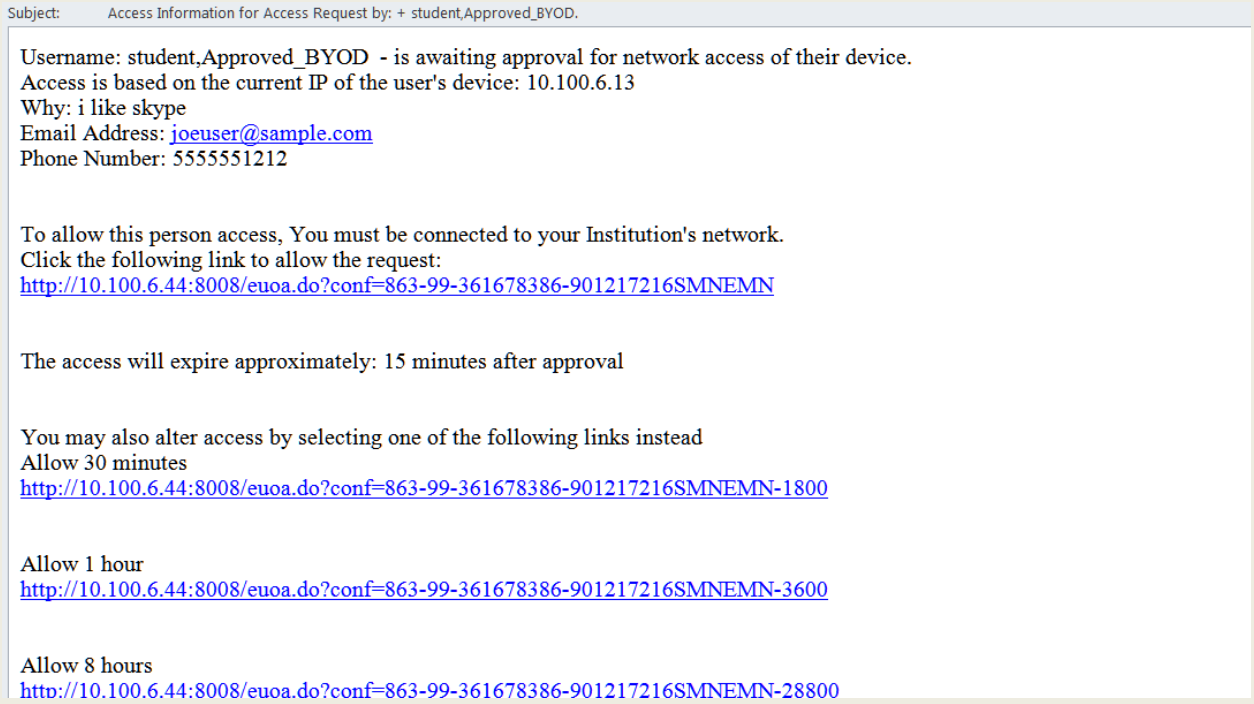
Administrator Access Request Approval Overview

The Access Request approval process will vary depending on the approval option that is in use by Safe•Connect

- **Automatic with no Notification**: The Access Request is immediately approved and no notification is sent to administrators. The user will still appear in the Open Access dashboard module.

- **Automatic with Notification**: The Access Request is automatically approved. An email is sent to administrators alerting them of the granted access request. If necessary, an administrator can revoke access via the Open Access dashboard module.

- **Approval Required for Notification**: If approval is required for Access Requests, an email is sent to administrators alerting them of the pending request. Administrators can click on the link in the email to approve the request. Alternatively, administrators can click on other links to extend the default time the user will have access. Users will be notified via text message or email of when an administrator approves or denies their request.



Subject: Access Information for Access Request by: + student,Approved_BYOD.

Username: student,Approved_BYOD - is awaiting approval for network access of their device.
Access is based on the current IP of the user's device: 10.100.6.13
Why: i like skype
Email Address: joeuser@sample.com
Phone Number: 5555551212

To allow this person access, You must be connected to your Institution's network.
Click the following link to allow the request:
http://10.100.6.44:8008/euoa.do?conf=863-99-361678386-901217216SMNEMN

