

SOLUTION BROCHURE

Welcome to Entrust Support



ENTRUST

SECURING A WORLD IN MOTION

Contents

- Contact Us 4
- TrustedCare 5
- Authorized Contacts 5
- How to Subscribe to Notifications and Alerts 6
- Entrust Product Security7
- Information Resources 8
- Calling Support 8
- How to Open a Case11
- How to Use nShield HSM Technical Support Services13
- nShield Premium Plus 14
- nShield Premium 14
- nShield Standard15
- nShield Device Replacement & Repair Services15
- Support Availability & Target Response Times16
- Training 18



Welcome pack

A guide to using Entrust technical and product support services

Entrust Support is available around the world, 24x7x365 to ensure that you succeed.

Our global technical support team is committed to providing a world-class service, with expert support engineers available to help you resolve any technical incidents related to your product.

This welcome pack will help you to understand how to access the range of support services available as part of your support package and ensure you get maximum value from Entrust Support.

Contact Us

How to contact us

There are three methods you can use to contact Entrust Support to log a query:

- Logging into TrustedCare
- Calling
- Emailing

TrustedCare

When we receive your email a case will be logged and an Entrust support engineer will contact you within the targeted time of your support contract. Email is monitored during normal business hours.

TrustedCare can be accessed from the following link:

<https://trustedcare.entrust.com>



Many questions and problems can be resolved using TrustedCare.

Benefits of TrustedCare

TrustedCare provides the following benefits;

- **Available 24x7:** TrustedCare is an easy-to-use self-service portal that provides unlimited access to a wealth of information via the web 24x7.
- **Search the Entrust Knowledge Base:** Through our comprehensive search capability, TrustedCare offers a Knowledge Base with valuable troubleshooting advice, how-to articles, and best practices.
- **Subscribe to product notifications and alerts:** TrustedCare offers a Newsletter feature that provides notifications of new software releases, product updates, security alerts, and other important support related news.

Once you have a registered account for TrustedCare, to subscribe for updates, you simply select the product you would like to be notified about.

Many questions and problems can be resolved using TrustedCare such as product documentation, product release notes, security alerts, and bug information.

How to Access TrustedCare

Request login credentials

Before you can access TrustedCare you must have an account with Entrust. If your company has a named contact, please ask the person to send an email with your full name, email, work address and phone number.

Either email at:

- nshield.support@entrust.com
- hytrust.support@entrust.com
- Support@entrust.com

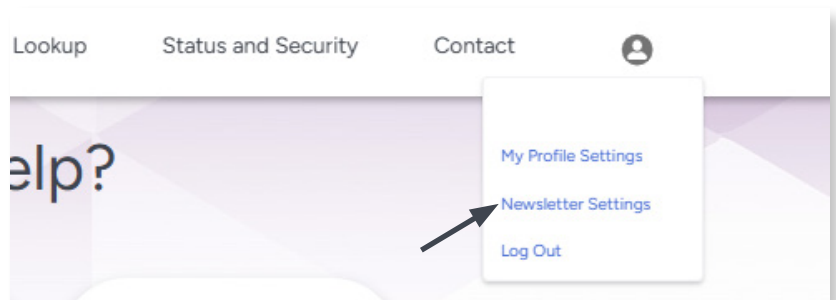
If you already have an account but don't know your password, you can click the "forgot my password" link to reset your access to the site.

Authorized Contacts (Named Contact)

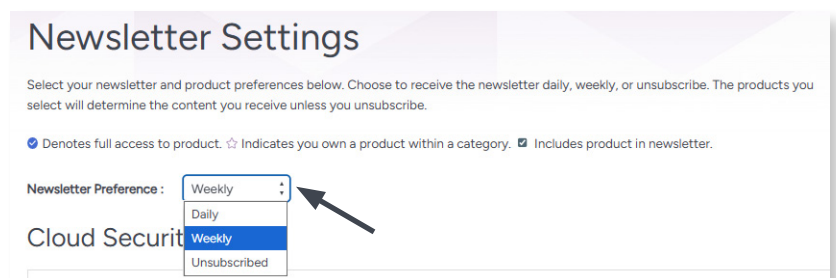
Authorized Contacts	To Request Named Support Contacts Status
Entrust is dedicated to the security of our customers and partners. Therefore, we provide support only to named contacts. You can find Entrust named contacts in the TrustedCare portal: • https://trustedcare.entrust.com/TrustedCare/	If Named Support Contacts is no longer at your company, and you require access, please submit your request to trustedcaresupport@entrust.com and include: • First and last name • Phone number • Company organization

