FORESCOUT

Forescout

Research and Intelligent Analytics Program

Data Security Document

Version 19.1.6

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-07-08 11:55

Table of Contents

About the Forescout Research and Intelligent Analytics Program

The goal of the Forescout Research and Intelligent Analytics Program (the 'Program') is twofold:

1. To improve the capabilities of the Forescout platform through telemetry for all Forescout customers.
2. To perform and publish research on industry, geographical, and global trends in enterprise network security.

Collecting endpoint data and associated environmental information from customers to the Forescout Device Cloud enables Forescout to use machine analytics as well as human researchers to improve the quality of its classification capabilities. This both improves the accuracy of existing classification profiles and better enables the creation of new profiles. Ongoing research constantly improves the Forescout platform's ability to assess endpoint posture based on the analysis of the data collected. The data also lets Forescout better understand the state of enterprise networks and ensure that it develops the right tools and features to help secure these networks. As a public service, some of this information may be published for market research in aggregated and totally anonymized forms.

Relevancy

Applies to the following versions:

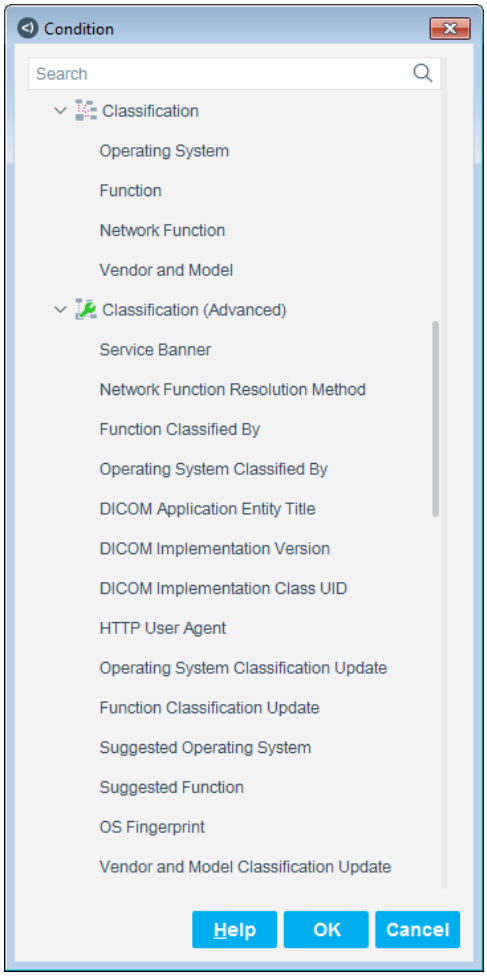
- Forescout version 8.0.1 with Device Profile Library 19.0.6
- Forescout version 8.1 with Device Profile Library 19.1.6 and Hybrid Cloud Module 2.0

Program Details

The Forescout platform internal database keeps track of the endpoints in your environment, associated endpoint properties, and environmental information regarding the endpoint domain. A 'property' is a name-value pair that describes a given attribute relating to that endpoint. Each deployment is unique in terms of the environment in which it runs, the plugins and modules that are installed, the version of the software running and the network access given to the product. The set of properties that the Forescout platform tracks for each endpoint differs between environments, and may even differ for endpoints within a given environment.

In general, customers can see which properties the Forescout platform can resolve in their environment by looking at the conditions available when creating or editing a policy condition. The actual properties that are resolved depend on the configuration.

Along with the specific properties utilized by Forescout platform policy conditions, some properties may be automatically resolved. The following shows a sample of policy conditions that may be available in your environment.



The Forescout platform also requires user configuration to communicate with network infrastructure and other third-party services. The relative amount of use of different components in the Forescout platform and the ability of Forescout to solve for use cases, depends on this configuration. To better understand and optimize the platform for Forescout customers, it is important to collect some configuration information specific to each customers' environment. The information of interest relates to how the various third-party services are configured (unrelated to credentials or any other authentication-related information), and how intensively they are used.

Under the Program, you may let the Forescout platform upload to the Device Cloud certain data about your endpoints and their properties with Forescout, in addition to the environmental configuration information described above.