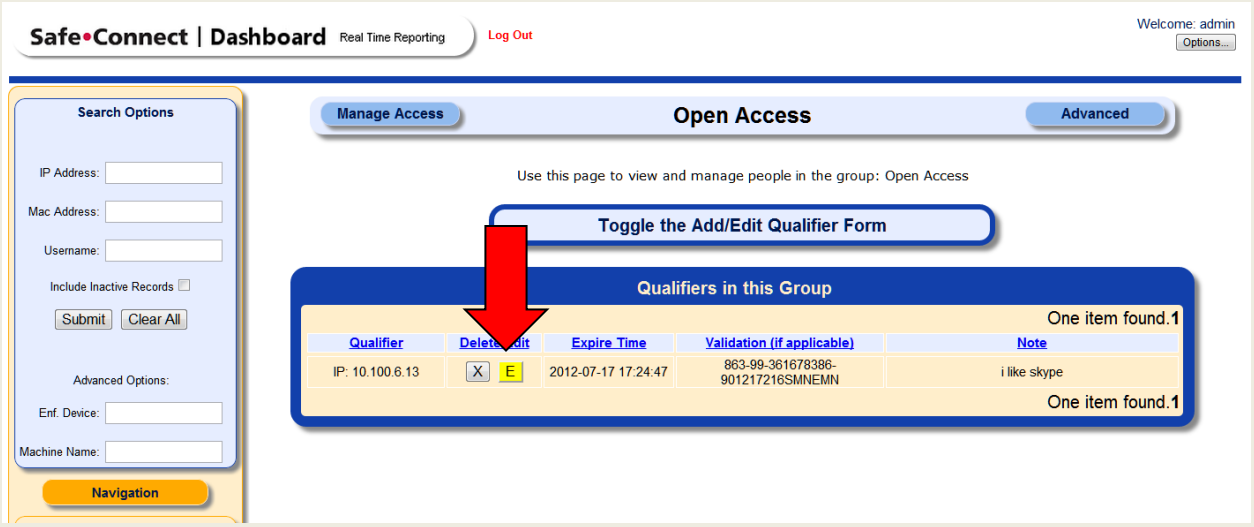
The access will expire approximately: 15 minutes after approval

You may also alter access by selecting one of the following links instead
Allow 30 minutes
http://10.100.6.44:8008/euoa.do?conf=863-99-361678386-901217216SMNEMN-1800

Allow 1 hour
http://10.100.6.44:8008/euoa.do?conf=863-99-361678386-901217216SMNEMN-3600

Allow 8 hours
http://10.100.6.44:8008/euoa.do?conf=863-99-361678386-901217216SMNEMN-28800

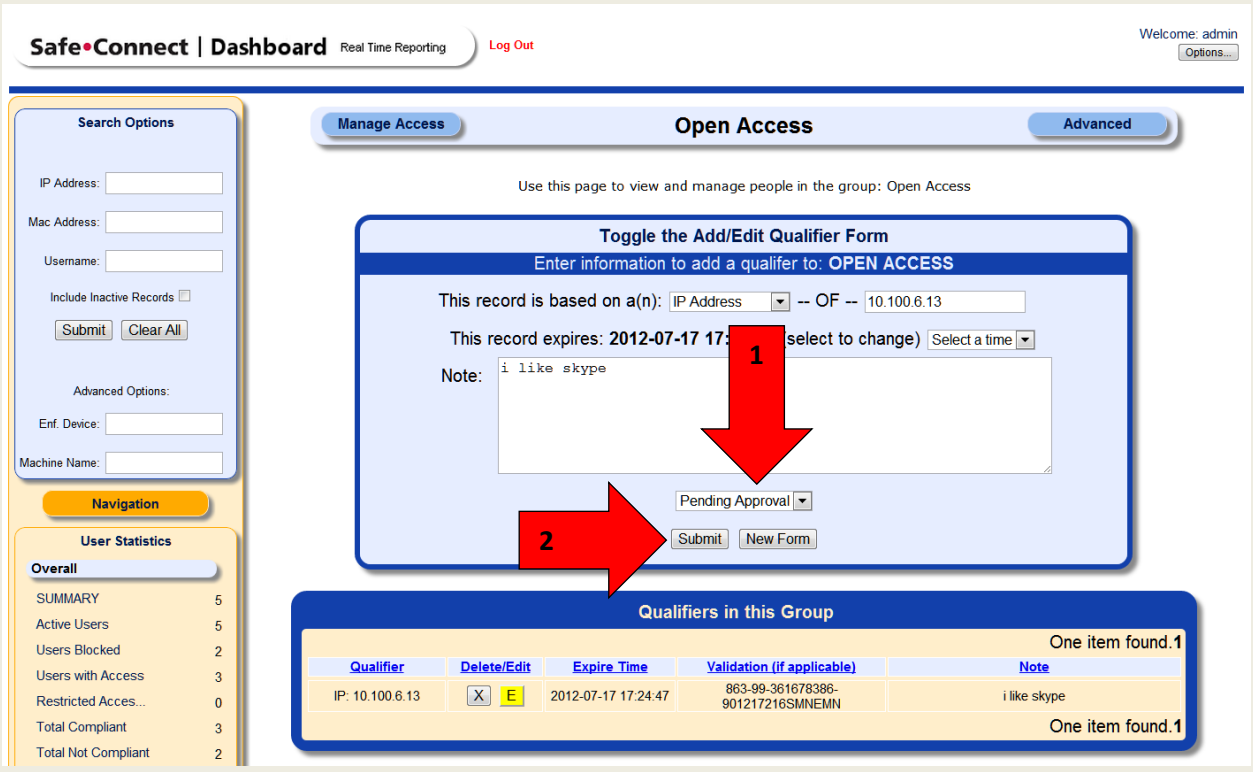
The ‘Open Access’ portal shows all pending access requests. Pending requests can be edited by clicking on the yellow ‘E’ button. To deny a request, an administrator can click on the ‘X’ button.



