RADWARE CLOUD DDOS PROTECTION SERVICE

ONBOARDING GUIDE

January 2021

TABLE OF CONTENTS

OVERVIEW

The purpose of this document is to guide customers who have purchased Radware's Cloud DDoS Protection Service to configure their service.

This document includes the following sections:

- Getting Ready for the Onboarding Process – Before starting the onboarding process; what you need to know and/or prepare prior to start the process.
- Configuring the Cloud DDoS Protection Service – Starting the onboarding process and a step-by-step guide on how to configure your services:
  - Verify Your Account Service Plan
  - Adding Sites
  - Adding SSL Certificates
  - Adding Assets
  - Running Diversion Tests

Note: Cloud WAF application onboarding is available now directly through the Cloud WAF portal. For more information, see the Cloud WAF Quick Start Guide.

Note: This document describes the standard methods for onboarding the Cloud DDoS Protection service, using a self-service approach. However, to onboard complex settings, or for any issues or questions, contact the Radware NOC/SOC team.

GETTING READY FOR THE ONBOARDING PROCESS

Preparing Environment Parameters

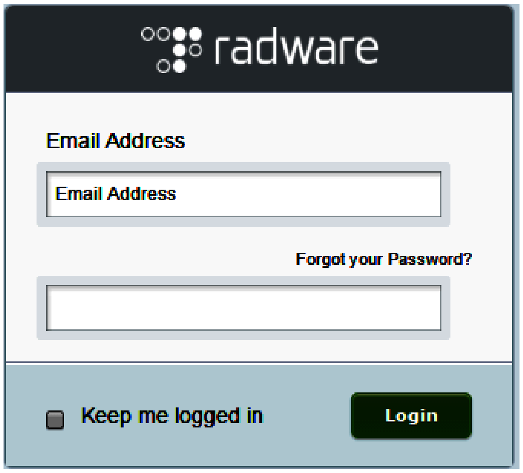
To have a fast, efficient onboarding experience, Radware recommends preparing beforehand the required parameters per each of the service's protected assets, including.

- Preferred diversion method (BGP/DNS)
- Networks
- Letter of Authorization (LOA)
- Subnets
- IP address ranges
- Used/unused IP addresses/ports
- Health check IP address/URL
- SSL certificate

Receiving Invitation to Access the Cloud DDoS Protection Service Portal

1. To start the onboarding process, you will receive an e-mail invitation containing your login link.
2. Click on the redirection link to access the portal and activate your user account.
3. Set your login password.
4. Make sure to save/write down your credentials (username and password) and store securely.
5. Log into the Cloud DDoS portal with your user:

Figure 1: Cloud DDoS Protection Service Login



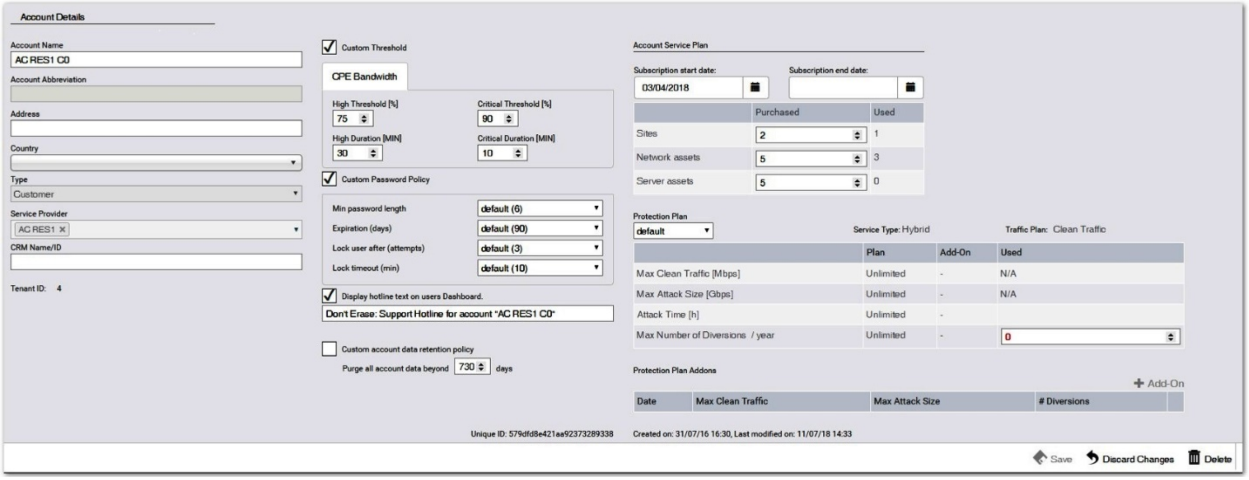
Note: Contact your Radware account manager or ert-soc@radware.com if you have not received the e-mail invitation.

