



Lookout Integration Guide

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2023, Ivanti, Inc. All rights reserved.

Protected by patents, see <https://www.ivanti.com/patents>.

Contents

Neurons for ZTA with Lookout Integration Guide	4
Introduction	5
Use Case 1: Private Cloud and On-prem Access with SSO into Salesforce	5
Use Case 2: Public Cloud Access	5
Use Case 3: Public Internet Access	5
Use Case 1: Private Cloud and On-prem Access with SSO into Salesforce	7
Use Case 2: Public Cloud Access	15
CASB Overviews	15
Forward Proxy Configuration	16
Proxy Auto Configuration	21
Importing the Trusted CA certificate to the nZTA	22
Use Case 3: Public Internet Access	24
SWG Overview	24
Enable SWG on Lookout	25
Downloading the PAC file from Lookout tenant and configure in nZTA Controller	28
Importing the Trusted CA certificate to the nZTA	29
Appendix	31
Documentation	33
Technical Support	33

Neurons for ZTA with Lookout Integration Guide

This integration guide covers three different use cases and walk through the basics of integration configuration. It is assumed that the user of this document has access to the required administrative consoles, both the Ivanti Neurons for Zero Trust Access and a Lookout console.

Introduction

This guide will only cover the high-level view of the required steps. For more information, access the respective help sections inside the respective administrator consoles.

Use Case 1: Private Cloud and On-prem Access with SSO into Salesforce

Use nZTA to route traffic securely to these resources, front ended by nZTA Gateways

This permits the administrator to ensure that all internal resources are protected from outside access. Rules applied for access are dynamic and continuously evaluated. Only users that both require access and currently meet the security parameters of access are permitted to reach these resources.

For Configuration details, see [Use Case 1](#) . This use case involves configurations related only to Ivanti side of the solution.

Use Case 2: Public Cloud Access

Use Lookout Cloud Access Security Broker (CASB), ensuring malware scanning and DLP policies for access

CASB can be configured in Forward Proxy or Reverse Proxy modes. This would permit secure access to all services being hosted outside of the customers control, such as standard SaaS apps. Using the CASB to control access, all data transmitted between the public cloud and the end user's device are scanned. Keeping sensitive documents inside the network, within reach of the corporate security policies. While keeping malware outside of the network, detecting it before it reaches the endpoint, the edge of the corporate network. This use case will involve complex configurations on both the Lookout and Ivanti products. It is suggested to use Forward Proxy in most cases. However, Reverse Proxy use case is used for unmanaged devices.

For Configuration details, see [Use Case 2](#). This use case requires configurations on both the Ivanti and Lookout consoles.

Use Case 3: Public Internet Access

Use Secure Web Gateway (SWG), ensuring malware scanning on all data coming from outside the network

With SWG, the admin can ensure that risky activities taken on by end users won't lead to network wide infections from malware. As the end user is accessing external, public internet resources, the traffic passes through the SWG, allowing all transactions to be scanned for malware. SWG is also able to enforce the core DLP policies.

For Configuration details, see [Use Case 3](#). This use case involves configurations related only to Lookout side of the solution.

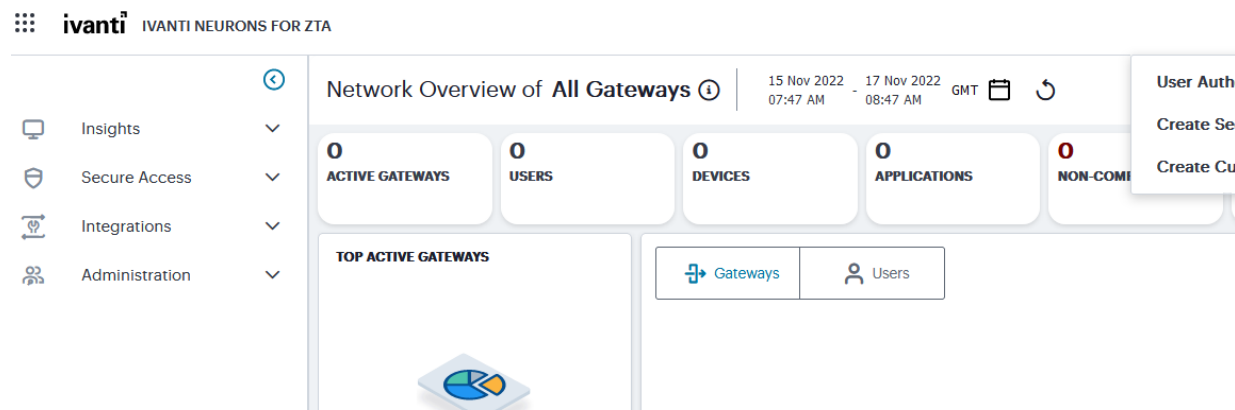
Use Case 1: Private Cloud and On-prem Access with SSO into Salesforce

Use ZTA to route traffic securely to these resources, front ended by ZTA Gateways. There are a few key configurations that are required before this use case can be met.

- [Creating or connecting user database](#)
- [Deploying a gateway in a location that permits access to a protected resource](#)
- [Configuration on the Salesforce domain for SSO integration into the ZTA domain](#)

Creating or connecting user database

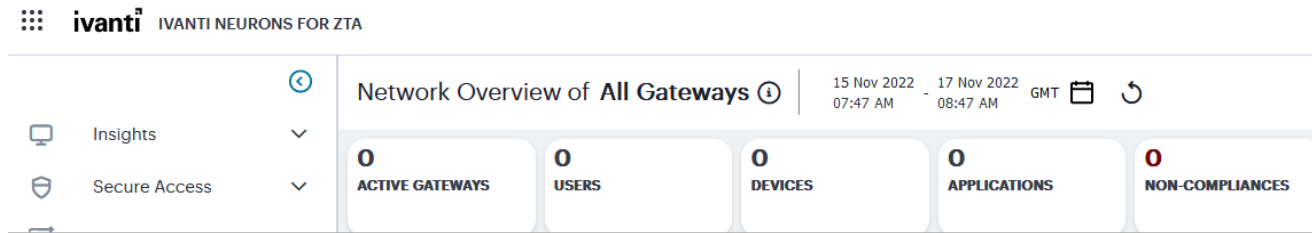
1. Local users can easily be added by the admin
2. SAML integration can also be used to link to an external user database
3. Use **Workflows > User Authentication** to start the configuration wizard



4. The admin will need to define authentication servers for at least Enrollment and User Signin and optionally Admin Signin.

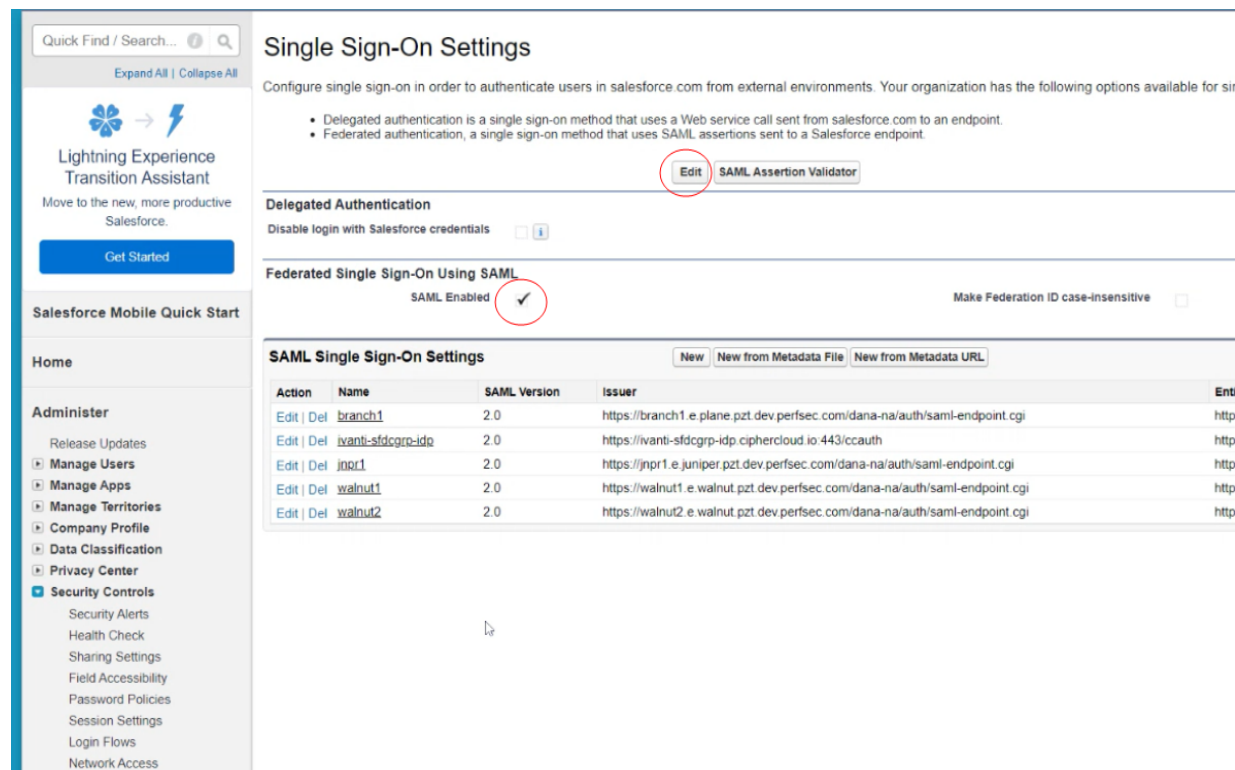
Deploying a gateway in a location that permits access to a protected resource

1. The steps to gateway deployment vary greatly depending on what type of hypervisor is being used
2. Follow the steps outlined in the Help documentation, Getting Started with ZTA.

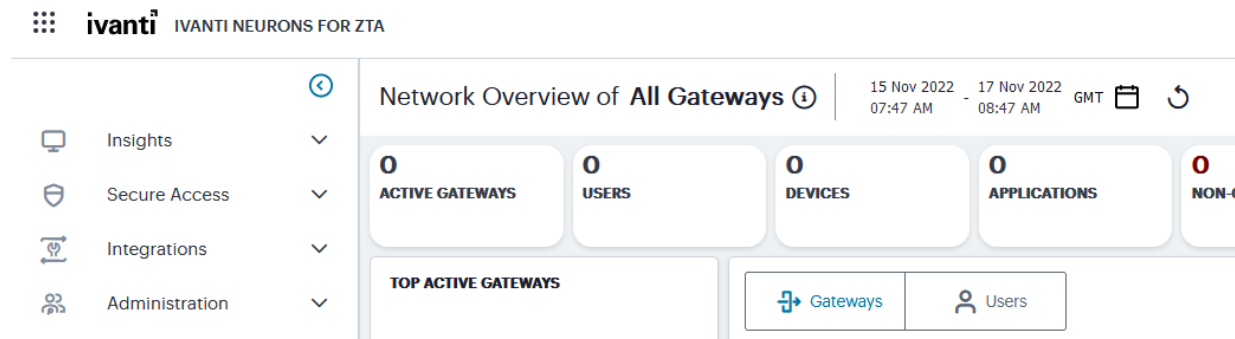


Configuration on the Salesforce domain for SSO integration into the ZTA domain

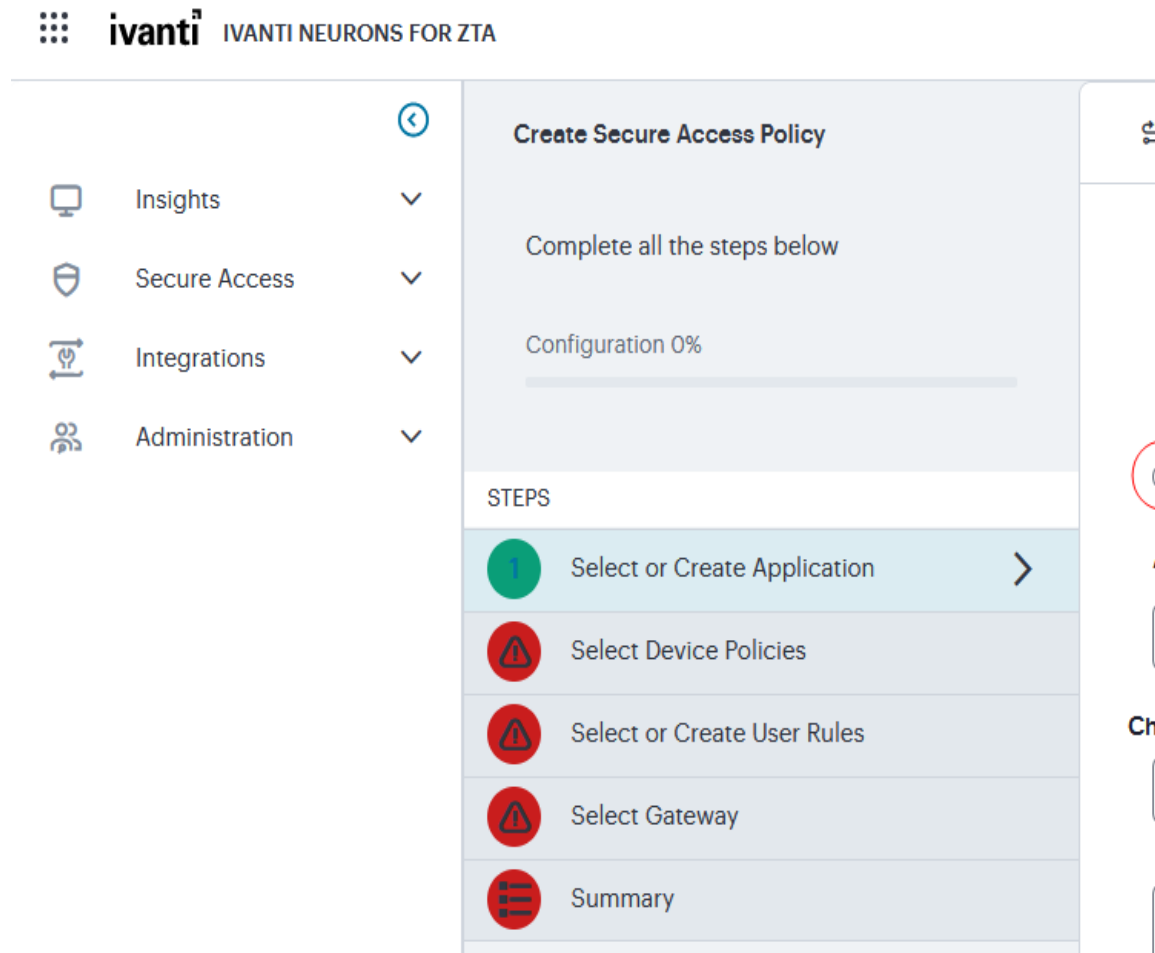
1. Sign up for a new [Salesforce Developer](#) account.
2. Once domain is registered, log in to the domain (Example: cloudsecure-dev-ed.my.salesforce.com).
3. Click setup located on top right corner of the page.
4. Navigate to **Security Controls** > **Single Sign-On** Settings on the left panel. Click on **Edit**, check **SAML Enabled** and click **Save**.



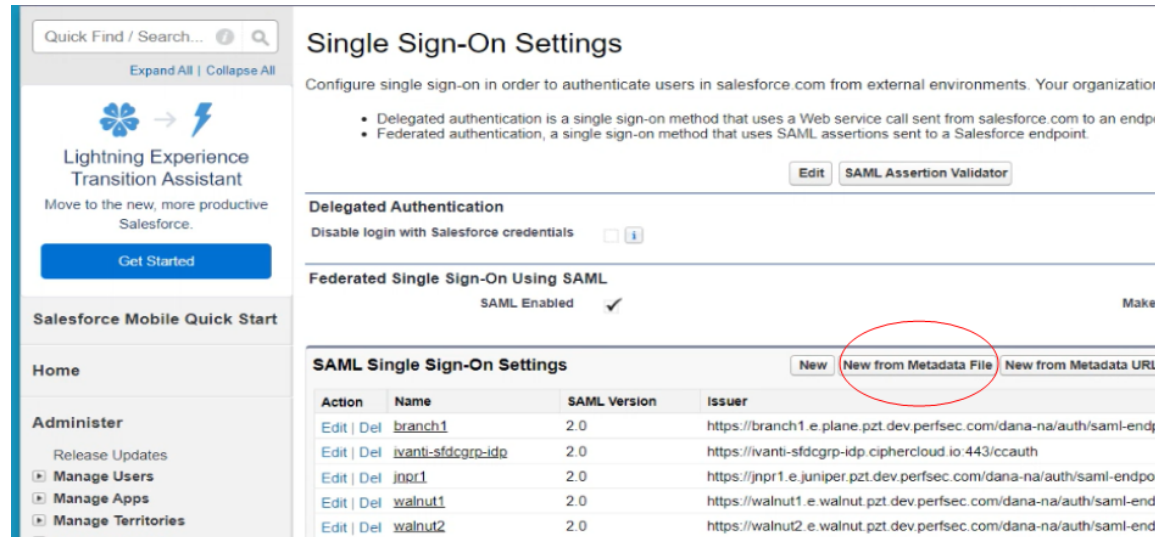
5. Return to the ZTA domain and begin the process of creating a Secure Access Policy



1. You will need to fill out the first few fields in order to get the SAML metadata file from ZTA before returning to the Salesforce domain to complete configuration.



- Return to Salesforce domain in the SAML SSO settings and select **New from Metadata File** and upload the file downloaded from ZTA



Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization can use either Delegated authentication or Federated authentication.

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

[Edit](#) [SAML Assertion Validator](#)

Delegated Authentication

Disable login with Salesforce credentials ☐ [i](#)

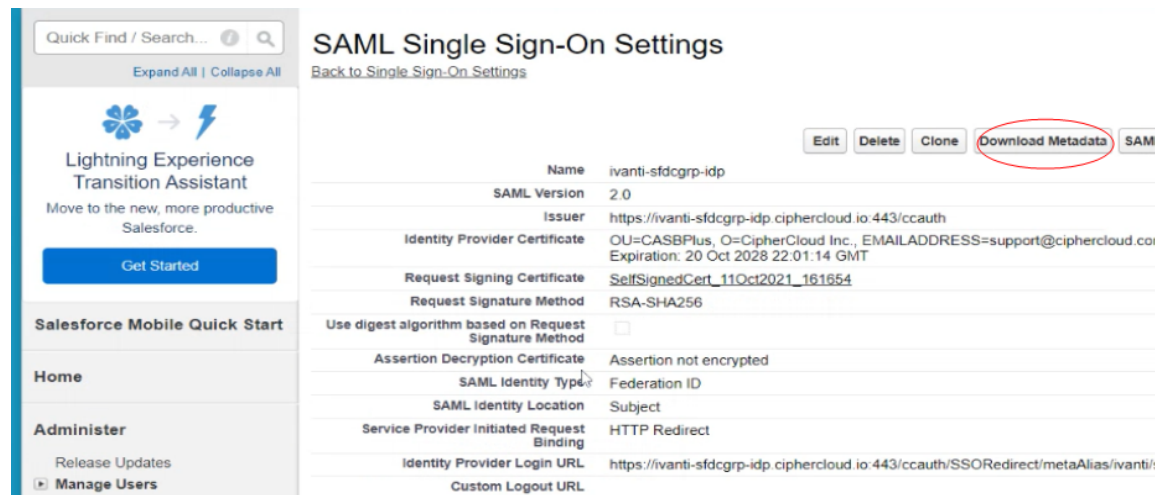
Federated Single Sign-On Using SAML

SAML Enabled ☒ [Make](#)

SAML Single Sign-On Settings [New](#) [New from Metadata File](#) [New from Metadata URL](#)

Action	Name	SAML Version	Issuer
Edit Del	branch1	2.0	https://branch1.e.plane.pzt.dev.perfsec.com/dana-na/auth/saml-endp
Edit Del	ivanti-sfdcgrp-idp	2.0	https://ivanti-sfdcgrp-idp.ciphercloud.io:443/ccauth
Edit Del	jnp1	2.0	https://jnp1.e.juniper.pzt.dev.perfsec.com/dana-na/auth/saml-endp
Edit Del	walnut1	2.0	https://walnut1.e.walnut.pzt.dev.perfsec.com/dana-na/auth/saml-end
Edit Del	walnut2	2.0	https://walnut2.e.walnut.pzt.dev.perfsec.com/dana-na/auth/saml-end

- Click the name of the new entry (next to Edit | Del) and download the metadata file associated with the new entry.



SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML](#)

Name	ivanti-sfdcgrp-idp
SAML Version	2.0
Issuer	https://ivanti-sfdcgrp-idp.ciphercloud.io:443/ccauth
Identity Provider Certificate	OU=CASBPlus, O=CipherCloud Inc., EMAILADDRESS=support@ciphercloud.co Expiration: 20 Oct 2028 22:01:14 GMT
Request Signing Certificate	SelfSignedCert_11Oct2021_161654
Request Signature Method	RSA-SHA256
Use digest algorithm based on Request Signature Method	<input type="checkbox"/>
Assertion Decryption Certificate	Assertion not encrypted
SAML Identity Type	Federation ID
SAML Identity Location	Subject
Service Provider Initiated Request Binding	HTTP Redirect
Identity Provider Login URL	https://ivanti-sfdcgrp-idp.ciphercloud.io:443/ccauth/SSORedirect/metaAlias/ivanti/
Custom Logout URL	

- Take the metadata file back to ZTA and upload (move the radio button selection from download to upload)

☐ Download IDP Metadata ☒ Upload SAML Metadata

UPLOAD METADATA

Add Saml Attributes

Attribute



Value



5. Select **Next** and move through the rest of the settings.
 1. Select the users who see the bookmark
 2. Apply an option host checking rule
 3. Attach the bookmark to a gateway for access
6. Navigate to **Domain Management > My Domain** on the left panel. Click **Edit** under the **Authentication**
7. Configuration section, check the box for the SSO profile created above and click **Save**.

Authentication Configuration

Authentication Configuration [Save] [Cancel] [Reset to Default]

Login Page Type Standard ▼

Authentication Service

- ☒ Login Form
- ☒ lookout-ntza

Logo File [Choose File] No file chosen

Background Color #F4F6F9

Right Frame URL

Use the native browser for user authentication on iOS ☐

Use the native browser for user authentication on Android ☐

[Save] [Cancel] [Reset to Default]

8. Navigate to **Administer > Manage Users > Users**. Click **New User** to create a new Salesforce user if user does not exist. Provide the following details, matching the user created on the ZTA domain:
 1. Provide **First Name**.
 2. Provide **Last Name**. Alias will get populated automatically.
 3. Provide **Email**. Username and Nickname will get populated automatically.
 4. Select **Role** for the user.
 5. Select **User License** as Salesforce.
 6. Select **Profile** for the user.
 7. Click **Save**. Leave Salesforce.
9. Take the downloaded file from [step](#) above back to ZTA and upload it in the Secure Access Policy Creation page.

☐ Add Allowed Domains

☒ SAML Access

☐ Download IDP Metadata

☒ Upload SAML Metadata

UPLOAD METADATA

Add Saml Attributes

Attribute



Value



10. Select **Add Allowed Domains** and upload the below listing for domains saved in an excel generated CSV file.



Only the top 4 are needed if a non-DLP setup is being created (SSO from ZTA to Salesforce, without Lookout).

*.salesforce.com

*.my.salesforce.com

*.force.com

*.lightning.com

*.salesforce-communities.com

*.eloqua.com

*.salesforcemarket.com

*.documentforce.com

*.forcesslreports.com

*.forceusercontent.com

*.salesforceliveagent.com

*.sfdcstatic.com

*.developerforce.com

11. Click **Next** and select a device policy if desired. This enforces a device posture rule for the resource to be accessed.
12. Select the users and sign-in policy to attach the resource.
13. Select the gateway to be used for access.
14. Save and publish the Secure Access Policy.



Register a device (using the Enrollment link found in **Secure Access > User > User Policies**) and bring up the ZTA connection in the Ivanti Secure Access Client to leverage the settings defined in the above steps.

Use Case 2: Public Cloud Access

CASB Overviews

In this use case the CASB sits between the enterprises and cloud applications, controlling data flow through a single gateway in “real-time”. This ensures the data always goes to the cloud in a protected form. Proxy-based deployments can be enabled via 2 models:

- **Forward proxy:** CASB in forward proxy mode routes all traffic from endpoint to the CASB instance. CASB can either work with existing proxy services that can forward traffic to CASB proxy, or an agent software needs to be installed on managed devices to forward traffic to CASB (in our case, this is done via the ZTA client and Proxy PAC files).
- **Reverse proxy:** CASB in reverse proxy mode provides secure agentless connectivity for all devices, including mobile and unmanaged devices. It works by simply redirecting all traffic through the CASB from the service provider. This can be done by integrating either with existing IDaaS solutions such as Azure AD, Okta, Ping etc. SSO or with the Lookout Secure Cloud Workspace to securely redirect traffic through CASB.



This configuration is listed in the [Appendix](#)

The forward proxy model involves different configurations. Where Lookout becomes a centerpiece to link together one or more IdPs and many SPs. While nZTA can be used to securely connect end users to resources, there are use cases where the connections benefit from passing through the Lookout CASB (DLP, for example). This requires a few different configurations, done here via SAML integrations. This section only covers managed devices (devices with have the PAC file and Lookout Certificates installed). There are additional integration steps required for unmanaged devices because the device first reaches out to the resource, at which point that resource needs to be aware of Lookout to permit return traffic to be redirected. With a managed device, the connection will be first routed to the Lookout proxy before going to the resource.

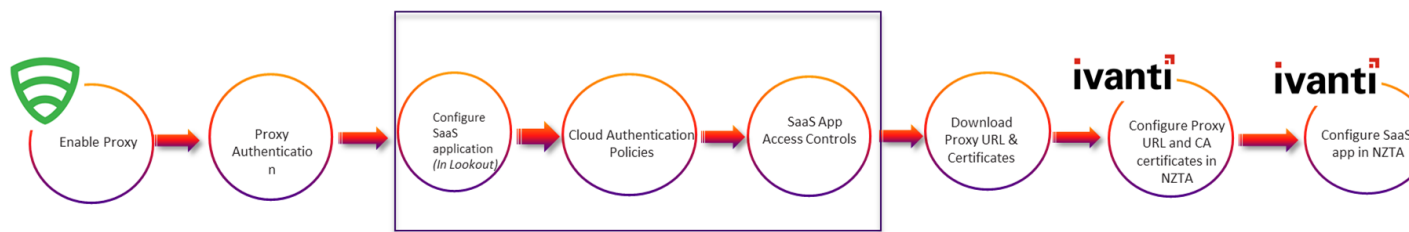
- Integration of Lookout and an SP (in this guide we use Salesforce)
 - This permits DLP between Lookout and Salesforce
- Integration of Lookout and an IdP (in this guide we use nZTA)
 - This links the nZTA users to Lookout users which is important for UEBA and user-based policies
- The integration of nZTA with Salesforce

- This permits SSO between the Ivanti Secure Access Client through Lookout CASB onto Salesforce

Onboarding the device with nZTA then allows the Ivanti Secure Access Client to route all resource access via the required policies. Either directly to the resource or passing it through the CASB for inspection. This routing is defined via a Proxy PAC file. This directs the client browser to forward all connections to the CASB/SWG proxy gateway, except those defined as exceptions (in [Step](#)) which would then instead be directly routed by nZTA to the resource.

Forward Proxy Configuration

Lookout CASB Configurations (Forward Proxy)



Enable Proxy

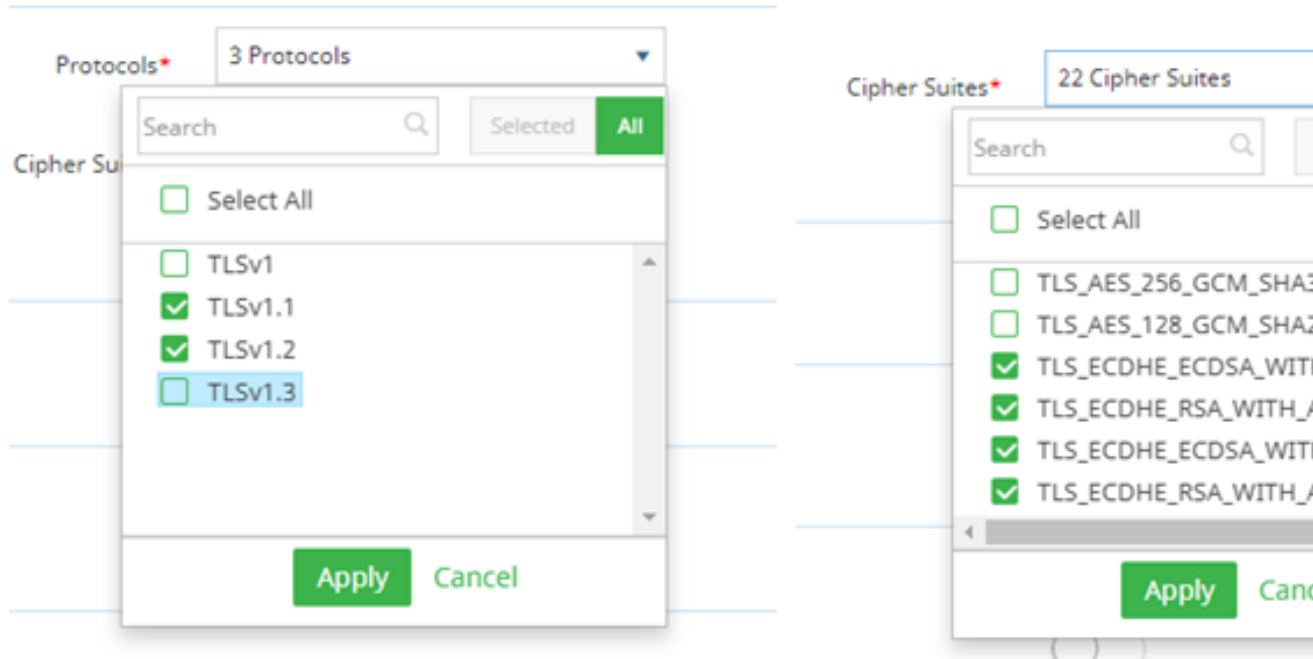
To Enable Proxy:

1. Login to lookout console and generate certificates: **Administration > Certificate Mgmt > Signing CA Certificates > Generate**
2. Enable Forward and Reverse Proxy: **Administration > Environment Mgmt > Default**
 1. Select the certificate from the dropdown that you just created.

The screenshot shows the 'Forward Proxy Settings' section in the Lookout console. A green toggle switch is turned on. Below the toggle, there are two fields: 'CA Certificate' with a dropdown menu showing 'CN=Ivanti.ForwardProxy,OU=SAS' and 'Proxy Address' with a text box containing 'fp-ivanti.ciphercloud.io:443'.

2. Define IP address range of ZTA connected devices (10.10.0.0/16)
 - This allows ZTA traffic to go directly to the controller and gateways without interference of the Lookout proxy.

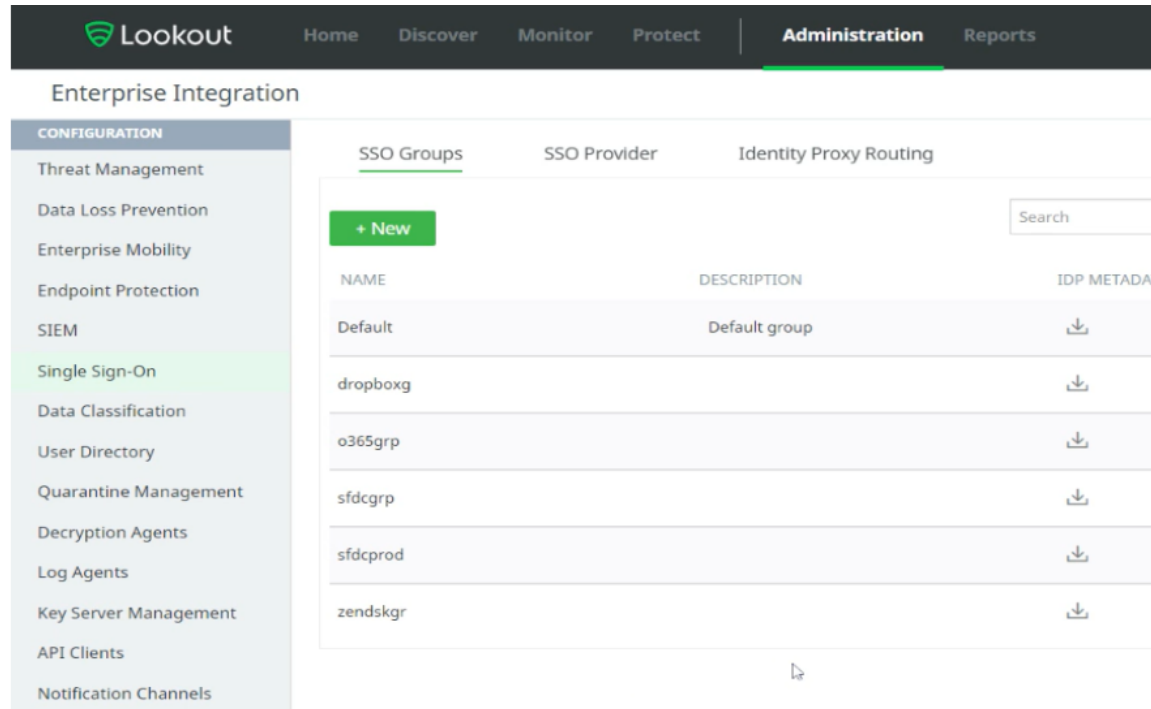
3. Define domains to exclude from CASB inspection (ZTA domain defined above as well as any network domains being accessed via ZTA to be excluded)
 - For example, there may be resources the admin wants to deploy through ZTA (like internal documentation) where CASB inspection is not required. This will allow access to be secured but go directly from client to ZTA gateway without being routed through the CASB for inspection.
3. Check TLS Settings, exclude TLS 1.3, select All ciphers, and then remove the top two selections.



Proxy Authentication

To configure Proxy Authentication:

1. Configure SAML IdP in Lookout: **Enterprise Integration > Single Sign-On**
 1. In Default SSO group, download the SP Metadata from Lookout. This will be used in your external IdP for configuration, nZTA is used as an IdP in this use case.



2. Common fields used for attributes in IdP configuration (nZTA UI)
 1. Attribute: email, Value: <username>
3. Login to nZTA console and open the **Secure Access Policy** wizard.
 1. Input the FQDN of the Lookout console as the resource location.
 2. Upload the SP Metadata file into nZTA and download the resulting Metadata file from the wizard.
 3. You can skip over the Device Policy and User Rules sections (accept defaults) and assign access to a gateway.
 - Once published it should show as a bookmark in nZTA
 4. Go back to lookout and go to **SSO Providers > New**
 5. Select Type: Identity Provider
 6. Select Type: Identity Provider and the default SSO group
 7. Upload the newly generated Metadata file from nZTA and validate
4. Enable Proxy Auth: **Administration > System Settings > Enterprise Authentication**

1. Select the IdP you created in the steps above in the settings

Continuous Authentication Configuration

Enable Continuous Authentication ☐

Enterprise Single Sign-On Settings

Identity Provider ProxyAuth_lookout-nzta.zta-...

Management Console ☒

Relay State Y2NzdHJpbmc=aHR0cHM6Ly9pdmFu Copy

Decryption Client ☒

Enterprise Proxy Authentication

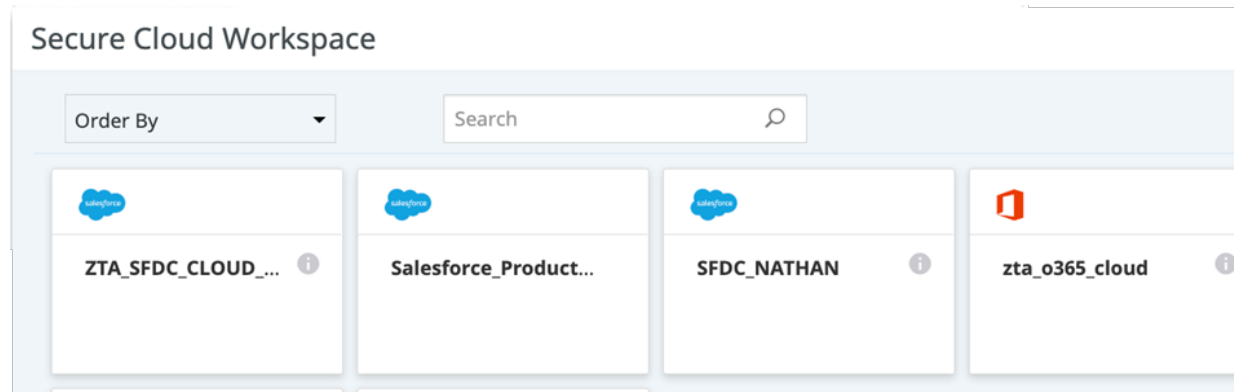
Lookout Proxy Authentication ☒

Proxy Authentication Method Enterprise Single Sign-on

Use Automatic User Agent Whitelisting ☒

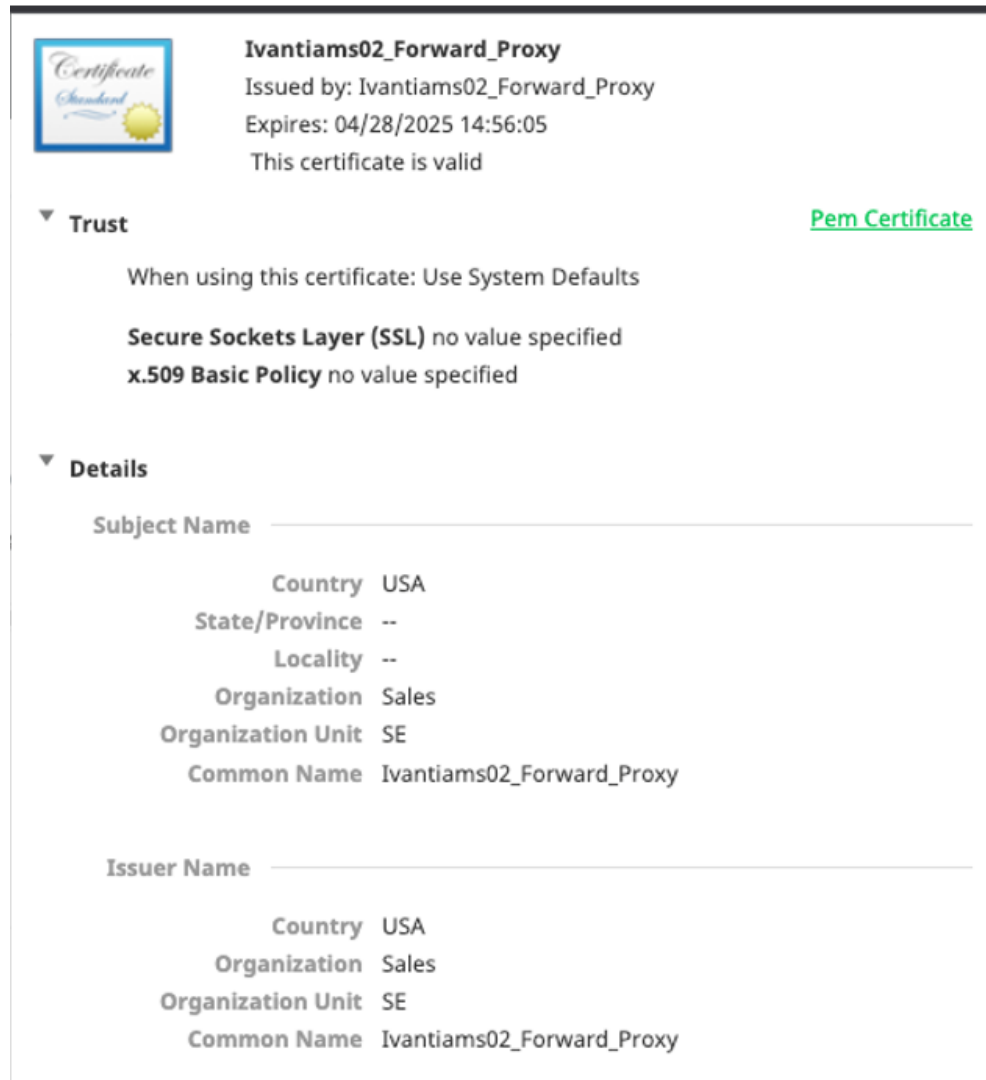
Download Proxy URL & Certs (install on endpoint)

1. To download Proxy URL, Navigate to: **Home > Secure Cloud Workspace** in Lookout.
 1. Right click on the download link for the HTTP/ HTTPS Proxy PAC file and select **copy link address**
 - Example of copied link: <https://domain-ms.ciphercloud.io/public/proxy-casb-https.pac>
 - Example of copied link: <https://domain-ms.ciphercloud.io/public/proxy.pac>



2. Download Certificates

1. To download Certificate, Navigate to: **Administration > Certificate Management > Signing CA Certificate**
2. Click Pem Certificate and copy contents, save as a .cer file on your desktop (You might need to update settings to show the file extension. Saving it as a *.cer.txt will not work.)



3. Install this certificate on the Endpoint



This certificate trust is required for Forward Proxy to operate properly

Proxy Auto Configuration

Proxy auto-configuration (PAC) file instructs a browser to forward traffic to a proxy server, instead of directly to the destination server. You can obtain the PAC URL for the Lookout tenant by clicking the PAC file icon from the Secure Cloud Workspace menu.

To get the PAC file URL from Lookout Tenant:

1. Click the **PAC file** icon located at the upper-right corner of the page.

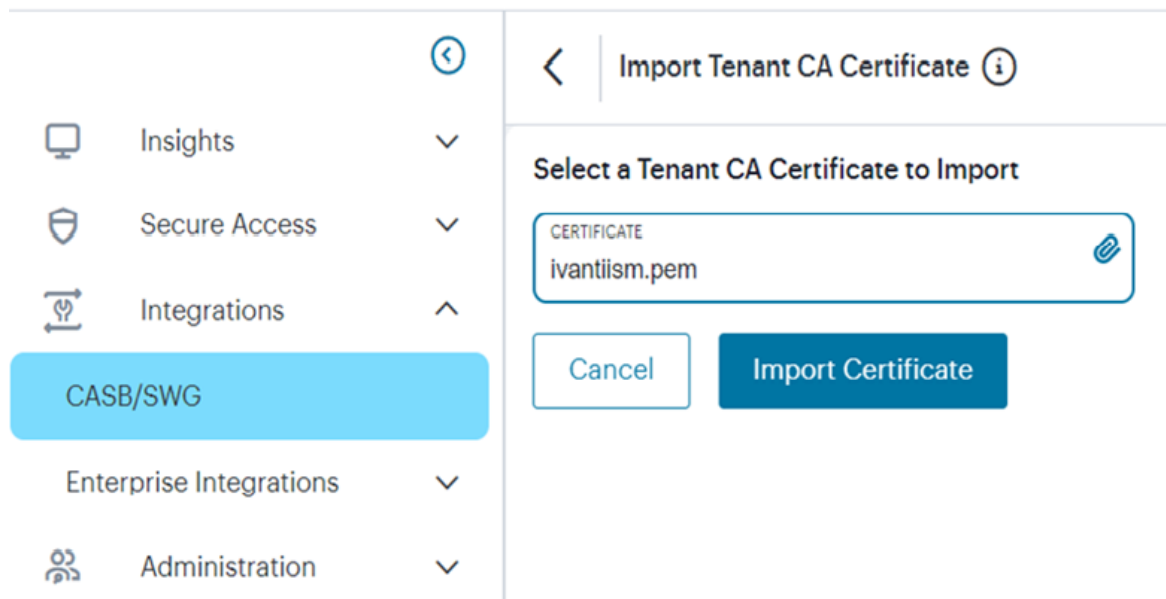
2. Hover over the PAC file to apply to your system configuration and click its clipboard copy icon to copy PAC URL.
3. Select PAC file URL type and paste the copied PAC URL in the “**Enter PAC file URL**” field.
4. Click **Save**.

Importing the Trusted CA certificate to the nZTA

Trusted CA certificate from Lookout Tenant is required to establish a secured connection. Download the certificate in the .pem format from the Trusted CAs tab (Administration > Certificate Management).

To get the Trusted CA cert from Lookout Tenant and import to the user device:

1. In the **Administration > Certificate Management** page in Lookout, click the **Trusted CAs tab**.
2. Download the certificate and save it in the .pem format.
3. Import the root CA certificate to nZTA : navigate to **Integrations > CASB/SWG** and click on **Import Certificate** and select pem file downloaded from steps 2.
4. Click **Save**.



For further information, refer to the *nZTA Tenant Admin Guide*.

Configure SaaS Application on nZTA domain

To configure Salesforce as SaaS application on nZTA domain refer, [here](#).

Use Case 3: Public Internet Access

SWG Overview

Secure WEB Gateway gains visibility, protection and controls access to Internet application to secure your data and safeguards user privacy.

This use case is the Secure Web Gateway (SWG). SWG keeps users safe from cyberthreats and unauthorized traffic from entering and spreading through their internal networks. As a cloud-based solution, SWG monitors user web traffic and enforces policies that define conditions for access to specific websites or types of sites. It plays an important role in protecting employee and user work environments from infections coming from malicious web traffic, sites with vulnerabilities, Internet - borne viruses, malware, and other cyberthreats. SWG also ensures implementation of and compliance with an organization's standards to protect confidential information from exposure. URL filtering, cloud anti-malware, ability to decrypt and inspect websites accessed via HTTPS, Data Loss Prevention (DLP), and Cloud Access Security Broker (CASB) are standard SWG functions .

URL filtering, cloud anti-malware, ability to decrypt and inspect websites accessed via HTTPS, Data Loss Prevention (DLP), and Cloud Access Security Broker (CASB) are standard SWG functions, all of which are available as part of Lookout SSE.

SWG addresses these common use cases:

- Monitor and control access to websites - Protect users from accessing applications, websites, and web content that does not comply with the organization's acceptable use policies.
- Monitor and control access to risky applications - Control usage and user activities based on analytics and insights. Gain visibility into sanctioned and unsanctioned applications and their risk levels.
- Detect and defend against threats - Protect users and devices from threats posed by access to malicious websites, or access to compromised websites that have unintended malicious content on both encrypted and clear-text web traffic.
- Provide data protection and application security - Prevent corporate data loss from insider threats, unintentional data sharing, or data exfiltration from accessing phishing or malicious websites.

Enable SWG on Lookout

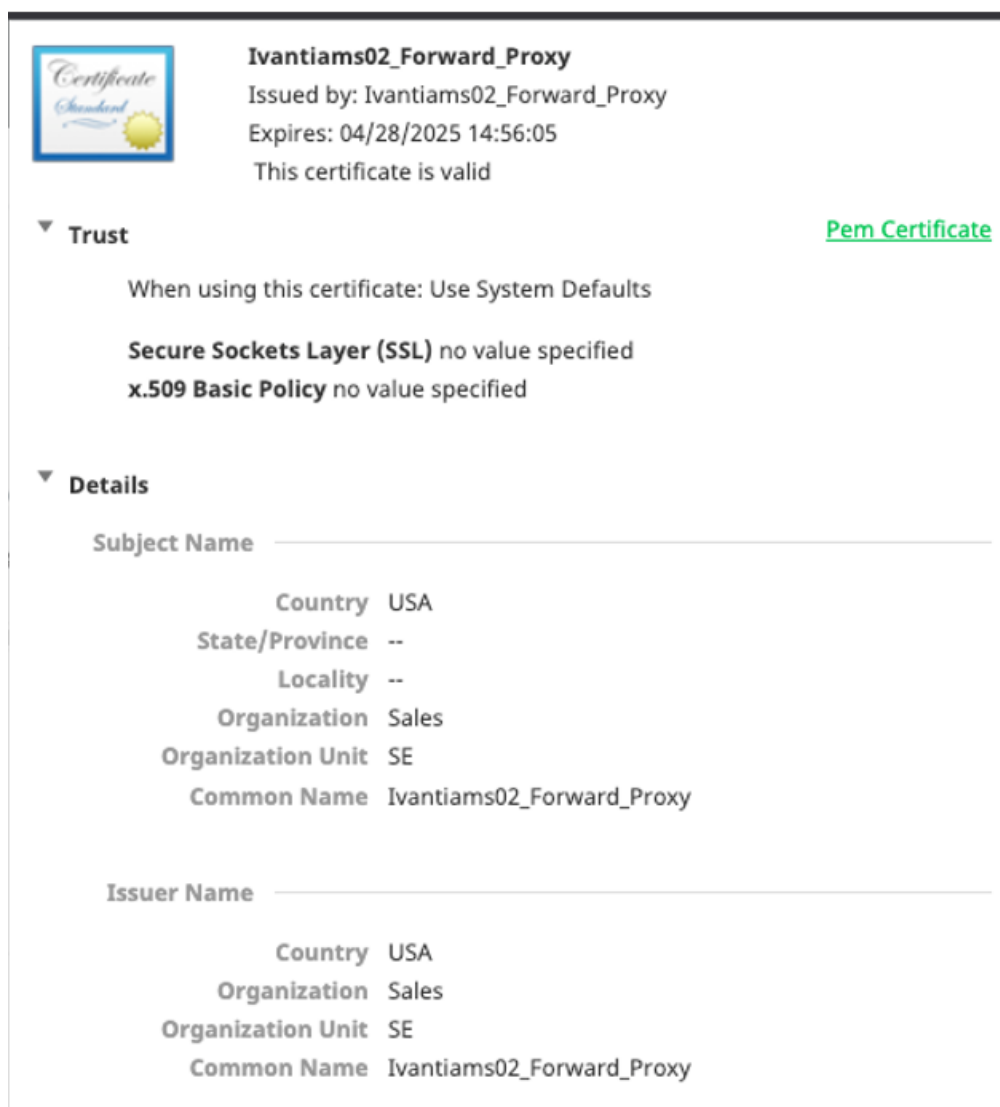
Pre-requisites

- [Enable Proxy](#)
- [Proxy Authentication](#)

Import or Create CA Certificate

To Import or Create CA Certificate:

1. Navigate to **Administration > Certificate Management > Signing CA Certificates**
2. The device must trust this certificate. If you generate a new one, the .pem file should be installed on the clients.
3. After CA Cert is generated, select the **view certificate details**, on the right of the given certificate to get the **PEM Certificate**



If users are using Firefox, the .pem may need to be installed in the browser itself. For best results, use a publicly trusted CA Certificate.



This certificate trust is required for SWG to operate properly.

Create SWG Rule

To create SWG rule in Lookout:

1. Navigate to **Protect > Access Control > New**.
2. Select **Malware Scan** in the Content Inspection Type.

3. Click **Next**.
4. Navigate to the **Websites** section of the left selection pane.
5. Select **System Category** (or some subset of this section).
6. Select **Activities > Select Download**.
7. Click **Next**.
8. Select **Action** and **Secondary Action**.
9. Click **Next** and **Confirm**.



Repeat full process for DLP (instead of Malware Scan) if desired.

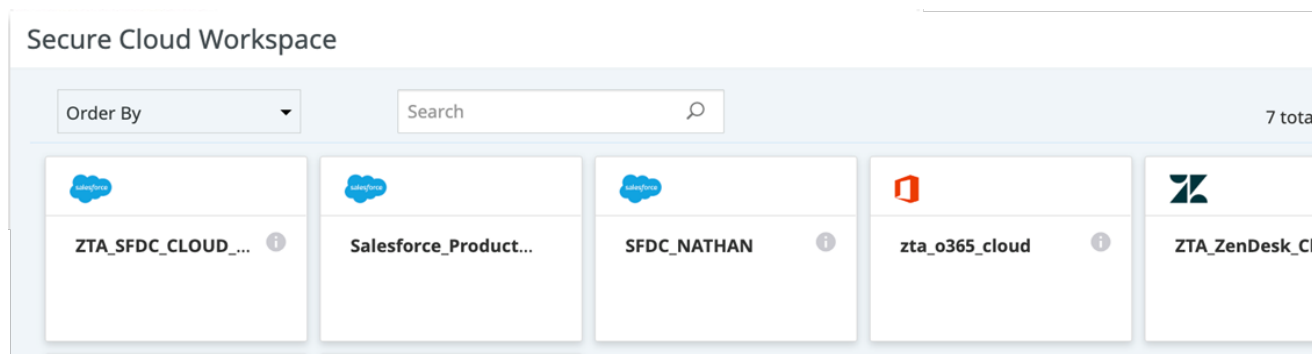
DLP rules are very granular and it is advisable to build separate rules for each action, otherwise debugging of failing rules can be very difficult (because any failure will show as the initial general rule)

For more information on DLP config, refer [Video walkthrough explaining on how DLP works](#)

Download Proxy URL & Certs (install on endpoint)

To download Proxy URL:

1. Navigate to: **Home > Secure Cloud Workspace**
2. Right click on the download link for the HTTP Proxy PAC file and select **copy link address**
 - Example of copied link: <https://domain-ms.ciphercloud.io/public/proxy-swg-http.pac>



Downloading the PAC file from Lookout tenant and configure in nZTA Controller

To download the PAC file:

1. Go to **Home > Secure Cloud Workspace** in Lookout.
2. Download or copy the PAC file link.
3. To configure the PAC file on the ZTA controller, navigate to **Integrations > CASB/SWG** and select Lookout URL type and update value of PAC URL got from step 2.

CASB/SWG

Proxy Auto-configuration (PAC) File URL

Proxy Auto-configuration (PAC) files allow web traffic to be forwarded to the Lookout proxy for inspection and protection before users are connected to the destination.

SELECT PAC FILE URL TYPE: CASB + SWG HTTPS PAC

ENTER PAC FILE URL: <https://ivanti-ms.ciphercloud.io/public/proxy-swg-http>

Tenant CA Certificate for CASB/Lookout Tenant

0 certificates

TENANT CA CERTIFICATE	VALID DATES

No certificate available



In case if HTTP proxy is configured instead of HTTPS then it will prompt for a pop up to enter user name and password on the endpoint when accessing internet or SaaS application using SWG and CASB respectively.

Enter the Lookout Tenant name in the username field and keep the password blank.



Importing the Trusted CA certificate to the nZTA

Trusted CA certificate from Lookout Tenant is required to establish a secured connection. Download the certificate in the .pem format from the Trusted CAs tab (Administration > Certificate Management).

To get the Trusted CA cert from Lookout Tenant and import to the user device:

1. In the **Administration > Certificate Management** page, click the **Trusted CAs tab**.
2. Download the certificate and save it in the .pem format.
3. Import the root CA certificate to the ZTA controller : navigate to **Integrations->CASB/SWG** and click on **Import Certificate** and select pem file downloaded from steps 2.
4. Click **Save**.

←

Import Tenant CA Certificate ⓘ

Select a Tenant CA Certificate to Import

CERTIFICATE
ivantiism.pem

📎

Cancel

Import Certificate

⌵

Insights

⌵

🛡️

Secure Access

⌵

🔗

Integrations

⌴

CASB/SWG

Enterprise Integrations

⌵

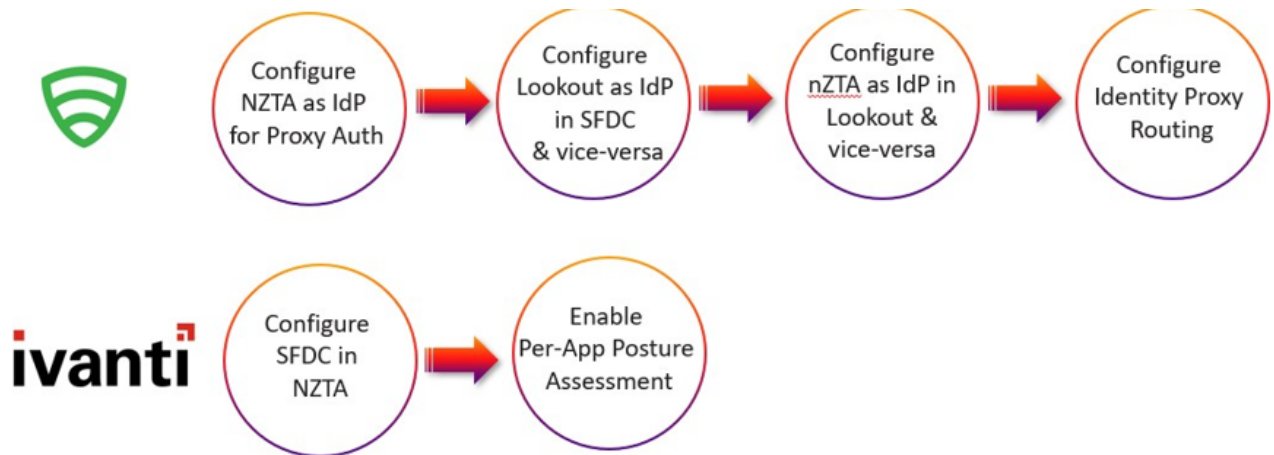
👤

Administration

⌵

Appendix

Reverse Proxy configuration: This configuration is not suggested for PoCs or new admins. The forward proxy will cover most use cases and do so more effectively. In Reverse Proxy mode, Lookout will insert itself into the communication flow as a "Man In The Middle", taking over after the user reaches out directly to the resource (in the return path of communication).



SAML Integration between Lookout (as IdP) and SaaS Application (as SP)

1. Create new SSO Group: **Enterprise Integration > Single Sign-On > SSO Groups**
2. Download Lookout's IdP Metadata for the new SSO Group created
3. Configure SaaS App as SAML SP in Lookout: **Enterprise Integration > Single Sign-On > SSO Providers**
4. Select Type as Cloud Service Provider and configured SSO Group
5. Select Application and Upload SP Metadata file and Validate
6. Configure Lookout as IdP in SaaS app
 - This will differ based on the SaaS Application being integrated

SAML Integration between ZTA (as IdP) and Lookout (as SP)

1. Navigate back to the new SSO Group created in the last section
2. Download Lookout's SP Metadata
3. Configure SaaS App as SAML SP in Lookout: **Enterprise Integration > Single Sign-On > SSO Providers**

4. Select Type as Cloud Service Provider and configured SSO Group
5. Select Application and Upload SP Metadata file and Validate
6. Configure Lookout as IdP in SaaS app
 - This will differ based on the SaaS Application being integrated

Identity Proxy Routing

1. Configure Identity Proxy Routing: **Administration > Enterprise Integration > Single Sign-On > Identity Proxy Routing**
2. Create New Routing Policy
3. Select SSO Group created previously
4. Ivanti NZTA IdP & Cloud Service Provider
5. Associate to create a new routing policy

Configure NZTA as SAML IdP for Proxy Auth

1. Configure NZTA as SAML IdP in Lookout: **Enterprise Integration > Single Sign-On > SSO Providers**
2. Upload NZTA Metadata file and Validate
3. Configure Lookout as Service Provider in IdP
4. Download Lookout SP Metadata: Enterprise Integration -> Single Sign-On -> SSO Providers
5. Upload SP metadata in NZTA Controller (IdP)
 - Add mail & email attributes
 - Attribute: subject_name_format, Value: other
 - Attribute: mail, Value: <username>
 - Attribute: email, Value: <username>
6. Enable Proxy Auth: **Administration > System Settings > Enterprise Authentication**

Documentation

Pulse documentation is available at <https://www.ivanti.com/support/product-documentation>.

Technical Support

When you need additional information or assistance, you can contact "Pulse Secure Global Support Center (PSGSC):

- <https://forums.ivanti.com/s/contactsupport>
- support@ivanti.com

For more technical support resources, browse the support website
<https://forums.ivanti.com/s/contactsupport>