Request to Add Contact to Netsurion Account

Once this form is completed, please email it to techsupport@netsurion.com.

Authorization Information

Please note that before completing the changes you outline below, Netsurion will contact an Account Administrator (usually the business owner) to provide authorization.

Name of the person completing this form (required):

Location Information

Please check one option, indicating if permissions are for a specific location or for all locations.

☐ **Permissions for a SINGLE location only:**

Business Name: Company Store/Unit Number:

Netsurion Location ID (if known):

City: State: Zip Code:

☐ **Permissions for ALL locations under an owner or entity:**

Name of legal owner entity:

Contact's Basic Information

All fields in this section are required for adding new contacts.

Name:

Title: Email:

Office #: Cell #:

Contact's Affiliation

☐ **Reseller** *(This contact is employed by the company that is selling Netsurion services at this location)*

☐ **Employed by Owner** *(This contact either owns the business that operates at this location or is employed by the owner)*

☐ **Third Party** *(This contact is not a reseller or owner and has some other affiliation to this location)*

Security Code Delivery Method

Please select one or both (not required for removing an existing contact). This will determine which method(s) we use to verify this person's identity when the need arises.

NOTE: *A shared email address cannot be used to verify a contact's identity; doing so is a breach of PCI DSS.*

☐ SMS Text (cell carrier is required, normal carrier fees apply): ☐ Email (provided above)

Permission Type(s)

Select permission(s) to add. Please note that some of these permissions may not apply to your account, depending on what features you have purchased. If you have any questions about which features your account has, please contact your salesperson. This form cannot be used to remove permissions. To remove a user's permission(s), please open a ticket with our technical support department at 713-929-0200 (option 2) or techsupport@netsurion.com.

Basic Permissions

☐ **Admin Contact** *(Will have authority to add / remove users, modify permissions for any users on your account, and authorize changes to firewall settings, configurations, and policies.) NOTE: There must be at least one admin contact for each location.*

☐ **Support Contact** *(May be contacted when there are technical issues and can assist with resolution. This permission also enables the contact to receive service monitoring alerts such as rogue device detection alerts.) NOTE: To receive service monitoring alerts, this permission must be selected.*

☐ **Remote Access** *(Can remotely access all computers which are set up for Netsurion remote access at all locations for which this user is granted permission.)*

EventTracker Permissions

These features may or may not apply to your account. Contact our EventTracker Support Team at 443-842-7335 or etsupport@eventtracker.com if you have any questions.

☐ **Advanced Threat Protection** *(If you purchased EventTracker endpoint monitoring or SIEM-at-the-Edge, grants user permissions to receive email reports and alerts and access the Advanced Threat Protection portal and device log files. Applies to endpoint monitoring and SIEM-at-the-Edge. If customer has subscribed to SIEM-at-the-Edge then will also receive critical notifications via phone call.)*

☐ **Sensor Download** *(If you purchased EventTracker endpoint monitoring or SIEM-at-the-Edge, you must designate a contact to receive email with link and instructions to install ATP sensors on devices for the Location.)*

☐ **FIM Sensor and Portal** (*If you purchased the file integrity monitoring (FIM) service, you must designate at least one contact who will receive the email with the link and instructions to install the FIM sensors and have access to the FIM portal.)*

PCI Compliance Permissions

These features may or may not apply to your account. Contact our PCI Compliance Team at 713-929-0200 (Option 2) or Compliance@netsurion.com if you have any questions.

☐ **Primary PCI Contact (See below)** *If you purchased a PCI package, you must designate a single contact as the primary PCI contact. This was done when your account was set up initially.*

The primary PCI contact:

1) Is responsible for managing the self-assessment questionnaire (SAQ) and external vulnerability scanning

2) Will receive compliance alerts via email

3) Is granted access to the PCI compliance manager portal to access SAQ tools and scan results

PLEASE NOTE: THERE CAN ONLY BE ONE PRIMARY PCI CONTACT PER LOCATION. ADDING THIS CONTACT WILL REPLACE THE CURRENT PRIMARY PCI CONTACT AT THE SPECIFIED LOCATION(S).

☐ **Secondary PCI Contact** *(Will be granted read-only access to the compliance portal to view SAQ and ASV scan results, but will not be able to edit any items or receive alerts.)*