Review Your Account Service Plan

A Radware Cloud DDoS Protection Services account is a customer's account associated with one of more protected assets, security policy profiles and protection plan.

The *Account Settings* pane displays information about the account, depending on the account type (Customer or Service Provider):

Figure 2: Account Settings Pane — Customer



Account Details

Account Name: AC RES1 C0

Account Abbreviation:

Address:

Country:

Type: Customer

Service Provider: AC RES1 ×

CRM Name/ID:

Tenant ID: 4

☑ Custom Threshold

CPE Bandwidth

High Threshold [%]: 75

Critical Threshold [%]: 90

High Duration [MIN]: 30

Critical Duration [MIN]: 10

☑ Custom Password Policy

Min password length: default (6)

Expiration (days): default (90)

Lock user after (attempts): default (3)

Lock timeout (min): default (10)

☑ Display hotline text on users Dashboard.

Don't Erase: Support Hotline for account "AC RES1 C0"

☐ Custom account data retention policy

Purge all account data beyond 730 days

Unique ID: 579dfd8e421aa92373289338

Account Service Plan

Subscription start date: 03/04/2018

Subscription end date:

	Purchased	Used
Sites	2	1
Network assets	5	3
Server assets	5	0

Protection Plan: default

Service Type: Hybrid

Traffic Plan: Clean Traffic

	Plan	Add-On	Used
Max Clean Traffic [Mbps]	Unlimited	-	N/A
Max Attack Size [Gbps]	Unlimited	-	N/A
Attack Time [h]	Unlimited	-	
Max Number of Diversions / year	Unlimited	-	0

Protection Plan Addons

Date	Max Clean Traffic	Max Attack Size	# Diversions

Created on: 31/07/16 16:30, Last modified on: 11/07/18 14:33

The **Account Service Plan** section displays the service plan details for the account, including the number of sites and assets purchased and used.

To check your Account Service Plan

1. From the *Radware Cloud DDoS Protection Services* window, click the drop-down list at the far-right top corner of the window header and select **Account Settings**.
2. Click the **Accounts** icon, located towards the center of the window header.
3. Review the Account Service Plan parameters:

   The **Account Service Plan** section displays the service plan details for the account, including the number of sites and assets purchased and used.

   When creating an account, the administrator sets these values. If the actual used assets have exceeded the number of assets purchased, the usage displays in red.

Table 1: Account Settings: Account Service Plan

Parameter	Description
Subscription start date	Date the subscription starts.
Subscription end date	Date the subscription ends.
Sites	The number of sites **Purchased** and **Used**.
Network assets	The number of network assets **Purchased** and **Used**.
Server assets	The number of server assets **Purchased** and **Used**.

Note: Contact your Radware account manager or ert-soc@radware.com to modify an account or for further assistance.

The **Protection Plan** section displays the protection plan details for the account and a summary of the actual usage for the previous month or the current month. If the actual usage has exceeded the plan limits, the usage displays in red.

Table 2: Account Settings: Protection Plan Parameters

Parameter	Description
Protection Plan	Name of the protection plan. This should be the same as the part item listed in the price list.
Traffic Plan	Can be one of the following traffic plans for the associated service type: • Legit—The Legitimate Traffic-based Model. The level of service is expressed by the regular non-attack traffic that shall be protected by the service. For all service types. • Attack—The Attack Traffic-based Model. For hybrid and on-demand service types only. The level of service is expressed by the maximum attack traffic level that the service shall protect against.
Max Clean Traffic (Mbps)	Maximum planned, add-on, and used clean traffic in Mbps.
Max Attack Size (Gbps)	Maximum planned, add-on, and used attack size in Gbps.
Attack Time (h)	Maximum planned, add-on, and used accumulated attack time in hours.
Max Number of Diversions/year	Maximum planned, add-on, and used number of diversions per year.

CONFIGURING THE CLOUD DDOS PROTECTION SERVICE

Adding Sites

A Site, representing a customer's data center, defines the set of Customer Premises Devices (CPEs) and the GRE (Generic Routing Encapsulation) tunnels configured between the scrubbing center router and the customer's edges. This section describes how to manage sites, including:

- Defining a New Site
- Defining CPE
- Defining GRE Tunnels

Defining a New Site

This procedure describes how to add a new customer Site.

