



# **Ivanti Neurons for Zero Trust Access**

## **Getting Started Guide**

**v22.3R4**

Published	Feb 13, 2023
Document Version	1.0
Document Build	release/zta-22.3R4 a6d92401

Ivanti  
10377 South Jordan Gateway  
Suite 110  
South Jordan, Utah 84095  
<https://www.ivanti.com>

© 2022, Ivanti, Inc. All rights reserved.

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](http://www.ivanti.com).

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

The information in this document is current as of the date on the title page.

#### END USER LICENSE AGREEMENT

The Ivanti product that is the subject of this technical documentation consists of (or is intended for use with) Ivanti software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <https://www.ivanti.com/company/legal/eula>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Contents

<b>Getting Started with Ivanti Neurons for Zero Trust Access</b>	<b>1</b>
What is nZTA	1
Deploying and Using nZTA	2
Manually Configuring Your nZTA Deployment	4
<b>Creating User Authentication Services</b>	<b>5</b>
Workflow: Creating a Local Authentication Policy	7
Workflow: Creating a SAML Authentication Policy with Azure AD	14
Workflow: Creating a SAML Authentication Policy with On-Prem ICS	23
Workflow: Adding TOTP to an Authentication Policy	32
Unlocking Locked User Accounts	37
Creating User Rules and User Groups	38
Creating User Rules	38
Creating User Groups	41
Next Steps	42
<b>Configuring Gateways</b>	<b>43</b>
Introduction	43
White-listing Required IP Addresses for your Services	45
High Availability	46
Configuring a Default Gateway	46
Gateway Deployment Workflows	46
Workflow: Creating a Gateway in VMware vSphere	47
Workflow: Creating a Gateway in Amazon Web Services	53
Workflow: Creating a Gateway in Microsoft Azure	59
Creating a Gateway through Azure Marketplace	64
Creating an Gateway using the Azure Template and Image Files	68
Workflow: Creating a Gateway in KVM/OpenStack	72
Preparing to Create a KVM Gateway	73
Adding a KVM Gateway in nSA	74
Preparing Metadata for OpenStack	77
Creating the KVM Gateway Virtual Machine Instance in OpenStack	79
Workflow: Creating a Gateway in Google Cloud Platform	84
Preparing to Create a GCP Gateway	84
Adding a GCP Gateway in nSA	87
Downloading Metadata for Google Cloud Platform	90
Uploading the GCP Virtual Machine Image onto the Google Cloud Platform	90
Creating a VM Instance of the Uploaded GCP Image Manually	92
Creating a VM Instance of the Uploaded GCP Image Using a Script/Template	97
Completing the Configuration of the Controller	99
Next Steps	100

<b>Creating Device Policies and Device Rules</b>	<b>101</b>
Introduction . . . . .	101
Creating Device Rules . . . . .	103
Options for Antispyware and Firewall Rules . . . . .	106
Options for Antivirus Rules . . . . .	107
Options for CVE Check Rules . . . . .	108
Options for Command Rules . . . . .	108
Options for File Rules . . . . .	108
Options for Location Rules . . . . .	109
Options for Hard Disk Encryption Rules . . . . .	109
Options for MAC Address Rules . . . . .	110
Options for Netbios Rules . . . . .	110
Options for Network Rules . . . . .	110
Options for OS Rules . . . . .	111
Options for Process Rules . . . . .	111
Options for Port Rules . . . . .	112
Options for Patch Management Rules . . . . .	112
Options for Registry Rules . . . . .	113
Options for Risk Sense Rules . . . . .	114
Options for System Integrity Rules . . . . .	115
Options for Time of Day Rules . . . . .	115
Creating Device Policies . . . . .	116
Next Steps . . . . .	119
<b>Creating Applications and Application Groups</b>	<b>121</b>
Introduction . . . . .	121
Adding Applications to the Controller . . . . .	122
Adding Application Groups to the Controller . . . . .	125
Next Steps . . . . .	127
<b>Creating a Secure Access Policy</b>	<b>129</b>
Introduction . . . . .	129
Workflow: Creating a Secure Access Policy . . . . .	131
Next Steps . . . . .	134

# Getting Started with Ivanti Neurons for Zero Trust Access

- [What is nZTA](#) (page 1)
  - [Deploying and Using nZTA](#) (page 2)
  - [Manually Configuring Your nZTA Deployment](#) (page 4)
- 

This guide is intended as an introduction to using Ivanti Neurons for Zero Trust Access (nZTA), a component part of Ivanti Neurons for Secure Access. It contains a brief description of the elements that make up the complete service, including a summary of the steps you need to follow to set everything up at a basic level. To obtain further details regarding any of the concepts discussed in this guide, refer to the *Tenant Admin Guide* available from the documentation link in the Ivanti Neurons for Secure Access Tenant Admin Portal.

## What is nZTA

nZTA is a cloud-based SaaS (software as a service) application that provides fully-managed zero-trust authentication and access control for an organization's application infrastructure. nZTA enables administrators to define end-to-end authorization and authentication policies that control application visibility, access, and security for all users and their devices.

An administrator can use the nZTA admin portal to define secure access policies for any combination of **users**, **devices**, **applications**, and **infrastructure**.

## Deploying and Using nZTA

A nZTA deployment consists of a Controller service, used to manage your secure access policies and user base, and one or more ZTA Gateway instances (referred to as *Gateways* in this guide) positioned at each location an organization hosts its resources and applications. This might be in a public or private cloud, within a datacenter, or inside a virtual host environment. The Gateways continually communicate with the Controller to ensure user access requests for the applications held at that location are valid and authentic.

*End-users* install and run Ivanti Secure Access Client on their devices in order to manage secure and encrypted access to their organization's applications. Ivanti Secure Access Client works with the Controller and Gateways to assess authentication and authorization rights so applications that appear to the end user are only those they are authorized to use.

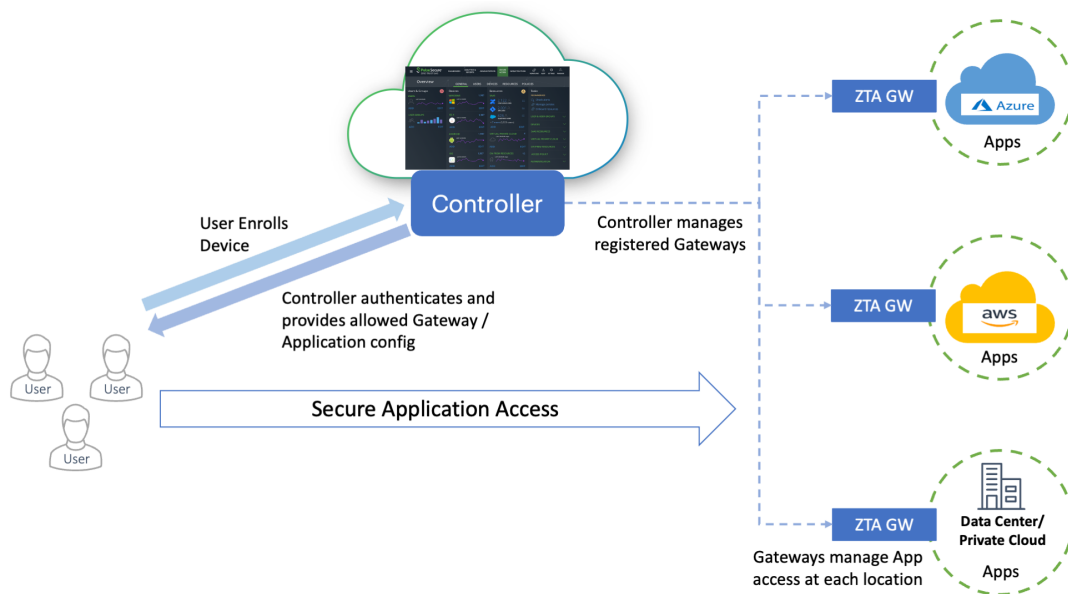


FIGURE 1.1 : The topology of a nZTA deployment

To use and configure the Controller, nZTA provides the *Tenant Admin portal*. This portal allows you to perform all of the tasks required to set up and maintain a working nZTA deployment.

To login to the Tenant Admin Portal, use the credential and domain information provided in your Welcome email. Contact your support representative for more information.

Until nZTA is a configured system, a **Welcome** dialog appears. Accept this dialog. The **Secure Access Setup** (Onboarding) wizard appears.

