Forescout
Research and Intelligent Analytics Program
Data Security Document

Version 19.1.2
# Table of Contents

**About the Forescout Research and Intelligent Analytics Program** .................. 4  
**Relevancy** ........................................................................................................ 4  

**Program Details** .................................................................................................. 4  
- Data Sanitization ........................................................................................................... 5  
  - Data Anonymization Process ...................................................................................... 6  
- Upload Methodology .................................................................................................... 7  
- Server Details ............................................................................................................. 7  
- Upload Frequency ........................................................................................................ 7  
- Bandwidth Used .......................................................................................................... 7  

**Data Storage Security** .......................................................................................... 8  

**Controlling Your Data** .......................................................................................... 8  

**Appendix A – Data Uploaded to the Forescout Device Cloud** ................................. 9  
- Properties Uploaded 'As Is' .......................................................................................... 9  
- Properties Anonymized before Upload ....................................................................... 13  
- Aggregated Cloud Deployment Data ........................................................................... 13  
- Additional NetFlow Properties Uploaded 'As Is' ......................................................... 14  
- Additional NetFlow Properties Anonymized before Upload ...................................... 15  

**Additional Forescout Documentation** .................................................................... 15  
- Documentation Downloads ......................................................................................... 16  
- Documentation Portal ................................................................................................ 16  
- Forescout Help Tools .................................................................................................. 17
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 19.0.2
- Forescout version 8.1 with Device Profile Library 19.1.2 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:

