

Quick Guide – Requesting Firewall Exceptions

Subject: IMS Firewall Exception Request

Intent: Instructions for filling out the online Firewall Exception Request form

Overview

The Identity Management System (IMS) Firewall Exception Request module enables UPMC staff to submit online requests for exceptions to current firewall configurations. This module consists of a series of Web-based forms.

With the online Firewall Exception Request utility, you can request new firewall exceptions. Firewall exceptions enable users who are outside a firewall to access protected resources within the firewall.

To use the online Firewall Exception Request form, you must log on to IMS and perform the following steps:

1. [Start the Firewall Exception Request form utility](#)
2. [Identify the person for whom the request is being made](#)
3. [Set the expiration date for the exception](#)
4. [Note which firewall systems will be affected](#)
5. [Submit the exception request](#)

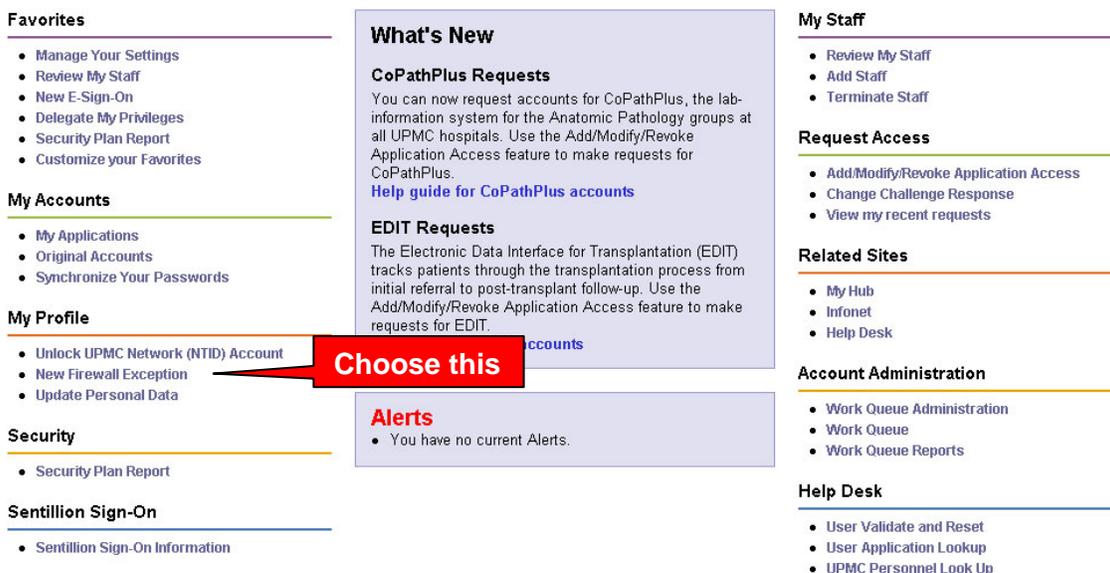
Once all of these steps are performed successfully, IMS will forward the request to the appropriate firewall administrators and send a confirmation e-mail.

Quick Guide – Firewall Exception Request Form

Step 1: Start the Utility

Go to the IMS Web site (<https://ims.upmc.com>), and log on using your E-Sign-On account ID and password.

The IMS Startup page appears:



The screenshot shows the IMS Startup page with several sections:

- Favorites:**
 - Manage Your Settings
 - Review My Staff
 - New E-Sign-On
 - Delegate My Privileges
 - Security Plan Report
 - Customize your Favorites
- My Accounts:**
 - My Applications
 - Original Accounts
 - Synchronize Your Passwords
- My Profile:**
 - Unlock UPMC Network (NTID) Account
 - New Firewall Exception** (highlighted with a red callout box labeled "Choose this")
 - Update Personal Data
- Security:**
 - Security Plan Report
- Sentillion Sign-On:**
 - Sentillion Sign-On Information
- What's New:**
 - CoPathPlus Requests:** You can now request accounts for CoPathPlus, the lab-information system for the Anatomic Pathology groups at all UPMC hospitals. Use the Add/Modify/Revoke Application Access feature to make requests for CoPathPlus. [Help guide for CoPathPlus accounts](#)
 - EDIT Requests:** The Electronic Data Interface for Transplantation (EDIT) tracks patients through the transplantation process from initial referral to post-transplant follow-up. Use the Add/Modify/Revoke Application Access feature to make requests for EDIT.
- Alerts:**
 - You have no current Alerts.
- My Staff:**
 - Review My Staff
 - Add Staff
 - Terminate Staff
- Request Access:**
 - Add/Modify/Revoke Application Access
 - Change Challenge Response
 - View my recent requests
- Related Sites:**
 - My Hub
 - Infonet
 - Help Desk
- Account Administration:**
 - Work Queue Administration
 - Work Queue
 - Work Queue Reports
- Help Desk:**
 - User Validate and Reset
 - User Application Lookup
 - UPMC Personnel Look Up

Select **New Firewall Exception** under the **My Profile** menu.

