Digital Certificate Quick Start Guide
for Extended Validation (EV) Certificates

February 2020
SecureTrust™ Extended Validation certificates offer the highest degree of validation. EV certificates enable secure connections, establish business identities, and assist in preventing fraud through a rigorous set of checks and validations. The SecureTrust Extended Validation Digital Certificate features 256-Bit encryption, and includes a $500,000 identification guarantee as well as free re-issues for the life of the Digital Certificate. Websites with an EV certificate instill consumer confidence in the identity of your web site.

To receive an EV certificate, you must order the certificate, submit the Subscriber Agreement, provide a certificate signing request, submit the Binding Authority Letter, and help SecureTrust validate your domain(s). Other validation documentation may be needed as well. This document explains how to perform each step in this process.

Order an Extended Validation Certificate

1. At https://certs.securetrust.com/, click the Customer Login link.
2. On the **SecureTrust Control Center Login** page, enter the username and password to your account.

![SecureTrust Control Center Login](image)

3. In the Control Center, use the accordion tabs on the left to open **Digital Certificates | Purchase New**. If you see the **Purchase New Certificates** page, you are already there.

![Purchase New Certificates](image)

4. On the **Purchase New Certificates** page, select a certificate and length of time and click its **Buy Now** button. The Customer Checkout page will be displayed next.
5. **On the Customer Checkout page:**

![Customer Checkout page](image)

- Enter the number of certificates that you want to purchase.
- Select how long those certificates should last.
- Add a promotional code if you have one and click **Apply**.
- Click **Continue >**.
6. On the second Customer Checkout page, your information automatically appears in the Customer Information fields.

Customer Checkout

My Order
1 SecureTrust Extended Validation - 1 Year
1 item
Subtotal: $299.00
Discount: $6.00
Tax: TBD
Total: $293.00

SecureTrust Digital Certificate Subscriber Agreement

Trustwave Subscriber Agreement for Digital Certificates
Ver. 16FEB17
IMPORTANT: PLEASE READ THIS AGREEMENT AND THE TRUSTWAVE CERTIFICATION PRACTICES STATEMENTS ("CPS") CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOUR ORGANIZATION. BY USING THE CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT AND THE CPS. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, E-MAIL US AT osd@trustwave.com OR CALL US AT 312-873-7500. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT APPLY FOR AND DO NOT CLICK ON "I ACCEPT" OR "I AGREE" BELOW, AND PROMPTLY EXIT THE BROWSER.

I agree with the terms and conditions of the Subscriber Agreement(s) and Trustwave®'s CPS.

a. In the SecureTrust™ Digital Certificate Subscriber Agreement section, mark the I agree with the terms and conditions check box.

b. Click Continue ->.
7. On the third **Customer Checkout** page:

**Customer Checkout**

![Order Details](image)

**Contact Information**
- **Name:** Jane Doe
- **Company:** Acme Inc.
- **Address:** 123 Main Street, Any Township, PA 15222, US
- **Email:** jdoe@example.com
- **Phone:** 412-555-1212

**Your Order**
- **Product:** 1 SecureTrust Extended Validation - 1 Year 1-year
  - **Subtotal:** $299.00
  - **Discount:** $0.00
  - **Tax:** $0.00
  - **Total:** $299.00

**Cardholder Details**
- **Required**
- **Cardholder’s Address**
- **Cardholder’s City**
- **Cardholder’s State**
- **Cardholder’s Zip/Postal Code**
- **Cardholder’s Country** United States

**Payment**

- **Visa**, **MasterCard**, **American Express**, **Discover**

- **Card Number**
- **Expiration Date:** 02 - February 2020
- **CVV2/CVC2/CID Code**

**My Order**

![SecureTrust Trusted Commercial](image)

- **Product:** 1 SecureTrust Extended Validation - 1 Year 1-year
  - **Subtotal:** $299.00
  - **Discount:** $0.00
  - **Tax:** $0.00
  - **Total:** $299.00

---

c. Double check your order details.
d. Fill out all of the **Cardholder Details** fields.
e. Enter **Payment** information.
f. Click **Purchase ->**.
8. On the **Thank you for your order!** page, click the **Control Center** link.

**Thank you for your order!**

Your Order

Product: 1 SecureTrust Extended Validation - 1 Year

Order Information

Order Total: $259.00
Order Date: Feb 26, 2020
Order #: 108962

You may now submit your Certificate Signing Request (CSR) via the **Control Center**. Submitting your CSR will begin the validation and issuance process. You will receive email confirmation of your order shortly, but you may also print this receipt.

Click here for help creating your CSR.