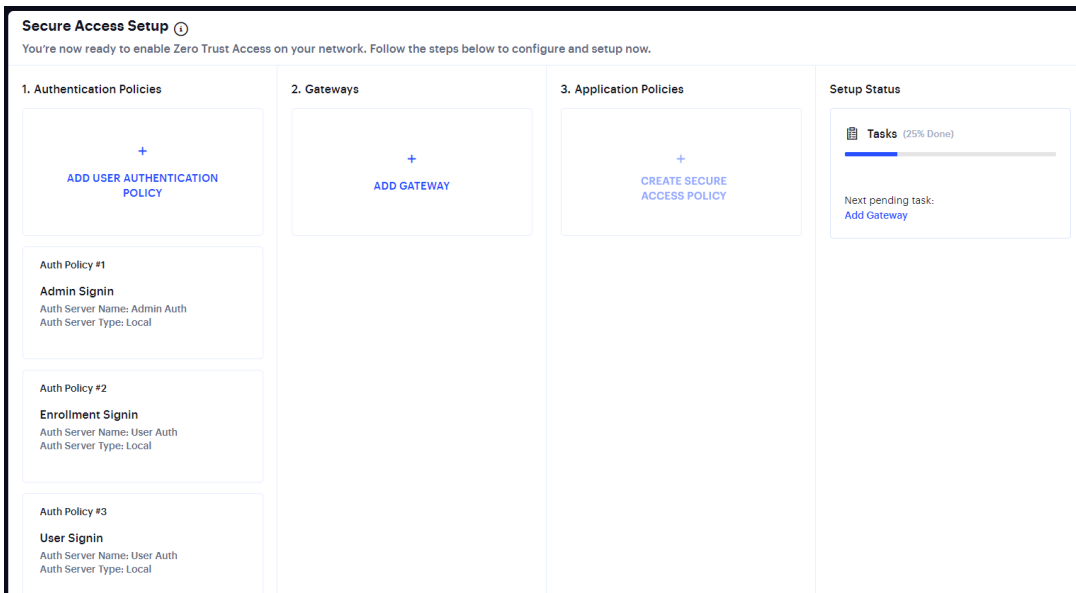


FIGURE 1.2 : The Secure Access Setup (Onboarding) Wizard

This wizard enables you to configure the required elements of nZTA using a number of pages and workflows:

- **Add User Authentication Policy.** This displays the **User Policies** page. Local authentication policies are present by default, which can be used immediately. If you choose to use the default local authentication policies, you can proceed directly to the **Add Gateway** step. If you choose to create your own local authentication policies, or to immediately implement SAML authentication, these must be performed separately from the **Onboarding** wizard, see [Creating User Authentication Services](#) (page 5).
- **Add Gateway.** This displays the Gateway Network Configuration dialog, see [Configuring Gateways](#) (page 43).
- **Application Policies.** This displays the **Create Secure Access Policy** wizard. This wizard enables you to create and publish a secure access policy as a single workflow. This involves the creation/selection of user rules/groups, applications, policies and a gateway selection. To perform these steps individually, and finally create a secure access policy, see [Manually Configuring Your nZTA Deployment](#) (page 4). To perform these steps using the wizard, refer to the *Tenant Admin Guide*.

As you complete each step, the **Setup Status** indicates the percentage of **Tasks** that are complete.

After all tasks are complete, click **Go to Dashboard**.

---

**Note:** You can also start the Onboarding wizard from the nZTA menu; click the **Secure Access** icon, then select **Onboarding**.

---

---

**Note:** To view guidance on client device enrollment and a description of the tools you can use to monitor your nZTA services, see the *Tenant Admin Guide*.

---

## Manually Configuring Your nZTA Deployment

To set up your nZTA deployment, follow these steps:

1. Create your user authentication methods, policies, and groups, see [Creating User Authentication Services](#) (page 5).
2. Create and deploy your nZTA application Gateways, see [Configuring Gateways](#) (page 43).
3. Create your device rules and device policies, see [Creating Device Policies and Device Rules](#) (page 101)
4. Create your applications and application groups, see [Creating Applications and Application Groups](#) (page 121)
5. Create a secure access policy for an application and publish this policy to your Gateways, see [Creating a Secure Access Policy](#) (page 129).



# Creating User Authentication Services

- [Workflow: Creating a Local Authentication Policy](#) (page 7)
- [Workflow: Creating a SAML Authentication Policy with Azure AD](#) (page 14)
- [Workflow: Creating a SAML Authentication Policy with On-Prem ICS](#) (page 23)
- [Workflow: Adding TOTP to an Authentication Policy](#) (page 32)
- [Creating User Rules and User Groups](#) (page 38)
- [Next Steps](#) (page 42)

---

Ivanti Neurons for Zero Trust Access (nZTA) provides user authentication through **authentication policies**. Policies define the application of an **authentication method** for a specified access URL.

nZTA facilitates *Multi-Factor Authentication* (MFA) through the configuration of an optional secondary authentication method in a policy. MFA-based policies can use *Local authentication* or *Time-based One Time Password (TOTP)* as the secondary method.

nZTA also provides for the definition of **user rules** and **user groups**. Rules act as filters and define the basic criteria by which users' credentials must match in order for authentication to proceed. Groups encapsulate an authentication policy with one or more user rules to provide a complete user authentication definition for your secure access policy. To learn more about creating **user rules** and **user groups**, see [Creating User Rules and User Groups](#) (page 38).

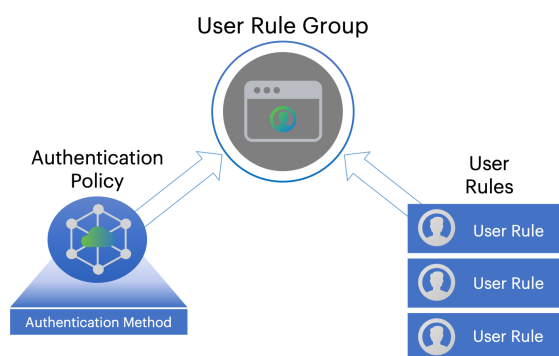


FIGURE 2.1 : The relationship between user groups, rules, authentication policies and methods

nZTA provides three default/built-in authentication policies, suitable for the primary use-cases of administrative sign-in, user enrollment, and user sign-in:

- *Admin SignIn*. This policy is used whenever admin users log in. That is, for connection requests to the `*/login/admin/` URL. It is referenced by the `ALLADMINUSERS` user rule, which associates it with the `ADMINISTRATORS` user rule group.
- *Enrollment SignIn*. This policy can be used for enrolling a desktop/mobile client device. That is, for connection requests to the `*/login/enroll/` URL. It is referenced by the `ALLENROLLMENTUSERS` user rule, which associates it with the `ENROLLMENT` user rule group. You typically do not invite your users to connect directly to this endpoint, and instead link the policy to an equivalent user sign-in policy (such that users connecting an un-enrolled device to the sign-in policy are automatically redirected here).
- *User SignIn*. This policy can be used as the primary connection endpoint for all user device sign-in and enrollment requests. That is, for connection requests to the `*/login/` URL. It is referenced by the `ALLUSERS` user rule, which associates it with the `USERS` user rule group. As mentioned above, users connecting an un-enrolled device to this policy are automatically redirected to the *Enrollment SignIn* policy.

These policies are fixed and cannot be deleted. However, you can edit them to reference specific authentication methods.

---

**Note:** MFA is supported for *Admin SignIn* and *User SignIn* policies only. To learn more, see the *Tenant Admin Guide*.

---

Furthermore, you can create additional custom authentication policies to enable bespoke authentication for specific groups of users or parts of your organization. Each policy should contain a unique access URL to which your users connect, and each should then be configured to link to authentication methods applicable for that purpose.

nZTA supports creating authentication services based on the following methods:

- **Local authentication:** An authentication system that is internal to the

Controller. You must create all users manually on the Controller, and configure any required authentication policies. See [Workflow: Creating a Local Authentication Policy](#) (page 7).

- **Azure AD SAML authentication:** An existing remote SAML authentication system based on an Azure AD server. See [Workflow: Creating a SAML Authentication Policy with Azure AD](#) (page 14).
- **On-prem |PCS\_shortcode| SAML authentication:** An existing remote SAML authentication system based on an On-Prem ICS server. See [Workflow: Creating a SAML Authentication Policy with On-Prem ICS](#) (page 23).
- **Time-based One Time Password (TOTP) authentication:** A one-time use password authenticator whereby a password (also known as a token) is generated by the Controller and the client from a shared secret key and the current time. TOTP is used as a secondary authentication method as part of a *Multi-Factor Authentication* deployment. See [Workflow: Adding TOTP to an Authentication Policy](#) (page 32).

---

**Note:** For further supported SAML authentication services, see the *Tenant Admin Guide*.

---

In each of the scenarios listed in this guide, to ensure that your users can access the authentication mechanism defined through this process, make sure your *Secure Access Policies* are configured with a **User Group** in which your newly-configured authentication policies are defined.

## Workflow: Creating a Local Authentication Policy

Local authentication involves creating user records held locally in the Controller. Before you begin this process, make sure you have all user details (name and password) ready.

To configure a *new* local authentication method:

1. Log into the Tenant Admin Portal as an administrator.
2. From the nZTA menu, select the **Secure Access** icon, then select **Manage Users > Authentication Servers**.

The **Authentication Servers** page appears. This page lists all existing user authentication methods. For example:

Manage Users ⊙

User Groups User Rules User Policies Authentication Servers Create Authentication Server

**Note**  
Authentication Servers which **default** OR linked to any **User Policy**, will be disabled from selection.  
Local Authentication Servers which have one or more users linked to them will be disabled from selection.

30 TOTAL SEARCH Batch Delete

<input type="checkbox"/>	STATUS	NAME ↑	DEFAULT ↑	AUTHENTICATION METHOD ↑	USERS	
<input type="checkbox"/>	>	account-auth		SAML (Azure AD)	N/A	⋮
<input type="checkbox"/>	>	account-enrollment		SAML (Azure AD)	N/A	⋮
<input type="checkbox"/>	>	Aditi		Local	1 Users	⋮
<input type="checkbox"/>	>	Admin Auth	⊙	Local	93 Users	⋮
<input type="checkbox"/>	>	auth-enroll-manual		SAML (Azure AD)	N/A	⋮
<input type="checkbox"/>	>	authsaml-man		SAML (Azure AD)	N/A	⋮
<input type="checkbox"/>	>	azure-auth-manual		SAML (Azure AD)	N/A	⋮
<input type="checkbox"/>	>	AzureAD-Auth		SAML (Azure AD)	N/A	⋮
<input type="checkbox"/>	>	AzureAD-Enroll		SAML (Azure AD)	N/A	⋮

FIGURE 2.2 : User Authentication Methods

3. Click **Create Authentication Server**.

A form appears that enables you to define the authentication method.