To approve the request, and send the user a notification:

1) Change the State to ‘Active’
2) Click ‘Submit’

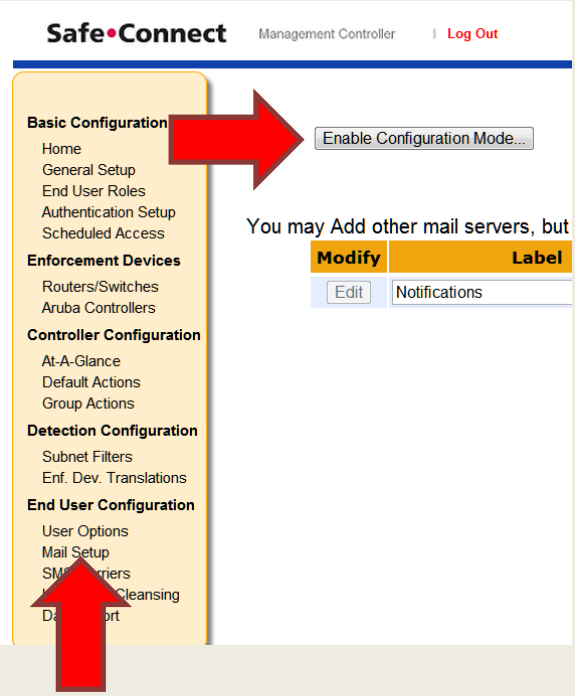
At this point a notification will be sent to the user via text message and/or email. If the user does not receive the notification, they can call the help desk.



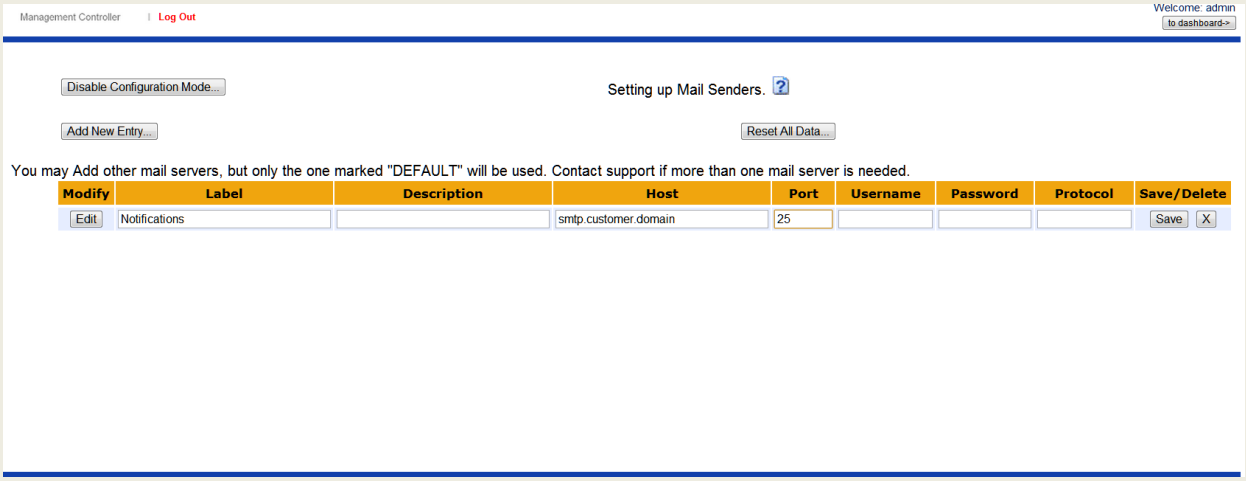
Configuration

Email Configuration

The configuration for Email can be found in the 'End User Configuration > Mail Setup' section of the system configuration page (https://auth.impulse.com:8443/config.s or your branded URL). Upon opening the page, an administrator will see the following screen. The Administrator must click on the "Enable Configuration Mode…" button in the upper left to activate any of the "Edit" buttons on this screen.



At a minimum, the host and port number of the smtp server should be entered. In most cases, a valid username and password will also be required. Optionally, a Description can be entered. The Label field should be always be 'DEFAULT'. When finished, click 'Save'. The Protocol field should be left blank unless specifically instructed by an Impulse representative.



