Xaccel CaaS Portal

Reseller User Guide

Xaccel LLC

Table of Contents

Xaccel CaaS Portal — Reseller User Guide

SSL/TLS Certificate Lifecycle Management

Version 2.0 | April 2026

Xaccel LLC | www.xaccel.net | (800) 533-4040 | sales@xaccel.net

CONFIDENTIAL

Table of Contents

1. Introduction

Welcome to the Xaccel CaaS Portal. This platform provides automated SSL/TLS certificate lifecycle management powered by Sectigo, one of the world's largest commercial Certificate Authorities.

As a reseller, you can use this portal to:

- Create and manage ACME accounts for yourself and your clients
- Add domains and automatically provision SSL certificates
- Generate ready-to-run installation scripts for any server platform
- Monitor certificate status and expiration dates
- View invoices, manage payment methods, and track billing
- Access your EAB credentials for manual ACME client configuration

How It Works

The CaaS (Certificate as a Service) model works differently from traditional per-certificate purchasing. You subscribe domains to your account, and anyone operating an ACME client with your credentials can obtain unlimited certificates for those domains at no additional cost during the subscription period.

Certificates are issued via the ACME protocol (RFC 8555), the same standard used by Let's Encrypt. The key difference is that Sectigo provides both Domain Validation (DV) and Organization Validation (OV) certificates, with the backing of a trusted commercial CA.

Certificate Types

Type	What It Validates	Best For
DV SSL	Domain ownership only (automated)	Blogs, marketing sites, internal tools, staging
DV Wildcard	Domain ownership for *.domain.com	Sites with many subdomains
OV SSL	Domain + verified organization identity	E-commerce, financial services, client portals
OV Wildcard	Domain + org identity for *.domain.com	Enterprises needing org validation across subdomains

Note: Certificate maximum duration is 90 days. Certificates auto-renew via the ACME client on your server — no manual intervention needed once configured.

---

2. Getting Started

Logging In

1. Open your browser and navigate to your portal URL (provided by your administrator).
2. Enter your email address and password.
3. If two-factor authentication (2FA) is enabled, enter the 6-digit code from your authenticator app.
4. Click **Sign In**.

Note: Your account is created by the Xaccel administrator. If you don't have credentials, contact your account manager.

First Login Checklist

1. Change your temporary password (Settings → Change Password).
2. Set up two-factor authentication (Settings → Two-Factor Authentication).
3. Add a payment method (Payment Methods → Add Payment Method).
4. Create your first ACME account (ACME Accounts → New Account).
5. Add your first domain (My Domains → Add Domain).

Password Requirements

Passwords must contain all of the following:

- At least 8 characters

- One uppercase letter (A–Z)
- One lowercase letter (a–z)
- One number (0–9)
- One special character (!@#$%^&*()_+-= etc.)

The portal shows a live strength indicator as you type.

---

3. Portal Overview

Navigation

The portal sidebar contains the following sections:

Overview - Dashboard — Account summary, quick actions, pricing, and recent invoices

Certificates - ACME Accounts — Create and manage ACME accounts with EAB credentials - My Domains — Add, remove, and search domains

Billing - Billing Summary — Account balance, outstanding payments, estimated monthly cost - Invoices — View and download invoices, make manual payments - Payment History — All payment transactions - Payment Methods — Add, remove, and manage credit cards

Account - Settings — Change password, set up 2FA, check service health

Dashboard

Your dashboard shows:

- Active domain count and ACME account count
- Your pricing schedule (DV and OV rates per year)
- Quick action buttons to create accounts and add domains
- Recent invoices with status

  Note: New accounts with zero ACME accounts will see an onboarding wizard with step-by-step setup instructions.

Theme

The portal supports both dark and light themes. Toggle between them using the theme button at the bottom of the sidebar. Your preference is saved automatically.

---

4. Managing ACME Accounts

What Is an ACME Account?

An ACME account is your connection to Sectigo's certificate issuance system. Each account comes with External Account Binding (EAB) credentials — a MAC Key and a Key ID — that you use to register your ACME client (Certbot, acme.sh, etc.) with Sectigo's server.

You can create multiple accounts to organize certificates by client, environment, or purpose.

Creating an ACME Account

1. Navigate to **ACME Accounts**.
2. Click **+ New ACME Account**.
3. Select the certificate type: DV (Domain Validation) or OV (Organization Validation).
4. Enter an optional label (e.g., "Production", "Client-Acme").
5. Select the subscription term: 1, 2, or 3 years.
6. Click **Create Account**.

The portal will display your EAB credentials. Save them securely — you'll need them to configure your ACME client.