Data Sanitization

The Forescout platform sanitizes the data it collects before uploading it to the Forescout Device Cloud. The data consists of certain Forescout platform properties for all endpoints discovered by the Forescout platform in your environment, together with the environmental information described in this document. The data that is uploaded does not contain any Personally Identifiable Information (PII) of the endpoint users in your environment. Additionally, Forescout takes great effort to ensure that no data that could identify your organization is stored with the uploaded data. Most identifying information is either removed or anonymized prior to upload. Minimal customer identifying information is required for authentication during the upload process. This information is stripped from the uploaded data before it is saved to a disk.

The uploaded data is divided into the following three groups:

Group	Upload Status	Description	Examples
PII	**Never Uploaded**	Any data that contains information about the user of the endpoint.	Properties such as: User, Email, Last Name, Guest User Name. Environmental data such as: credentials for connecting to a Cloud provider.
Sensitive Data	**Anonymized Prior to Upload**	Any data that may reveal sensitive information about your environment. See Properties Anonymized before Upload and Additional NetFlow Properties Anonymized before Upload.	Properties such as: IP Address, MAC Address, Hostname, and internal DNS properties.
Generic Data	**Uploaded 'As Is'**	Any data that does not contain Sensitive Data, but can be used to characterize endpoints or the environment in which Forescout is configured. See Properties Uploaded 'As Is', Aggregated Cloud Deployment Data, and Additional NetFlow Properties Uploaded 'As Is'.	Properties such as: Linux Version, Windows Cloud Application Installed, DHCP Vendor Class, Manual Classification. Environmental data such as: the number of AWS accounts configured.

Data Anonymization Process

For properties in the Sensitive Data group, the Forescout platform employs an anonymization process prior to uploading the data to the Forescout Device Cloud. The process works as follows:

- All IP addresses discovered by the Forescout platform are re-enumerated such that each endpoint is given a unique 'fake' IP address. This 'fake' IP address is maintained in order to identify and track the endpoint data post-anonymization. Those outside your Forescout platform environment cannot use these 'fake' IP addresses to reverse engineer the actual IP addresses of the endpoints in your environment.
- The first 36 bits of MAC addresses are maintained so that this portion of the address can be used to identify the NIC vendor, which is useful for classification. The remaining 12 bits of all MAC addresses are hashed.
- Actual hostnames and DNS names of endpoints in your environment are not uploaded; however, metadata may be extracted from the names and uploaded. For example, if an endpoint's name starts with 'dc', the metadata might note a possible indication of a Domain Controller (due to the common practice of naming conventions). This information is useful in classifying the endpoint as a Windows server.

Upload Methodology

When the Forescout platform is ready to upload the data, the data is sanitized, anonymized and compressed, and then uploaded to the Forescout Device Cloud. If you have an Enterprise Manager, the data is uploaded via the Enterprise Manager; otherwise your standalone CounterACT® Appliance uploads the data. The Forescout platform employs mutual authentication to help ensure that it uploads data to Forescout's servers only, and not to another site that may attempt to spoof it.

Server Details

The Device Cloud is hosted by Amazon Web Services (AWS). The server that your Enterprise Manager or standalone Appliance connects to is ds.forescout.com, and all connections are over HTTPS (port 443/TCP).

Upload Frequency

Each standalone Appliance or Enterprise Manager will attempt to upload data in bulk every 24 hours. If an upload fails for any reason, no attempts will be made to upload the content until the following day.

Bandwidth Used

The amount of data uploaded from your environment to Forescout is dependent on the following primary factors:

- The number of endpoints in your environment. The more endpoints, the greater the amount of data.
- Which plugins and modules you have installed. Although not all host properties are uploaded, in general, the more host properties that are resolved for your endpoints, the greater the amount of data to be uploaded.

The following table provides an estimated baseline of how much bandwidth is used per upload, which depends on the number of endpoints discovered by the Forescout platform and the number of properties to be uploaded. The table assumes an average of 14 uploaded properties per endpoint. See Appendix A – Data Uploaded to the Forescout Device Cloud for a complete list of properties that may be uploaded.

