

Converge

Getting Started Guide

Revision Date: November 2015

Copyright

Copyright © 2015 Elavon, Incorporated. All rights reserved. No part of this publication may be reproduced or distributed without the prior consent of Elavon, Inc., Two Concourse Parkway, Suite 800, Atlanta, GA 30328.

Disclaimer

Elavon, Inc. provides this publication *as is* without warranty of any kind, either expressed or implied. This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes will be incorporated in new editions of the publication. Elavon, Inc. may make improvement and/or changes in the product(s) and/or programs(s) described in this publication at any time.

Trademarks

Converge is a registered trademark of Elavon, Inc. All other brand and product names are trademarks or registered trademarks of their respective companies:

ActiveX®

MasterCard®

American Express®

MasterCard SecureCode™

Diners Club®

Microsoft®

Discover®

RDM®

Epson®

Star Micronics®

Equinox®

UnionPay®

Ingenico®

Verified by Visa™

JCB®

Visa®

MagTek®

WinZip®

Preface

This document describes step by step procedures on how to use Converge including:

- Features and options
- User interface overview
- System requirements
- Account set up information
- Logon process
- Password reset processes

This document is intended for all users of the Converge product and contains the information necessary for you to be able to use all the features of the product effectively.

Typographical Conventions

Throughout this guide, you will see words and phrases that appear in different fonts and formats. The following list describes the typographical conventions used in this guide.

- **Bold text**

Indicates a menu option, a window title, buttons, and so on that you can use to identify a part of the user interface.

Examples:

Print or **Save As** dialog box

- **Menu selection sequences**

Indicates a series of menu options that you need to select in a particular sequence and listed in one step. Each menu option is separated by a pipe (|).

1. Choose **File | Save As | File Name** and enter the name of the document.

- **Courier text**

Indicate examples of software code. Usually this type of text is encapsulated in a code box as illustrated below.

Begin Header

```
POST /VirtualMerchantDemo/process.do HTTP/1.1
```

```
_url=http3A2F2Fwww.url.com2Fcgi-bin
```

```
2Ftesttran.cgi&ssl_receipt_apprvl_method=REDG&ssl_receipt_apprvl  
_get_url=http3A2
```

End Header

- **Bold courier text**

Indicates a command that you would type into a command prompt window as illustrated below.

```
cd c:\users\
```

- **Italicized text**

Indicates that the word or phrase is:

- A reference to another document as illustrated below.

Refer to the *Elavon User Guide*.

- Emphasized for clarification as illustrated below.

You *do not* need to select **Apply**.

- The word is replacement text, such as a variable for a piece of code that you need to enter the appropriate value for your implementation as illustrated below.

```
<xml>  
<country_code>Country Code</country_code>  
</xml>
```

Related Documentation

The following documents are available related to the Converge product.

- Converge Administration Guide
- Converge Transaction Processing Guide
- Converge Chip and PIN (EMV) Transaction Processing Addendum
- Converge Peripheral Device Installation and Setup Guide
- VirtualMerchant Mobile Classic
- VirtualMerchant Mobile 2.2 User Guide

Revision History

The following table provides a description of the changes made to this document from its origination to the current release.

Revision	Date	Revision Notes
A	SEP-2014	Original release of the Converge Getting Started Guide
B	OCT-2014	New Sign In page
C	NOV-2014	Enhancement of password requirements
D	FEB-2015	Loyalty card and EMV (Canada) capabilities
E	MAR-2015	Password reset change
F	MAY-2015	Addition of ConvergeConnect and enhancement of home page
G	JUL-2015	New URL for launching Converge: www.convergepay.com
H	OCT-2015	Added Chip read (EMV) for U.S. and key entry is now supported
I	NOV-2015	Added support of Ingenico iCMP for U.S.

Table of Contents

Chapter 1: Introduction	1
Features	2
Converge Options	4
Transaction Options	5
Market-Specific Options	5
Payment Options	5
Processing Options.....	6
Reporting Options.....	7
Account Options.....	7
Customization Options.....	7
Peripherals Options.....	8
Security Features	8
System Timeouts.....	9
System Logins.....	9
Enhanced Logins with IP Recognition	9
Password Requirements	10
Email Notifications	10
Fraud Protection Features	10
Referrer URLs	11
Fraud Prevention Rules.....	11
Business Rules.....	14
Business Rules Types.....	14
Business Rules Filters	15
3D Secure Authentication (Verified by Visa® and MasterCard® SecureCode™)	18
Chapter 2: Getting Started.....	19
System Requirements	19
Supported Internet Browsers	19

Browser Pop-up Blockers	20
Setting Up Converge Accounts	20
Launching Converge.....	21
Signing In to Converge	22
Resetting Your Initial Password	24
Resetting Your Latest Password.....	26
Converge Interface.....	29
Support Menu Options	29
The MerchantConnect Link.....	30
The Support Section Link	30
The Help Link.....	36
The Logout Link	38
Transaction Menu Options	38
Getting Assistance from Elavon	39
Additional Resource Guides	39

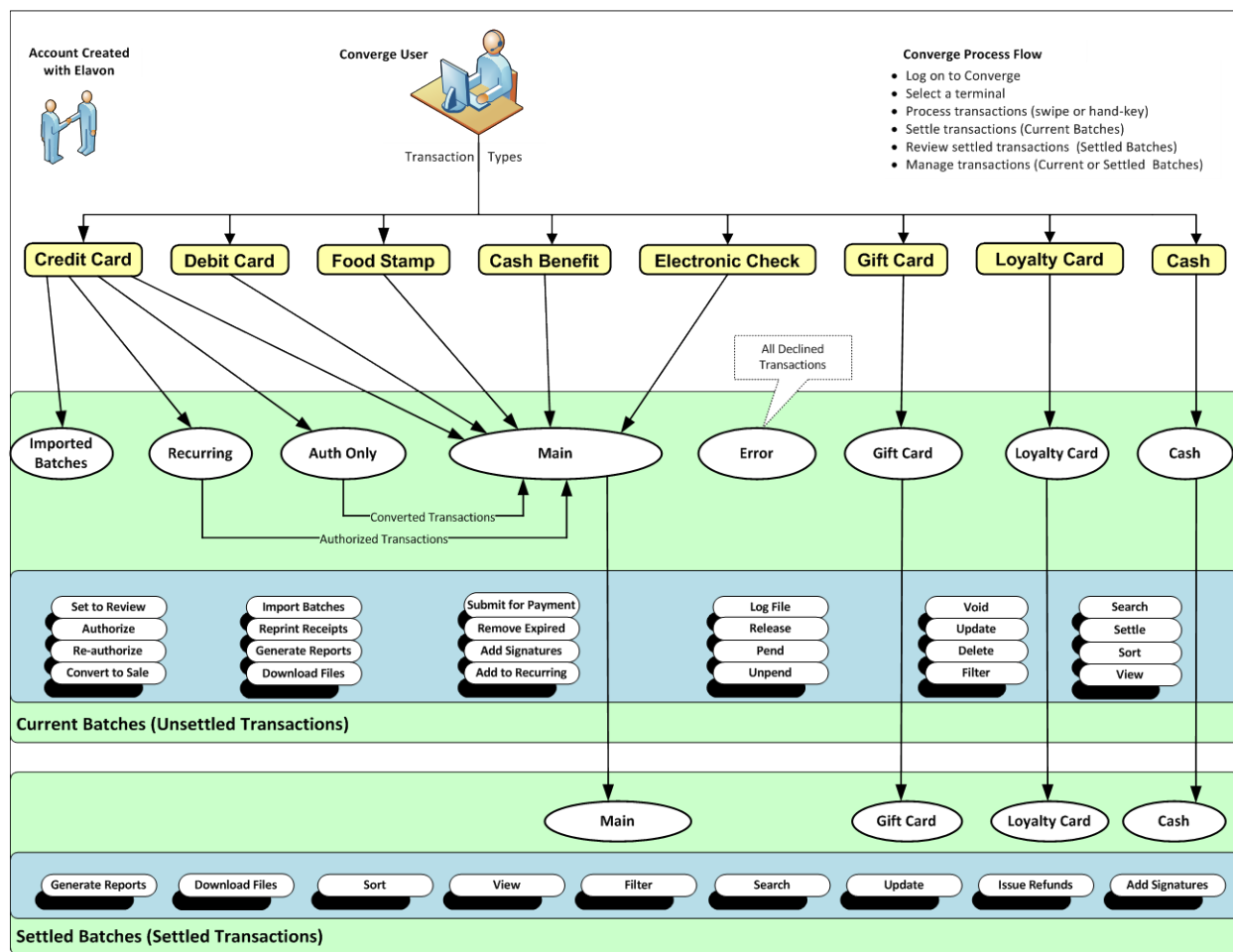
Chapter 1: Introduction

The Converge application is a secure server-based system that supports transaction processing (authorization and settlement) in real-time. The application allows use of a standard web-browser to process transactions as a cost-effective payment solution.