EAB Credentials

Each ACME account has three critical values:

Credential	Description
ACME Server URL	The Sectigo endpoint: `https://acme.sectigo.com/v2/DV` or `/v2/OV`
EAB MAC Key	The HMAC key used to authenticate your ACME client registration (base64url encoded)
EAB Key ID	The key identifier paired with the MAC Key (base64url encoded)

> **Warning:** EAB credentials link the ACME client to your Xaccel account. Do not share them with unauthorized parties.

Viewing Credentials Later

Click **EAB & Scripts** on any ACME account to view the credentials again. The modal has three tabs:

- **EAB Credentials** — Click any field to select it for copying
- **Validation Guide** — Step-by-step explanation of HTTP-01 and DNS-01 validation
- **Install Script** — Generate a ready-to-run script for your server

5. Managing Domains

Adding a Domain

1. Navigate to **My Domains**.
2. Click **+ Add Domain**.
3. Select which ACME account to associate the domain with.
4. Enter the domain name (e.g., `example.com` or `*.example.com`).
5. For OV accounts, enter the OV Anchor Order Number if required.
6. Click **Add Domain**.

Automatic Companion Domains

The portal automatically adds companion domains at no extra charge:

You Enter	Portal Also Adds	Why
`example.com`	`www.example.com` (free)	Most sites need both
`www.example.com`	`example.com` (free, becomes primary)	Bare domain needed
`*.example.com`	`example.com` (free)	Wildcard doesn't cover the apex
`app.example.com`	Nothing	Specific subdomain, no companion needed

> **Note:** You can opt out of automatic companion domains by checking "Don't include www" in the add domain dialog.

Bulk Import (CSV)

To add many domains at once:

1. Click **Bulk Import** on the My Domains page.
2. Select the ACME account.
3. Upload a CSV file with a column named "domain" or "domain_name".
4. Click **Import**.

Example CSV:

```
domain
example.com
www.example.com
*.mysite.org
shop.anothersite.com
```

Removing a Domain

Click the **Remove** button next to any active domain. If the domain was added within the last 30 days, a credit is automatically issued to your account.

> **Warning:** Removing a domain prevents new certificate issuance for that domain. Existing certificates remain valid until they expire.

Searching Domains

Use the search bar at the top of the My Domains page to filter by domain name. The search is instant and works client-side.

---

6. Domain Validation Guide

Before Sectigo issues a certificate, it must verify that you control the domain. This happens automatically when you run the ACME client. There are two validation methods.

HTTP-01 Validation (Standard Domains)

This is the default and simplest method. Your ACME client (Certbot) places a temporary file on your web server, and Sectigo's server fetches it to prove domain ownership.

Requirements:

- Port 80 must be open and reachable from the internet
- Your web server (Nginx, Apache) must be running
- Certbot needs write access to the web server config or document root

Customer action: None. This is fully automatic.

DNS-01 Validation (Required for Wildcards)

For wildcard certificates (`*.example.com`), you must use DNS-01 validation. There is no alternative. You add a TXT record to your domain's DNS.

The DNS record format:

Field	Value
Type	TXT
Name	`_acme-challenge.yourdomain.com`
Value	(Generated by Certbot at runtime — different each time)
TTL	300 (or lowest available)

Option A: Automated DNS Plugin (Recommended)

If your DNS is managed by Cloudflare, AWS Route53, DigitalOcean, or GoDaddy, use a DNS plugin that creates and removes the TXT record automatically. This means renewals are fully hands-off.

Select your DNS provider in the Install Script Generator (ACME Accounts → EAB & Scripts → Install Script tab) and the generated script will include the plugin setup.

Supported providers:

Provider	Plugin	Credential Needed
Cloudflare	certbot-dns-cloudflare	API Token (Zone:DNS:Edit)
AWS Route53	certbot-dns-route53	IAM credentials
DigitalOcean	certbot-dns-digitalocean	API Token
GoDaddy	certbot-dns-godaddy	API Key + Secret

Option B: Manual DNS

If you don't use a supported DNS plugin:

1. Run the install script on your server.
2. Certbot will pause and display the TXT record value.
3. Log into your DNS provider (GoDaddy, Cloudflare, Namecheap, etc.).
4. Add the TXT record shown by Certbot.
5. Wait 1–2 minutes for DNS propagation.
6. Press Enter in the terminal to continue.

Warning: Manual DNS-01 means you must update the TXT record every 60–90 days at renewal. We strongly recommend using an automated DNS plugin for wildcard certificates.

Important: For wildcard + bare domain, Certbot will ask twice — add BOTH TXT records before pressing Enter.

