

Forescout Pre-Installation Checklist

|  |
| --- |
| **[Customer]** |
| **Customer Point of Contact Name:** |  |
| **Email:** |  |
| **Phone:** |  |
| **Customer Address:** |  |
| **Delivery Dates:** |  |

# Company Proprietary Information

This document contains Forescout proprietary and confidential information and must be protected by the recipient accordingly. Its contents are not meant for general dissemination and may only be used by the recipient in connection with the services reflected in this document. No portion of this document may be reproduced, stored, transmitted or disclosed for any purpose to any third party without prior written consent from Forescout.
Please contact your account team if you have any questions.

# Introduction

This document covers the preparation and information gathering that must be completed prior to installing the Forescout platform. Most of this effort involves gathering the appropriate information, permissions and resources for the installation. This document consists of the following sections:

1. ActiveCare Support Credentials
2. Deployment Overview
3. Appliance Information
4. Network Information
5. Host Management Information
6. Assumptions

Please refer to the Statement of Work (SOW) document for information that clearly defines the scope of the project, establishes project milestones and deliverables, clarifies roles and responsibilities and outlines appropriate and agreed-upon change-control procedures. The SOW is based on information previously provided by the customer, and in part, on information possibly gathered through this document. Please discuss major changes to the infrastructure with Forescout Professional Services engineers to ensure a smooth implementation.

For training purposes, Forescout reserves the right to allow a designated engineer-in-training to accompany/shadow our professional services engineer throughout this engagement.

# 1. ActiveCare Support Credentials

ActiveCare is the overarching term to describe Forescout’s support and maintenance services. We’re dedicated to providing our customers and partners with timely, high-quality technical support. Our objective is to help customers alleviate issues, expand product use and optimize their value from Forescout’s solutions.

Did you receive your Active Care Support Credentials:   **Yes**   **No**

**Who is the entitlement admin for this account? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# 2. Deployment Overview

The following information ensures that the installation engineer understands the installation scope and is prepared for any additional plugins or unique customer requirements.

|  |  |
| --- | --- |
| Item | Comment |
| **Appliance Configuration Information** |
| **Approximate Total Number of Hosts:** This number can be estimated to the nearest thousand. | Number of **Total** Hosts:  |
| **Site Distribution:** Please indicate the location of appliances and if SPAN/mirror is required. Also indicate any appliances that are deployed as an HA pair. |  |
| HA pairs are typically used as a resiliency option for dedicated, focal appliances, and the EM/REM. For regular, non-specialized appliances, the typical resiliency solution is to utilize Failover Groups.If SPAN/mirror traffic is required for information-gathering, Forescout recommends an HA pairing of the SPAN appliances and/or utilizing a packet broker solution that can distribute SPAN/mirror traffic to multiple appliances. |
| **Internet Connectivity configuration:** Internet connectivity required for licensing and eyeExtend Connect apps (proxy, firewall, or IPS) |  |
| ***Why Internet connectivity?*** Forescout Enterprise Manager will need to contact Forescout licensing servers to validate customer licenses. |
| **Recovery Groups:** only if recovery license purchased. |  |
| **Network Topology**: (used for SPAN / Netflow)The Forescout platform should monitor traffic going to the DHCP, Active Directory, email servers and internet connections. Please indicate whether the Forescout platform will monitor this traffic in planned SPAN sessions. | * Internet Traffic:
* AD/LDAP Traffic:
* DHCP Traffic:
* Email Server Traffic:
 |
| If SPAN/mirror traffic will not be used, Forescout strongly recommends using DHCP relay statements on switches to send that information to the appliances. If SPAN/mirror traffic is unavailable. Forescout recommends utilizing flow traffic to provide appliances with IP address endpoint information and ports utilized in network communications.  |
| **Virtual Appliances:** Dedicated physical NIC and additional compute resources are required for each VM that will receive a SPAN session. SPAN should come directly from the switch to the physical NIC on the virtual appliance.Also indicate if on dedicated chassis or in environment with other hosts. |  |
| ***Why dedicated compute resources?*** Forescout virtual appliances are not like other Linux/Windows VMs in that they still expect to have full access to hardware components such as CPU, RAM, and HDD. If these resources are not dedicated, the platform will suffer performance degradation and is more likely to encounter production issues. |
| **Cloud Instance Appliances (Azure/AWS):** |  |
| **Will physical appliances need to be multi-homed?** Do appliances require interfaces in multiple user/management networks, independent of the iDRAC interface? |  |
| **OT Sensor Deployment Locations:** |  |

|  |
| --- |
| Point of Contact – Accessible and available contact while Forescout is working. |
| **Customer points of contact:** Forescout should have a dedicated resource available to the engineer capable of getting appropriate networking, Windows domain, security team and help desk resources as necessary. These are persons in addition to the one identified on page one, if needed. |
| Name | Position | Contact Information |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 3. Appliance Information