The information needed to process the transactions is sent over a secure, encrypted Internet connection. At its basic level, the terminal submits a customer's transaction information to the Converge server. The Converge server connects with the network for payment authorization and, if the sale is authorized, the program prints or returns a receipt for the customer. Email messages to confirm the order can be sent to customers and the merchant as notification of a new sale. Elavon settles the transaction and deposits the funds into your bank account. Transactions are automatically stored so they can be referred to at a later date.

Converge can:

- Take payments quickly and securely anywhere, anytime – without major investment of money or effort.
- Accommodate organizations of any size, in any business segment.
- Accept a full range of payment types and card brands.
- Process transactions in physical face-to-face, mail order/telephone order (MOTO) or e-Commerce environments.
- Support businesses that accept tips.
- Capture signatures during and after transaction processing (open and settled).
- Easily handle recurring and installment payments.
- Tokenize and store customers' sensitive payment information, simplifying PCI-DSS compliance.
- Support encryption with keyed, swiped, chip, and contactless/NFC transactions.
- Process chip transactions with an EMV enabled device.
- Protect financial data and ensure compliance with the latest industry security standards and regulations.



Features

The following categories describe the main features of Converge.

Versatile and Flexible

Converge is a very versatile and flexible payment solution with the ability to:

- Support card present processing for retail and service (tip) environments, card-not-present processing for MOTO environments, and Electronic Commerce Indicators (ECI) for consumer-initiated transactions on the Internet.
- Offer the ability to swipe, hand-key, contactless, or chip read (EMV) transactions as well as multi-entry and batch import.
- Set up multiple users with unique login information under one Converge ID. This feature allows you to grant or restrict access levels for security and accountability, and permits multiple users to work simultaneously.
- Support the capturing of tips for businesses such as bars, beauty and barber salons, health and beauty spas, and restaurants.

- Offer Fanfare loyalty program to allow merchants to accept and take advantage of promotional cards payment, for example, discount or percentage off goods or services.
- Offer bill payment capabilities through ECheck ACH for Internet, Telephone, and Back-offices for single, recurring, and preapproved payment.
- Accept: Credit Card, PIN-Based Debit Card, Electronic Benefit Transactions (Food Stamp and Cash Benefits), Electronic Check, Cash Tender, Loyalty, and Electronic Gift Cards as well as recurring and installment transactions.
- Offer a wide variety of card types including Visa®, JCB®, Discover®, MasterCard®, American Express®, Diners Club®, UnionPay® and local debit brands based home and abroad.
- Provide businesses an easy and affordable solution to grow revenue by servicing to international clientele and expanding into new geographies using Multi-Currency and Dynamic Currency offerings. Capture signature for transactions processed in the user interface with a certified signature capture device.
- Offer the merchant more payment options using the virtual terminal, integrated solution, or Converge Mobile application.
- Provide payment flexibility by offering merchants the ability to store customer information for repeat purchases or recurring payments.
- Offer MasterPass as a service that enables consumers to checkout on a merchant Web site using any MasterPass-connected wallet (Canadian merchants).
- Offer Account Updater to prevent disruption of recurring payments, which improves customer satisfaction by reducing authorization declines.
- Provide a detailed 12-month history with easy-to-use tools to identify trends and analyze transactions over time.
- Allow smaller businesses to leverage existing PCs to handle all their accounting, inventory management, and payment processing needs.
- Provide software upgrades as part of the hosted service.

Powerful and Secure Data Management

Converge provides powerful and secure data management with the following features:

- Fully-hosted solution minimizes security liability and ensures card association regulations and standards are met.
- Buy Button functionality for secure processing of e-Commerce transactions.
- Tokenization by providing returning customers the convenience of not having to re-enter their personal data every time they make a purchase.
- End-to-End Encryption helping to protect cardholder data, at rest and in transit for face-to-face environments using MagTek® secure card readers.
- 3D Secure Authentication reducing risk of chargebacks and offering maximum security for e-Commerce businesses.

- Fraud prevention rules can be established for e-Commerce transactions that fall outside of normal processing. Examples: decline transactions based on card number, cardholder IP, email address, or other criteria.
- Business rules can be established for e-Commerce transactions that fall outside of normal business parameters. Examples: flag transactions by type, value, or other criteria (those that need further review can be pended).
- The number of computers that uses Converge can be limited and so can those persons who will have access.
- Comma separated value (CSV) data can be exported into other applications by further analysis or tracking.
- The latest SSL certificate encryption technologies are employed to ensure transactions are processed in a safe and secure manner.
- Converge can be easily configured to ensure user access to appropriate data and reports.

Efficient and Cost-Effective

Converge leverages existing PCs and Internet connections and eliminates the expense to invest in dedicated payment terminals and telephone lines. Transactions are processed in as little as 3 seconds over a high-speed connection. Authorizations can be processed at the time of the sale or submitted for settlement at a later date, without re-keying the transaction data, for example: MOTO or delayed delivery environments.

Reliable and Easy to Use

Converge provides quick and easy access from any web-browser that uses a secure login and does not require hardware specifications, network infrastructure or software installation. Instant assistance is also provided when needed by means of screen-sensitive Help.

Converge Options

With Converge, you have a number of options available to you, including:

- Transaction options
- Market-specific options
- Payment options
- Processing options
- Reporting options
- Account options
- Customization options
- Peripherals options

Transaction Options

The following table describes what Converge supports for transaction options.

What Converge Supports	Description
Single Transactions	Keying and submittal for authorization of a single hand-keyed, swiped, contactless, or chip transaction.
Multi-Entry Transactions	Keying and submittal for authorization of multiple transactions.
Batch Import Transactions	Supports the ability to process a comma delimited or XML file of transactions.
HTTPS Authorization Interface	Features an SSL interface to process consumer-initiated transactions for payment integration using XML processxml.do or HTML process.do

Market-Specific Options

The following table describes what Converge supports for market-specific options.

What Converge Supports	Description
Market Segment Processing	Supports several market segments including: <ul style="list-style-type: none">• Internet• Retail• Service• Mail Order/Telephone Order
Travel Addendum	Allows merchants to send travel information such as departure and completion dates to the Merchant Airline Risk Management System (MARMS) to monitor risks associated with merchants that collect payments for future services or for bookings made in advance. In particular, airlines and travel/tour agencies.

Payment Options

The following table describes what Converge supports for payment options.

What Converge Supports	Description
Variety of Payments	Supports Credit, PIN Based Debit, Food Stamp, Cash Benefits, Gift, Loyalty, PINless Debit, Check, and Cash transactions.
Wallets	Supports MasterPass as a payment option at the merchant Web site (Canadian merchants).
Partial Authorization	Supports the ability of prepaid credit card transactions.

Processing Options

The following table describes what Converge supports for processing options.

What Converge Supports	Description
Recurring and Installment Billing	Allows you to setup automatic billing of credit cards and ACH ECheck at regular intervals (that is, monthly, quarterly, annually) on a continual basis or for a predetermined number of payments.
Tokenization	Allows you to store and manage customer credit cards and billing information (card on file) in the Card Manager and process transaction manually at a later time.
Account Updater	Allows you to set up your recurring batch with automatic updates, Converge will check periodically for the latest card information from the issuer and perform an update to the card information when necessary without the need for manual administration. This process ensures that the most updated information is on file and streamlines payments reducing authorization declines.
Dynamic Currency Conversion (DCC)	<p>With Elavon's DCC service, international Visa® and MasterCard® credit card purchases are converted instantly at the point of sale to the cardholder's home currency. To offer DCC, you must be registered and your terminal must be set up to process DCC transactions.</p> <p>DCC is an optional service that gives the cardholder the choice to process and accept the transaction in local or home currency. Rates are automatically updated daily, so merchants can take advantage of the most up-to-date exchange rates in the market. Elavon manages the entire conversion process.</p>
Multi-Currency Conversion (MCC)	Allows you to sell your products and services in a variety of currencies and receive funding in your home currency.
Purchasing Card/Business Card Capable	Prompts for customer code and sales tax information to meet Level Two processing requirements.
CVV2 Processing	Meets current Card Verification Value 2 (CVV2, CVC2, and CID) requirements for Card-Not-Present (CNP) transactions.
Address Verification (AVS) Processing	Used to comply with Visa® and MasterCard® direct marketing requirements and to minimize fraudulent Internet and mail order/telephone order transactions.

Reporting Options

The following table describes what Converge supports for reporting options.

What Converge Supports	Description
Batch Download Options	Supports an XML, tab- or comma-delimited download for currently open and previously settled batches.
Export Script	Allows merchants to export payment transactions in real-time. Payment transactions are returned to a merchant's Web site for reasons such as inventory control, sales analysis or database maintenance

Account Options

The following table describes what Converge supports for account options.

