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

February 2023

VikingCloud™ 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 VikingCloud 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 VikingCloud validate your domain(s). Other validation documentation may be needed as well. This document explains how to perform each step in this process.
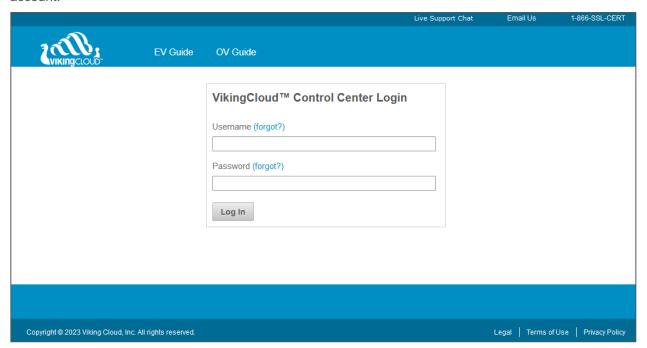
Contents

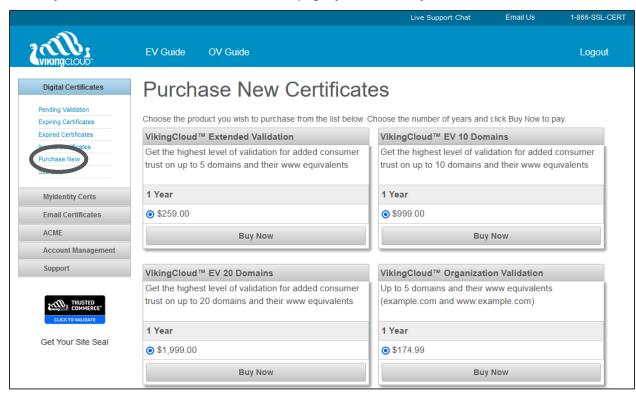# Order an Extended Validation Certificate

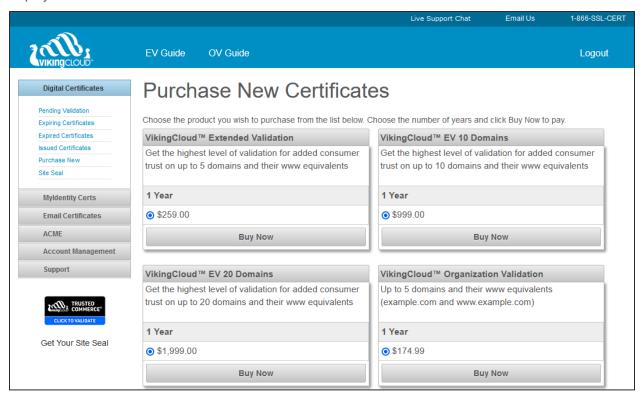1. At https://certs.securetrust.com/ , click the **Customer Login** link.

2. On the **VikingCloud Control Center Login** page, enter the username and password to your account.
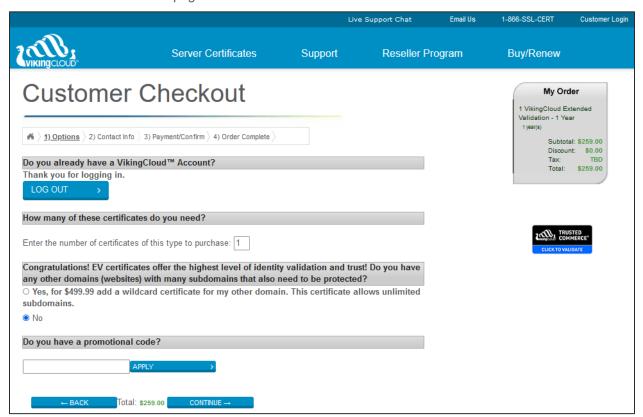

3. In the Control Center, use the accordion tabs on the left to open **Digital Certificates** | **Purchase New**. If you see the **Purchase New Certificates** page, you are already there.