---

7. Installing Certificates — Linux

Using the Provisioning Script Generator

The easiest way to install certificates is to use the built-in script generator:

1. Go to **ACME Accounts** and click **EAB & Scripts** on your account.
2. Click the **Install Script** tab.

3. Select your platform (Ubuntu/Debian + Nginx, Ubuntu/Debian + Apache, or CentOS/RHEL).
4. Select your web server type.
5. Enter your notification email.
6. Enter your domains (one per line), or leave blank to use all domains on the account.
7. If using wildcards, select your DNS provider.
8. Click **Generate Install Script**.
9. Click **Download .sh** or **Copy** to clipboard.
10. Transfer the script to your server and run it:

```
chmod +x setup-ssl.sh
sudo bash setup-ssl.sh
```

The script handles everything: installing Certbot, registering with Sectigo, requesting the certificate, configuring your web server, and setting up auto-renewal.

Manual Installation — Ubuntu/Debian + Nginx

Step 1: Install Certbot

```
sudo apt-get update
sudo apt-get install -y certbot python3-certbot-nginx
```

Step 2: Register with Sectigo

```
sudo certbot register \
  --server https://acme.sectigo.com/v2/DV \
  --eab-kid "YOUR_EAB_KEY_ID" \
  --eab-hmac-key "YOUR_EAB_MAC_KEY" \
  --email admin@yourdomain.com \
  --agree-tos --no-eff-email
```

Replace `YOUR_EAB_KEY_ID` and `YOUR_EAB_MAC_KEY` with the values from your ACME account in the portal.

Step 3: Request Certificate

```
sudo certbot --nginx \
  --server https://acme.sectigo.com/v2/DV \
  -d example.com -d www.example.com \
  --non-interactive
```

Step 4: Verify Auto-Renewal

```
sudo certbot renew --dry-run
sudo systemctl enable certbot.timer
sudo systemctl start certbot.timer
```

Manual Installation — CentOS / RHEL / Rocky / Alma

```
sudo dnf install -y epel-release
sudo dnf install -y certbot python3-certbot-nginx
```

Then follow the same Steps 2–4 as Ubuntu above.

Manual Installation — Ubuntu/Debian + Apache

```
sudo apt-get update
sudo apt-get install -y certbot python3-certbot-apache
```

Then register (Step 2 above) and request with `--apache` instead of `--nginx`:

```
sudo certbot --apache \
  --server https://acme.sectigo.com/v2/DV \
  -d example.com -d www.example.com
```

Certificate File Locations

After successful issuance, certificates are stored at:

```
/etc/letsencrypt/live/yourdomain.com/fullchain.pem   (certificate + chain)
/etc/letsencrypt/live/yourdomain.com/privkey.pem      (private key)
/etc/letsencrypt/live/yourdomain.com/cert.pem         (certificate only)
/etc/letsencrypt/live/yourdomain.com/chain.pem        (CA chain only)
```

Verifying the Certificate

```
sudo openssl x509 -in /etc/letsencrypt/live/yourdomain.com/fullchain.pem \
  -noout -subject -issuer -dates
```

---

8. Installing Certificates — Windows

Using win-acme (Recommended for IIS)

win-acme is the recommended ACME client for Windows Server and IIS.

Step 1: Download win-acme

Download the latest release from https://www.win-acme.com/ and extract to `C:\win-acme\`.

Step 2: Register with Sectigo (PowerShell as Administrator)

```
cd C:\win-acme
.\wacs.exe --baseuri https://acme.sectigo.com/v2/DV `
  --eab-kid "YOUR_EAB_KEY_ID" `
  --eab-key "YOUR_EAB_MAC_KEY" `
  --emailaddress admin@yourdomain.com `
  --accepttos
```

Step 3: Request Certificate and Bind to IIS

```
.\wacs.exe --target manual `
  --host example.com --host www.example.com `
```

```
  --baseuri https://acme.sectigo.com/v2/DV `
  --validation selfhosting `
  --installation iis
```

Step 4: Automatic Renewal

win-acme automatically creates a Windows Scheduled Task for renewal. No additional configuration needed. You can verify it exists in Task Scheduler under `win-acme-renew`.

Certificate Location

```
C:\ProgramData\win-acme\certs\
```

> **Note:** The provisioning script generator can also produce a PowerShell script for Windows. Select "Windows / IIS (win-acme)" in the platform dropdown.

Using Certbot on Windows (Alternative)

Certbot also supports Windows. Install via the official installer at https://certbot.eff.org/instructions?ws=other&os=windows, then use the same commands as the Linux manual installation, adjusting paths for Windows.