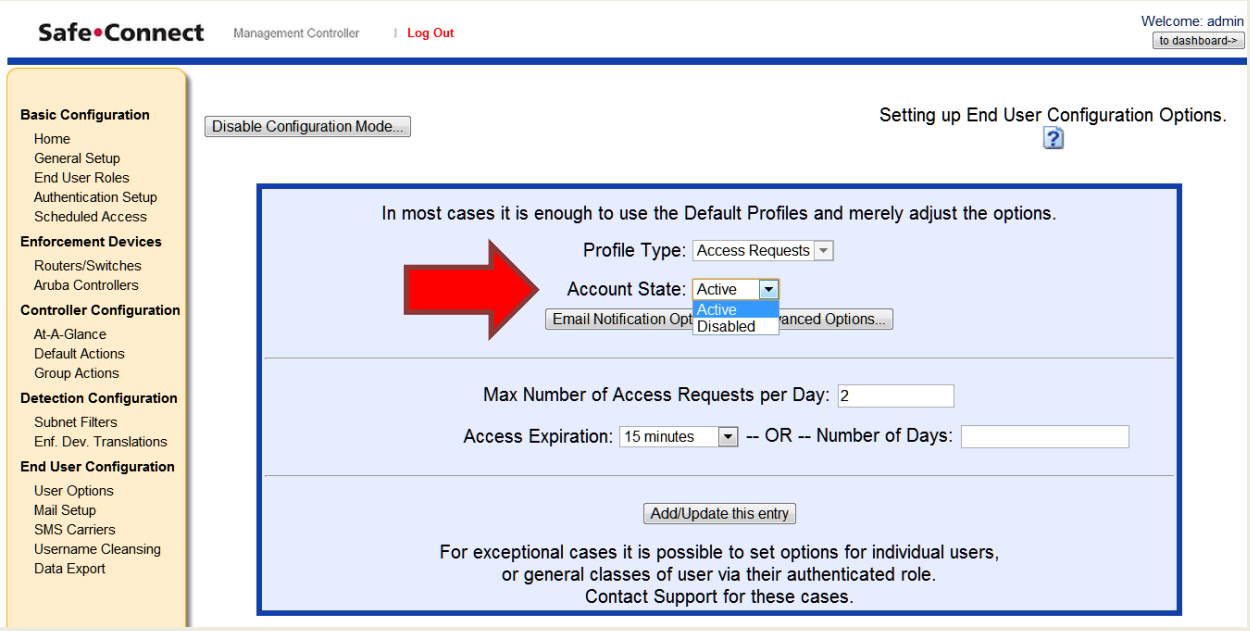
*If this has already been configured for other end-user portals, this configuration can be skipped as only one email server needs to be configured.

Dashboard Configuration

The configuration for Access Requests can be found in the 'End User Configuration > User Options' section of the system configuration page (https://auth.impulse.com:8443/config.s or your branded URL). Upon opening the page, an administrator will see the following screen. For our purposes, we will be concerned with "Access Request" options. The Administrator must click on the "Enable Configuration Mode…" button in the upper left to activate any of the "Edit" buttons on this screen.

Default Access Request Configuration

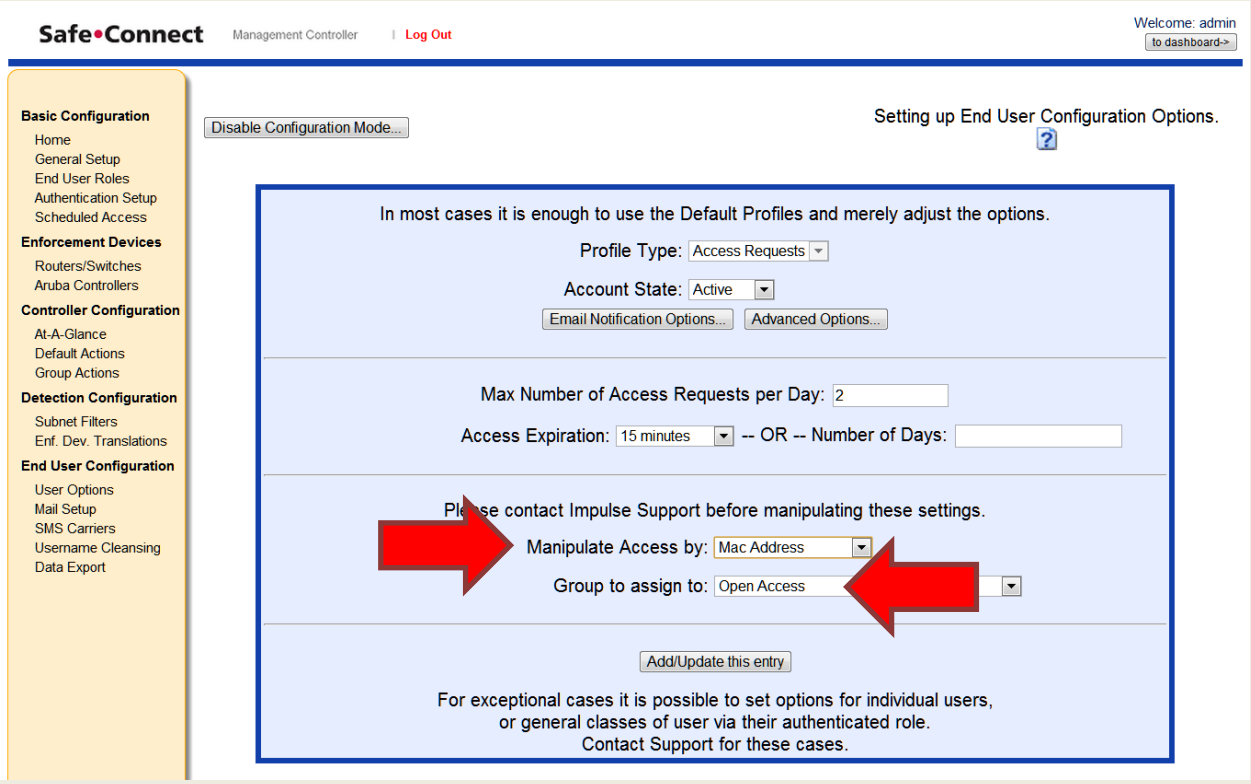
For “Access Request” options, clicking on the edit button will open the base configuration form as seen below:



The “Account State” option is the on/off switch for Access Requests. The default setting for this is “Active”; the “Disabled” option turns it off. A default number of requests allowed per day and expiration times can be chosen. Expiration times can be chosen from the dropdown, or specified as a number of days. The Profile Type field should be left as default unless a representative from Impulse Point specifically states that this should be changed.

Advanced Options

Clicking on the "Advanced Options…" button will expand the dialogue box to include options for manipulating Access based on Mac Address, IP address, or authentication name. The 'Group to assign to' option corresponds to the policy group will be used when the access request is granted.



In most cases, granting access by Mac Address will be sufficient, however, in some cases, it may be desirable to grant access based on the IP address or the username. Once access is granted, the user/device will be moved to the specified policy group. Using the Open Access policy group will move the user/device to the same policy group they would be moved to if open access was granted through the dashboard.

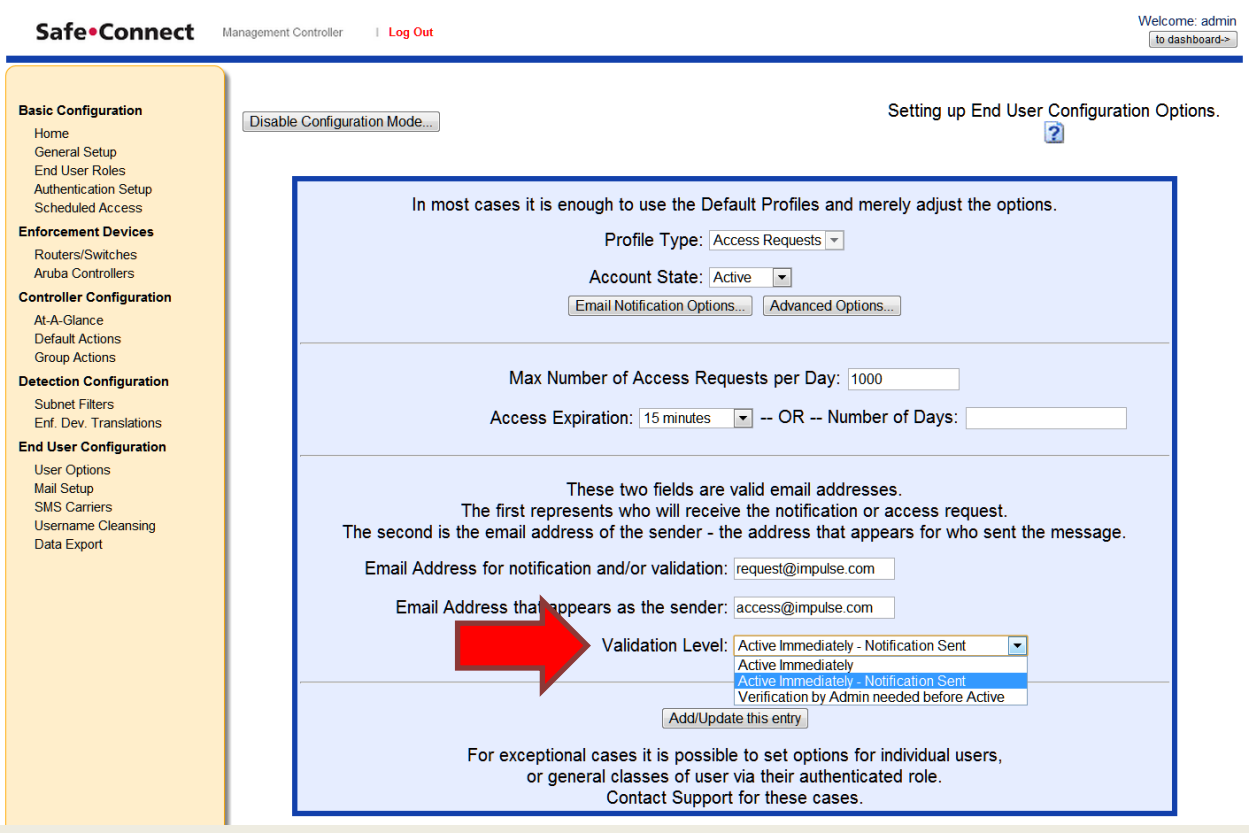
Notification/Validation Options

The Access Request module comes with expiration and notification/validation settings. The notification options have three validation levels and can be seen in the illustration below:

- **Active Immediately** – Once the access request is submitted, it is immediately granted and no validation response is needed from the administrator. The Administrator is not notified via email that access was granted.
- **Active Immediately – Notification Sent** – Once the access request is submitted, it is immediately granted. A notification email is sent to the configured administrative notification email address.
- **Verification by Admin needed before Active** – Once the access request is submitted, a notification email is sent to the configured administrative notification email address with the option to accept or decline the request.