What Converge Supports	Description
Multi-Merchant Processing	Allows for the processing of multiple merchant accounts.
Enhanced User Rights	Allows you to manage each user's access to select features within the application. Access can be granted or denied at an individual user level.

Customization Options

The following table describes what Converge supports for customization options.

What Converge Supports	Description
Multiple-User Capable	Allows you to set up hierarchical user structure for increased user security.
Customizable Payment Forms	Allows for online payment and Virtual Terminal payment forms to be configured for unique business needs.
Auto Settlement	Allows for programs to be configured to automatically settle unpended transactions.
Custom Decline Messages	Allows for non-approved authorization responses to be customized for consumer-initiated transactions.
User-Defined Fields	Supports additional user-defined transaction prompts on all payment forms.
Dynamic DBA	Allows you to control the descriptor on customer's credit card statements. You can specify, on a per transaction basis, wording that is more recognizable to the customer.

Peripherals Options

The following table describes what Converge supports for peripheral device options.

What Converge Supports	Description
Printing Peripheral	Converge supports printing receipts using the following devices: <ul style="list-style-type: none">Serial Printer Epson T20 Thermal Printer using the DeviceAssistantStar Micronics TSP650II Thermal Printer using ConnectConvergeParallel printer using any connected network printer
Swipe Only Devices	Converge supports the following swipe devices: <ul style="list-style-type: none">MagTek Mini Wedge USB (Keyboard Emulation) (traditional)MagTek MagneSafe Mini Wedge USB (Keyboard Emulation) (end-to-end encryption)
PIN Entry Devices	<ul style="list-style-type: none">PIN Pad 1000SE (US Only): PINEquinox L5200 signature capture (US Only): Swipe, PIN, and SignatureIngenico iPP320 PIN Pad – EMV enabled for CanadaIngenico iSC Touch 250: Key, Swipe, Contactless, PIN, Chip and Signature – EMV enabled for U.S.Ingenico iCMP: Key, Swipe, Contactless, PIN, Chip and Signature – EMV enabled for U.S.
Check Scanners	<ul style="list-style-type: none">RDM 7111 with MSRMagTek MICR Imager with MSR

Note: In order to support peripheral devices with Converge, you must download either ConvergeConnect or DeviceAssistant depending on the device you wish to use. Refer to the *Converge Peripheral Device Installation and Setup Guide* for more information on how to install and configure your peripheral devices.

Security Features

Various security features are built into Converge and include:

- System timeouts after inactivity
- Restricted system logins
- Enhanced Logins with IP Recognition
- Password requirements

System Timeouts

Converge allows a session to be inactive for up to 15 minutes. If you are logged in and your session is inactive for 15 minutes, the system automatically logs you out and returns you to the Converge **User Login** page.

System Logins

Converge only allows one concurrent login per user. If you are logged on from one browser and you access your user account from another browser, the system logs you out of the first browser.

Converge allows up to five (5) login attempts before locking the user out of the system. Once locked, users are redirected to the **Security Questions** page in order to reset their passwords. The user can also use the **Forgot Password** link located on the login page. If you still need assistance contact your system administrator for login or password reset.

Enhanced Logins with IP Recognition

The Converge login page has been enhanced with additional security to recognize where you are logging into the application. With this release, you will be asked to answer your security questions when trying to log on from a different, unrecognized computer or device. Because only you know the answer to your security questions, Converge can confirm your identity and protect you from a fraudulent login.

Criminals today work hard to steal merchant credentials. Converge proactively protects merchants while doing online transactions with us. This enhanced logon helps us safeguard your information.

If an unauthorized person tries to log on using your credentials, we won't recognize the computer he or she is using, so we will ask that person to answer the security questions that you created when you initially setup your Converge account. Because only you know the answers to the security questions, the individual will not be able to log on.

When you initially set up your Converge account, you create a password and answer a series of security questions for account verification. Converge will save a list of safe devices associated to you so the computer is recognized for use in the future. If you log on from a unrecognized device, you will be prompted to answer one of your security questions from the list you created when you set up your account. Converge has no limit to how many different computers you can use to log on to your account.

Password Requirements

To use Converge, you must meet the following password requirements:

- Passwords are case sensitive (the system differentiates between upper- and lower-case characters)
- Passwords must be a minimum of eight (8) characters long and a maximum of sixty-four (64) characters long
- Passwords must contain the following:
 - At least one lower-case letter
 - At least one upper-case letter
 - At least one number
 - At least one special character
- Passwords must be changed at a minimum of every 90 days
- You cannot reuse any of your previous 13 passwords

Email Notifications

Email notifications will be sent in the following instances:

- Welcome email when account is set up
- Email notification when you change email
- Email notification when you change your security questions
- Email notification when you change your password

Fraud Protection Features

Various fraud protection features are built into Converge and include:

- Referrer URLs
- Fraud Prevention Rules
- Business Rules
- 3D Secure Authentication (Verified by Visa™ and MasterCard SecureCode™)

Referrer URLs

Setting up HTTP referrers in the terminal tells Converge to accept transactions from an approved list of Web sites. Although it requires more work to implement, this action helps to prevent fraudulent users from submitting transactions from a different source other than your Web sites.

Every Gateway transaction captures the URL of the Web site from which the order originated. This is called the **Referrer URL** and is used to ensure that transactions processed through the merchant account originated from the Web sites specified. For example, if your application is set up to accept payments for products and services from www.mywebsite.com, Converge's security system automatically blocks any payment requests that come from another Web address. Refer to the **To Configure Your HTTP Options** section in the *Converge System Administration Guide* for information about how to set up referrer URLs.

Fraud Prevention Rules

Fraud prevention rules are customizable set of rules that allow you to build constraints to match your business needs and control how you handle transactions that include the ability to approve or decline transactions or return an error. These rules can serve as an important tool to help you to fight, manage and prevent suspicious and costly fraudulent activities. Refer to the **Setting Up Fraud Prevention Rules** section in the *Converge System Administration Guide* for information about how to set up your fraud prevention rules.

Converge allows you to setup the following fraud prevention rules on terminals:

- Auto Pend Filter
- Merchant IP Address Filter
- Mobile Payment Filter
- IP Address Filter
 - Individual/Ranges Filter
 - Country IP Address Filter
- Country Filter
 - Billing Country Filter
 - Shipping Country Filter
- IP Address & Country Mismatch Filter
 - IP Address & Billing Country Mismatch Filter
 - IP Address & Shipping Country Mismatch Filter
- Email Address Filter
- Card Number Filter

- Transaction Velocity Filter
 - Hourly Transaction Velocity Filter
 - Daily Transaction Velocity Filter
 - IP Address Velocity Filter
- Email Domain Filter
- Transaction Timeout Filter

Notes:

- Rules are only triggered through integration and do not apply to any transaction initiated from the user interface (Virtual Terminal).
- It is recommended that you get familiar with the capabilities of each of these filters and monitor your processing trends to determine which ones work best for your business needs.
- For terminals that are set up with more than one of the above fraud prevention rules, Converge executes these rules in the order presented before 3D Secure.

- **Auto Pend Filter:**

Enables you to designate which transaction types you want to set to **Pend**. You can choose to pend **Credit Card Sale**, **Credit Card Auth Only**, **Credit Card Force**, or **Credit Card Returns**. If you use this filter and receive approved transactions, they are automatically pending when entered through the Converge integration. You must log on to the application to release those transactions from the **Pend** state. Pending transactions cannot be settled until they are unpended.

- **Merchant IP Address Filter**

Enables you to designate and maintain a list of IP addresses from which you allow transactions to originate. If you use this filter and receive transactions from an IP address that is not in your allowed list, the transactions will be declined.

- **Mobile Payment Filter**

Enables you to designate and maintain a list of mobile devices from which you allow transactions to originate based on the mobile identification numbers. If you use this filter and receive transactions from a mobile device that is not in your allowed list, the transactions will be declined.

- **IP Address Filter**

Enables you to designate and maintain a list of IP addresses of cardholders from which you do not allow transactions to originate. If you use this filter and receive transactions from an IP address that is in your blocked list, the transactions will be declined.

- **Billing Country Filter**

Enables you to designate and maintain a list of billing countries from which you do not allow transactions to originate. If you use this filter and receive transactions from a billing country that is in your blocked list, the transactions will be declined.

- **Shipping Country Filter**

Enables you to designate and maintain a list of shipping countries from which you do not allow transactions to be shipped to. If you use this filter and receive transactions where the shipping country is in your blocked list, the transactions will be declined.