Note: The items on this page are based on your access privileges and any preferences you may have set. Therefore the menus you see and their placement may be different from what appears on the screen shown above.

Quick Guide – Firewall Exception Request Form

Or, click here:

My Menus	My Profile (formerly Employee Menu)	
<ul style="list-style-type: none"> • Account Administration • Application Maintenance Menu • Compliance • Firewall Exception • Help Desk 	<ol style="list-style-type: none"> 1 Unlock UPMC Network (NTID) Account Confirm your identification in IMS to unlock your UPMC Network account. 2 Change Challenge Response Update your secret question and answer, which are used to validate your identity in IMS. This powerful tool replaces the need for Social Security numbers. 3 New Firewall Exception Submit a request for an exception to a firewall configuration. 	<ol style="list-style-type: none"> 6 Change E-Sign-On Identity Change the name of your ESO ID (e.g., from smithw to jonesrw after a marriage). 7 My System Security Plans My System Security Plans 8 Set Data Preference Set Data Preference 9 My System Security Plans My System Security Plans

Click here

IMS displays the following screen:

As per UPMC Policy HS-IS0208, an approved system security plan is required for all computer systems and applications, and is required before any firewall exception will be granted. [System Security Plan](#)

Please contact ISG at SecurityPlans@upmc.edu if you have any questions.



If you want to see a list of your current security plans, need to edit an existing plan, or need to create a new security plan for the exception you are requesting, click the **System Security Plan** link.

Otherwise, click **Continue**.

If you have any existing security plans, the following screen loads showing a list of your existing plans:

Quick Guide – Firewall Exception Request Form

System Security Plan

[System Security Plan Overview](#)

Security Plan ID	Security Plan	Date Changed	Status	Plan Approved Date	Action	Add Owners
Test3Testology2007.1.0	Test3	3/15/2007 12:18:58 PM			View Edit	EDIT OWNERS
Test_2Testology2007.1.0	Test 2	3/15/2007 12:18:14 PM	1. Submitted		View Edit	EDIT OWNERS
Robins_PlaTestology2007.1.0	Robins Test Security Plan	3/15/2007 9:28:01 AM			View Edit	EDIT OWNERS

On this screen you may view or edit existing plans, edit the owners of the plan, or add a new plan. If you need help adding a new plan, see [Quick Guide – Working With Security Plans](#).

IMS displays the following search form:

Firewall Exception Request E-Sign-On Account Lookup

First, you must verify that the Requestor has a [UPMC E-Sign-On Account](#). Enter the last name of the Requestor. Enter more information only if you want to narrow your search results.

UPMC E-Sign-On Search:	
Last Name:	<input type="text" value="sandwich"/> <input type="checkbox"/> Exact Match I am the Owner
First Name:	<input type="text"/>
Middle Initial:	<input type="text"/>
UPMC E-Sign-On:	<input type="text"/>
<input checked="" type="checkbox"/> Include Service Accounts	

Show Search Results Below

You can now identify the person for whom you are making the firewall exception request.



Quick Guide – Firewall Exception Request Form

Step 2: Identify the Computer User

*If you are the owner of this firewall exception request, click on the **I am the Owner** link on the right side of the Search Engine window. IMS will automatically take you to the Submit New Firewall Exception Request form with your name already entered in the Identity Information section. You can then proceed to Step 3.*

If you are not the owner of the request, you must identify the person for whom the request is being made. This is done using the E-Sign-On Search engine to find the UPMC employee or non-employee in the IMS database.

You can search for a person just by entering that person's last name and clicking on **Show Search Results Below**. You will see a list of every IMS record with the last name you typed in. Additionally, the E-Sign-On Account Search engine uses wild cards. Therefore, if you type in "john" as a last name, the result list shows anyone with the last name of John, Johnson, Johnston, Johnstone, etc. You can narrow your search by typing in the person's first initial, middle initial or first name.

Note: You can turn off the wild-card feature by checking the **Exact Match** check box before running a search.

If you know the person's E-Sign-On, you can enter it to find that person's records directly.

Quick Guide – Firewall Exception Request Form

Firewall Exception Request E-Sign-On Account Lookup

First, you must verify that the Requestor has a [UPMC E-Sign-On Account](#). Enter the last name of the Requestor. Enter more information only if you want to narrow your search results.