4. On the **Purchase New Certificates** page, select the EV certificate with the correct number of domains you wish to use and click its **Buy Now** button. The Customer Checkout page will be displayed next.
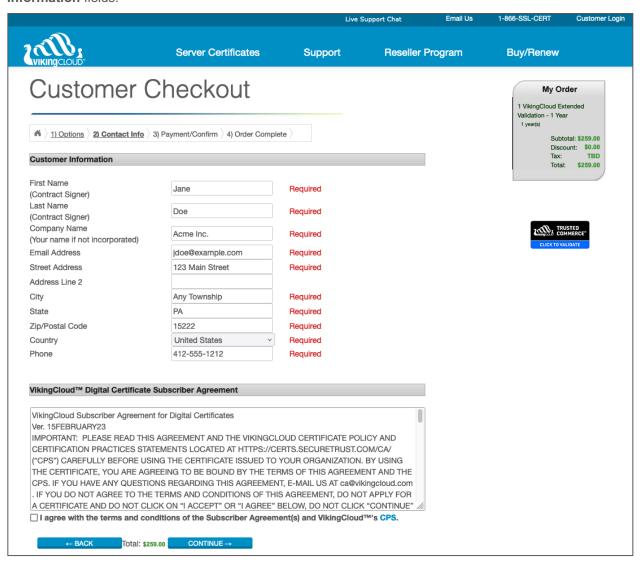
5. On the Customer Checkout page:

a. Enter the number of certificates that you want to purchase. (Defaults to 1).

b. Select **Yes** if you would also like purchase an OV Wildcard certificate. (Defaults to No).

c. Add a promotional code if you have one and click **Apply**.
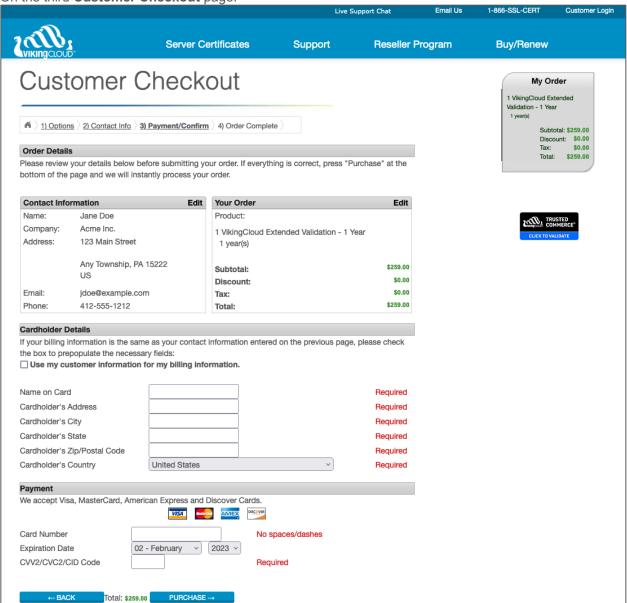
d. Click **Continue**.

Tip: If you make changes to your order, your order will be updated in the My Order panel on the top right. Your total will also be updated between the Back and Continue buttons.

6. On the second **Customer Checkout** page, your information automatically appears in the **Customer Information** fields.
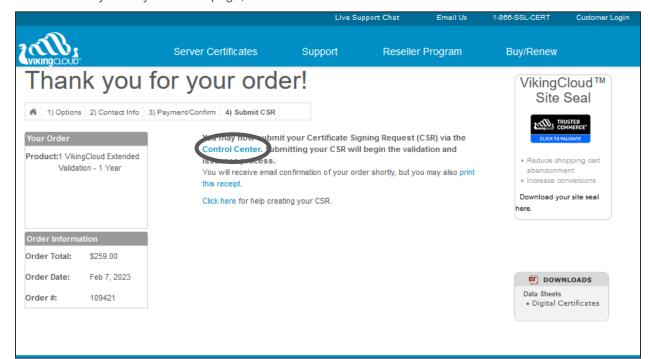

a. In the **VikingCloud™ Digital Certificate Subscriber Agreement** section, mark the **I agree with the terms and conditions** check box.

b. Click **Continue**.

7. On the third **Customer Checkout** page:

a. Double check your order details.

b. Fill out all of the **Cardholder Details** fields.

c. Enter **Payment** information.

d. Click **Purchase**.

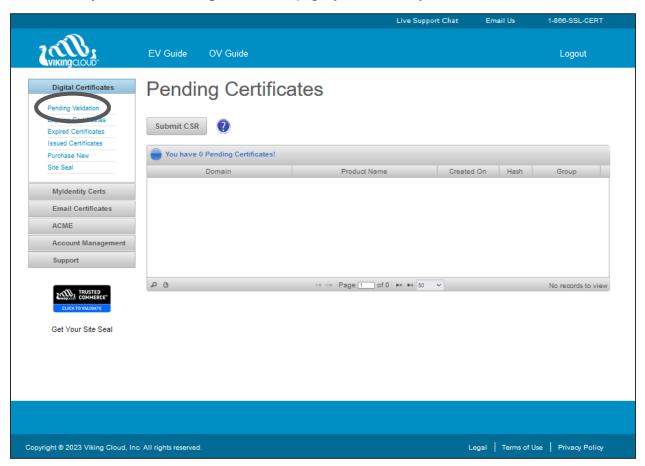8. On the Thank you for your order! page, click the Control Center link.