- **IP Address & Billing Country Mismatch Filter**

Enables you to designate and maintain a list of billing countries and compare the transaction's originating IP address with the billing country provided. This helps to determine if the transaction was placed in the country in which it originated. If you use this filter and receive transactions where the billing country does not match the IP address for those countries you have specified in the list, the transactions will be declined.

- **IP Address & Shipping Country Mismatch Filter**

Enables you to designate and maintain a list of shipping countries and compare the transaction's originating IP address with the shipping country provided. This helps to determine if the transaction was placed in the country in which the order will be shipped. If you use this filter and receive transactions where the shipping country does not match the IP address for those countries you have specified in the list, the transactions will be declined.

- **Email Address Filter**

Enables you to designate and maintain a list of email addresses of cardholders from which you do not accept transactions. If you use this filter and receive transactions from an email address that is in your blocked list, the transactions will be declined.

- **Card Number Filter**

Enables you to designate and maintain a list of card numbers of cardholders from whom you do not accept transactions. If you use this filter and receive transactions from a card number that is in your blocked list, the transactions will be declined.

- **Hourly Transaction Velocity Filter**

Enables you to specify a threshold for the number of transactions allowed for a terminal within 60 minutes. All transactions received that exceeds the threshold will be declined.

- **Daily Transaction Velocity Filter**

Enables you to specify a threshold for the number of transactions allowed for a terminal within 24 hours. All transactions received that exceeds the threshold will be declined.

- **IP Address Velocity Filter**

Allows you to specify a threshold for the number of transactions allowed for a terminal from the same cardholders' IP address. All transactions received that exceeds the threshold will be declined.

- **Email Domain Filter**

Enables you to validate that the email address entered by cardholders on transactions is a valid domain. If you use this filter and receive transactions from an email address with an invalid domain, an error will be returned.

- **Transaction Timeout Filter**

Enables you to specify a time limit in minutes for a single transaction. If the transaction exceeds the time allowed for processing, it will be declined.

Business Rules

Business Rules is a customizable tool that allows you to build constraints to match your business needs and control how you handle transactions that include the ability to approve, decline or set transactions to a status of **Pend** or **Review**. These rules can serve as an important tool to help you fight, manage and prevent suspicious and costly fraudulent activities.

Business Rules Types

There are two types of business rules in Converge:

- Pre-processing business rules
- Post-processing business rules

Pre-Processing Business Rules

These rules are applied to transactions before they are sent for authorization and will be declined if the criteria defined are not met. They include:

- Ship to Postal Code
- Bill to Postal Code
- Tran Amount
- Return Amount
- Duplicate Checking

Post-Processing Business Rules

These rules are applied to transactions after they are sent for authorization. You can make a decision to **Set to Pend** or **Set to Review** these transactions. They include:

- Ship to Postal Code
- Bill to Postal Code
- Tran Amount
- Return Amount
- AVS Response
- CVV response
- Settlement

Additionally, Converge offers enhanced AVS and CVV post-processing to handle filters, where you can make a decision to decline previously authorized transactions that return specific AVS and CVV response codes. Refer to the **Response Codes** section in the *Converge Transaction Processing Guide* for a complete list of AVS and CVV response codes.

Note: Converge initiates a reversal on the merchant's behalf for Visa®, MasterCard®, and Discover® credit card transactions that are set to decline based on the AVS or CVV rules. The reversal attempts to cancel an authorization and restore the cardholders open to buy, as the card is authorized at the cardholder's issuing bank and then declined due to the AVS or CVV rule settings. If the reversal is not successful or delayed, your customers could mistake this authorization for a charge as the authorization reduces their available limit. However, a transaction declined for AVS or CVV will not settle and your customer will not be charged.

Business Rules Filters

The following lists the Business Rules Filters available to you within Converge.

- **Ship to Postal Code:**
Allows you to set up a rule based on a transaction's postal code. This rule is valid only when the comparison value is **Bill to Postal Code** or a numeric or alphanumeric value.

Example:
You can set up a **Ship to Postal Code** rule and specify that transactions should decline if the postal code value is equal to 99999. If a consumer enters this value as a postal code in the payment form, the transaction will be automatically declined.

- **Bill to Postal Code:**

Allows you to set up a rule based on a transaction's **Bill to Postal Code**. This rule is valid only when the comparison value is **Ship to Postal Code** or a numeric or alphanumeric value.

Example:

You can set up a **Bill to Postal Code** rule and specify that transactions should be set to **Pend** if the **Bill to Postal Code** value is not equal to **Ship to Postal Code**.

- **Tran Amount:**

Allows you to set up a transaction amount or threshold amount for which a rule should trigger a **Pend**, **Set to Review** or **Decline**. This rule applies to **Sale**, **Auth Only**, and **Force** transactions.

Example:

You can set up a **Tran Amount** rule and specify that transactions should be **Set to Review** if the transaction amount exceeds \$100.00.

- **Return Amount:**

Allows you to set up a refund threshold amount for which a rule should trigger a **Pend**, **Set to Review**, or **Decline**. This rule applies to **Refund** transactions.

Example:

You can set up a transaction to automatically decline if refund is greater than \$100.00.

- **AVS Response:**

Allows you to set up a rule based on the **Address Verification** response. AVS compares the billing address provided by your customer during the transaction to the address on file with the credit card issuer. This rule allows you to choose to **Pend**, **Set to Review**, or **Decline** a transaction that has returned a specific AVS response as defined in the rule. To implement AVS, you must collect the customer's billing address and ZIP code (Refer to the **AVS Response Codes** section in the *Converge Transaction Processing Guide* for a complete list of AVS response codes).

Example:

You can set up a transaction to **Set to Review** if the address passed in the authorization does not match the address at the bank.

- **CVV Response:**

Allows you to set up a rule based on the **Card Verification Value** response. This rule compares the CVV/CID value provided by the customer at the time of the authorization to the CVV value on file with the credit card issuer returned in the authorization response. This rule allows you to **Pend**, **Set to Review**, or **Decline** a transaction that has returned a specific CVV response as defined in the rule. To implement CVV, you must pass the CVV/CID value (Refer to the **CVV2 Response Codes** section in the *Converge Transaction Processing Guide* for a complete list of CVV response codes).

Example:

You can set up a transaction to **Pend** if the **Card Verification Value** does not match.

- **Settlement:**

Allows you to set up a rule based on the batch settlement response. This rule is defined to check to see if the settlement was successful.

Example:

User can receive an email notification if a batch settlement is successful or not.

Note: Refer to the **Setting Up Business Rules** section in the *Converge System Administration Guide* for information about how to set up your business rules.

- **Duplicate Checking:**

Allows a merchant to decline duplicate transactions before they are sent for authorization.

A transaction is considered duplicate based on the same **Account Number**, **Transaction Type** and **Transaction Amount** within the same open batch for all payment transaction types, as a minimum condition. In addition to those criteria, you can check for duplicate transactions based on **Invoice Number**, a **Required User Defined** field or a pre-defined timeframe in which to look for duplicate transactions and includes:

- 5 minutes
- 10 minutes
- 15 minutes
- 30 minutes
- 1 hour

Notes:

- The original transaction must be approved in the batch to trigger the duplicate rule. The rule is not triggered if Converge has not received the response from the original transaction.
 - The **Duplicate Checking** rule does not apply to transactions in a closed batch. For example: a merchant can send a transaction, settle the transaction and then re-send the same transaction. This is not considered a duplicate transaction.
-

3D Secure Authentication (Verified by Visa[®] and MasterCard[®] SecureCode[™])

3D Secure is a security tool that enables cardholders to authenticate their identity to their card issuer through the use of Visa's Verified by Visa[™] and MasterCard's SecureCode[™] services. 3D Secure adds another layer of security to cardholders by the prevention of fraudulent purchases in an e-Commerce environment. For our merchants, it reduces the number of unauthorized transactions. Converge users who process transactions in an integrated e-Commerce environment are able to take advantage of this functionality with no additional charge.

Cardholders who have a Visa[®] or MasterCard[®] from a participating Issuer are presented an additional window hosted by the Card Issuer. If cardholders have already established a password or private code for their credit card, they are prompted to enter that identifier to authenticate them before the transaction is submitted for authorization. If a cardholder has a participating credit card but has not yet established their password or private code, they are prompted to do so.

Note: Refer to the **To Set Up 3D Secure** section in the *Converge System Administration Guide* for information about how to set up 3D Secure.

Chapter 2: Getting Started

This chapter provides some basic information that you may need before you are able to use Converge. You will need to know how to:

- Ensure your computer meets the minimum system requirements
- Set up your Converge account
- Launch the application
- Log on to the application
- Reset your password
- Use the components of the Converge interface
- Seek assistance if necessary

System Requirements

To use Converge, you must meet the following minimum system requirements:

- Use supported Internet browsers
- Allow Converge to display pop-ups in the browser pop-up blockers

Supported Internet Browsers

Converge supports most Internet browsers. However, because so many variations of browsers exist in the market, Elavon cannot guarantee that all browsers and browser versions will work.