UPMC E-Sign-On Search:	
Last Name:	<input type="text" value="sandwich"/> <input type="checkbox"/> Exact Match I am the Owner
First Name:	<input type="text"/>
Middle Initial:	<input type="text"/>
UPMC E-Sign-On:	<input type="text"/>
<input checked="" type="checkbox"/> Include Service Accounts	

Show Search Results Below

» Click on the [UPMC E-Sign-On link below](#).

NAME	UPMC E-Sign-On	JOB TITLE	DEPARTMENT	HOSPITAL	ESO_FL_ID
sandwich, icecream x	sandwi6246	Tester	Testology	Magee-Womens Hospital	199573
sandwich, icecream x	sandwi9862	Tester	Testology		199586
sandwich, icecream x	sandwi8261	Tester	Testology		199587
sandwich, meatball x	sandwm9036	Tester	Testology	Magee-Womens Hospital	199554
sandwich, pepperoni x	sandwp8675	Tester	Testology	Magee-Womens Hospital	199553
sandwich, salmon x	sandws2407	Tester	Testology	Magee-Womens Hospital	199560
sandwich, spam x	sandws1594	Tester	Testology	Magee-Womens Hospital	199552

Once you find the person for whom you are making the firewall exception request, select that person's E-Sign-On account link.



Quick Guide – Firewall Exception Request Form

If you do not find the person in the IMS database, it means one of the following:

1. The person is a UPMC non-employee without computer access
2. The person is a recently hired UPMC employee whose data hasn't yet been entered by Human Resources

You can give non-employees computer access by creating an E-Sign-On account for them. See the Help document “[Quick Guide – Add a Non-Employee to IMS](#)” for more information.

For new hires whose data hasn't been imported into IMS yet, you can also manually create an E-Sign-On account for them in order to make a firewall exception request. The employees' E-Sign-On accounts will then be updated by the Human Resources data as long as you use the correct Social Security numbers.

If the E-Sign-On account you choose has missing information associated with it, you will first see the Update E-Sign-On Account page. You must enter the missing information before you can request a firewall exception. For more information, see the Help document “[Quick Guide – Update an E-Sign-On Account](#).”

Step 3: Set the Expiration Date for the Exception

Once you find the computer user, select his or her E-Sign-On link. IMS will display the following form with that user's Identity Information at the top:

Submit New Firewall Exception Requests

Please Click on the "Add More Exception Details" Button to enter exception details for a firewall System.

Identity Information	
Name (LN, FN, MI):	<input type="text" value="icecream"/> <input type="text" value="sandwich"/> <input type="text" value="x"/> <small>First Name Last Name MI</small>
Account Expiration Date:	<input type="text" value="3"/> / <input type="text" value="21"/> / <input type="text" value="2008"/> <input type="checkbox"/> Permanent (NOTE: All firewall exceptions are reviewed annually.)
Firewall System:	<input type="text" value="Arnold Palmer Cancer Center"/>
Security Plan ID:	<input type="text"/>
Description:	<input type="text"/>
Action:	<input type="text" value="Accept"/>
Service:	<input type="text"/>
Destination:	<input type="text"/>
Source:	<input type="text"/>
Comments/Special Instructions	
<input type="text"/>	
<input type="button" value="Add Exception Firewall Request"/>	



Quick Guide – Firewall Exception Request Form

Select the month, day, and year when this firewall exception will expire. The default is one year from the day of request. To make this exception permanent, click on the **Permanent** check box.

Submit New Firewall Exception Requests

Please Click on the "Add More Exception Details" Button to enter exception details for a firewall System.

Identity Information			
Name (LN, FN, MI):	<input type="text" value="icecream"/>	<input type="text" value="sandwich"/>	<input type="text" value="X"/>
	<small>First Name</small>	<small>Last Name</small>	<small>MI</small>
Account Expiration Date:	<input type="text" value="3"/> / <input type="text" value="21"/> / <input type="text" value="2008"/>	<input type="checkbox"/> Permanent	(NOTE: All firewall exceptions are reviewed annually.)

Note: All firewall exceptions are reviewed annually, including permanent exceptions.

Note: This date will apply to all exceptions created by the request. If you need to request firewall exceptions for a user but need different expiration dates, submit multiple requests.

Once you have chosen an expiration date, you are ready for the next step.

Step 4: Note Which Firewall Systems Will Be Affected

From the list of Firewall Systems, note the ones that will be affected by selecting one at a time from the drop-down list, filling in the Security Plan ID of the plan to be associated with each system, and other related details. Click **Add Exception Firewall Request** to add the exception to your request.

Note: If you do not enter at least one set of exception details, you will not be able to proceed with your request.

Firewall System:	Arnold Palmer Cancer Center
Security Plan ID:	
Description:	
Action:	Accept
Service:	
Destination:	
Source:	
Comments/Special Instructions	



After entering each system the page reloads showing a list of the security plans that have been added.