<table>
<thead>
<tr>
<th>Group</th>
<th>Upload Status</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>Never Uploaded</td>
<td>Any data that contains information about the user of the endpoint.</td>
<td>Properties such as: User, Email, Last Name, Guest User Name. Environmental data such as: credentials for connecting to a Cloud provider.</td>
</tr>
<tr>
<td>Sensitive Data</td>
<td>Anonymized Prior to Upload</td>
<td>Any data that may reveal sensitive information about your environment. See Properties Anonymized before Upload and Additional NetFlow Properties Anonymized before Upload.</td>
<td>Properties such as: IP Address, MAC Address, Hostname, and internal DNS properties.</td>
</tr>
<tr>
<td>Generic Data</td>
<td>Uploaded 'As Is'</td>
<td>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'.</td>
<td>Properties such as: Linux Version, Windows Cloud Application Installed, DHCP Vendor Class, Manual Classification. Environmental data such as: the number of AWS accounts configured.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Number of Endpoints Managed by the Appliance</th>
<th>Bandwidth Used per Upload</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4KB</td>
</tr>
<tr>
<td>10</td>
<td>5KB</td>
</tr>
</tbody>
</table>
### 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’.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Internal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admission</td>
<td>adm</td>
</tr>
<tr>
<td>AirWatch Applications</td>
<td>aw_DeviceAppsResult</td>
</tr>
<tr>
<td>AirWatch Compromised Status</td>
<td>aw_IsCompromised</td>
</tr>
<tr>
<td>AirWatch Model</td>
<td>aw_Model</td>
</tr>
<tr>
<td>AirWatch OS Version</td>
<td>aw_OperatingSystem</td>
</tr>
<tr>
<td>AirWatch Platform</td>
<td>aw_Platform</td>
</tr>
<tr>
<td>Applications Installed</td>
<td>application</td>
</tr>
<tr>
<td>Azure Virtual Machine Size Type</td>
<td>azure_instance_vm_size_type</td>
</tr>
<tr>
<td>Azure VM Delete Protection Enabled</td>
<td>azure_instance_delete_protected</td>
</tr>
<tr>
<td>Azure VM OS Profile</td>
<td>azure_instance_OSprofile</td>
</tr>
<tr>
<td>Azure VM State</td>
<td>azure_instance_state</td>
</tr>
<tr>
<td>Classification Method</td>
<td>cl_type</td>
</tr>
<tr>
<td>Classification Method (Classification Version 3)</td>
<td>cl_type3.0</td>
</tr>
<tr>
<td>Classification Rule</td>
<td>cl_rule</td>
</tr>
<tr>
<td>Classification Rule (Classification Version 3)</td>
<td>cl_rule3.0</td>
</tr>
<tr>
<td>Classified by Action</td>
<td>operator_classified</td>
</tr>
<tr>
<td>Classified Action Result</td>
<td>classify_action_result</td>
</tr>
<tr>
<td>Credential Vulnerability*</td>
<td>posture_scan_protocol</td>
</tr>
<tr>
<td>* The actual login credentials are never uploaded.</td>
<td></td>
</tr>
<tr>
<td>Device Interfaces</td>
<td>device_interfaces</td>
</tr>
<tr>
<td>Device is DHCP Relay</td>
<td>is_dhcp_relay</td>
</tr>
<tr>
<td>Device is DHCP Server</td>
<td>is_dhcp_server</td>
</tr>
<tr>
<td>Device is NAT</td>
<td>nat</td>
</tr>
<tr>
<td>DHCP device class</td>
<td>dhcp_class</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>DHCP device OS</td>
<td>dhcp_os</td>
</tr>
<tr>
<td>DHCP options fingerprint</td>
<td>dhcp_opt_fingerprint</td>
</tr>
<tr>
<td>DHCP request fingerprint</td>
<td>dhcp_req_fingerprint</td>
</tr>
<tr>
<td>DHCP Vendor Class</td>
<td>dhcp_vendor_class</td>
</tr>
<tr>
<td>EC2 Dedicated Tenancy</td>
<td>aws_instance_dt</td>
</tr>
<tr>
<td>EC2 Instance Type</td>
<td>aws_instance_type</td>
</tr>
<tr>
<td>EC2 Kernel ID</td>
<td>aws_instance_kernelID</td>
</tr>
<tr>
<td>EC2 Location</td>
<td>aws_instance_location</td>
</tr>
<tr>
<td>EC2 State</td>
<td>aws_instance_state</td>
</tr>
<tr>
<td>EC2 Termination Protection</td>
<td>aws_instance_termination</td>
</tr>
<tr>
<td>ePO Host NAC Health Status</td>
<td>epo_host_nac_health_status</td>
</tr>
<tr>
<td>External Classification</td>
<td>extcls</td>
</tr>
<tr>