**Tip**: If you don’t have time to continue right now, feel free to take a break. You can return later to complete the process. Just go to [https://certs.securetrust.com/](https://certs.securetrust.com/) to log in.
Enter a CSR

SecureTrust requires a certificate signing request (CSR) in order to issue a certificate. While you are responsible for generating your CSR, SecureTrust offers instructions on how to do so on a variety of platforms. Once your CSR is ready, you can then submit it to SecureTrust.

1. Create a CSR for your certificate. Either go to https://certs.securetrust.com/support/create-csr.php or in the Control Center, open Support | CSR Creation for help on how to create one.

2. In the Control Center, use the accordion tabs on the left to open Digital Certificates | Pending Validation. If you see the Pending Certificates page, you are already there.

3. Click the Submit CSR button.

The Submit Certificate Signing Request form opens.
4. Select the certificate type that you want to submit from the **Product** drop-down list.

5. Copy and paste your CSR into the large text box.

6. Click **Parse CSR**.

7. If you want, on the second **Submit Certificate Signing Request** form add more domains.

8. Click **Submit**.
   SecureTrust will begin the setup for the domain validation process. This may take several minutes.
SecureTrust Digital Certificate
Quick Start Guide for Extended Validation (EV) Certificates - March 2, 2020

Validate Your Domains

Before SecureTrust can issue your certificate, it must ensure that you are authorized to have a certificate for all of the domains you included in your certificate request. This process is called domain validation. SecureTrust offers several validation methods: email, DNS, and domain beacon. In general, email validation is the most convenient method.

1. On the Domain Validation Methods form, select Email in the Validation Method drop down list for each domain. Some domains may be grouped together for efficiency.

   a. If email is not available, choose another method.

   Tip: The Validation Method Help link leads to information on these other methods.

2. Click Save Validation Method.

   a. If you use the email validation method, you will receive an email from ssisupport@trustwave.com asking you to validate the domain(s). To validate your domains via email, continue with step 3 below.

   b. If you are using one of the other validation methods, follow the instructions that you are given in Control Center and skip to step 5.
3. Click the **Approve/Decline Domain Validation** link in the email.  
A browser will open to the **Confirm Domain Validation** page.

![Confirm Domain Validation](image)

4. Click the large green **Approve** button.  
A confirmation page will appear.

5. Return to the Control Center’s **Pending Certificates** page and scroll down to the **Additional EV Steps** section.
6. Click **Subscriber Agreement** to open the **EV Subscriber Agreement** form.

![EV Subscriber Agreement](image)

a. Enter the names of the applicant and contract signer in the two fields.
b. Click **Accept & Continue** at the bottom of the form.

7. Click **Certificate Request Form** to open the **EV Certificate Request Form**.

![EV Certificate Request Form](image)

a. Fill out as many of the fields as possible. No field is required but the more information you provide, the easier it will be for SecureTrust to confirm your business’ identity.
b. **Tip**: Click the **Business Type Help** link to learn what the different types are.
c. Click **Save & Continue** at the bottom of the form.
8. Click **Binding Authority Letter** to open the **EV Binding Authority** form.

![Binding Authority Letter](image)

a. In the eight fields, enter the information of the person which SecureTrust can contact to complete validation. If the business type is an unincorporated entity, then SecureTrust will attempt to conduct a video conference to fulfill one of the validation requirements.

b. Click **Accept & Continue** at the bottom of the form.

If you return to the **Pending Certificates** page, you will find that SecureTrust is in the process of validating the domains and your organization for your certificate. SecureTrust Support follows these steps to validate your domain:

- Verify your organization’s legal existence and identity, typically through a public, government database. Additional steps may be required depending on business type.
- Verify your organization’s physical existence, typically through a trusted, third party database.
- Verify your organization’s operational existence, typically through a public, government database.
- Verify the Domain control.
- Verify that the communication method you supplied is reliable, typically telephone or email is verified through a trusted, third party database.
- Verify the name, title and authority of the Contract Signer, Certificate Approver, and Certificate Requestor; typically through a trusted, third party database or verified with a senior member of your organization.
- Verify all appropriate approvals for EV issuance, typically confirmed via email or telephone.

Please allow 24 hours for SecureTrust Support to reply with any additional validation requirements. Be patient as these validations often take some time to complete. Once done, your certificate can be issued.
Legal Notice

Copyright © 2020 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.
The most current version of this document may be obtained by contacting:

**Trustwave SSL Support:**
Phone: +1.866.775.2378
Email: sslsupport@trustwave.com

**Trademarks**

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

**About Trustwave®**

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit [https://www.trustwave.com](https://www.trustwave.com).