Tip: If you don't have time to continue right now, you can return later to complete the process. Just go to https://certs.securetrust.com/ to log in.
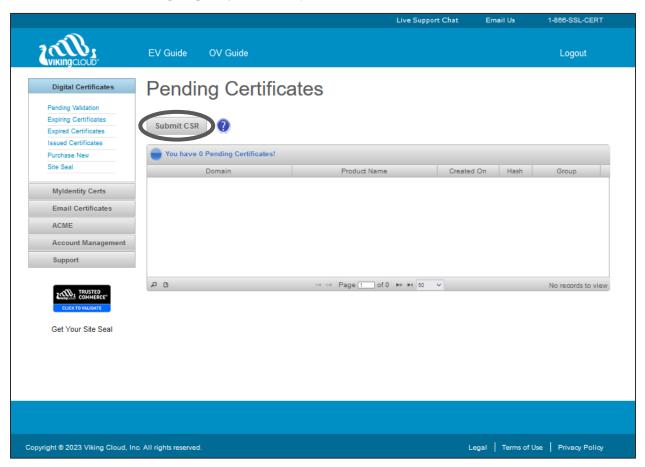
Enter a CSR

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

1. 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.
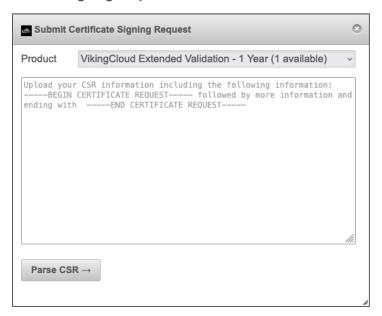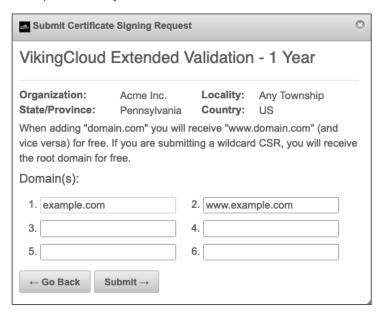
2. Click the **Submit CSR** button.

   The **Submit Certificate Signing Request** form opens.

3. On the **Submit Certificate Signing Request Form:**

a. Select the certificate type that you want to submit from the **Product** drop-down list.

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

c. Click **Parse CSR**.

4. Review the information pulled from your CSR.

Tip: The system displays the number of domains available for the certificate type selected. If you want to include additional domain(s), you can submit them in the available textbox fields.
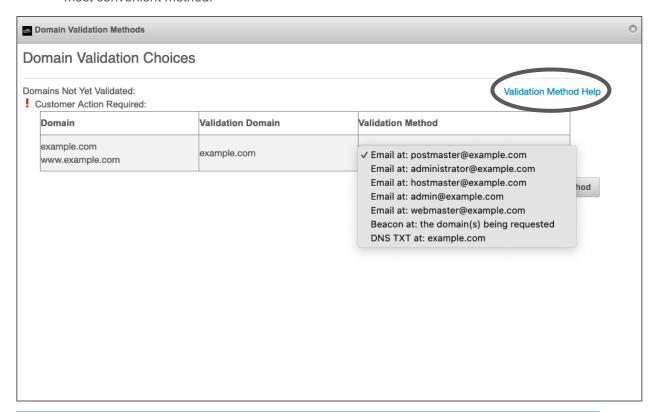
5. Click **Submit**.
VikingCloud will begin the setup for the domain validation process. This may take several minutes.

Validate Your Domains

Before VikingCloud 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.
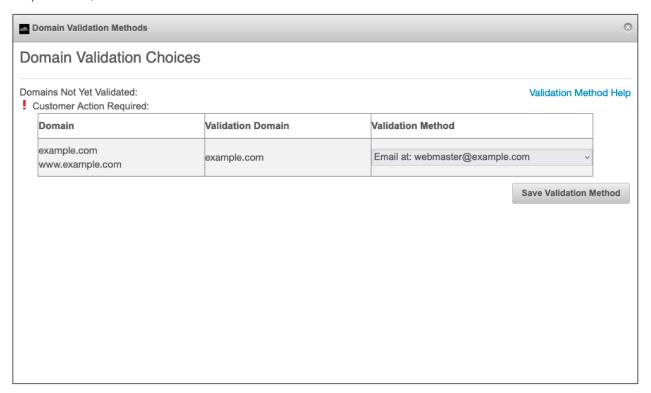
1. On the **Domain Validation Methods** form, you will be presented with:

   a. A list of the Domains submitted from the Submit Certificate Signing Request window.