< Create Authentication Server ⊙

**Create Authentication Server**  
An authentication method is referenced from one or more authentication policies. nSA supports user authentication through the following user authentication methods: Local, SAML (Azure AD) and SAML (Custom). Reset Fields

Choose Server Name and Authentication Type

Authentication Server Name\* ⊙ AUTHENTICATION TYPE Local ⊙

**LIST OF LOCAL USERS**  
0 USER(S) FOUND CREATE USER Batch Delete

<input type="checkbox"/>	USERNAME	FULL NAME	CHANGE PASSWORD	EMAIL

Cancel Create Authentication Server

FIGURE 2.3 : User Authentication Method Wizard

**Note:** At any point during this process, you can reset the form data by clicking **Reset Fields**.

4. Under **Choose name and type**:

- Specify an **Authentication Server Name**.
- Select the **Authorization Type** of *Local*.

5. Click **Create User**. The *Create Local User* dialog appears to show additional local authentication settings:

FIGURE 2.4 : Adding local users to a new authentication method

6. Enter the following settings:

- Specify a **User Name**, **Full Name**, and **Email** for the user.
- Specify a **Password** and **Confirm Password** for the user.
- (Optional) Select the **Temporary Password** check box if you want the user to change their password when they first log in.
- Click **Create User**.

The user is added to the list of users.

7. Repeat the previous step for each required user.

8. Click **Create Authentication Server**.

The new local user authentication method is added to the list of methods and the process is complete.

After you have created your local authentication method, create or update your authentication policies with the new authentication method. In most cases, you need a minimum of two policies:

- user enrollment
- user sign-in

nZTA provides built-in policies to cover both basic cases. In addition, nZTA allows for the definition of custom policies to facilitate separate authentication endpoints for specific groups of users. To learn more, see the *Tenant Admin Guide*.

Repeat the following steps for each policy, starting with enrollment:

1. From the nZTA menu, click the **Secure Access** icon, then select **Manage Users > User Policies**.

The **User Policies** page appears. This page lists all existing user authentication policies.

STATUS	NAME	DEFAULT	POLICY USER	ACCESS URL	SERVER	SERVER TYPE	DEVICE POLICY
<input type="checkbox"/>	> accounts-euth		user	*/login/accounts/	account-a...	SAML (Azu...	⋮
<input type="checkbox"/>	> accounts-enrollment		enroll	*/login/accountsenro...	account-e...	SAML (Azu...	⋮
<input type="checkbox"/>	Admin Signin	<input checked="" type="checkbox"/>	admin	*/login/admin/	Admin Auth	Local	⋮
<input type="checkbox"/>	cxo		admin	*/login/cxo/	cxo	Local	⋮
<input type="checkbox"/>	cxoics		admin	*/login/cxoics/	cxoics	Local	⋮
<input type="checkbox"/>	> Enrollment Signin	<input checked="" type="checkbox"/>	enroll	*/login/enroll/	AzureAD-E...	SAML (Azu...	⋮
<input type="checkbox"/>	> kan_mfa		admin	*/login/QA/	kan-samla...	SAML (Azu...	⋮
<input type="checkbox"/>	netadmin		admin	*/login/netadmin/	net-admin	Local	⋮

FIGURE 2.5 : User Authentication Policies

From this page, either create a new custom policy or edit an existing policy.

2. To add a new custom policy, click **Create User Policy**.

The **Create Authentication Policy** form appears.

FIGURE 2.6 : Create Authentication Policy

---

**Note:** To learn more about how custom policies are used for user login and enrollment, see the *Tenant Admin Guide*.

---

3. Enter a **Policy Name**.

4. Enter a **Login URL** using the format `*/login/<path>/`.

The URL must start with `*/login/` and cannot contain any special characters. `<path>` should be set to a unique value reflecting the endpoint URL you want to define for this authentication policy (appended with a backslash):

- In the case of user sign-in policies, this is the URL endpoint (appended to the tenant FQDN) to which new users are invited to connect to enroll or sign-in a device with the Controller. Example value: `*/login/saleslogin/`.
- In the case of user enrollment policies, this endpoint identifies the enrollment URL to which users are redirected if they attempt to connect to the equivalent sign-in policy with an un-enrolled device. In most cases, you do not advertise this endpoint to your users. Example value: `*/login/salesenroll/`.

---

**Note:** In some enrollment circumstances, such as when using a device pre-installed with an older version of Ivanti Secure Access Client, you connect directly to the enrollment policy endpoint to enroll the device. For more details, see the *Tenant Admin Guide*.

---

5. (Optional) Enter a description for the authentication policy.

6. Select a **User Type** based on the intended authentication activity for this policy. Choose from:

- **Enrollment Users:** Select this option to define the authentication endpoint for enrollment of new end-user devices. This endpoint is reserved for enrollment and not normally provided directly to users.
- **Users:** Select this option to define the user sign-in endpoint for enrolled devices. This is the endpoint that you provide to your users to access the service (regardless of enrollment status).
- **Administrators:** Select this option to define the authentication endpoint for administrator-level sign-in. This endpoint is used for administrator login to the Controller only.

7. (for policies with a **User Type** of “Users” only): Select an **Enrollment Policy** from the drop-down list to be linked to this sign-in policy (as indicated):

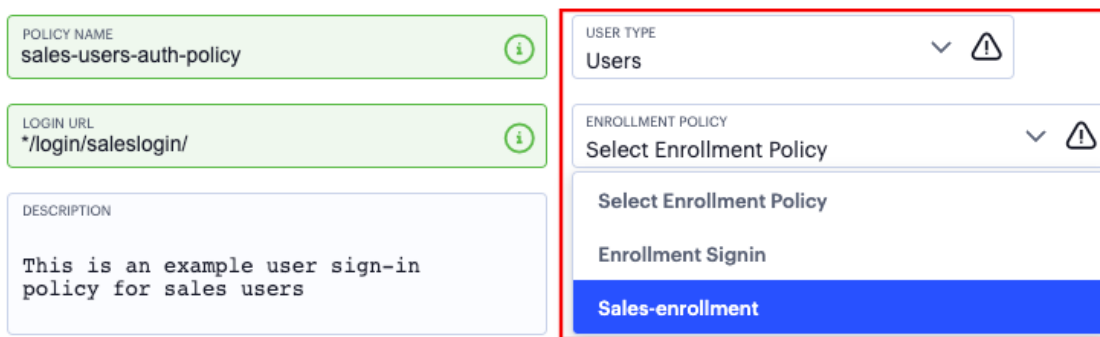


FIGURE 2.7 : Linking an enrollment policy to a user sign-in policy

This is the enrollment policy to which a user is redirected if it is determined that the device is not yet enrolled.

- Under **Policy Server Details**, click **Primary Auth Server**, and choose the required authentication method for the policy from the drop-down list:

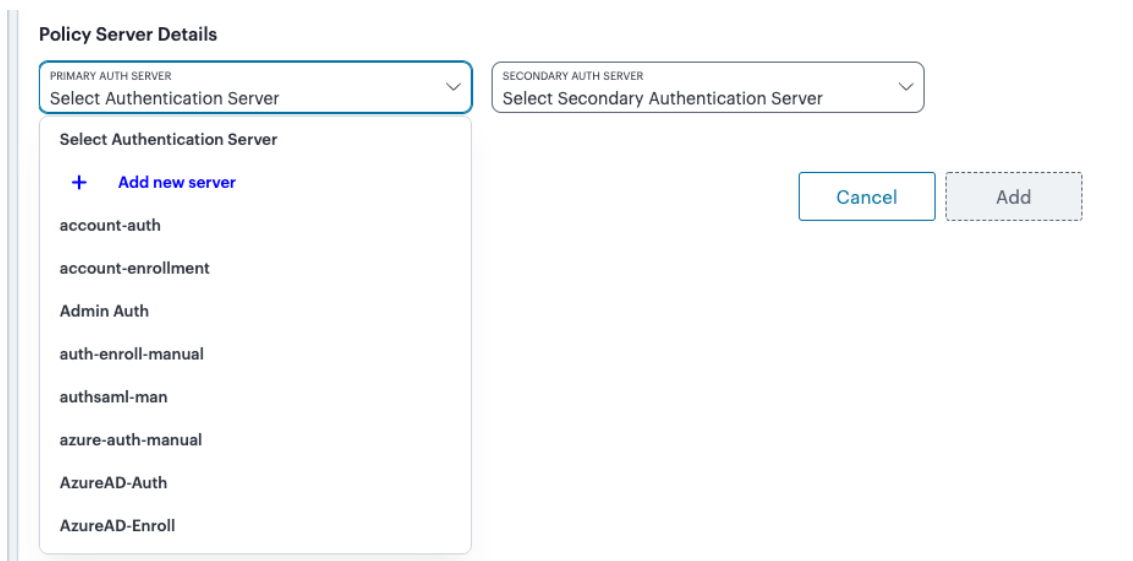


FIGURE 2.8 : Selecting a primary authentication method for this policy

Alternatively, select *Add New Server* and create a new authentication method as per the steps described earlier in this section.

- (Optional) Where a secondary method is required for Multi-Factor Authentication, repeat the previous step for **Secondary Auth Server**.

---

**Note:** Secondary authentication methods do not apply to *Enrollment User* type policies. The relevant field is hidden in this case.

---

- Click **Create User Policy** to create the new policy.

The new policy is added to the list of authentication policies.

If you instead elect to update an existing custom or built-in policy:



1. Click the three dots adjacent to the relevant policy and click **Edit**.

The **Edit authentication policy** form appears.