How to Subscribe to Notifications and Alerts

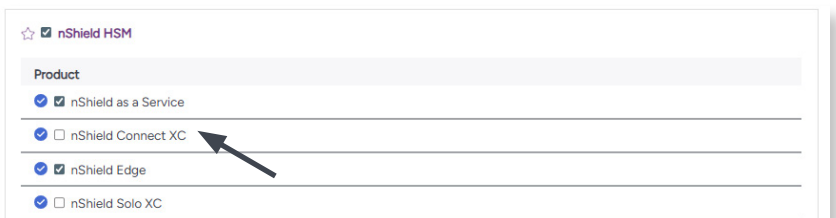
1. Click on Newsletter Settings



2. Select your newsletter preferences



3. Select your product preferences



Entrust Product Security

We know that our customers are concerned about security vulnerabilities that may impact Entrust products. If an Entrust product you use is affected, you'll receive an email.

You can always get updates on your products by reading the security bulletins:

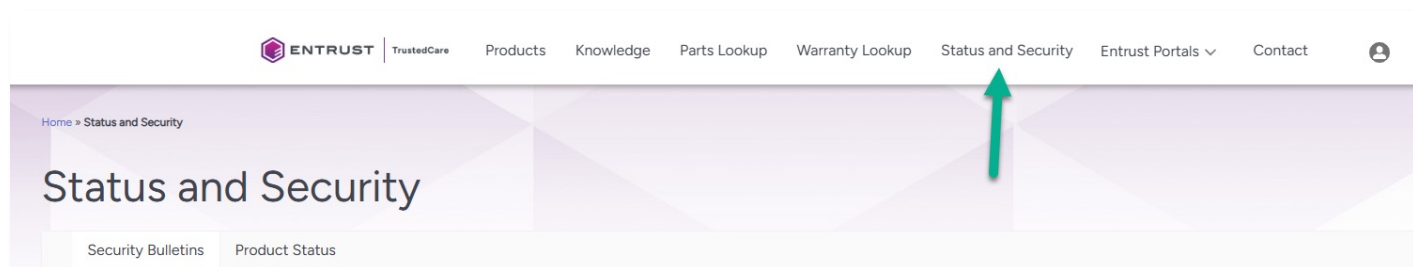
- In the Entrust newsletter
- On the Support portal for your product
- In the Knowledge Base by searching for "Security Bulletin"

Finding Security Bulletins

Security Bulletins in the TrustedCare portal

On the TrustedCare portal at <https://trustedcare.entrust.com/>.

Go to the **Status and Security** page.



Information Resources

Find information about Entrust products using the resources below.

Knowledge Base

Check out information in several formats, including product documentation, how-to instructions, frequently asked questions, white papers, and videos. Use the Search feature to look for information by product name, type of resource, or guide name.

Product Support & Integration Center (PSIC)

You can find more information on our TrustedCare portal by choosing a product name. Look for the PSIC information on the DOCUMENTS tab. Sample Name: PSIC <Product Name, Version>

PSIC provides information specific to each Entrust product and aligns supported third-party products and versions that we test and support.

Any products falling outside these specifications could pose problems to your organization, resulting in an impact to your business, for which your organization assumes sole liability. Before you upgrade any third-party components, we highly recommend you review our PSIC documentation.

Don't see the product or version you're looking for?

Send an enhancement request to your Entrust Support professional. We are happy to gather requirements, act as your advocate, and keep you updated on the status of your request.

Contacting Support for:

nShield HSMs and HSM-related software

EMEA

8:30am–5pm (GMT)

+44 (0)1223 723680

APAC

9am–5pm (GMT)

+852 28 210 120

Australia

+61 870 921 910

Japan

+81 3 4213-1750

AMERICAS

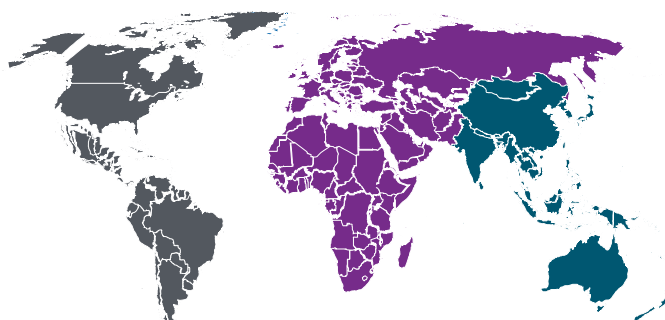
9am–5pm (GMT-5)

+1 833-902-4990

+1 952-988-1550

Brazil

+55 11 4560 3640



Email: nshield.support@entrust.com

Contacting Support for:

- Cryptographic Security Platform (CSP) Compliance Manager (formerly known as KeyControl Compliance Manager)
- Cryptographic Security Platform (CSP) Key and Secrets Management (formerly known as KeyControl Vault)
- CSP as a Service (CSPaaS) Key Manager (formerly known as KeyControl as a Service Vault)
- CSP as a Service (CSPaaS) Compliance Manager (formerly known as KeyControl as a Service Compliance Manager)
- CloudControl

APAC

Japan

+81 3 4221 9718

AMERICAS

North America

+1 605-681-8100

Toll-free, select option 2

+1 844-681-8100

Email: hytrust.support@entrust.com

Contacting Support for:

- PKI solutions (software and hosted services)
- Cryptographic Security Platform (CSP) Certificate Management
- CSP as a Service (CSPaaS) - PKIaaS
- Identity and Access Management (IDaaS, Identity Enterprise, Identity Essentials, Get Access)

EMEA

Europe

+44 800 121 6078

+44 118 953 3088

Middle East

+014 800 3687 7863

APAC

Indonesia

+62 215 0861 648

Japan

+81 3 4221 9718

AMERICAS

North America

+1 877-754-7878

Caribbean, Latin America

+1 613-270-3746

Email: support@entrust.com

Support Phone Numbers Online

Product Line	https://www.entrust.com/contact-support
PKI solutions (software and hosted services) Cryptographic Security Platform (CSP) Certificate Management CSP as a Service (CSPaaS) - PKIaaS Identity & Access Management (IDaaS, Identity Enterprise, Identity Essentials, Get Access)	Choose PKI solutions (software and hosted services) Cryptographic Security Platform (CSP) Certificate Management CSP as a Service (CSPaaS) - PKIaaS Identity and Access Management (IDaaS, Identity Enterprise, Identity Essentials, Get Access) to reveal numbers.
Cryptographic Security Platform (CSP) Compliance Manager (formerly known as KeyControl Compliance Manager) Cryptographic Security Platform (CSP) Key and Secrets Management (formerly known as KeyControl Vault) CSP as a Service (CSPaaS) Key Manager (formerly known as KeyControl as a Service Vault) CSP as a Service (CSPaaS) Compliance Manager (formerly known as KeyControl as a Service Compliance Manager) CloudControl	Choose Cryptographic Security Platform (CSP) Compliance Manager (formerly known as KeyControl Compliance Manager) Cryptographic Security Platform (CSP) Key and Secrets Management (formerly known as KeyControl Vault) CSP as a Service (CSPaaS) Key Manager (formerly known as KeyControl as a Service Vault) CSP as a Service (CSPaaS) Compliance Manager (formerly known as KeyControl as a Service Compliance Manager) CloudControl to reveal numbers
nShield HSMs and HSM-related software	Choose nShield HSMs to reveal numbers



How to Open a Case

If you need to report an incident or issue, follow the 2 steps described in the sections below: Depending on your product, determine first the severity level of your issue, then create a case.

Step 1/2: Determine the severity level.

Severity levels for nShield HSMs and HSM-related software

How you report an incident depends on the severity. There are four severity levels.	
Severity 1 (Urgent)	Severe problem preventing customer from performing critical business functions.
Severity 2 (High)	Customer or workgroup able to perform job function, but performance of job function degraded or severely limited.
Severity 3 (Normal)	Customer or workgroup performance of job function is largely unaffected.
Severity 4 (Low)	Minimal system impact; includes feature requests and other non-critical questions.

Severity levels for Cryptographic Security Platform (CSP) Compliance Manager (formerly known as KeyControl Compliance Manager), Cryptographic Security Platform (CSP) Key and Secrets Management (formerly known as KeyControl Vault), CSP as a Service (CSPaaS) Key Manager (formerly known as KeyControl as a Service Vault), CSP as a Service (CSPaaS) Compliance Manager (formerly known as KeyControl as a Service Compliance Manager), CloudControl

How you report an incident depends on the severity. There are four severity levels.	
Severity 1 (Urgent)	Software is completely inoperative or at least one component of mission-critical functionality does not perform.
Severity 2 (High)	The overall performance of software is degraded or at least one component of material (but not mission-critical) functionality does not perform.
Severity 3 (Normal)	Any problem that affects performance of the software but does not degrade any material or mission-critical functionality.
Severity 4 (Low)	General questions, feature requests, etc.

Severity levels for PKI solutions (software and hosted services), Cryptographic Security Platform (CSP) Certificate Management, CSP as a Service (CSPaaS) - PKIaaS, Identity and Access Management (IDaaS, Identity Enterprise, Identity Essentials, Get Access)

How you report an incident depends on the severity. There are three severity levels.	
Severity 1 (Critical)	Production server or other mission-critical system(s) are down, and no workaround is immediately available. End-user must have dedicated resources available to work on the issue on an ongoing basis during reported incident. All Severity 1 incidents must be confirmed via telephone.
Severity 2 (Major)	Major functionality is impacted, or significant performance degradation is experienced. The situation is causing a high impact to portions of your business operations, and no reasonable workaround exists. All Severity 2 incidents must be confirmed via telephone.
Severity 3 (Minor)	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation, or configuration; bug affecting low number of users. Acceptable workaround available.

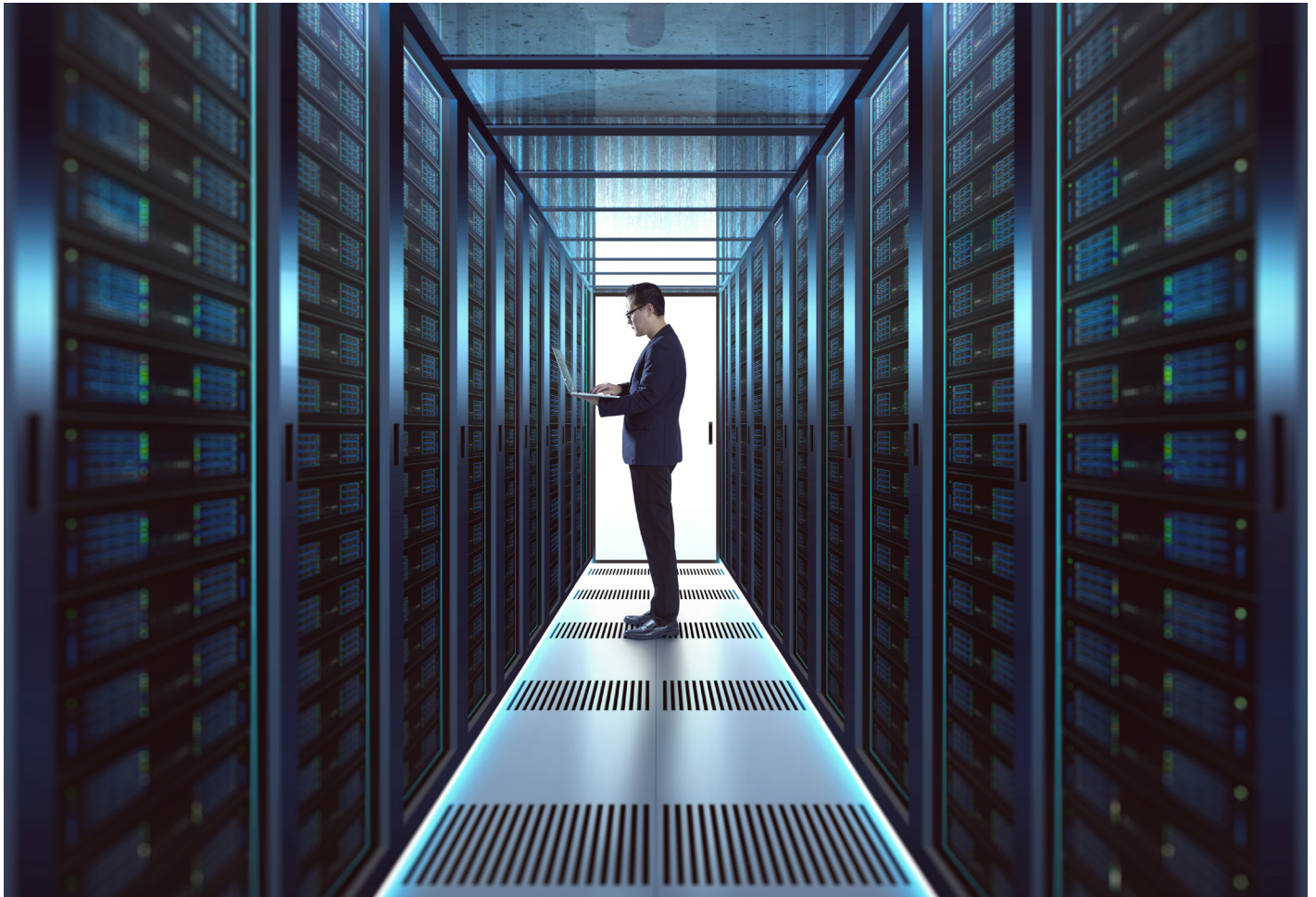
Step 2/2: Create a case

How you open a case depends on the severity level (see step 1).