---

9. Installing Certificates — Plesk

Plesk manages its own web server configuration, so the installation process is slightly different.

Method: Certbot + Plesk Import

1. SSH into your Plesk server as root.
2. Install Certbot:

```
apt-get install -y certbot
```

3. Register with Sectigo:

```
certbot register \
  --server https://acme.sectigo.com/v2/DV \
  --eab-kid "YOUR_EAB_KEY_ID" \
  --eab-hmac-key "YOUR_EAB_MAC_KEY" \
  --email admin@yourdomain.com \
  --agree-tos
```

4. Request the certificate (standalone mode to avoid conflicts with Plesk's web server):

```
certbot certonly --standalone \
  --pre-hook "plesk sbin websrvmng --stop-proxy" \
  --post-hook "plesk sbin websrvmng --start-proxy" \
```

```
  --server https://acme.sectigo.com/v2/DV \
  -d example.com -d www.example.com
```

5. Import the certificate into Plesk:

```
plesk bin certificate --install \
  -domain example.com \
  -key-file /etc/letsencrypt/live/example.com/privkey.pem \
  -cert-file /etc/letsencrypt/live/example.com/cert.pem \
  -cacert-file /etc/letsencrypt/live/example.com/chain.pem
```

6. Set up auto-renewal with Plesk import hook:

```
mkdir -p /etc/letsencrypt/renewal-hooks/deploy

cat > /etc/letsencrypt/renewal-hooks/deploy/plesk-import.sh << 'EOF'
#!/bin/bash
for domain in $RENEWED_DOMAINS; do
  plesk bin certificate --install \
    -domain "$domain" \
    -key-file "$RENEWED_LINEAGE/privkey.pem" \
    -cert-file "$RENEWED_LINEAGE/cert.pem" \
    -cacert-file "$RENEWED_LINEAGE/chain.pem" 2>/dev/null || true
done
EOF

chmod +x /etc/letsencrypt/renewal-hooks/deploy/plesk-import.sh
```

7. Add renewal cron:

```
(crontab -l 2>/dev/null; echo "0 3 * * * certbot renew --quiet") | sort -u |
crontab -
```

---

10. Installing Certificates — cPanel

cPanel works best with `acme.sh` rather than Certbot because it integrates with cPanel's API directly.

Method: acme.sh + cPanel API

1. SSH into your cPanel server as root.

2. Install acme.sh:

```
curl https://get.acme.sh | sh -s email=admin@yourdomain.com
```

3. Register with Sectigo using EAB:

```
~/.acme.sh/acme.sh --register-account \
  --server https://acme.sectigo.com/v2/DV \
```

```
  --eab-kid "YOUR_EAB_KEY_ID" \
  --eab-hmac-key "YOUR_EAB_MAC_KEY"
```

4. Issue the certificate:

```
~/.acme.sh/acme.sh --issue \
  --server https://acme.sectigo.com/v2/DV \
  -d example.com -d www.example.com \
  --webroot /home/username/public_html
```

5. Deploy to cPanel:

```
~/.acme.sh/acme.sh --deploy \
  -d example.com -d www.example.com \
  --deploy-hook cpanel_uapi
```

acme.sh automatically installs its own cron for renewal. No additional setup needed.

---

11. Billing & Invoices

Pricing

Your pricing is set by the Xaccel administrator and is visible on your dashboard. Pricing varies by:

- **Certificate type:** DV or OV
- **Standard vs. Wildcard:** Wildcard certificates cover all subdomains and cost more
- **Subscription term:** 1, 2, or 3 years (longer terms offer better rates)

Companion domains (auto-added www or bare domain) are always free.

Billing Summary

Navigate to **Billing Summary** to see:

- **Total Paid** — All-time payments
- **Outstanding Balance** — Unpaid invoices
- **Available Credits** — Credits from domain removals
- **Estimated Monthly Cost** — Current annual commitment divided by 12

Invoices

Invoices are generated monthly on the 1st (or the billing day set by your administrator). Each invoice includes:

- Line items for each active domain
- Monthly pro-rated amounts (annual price ÷ 12 for 1-year, ÷ 24 for 2-year, ÷ 36 for 3-year)

- Any credits applied

Viewing and Printing Invoices

1. Navigate to **Invoices**.
2. Click **Details** on any invoice to see line items.
3. Click **Print / PDF** to open a printable view with Xaccel branding.
4. Use your browser's Print dialog to save as PDF or print.

Making a Manual Payment

If an invoice is pending or failed:

1. Navigate to **Billing Summary** or **Invoices**.
2. Click the **Pay Now** button on the outstanding invoice.
3. Confirm the charge amount.
4. The payment is charged to your card on file.