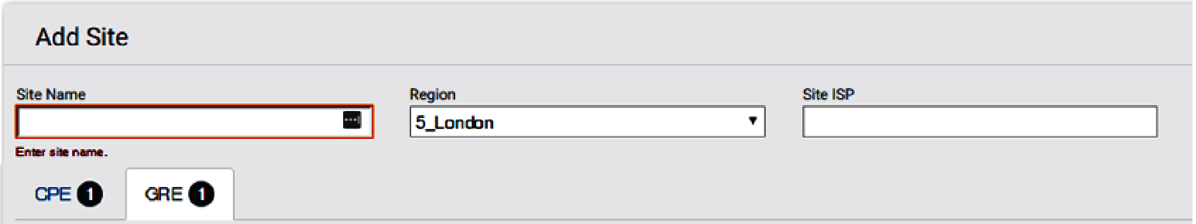
Notes:

- Only users that have the **Site-Create** role can add an account. Other roles only allow a user to view an existing site. Only the Radware NOC can modify or delete an existing site.
- If you add a new site that exceeds the number of sites as defined in your service plan, an error notification displays.

To add a new customer site

1. From the *Radware Cloud DDoS Protection Services* window, click the drop-down list at the far-right top corner of the window header and select **Account Settings**.
2. Click the WWW Sites icon at the top of the page.
3. At the top right of the pane, click the ⊕ Add Site button.

   Note: Mandatory fields are highlighted in red. If you do not complete all mandatory fields, you cannot **Save** the new site.

   Add Site

   Site Name:
   Enter site name.

   Region: 5_London ▾

   Site ISP:

4. Enter the customer **Site Name**.
5. Select the **Region** (Radware's scrubbing center region) for the site.
6. Enter the **Site ISP** name.
7. Add CPE Details (see CPE Details) and/or GRE Details (see GRE Details) as required.

   Important Note: Make sure that all GRE and CPE details are defined before saving.
8. Click **Save** to save all changes, including GRE and CPE details.

   Note: At the bottom of the *Sites* pane, a timestamp displays with the following information:

   - **Created on**—Date and time the site was created.
   - **Last modified on**—Date and time the site was last modified.

   The user sees only his own information. The Admin user can see the user information for other users that the Admin manages.

Note: For customers using NetFlow-based visibility and diversion, the Service includes two additional internal auto-diversion criteria settings available to Radware's NOC. Contact the Radware NOC team to provision/edit sites that require NetFlow configuration and/or for NetFlow settings best practices.

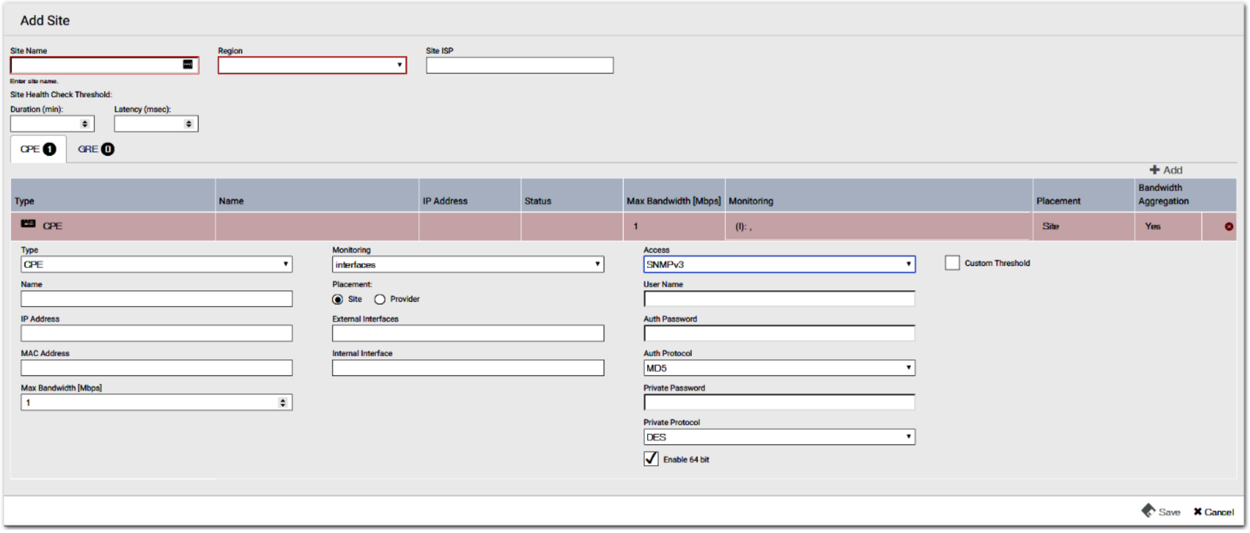
Defining CPE

This section describes how to configure a CPE for the customer site. The CPE is a customer on-premises device that can either be a DefensePro device or a router that the service is monitoring.

