

Service Installation: Customer Responsibilities Guide

March 2022

Table of contents

Your responsibilities for service installation	3
General responsibilities for all solutions	3
Project Management team	3
LAN	3
WAN	3
Service-specific responsibilities	4
Software Defined Wide Area Network (SD-WAN)	4
Managed Network Security (MNS)	4
XCaaS (General)	5
OfficeSuite UC®	6
XCaaS (Avaya)	6
Professional Services	6
Additional resources	6

Your responsibilities for service installation

To ensure a successful service implementation, we will partner with and guide you every step of the way. To get started, please review and confirm that your organization can support the following elements for the pending installation. If any of the items outlined below will be challenging to fulfil throughout the duration of the project, Windstream Enterprise may be able to provide additional resources via our Professional Services team.

General responsibilities for all solutions

Project Management team

- + Identify implementation team members, including your:
 - Project manager
 - Technical site contact for each location
 - Subject matter expert(s), as required
 - One or more security contacts that are authorized to make firewall policy change requests, as required
 - Technical resource for each test and turn up
 - Operations contact(s)
 - Billing contact(s)
 - Scope change management contact(s)
- + Provide project timing constraints for the development of the implementation plan (i.e., holidays, after hours, blackout dates, contractual commitments and implementation resources)
- + Supply all configuration and programming information in the Windstream Enterprise format
- + Prepare to be an active participant in the collection of information and complete implementation process
- + Provide a change control window for maintenance

LAN

- + Confirm information for each location to is up to date
- + Provide location, space, power, lighting and environment suitable for Windstream Enterprise managed devices
- + Provide inside wiring, extensions and cross-connections, as needed
- + Provide information about the hand-off to Windstream Enterprise managed devices:
 - Physical media and ports
 - Layer 2 specification for VLANs
 - Layer 3 protocol details and IP subnets addressing (public/private)
 - DHCP details (provided by you and Windstream Enterprise)
 - DNS details (i.e., provider, target IP, etc.)
 - Connectivity and access through customer-managed LAN environments
- + Disable SIP ALG (typically fixed wireless or modem)

WAN

- + Provide circuit details (contracted bandwidth, provider, and hand-off details).
- + Perform test and turn up of circuit from carrier prior to implementation of Windstream Enterprise services to ensure connection is functional.

Service-specific responsibilities

Software Defined Wide Area Network (SD-WAN)

- + Provide test and turn-up application policies:
 - Application name
 - Hosting location (i.e., premises, cloud, SaaS, etc.)
 - Match criteria details (i.e., source, destination or application group)
 - Action criteria details (i.e., priority, rate limit, dedicated path or steering)
- + Provide remote VPN access details:
 - Protocol (IPsec/SSL)
 - User authentication server details:
 - Type (i.e., local, LDAP, etc.)
 - Target (i.e., IP address, port and distinguished name)
- + Confirm NAT or PAT policies, as needed

Managed Network Security (MNS)

- + Ensure your technical resource attends pre-deployment planning calls to answer questions regarding your networking and security requirements, including:
 - Existing network topology, including existing firewalls and IP addressing
 - Internet outbound/inbound traffic filtering policies
 - Confirm NAT or PAT policies, as needed
 - DMZ (demilitarized zone) sub-network requirements
 - Web and application filtering
 - Site-to-site VPN configuration details
 - Remote access VPN and user authentication requirements (e.g., active directory integration)
 - Convert any existing firewall configurations to practical firewall rules/security policies
- + Provide estimated log volume and/or average events per second per device when threat monitoring is purchased with MNS Premium
- + Review additional requirements for MNS customer premises equipment (CPE) and Virtual Network Function (VNF):
 - Provide LAN ports for trusted MNS firewall (e.g., FortiGate) interfaces
 - Obtain any permits, licenses or authorizations required to deploy MNS CPE
 - Allocate a secure location with sufficient connectivity, power, space and ventilation (e.g., locked room or cabinet)
 - Provide Windstream Enterprise field technician access to the location where the MNS CPE will be placed
 - Securely store and promptly provide MNS CPE (i.e., FortiGate devices) sent to your site for Windstream Enterprise field technician(s) during scheduled installation
 - Ensure the Windstream Enterprise Cyber Security Operations Center (CSOC) can remotely use SSH and HTTPS to securely access FortiGate firewalls and SNMPv3 (read-only) for polling and traps
 - Provide “Smart Hands” when needed to assist the CSOC in troubleshooting a service-disrupting event
- + Provide routable IP address and desired port for Syslog server when this external logging method is required, as needed
- + Use the WE Connect Firewall/MNS Dashboard for web filtering, application control and remote access VPN user management
- + Present a private passcode to the CSOC for authentication when requesting a change to the MNS service