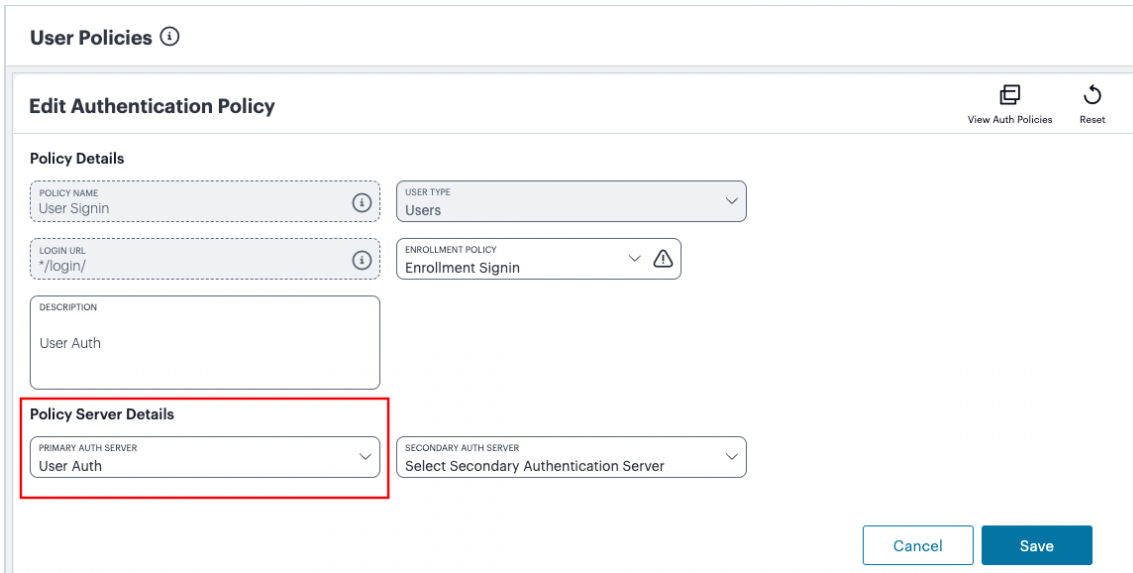
---

**Note:** For built-in authentication policies, all properties except **Primary Auth Server** and **Secondary Auth Server** (where applicable) are read-only.

---

2. Configure the primary and/or secondary authentication methods, as required:

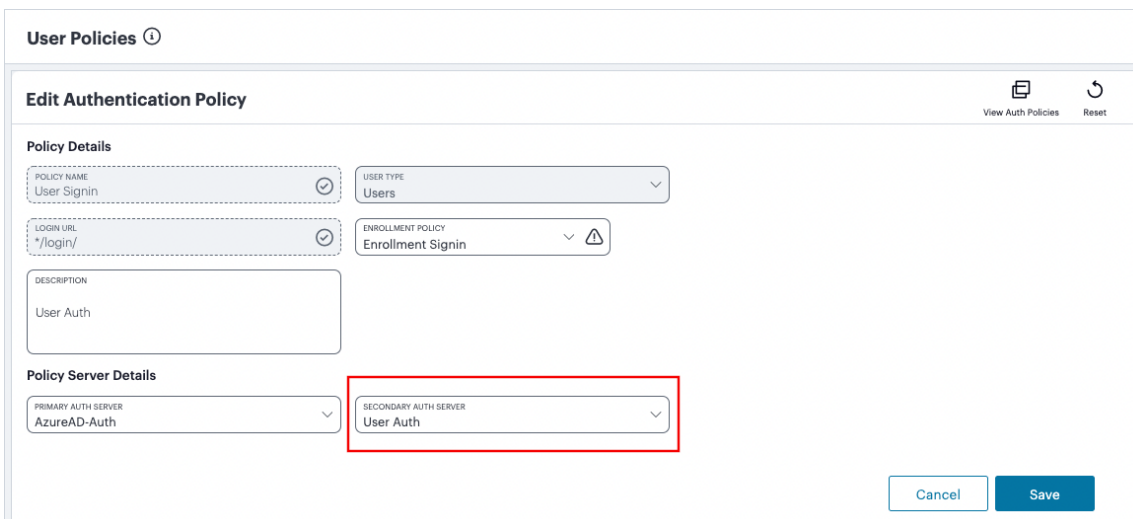
- Set the **Primary Auth Server** to be the new local user authentication method (indicated):



The screenshot shows the 'Edit Authentication Policy' form. The 'Policy Details' section includes fields for 'POLICY NAME' (User Signin), 'USER TYPE' (Users), 'LOGIN URL' (\*login/), and 'ENROLLMENT POLICY' (Enrollment Signin). The 'DESCRIPTION' field contains 'User Auth'. The 'Policy Server Details' section is highlighted with a red box and contains two dropdown menus: 'PRIMARY AUTH SERVER' (set to 'User Auth') and 'SECONDARY AUTH SERVER' (set to 'Select Secondary Authentication Server'). At the bottom right, there are 'Cancel' and 'Save' buttons.

FIGURE 2.9 : Editing the primary auth server

- If you are configuring a policy for MFA, set the **Secondary Auth Server** to be the new local user authentication method (indicated):



The screenshot shows the 'Edit Authentication Policy' form. The 'Policy Details' section includes fields for 'POLICY NAME' (User Signin), 'USER TYPE' (Users), 'LOGIN URL' (\*login/), and 'ENROLLMENT POLICY' (Enrollment Signin). The 'DESCRIPTION' field contains 'User Auth'. The 'Policy Server Details' section is highlighted with a red box and contains two dropdown menus: 'PRIMARY AUTH SERVER' (set to 'AzureAD-Auth') and 'SECONDARY AUTH SERVER' (set to 'User Auth'). At the bottom right, there are 'Cancel' and 'Save' buttons.

FIGURE 2.10 : Editing the Secondary auth server

---

**Note:** If you configure a secondary authentication method in a policy that is currently in use, any active user sessions must be disconnected and reconnected for the changes to take effect.

---

3. Click **Save**.

The list of authentication policies updates.

4. Repeat until all required authentication policies are configured with the local authentication method.

## Workflow: Creating a SAML Authentication Policy with Azure AD

Use this workflow to configure the Controller to act as a SAML Service Provider (SP) and engage Azure AD as a remote SAML Identity Provider (IdP).

As a minimum, configuring nZTA to use SAML authentication requires you to create separate SAML apps on the Azure AD platform for the following primary activities:

- User enrollment
- User sign-in

The Controller includes built-in default authentication policies for each of these purposes, and also includes the ability to create your own custom policies for separate authentication of specific user groups. You create an authentication method referencing one of the Azure AD SAML apps described above and then assign the method to an authentication policy of the same type (either the built-in policy, or one you create). Begin with enrollment, and then repeat the process for user sign-in.

Before you can start configuring nZTA, you must first perform the following steps in Azure AD:

1. Create a SAML app for the required activity (enrollment or sign-in) and define at least the following **Basic SAML Configuration fields**:
  - **Identifier (Entity ID)**. This is the URL of the SAML endpoint on the Controller. This is the audience of the SAML response for IdP-initiated SSO. This cannot be left blank.
  - **Reply URL (Assertion Consumer Service URL)**. This is the URL of the SAML consumer on the Controller. This is the destination URL in the SAML response for IdP-initiated SSO. This cannot be left blank.
2. Download the Federation metadata XML definition for the SAML app to your local workstation. Retain this file for later use.
3. Repeat these steps for each activity.

**Note:** For details on how to create SAML apps in Azure AD, see the Azure AD SAML documentation.

After you have completed the above prerequisite steps, you can proceed to configure the Controller. For each SAML app you just created, perform the following steps:

1. Log into the Tenant Admin Portal as an administrator.
2. From the nZTA menu, click the **Secure Access** icon, then select **Manage Users > Authentication Servers**.

The *Authentication Servers* page appears. This page lists all existing user authentication methods. nZTA includes two default authentication methods, one for admins and one for users.

Manage Users ⓘ

User Groups User Rules User Policies Authentication Servers Create Authentication Server

**Note**  
Authentication Servers which **default** OR linked to any **User Policy**, will be disabled from selection.  
Local Authentication Servers which have one or more users linked to them will be disabled from selection.

30 TOTAL SEARCH Batch Delete

<input type="checkbox"/>	STATUS	NAME ↑	DEFAULT ↑	AUTHENTICATION METHOD ↑	USERS
<input type="checkbox"/>	>	account-euth		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	account-enrollment		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	Aditi		Local	1 Users
<input type="checkbox"/>	>	Admin Auth	⊙	Local	93 Users
<input type="checkbox"/>	>	auth-enroll-manual		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	authsemi-man		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	azure-auth-manual		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	AzureAD-Auth		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	AzureAD-Enroll		SAML (Azure AD)	N/A

FIGURE 2.11 : User Authentication Methods

3. Click **Create Authentication Server**.

A form appears that enables you to define the authentication method.

< Create Authentication Server ⓘ

**Create Authentication Server**  
An authentication method is referenced from one or more authentication policies. nSA supports user authentication through the following user authentication methods: Local, SAML (Azure AD) and SAML (Custom). Reset Fields

Choose Server Name and Authentication Type

Authentication Server Name\* ⓘ AUTHENTICATION TYPE Local ⓘ

**LIST OF LOCAL USERS**  
0 USER(S) FOUND CREATE USER Batch Delete

<input type="checkbox"/>	USERNAME	FULL NAME	CHANGE PASSWORD	EMAIL

Cancel Create Authentication Server

FIGURE 2.12 : User Authentication Method Wizard

**Note:** At any point during this process, you can reset the form data by clicking **Reset Fields**.

4. Under **Choose name and type:**

- Specify an **Authentication Server Name**. For example: *Enrollment* or *SignIn*.
- Select the **Authorization Type** of SAML (*Azure AD*).