Both a Notification and a Sender email address is required for email notifications to work properly. These addresses must be different.

NOTE: *If required, please ensure that the sender address is valid in your directory structure.*



Policy Manager Configuration

Access Request Page

If Access Requests will be allowed on your network, the most efficient way to for users to reach the Access Request pages is to display a link on the remediation pages. This is done through the Policy Manager.

After logging into the Policy Manger, perform the following steps:

1) Click on the "Download Data" button to download your policy information from the Safe•Connect server
2) Click on "Custom Messaging" to open the Custom Messaging interface
3) Select your normal remediation page from the drop down menu at the top center of the screen
4) Click on "Create a Copy"
5) Give your new authentication page a name (i.e. "XXX with Access Request")
6) Give an optional description if you wish
7) Click "OK" to save the new page

The next step is to add the Access Request button to your remediation page. Perform the following steps to add the Access Request button to the appropriate remediation page:

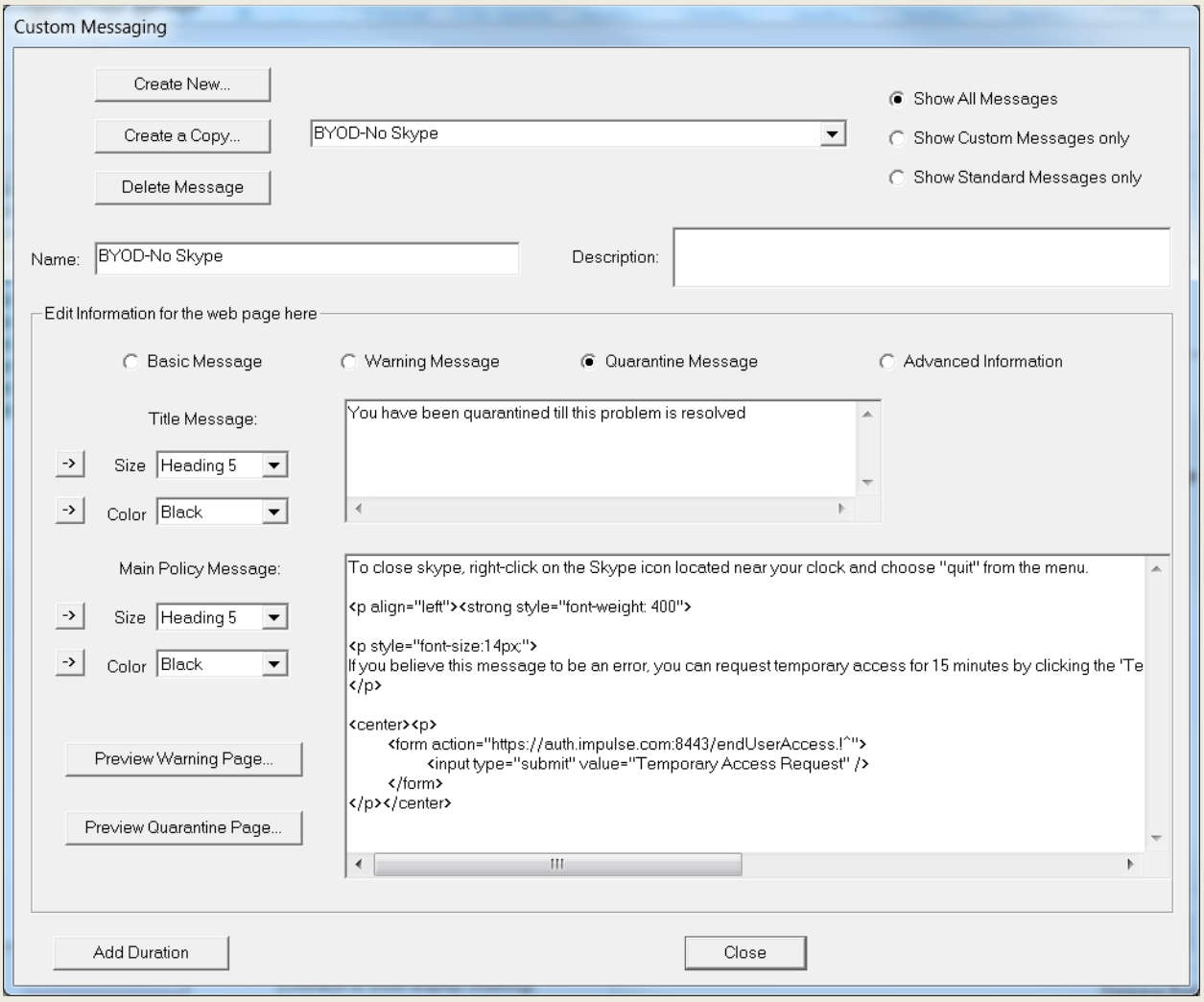
1) Select the appropriate remediation page from the drop down menu at the top center of the screen
2) Click the "Quarantine Message" radio button to display the source code for the remediation page
3) Add the following code at the end of the source code (Text can be customized to fit your needs):

```
<p align="left"><strong style="font-weight: 400">

<p style="font-size:14px;">
If you believe this message to be an error, you can request temporary access
for 15 minutes by clicking the 'Temporary Access Request' button below.  If
the problem persists, please contact the help desk at ext. 4357.
</p>

<center><p>
      <form action="https://auth.impulse.com:8443/access">
            <input type="submit" value="Temporary Access Request" />
      </form>
</p></center>
```