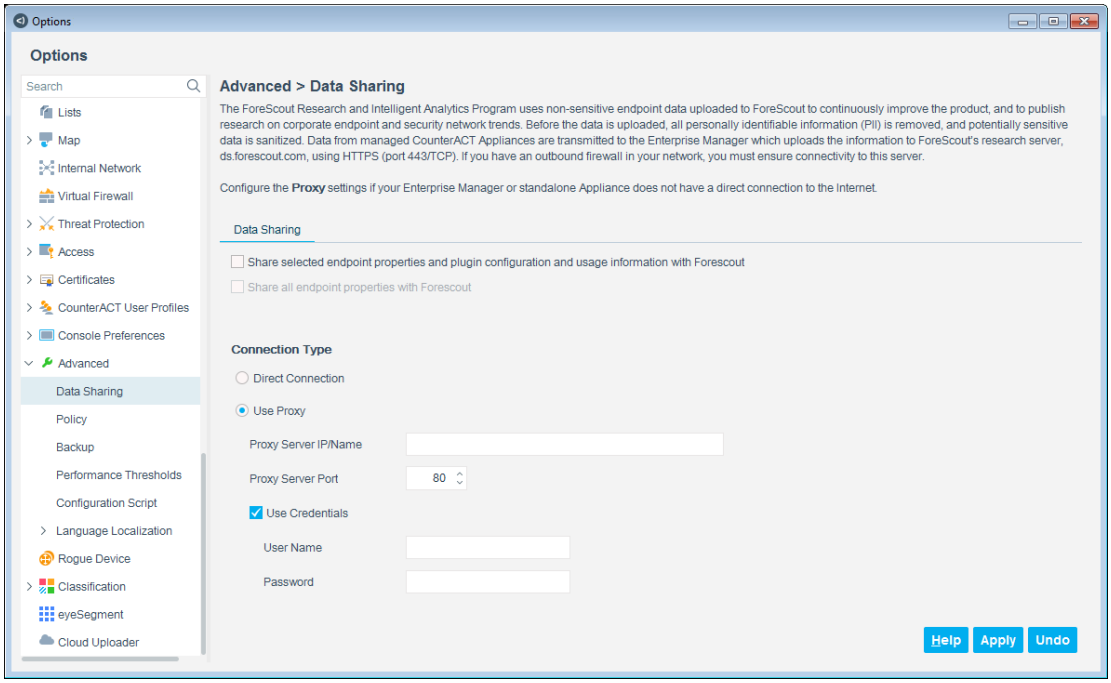
Number of Endpoints Managed by the Appliance	Bandwidth Used per Upload
1	4KB
10	5KB
100	18KB
1,000	152KB
10,000	1.68MB

Data Storage Security

All data uploaded to the Forescout Device Cloud is encrypted using a combination of RSA-1024 and AES-256 encryption, and can only be decrypted by a dedicated team of Forescout researchers.

Controlling Your Data

You can opt in and opt out of the Program at any time via the *Advanced* > *Data Sharing* pane in the Options dialog of the Console. Changes take effect as soon as you select **Apply**. If you opt out, any data that was previously uploaded prior to your opt-out will remain in the Program, but the Forescout platform will not upload any additional data.



The first option, *Share selected endpoint properties and plugin configuration and usage information with ForeScout*, allows the sharing of only a subset of properties with Forescout. The second option, *Share all endpoint properties with ForeScout*, allows the sharing of additional properties with Forescout. Currently, this includes sampled, statistical network traffic flow information. This additional data is used to develop more advanced classification and posture assessment profiles which may be delivered to customers in future versions of the Forescout platform.

Appendix A – Data Uploaded to the Forescout Device Cloud

The data listed below is provided by various plugins and modules within the Forescout platform. Some of the properties are hidden and not all of them necessarily exist in your environment. Additionally, some of the properties and data items listed in this appendix may not be applicable to the version of the Forescout platform you are running.

Properties Uploaded 'As Is'

The following properties contain generic information that the Forescout platform will upload 'as is'.