The form expands to show additional settings:

The screenshot shows a web form titled "User Authentication" with a sub-header "Add Authentication Method". The form is for configuring SAML (Azure AD) authentication. It includes the following fields and options:

- Choose name and type:**
  - Authentication Server Name:** A text input field containing "samlauthtest".
  - Authentication Type:** A dropdown menu set to "SAML (Azure AD)".
- Fields required for SAML Authentication Server:**
  - Allow Unsigned Metadata
  - Single Logout URL:** A text input field.
  - Upload/Enter Manually:** Radio buttons for "Upload" (selected) and "Enter Manually".
  - Location:** A dropdown menu set to "File".
  - File:** A text input field with the placeholder "Upload a file here" and a file upload icon.
- Buttons:** "Cancel" and "Add" buttons at the bottom right.

FIGURE 2.13 : Configuring SAML (Azure AD) authentication settings

5. (Optional) Specify a **Single Logout URL**. For more information, see the *Tenant Admin Guide*.
6. To provide your SAML IdP settings, select one of the following:

- Select **Upload** to upload a digitally-signed (or unsigned) federation metadata XML definition file downloaded for this SAML activity from Azure AD. That is, for either user enrollment or user sign-in.

**Note:** By default, the Controller expects a signed metadata definition file. To allow an unsigned metadata file, select **Allow Unsigned Metadata**.

Then, upload your metadata file by clicking **Upload a file here**.

- Select **Enter Manually** to manually enter the required IdP SAML settings. Use this option in scenarios where a SAML federation metadata file is not available or incomplete.

Then, enter the following details:

**Fields required for SAML Authentication Server**

Upload  Enter Manually






IDP Entity Id	
IDP SSO URL	
IDP Slo Service	
<small>USER NAME TEMPLATE</small> <assertionNameDN.uid>	
IDP Signing Certificate	

FIGURE 2.14 : Configuring SAML (Azure AD) IdP settings manually

The following minimum settings are required for your SAML authentication service to function correctly. Each setting relates to a value configured in the SAML application on your IdP. Contact your IdP administrator to obtain the relevant details:

- **IDP Entity ID:** The entity ID is sent as the Issuer value in the SAML assertion generated by the IdP. Specify the Issuer value in assertions generated by the SAML identity provider.
- **IDP SSO URL:** A URL provisioned by the SAML IdP to support service-provider-initiated Single Sign-On. Use the format `https://<FQDN>`.
- **IDP Slo Service:** (Optional) A URL to specify the Single Log-Out/sign out endpoint if you want to force re-authentication for increased security. Use the format `https://<FQDN>`. For more information, see the *Tenant Admin Guide*.
- **User Name Template:** Specify how the system is to derive the username from the SAML assertion. The default value can be used, or replaced with an alternative specifier that the Controller uses from the incoming assertion. For example: `<assertionNameDN.uid>`, the NameID value where ICS is the IdP, the UID from X509SubjectName, `<userAttr.attr>`, attr from AttributeStatement attributes.
- **IDP Signing Certificate:** The signing certificate to be used with the SAML app on the IdP. Type or paste in the contents of your Base-64 encoded public key.

**Note:** If, at a later date, you need to modify the metadata definition file, edit the authentication method through the *User Authentication* page and repeat

this step. However, note that federation metadata files from Azure AD are digitally-signed and so cannot be manually edited prior to upload back into nSA. This process supports replacing a definition file *only* with another digitally-signed and validated definition file.

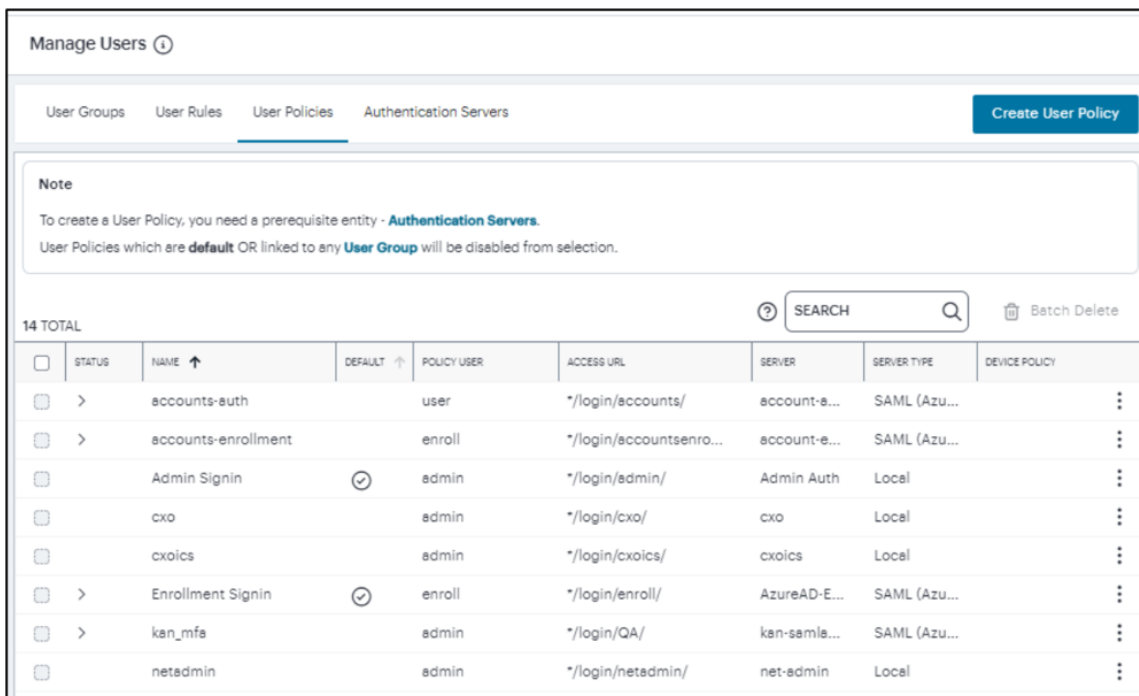
7. Confirm that your settings are correct, then select **Add** to create the authentication method.

The new SAML user authentication method is added to the list of methods displayed in the **User Authentication** page, and the process completes.

After you have created your SAML authentication method, create or update your authentication policies with the new authentication method:

1. From the nZTA menu, click the **Secure Access** icon, then select **Manage Users > User Policies**.

The **User Policies** page appears. This page lists all existing user authentication policies.



The screenshot shows the 'Manage Users' interface with the 'User Policies' tab selected. A note indicates that a prerequisite entity 'Authentication Servers' is needed to create a policy. Below the note is a table of 14 policies. The table has columns: STATUS, NAME, DEFAULT, POLICY USER, ACCESS URL, SERVER, SERVER TYPE, and DEVICE POLICY. The 'Admin Signin' and 'Enrollment Signin' policies are marked as default with a checkmark icon.

STATUS	NAME	DEFAULT	POLICY USER	ACCESS URL	SERVER	SERVER TYPE	DEVICE POLICY
<input type="checkbox"/>	> accounts-auth		user	*/login/accounts/	account-a...	SAML (Azu...	⋮
<input type="checkbox"/>	> accounts-enrollment		enroll	*/login/accountsenro...	account-e...	SAML (Azu...	⋮
<input type="checkbox"/>	Admin Signin	<input checked="" type="checkbox"/>	admin	*/login/admin/	Admin Auth	Local	⋮
<input type="checkbox"/>	cxo		admin	*/login/cxo/	cxo	Local	⋮
<input type="checkbox"/>	cxoics		admin	*/login/cxoics/	cxoics	Local	⋮
<input type="checkbox"/>	> Enrollment Signin	<input checked="" type="checkbox"/>	enroll	*/login/enroll/	AzureAD-E...	SAML (Azu...	⋮
<input type="checkbox"/>	> kan_mfa		admin	*/login/QA/	kan-samle...	SAML (Azu...	⋮
<input type="checkbox"/>	netadmin		admin	*/login/netadmin/	net-admin	Local	⋮

FIGURE 2.15 : User Authentication Policies

To learn more about the policies on this page, see the *Tenant Admin Guide*.

From this page, either create a new custom policy or edit an existing policy.

2. To add a new custom policy, click **Crate User Policy**.

The **Create Authentication Policy** form appears.

The screenshot shows a web interface for creating an authentication policy. The title is 'Create User Policies' with a back arrow and an information icon. Below the title is the sub-header 'Create Authentication Policy' and a prompt 'Enter a name and description for the Authentication Policy'. The form contains several input fields: 'POLICY NAME' (with a placeholder 'Enter a name'), 'LOGIN URL' (with a placeholder '\*/login/your-path'), and 'DESCRIPTION' (with a placeholder 'Add a description of the Authentication Policy'). There are also two dropdown menus: 'USER TYPE' (set to 'Enrollment Users') and 'DEVICE POLICY' (set to 'Select a Device Policy'). A section titled 'Auth Servers' includes a 'Note' about Local and SAML servers and a 'PRIMARY AUTH SERVER (REQUIRED)' dropdown set to 'Select from Local and SAML Auth Servers'. At the bottom right, there are 'Cancel' and 'Create User Policy' buttons.

FIGURE 2.16 : Add User Authentication

---

**Note:** At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing authentication policies in a pop-up dialog by clicking **View Auth Policies**.

---

**Note:** To learn more about how custom policies are used for user login and enrollment, see the *Tenant Admin Guide*.

---

3. Enter a **Policy Name**.
4. Enter a **Login URL** using the format `*/login/<path>/`.

The URL must start with `*/login/` and cannot contain any special characters. `<path>` should be set to a unique value reflecting the endpoint URL you want to define for this authentication policy (appended with a backslash):

- In the case of user sign-in policies, this is the URL endpoint (appended to the tenant FQDN) to which new users are invited to connect to enroll or sign-in a device with the Controller. Example value: `*/login/saleslogin/`.
- In the case of user enrollment policies, this endpoint identifies the enrollment URL to which users are redirected if they attempt to connect to the equivalent sign-in policy with an un-enrolled device. In most cases, you do not advertise this endpoint to your users. Example value: `*/login/salesenroll/`.