To configure CPE details

1. The Site Settings pane displays the sites defined for this account in the left-hand column, and the CPE and GRE tabs for each site.

   To add a new CPE, at the right-hand side above the CPE table, click **+Add**.



Add Site

Site Name: (empty)
Enter site name.
Region: (empty)
Site ISP: (empty)
Site Health Check Threshold:
Duration (min): (empty)
Latency (msec): (empty)

Type	Name	IP Address	Status	Max Bandwidth [Mbps]	Monitoring	Placement	Bandwidth Aggregation
CPE				1	(I): ,	Site	Yes

Type: CPE
Name: (empty)
IP Address: (empty)
MAC Address: (empty)
Max Bandwidth [Mbps]: 1
Monitoring: interfaces
Placement: ● Site ○ Provider
External Interfaces: (empty)
Internal Interface: (empty)
Access: SNMPv3
User Name: (empty)
Auth Password: (empty)
Auth Protocol: MD5
Private Password: (empty)
Private Protocol: DES
☑ Enable 64 bit
□ Custom Threshold

2. Set the CPE parameters, as required:

Table 3: CPE Details: General Parameters

Parameter	Description
Type	Asset type. Select CPE. The CPE is a DefensePro device or a router that is being monitored.
Name	User-defined name of the CPE.
IP Address	IP address of the CPE.
MAC Address	MAC address of the CPE.

Parameter	Description
Max Bandwidth (Mbps)	Maximum CPE bandwidth capacity in Mbps. Cloud DDoS monitors the CPE bandwidth. If the bandwidth is greater than the **Custom Threshold** setting (see **Error! Reference source not found.**), a Resource Utilization operational alert is issued.
Monitoring	Monitoring of either the DefensePro device interface or router interfaces, or the DefensePro device policies. Values: • Interfaces — The interfaces parameters display: ▪ Placement — The physical placement of the CPE device. Values: o Site — The CPE site where the CPE device is located. o Provider — The CPE provider where the CPE device is located. ▪ External Interfaces — The external interfaces from which traffic is read. ▪ Internal Interface — The internal interface from which traffic is read. • Policies — The **Policy Names** parameter displays.

Table 4: CPE Details: Site Parameters

Parameter	Description
Access	Method by which the CPE device is accessed. Values: SNMPv2c, SNMPv3, APSVision
Specific SNMPv2 parameters	
Community	SNMPv2 community.
Specific SNMPv3 parameters	
User Name	SNMPv3 name.
Auth Password	SNMPv3 authorized password.
Auth Protocol	SNMPv3 authorized protocol.
Private Password	SNMPv3 private password.
Private Protocol	SNMPv3 private protocol.

Parameter	Description
Parameters for all Access methods	
Enable 64 bit	Whether to enable 64-bit.
Custom Threshold	If disabled, the service uses the default diversion thresholds. When enabled, you can modify the diversion thresholds. • High Threshold (%) — The high threshold for percentage of traffic. When the percentage of available traffic reaches this threshold for the duration as defined by the **High Duration (MIN)** value, diversion occurs per the defined diversion method (automatic or user-controlled). Default: 75 • High Duration (MIN) — The high threshold duration, in minutes. When the percentage of available traffic reaches the threshold as defined by the **High Threshold (%)** for the duration set by **High Duration (MIN)**, diversion occurs per the defined diversion method (automatic or user-controlled). Default: 10 • Critical Threshold (%) — The critical threshold for percentage of traffic. When the percentage of available traffic reaches this threshold for the duration as defined by the **Critical Duration (MIN)** value, diversion occurs per the defined diversion method (automatic or user-controlled). Default: 90 • Critical Duration (MIN) — The critical threshold duration, in minutes. When the percentage of available traffic reaches the threshold as defined by the **Critical Threshold (%)** for the duration as set by **Critical Duration (MIN)**, diversion occurs per the defined diversion method (automatic or user-controlled). Default: 5