Property Name	Internal Name
802.1x Authenticating Appliance ID	dot1x_auth_appliance_id
802.1x Authorization Source	dot1x_auth_source
802.1x Authorize Action Summary	dot1x_access_action_comment

802.1x Last Authorize Action Failure	dot1x_action_failure_time
802.1x RADIUS Authentication State	dot1x_auth_stat
802.1x Requested Authorize Action	dot1x_req_restrictions
Admission	adm
AirWatch Applications	aw_DeviceAppsResult
AirWatch Compromised Status	aw_IsCompromised
AirWatch Model	aw_Model
AirWatch OS Version	aw_OperatingSystem
AirWatch Platform	aw_Platform
Applications Installed	application
Assigned Label	goodies_label_list
Assigned Meraki Policy	meraki_assigned_group_policy
Azure Virtual Machine Size Type	azure_instance_vm_size_type
Azure VM Delete Protection Enabled	azure_instance_delete_protected
Azure VM OS Profile	azure_instance_OSprofile
Azure VM State	azure_instance_state
Classification Method	cl_type
Classification Method (Classification Version 3)	cl_type3.0
Classification Rule	cl_rule
Classification Rule (Classification Version 3)	cl_rule3.0
Classified by Action	operator_classified
Classified Action Result	classify_action_result
Credential Vulnerability* * The actual login credentials are never uploaded.	posture_scan_protocol
Device Interfaces	device_interfaces
Device is DHCP Relay	is_dhcp_relay
Device is DHCP Server	is_dhcp_server
Device is NAT	nat
DEX Simulated Action	dex_action_statement
DHCP device class	dhcp_class
DHCP device OS	dhcp_os
DHCP options fingerprint	dhcp_opt_fingerprint
DHCP request fingerprint	dhcp_req_fingerprint
DHCP Vendor Class	dhcp_vendor_class
Discovery source	admnew
EC2 Dedicated Tenancy	aws_instance_dt

EC2 Instance Type	aws_instance_type
EC2 Kernel ID	aws_instance_kernelID
EC2 Location	aws_instance_location
EC2 State	aws_instance_state
EC2 Termination Protection	aws_instance_termination
ePO Host NAC Health Status	epo_host_nac_health_status
External Classification	extcls
External Device Connected (By Class)	external_class_device
External Network Function	external_netfunc
FireEye HX Network Info	fireeye_hx_host_network_info
FireEye HX OS Info	fireeye_hx_host_os_info
FireEye HX Threat Detections	fireeye_hx_detected_ioc
FireEye NX Threat Detections	fireeye_detected_ioc
Function	prim_classification
General Vulnerabilities	vulns_nessus
Host is online	online
HTTP Headers	http_headers
HTTP User Agent	ebanner_http
Identified Vulnerabilities	otsm_details_cves
IOCs Detected by CounterACT	atc_detected_ioc
Last Scan Status	atc_scan_details
Linux Manageable (SecureConnector)	linux_manage
Linux Manageable (SSH Direct Access)	ssh_linux_manage
Linux Version	linux_operating_system
Logged In Status	gst_signed_in_stat
MAC Prefix	mac_prefix32
MAC Spoofing Suspected - Blocked Locations	rogued_blocked_ports
Macintosh Applications Installed	mac_app_installed_detected
Macintosh Manageable (SecureConnector)	mac_manage
Macintosh Manageable (SSH Direct Access)	ssh_mac_manage
Macintosh Software Updates	mac_software_updates
Macintosh Version	mac_operating_system
Macintosh-OS Version	va_mac_os
Malicious Event	malic
Manual Network Function	operator_netfunc
Matched Fingerprints	matched_fingerprints

Member of Group	in-group
Microsoft Applications Installed	product
Microsoft Vulnerabilities	vulns
Microsoft Vulnerabilities Fine-tuned	vulns_comp
Miscellaneous Events	misc_events
MobileIron Android Device Rooted	mi_android_rooted
MobileIron iOS Device JailBroken	mi_ios_jailbroken
MobileIron Manufacturer	mi_manufacturer
MobileIron Model	mi_model
MobileIron Platform	mi_platform
MS-RRP Reachable	rpc_manage
MS-SMB Reachable	smb_manage
MS-WMI Reachable	wmi_manage
Network Function	va_netfunc
Network Function (Classification Version 3)	va_netfunc3.0
NIC Vendor	vendor
Nmap - Banner (Ver. 5.3)	nmap_banner5
Nmap - Banner (Ver. 7)	nmap_banner7
Nmap - Network Function (Ver. 5.3)	nmap_netfunc5
Nmap - Network Function (Ver. 7)	nmap_netfunc7
Nmap - OS Fingerprint (Ver. 5.3)	nmap_def_fp5
Nmap - OS Fingerprint (Ver. 7)	nmap_def_fp7
Number of IP Addresses	host_ips
Open Ports	openports
Open Ports Delay	openportsdelay
Operating System	os_classification
OS Classify Action Result	os_classify_action_result
Recent appliances	recent_apps
SMB Signing	smb1_signing
Service Banner	banner
Suggested Operating System	suggested_os_classification
Suggested Function	suggested_prim_classification
Switch Port Action	sw_port_action
Switch Port Name	sw_port_desc
Switch Port PoE Connected Device	sw_port_poe_desc
Switch Port PoE Power Consumption	sw_port_poe_power