---

**Note:** In some enrollment circumstances, such as when using a device

pre-installed with an older version of Ivanti Secure Access Client, you connect directly to the enrollment policy endpoint to enroll the device. For more details, see the *Tenant Admin Guide*.

5. (Optional) Enter a description for the authentication policy.
6. Select a **User Type** based on the intended authentication activity for this policy. Choose from:
  - **Enrollment Users:** Select this option to define the authentication endpoint for enrollment of new end-user devices. This endpoint is reserved for enrollment and not normally provided directly to users.
  - **Users:** Select this option to define the user sign-in endpoint for enrolled devices. This is the endpoint that you provide to your users to access the service (regardless of enrollment status).
  - **Administrators:** Select this option to define the authentication endpoint for administrator-level sign-in. This endpoint is used for administrator login to the Controller only.
7. (for policies with a **User Type** of “Users” only): Select an **Enrollment Policy** from the drop-down list to be linked to this sign-in policy (as indicated):

The screenshot displays a configuration form for a policy. On the left, there are three fields: 'POLICY NAME' with the value 'sales-users-auth-policy', 'LOGIN URL' with the value '\*/login/saleslogin/', and 'DESCRIPTION' with the text 'This is an example user sign-in policy for sales users'. On the right, there are three dropdown menus. The first is 'USER TYPE' set to 'Users'. The second is 'ENROLLMENT POLICY' set to 'Select Enrollment Policy'. The third is a list of enrollment policies: 'Select Enrollment Policy', 'Enrollment Signin', and 'Sales-enrollment', with 'Sales-enrollment' highlighted in blue. A red box highlights the 'USER TYPE' and 'ENROLLMENT POLICY' dropdowns.

FIGURE 2.17 : Linking an enrollment policy to a user sign-in policy

This is the enrollment policy to which a user is redirected if it is determined that the device is not yet enrolled. To learn more, see the *Tenant Admin Guide*.

8. Under **Policy Server Details**, click **Primary Auth Server**, and select the required authentication method from the drop-down list:



The screenshot shows the 'Policy Server Details' form. It has two dropdown menus: 'PRIMARY AUTH SERVER' and 'SECONDARY AUTH SERVER'. The 'PRIMARY AUTH SERVER' dropdown is open, showing a list of authentication servers: '+ Add new server', 'account-auth', 'account-enrollment', 'Admin Auth', 'auth-enroll-manual', 'authsaml-man', 'azure-auth-manual', 'AzureAD-Auth', and 'AzureAD-Enroll'. To the right of the dropdowns are 'Cancel' and 'Add' buttons.

FIGURE 2.18 : Selecting a primary authentication method for this policy

Alternatively, select *Add New Server* and create a new authentication method as per the steps described earlier in this section.

9. (Optional) Where a secondary method is required for Multi-Factor Authentication, repeat the previous step for **Secondary Auth Server**.

---

**Note:** Secondary authentication methods do not apply to *Enrollment User* type policies. The relevant field is hidden in this case.

---

10. Click **Add** to create the new policy.

The new policy is added to the list of authentication policies.

If you instead elect to update an existing custom or built-in policy:

1. Click the three dots adjacent to the relevant policy and click **Edit**.

The **Edit authentication policy** form appears.

---

**Note:** For built-in authentication policies, all properties except **Primary Auth Server** and **Secondary Auth Server** (where applicable) are read-only.

---

2. Set the **Primary Auth Server** to be the new SAML user authentication method (indicated):

The screenshot shows the 'Edit Authentication Policy' configuration page. The 'Policy Server Details' section is highlighted with a red border. It contains two dropdown menus: 'PRIMARY AUTH SERVER' with 'User Auth' selected, and 'SECONDARY AUTH SERVER' with 'Select Secondary Authentication Server' selected. Other fields include 'POLICY NAME' (User Signin), 'USER TYPE' (Users), 'LOGIN URL' (\*login/), and 'ENROLLMENT POLICY' (Enrollment Signin). At the bottom right, there are 'Cancel' and 'Save' buttons.

FIGURE 2.19 : Editing the primary auth server

**Note:** SAML authentication can be used only as a Primary Auth Server. If you are using MFA, specify either a *local authentication* or *TOTP* method as the **Secondary Auth Server**.

**Note:** If you configure a secondary authentication method in a policy that is currently in use, any active user sessions must be disconnected and reconnected for the changes to take effect.

3. Select **Save**.

The list of authentication policies updates.

4. Repeat until all required authentication policies are updated.

At this point, the Controller uses the uploaded Federation Metadata to contact the SAML service. After this process completes, a **Download** function becomes available for each relevant policy. This metadata file is required to configure trusted communication with the remote SAML service:

1. Refresh your browser until the **Download** action is visible for the relevant policies.
2. Select the check box for the policy metadata you want to download and clear all other check boxes.
3. Click **Download** and save the metadata file.

**Note:** As mentioned previously, make sure you repeat this procedure for each required SAML app on your Azure AD platform. That is, you require separate XML

metadata files for the enrollment authentication policy and the login authentication policy.

---

After you have configured a user authentication policy, you can configure the Azure AD platform with the SAML SP Metadata configuration of the Controller. You can also optionally configure the use of Multi-Factor Authentication with Azure AD. For details, see the *Tenant Admin Guide*.

## **Workflow: Creating a SAML Authentication Policy with On-Prem ICS**

Use this workflow to configure the Controller to act as a SAML Service Provider (SP) and engage Ivanti Connect Secure (ICS) as a remote (or local) on-prem SAML Identity Provider (IdP).

Configuring nZTA to use SAML authentication requires you to create separate SAML apps on the on-premises ICS server for the following primary activities:

- User enrollment
- User sign-in

The Controller includes built-in default authentication policies for each of these purposes, and also includes the ability to create your own custom policies for separate authentication of specific user groups. You create an authentication method referencing one of the Azure AD SAML apps described above and then assign the method to an authentication policy of the same type (either the built-in policy, or one you create). Begin with enrollment, and then repeat the process for user sign-in.

Before you begin configuring the Controller, make sure you have configured your ICS instance to perform the function of a SAML IdP and obtained the IdP Metadata file necessary for uploading to nZTA. For full instructions, see the ICS documentation held at <https://www.ivanti.com/support/product-documentation>. A summary of the steps is also contained in the “Ivanti Neurons for Secure Access: Tenant Admin Guide”.

After you have obtained the IdP metadata files from ICS, configure nZTA to use SAML authentication by performing the following steps:

---

**Note:** You must complete these steps for each SAML app on your ICS server. That is, for both enrollment and sign-in.

---

1. Log into the Tenant Admin Portal as an administrator.
2. From the nZTA menu, click the **Secure Access** icon, then select **Manage Users > Authentication Servers**.

The *Authentication Servers* page appears. This page lists all existing user authentication methods. nZTA includes two default authentication methods, one for admins and one for users.

Manage Users

User Groups User Rules User Policies Authentication Servers [Create Authentication Server](#)

**Note**  
Authentication Servers which **default** OR linked to any **User Policy**, will be disabled from selection.  
Local Authentication Servers which have one or more users linked to them will be disabled from selection.

30 TOTAL  [Batch Delete](#)

<input type="checkbox"/>	STATUS	NAME ↑	DEFAULT ↑	AUTHENTICATION METHOD ↑	USERS
<input type="checkbox"/>	>	account-auth		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	account-enrollment		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	Aditi		Local	1 Users
<input checked="" type="checkbox"/>	>	Admin Auth	☑	Local	93 Users
<input type="checkbox"/>	>	auth-enroll-manual		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	authsaml-man		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	azure-auth-manual		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	AzureAD-Auth		SAML (Azure AD)	N/A
<input type="checkbox"/>	>	AzureAD-Enroll		SAML (Azure AD)	N/A

FIGURE 2.20 : Authentication Servers

### 3. Click **Create Authentication Server**.

A form appears that enables you to define the authentication method.

[Create Authentication Server](#)

**Create Authentication Server**  
An authentication method is referenced from one or more authentication policies. nSA supports user authentication through the following user authentication methods: Local, SAML (Azure AD) and SAML (Custom). [Reset Fields](#)

Choose Server Name and Authentication Type

Authentication Server Name\*  Authentication Type: Local

**LIST OF LOCAL USERS**  
0 USER(S) FOUND [CREATE USER](#) [Batch Delete](#)

<input type="checkbox"/>	USERNAME	FULL NAME	CHANGE PASSWORD	EMAIL

[Cancel](#) [Create Authentication Server](#)

FIGURE 2.21 : User Authentication Method Wizard

**Note:** At any point during this process, you can reset the form data by clicking **Reset Fields**.

### 4. Under **Choose name and type**:

- Specify an **Authentication Server Name**. For example: *Enrollment* or *SignIn*.
- Select the **Authorization Type** of *SAML (Custom)*.

The form expands to show additional settings:

The screenshot shows the 'User Authentication' configuration page. At the top, there is a header 'User Authentication' with an information icon. Below it is a section titled 'Add Authentication Method' with 'View Auth Methods' and 'Reset' links. The main configuration area is titled 'Choose name and type' and contains two input fields: 'AUTHENTICATION SERVER NAME' with the value 'samlauthtest' and 'AUTHENTICATION TYPE' with the value 'SAML (Custom)'. Below this is a section titled 'Fields required for SAML Authentication Server' with a checkbox for 'Allow Unsigned Metadata'. There is a text input field for 'Single Logout URL'. Below that are radio buttons for 'Upload' (selected) and 'Enter Manually'. At the bottom, there is a 'LOCATION' dropdown menu set to 'File' and a 'FILE' input field with the text 'Upload a file here' and a file upload icon. At the bottom right, there are 'Cancel' and 'Add' buttons.