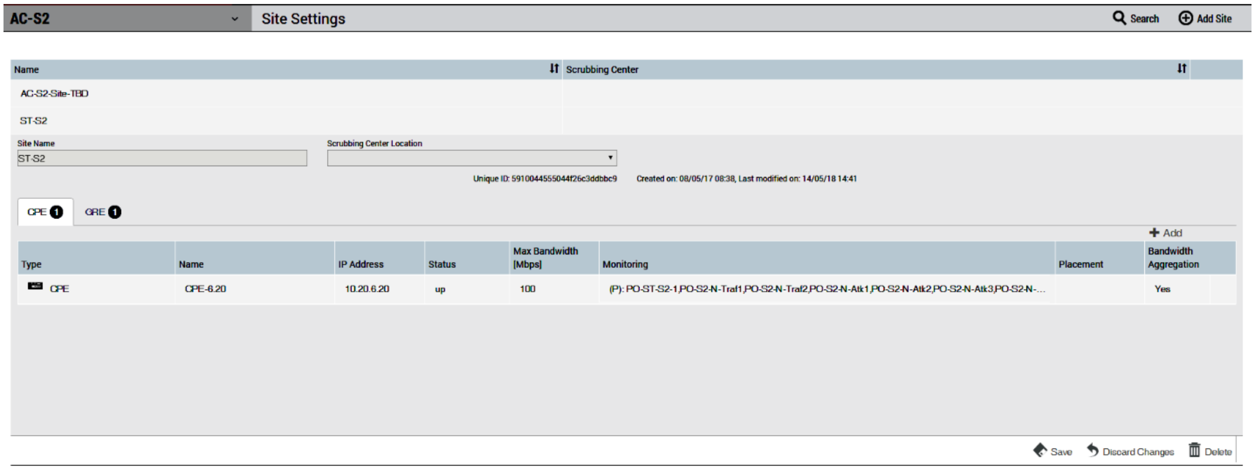
Defining GRE Tunnels

This section describes how to set up a GRE connections and direct/cross connections from the scrubbing center to the customer site.

To add a GRE tunnel or direct/cross connection

1. The Site Settings page displays the sites defined for this account in the left-hand column, and the CPE and GRE tabs for each site.

   To add a new GRE Tunnel, Select the *GRE* tab, and click **+Add**.



Name	Scrubbing Center
AC-S2-Site-TBD	
ST-S2	

Site Name: ST-S2

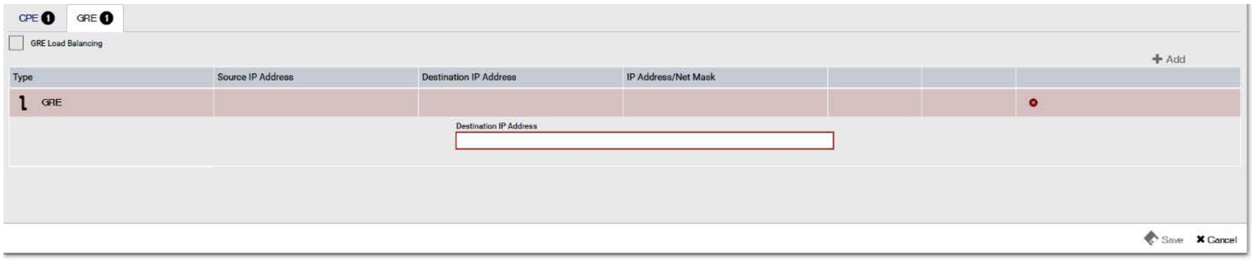
Scrubbing Center Location:

Unique ID: 5910044555044f26c3ddbbc9 Created on: 08/05/17 08:38, Last modified on: 14/05/18 14:41

Type	Name	IP Address	Status	Max Bandwidth [Mbps]	Monitoring	Placement	Bandwidth Aggregation
CPE	CPE-6.20	10.20.6.20	up	100	(P): PO-ST-S2-1,PO-S2-N-Traf1,PO-S2-N-Traf2,PO-S2-N-Atk1,PO-S2-N-Atk2,PO-S2-N-Atk3,PO-S2-N-...		Yes

2. Set the Destination IP Address of the GRE connection (this is the public IP address of the tunnel's source on the customer site).

   Note: The Service Provider user can only define/modify the Destination IP address.



☐ GRE Load Balancing

Type	Source IP Address	Destination IP Address	IP Address/Net Mask			
GRE						

Destination IP Address:

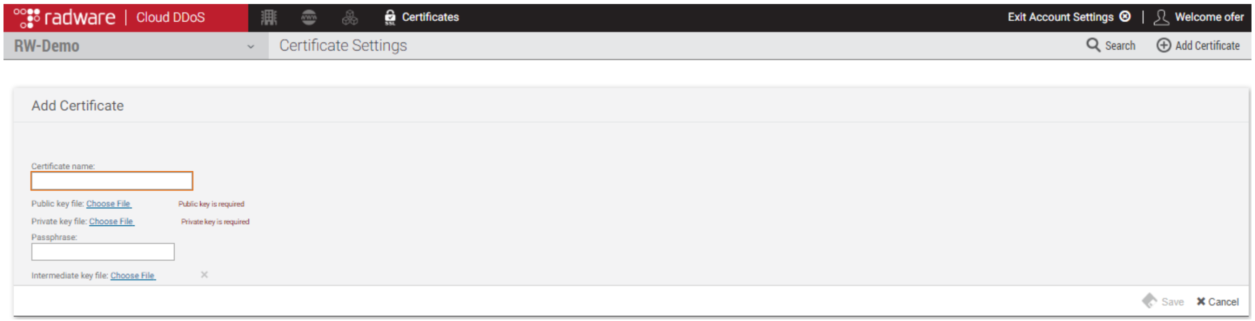
Adding SSL Certificates

Users with the Asset-Create or Site-Create roles can upload SSL certificate files to be assigned to server asset domains.

To add an SSL certificate

1. From the *Radware Cloud DDoS Protection Services* window, click the drop-down list at the far-right top corner of the window header and select **Account Settings**.
2. Click the **Add Certificates** icon, located towards the center of the window header.
3. To add a new certificate, at the right-hand side above the *Certificates Settings* table, click **+Add Certificate**.

   Note: Mandatory fields are highlighted in red. If you do not complete all mandatory fields, you cannot Save the new SSL certificate.



Public key is required

Private key is required

4. Configure the certificate parameters:

Table 5: Certificate Parameters

Parameter	Description
Certificate Name	Enter a name for the certificate.
Public Key File	(Mandatory) Select the Public Key file to upload.
Private Key File	(Mandatory) Select the Private Key file to upload.
Passphrase	(Optional) Enter a passphrase to encrypt the certificate.
Intermediate Key File	(Optional) Select an Intermediate Key file to upload.

5. Click **Save**.
6. The Certificate Settings table displays the certificates that have been added to your account.

Note:

If you want to assign an SSL certificate to a server asset using HTTPS, make sure you have uploaded the SSL certificate to Cloud DDoS Protection Services.

Adding Assets

A protected asset is a network (IP subnet) or specific service (FQDN or IP address and port) that is protected by the Service. The *Assets* pane lets you manage information for protected assets.

Prerequisites:

- Only users that have the **Asset-Create** role can add an asset. Other roles only allow a user to view an existing asset. Only the Radware NOC can modify or delete an existing asset.

Notes:

- When an asset is created or deleted, the management system automatically configures the scrubbing center's networking devices with the asset-specific traffic diversion parameters.
- If you add a new asset that exceeds the number of assets as defined in your service plan, an error notification displays.

- If you want to assign an SSL certificate to a server asset, make sure you have uploaded the SSL certificate to Cloud DDoS Protection Services
- If you did not assign the SSL certificate when you added the asset, you can request the Radware NOC to do so.

To add an Asset:

1. From the *Radware Cloud DDoS Protection Services* window, click the drop-down list at the far-right top corner of the window header and select **Account Settings**.
2. Click the **Assets** icon, located towards the center of the window header.
3. To add a new asset, at the right-hand side above the Assets table, click **+Add Asset**.
4. For the **Asset Type**, select **server** or **network** as appropriate.
5. Configure the asset per the selected asset type (for server asset details, see Adding Server Asset; for network asset details, see Adding Network Asset).
6. To assign a site to the asset, click **+Add** at the far-right above the *Site* table, and set the site parameters.
7. Click **Save**.

   Notes:

   - You must submit the added asset for it to be considered for approval and eventually announce your asset via the Cloud DDoS scrubbing center. In addition, for network assets, the submittal must be accompanied by a relevant signed Letter of Authorization (LOA).
   - Mandatory fields are highlighted in red. If you do not complete all mandatory fields, you cannot **Save** the new asset.

Adding Server Asset

- Select Asset type **Server**.

Parameter	Description
Asset Settings	
Asset Name	User-defined name of the asset.
X-Forward	When selected, the X-Forward-For parameter (the original client IP address) is added to the HTTP header.
Domains	Domains assigned to the asset. To add a domain, click **+Add** and set the following parameters: • Domain — Enter the domain name. • Certificate — Select an SSL certificate to associate with the domain. For more information on how to upload SSL certificates, see Adding SSL Certificates.

