

Network Onboarding Form

MSNS-R-001.doc

Revision Date: 03/06/2026

Welcome to MacStadium! This network provisioning form collects vital data necessary for accessing MacStadium cloud services.

Complete and submit via your account team member or via support ticket in the customer portal.

NOTE: Rework from inaccurate information may result in Professional Services charges.

Customer Information

Company Name:

Primary Contact

Name:

Email:

Role:

MacStadium Cloud Service

Please select the preferred cloud service:

☐

Bare Metal

(Mac Hardware)
RFC1918 Private /24

☐

Orka

Default Private /23
10.221.188.0/23

☐

Private Cloud

(non-Mac)
RFC1918 or Public /28

☐

Custom network address (if required to prevent IP overlap):

/ CIDR:

Connecting to MacStadium

Select the network access connection option:

☐

Option 1: Point-to-Site VPN

P2S VPN from workstation using Cisco AnyConnect.

Pros: Easiest setup, works on any machine

Cons: Not for long-term/enterprise use

☐

Option 2: Public IPs with Whitelist

Firewall accepts traffic from approved IPs only.

Pros: Minimal networking config needed

Cons: Minor charge per node, 5-day SLA

☐

Option 3: IPsec Tunnel (Site-to-Site VPN)

Most secure - extends your network to MacStadium.

Pros: No public IPs, well documented

Cons: Encryption overhead, longer lead time

☐

Option 4: Other

Other options for production systems.

POCs must use options 1-3.

Describe below:

For Site-to-Site VPN (Option 3): Do you have access to a network engineer for IPsec config?

☐

Yes

☐

No

☐

Need assistance from MacStadium

Network Onboarding Form

IPsec Tunnel Configuration

Complete this section if you selected Option 3 (Site-to-Site VPN). Requires network engineer input.

Documentation: <https://support.macstadium.com/hc/en-us/articles/28297916166683-Site-to-Site-VPN-Config>

VPN Type: ☐ Route-Based ☐ Policy-Based

Route-Based Configuration

☐ Static

Network-1:

Network-2:

☐ Dynamic (BGP)

AS-1 (Source):

AS-2 (Dest):

☐ Virtual Interface IP

Network Address:

Interface-1 (A):

Interface-2 (B):

Policy-Based Configuration

Peer IP Address:

Encryption Domain:

Remote-side IP:

Local-side IP:

VPN Negotiation Parameters

Phase 1 (IKE)

Encryption Type:

- ☐ Symmetric-key
☐ Public-key
☐ Handshake (RSA)
☐ Secure Hash (SHA)

Hash/Integrity Type:

- ☐ MD5
☐ SHA-1
☐ SHA-2
☐ NTLM
☐ LANMAN

Diffie-Hellman Group: Group#: Bits:

Auth Type: (Pre-shared preferred)

Lifetime:

Phase 2 (IPsec)

Encryption Type:

- ☐ DES
☐ 3DES
☐ AES
☐ AES-GCM

Hash/Integrity Type:

- ☐ MD5
☐ SHA-1
☐ SHA-2
☐ NTLM
☐ LANMAN

Lifetime:

PFS Group Value:

Network Onboarding Form

Public Cloud Connection

If connecting to a public cloud, specify the provider:

☐ AWS

☐ Azure

☐ GCP

☐ Other

If Other, specify:

Public IP Whitelist Configuration (For Option 2)

Source IP addresses/ranges to be whitelisted (use CIDR notation, e.g., 192.168.1.0/24):

What services do you need to access?

☐ SSH (22)

☐ HTTPS (443)

☐ RDP (3389)

☐ VNC (5900)

☐ HTTP (80)

☐ Custom:

(e.g., 8080, 3000-3010)

What MacStadium network/IPs will you access?

Traffic Direction:

☐ Inbound (to MacStadium)

☐ Outbound (from MacStadium)

☐ Both

Additional Considerations

Any specific requirements or details about your VPN setup:

Network Onboarding Form

Internal Use Only

This section is for MacStadium internal use. Customers may leave blank.

Received By:

Date:

Assigned Engineer:

Implementation Notes:

Validation Checklist:

- ☐ Customer information complete
- ☐ Service type selected
- ☐ Connection option selected
- ☐ IPsec parameters complete (if Option 3)
- ☐ Network engineer confirmed (if Option 3)
- ☐ Whitelist IPs, services, and traffic direction provided (if Option 2)
- ☐ Implementation timeline communicated