FIGURE 2.22 : Configuring SAML (Custom) authentication settings

5. (Optional) Specify a **Single Logout URL**. For more information, see the *Tenant Admin Guide*.
6. To provide your SAML IdP settings, select one of the following:
  - Select **Upload** to upload a digitally-signed (or unsigned) federation metadata XML definition file downloaded for this SAML activity from your IdP. That is, for either user enrollment or user sign-in.

---

**Note:** By default, the Controller expects a signed metadata definition file. To allow an unsigned metadata file, select **Allow Unsigned Metadata**.

---

Then, upload your metadata file by clicking **Upload a file here**.

- Select **Enter Manually** to manually enter the required IdP SAML settings. Use this option in scenarios where a SAML federation metadata file is not available or incomplete.

Then, enter the following details:

**Fields required for SAML Authentication Server**

Upload  Enter Manually






IDP Entity Id	
IDP SSO URL	
IDP Slo Service	
<small>USER NAME TEMPLATE</small> <assertionNameDN.uid>	
IDP Signing Certificate	

FIGURE 2.23 : Configuring SAML (Azure AD) IdP settings manually

- **IDP Entity ID:** The entity ID is sent as the Issuer value in the SAML assertion generated by the IdP. Specify the Issuer value in assertions generated by the SAML identity provider.
- **IDP SSO URL:** A URL provisioned by the SAML IdP to support service-provider-initiated Single Sign-On. Use the format `https://<FQDN>`.
- **IDP Slo Service:** (Optional) A URL to specify the Single Log-Out/sign out endpoint if you want to force re-authentication for increased security. Use the format `https://<FQDN>`. For more information, see the *Tenant Admin Guide*.
- **User Name Template:** Specify how the system is to derive the username from the SAML assertion. The default value can be used, or replaced with an alternative specifier that the Controller uses from the incoming assertion. For example: `<assertionNameDN.uid>`, the NameID value where ICS is the IdP, the UID from X509SubjectName, `<userAttr.attr>`, attr from AttributeStatement attributes.
- **IDP Signing Certificate:** The signing certificate to be used with the SAML app on the IdP. Type or paste in the contents of your Base-64 encoded public key.

---

**Note:** If, at a later date, you need to replace the metadata definition file with a modified version, edit the authentication method through the *User Authentication* page and repeat this step. Either edit the existing metadata file and re-upload, or replace it completely with a new version. In both cases, however, make sure your metadata file is valid before uploading it through this process.

---

7. Confirm that your settings are correct, then select **Add** to create the authentication method.

The new SAML user authentication method is added to the list of methods displayed in the **User Authentication** page, and the process completes.

After you have created your SAML authentication method, create or update your authentication policies with the new authentication method.

From the nZTA menu, click the **Secure Access** icon, then select **Manage Users > User Policies**.

The **User Policies** page appears. This page lists all existing user authentication policies.

**Manage Users** ⓘ

User Groups   User Rules   **User Policies**   Authentication Servers   [Create User Policy](#)

**Note**  
To create a User Policy, you need a prerequisite entity - [Authentication Servers](#).  
User Policies which are **default** OR linked to any **User Group** will be disabled from selection.

14 TOTAL      [Batch Delete](#)

<input type="checkbox"/>	STATUS	NAME ↑	DEFAULT ↑	POLICY USER	ACCESS URL	SERVER	SERVER TYPE	DEVICE POLICY
<input type="checkbox"/>	>	accounts-auth		user	*/login/accounts/	account-e...	SAML (Azu...	⋮
<input type="checkbox"/>	>	accounts-enrollment		enroll	*/login/accountsenro...	account-e...	SAML (Azu...	⋮
<input type="checkbox"/>		Admin Signin	☑	admin	*/login/admin/	Admin Auth	Local	⋮
<input type="checkbox"/>		cxo		admin	*/login/cxo/	cxo	Local	⋮
<input type="checkbox"/>		cxoics		admin	*/login/cxoics/	cxoics	Local	⋮
<input type="checkbox"/>	>	Enrollment Signin	☑	enroll	*/login/enroll/	AzureAD-E...	SAML (Azu...	⋮
<input type="checkbox"/>	>	kan_mfa		admin	*/login/QA/	kan-samla...	SAML (Azu...	⋮
<input type="checkbox"/>		netadmin		admin	*/login/netadmin/	net-admin	Local	⋮

FIGURE 2.24 : User Authentication Policies

To learn more about the policies on this page, see the *Tenant Admin Guide*.

From this page, either create a new custom policy or edit an existing policy. To add a new custom policy:

1. Click **Create User Policy**.

The **Create Authentication Policy** form appears.

The screenshot shows a web form titled "Create User Policies" with a sub-header "Create Authentication Policy". The form contains the following elements:

- POLICY NAME:** A text input field with the placeholder "Enter a name".
- LOGIN URL:** A text input field with the placeholder "\*/login/your-path".
- DESCRIPTION:** A text area with the placeholder "Add a description of the Authentication Policy".
- USER TYPE:** A dropdown menu currently showing "Enrollment Users".
- DEVICE POLICY:** A dropdown menu with the placeholder "Select a Device Policy".
- Auth Servers:** A section with a "Note" stating: "Only Local and SAML servers will be available for selection as a Primary Auth Server. A server which is selected as secondary(if applicable) would not be available for selection as primary." Below this is a dropdown menu labeled "PRIMARY AUTH SERVER (REQUIRED)" with the placeholder "Select from Local and SAML Auth Servers".
- Buttons:** "Cancel" and "Create User Policy" (dashed border) buttons at the bottom right.

FIGURE 2.25 : Add User Authentication

---

**Note:** At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing authentication policies in a pop-up dialog by clicking **View Auth Policies**.

---

**Note:** To learn more about how custom policies are used for user login and enrollment, see the *Tenant Admin Guide*.

---

2. Enter a **Policy Name**.
3. Enter a **Login URL** using the format `*/login/<path>/`.

The URL must start with `*/login/` and cannot contain any special characters. `<path>` should be set to a unique value reflecting the endpoint URL you want to define for this authentication policy (appended with a backslash):

- In the case of user sign-in policies, this is the URL endpoint (appended to the tenant FQDN) to which new users are invited to connect to enroll or sign-in a device with the Controller. Example value: `*/login/saleslogin/`.
- In the case of user enrollment policies, this endpoint identifies the enrollment URL to which users are redirected if they attempt to connect to the equivalent sign-in policy with an un-enrolled device. In most cases, you do not advertise this endpoint to your users. Example value: `*/login/salesenroll/`.

---

**Note:** In some enrollment circumstances, such as when using a device



pre-installed with an older version of Ivanti Secure Access Client, you connect directly to the enrollment policy endpoint to enroll the device. For more details, see the *Tenant Admin Guide*.

4. (Optional) Enter a description for the authentication policy.
5. Select a **User Type** based on the intended authentication activity for this policy. Choose from:
  - **Enrollment Users:** Select this option to define the authentication endpoint for enrollment of new end-user devices. This endpoint is reserved for enrollment and not normally provided directly to users.
  - **Users:** Select this option to define the user sign-in endpoint for enrolled devices. This is the endpoint that you provide to your users to access the service (regardless of enrollment status).
  - **Administrators:** Select this option to define the authentication endpoint for administrator-level sign-in. This endpoint is used for administrator login to the Controller only.
6. (for policies with a **User Type** of “Users” only): Select an **Enrollment Policy** from the drop-down list to be linked to this sign-in policy (as indicated):

The screenshot displays a configuration form for a policy. On the left, there are three fields: 'POLICY NAME' with the value 'sales-users-auth-policy', 'LOGIN URL' with the value '\*login/saleslogin/', and 'DESCRIPTION' with the text 'This is an example user sign-in policy for sales users'. On the right, a red box highlights the 'USER TYPE' dropdown menu, which is set to 'Users'. Below it, the 'ENROLLMENT POLICY' dropdown menu is open, showing a list of options: 'Select Enrollment Policy', 'Enrollment Signin', and 'Sales-enrollment'. The 'Sales-enrollment' option is highlighted in blue.

FIGURE 2.26 : Linking an enrollment policy to a user sign-in policy

This is the enrollment policy to which a user is redirected if it is determined that the device is not yet enrolled.

7. Under **Policy Server Details**, click **Primary Auth Server** and choose the required authentication method for the policy from the drop-down list:

The screenshot shows the 'Policy Server Details' section of a web interface. It features two dropdown menus: 'PRIMARY AUTH SERVER' and 'SECONDARY AUTH SERVER'. The 'PRIMARY AUTH SERVER' dropdown is open, displaying a list of authentication methods: 'account-auth', 'account-enrollment', 'Admin Auth', 'auth-enroll-manual', 'authsaml-man', 'azure-auth-manual', 'AzureAD-Auth', and 'AzureAD-Enroll'. At the top of this list is a '+ Add new server' link. To the right of the dropdowns are 'Cancel' and 'Add' buttons. The 'Add' button is currently disabled (greyed out).

FIGURE 2.27 : Selecting a primary authentication method for this policy

Alternatively, select *Add New Server* and create a new authentication method as per the steps described earlier in this section.

8. (Optional) Where a secondary method is required for Multi-Factor Authentication, repeat the previous step for **Secondary Auth Server**.

---

**Note:** Secondary authentication methods do not apply to *Enrollment User* type policies. The relevant field is hidden in this case.

---

9. Click **Add** to create the new policy.

The new policy is added to the list of authentication policies.

If you instead elect to update an existing custom or built-in policy:

1. Click the three dots adjacent to the relevant policy and click **Edit**.

The **Edit authentication policy** form appears.

---

**Note:** For built-in authentication policies, all properties except **Primary Auth Server** and **Secondary Auth Server** (where applicable) are read-only.