Quick Guide – Firewall Exception Request Form

Submit New Firewall Exception Requests

Please Click on the "Add More Exception Details" Button to enter exception details for a firewall System.

Identity Information

Name (LN, FN, MI):
First Name Last Name MI

Account Expiration Date: / / Permanent **(NOTE: All firewall exceptions are reviewed annually.)**

Security Plan ID	Firewall System	Source	Destination	Service	Description	Action		
Test3	ISG	test	test	HTTP	I need this exception because...	Accept	<input type="button" value="EDIT"/>	<input type="button" value="DELETE"/>

Firewall System:

Security Plan ID:

A list of added exception requests displays

At this point you can edit the plan(s) associated with the request by clicking **EDIT** or delete them by clicking **DELETE**.

You may also click the **Add Exception Firewall Request** button again to add additional requests or click **Proceed with Exception Firewall Requests** to submit the one(s) you have entered. Again, you may add as many systems as are needed.



Quick Guide – Firewall Exception Request Form

The Details Fields

In the field next to **Description**, enter a brief description for the exception request.

Choose an action from the **Action** menu. This will be the action performed by the selected firewall(s) on network packets from the selected user, which he or she has entered in the fields above. The meanings of the actions are as follows:

Action	Meaning
Accept	Network traffic is allowed.
Drop	Network traffic is blocked without notification.
Reject	Network traffic is blocked, and notification is sent to the source computer.
Client Authenticate	Only traffic authenticated by the client software (usually VPN software) is allowed.
Client Encrypt	Traffic is allowed and is encrypted at the firewall on a client-by-client basis.
Encrypt	Traffic is allowed, and the firewall encrypts all traffic.
Session Authenticate	A user name and password are required to authenticate traffic on a session-by-session basis.
User Authenticate	A user name and password are required to authenticate traffic on a user-by-user basis.

Most firewall exceptions have Accept actions, as they are intended to allow packets through the firewall that would ordinarily be blocked.

In the field next to **Service**, enter the names or port numbers of the service(s) that are the subject of this exception. Common services are “HTTP,” “FTP,” “SMTP,” “SNMP,” “Port 143,” “tcp 4201,” etc.



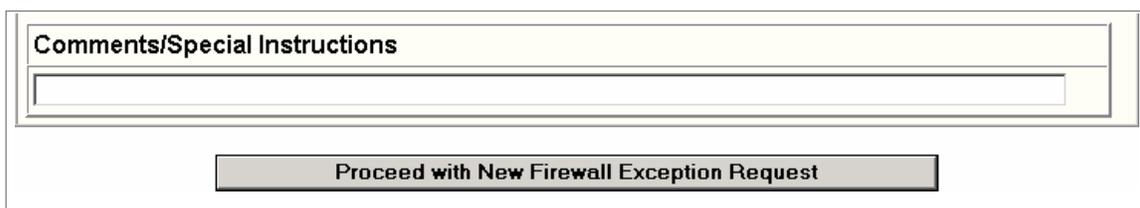
Quick Guide – Firewall Exception Request Form

In the field next to **Destination**, enter the IP Address of the destination computer inside of the firewall. This should be the computer that the user will be accessing from the source computer. Again, you can enter multiple IP addresses separated by commas.

In the field next to **Source**, enter the IP Address of the source computer outside the firewall. This should be the user's computer that will need a firewall exception. You can enter as many IP addresses as are needed. Separate the IP addresses with commas.

Step 5: Submit the Exception Request

Once you are finished defining the details for each firewall exception, you are ready to finalize your request and submit it.



Comments/Special Instructions

Proceed with New Firewall Exception Request

Enter any comments or special instructions that the firewall administrators may need in order to handle your request.

Review the information in the form, and make sure that it is all correct.

If you are satisfied with the information in the form, press **Proceed with New Firewall Exception Request** to complete the form entry process and submit your request.

Result: IMS starts processing your Firewall Exception Request

When you successfully submit the firewall exception request through IMS, it displays the following confirmation:



Email Sent to appropriate data owners for further Request Processing...

Please Click [Here](#) to make another request

IMS automatically assigns a unique tracking number to your request. You will receive an automated e-mail from IMS to notify you that the request is being processed.



Quick Guide – Firewall Exception Request Form

Document Information

Subject: IMS Firewall Exception Request

Title: Quick Guide – Online Firewall Exception Request Form

Subtitle:

Deliverable ID:

Date/Revision: 03/21/2007; Rev: 2.0

Author/Department: [Robin Fowler / ISG](#)

Audience: UPMC computer users

Intent: Instructions for using the online Firewall Exception Request form

Related Documents: