



Tips for Businesses

- Run audit reports regularly on employee activity.
- Delete the user profile for any employee that leaves the company.
- Do not suppress any email notifications within Business Banking.
- Utilize balance alerts.
- Keep access to Business Banking restricted to only those employees that need to have access.
- Know all types of transaction limits, and grant limits only for what is necessary for business operations.
- Have a second person at the business approve submission of wire transfers, ACH files, and EFTPS files. The second person should use a different computer than the one used to initiate an action.
- Periodically evaluate controls and end user permissions.
- Monitor account activity for anomalies or suspicious transactions and investigate/report to your financial institution immediately.
- Install Trusteer Rapport

Run audit reports regularly on employee activity.

The Juniata Valley Bank

Administration Account Activities & Reporting Payments & Transfers Online Requests

Manage Users
Add/Change/Remove Users
View User Activity Reporting

Manage Company
Set Account Name
Change Timeout

My Profile
Change My Password
Manage Security Code Delivery
Unenroll Computers
Activate Token
Set Main Page

Submit Delete

Date Selection

Search by Log File
Select Log File

OR

Search by Range of Dates
From
To

Query Selection
 All Activities

First Query
Transaction Type (none)
Print to Search
Value
And / Or (none)

https://www.jvonline.com/online/serve/04/asklogReport.cgi?date=displ... Local time: 8/29/16

Enter the date range desired, you can also choose specific activities or select “all activities”. This report can be saved to make it easier to quickly run on a daily basis.

8/29/16

Delete the user profile for any employee that leaves the company.

The Juniata Valley Bank

Administration Account Activities & Reporting Payments & Transfers Online Requests

Add/Change/Remove Users

Select a user from the drop-down list or New to clear fields and add a new user.

Current User: JTEST OR New

User Name: Jvb Tester
User ID: JTEST
User Password: []
Confirm Password: []
Email Address: admin@jvbonline.com

Update Delete Reset List

Security Options

Reset All MFA Credentials: Unenroll computers and invalidate existing password. Requires entry of a new password before clicking this button.

Unenroll Computers: Unenroll user's computers and force an MFA challenge at next login.

MFA Security Code Delivery Options

If no MFA delivery options exist, the user's contact email address will be used.

Email Address	Phone Number	Ext.	Ext. Dial Delay	Voice Test
[]	[]	[]	N/A	[] []
[]	[]	[]	N/A	[] []
[]	[]	[]	N/A	[] []
[]	[]	[]	N/A	[] []

8/29/16

Do not suppress any email notifications within Business Banking.

Add/Change/Remove Users

Wire Transfer

<input checked="" type="checkbox"/> Allow Wire Transfer	<input type="checkbox"/> Initiate Group
<input checked="" type="checkbox"/> Initiate Template	<input checked="" type="checkbox"/> Approval
<input type="checkbox"/> Initiate Freeform	<input type="checkbox"/> Template Group Maintenance
<input type="checkbox"/> Template Maintenance	<input type="checkbox"/> Suppress Email Approval Request ←
<input type="checkbox"/> Investigation Request	
<input type="checkbox"/> Foreign Exchange Rates	

Daily Limit	Transaction Limit	Daily Approval Limit	Transaction Approval Limit
<input type="text" value="\$1.00"/>	<input type="text" value="\$1.00"/>	<input type="text" value="\$1.00"/>	<input type="text" value="\$1.00"/>

Stop Payments

<input type="checkbox"/> Allow Stop Payments
<input type="checkbox"/> Stop Payments

ACH

<input checked="" type="checkbox"/> Allow ACH	<input type="checkbox"/> Assign Participant to Batch
<input type="checkbox"/> Participant Maintenance	<input type="checkbox"/> Suppress Email Approval Request ←
<input checked="" type="checkbox"/> ACH Approval	<input checked="" type="checkbox"/> Initiate Batch
<input type="checkbox"/> Batch Template Maintenance	<input type="checkbox"/> Import ACH Data
<input type="checkbox"/> Reversal	<input type="checkbox"/> Send ACH File

Daily Credit Limit	Daily Debit Limit	Batch Credit Limit	Batch Debit Limit
<input type="text" value="\$1.00"/>	<input type="text" value="\$0.00"/>	<input type="text" value="\$1.00"/>	<input type="text" value="\$0.00"/>
Daily Approval Credit Limit	Daily Approval Debit Limit	Batch Approval Credit Limit	Batch Approval Debit Limit
<input type="text" value="\$1.00"/>	<input type="text" value="\$0.00"/>	<input type="text" value="\$1.00"/>	<input type="text" value="\$0.00"/>

Federal Tax Payments

Allow Federal Tax Payments

Federal Tax Payments

Federal Tax Payments Approval

Suppress Email Approval Request

Daily Limit

\$1.00

Transaction Limit

\$1.00

Daily Approval Limit

\$1.00

Transaction Approval

\$1.00

Additional Services

Online Statements

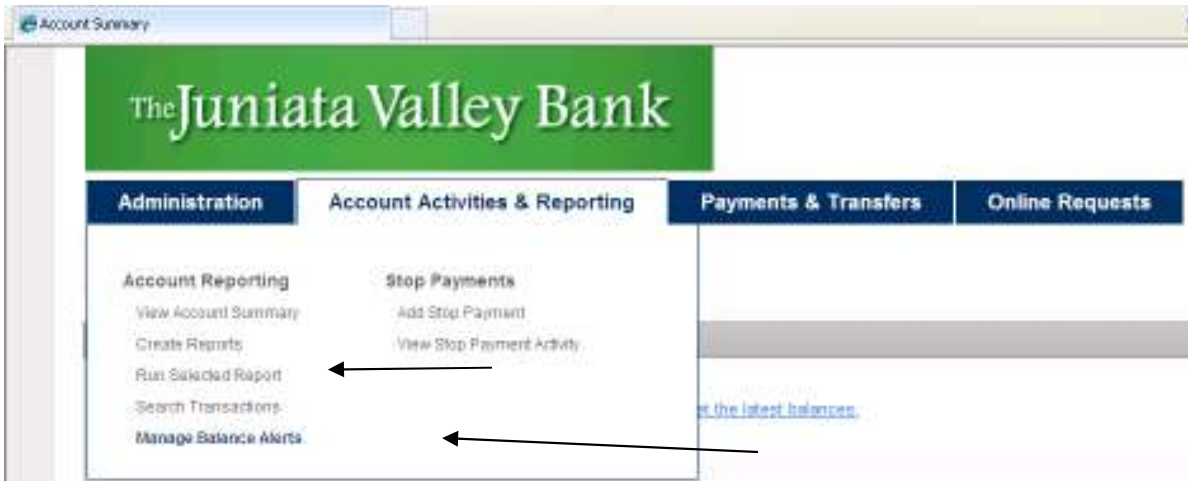
Update

Delete

Reset

List

Utilize balance alerts



8/29/16

The Juniata Valley Bank

Administration Account Activities & Reporting Payments & Transfers Online Requests

Company: JAMIE BUNNY

Manage Balance Alerts

Add An Alert

Current Alert(s)

Select	Account	Balance Type	Balance Condition	Amount	Email Address
--------	---------	--------------	-------------------	--------	---------------

Know all types of transaction limits, and grant limits only for what is necessary for business operations

The Juniata Valley Bank

Administration Account Activities & Reporting Payments & Transfers Online Requests

Manage Users
 Add/Change/Remove Users
 View User Activity Reporting

Manage Company
 Set Account Name
 Change Timeout

My Profile
 Change My Password
 Manage Security Code Delivery
 Uninstall Computers
 Activate Token
 Set Main Page

8/29/16

Wire Transfer

<input checked="" type="checkbox"/> Allow Wire Transfer	<input type="checkbox"/> Initiate Group		
<input checked="" type="checkbox"/> Initiate Template	<input checked="" type="checkbox"/> Approval		
<input type="checkbox"/> Initiate Freeform	<input type="checkbox"/> Template Group Maintenance		
<input type="checkbox"/> Template Maintenance	<input type="checkbox"/> Suppress Email Approval Request		
<input type="checkbox"/> Investigation Request			
<input type="checkbox"/> Foreign Exchange Rates			
Daily Limit \$1.00	Transaction Limit \$1.00	Daily Approval Limit \$1.00	Transaction Approval Limit \$1.00