   b. A selection for the Validation Domain to be used for validating the domain. Note: Some domains may be grouped together based on the lowest common domain to expedite validation. This can be changed by selecting the Validation Domain drop-down and choosing the domain that you wish to use.

   c. A selection for the Validation Method to be used for validating the domain. VikingCloud offers several validation methods: email, DNS, and domain beacon. In general, email validation is the most convenient method.

Tip: The **Validation Method Help** link leads to information on each method.

2. For this guide, the Email domain validation method will be used. On the **Validation Methods** dropdown list, select **Email**.
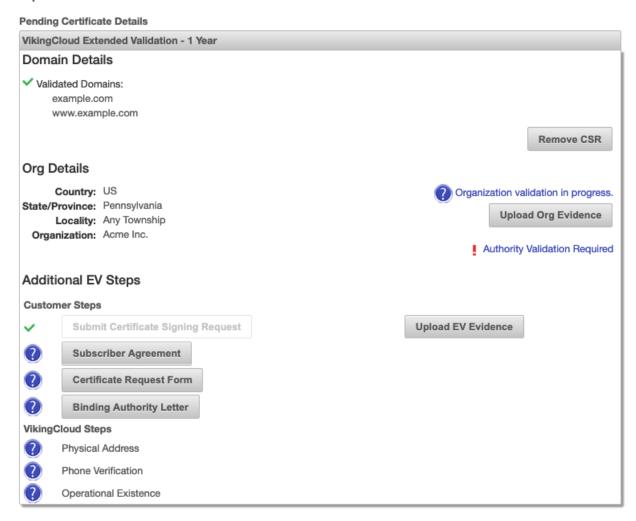

3. Click **Save Validation Method**.

    a. For the email validation method, you will receive an email from sslsupport@vikingcloud.com asking you to validate the domain(s). To validate your domains via email, continue with step 4 below.

    b. When using one of the other validation methods, follow the instructions that you are given in Control Center and skip to step 6.

4. Click the **Approve/Decline Domain Validation** link in the email.
   A browser will open to the **Confirm Domain Validation** page.

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

6. Return to the Control Center's **Pending Certificates** page and scroll down to the **Additional EV Steps** section.

7. Click **Subscriber Agreement** to open the **EV Subscriber Agreement** form.

EV Subscriber Agreement

VikingCloud™ Subscriber Agreement for Digital Certificates

Ver. 15FEBRUARY23

IMPORTANT: PLEASE READ THIS AGREEMENT AND THE VIKINGCLOUD CERTIFICATE POLICY AND CERTIFICATION PRACTICES STATEMENTS LOCATED AT HTTPS://CERTS.SECURETRUST.COM/CA/ ("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 ca@vikingcloud.com . IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT APPLY FOR A CERTIFICATE AND DO NOT CLICK ON "I ACCEPT" OR "I AGREE" BELOW, DO NOT CLICK "CONTINUE" AND PROMPTLY EXIT THE BROWSER.

THIS VIKINGCLOUD SUBSCRIBER AGREEMENT FOR DIGITAL CERTIFICATES ("Agreement") is effective as of the date of the accompanying Certificate (the "Effective Date") and is entered into by Viking Cloud, Inc. ("VikingCloud", Provider", "We", "Our", or "Us") and the applicant set forth in the Order Form and that is receiving the Certificate ("Client").

The legal name of the Client is [   ].

The name of the Contract Signer (as hereinafter defined) duly authorized by the Client to bind the Client to this Agreement is [   ].

Each Certificate that VikingCloud issues to Client shall be governed by this Agreement, any Order Form, and the CPS. Further, the parties hereby agree that Relying Parties and Application Software Vendors (as such terms are defined below) are intended third party beneficiaries of this Agreement.