Notes:

- When using Converge with devices via the **DeviceAssistant** you must use Internet Explorer 8 and higher. ActiveX® controls support is required and must be enabled under Internet Explorer advanced settings.
 - When using Converge with devices via **ConvergeConnect** you can use either Internet Explorer (10 and higher) or Chrome.
 - When using Converge without any devices, most browsers are supported.
-

Browser Pop-up Blockers

Converge uses pop-up windows as part of the application. Use the following information for pop-up windows:

- You must set up your Internet browser to accept pop-ups before you use Converge to process transactions.
- You need to add the Converge site to the allowed sites in the pop-up blocker for your browser before you begin to use the application. The steps to do this vary and depend on which browser you use. Consult the **Help** for your browser to learn how to add the Converge site to the allowed sites.

Note: Pop-ups are small Internet browser windows that appear on top of the Web site that you are viewing.

Setting Up Converge Accounts

Before you can access Converge, you must have your account set up by Elavon's system administrators. If you have not already had your account created, contact the Elavon Merchant Activation Department at 1-866-451-4007, then follow prompts.

After your account is set up, you will receive a Welcome Email from Converge. This email contains useful information about how you can start using your account and process transactions using the Virtual Terminal, Mobile application, or the Converge API. This email also contains important information about your Converge account, such as:

- Account ID
- Profile Friendly Name
- Merchant Number (MID)
- Currency
- Important Links and Contact Phone Numbers

Notes:

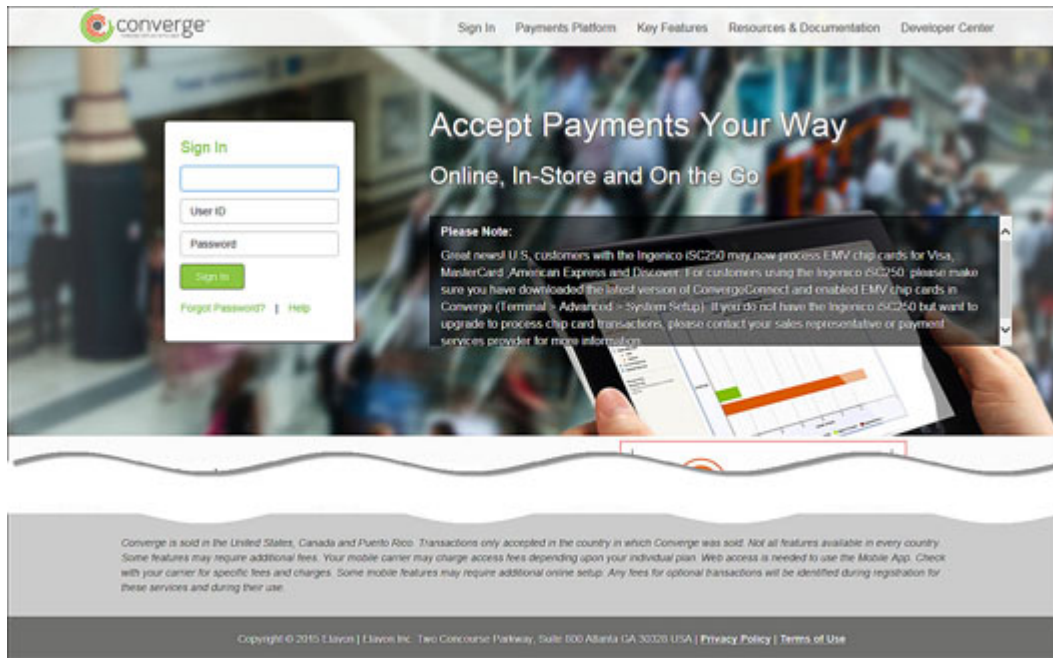
- This email should be kept for future reference.
 - The Welcome Email is automated and does not have reply capabilities. Therefore, if you need assistance with your accounts, you must contact our Software Technical Support at 1-800-377-3962, Option 2, then Option 2 (in Canada you are asked to choose either English or French for your language). If you have question about the activation or training, contact the Elavon Merchant Activation Department at 1-866-451-4007, then follow prompts.
-

Launching Converge

You can access Converge through your Internet-connected personal computer (PC).

Enter URL <https://www.convergepay.com> in your browser window.

The Converge **Launch** page appears.



The launch page contains:

- **Sign In**
Allows you to sign in to the application.
- **Alert Section**
Alert messages will appear next to the sign in section when the system updates or an important message needs to be communicated.
- **Converge Demonstration Video**
View the Converge demonstration video to gain a full understanding of all that is offered through our web-based, transaction processing system.
- **Payments Platform**
Describes the supported payment segments that allow you to expand your business.
- **Key Features**
Describes the payment methods and some of the advanced features.
- **Resources & Documentation**
The **Resources** side allows you access to useful links such as MerchantConnect to help you with your card processing needs.

The **Documentation** side allows you access to the latest releases of the Converge documentation.

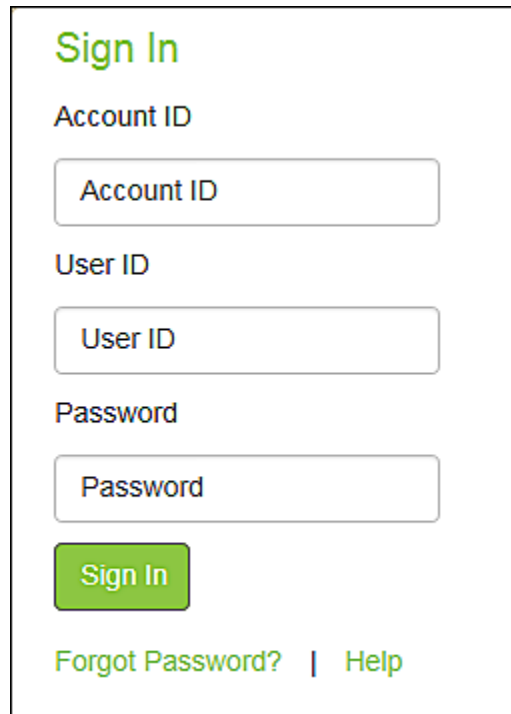
Signing In to Converge

Before you can sign in to Converge, you will need to have had an account set up for you. If you have not already done so, Refer to the **Setting Up Converge Accounts** section in the *Converge System Administration Guide* for more information.

Notes:

- If this is your first time to sign in, you will be prompted to reset your password. Refer to the [Resetting Your Initial Password](#) procedure for more information.
 - Username and passwords are case sensitive (the system differentiates between upper- and lower-case characters).
 - If the user is locked after too many failed attempts the user is redirected to the Security Questions screen. Refer to [Resetting Your Latest Password](#) for more information.
-

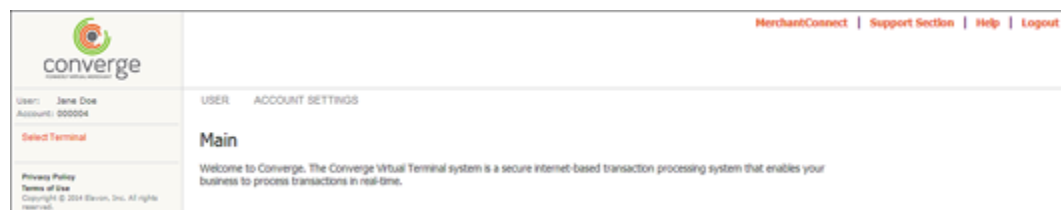
1. Enter your **Account ID**.
2. Enter your **User ID**.
3. Enter your **Password**.



The image shows a 'Sign In' form with a green title. It contains three input fields: 'Account ID', 'User ID', and 'Password'. Below the fields is a green 'Sign In' button. At the bottom, there are links for 'Forgot Password?' and 'Help'.

Refer to the [Password Requirements](#) section for more information about how to setup your password.

4. Click **Sign In** to continue to the Converge **Main** page.



The image shows the 'Main' page of the Converge system. The header includes the Converge logo and navigation links: 'MerchantConnect', 'Support Section', 'Help', and 'Logout'. The left sidebar contains user information (Jane Doe, Account: 000004), a 'Select Terminal' button, and links for 'Privacy Policy' and 'Terms of Use'. The main content area has tabs for 'USER' and 'ACCOUNT SETTINGS', with 'Main' selected. A welcome message states: 'Welcome to Converge. The Converge Virtual Terminal system is a secure internet-based transaction processing system that enables your business to process transactions in real-time.'

Resetting Your Initial Password

When you first access Converge, you must use the password assigned to you by Elavon's customer service. After you use that initial password to log on, you will be prompted to reset your password as shown below.

