Credential Recovery & Corporate VPN Endpoint Setup Guide

This document outlines standard operating procedures for establishing secure Virtual Private Network (VPN) tunnels to Sunrise Health corporate enclaves, and recovering lost client credentials.

To satisfy corporate governance guidelines and ensure complete data isolation, all employees, on-site contractors, and technical operations staff must use approved MFA-hardened endpoints described in this guide.

RESTRICTED CONNECTION PARAMS: This instruction set contains cryptographic initialization parameters, client profile usernames, and gateway addresses. Storing this on unencrypted external media or sharing it outside authorized IT teams will trigger automated threat alerts.

Version	Date	Author	Change Description	Status
v2.0	2026-05-12	net-sec-admin	Initial guide release	Approved
v2.1	2026-05-19	sec-ops-lead	Updated gateway CIDR blocks and rotated client certificate keys	Approved
v2.2	2026-05-26	sec-ops-lead	Updated gateway CIDR blocks and rotated client certificate keys	Approved
v2.3	2026-06-02	sec-ops-lead	Updated gateway CIDR blocks and rotated client certificate keys	Approved
v2.4	2026-06-09	sec-ops-lead	Updated gateway CIDR blocks and rotated client certificate keys	Approved
v2.5	2026-08-10	sec-ops-lead	Updated gateway CIDR blocks and rotated client certificate keys	Current Version

2. Connection Provisioning & Endpoint Registration Workflow

Technicians must run through the connection provisioning workflow below to register their local endpoints with the security perimeter.

Failure to complete MFA validation within three (3) consecutive attempts will lock the account on the Active Directory Domain Controller and require a manual service ticket.

Phase	Activity Title	Step-by-Step Technical Requirements	Required Level
Step 1	Client Selection	Download corporate-signed AnyConnect or OpenVPN Wrapper from software catalog	Required
Step 2	Gateway Input	Input the exact gateway IP or resolving DNS domain matching your region	Required
Step 3	SSO Challenge	Enter corporate SSO credentials and accept the Okta/Duo push prompt	Required
Step 4	Recovery Check	If credential recovery is required, input the Master Key listed on Page 3	Conditional
Step 5	Verify Tunnel	Ensure ping connectivity succeeds to `dns-primary.corp.internal`	Required

3. Regional VPN Endpoints & Provisioning Keys

This key registry lists the regional VPN endpoints, default administrative portal gateways, and the initial onboarding tokens allocated for endpoint provisioning.

These keys expire every seven calendar days. If your onboarding token has expired, contact the IT service desk to request a temporary credentials rebuild.

VPN Endpoint / Gateway	Access URL / Gateway IP	Provisioned Username	Recovery Master Key	Temporary Setup OTP	Required Auth Type
Corporate IPSec VPN Gateway	10.32.79.108	vpn-setup-herrerasean	3664-7015-2757-9750	650255	SSO + Duo MFA
Azure Portal OpenVPN Portal	10.165.209.236	vpn-setup-robert75	3857-6255-7268-7310	361914	Certificate + Pin
AWS Client VPN Endpoint	10.171.217.211	vpn-setup-jilljones	4931-8198-6387-1620	410550	SSO + Duo MFA
Global SSL-VPN Gateway (Okta SSO)	10.38.134.139	vpn-setup-englishrobert	9209-4863-2607-8126	202682	Certificate + Pin
FortiGate Edge Firewall (Client Portal)	10.225.240.38	vpn-setup-smithgarrett	6051-2798-7716-6945	681164	SSO + Duo MFA
Cisco AnyConnect Hub	10.65.164.95	vpn-setup-antonio32	3125-7088-9447-3847	486089	Certificate + Pin