<td>External Device Connected (By Class)</td>
<td>external_class_device</td>
</tr>
<tr>
<td>External Network Function</td>
<td>external_netfunc</td>
</tr>
<tr>
<td>FireEye HX Network Info</td>
<td>fireeye_hx_host_network_info</td>
</tr>
<tr>
<td>FireEye HX OS Info</td>
<td>fireeye_hx_host_os_info</td>
</tr>
<tr>
<td>FireEye HX Threat Detections</td>
<td>fireeye_hx_detected_ioc</td>
</tr>
<tr>
<td>FireEye NX Threat Detections</td>
<td>fireeye_detected_ioc</td>
</tr>
<tr>
<td>Function</td>
<td>prim_classification</td>
</tr>
<tr>
<td>General Vulnerabilities</td>
<td>vulns_nessus</td>
</tr>
<tr>
<td>Host is online</td>
<td>online</td>
</tr>
<tr>
<td>HTTP Headers</td>
<td>http_headers</td>
</tr>
<tr>
<td>HTTP User Agent</td>
<td>ebanner_http</td>
</tr>
<tr>
<td>Identified Vulnerabilities</td>
<td>otsm_details_cves</td>
</tr>
<tr>
<td>Linux Version</td>
<td>linux_operating_system</td>
</tr>
<tr>
<td>MAC Prefix</td>
<td>mac_prefix32</td>
</tr>
<tr>
<td>Macintosh Applications Installed</td>
<td>mac_app_installed_detected</td>
</tr>
<tr>
<td>Macintosh Software Updates</td>
<td>mac_software_updates</td>
</tr>
<tr>
<td>Macintosh Version</td>
<td>mac_operating_system</td>
</tr>
<tr>
<td>Macintosh-OS Version</td>
<td>va_mac_os</td>
</tr>
<tr>
<td>Malicious Event</td>
<td>malic</td>
</tr>
<tr>
<td>Manual Network Function</td>
<td>operator_netfunc</td>
</tr>
<tr>
<td>Matched Fingerprints</td>
<td>matched_fingerprints</td>
</tr>
<tr>
<td>Member of Group</td>
<td>in-group</td>
</tr>
<tr>
<td>Microsoft Applications Installed</td>
<td>product</td>
</tr>
<tr>
<td>Microsoft Vulnerabilities</td>
<td>vulns</td>
</tr>
<tr>
<td>Requested Attribute</td>
<td>VENV</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Microsoft Vulnerabilities Fine-tuned</td>
<td>vulns_comp</td>
</tr>
<tr>
<td>Miscellaneous Events</td>
<td>misc_events</td>
</tr>
<tr>
<td>MobileIron Android Device Rooted</td>
<td>mi_android_rooted</td>
</tr>
<tr>
<td>MobileIron iOS Device JailBroken</td>
<td>mi_ios_jailbroken</td>
</tr>
<tr>
<td>MobileIron Manufacturer</td>
<td>mi_manufacturer</td>
</tr>
<tr>
<td>MobileIron Model</td>
<td>mi_model</td>
</tr>
<tr>
<td>MobileIron Platform</td>
<td>mi_platform</td>
</tr>
<tr>
<td>Network Function</td>
<td>va_netfunc</td>
</tr>
<tr>
<td>Network Function (Classification Version 3)</td>
<td>va_netfunc3.0</td>
</tr>
<tr>
<td>NIC Vendor</td>
<td>vendor</td>
</tr>
<tr>
<td>Nmap - Banner (Ver. 5.3)</td>
<td>nmap_banner5</td>
</tr>
<tr>
<td>Nmap - Banner (Ver. 7)</td>
<td>nmap_banner7</td>
</tr>
<tr>
<td>Nmap - Network Function (Ver. 5.3)</td>
<td>nmap_netfunc5</td>
</tr>
<tr>
<td>Nmap - Network Function (Ver. 7)</td>
<td>nmap_netfunc7</td>
</tr>
<tr>
<td>Nmap - OS Fingerprint (Ver. 5.3)</td>
<td>nmap_def_fp5</td>
</tr>
<tr>
<td>Nmap - OS Fingerprint (Ver. 7)</td>
<td>nmap_def_fp7</td>
</tr>
<tr>
<td>Number of IP Addresses</td>
<td>host_ips</td>
</tr>
<tr>
<td>Open Ports Delay</td>
<td>openportsdelay</td>
</tr>
<tr>
<td>Operating System</td>
<td>os_classification</td>
</tr>
<tr>
<td>OS Classify Action Result</td>
<td>os_classify_action_result</td>
</tr>
<tr>
<td>Recent appliances</td>
<td>recent_apps</td>
</tr>
<tr>
<td>SMB Signing</td>
<td>smb1_signing</td>
</tr>
<tr>
<td>Service Banner</td>
<td>banner</td>
</tr>
<tr>
<td>Suggested Operating System</td>
<td>suggested_os_classification</td>
</tr>
<tr>
<td>Suggested Function</td>
<td>suggested_prim_classification</td>
</tr>
<tr>
<td>Switch Port Name</td>
<td>sw_port_desc</td>
</tr>
<tr>
<td>Switch Port PoE Connected Device</td>
<td>sw_port_poe_desc</td>
</tr>
<tr>
<td>Switch Port PoE Power Consumption</td>
<td>sw_port_poe_power</td>
</tr>
<tr>
<td>Switch Port VLAN</td>
<td>sw_port_vlan</td>
</tr>
<tr>
<td>Switch Port Vlan Group</td>
<td>sw_port_vlan_group</td>
</tr>
<tr>
<td>Switch Port Voice Device</td>
<td>sw_port_voice_device</td>
</tr>
<tr>
<td>Switch Port Voice VLAN</td>
<td>sw_port_voice_vlan</td>
</tr>
<tr>
<td>Switch Ports Host ACL Locations – Enforced</td>
<td>sw_port_acl_restricted_locations</td>
</tr>
<tr>
<td>Switch Vendor</td>
<td>sw_vendor</td>
</tr>
<tr>
<td>Switch Virtual Interface</td>
<td>sw_virtual_interface</td>
</tr>
<tr>
<td><strong>Switch VoIP Port</strong></td>
<td><code>sw_voip_port</code></td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>System Description</strong></td>
<td><code>sw_netfunc_os</code></td>
</tr>
<tr>
<td><strong>TCP/IP Syn Ack Fingerprint</strong></td>
<td><code>p0f_sa_fingerprint</code></td>
</tr>
<tr>
<td><strong>TCP/IP Syn Fingerprint</strong></td>
<td><code>p0f_fingerprint</code></td>
</tr>
<tr>
<td><strong>The firmware version of this device</strong></td>
<td><code>otsm_details_firmware_version</code></td>
</tr>
<tr>
<td><strong>The host criticality</strong></td>
<td><code>otsm_details_criticality</code></td>
</tr>
<tr>
<td><strong>The host Purdue level</strong></td>
<td><code>otsm_details_purdue_level</code></td>
</tr>
<tr>
<td><strong>The manufacturer</strong></td>
<td><code>otsm_details_manufacturer</code></td>
</tr>
<tr>
<td><strong>The model of this device</strong></td>
<td><code>otsm_details_model</code></td>
</tr>
<tr>
<td><strong>The role of this asset</strong></td>
<td><code>otsm_details_role</code></td>
</tr>
<tr>
<td><strong>Traffic seen</strong></td>
<td><code>engine_seen_packet</code></td>
</tr>
<tr>
<td><strong>Vendor and Model</strong></td>
<td><code>vendor_classification</code></td>
</tr>
<tr>
<td><strong>Virtual Machine Guest Health</strong></td>
<td><code>vmware_guest_health</code></td>
</tr>
<tr>
<td><strong>Virtual Machine Guest OS</strong></td>
<td><code>vmware_guest_os</code></td>
</tr>
<tr>
<td><strong>Virtual Machine Peripheral Devices</strong></td>
<td><code>vmware_vm_peripherals</code></td>
</tr>
<tr>
<td><strong>VMware Server OS Type</strong></td>
<td><code>vmware_server_os_type</code></td>
</tr>
<tr>
<td><strong>VMware Server Product ID</strong></td>
<td><code>vmware_server_product_line_id</code></td>
</tr>
<tr>
<td><strong>VMware Server Product Name</strong></td>
<td><code>vmware_server_product_name</code></td>
</tr>
<tr>
<td><strong>VMware Server Vendor</strong></td>
<td><code>vmware_server_vendor</code></td>
</tr>
<tr>
<td><strong>VMware Server Version</strong></td>
<td><code>vmware_server_version</code></td>
</tr>
<tr>
<td><strong>WildFire Server Is Reachable</strong></td>
<td><code>apt_pan_connection_up</code></td>
</tr>
<tr>
<td><strong>WildFire Threat Detections</strong></td>
<td><code>pan_apt_detected_ioc</code></td>
</tr>
<tr>
<td><strong>Windows Anti-Spyware Installed</strong></td>
<td><code>spyware_installed</code></td>
</tr>
<tr>
<td><strong>Windows Antivirus Installed</strong></td>
<td><code>av_install</code></td>
</tr>
<tr>
<td><strong>Windows Antivirus Running</strong></td>
<td><code>av_active_new</code></td>
</tr>
<tr>
<td><strong>Windows Antivirus Update Date</strong></td>
<td><code>av_update_date</code></td>
</tr>
<tr>
<td><strong>Windows Personal Firewall</strong></td>
<td><code>fw_active</code></td>
</tr>
<tr>
<td><strong>Windows Security Center Antivirus Status</strong></td>
<td><code>win_security_center</code></td>
</tr>
<tr>
<td><strong>Windows Service Installed/Removed</strong></td>
<td><code>service_installed</code></td>
</tr>
<tr>
<td><strong>Windows Services Running</strong></td>
<td><code>service</code></td>
</tr>
<tr>
<td><strong>Windows Version</strong></td>
<td><code>va_os</code></td>
</tr>
<tr>
<td><strong>Windows Version Fine-tuned</strong></td>
<td><code>va_os_comp</code></td>
</tr>
<tr>
<td><strong>Wireless Device (Banner)</strong></td>
<td><code>access_point</code></td>
</tr>
<tr>
<td><strong>WLAN AP Location</strong></td>
<td><code>wifi_ap_location</code></td>
</tr>
<tr>
<td><strong>WLAN Association Status</strong></td>
<td><code>wifi_client_status</code></td>
</tr>
<tr>
<td><strong>WLAN Client User Agent</strong></td>
<td><code>user_agent</code></td>
</tr>
</tbody>
</table>
Properties Anonymized before Upload

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

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Internal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Domain Name</td>
<td>dhcp_domain_name</td>
</tr>
<tr>
<td>DHCP Hostname</td>
<td>dhcp_hostname</td>
</tr>
<tr>
<td>DHCP Server Address</td>
<td>dhcp_server</td>
</tr>
<tr>
<td>DNS Event</td>
<td>dnsniff_event</td>
</tr>
<tr>
<td>IP Address</td>
<td>ip</td>
</tr>
<tr>
<td>Last known IP Address</td>
<td>lost_ip</td>
</tr>
<tr>
<td>MAC Address</td>
<td>mac</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>composite_network_adapters</td>
</tr>
<tr>
<td>OS 445/TCP (Client)</td>
<td>eos_smb</td>
</tr>
<tr>
<td>OS 445/TCP (Server)</td>
<td>eos_smb_srv</td>
</tr>
<tr>
<td>Sessions as Client</td>
<td>client_session</td>
</tr>
<tr>
<td>Sessions as Server</td>
<td>server_session</td>
</tr>
<tr>
<td>Splunk Alerts</td>
<td>splunk_alerts</td>
</tr>
<tr>
<td>Splunk Last Alert</td>
<td>splunk_last_alert</td>
</tr>
<tr>
<td>Switch IP</td>
<td>sw_ip</td>
</tr>
<tr>
<td>Switch IP and Port Name</td>
<td>sw_ipport_desc</td>
</tr>
<tr>
<td>Switch Location</td>
<td>sw_location</td>
</tr>
<tr>
<td>Switch Port VLAN Name</td>
<td>sw_port_vlan_name</td>
</tr>
<tr>
<td>Virtual Machine Guest Hostname</td>
<td>vmware_guest_host</td>
</tr>
<tr>
<td>Virtual Machine Guest Network Adapters</td>
<td>vmware_guest_nic_info</td>
</tr>
<tr>
<td>Virtual Machine Guest Primary IP</td>
<td>vmware_guest_ip</td>
</tr>
<tr>
<td>VMware vCenter Server IP</td>
<td>vmware_vcenter_ip</td>
</tr>
<tr>
<td>WLAN AP Name</td>
<td>wifi_ap_name</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Internal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of AWS Accounts</td>
<td></td>
</tr>
<tr>
<td>Total Number of Azure Accounts</td>
<td></td>
</tr>
<tr>
<td>Per Account: Proxy Configured</td>
<td></td>
</tr>
<tr>
<td>Per Account: Full Poll Interval</td>
<td></td>
</tr>
<tr>
<td>Per Account: Delta Poll Configured</td>
<td></td>
</tr>
<tr>
<td>Per Account: Delta Poll Interval</td>
<td></td>
</tr>
<tr>
<td>Per Account: Key Rotation Configured (AWS Only)</td>
<td></td>
</tr>
<tr>
<td>Per Account: Key Rotation Interval (AWS Only)</td>
<td></td>
</tr>
<tr>
<td>Per Account: Number of Regions Selected (AWS Only)</td>
<td></td>
</tr>
<tr>
<td>Per Account: Regions in Use (AWS Only)</td>
<td></td>
</tr>
<tr>
<td>Per Account: Number of Subscriptions Selected (Azure Only)</td>
<td></td>
</tr>
<tr>
<td>Per Account: Number of IAM Users (AWS Only)</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Region: Total Number of AWS EC2 instances</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Subscription: Total Number of Azure VM instances</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Region: Total Number of Running AWS EC2 instances</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Subscription: Total Number of Running Azure VM instances</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Subscription: Number of Azure Windows-based VM instances</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Subscription: Number of Azure Linux-based VM instances</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Subscription: Number of Azure other VM instances</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Region: Number of AWS VPCs</td>
<td></td>
</tr>
<tr>
<td>Per Account/Per Subscription: Number of Azure VNets</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

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

### 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.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Internal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetFlow Sessions as Client</td>
<td>netflowtool_client_session</td>
</tr>
<tr>
<td>NetFlow Sessions as Server</td>
<td>netflowtool_server_session</td>
</tr>
<tr>
<td>NetFlow Sessions as Client (DNS)</td>
<td>netflowtool_client_session_dns</td>
</tr>
<tr>
<td>NetFlow Sessions as Server (DNS)</td>
<td>netflowtool_server_session_dns</td>
</tr>
</tbody>
</table>

### 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:

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).