Switch Port VLAN	sw_port_vlan
Switch Port Vlan Group	sw_port_vlan_group
Switch Port Voice Device	sw_port_voice_device
Switch Port Voice VLAN	sw_port_voice_vlan
Switch Ports Host ACL Locations – Enforced	sw_port_acl_restricted_locations
Switch Vendor	sw_vendor
Switch Virtual Interface	sw_virtual_interface
Switch VoIP Port	sw_voip_port
System Description	sw_netfunc_os
TCP/IP Syn Ack Fingerprint	p0f_sa_fingerprint
TCP/IP Syn Fingerprint	p0f_fingerprint
The firmware version of this device	otsm_details_firmware_version
The host criticality	otsm_details_criticality
The host Purdue level	otsm_details_purdue_level
The manufacturer	otsm_details_manufacturer
The model of this device	otsm_details_model
The role of this asset	otsm_details_role
Traffic seen	engine_seen_packet
Vendor and Model	vendor_classification
Virtual Machine Guest Health	vmware_guest_health
Virtual Machine Guest OS	vmware_guest_os
Virtual Machine Peripheral Devices	vmware_vm_peripherals
VMware Server OS Type	vmware_server_os_type
VMware Server Product ID	vmware_server_product_line_id
VMware Server Product Name	vmware_server_product_name
VMware Server Vendor	vmware_server_vendor
VMware Server Version	vmware_server_version
Wildfire Server Is Reachable	apt_pan_connection_up
WildFire Threat Detections	pan_apt_detected_ioc
Windows Anti-Spyware Installed	spyware_installed
Windows Antivirus Installed	av_install
Windows Antivirus Running	av_active_new
Windows Antivirus Update Date	av_update_date
Windows Manageable Domain	manage
Windows Manageable SecureConnector	manage_agent
Windows Personal Firewall	fw_active

Windows Security Center Antivirus Status	win_security_center
Windows Service Installed/Removed	service_installed
Windows Services Running	service
Windows Version	va_os
Windows Version Fine-tuned	va_os_comp
Wireless Device (Banner)	access_point
WLAN AP Location	wifi_ap_location
WLAN Association Status	wifi_client_status
WLAN Client User Agent	user_agent
WLAN CTP Vendor	wifi_vendor
WLAN Detected Client Type	host_os
WLAN Managing Controller	wifi_ap_wlc
WLAN Network Function	wireless_netfunc_role
WLAN SSID	wifi_ssid

Properties Anonymized before Upload

All sensitive information in the following properties will be anonymized before being uploaded to Forescout.

Property Name	Internal Name
802.1x Authenticating Appliance	dot1x_auth_appliance
DHCP Domain Name	dhcp_domain_name
DHCP Hostname	dhcp_hostname
DHCP Server Address	dhcp_server
DNS Event	dnsniff_event
IP Address	ip
Last known IP Address	lost_ip
MAC Address	mac
Network Adapters	composite_network_adapters
OS 445/TCP (Client)	eos_smb
OS 445/TCP (Server)	eos_smb_srv
Sessions as Client	client_session
Sessions as Server	server_session
Splunk Alerts	splunk_alerts
Splunk Last Alert	splunk_last_alert
Switch IP	sw_ip
Switch IP and Port Name	sw_ipport_desc

Property Name	Internal Name
Switch Location	sw_location
Switch Port VLAN Name	sw_port_vlan_name
Virtual Machine Guest Hostname	vmware_guest_host
Virtual Machine Guest Network Adapters	vmware_guest_nic_info
Virtual Machine Guest Primary IP	vmware_guest_ip
VMware vCenter Server IP	vmware_vcenter_ip
WLAN AP Name	wifi_ap_name

Aggregated Cloud Deployment Data

Cloud deployment data is aggregated and sanitized before being uploaded to Forescout when you select *Share selected endpoint properties and plugin configuration and usage information with Forescout*. This information is collected to evolve services associated with endpoints in the Cloud and is only relevant to version 8.1.