Stop Payments

<input type="checkbox"/> Allow Stop Payments
<input type="checkbox"/> Stop Payments

ACH

<input checked="" type="checkbox"/> Allow ACH	<input type="checkbox"/> Assign Participant to Batch		
<input type="checkbox"/> Participant Maintenance	<input type="checkbox"/> Suppress Email Approval Request		
<input checked="" type="checkbox"/> ACH Approval	<input checked="" type="checkbox"/> Initiate Batch		
<input type="checkbox"/> Batch Template Maintenance	<input type="checkbox"/> Import ACH Data		
<input type="checkbox"/> Reversal	<input type="checkbox"/> Send ACH File		
Daily Credit Limit \$1.00	Daily Debit Limit \$0.00	Batch Credit Limit \$1.00	Batch Debit Limit \$0.00
Daily Approval Credit Limit \$1.00	Daily Approval Debit Limit \$0.00	Batch Approval Credit Limit \$1.00	Batch Approval Debit Limit \$0.00

Federal Tax Payments

<input checked="" type="checkbox"/> Allow Federal Tax Payments	<input checked="" type="checkbox"/> Federal Tax Payments Approval		
<input checked="" type="checkbox"/> Federal Tax Payments			
<input type="checkbox"/> Suppress Email Approval Request			
Daily Limit \$1.00	Transaction Limit \$1.00	Daily Approval Limit \$1.00	Transaction Approval Limit \$1.00

Information Security Best Practices

- The Super User Account should only be used on a dedicated machine which should be physically secured and password protected.
 - The Criteria for a Super User dedicated machine
 - The computer should be physically secured.
 - The computer should be behind a physical firewall.
 - The computer should be placed on its own subnet if possible.
 - All Security Patches Must Be Up To Date.

8/29/16

- Anti-Virus Software Should be Installed and definitions Must Be Up To Date.
- Anti-Spyware/Anti-Malware is also recommended.

- Best Practices should also be followed for any other computer that can approve any wire transfers.

- Close all other applications and browser windows before initiating online banking.

- Look for any strange or foreign changes on the website. If you see anything different, call the financial institution.

- Having issues remembering passwords?

- Try using Password Safe <https://pwsafe.org/>

- Do not use the same password for multiple accounts.

- Do not share any passwords.

- It is highly suggested that the Super User for the company only use their access for resetting or setting up any sub users. The super user should have a separate login for doing Business Banking transactions. The reason this is suggested is if the Super Users credentials are compromised, the fraudster has access to all controls and even creating sub users to allow access for approving transactions.

- The Company should allow one designated machine in the office for doing strictly Business Banking transactions. This machine should not be allowed to surf the internet, check email, etc.

The best way to avoid becoming a victim of a cyberheist is not to let computer crooks into the computers you use to access your organization's bank accounts online. The surest way to do that is to maintain a clean computer: Start with a fresh install of the operating system and all available security updates.

If possible, use something other than Microsoft Windows. Most malware only runs in a Microsoft Windows environment, so using a different operating system for the dedicated machine is an excellent way to drastically reduce the likelihood of becoming a cyberheist victim. A "live CD" is a free and relatively painless way to temporarily boot a Windows PC into a Linux environment. The beauty of this approach is that even if you fail to maintain a clean Windows PC, malicious software can't touch or eavesdrop on your banking session while you're booted into the Live CD installation.

8/29/16

If you installed it, patch it. Keep the operating system up-to-date with patches. It's equally important to update the third-party software on your system, especially browser plugins. One leading cause of malware infections are exploit kits, which are attack tools stitched into hacked Web sites that exploit unpatched or undocumented vulnerabilities in widely-used browser plugins. Tools such as File Hippo's Update Checker and Secunia's Personal Software Inspector will alert you to new security updates available for third-party programs installed on your PC.

Remove any unneeded software from dedicated systems used to access the bank's site. In particular, unneeded plugins (such as Java) should be junked.

Use a bookmark to access the bank's site. Avoid "direct navigation," which involves manually typing the bank's address into a browser; a fat-fingered keystroke may send you to a look-alike phishing Web site or one that tries to foist malicious software.

Remember that antivirus software is no substitute for common sense. A majority of today's cyberheists begin with malware that is spread via email attachments. Many of these threats will go undetected by antivirus tools in the first few days.