Please obtain this information for EACH appliance to be installed.

|  |  |
| --- | --- |
| Item  | Comment |
| **Appliance Configuration Information –** Used to configure the Forescout platform with basic setup information.  |
| **Appliance hostnames**: |  |
| **Company domain name(s):** For example, HOSTNAME.COMPANY.COM |  |
| **Appliances IP/Mask/Gateway:** This is used both for management and interaction with endpoints. It should have unfiltered connectivity to all devices on the protected network. Three IP addresses are required per High Availability pair. |  |
| **OT Sensor IP/Mask/Gateway:** |  |
| **SPAN port assignment:** example ETH1, ETH2, ETH3, etc.. |  |
| **OT Sensor SPAN port assignment:** |  |
| **Remote Management Module IP/Mask/Gateway:** This allows remote KVM access to the appliance via the iDRAC interface. Only applies to physical appliances. |  |
| **DNS server IP addresses:** DNS is used to perform reverse-name resolution of internal IP addresses. |  |
| **Administrator email address:** Administrative emails will be sent to this address. |  |
| **Mail relay IP address:** (optional) The appliance can also send alert emails using its internal SMTP server. Indicate it open relay or requires authentication.  |  |
| **NTP Server IP Address:** You can synchronize Forescout appliance(s) time with your timeserver.Designate separate NTP servers for IT and OT, if required |  |
| **Network Segments –** The segments allow you to use ranges within Forescout policies and filters. |
| **Company IP Assignments:** Please have ready all IP address ranges on the network that will be monitored by the Forescout platform along with their locations and designated purpose (e.g., PC, server, voice, etc.).  | IMPORTANT! Please include in separate spreadsheet. |
| **OT IP Assignments:** These are ranges with an operational technology presence that would be sensitive to NMAP scan or other probes | IMPORTANT! Please include in separate spreadsheet. |
| **Other known sensitive ranges:** (could possibly include servers, printers, IOT device ranges – typically these are excluded from vulnerability scan ranges) | IMPORTANT! Please include in separate spreadsheet. |
| Forescout recommends defining network ranges in a hierarchical manner, typically along regional/site lines, with specific network types defined below the site level, such as wired, wireless, server, printer, OT, mixed/miscellaneous, and other such IP range functions.Example:Americas Region* Chicago Site > Wired Ranges > Wireless Ranges > Server Ranges > VoIP Ranges
* Kansas City Site > Wired Ranges > Wireless Ranges > VoIP Ranges > Manufacturing Ranges
 |

# 4. Network Information

This information is necessary to allow the Forescout platform to communicate with your network infrastructure:

|  |  |
| --- | --- |
| Item | Comment |
| **Managed Switch Information –** Used to query network equipment for information and optionally take actions |
| **Switch Vendor:** Vendor of the switches to monitor. |  |
| **L2 Switch IP Address:** these are dedicated in the access switch role. (MAC address table) | IMPORTANT! Please include in separate spreadsheet. |
| **L3 Switch IP Address:** these are dedicated Core/Distribution/Routers devices. (ARP table) | IMPORTANT! Please include in separate spreadsheet. |
| **L2/L3 Switch IP Address**: these are switches with both access and distribution roles such as stacks or chassis switches. (both MAC and ARP) | IMPORTANT! Please include in separate spreadsheet. |
| Forescout requires information from the access and distribution switches to retrieve IP and MAC address information on endpoints. Without this information, Forescout will not be able to reliably link discovered IP addresses with MAC addresses. Also, the MAC address is a key piece in identifying the function of an endpoint, so it is vital for providing full visibility. |
| **VLANs:** List VLANs you wish to monitor or specify ALL. (for Span traffic) |  |
| **SNMP Community String / V3 credentials:** Please have this ready and verify SNMP Read is enabled on the switches you wish to monitor as needed. Write permission will be needed for control. |  |
| **SSH/Telnet Credentials:** Please have this ready and verify CLI Read or Write access is enabled on the switches you wish to monitor as needed. | DO NOT RECORD PASSWORDS HERE! |
| **SNMP Trap Configuration:** Configuration of port up/down and MAC notification traps sent to appliances managing switch. (if supported by switch vendor) | DO NOT RECORD PASSWORDS HERE! |
| Forescout will require SNMP and CLI access to most switch vendor platforms in order to retrieve endpoint information. During visibility phases of implementation, Read-Only access is sufficient. For control actions impacting network access, Read-Write access will be required for either SNMP, CLI, or both modes of access. |
| **VPN:** Provide the make and model of your VPN appliance, IP address and Radius/SNMP configuration as needed. |  |
| **Wireless Vendor:** Vendor of the WLCs to monitor. |  |
| **Wireless IP address:** Controller/Access Point IP Address(es)  | IMPORTANT! Please include in separate spreadsheet. |
| **Wireless SNMP/CLI credentials:** Please have this ready and verify SNMP Read is enabled on the WLCs you wish to monitor as needed. Write permission will be needed for control. |  |
| **DHCP Relay:** Identify Forescout appliances that will receive DHCP packets |  |
| If not provided via SPAN/mirror traffic monitoring, Forescout strongly recommends specifying one or more appliances as recipients of DHCP requests. Forescout will not respond to such requests and will therefore not interfere with DHCP address assignments. Forescout uses the DHCP request packet to identify endpoint-specific information regarding vendor, operating system, and versioning information. |
| **Netflow:** Identify Forescout appliances that will receive Netflow (optional) |  |
| **VOIP:** Make and model of VOIP phones. If enduser devices are connected through VOIP devices then extra switch configurations are needed. example: MAC address add is need per interface. |  |
| **Security Devices Inline (Firewall, IPS, Proxy):** Any device that would potentially block or alert on Forescout activity such as NMAP scans or multiple logon attempts to endpoints |  |
| **Security Routing Infrastructure:** Any routing considerations between Forescout appliances and end-user endpoints, switches, integrated systems |  |
| Forescout engages in NMAP scanning and repeated logins that other security systems can identify as hostile behavior if Forescout is not exempted from alerting. Other security systems, likewise, can appear to Forescout as threats if not exempted in Forescout. Forescout will also require permissions to traverse security infrastructure without incident or alerting. If there are complications in routing that could adversely impact Forescout traffic, we want to call them out here so that they can be addressed in the overall design. |

# 5. Host Management Information

This information allows the Forescout platform to query Active Directory for user information and to query domain hosts for endpoint information.

|  |  |
| --- | --- |
| Item | Comment |
| **Active Directory Setup –** Used to query LDAP for user information |
| **Directory Server Address, Service Account and Password:** This account allows the Forescout platform to retrieve user information from Active Directory. Also, this integration will allow to use company logins. (This will be a separate account from the HPS account.) Indicate if TLS is used in connecting to AD. | DO NOT RECORD PASSWORDS HERE! |
| **AD domains with trust relationships:** |  |
| **AD domains without trust relationships:** |  |
| For AD domains with trust relationships, Forescout recommends a single account in a trusted domain for Windows host manageability, below. This account needs to be a separate account from the account used in the User Directory object to look up account info. For AD domains without trust relationships, Forescout recommends either a second HPS account for those domains, preferably one that is geographically limited if at all possible, or utilization of the SecureConnector agent to administer Windows endpoints in untrusted domains. |
| **Host Property Scanner Setup –** Used to query domain hosts for endpoint information |
| **Preferred Host Manageability Options:** Options available for managing endpoints include:* Domain account or SecureConnector™ agent for Windows assets
* SSH username/key or SecureConnector agent for Mac/Linux endpoints
 |  |
| **SSH Account and Key Installation:** Required for agentless manageability of Mac/Linux hosts. |  |
| **Domain Service Account and Password:** This username should be a domain account in the local administrator group of endpoints to be managed. (This should be a separate account from AD server account.)Also need to ensure:* Access from appliances to endpoints on ports 135/139/445
* Remote Registry Service or WMI, RPC and Server service to be started.
* Access to C$ admin share

Please indicate if any of the above requirements are not available or if there are any workstations/Servers with a regulatory-mandated configuration.Also indicate if Kerberos is required for logging on to Windows workstations over the network. | DO NOT RECORD PASSWORDS HERE! |
| **List of Authentication Servers –** Used to gather username information and for some policy conditions. |
| **Authentication Server List:** Please have the IP address of each Active Directory and Exchange server ready to input into the Forescout platform. (used with SPAN or Captive Portal configurations.) |  |
| **Host Access and Compliance Criteria –** Used to gather username information and for some policy conditions. |
| **Preferred Admittance Criteria:** Please indicate what criteria you have in mind or have discussed with Forescout engineers for determining whether a host should be part of the network. |  |
| **Preferred Compliance Criteria:** Please indicate what criteria you have in mind or have discussed with Forescout engineers. |  |

|  |  |
| --- | --- |
| Item | Comment |
| **Optional Items –** Not required for initial installation/configuration |
| **SCCM Connection Credentials:** Read-only account for accessing SCCM database. | DO NOT RECORD PASSWORDS HERE! |
| **VMWare VSphere account:** Account used to gather information from the VM environment hosted on VMWare ESXi servers. | DO NOT RECORD PASSWORDS HERE! |
| **For eyeExtend Modules, please consult with Forescout regarding configuration details. Information on the modules is available at the Forescout support and documentation portal.** |  |