   a. Click the "Preview Quarantine Page…" button to see how the page will look
   b. You may have to adjust the location of the button code to ensure proper placement on the screen
   c. When you are satisfied with how the page looks, click "Close"
   d. Click the "Upload Data" button to save the changes and commit them to the Safe•Connect server
   e. See the Screenshot below for an example



Appendix

Access Request Links

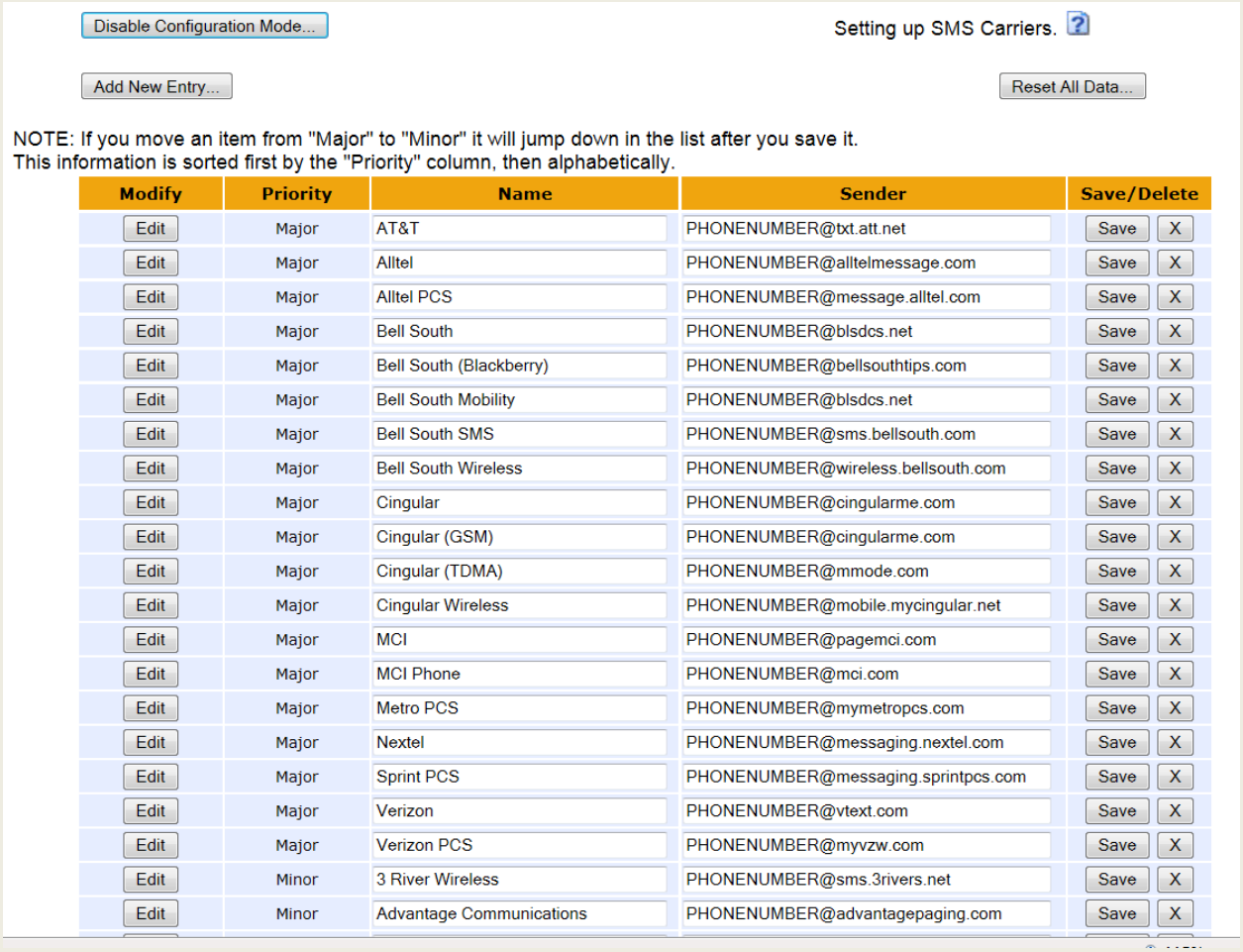
- Access Request Portal:
  - Standard: https://auth.impulse.com:8443/access
  - Branded example: https://safeconnect.customer.edu:9443/access
- Administrative Links:
  - Standard: https://auth.impulse.com:8443/config.s
  - Branded example: https://safeconnect.customer.edu:9443/config.s
    - User Options >> Access Request
    - SMS Carriers
- Notes:
  - In a clustered deployment, please reference the manager IP.
  - The standard default port is 8443, however in a branded deployment it will default to 9443.