User Login

Your password has expired

Before you update your password, you must select three security questions and provide answers to them in the space provided below. Should you forget your password, these questions will enable you to reset your password without having to contact customer support.

Security Questions

Question1	Select	Answer	
Question2	Select	Answer	
Question3	Select	Answer	

1. Select your security question from the **Question1** list.

User Login

Your password has expired

Before you update your password, you must select three security questions and provide answers to them in the space provided below. Should you forget your password, these questions will enable you to reset your password without having to contact customer support.

Security Questions

Question1	Select	Answer	
Question2	Select	Answer	
Question3	Select	Answer	

Your selected question appears.

User Login

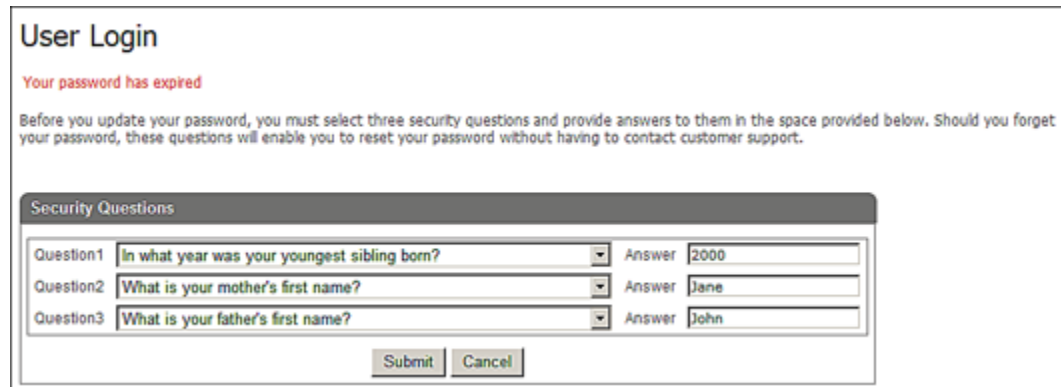
Your password has expired

Before you update your password, you must select three security questions and provide answers to them in the space provided below. Should you forget your password, these questions will enable you to reset your password without having to contact customer support.

Security Questions

Question1	In what year was your youngest sibling born?	Answer	
Question2	Select	Answer	
Question3	Select	Answer	

2. Enter your **Answer** to **Question1**.
3. Select your security question from the **Question2** list.
4. Enter your **Answer** to **Question2**.
5. Select your security question from the **Question3** list.
6. Enter your **Answer** to **Question3**.



User Login

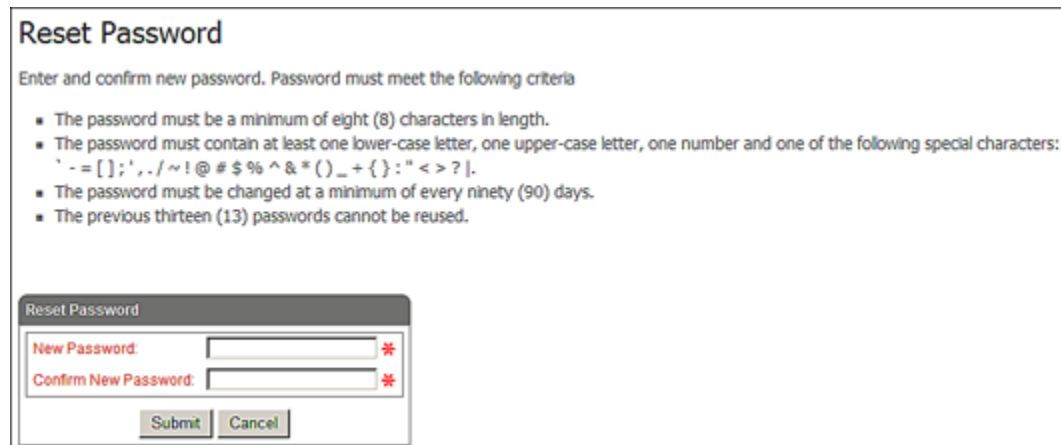
Your password has expired

Before you update your password, you must select three security questions and provide answers to them in the space provided below. Should you forget your password, these questions will enable you to reset your password without having to contact customer support.

Security Questions			
Question1	In what year was your youngest sibling born?	Answer	2000
Question2	What is your mother's first name?	Answer	Jane
Question3	What is your father's first name?	Answer	John

7. Click **Submit**.

The **Reset Password** screen displays.



Reset Password

Enter and confirm new password. Password must meet the following criteria

- The password must be a minimum of eight (8) characters in length.
- The password must contain at least one lower-case letter, one upper-case letter, one number and one of the following special characters: ` - = [] ; ' , . / ~ ! @ # \$ % ^ & * () _ + { } : " < > ? | .
- The password must be changed at a minimum of every ninety (90) days.
- The previous thirteen (13) passwords cannot be reused.

Reset Password	
New Password:	<input type="password"/>
Confirm New Password:	<input type="password"/>

8. Enter your **New Password**.
9. Enter your new password again in the **Confirm New Password** field.
10. Click **Submit**.

The Converge **Main** page displays.

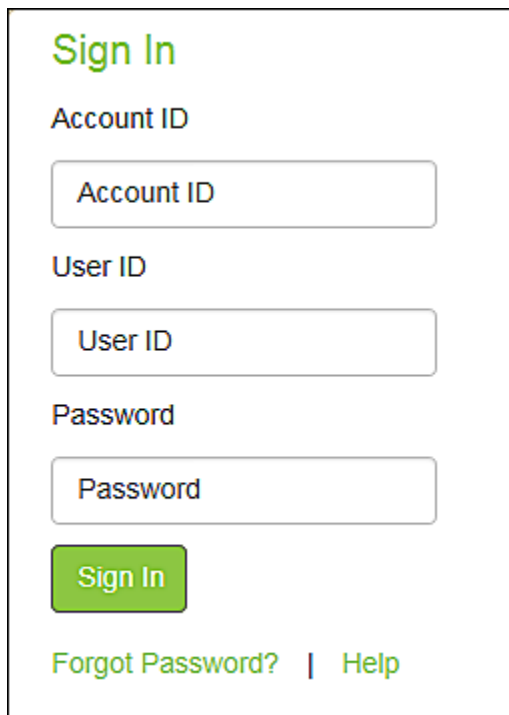


The screenshot shows the Converge Main page. At the top left is the Converge logo. To the right of the logo, there is a navigation bar with links: MerchantConnect, Support Section, Help, and Logout. Below the logo, there is a user profile section showing 'User: Jane Doe' and 'Account: 000004'. Below this is a 'Select Terminal' button. To the right of the user profile, there is a 'Main' heading and a welcome message: 'Welcome to Converge. The Converge Virtual Terminal system is a secure internet-based transaction processing system that enables your business to process transactions in real-time.' At the bottom left, there is a 'Privacy Policy' link and a 'Terms of Use' link. At the bottom right, there is a copyright notice: 'Copyright © 2014 Elavon, Inc. All rights reserved.'

Resetting Your Latest Password

You can reset your password within the Converge application without a call to Customer Support in the event you forget your password or your account is locked. You can find this option on the **User Sign In** screen.

Note: When your account is locked, you are automatically re-directed to the **Security Questions** screen.

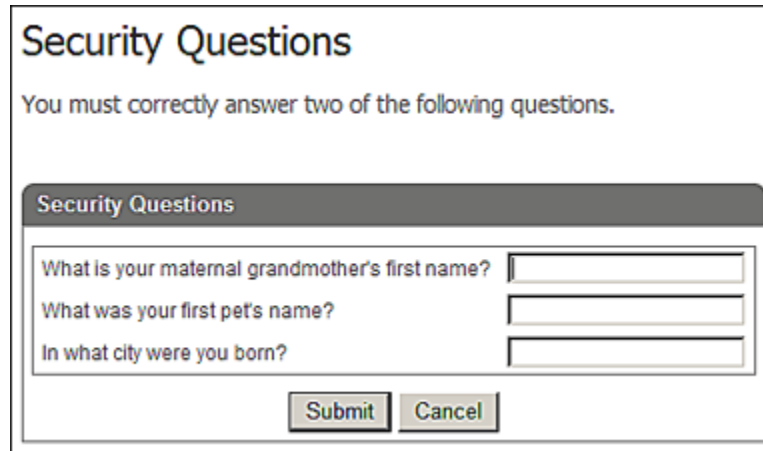


The screenshot shows the User Sign In screen. It has a green 'Sign In' heading. Below the heading are three input fields: 'Account ID', 'User ID', and 'Password'. Each field has a placeholder text matching its label. Below the input fields is a green 'Sign In' button. At the bottom, there are two links: 'Forgot Password?' and 'Help'.