# 6. Assumptions

Forescout will make the following assumptions:

* All information requested in this document is provided and ready.
* All endpoint issues and changes will be the customer’s responsibility.
* The customer will provide all necessary patch cables.
* All equipment required for connectivity is available and configured before installation, such as switches, routers and any infrastructure devices.
* Internet connections are up and operational before installation (if required for final testing)
* The Forescout platform will be installed with identically configured Monitor and Response ports, trunked and 802.1q tagged for the switch on which it is installed unless previously discussed and agreed to by a Forescout engineer. If the switch is part of a switch pair, both switches will have a Monitor and Response port. A separate Management port will connect into the same switch as the Monitor and Response ports.

# 802.1x Information

|  |  |
| --- | --- |
| Authentication (general): | Scope: |
| 802.1X on wired network:    **Yes**   **No** |
| 802.1X on wireless network:    **Yes**   **No** |
|  |  **Wired** |  **Wireless** |
| **Authentication Method** |  User  Computer Certificate N/A |  User  Computer Certificate N/A |
| **Guest Access** |  Yes  No |  Yes (requires user account) No |
| **Internal Network – Permitted devices:** |  Windows Macintosh Linux/Unix |  Windows Macintosh Linux/Unix Mobile |
| **Any other VLANs/access levels beyond guest/internal? Please describe.** |  |  |
| **RADIUS Parameters** | Local RADIUS Authentication Port: \_\_\_\_Local RADIUS Accounting Port: \_\_\_\_Using the bundled RADIUS Server?   **Yes**   **No****If YES:** Choose “User Directory Server Name” (the choices are pulled directly from the info in your User Directory Plugin)**If NO:** Choose “Proxy to external RADIUS”* Primary RADIUS Address: \_\_\_.\_\_\_.\_\_\_.\_\_\_
* Secondary RADIUS Address: \_\_\_.\_\_\_.\_\_\_.\_\_\_
* RADIUS Timeout in seconds: \_\_\_\_
* (External) RADIUS Authentication Port: \_\_\_\_
* (External) RADIUS Accounting Port: \_\_\_\_
* RADIUS Server Secret: \_\_\_\_\_(Does not need to be given until on-site install/configuration)
 |

|  |  |
| --- | --- |
| Plugin Assignment:(This is for the MAR – You can assign additional settings here for) | Desired time out for 802.1x actions (in seconds): \_\_\_\_Do you have a MAC Address Repository (MAR?):   Yes   No(This determines if we need to generate a list of MACs without proper supplicants – for example: printers or legacy devices)Do you want to DENY access as the default secondary action if a host times out a RADIUS authentication request? |
| **Server Certificate Info** | Are you using Self-Signed Certs?   **Yes**   **No**If NO: You will need to generate a CSR from the Forescout platform in order to validate against incoming certificates to your CA.Parameters you will need:Encryption Algorithm:   **sha1**   **md5**CA Host Operating System:   **UNIX-based**   **Windows Based**Private Key: \_\_\_ (not necessary in this file)Subject Server Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Subject Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Organization Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Country Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_State or Province: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Locality Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Additional Items** | Are you using any devices (VoIP phones) which could lose connection if a port up/down action takes place to force re-authentication?   **Yes**   **No**If yes, describe: Do you have an OCSP?   **Yes**   **No**OSCP URL: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Do you want cache authentication requests for fast authentication?   **Yes**   **No**If YES:How many requests should be cached (Default: 24)? \_\_\_\_\_\_Maximum desired sessions: \_\_\_\_\_\_Dynamic Authorization Port #: \_\_\_\_\_\_ (Default 3799) |

**Copyright © 2021 by Forescout Technologies, Inc.**

© 2021 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

Photography, illustration, video, audio, text and computer programs which constitute and are incorporated into Forescout documents, discussions, presentations and publications (‘Content’) are copyright protected by Forescout or other owners and/or representatives. Distributing, downloading, screen capturing, recording or copying this Content in any manner for any use other than personally viewing the original Content in its entirety is prohibited by copyright law. Any reproduction of the Content requires written approval by the Content owner.

**Notice to U.S. Government End Users**

Forescout Hardware, Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202,as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. § §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.