SMS Carriers

Safe•Connect is pre-configured with all of the major mobile carriers and as many of the regional carriers as could be reasonably included. For a carrier to be listed in the user's drop down selection box of the Access Request Page, they must be configured in Safe•Connect with their priority set to "Major" in the SMS Carriers configuration page.

To access this page, select "SMS Carriers" from the "End User Configuration" section of the system configuration page. To make any changes to a listed Carrier, you must first click "Enable Configuration Mode…" to enable the "Edit" buttons. Clicking an "Edit" button will toggle the drop down menu to change the Priority of that Carrier. You can also edit a Carrier's name and SMS Gateway email destination. Additional Carriers can be added by clicking the "Add New Entry" button. Be sure to click "Save" for each carrier after making any modifications to that Carrier. To delete a listed Carrier, click the "X" button to the right of the Carrier.

Clicking the "Reset All Data" button will return this page to the factory defaults.



Modify	Priority	Name	Sender	Save/Delete
Edit	Major	AT&T	PHONENUMBER@txt.att.net	Save X
Edit	Major	Alltel	PHONENUMBER@alltelmessage.com	Save X
Edit	Major	Alltel PCS	PHONENUMBER@message.alltel.com	Save X
Edit	Major	Bell South	PHONENUMBER@blsdcs.net	Save X
Edit	Major	Bell South (Blackberry)	PHONENUMBER@bellsouthtips.com	Save X
Edit	Major	Bell South Mobility	PHONENUMBER@blsdcs.net	Save X
Edit	Major	Bell South SMS	PHONENUMBER@sms.bellsouth.com	Save X
Edit	Major	Bell South Wireless	PHONENUMBER@wireless.bellsouth.com	Save X
Edit	Major	Cingular	PHONENUMBER@cingularme.com	Save X
Edit	Major	Cingular (GSM)	PHONENUMBER@cingularme.com	Save X
Edit	Major	Cingular (TDMA)	PHONENUMBER@mmode.com	Save X
Edit	Major	Cingular Wireless	PHONENUMBER@mobile.mycingular.net	Save X
Edit	Major	MCI	PHONENUMBER@pagemci.com	Save X
Edit	Major	MCI Phone	PHONENUMBER@mci.com	Save X
Edit	Major	Metro PCS	PHONENUMBER@mymetropcs.com	Save X
Edit	Major	Nextel	PHONENUMBER@messaging.nextel.com	Save X
Edit	Major	Sprint PCS	PHONENUMBER@messaging.sprintpcs.com	Save X
Edit	Major	Verizon	PHONENUMBER@vtext.com	Save X
Edit	Major	Verizon PCS	PHONENUMBER@myvzw.com	Save X
Edit	Minor	3 River Wireless	PHONENUMBER@sms.3rivers.net	Save X
Edit	Minor	Advantage Communications	PHONENUMBER@advantagepaging.com	Save X