To reset your password, follow the steps below:

1. Enter your **Account ID** and **User ID**
2. Click **Forgot Password?**.

The **Security Questions** screen displays.



Security Questions

You must correctly answer two of the following questions.

Security Questions

What is your maternal grandmother's first name?

What was your first pet's name?

In what city were you born?

3. Enter your answers to the three security questions.

Note: You must answer two of the three security questions correctly.

4. Click **Submit**.

The **Reset Password** screen displays and an email is sent to you with a security code.

5. Check your email.

Note: You must check the email we have on file. There is a 10 minute limit on the life span of a security code.

6. Click **Submit**.
7. Enter or copy and paste the security code provided to you in the email in the **Security Code** field.
8. Enter your **New Password**.
9. Confirm your password in the **Confirm New Password** field.
10. Click **Submit**.

The system successfully resets your password and the Converge **Main** screen displays.

Converge Interface

When you launch Converge the **Main** screen displays. Components of the Converge interface include:

- Support Menu Options
- Configuration Menu Options
- Transaction Menu Options



Support Menu Options

The **Support Menu Options** contains the following links:

- MerchantConnect
- Support Section
- Help
- Logout



The MerchantConnect Link

To access the MerchantConnect link, click **MerchantConnect**.



The **MerchantConnect Home** page opens in a new browser window. MerchantConnect is the online support and reporting tool that provides free access to your monthly statements, recent deposits, charge backs and retrieval requests, customer support and much more.



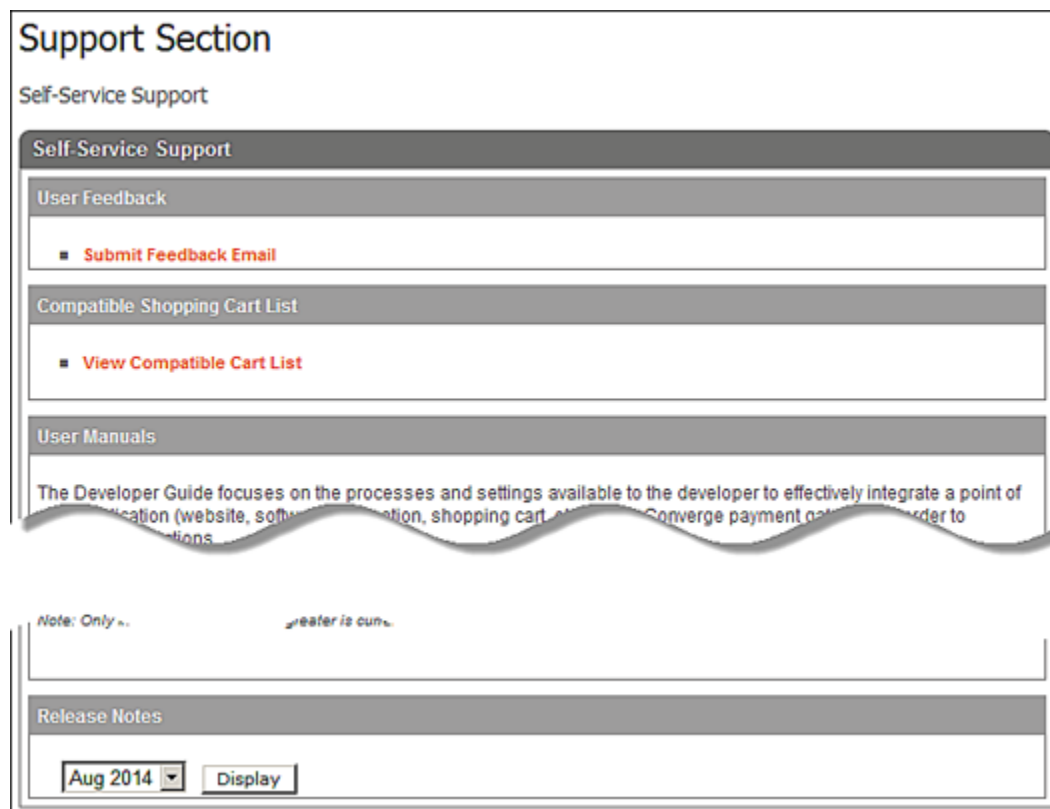
The Support Section Link

To access the **Support Section** link, click **Support Section**.



The **Support Section** screen displays. This screen gives you access to:

- Other links to submit feedback by email
- View compatible shopping cart information
- Download the developer guide, various user guides, and VM mobile guides
- Download the peripheral driver for the devices that are used with Converge
- Access release notes for the application



User Feedback

In the **User Feedback** section, the **Submit Feedback Email** link allows you to submit product feedback by email to the Converge support channel for assistance.

1. Click the **Submit Feedback Email** link.



The **Feedback Email** screen displays.

Feedback Email

Please share your feedback on any issues you find throughout the Converge Web site. The drop menu beside the Description of Feedback section will give you a choice of the issue that most closely describes the problem you are encountering.

Please give Converge the exact **URL (Web address)** of the page on which you encountered the issue. This can be done by copying the address from the window at the top of the opened Web page and pasting it in the **URL (Web address)** section window.

In the Feedback Message window, please give Converge a detailed description telling exactly how you found the issue. This will help Converge quickly correct the issue.

Note that all fields with an asterisk (*) are required.

Feedback Form

Description of Feedback: Feedback ▾

System Name:

URL (Web Address):

Your E-mail Address: *

Feedback Message (Max 2000 chars allowed): *

Submit Feedback Cancel

2. In the **Description of Feedback** list, select the category for the feedback request from the following:
 - **Feedback**
Used to make any additional comments or ask questions that relates to the Converge application
 - **Suggestion**
Used to make suggestions for improvement in the Converge application
 - **Issue**
Used to indicate any processing problems encountered within the Converge application
 - **Complaint**
Used to send an email complaint to our customer service team
3. Enter your company name in the **System Name** field.
4. Enter the Converge URL related to content of the email in the **URL (Web Address)** field.
5. Enter the email address for a response in the **Your Email Address** field.

Note: This is a required field.

6. Enter **Feedback Message**.

Be very descriptive and indicate the exact steps that led to the problem.

7. Click **Submit Feedback**.

The system sends an email to your email account, closes the **Feedback Email** screen, and displays a message.

Thank you for your comments. They have been submitted to the appropriate personnel.

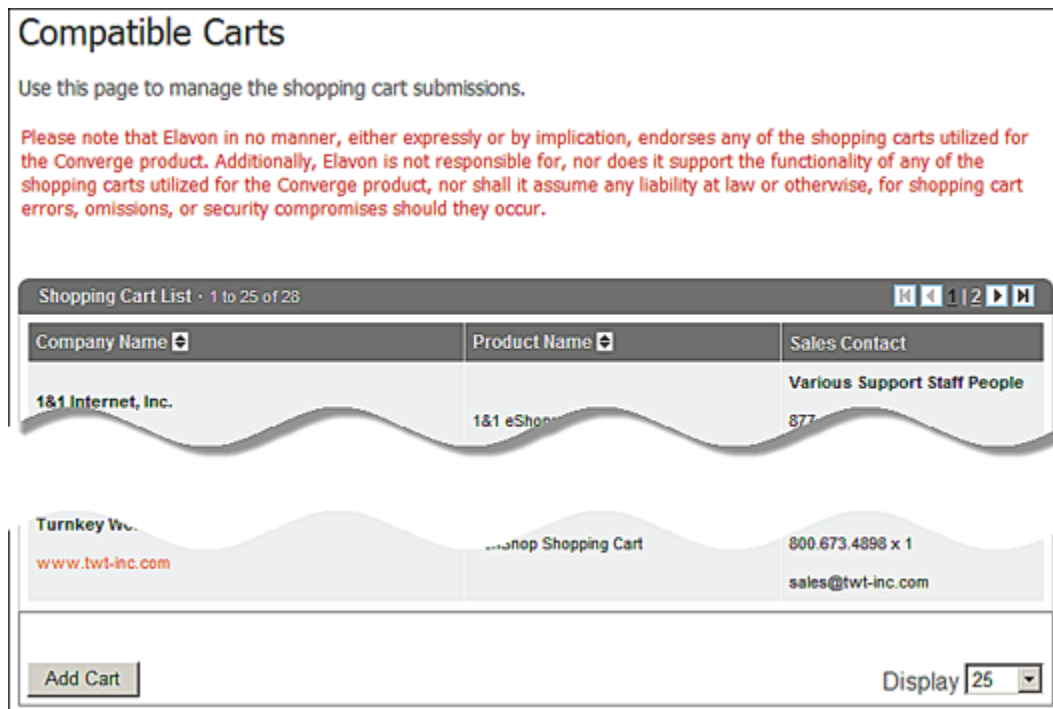
Compatible Shopping Cart List

Not all Internet shopping carts are compatible with Converge. The **View Compatible Cart List** link shows all of the shopping carts that are compatible for use with the Converge application.