For high-severity cases you must call in. You can open the cases first, but it is optional.

1. Go to TrustedCare at <https://trustedcare.entrust.com>.
2. Log in with your email address and password. Click NEXT.
3. Click CREATE A CASE.
4. Fill in the mandatory fields. Add as many details as you can about the issue.
5. Optional: If you have an attachment, such as a log file, click ATTACH FILE and browse to your file.
6. Click Done. The case appears. Your case goes to the support queue.
7. After opening a Severity 1 or 2 case, the Named Support Contact must call the Technical Product Team. Be sure to have the case number for reference.

After the case is open, we'll send you regular updates as we work through your incident.



How to Use Entrust nShield Technical Support Services

	PREMIUM PLUS	PREMIUM	STANDARD
Phone support 24 × 7 × 365	•		
Phone support during regional business hours*	•	•	•
Log requests via TrustedCare and email support (regional business hours)	•	•	•
Maximum 4-hour response to initial query	•	•	
Maximum 8-hour response to initial query			•
Access to knowledge articles, product announcements, and information via TrustedCare	•	•	•
Advance replacement of faulty hardware	•	•	
Return failed hardware to Entrust for repair or replacement (15-day turnaround)			•
Firmware and software updates	•	•	•
Hotfix for firmware and software issues, if available	•	•	•

*See section **How to contact Entrust nShield technical support**



Premium Plus

- 24/7 access to our expert technical support via TrustedCare, phone, and email
- Initial response within four hours
- Critical incident management process, to handle mission-critical technical issues
- Hotfixes for software and firmware issues
- Advance hardware replacement
- Access to TrustedCare and Knowledge Base
- Software, firmware, and documentation updates
- Priority escalation handling

Our Premium Plus support package provides our highest level of 24x7 technical support. It is designed for organizations who cannot allow their business to be impacted by extended outages within their critical live environment.

Premium Plus support includes access to our highly skilled team of technical support engineers, 24 hours a day, 365 days a year (by phone only at weekends and public holidays) and our Advance Replacement service. Once the fault is confirmed this service dispatches a replacement device by the end of the next business day, without the need to return the faulty hardware first.

Advance replacement – Please note that a replacement unit always contains the most up-to-date software, while your existing unit may contain a different version. This means that you may be required to make adjustments in order to operate the replacement unit. Should you require a different software version to be loaded onto your replacement unit, then please alert us in advance.

You will need to remove and return the failed product to us and install the repaired/replacement product at your cost, including any taxes and duties.

Premium

- Access to our expert technical support team via TrustedCare, phone, and email during regional business hours
- Initial response within four hours
- Critical incident management process, to handle mission-critical technical issues
- Hotfixes for firmware and software issues
- Advance hardware replacement
- Access to the Knowledge Base
- Software, firmware, and documentation updates
- Priority escalation handling

Our Premium support package includes most of the features of the Premium Plus package, including advance hardware replacement, faster response times, and priority escalation handling. It's suitable for your live system environments, where a 24/7 service is not required.



Please phone Technical Support for immediate assistance with critical issues.

nShield Standard

- Access to our expert technical support team via TrustedCare, phone, and email during regional business hours
- Initial response within eight business hours
- Hotfixes for software and firmware issues
- Access to Knowledge Base
- Repair or replacement of verified faulty units within 15 working days of receipt

The Entrust Standard support package provides your organization with the technical support services you may need for a non-critical, development, or test environment. It allows you access to our team of technical support engineers, who will endeavor to answer any questions you may have about installing, configuring, and maintaining your Entrust products.