Automatic Billing

If you have a card on file, invoices are automatically charged on the due date. If the charge fails, the system retries on days 3, 5, and 7. If all retries fail, your account may be suspended.

---

12. Payment Methods

Adding a Card

1. Navigate to **Payment Methods**.
2. Click **+ Add Payment Method**.
3. Enter your card number, expiration date, CVV, name, and billing ZIP.
4. Click **Add Card**.

Your card is securely tokenized via Authorize.net — the portal never stores your full card number.

Managing Cards

- Set a card as **default** (used for automatic billing)
- **Remove** a card you no longer use
- Add multiple cards for backup

Warning: If no payment method is on file and an invoice is due, the charge will fail and your account may be suspended after the retry period.

---

13. Account Settings & Security

Changing Your Password

1. Navigate to **Settings**.
2. Enter your current password and your new password.
3. The strength indicator shows which requirements are met.
4. Click **Update Password**.

Two-Factor Authentication (2FA)

We strongly recommend enabling 2FA for all accounts.

1. Navigate to **Settings → Two-Factor Authentication**.
2. Click **Setup 2FA**.
3. Scan the QR code with your authenticator app (Google Authenticator, Authy, 1Password, etc.).
4. Enter the 6-digit code to confirm.
5. Click **Verify & Enable**.

Once enabled, you'll need the 6-digit code at every login.

Service Health Check

Navigate to **Settings** and click **Run Health Check** to verify connectivity to:

- **PostgreSQL Database** — connection status and latency
- **Sectigo CaaS API** — credential verification and endpoint reachability
- **Authorize.net** — payment gateway connectivity
- **SMTP** — email service configuration

Account Lockout

After 5 failed login attempts, your account is locked for 15 minutes. If this happens:

- Wait 15 minutes and try again
- Or contact your Xaccel administrator to unlock your account immediately

---

14. Troubleshooting

Login Issues

Problem	Solution
"Invalid credentials"	Check email/password. Passwords are case-sensitive.
"Account locked"	Wait 15 minutes or contact admin for unlock.

Problem	Solution
"Organization suspended"	Your reseller account has been suspended — contact Xaccel.
2FA code rejected	Ensure your phone's clock is synced. Codes change every 30 seconds.

Certificate Issuance Issues

Problem	Solution
"Connection refused" on certbot	Ensure port 80 (HTTP-01) or port 443 is open in your firewall.
"DNS problem" on validation	For HTTP-01: ensure the domain resolves to your server's IP. For DNS-01: ensure the TXT record is published and propagated.
"Unauthorized" or "Invalid EAB"	Your EAB credentials may be wrong. Copy them again from the portal.
"Rate limited"	Sectigo has issuance rate limits. Wait an hour and retry.
Certificate issued but not trusted	Ensure you're using `fullchain.pem`, not `cert.pem`. The full chain includes the intermediate CA.

Wildcard Certificate Issues

Problem	Solution
"No TXT record found"	DNS propagation may take 1–5 minutes. Use `dig _acme-challenge.yourdomain.com TXT` to verify.
Certbot asks twice for TXT	This is normal for wildcard + bare domain. Add BOTH TXT records before pressing Enter.
Renewal fails (manual DNS)	You must update the TXT record at every renewal. Consider switching to an automated DNS plugin.

Billing Issues

Problem	Solution
Invoice shows wrong price	Contact admin — they can recalculate pricing for your account.
Payment failed	Check that your card is valid and has sufficient funds. Update your payment method and use "Pay Now" to retry.
Need a refund	Domains removed within 30 days receive automatic credits. For other refunds, contact Xaccel support.

15. Support & Contact

Getting Help

- **Portal:** Use the health check (Settings → Run Health Check) to diagnose connectivity issues
- **Email:** support@xaccel.net
- **Phone:** (800) 533-4040
- **Website:** www.xaccel.net

Reporting Issues

When reporting an issue, please include:

- Your reseller company name and email
- The domain name(s) affected
- The exact error message (screenshot if possible)
- The platform and web server you're using
- The output of `certbot --version` (for Linux issues)

Useful External Resources

- Certbot documentation: https://certbot.eff.org/docs/
- acme.sh documentation: https://github.com/acmesh-official/acme.sh
- win-acme documentation: https://www.win-acme.com/reference/cli
- Sectigo ACME documentation: https://sectigo.com/knowledge-base/detail/Sectigo-ACME-Protocol/kA01N000000bvPF

This document is confidential and intended for authorized Xaccel resellers only.

© 2026 Xaccel LLC. All rights reserved.