1. Click the **View Compatible Cart List** link.



The **Compatible Carts** screen displays.



2. In the **Display** list, select the number of carts you want to be shown at a time from the following: 25, 50, 75, 100, 250, 500, 750 and 1000.

The screen refreshes to reflect the new selection.

3. Click **Add Cart** to submit a request to have an additional shopping cart added to the list.

The **Add cart** screen displays.

Add cart

Add the information from the shopping cart submission. Note that all fields with an asterisk (*) are required.

Request Information	
Company Name	<input type="text"/> *
Product Name	<input type="text"/> *
Web Site	<input type="text"/>
Business Contact Name	<input type="text"/> *
Business Contact Phone	<input type="text"/> *
Business Contact E-mail	<input type="text"/> *
Sales Contact Name	<input type="text"/>
Sales Contact Phone	<input type="text"/>
Sales Contact Email	<input type="text"/>

4. Enter the appropriate information and click **Add** to send the request to the Converge support channel for review.

Note: Elavon uses the **Business Contact** information to contact the shopping cart company and copies the **Sales Contact Information** in the **Compatible Carts List** for external contact information.

User Manuals

Click the *Download Developer Guide*, *Download Getting Started Guide*, *Download Administration Guide*, *Download Transaction Processing Guide*, *Download Chip and PIN (EMV) Addendum*, *Download VirtualMerchant Mobile 2 Guide*, *Download VirtualMerchant Mobile Classic Guide*, or the *Download Converge Peripheral Driver Guide* link to open the respective guides.

- **Developer Guide**

Provides information about how to integrate Converge into a personal site, with examples that show the functions of the Converge features.

- **User Guides**

Provides information about what you need to know before using Converge, the administrative functions of Converge, and the daily use of Converge.

- **VirtualMerchant Mobile Guides**

Provides information about the daily use of the VirtualMerchant Mobile application.

- **Peripheral Driver Guide**

Provides information about installation and configuration of your peripheral devices using ConvergeConnect or DeviceAssistant.

Note: You need Adobe Acrobat Reader to read the PDF formatted guides.

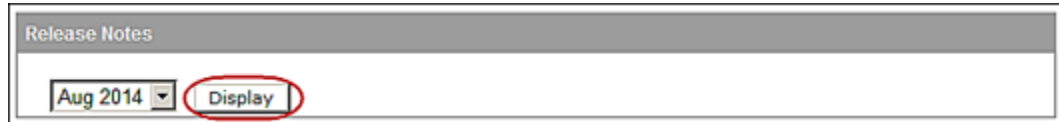
Peripheral Drivers

Use the **Download ConvergeConnect** or **Download DeviceAssistant** link to download the Windows-based peripheral driver application so that you can use supported peripheral devices to generate receipts, capture PIN information and check images. Refer to the *Converge Peripheral Device Installation and Setup Guide* for more information on how to install and configure your peripheral devices.

Release Notes

Release Notes provide links to supplementary documents that are delivered to the customer when bugs are fixed or enhancements are made to the Converge application.

1. On the drop-down list, choose the month of the release notes you want to view.



2. Click **Display** to open the pdf document of the selected month of release notes.

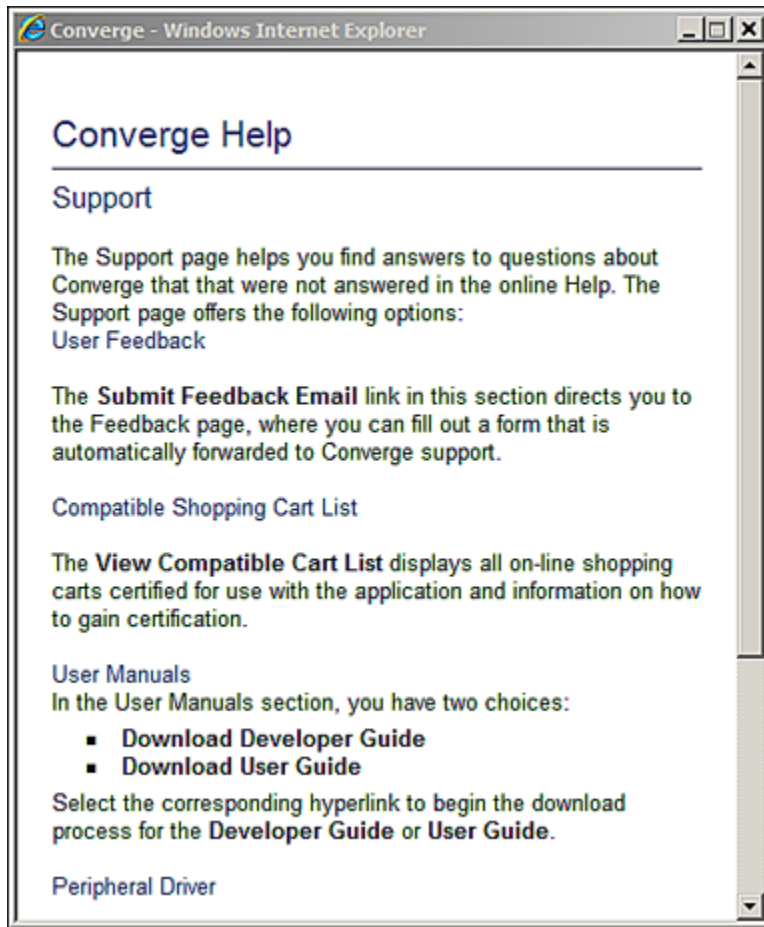
Note: You need Adobe Acrobat Reader to read the PDF formatted guides.

The Help Link

To access the Help link, click **Help**.



The **Converge Help** screen displays in a new browser window. This screen displays the help contents for the current section. Select the subject for which you require more information.



The Logout Link

To access the **Logout** link, click **Logout**.

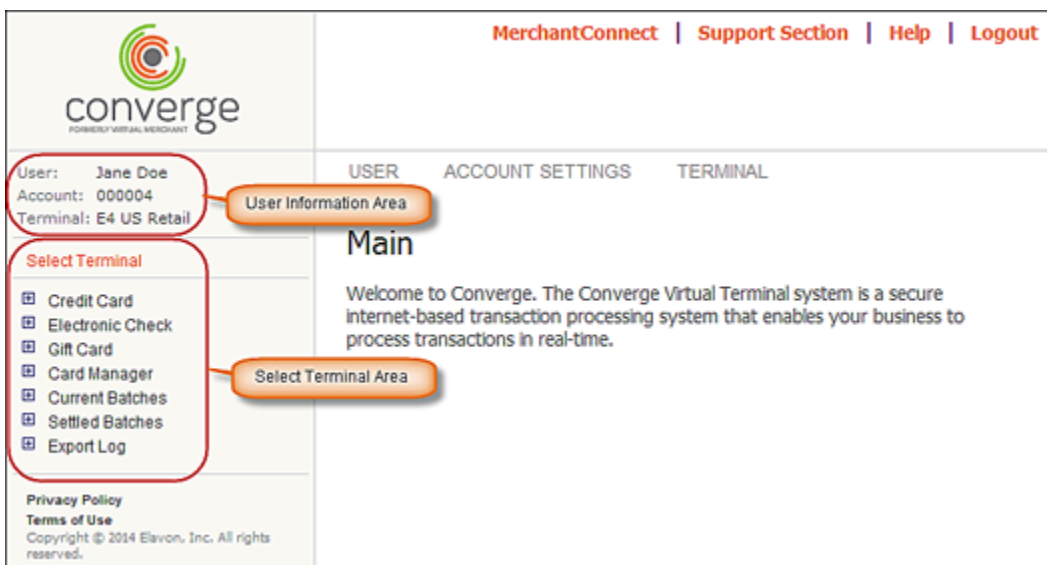


This option logs you out of the Converge application.

Transaction Menu Options

The **Transaction Menu Options** contains two areas:

- **User Information**
Displays your user ID, account number, and terminal ID
- **Select Terminal**
Contains a list of the rights to which you are assigned when you select a terminal



Getting Assistance from Elavon

You may occasionally require assistance from Customer Service for issues when you:

- Lose log in information for new customers such as account IDs, user IDs and temporary passwords
- Forget your current password
- Need assistance to use Converge

You can contact Elavon's Customer Service at 1-866-451-4007, then follow prompts.

Additional Resource Guides

For additional information regarding the integration, administration, or daily use of Converge and the Virtual Terminal refer to:

- Converge Administration Guide
- Converge Transaction Processing Guide
- Converge Chip and PIN (EMV) Transaction Processing Addendum
- Converge Peripheral Device Installation and Setup Guide
- Converge Developer Guide