1. DEFINITIONS

Application Software Vendors

A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as, but not limited to, KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
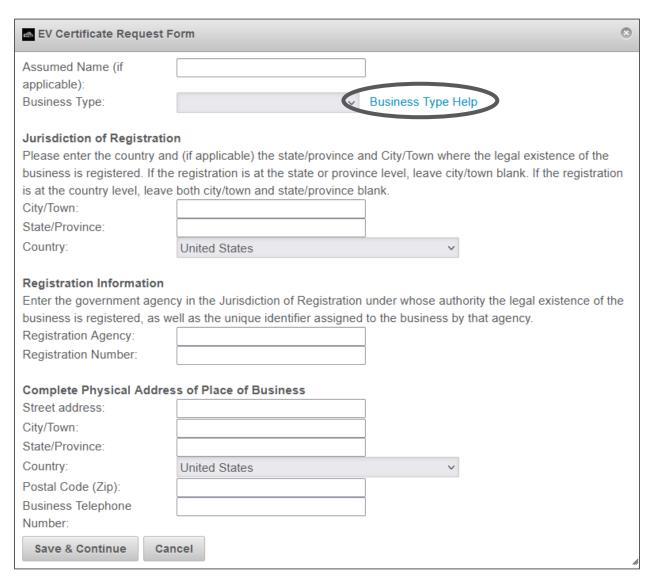
Certificate

Any certificate that contains information specified in the CPS and/or the Guidelines, as applicable, and that has been validated in accordance with the CPS and/or the Guidelines, as applicable.

Certificate Revocation List ("CRL")

a. Enter the names of the Applicant and Contract Signer in the two fields.

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

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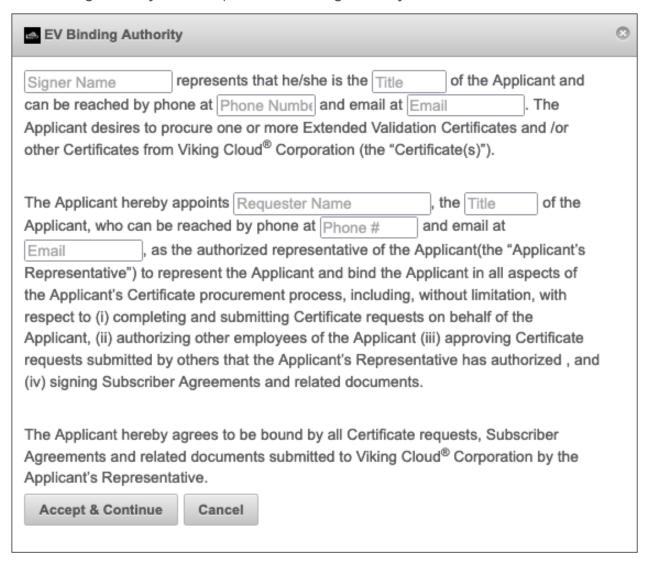

a. Fill out as many of the fields as possible. No field is required but the more information you provide, the easier it will be for VikingCloud to confirm your business' identity.

Tip: Click the **Business Type Help** link to learn what the different types are.

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

9. Click **Binding Authority Letter** to open the **EV Binding Authority** form.

a. In the eight fields, enter the information of the person which VikingCloud can contact to complete validation. If the business type is an unincorporated entity, then VikingCloud 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 Control Center's **Pending Certificates** page, you may find that VikingCloud is in the process of additional evaluation of your domains. Additional validations are required before your EV certificate can be issued. VikingCloud will be in the process of validating your organization existence and the authority to issue certificates on behalf of that organization. VikingCloud Support follows these steps to validate your EV:

- 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 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 VikingCloud Support to reply with any additional validation requirements. Be patient as these validations often take some time to complete. Once complete, your certificate can be issued.

Legal Notice

Copyright © 2023 Viking Cloud, Inc.("VikingCloud") or its affiliates.

The most current version of this document may be obtained by contacting:

VikingCloud SSL Support:
Phone: +1.866.775.2378
Email: sslsupport@vikingcloud.com

Trademarks

About VikingCloud™

VikingCloud provides end-to-end security and compliance solutions to businesses around the world, offering the latest in cloud-based solutions to secure networks and maintain compliance. Almost 5 million businesses use VikingCloud's award-winning platform, and the company maintains partnerships with many of the world's leading acquirers and payment service providers. VikingCloud also works with the world's largest brands helping them proactively mitigate evolving cyber threats and business risk. VikingCloud's Asgard Platform™ processes billions of security events daily, providing real-time intelligence access to an organization's cyber risk landscape. Headquartered in Dublin, Ireland, with operations in the United States, Australia, Brazil, Canada, Germany, India, Mexico, Philippines, Poland, South Africa, and the United Kingdom, VikingCloud has clients in more than 70 countries and a global team of more than 1,000. For more information about VikingCloud, visit https://www.vikingcloud.com.