Parameter	Description
Site Settings To assign a site to the asset, click **+Add** at the far-right above the Site table, and set the site parameters. The Radware NOC can assign multiple sites to an asset. Users who are not the Radware NOC can only assign one site to an asset. **Note:** Mandatory fields are highlighted in red. If you do not complete all mandatory fields, you cannot **Save** the new asset.	
Site Name	Site name assigned to the asset.
Site Real IPs	Displays a dialog box to add real servers related to the site, including: • Real FQDN/IP Address—The FQDN or IP address of the real server. ▪ Protocol—The protocol used by the real server. Default: TCP **Note:** Only the Radware NOC can modify this parameter. ▪ Port—The real server port. For users who are not the Radware NOC, values are limited to: 80, 8080, 8081, 443 If you want to delete an entire Real FQDN/IP Address entry you are adding, or one of the sub-entries for that Real FQDN or IP address, click the red x icon for that entry or sub-entry. After setting the parameters, click **Update Table**.
Policies	Names of the policies assigned to the asset. For multiple policies, separate the policy names by a comma (“,”). These are the policies that are synced with the Cloud DDoS service in peacetime and are used for immediate mitigation upon diversion to the Radware scrubbing center. **Example policy1, policy2, policy3**
Additional policies	Additional policy names associated with CPE assets. For multiple assets, separate the asset names by a comma (“,”). **Example asset1, asset2, asset3**

Parameter	Description
Site Health Check	To add a site health check, click **+Add** above the **Actions** column. Health check type: Values: Ping, URL **Note:** limited to 5 health checks
Monitored Object	Based on the **Site Health Check** you selected, set the **Monitored Object** value: • If the **Site Health Check** is **Ping**, set the IP address to monitor. • If the **Site Health Check** is **URL**, set the URL to monitor. You can set the full site with the “http” or “https” protocol prefix. If you do not include a prefix, by default the protocol is HTTP.
Actions	If you want to delete a health check you are adding, click the red x icon for that health check.

Protecting Assets on AWS

Radware offers Cloud DDoS protection service to protect applications hosted on AWS with integrated, unified protection across data centers and public cloud environments. This provides organizations that host their applications on a mix of on-premises and public Cloud environments, unified DDoS protection with consistent security policy and a single pane-of-glass. This includes a single emergency response team and focal point, a unified Web security portal, single reporting tool and single DDoS protection technology across premises- and cloud-based protections.

In addition to its robust DDoS protection offering for premises and private Cloud-based applications, Radware provides applications hosted on public Clouds with the widest protection from the full breadth of DDoS attacks with real-time mitigation and no added latency in peacetime. The offerings include:

- Always-On Cloud DDoS Protection Service for applications hosted on AWS where the application's traffic is constantly routed through Radware's Cloud scrubbing centers providing real-time attack detection and mitigation.

  Onboarding of this mode is done using the usual Always-on process.
- On-demand Cloud DDoS Protection Service for applications hosted on AWS.

  The capability is based on DNS diversion onboarding.

  For information on the installation procedure, refer to the *Hybrid and Cloud DDoS On-Demand for AWS Getting Started Guide*.
- Hybrid Cloud DDoS Protection Service for applications hosted on AWS.

The capability is based on DNS diversion onboarding.

For more information on the installation procedure, refer to the *Hybrid and Cloud DDoS On-Demand for AWS Getting Started Guide*.

Adding Network Asset

- Select Asset type **Network**.

Parameter	Description
Asset Settings	
Asset Name	The auto-generated name of the asset.
Domain Name	Domain name assigned to the network asset.
AS for BGP Advertising	Adds the customer AS number to BGP announcements. This gives the customer the flexibility to add the customer's ASN in addition to Radware's ASN when diverting the traffic to Radware's scrubbing center. **Note**: Only the Radware NOC can modify this parameter.
IP Address/Net Mask	Protected network address and net mask. **Note**: 192.168.179.0/24
Download LOA Template	When you add an asset, you first must submit it for approval (see step 9). In addition to submitting the addition for approval, you must have submitted a signed LOA (Letter of Authorization) to Radware to complete the approval process. You can download a temple for this LOA by clicking **LOA Template**.
Upload Signed LOA	After signing the LOA (Letter of Authorization), you have the choice to either upload the LOA to the system, or fax it to Radware for approval. If you want to upload it to the system, click **Upload Signed LOA** and upload the file from your local system.
Site Settings To assign a site to the asset, click **+Add** at the far-right above the Site table, and set the site parameters. The Radware NOC can assign multiple sites to an asset. Users who are not the Radware NOC can only assign one site to an asset. **Note:** Mandatory fields are highlighted in red. If you do not complete all mandatory fields, you cannot **Save** the new asset.	
Site Name	Site name assigned to the asset.