Service Installation: Customer Responsibilities Guide

- + Notify CSOC at least 24 hours in advance of the following events:
 - Network or security architecture configuration changes that may impact the operation of the MNS service
 - Uncommon network traffic that could generate false alerts (e.g., unscheduled backups, an anticipated increase in legitimate inbound web traffic)
- + Install Fortinet Single Sign-On (FSSO) for active directory integration, as needed
- + Provide end-user remote access VPN client support for computers and mobile devices
 - Client software installation
 - End-user identification and authentication:
 - Maintain users' list and passwords
 - Configure and maintain any external authentication technologies, including, but not limited to, RADIUS, TACACS, Active Directory and Multi-factor Authentication (MFA) servers or cloud-based services

XCaaS (General)

- + Provide PoE switches or order power supplies for IP phones
- + Provide make, model and specs for any third-party devices
 - *Note: All devices must have been discussed in pre-sales conversations for proper integration into the Windstream Enterprise solution.*
- + Ensure each phone has a cable back to the switch
 - *Note: There can be no daisy chained phones.*
- + Ensure your switches have GigE to support any GigE phones
- + Provide the following information if you have unified communications (UC) solutions:
 - Locations broken down by users
 - Locations that will have hardware
 - Dial plan review
 - Remote/telework users/agents
- + Provide the following information for all contact center agents:
 - Names of individual agents
 - Contact center supervisor information
 - Shift information for contact center staff
- + Identify contact center line of business owners:
 - Review contact center integrations
 - Provide detailed contact center call flows with documentation
 - Identify application ownership for points of integration
- + Provide secure location for delivery of onsite hardware (i.e., IP phones, gateways, etc.)
- + Tag the following devices, such as, but not limited to:
 - Door boxes
 - Overhead paging
 - Fax lines
 - Alarm lines
 - Modems
 - WAN devices
- + Confirm all numbers, including toll-free, for porting and directory listings, and provide the recent bill required for these numbers
- + Have at least 100 Kbps LAN/WAN bandwidth per call capacity per site for voice; more will be needed for additional functions
- + Confirm video conferencing recommended bandwidth:

Service Installation: Customer Responsibilities Guide

- For high-quality 1:1 calling: 600Kbps (up/down) and 1.2 Mbps (up/down) for HD video
- For high-quality group calling: 600Kbps/1.2Mbps (up/down) and 1.5Mbps/1.5Mbps (up/down) for gallery view

OfficeSuite UC®

- + Have any necessary public static IP addresses
- + Develop and maintain code to utilize our application programming interface (API)

XCaaS (Avaya)

- + Review statement of work (SOW) with your Windstream Enterprise project team
- + Review any third-party API requirements as a part of the SOW

Professional Services

- + Review statement of work (SOW) with your Windstream Enterprise project team

Additional resources

For support, please consult with your dedicated Windstream Enterprise project team. To learn more about Windstream Enterprise services, visit our [Terms & Conditions](#).

About Windstream Enterprise

Cloud-enabled connectivity, communications and security—guaranteed.

Windstream Enterprise drives business transformation through the convergence of our proprietary software solutions and cloud-optimized network to unlock our clients' revenue and profitability potential. Our managed services streamline operations, enhance productivity and elevate the experience of our clients and their end users while securing their critical data and brand reputation. Analysts certify Windstream Enterprise as a market leader for our product innovation, and clients rely on our unrivaled service guarantees and best-in-class management portal. Businesses trust Windstream Enterprise as their single-source for a high-performance network and award-winning suite of connectivity, collaboration and security solutions—delivered by a team of technology experts whose success is directly tied to our clients' complete satisfaction.

windstreamenterprise.com