Aggregated Cloud Data
Total Number of AWS Accounts
Total Number of Azure Accounts
Per Account: Proxy Configured
Per Account: Full Poll Interval
Per Account: Delta Poll Configured
Per Account: Delta Poll Interval
Per Account: Key Rotation Configured (AWS Only)
Per Account: Key Rotation Interval (AWS Only)
Per Account: Number of Regions Selected (AWS Only)
Per Account: Regions in Use (AWS Only)
Per Account: Number of Subscriptions Selected (Azure Only)
Per Account: Number of IAM Users (AWS Only)
Per Account/Per Region: Total Number of AWS EC2 instances
Per Account/Per Subscription: Total Number of Azure VM instances
Per Account/Per Region: Total Number of Running AWS EC2 instances
Per Account/Per Subscription: Total Number of Running Azure VM instances
Per Account/Per Subscription: Number of Azure Windows-based VM instances
Per Account/Per Subscription: Number of Azure Linux-based VM instances
Per Account/Per Subscription: Number of Azure other VM instances
Per Account/Per Region: Number of AWS VPCs
Per Account/Per Subscription: Number of Azure VNets

Additional NetFlow Properties Uploaded 'As Is'

The following additional properties contain generic information that the Forescout platform will upload 'as is' if you select *Share all endpoint properties with ForeScout*.

Property Name	Internal Name
NetFlow Inbound Bits Per Second (daily)	flow_in_bps2
NetFlow Inbound Bits Per Second (hourly)	flow_in_bps1
NetFlow Inbound Bits Per Second (per minute)	flow_in_bps0
NetFlow Inbound Idle Time Percentage (daily)	flow_in_idle2
NetFlow Inbound Idle Time Percentage (hourly)	flow_in_idle1
NetFlow Inbound Idle Time Percentage (per minute)	flow_in_idle0
NetFlow Inbound Packet Size (daily)	flow_in_pktlen2
NetFlow Inbound Packet Size (hourly)	flow_in_pktlen1
NetFlow Inbound Packet Size (per minute)	flow_in_pktlen0
NetFlow Inbound Packets Per Second (daily)	flow_in_pps2
NetFlow Inbound Packets Per Second (hourly)	flow_in_pps1
NetFlow Inbound Packets Per Second (per minute)	flow_in_pps0
NetFlow Outbound Bits Per Second (daily)	flow_out_bps2
NetFlow Outbound Bits Per Second (hourly)	flow_out_bps1
NetFlow Outbound Bits Per Second (per minute)	flow_out_bps0
NetFlow Outbound Idle Time Percentage (daily)	flow_out_idle2
NetFlow Outbound Idle Time Percentage (hourly)	flow_out_idle1
NetFlow Outbound Idle Time Percentage (per minute)	flow_out_idle0
NetFlow Outbound Packet Size (daily)	flow_out_pktlen2
NetFlow Outbound Packet Size (hourly)	flow_out_pktlen1
NetFlow Outbound Packet Size (per minute)	flow_out_pktlen0
NetFlow Outbound Packets Per Second (daily)	flow_out_pps2
NetFlow Outbound Packets Per Second (hourly)	flow_out_pps1
NetFlow Outbound Packets Per Second (per minute)	flow_out_pps0

Additional NetFlow Properties Anonymized before Upload

These additional properties will be uploaded to Forescout if you select *Share all endpoint properties with ForeScout*. All sensitive information in these properties will be anonymized before being uploaded.

Property Name	Internal Name
NetFlow Sessions as Client	netflowtool_client_session
NetFlow Sessions as Server	netflowtool_server_session

Property Name	Internal Name
NetFlow Sessions as Client (DNS)	netflowtool_client_session_dns
NetFlow Sessions as Server (DNS)	netflowtool_server_session_dns

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).