Parameter	Description
Policies	Names of the policies assigned to the asset. For multiple policies, separate the policy names by a comma (“,”). These are the policies that are synced with the Cloud DDoS service in peacetime and are used for immediate mitigation upon diversion to the Radware scrubbing center. **Example policy1, policy2, policy3**
Additional policies	Additional policy names associated with CPE assets. For multiple assets, separate the asset names by a comma (“,”). **Example asset1, asset2, asset3**
Site Health Check	To add a site health check, click **+Add** above the **Actions** column. Health check type: Values: Ping, URL **Note:** limited to 5 health checks
Monitored Object	Based on the **Site Health Check** you selected, set the **Monitored Object** value: • If the **Site Health Check** is **Ping**, set the IP address to monitor. • If the **Site Health Check** is **URL**, set the URL to monitor. You can set the full site with the “http” or “https” protocol prefix. If you do not include a prefix, by default the protocol is HTTP.
Actions	If you want to delete a health check you are adding, click the red x icon for that health check.

Running Diversion Tests

By default, diversion tests are allowed to be exercised via the portal. This lets customers test and verify the networking aspects of the new site and enables the site to become operationally active almost immediately, saving valuable time.

Prerequisites:

A user who has the **asset-creator** role can self-run a diversion test to determine if the diversion configuration is working as expected.

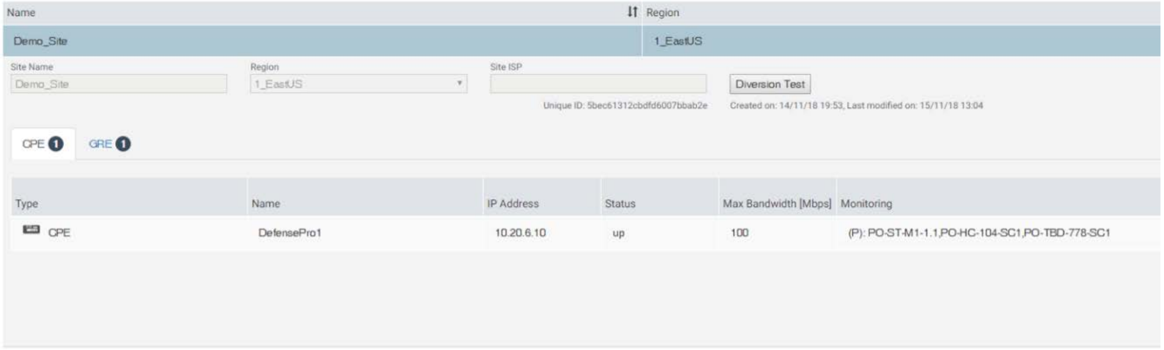
Only one diversion test is allowed per site and only for one asset. During this time the asset is diverted for up to four (4) hours and customers cannot perform any DDoS attack simulation during this time.

Note: A diversion test will not be deducted from the real mitigation quota if the number of diversions is limited.

The **Diversion Test** button is not visible if the site is being added or modified or if any of the assets are being diverted.

To run a diversion test

1. From the *Site Settings* pane, click **Diversion Test**.



Name	Region
Demo_Site	1_EastUS

Site Name: Demo_Site
Region: 1_EastUS
Site ISP:

Unique ID: 5bec61312cbdfd6007bbab2e
Created on: 14/11/18 19:53, Last modified on: 15/11/18 13:04

Type	Name	IP Address	Status	Max Bandwidth [Mbps]	Monitoring
CPE	DefensePro1	10.20.6.10	up	100	(P): PO-ST-M1-1.1,PO-HC-104-SC1,PO-TBD-778-SC1

   The *Diversion Test* dialog box displays.

2. Select the asset to be tested.
3. Click **Divert**. The Diversion Test runs.
4. After 4 hours the diversion will automatically be deactivated.

   If you have any issues or questions while the test is running or after completed, contact the Radware NOC/SOC team.

Note: The customer must execute a full Service Validation Procedure together with Radware to ensure that the service is configured appropriately to safeguard the customer's protected assets. The service will commence on the earlier to occur of: (i) the **Onboarding Completion Date** or (ii) if the customer fails to complete its onboarding obligations pursuant to section, immediately upon the lapse of 10 calendar days from the date of the initial Purchase Order for the Service (as applicable the "**Service Start Date**").

North America
Radware Inc.
575 Corporate Drive
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: 972 3 766 8666