Hardware replacement (standard package)

We will repair an original hardware unit or provide a replacement following receipt of your report and our acknowledgment that the product unit has failed. We will then ship the repaired or replacement unit within 15 business days of receipt of the failed unit. You will need to remove and return the original product to us and install the repaired/replacement product at your cost, including any taxes and duties. Please note that a replacement unit always contains the most up-to-date software, while your unit may contain a different version. This means that you may be required to make adjustments in order to operate the replacement unit. Should you require a different software version to be loaded onto your replacement unit, please alert us in advance.

nShield Device Replacement & Repair Services

Customer Services

Once the nShield technical support team has diagnosed that your hardware is faulty, our dedicated Customer Services team will work with you to coordinate the logistics of replacing or repairing your failed device.

Premium and Premium Plus

Upon confirmation of delivery details, our customer service team will work toward shipping an equivalent replacement device by the end of the next working day.

Return of the failed device is not required until you have received the replacement device.

Standard

Our Customer Services team will arrange for collection of your failed device. Once received at our hub the device will be repaired and returned within 15 working days of receipt. If the device is irreparable, a replacement will be shipped. In all cases a pre-paid shipment will be offered for both the replacement and return.

Additional Information

- Entrust Data Protection Solutions has a logistics hub based in the European Union to alleviate shipping delays following Brexit.
- Unless otherwise requested the repaired/replaced device will be returned on our latest FIPS-approved firmware.
- For Premium Plus and Premium, following receipt of the replacement device, the faulty unit must be returned within two weeks.

Support Availability & Target Response Times

Target response times by service level - Cryptographic Security Platform (CSP) Compliance Manager (formerly known as KeyControl Compliance Manager), Cryptographic Security Platform (CSP) Key and Secrets Management (formerly known as KeyControl Vault), CSP as a Service (CSPaaS) Key Manager (formerly known as KeyControl as a Service Vault), CSP as a Service (CSPaaS) Compliance Manager (formerly known as KeyControl as a Service Compliance Manager)

Severity Level	Impact	Initial Response by Entrust
Severity 1	Software is completely inoperative or at least one component of mission-critical functionality does not perform.	Within one business hour. Error diagnosis to commence immediately.
Severity 2	The overall performance of software is degraded or at least one component of material (but not mission-critical) functionality does not perform.	Within four business hours. Error diagnosis to commence immediately.
Severity 3	Any problem that affects performance of the software but does not degrade any material or mission-critical functionality.	Within 12 business hours. Error diagnosis to commence immediately.
Severity 4	General questions, feature requests, etc.	Within 12 business hours.

Support availability and response time for PKI solutions (software and hosted services), Cryptographic Security Platform (CSP) Certificate Management, CSP as a Service (CSPaaS) - PKIaaS, Identity and Access Management (IDaaS, Identity Enterprise, Identity Essentials, Get Access)

Availability	Contact Method	Silver	Platinum
Support Services & hours	Phone	24/5 Sunday 8 PM ET to Friday 8 PM ET	24/7 Dedicated Phone line to move your call to the top of the queue.
	Email/Chat	24/5 Sunday 8 PM ET to Friday 8PM ET	24/5 Sunday 8 PM ET to Friday 8PM ET
	Prioritized requests	X	Yes
Emergency phone support (During non-supported hours)	Severity 1	Yes	Yes
	Severity 2	Paid support available	Yes
	Severity 3	Paid support available	Yes

To protect the security of our customers and partners, Entrust provides support only to Named Support Contacts. See "Authorized contacts" for details.

Target response times by service level – PKI solutions (software and hosted services), Cryptographic Security Platform (CSP) Certificate Management, CSP as a Service (CSPaaS) - PKIaaS, Identity and Access Management (IDaaS, Identity Enterprise, Identity Essentials, Get Access)

Each case is unique. The Entrust team will make reasonable efforts to respond based on the service level.

Response times*	Severity	Silver	Platinum
Service Level	Severity 1	8 to 48 hours	4 to 24 hours
	Severity 2	2 to 5 Business Days	2 to 5 Business Days
	Severity 3	4 to 20 Business Days	2 to 20 Business Days

*Response times differ for each product. The extended times are for on-premises offerings due to multiple dependencies on products and services other than Entrust.



Expand Your Knowledge With World-Class Training

Enhance your security knowledge and join more than 5,000 security professionals who have received world-class training from Entrust.

Courses cover how to deploy, operate, administer, extend, customize, and support Entrust's award-winning digital identity and information security solutions.

Entrust training professionals provide hands-on courses that will equip you to speed the deployment of your security platforms and solutions.

Click this link to see a full list of course descriptions:

[Information Security Solution Training Services | Entrust](#)

Don't see the course you're looking for? Ask your Named Support Contact and we will put you in touch with one of our professionals.



ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.