---

2. Set the **Primary Auth Server** to be the new SAML user authentication method (indicated):

**User Policies** ⓘ

**Edit Authentication Policy** View Auth Policies Reset

**Policy Details**

POLICY NAME: User Signin ⓘ USER TYPE: Users

LOGIN URL: /login/ ⓘ ENROLLMENT POLICY: Enrollment Signin ⚠

DESCRIPTION: User Auth

**Policy Server Details**

PRIMARY AUTH SERVER: User Auth

SECONDARY AUTH SERVER: Select Secondary Authentication Server

Cancel Save

FIGURE 2.28 : Editing the primary auth server

**Note:** SAML authentication can be used only as a Primary Auth Server. If you are using MFA, specify either a *local authentication* or *TOTP* method as the **Secondary Auth Server**.

**Note:** If you configure a secondary authentication method in a policy that is currently in use, any active user sessions must be disconnected and reconnected for the changes to take effect.

### 3. Click **Save**.

The list of authentication policies updates.

At this point, the Controller uses the uploaded metadata to contact the SAML service. After this process completes, a **Download** function becomes available for the policy. This metadata file is required to configure trusted communication with the remote SAML service. Perform the following steps:

1. Refresh your browser until the **Download** action is visible for the relevant policy.
2. Select the check box for the policy and clear all other check boxes.
3. Click **Download** and save the metadata file.

**Note:** Repeat these steps for each required SAML app on your On-Prem ICS server. That is, you require separate XML metadata files for the enrollment authentication policy and the login authentication policy.

After you have configured authentication policies, you can configure your ICS SAML app with the SP Metadata configuration of the Controller. You can optionally also

configure the use of Multi-Factor Authentication with ICS. For more information, see the *Tenant Admin Guide*.

## Workflow: Adding TOTP to an Authentication Policy

---

**Note:** This feature is supported for client and gateway versions applicable to release 22.2R1 and later only.

---

nZTA supports the use of Time-based One Time Password (TOTP) as a secondary authentication method in *Multi-Factor Authentication* deployments.

To use TOTP, first create a TOTP authentication method in nZTA and then associate it with your user sign-in authentication policies.

To ensure that your users can access the authentication mechanism defined in the policies you configure through this process, make sure your *Secure Access Policies* are configured with a **User Group** in which these authentication policies are defined. To learn more, see [Creating a Secure Access Policy](#) (page 129).

To configure a new TOTP authentication method:

1. Log into the Controller as a Tenant Admin.
2. From the nZTA menu, select the **Secure Access** icon, then select **Manage Users > Authentication Servers**.

The **Authentication Servers** page appears. This page lists all existing user authentication methods. For example:

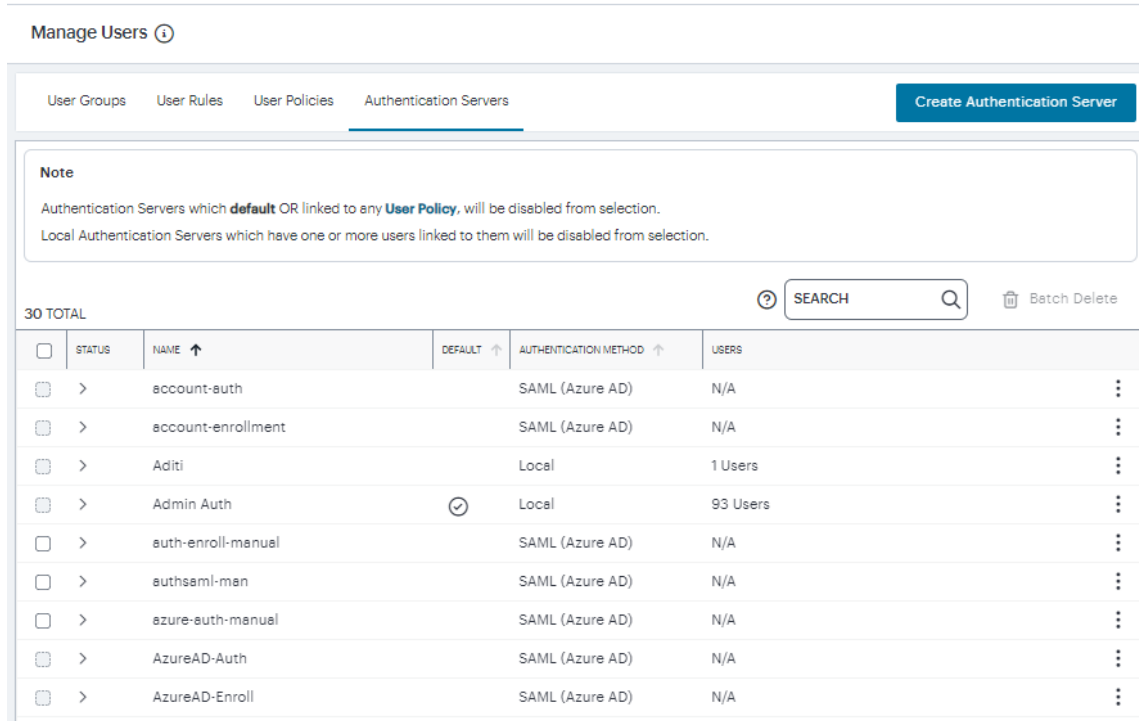


FIGURE 2.29 : Authentication Servers

3. Select **Create Authentication Server**.

A form appears that enables you to define the authentication method.

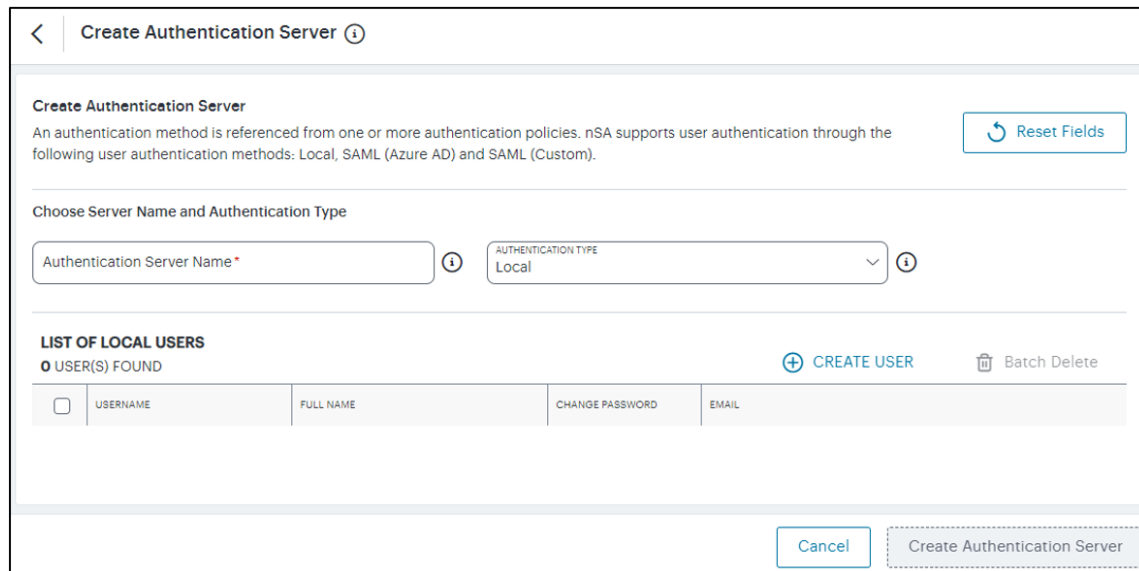


FIGURE 2.30 : Adding a new TOTP user authentication method

**Note:** At any point during this process, you can reset the form data by selecting **Reset**. You can also view existing authentication methods in a pop-up dialog by selecting **View Auth Methods**.

#### 4. Under **Choose name and type:**

- Specify an **Authentication Server Name**.
- Select the **Authorization Type** of *TOTP*.

The form expands to show additional TOTP authentication settings:

The screenshot shows the 'User Authentication' configuration interface. The main section is titled 'Add Authentication Method'. It includes the following fields and options:

- Choose name and type:**
  - Authentication Server Name: `totpauth` (with a checkmark icon)
  - Authentication Type: `TOTP` (with a checkmark icon)
- Number of Attempts:**
  - Max number of consecutive wrong attempts allowed after which account will be locked: `3` (with a dropdown arrow)
- Custom message for registration page:**
  - You will need to install two factor authentication application(Google Authenticator) on your smart phone or tablet
  - Custom Message for Registration Page: `TOTP auth for user signin` (with a checkmark icon)
- Allow Auto Unlock:**
  - Allow Auto Unlock
  - Locked account will be automatically unlocked after specified period (min: 10 minutes to max:90 days)
  - Auto Unlock Period: `10` (with a checkmark icon)
  - Minutes: `Minute(s)` (with a dropdown arrow)
- Display QR code during User Registration:**
  - Display QR code during User Registration
- Disable Generation of Backup Codes:**
  - Disable Generation of Backup Codes

At the bottom right, there are 'Cancel' and 'Add' buttons.

FIGURE 2.31 : Adding TOTP authentication settings

#### 5. Enter the following settings:

---

**Note:** This release supports a **Server Type** of *local* only. This field is read-only.

---

- **No of Attempts:** The maximum number of consecutive wrong attempts allowed before which the account is locked (minimum: 1 attempt, maximum: 5 attempts). To view user attempts and to unlock locked accounts, see [Unlocking Locked User Accounts](#) (page 37).
- **Custom message for registration page:** A custom message to be shown on the new TOTP-user registration web page.
- **Allow Auto Unlock:** When selected, a locked account is automatically unlocked after the specified **Auto Unlock Period**. (minimum: 10 minutes, maximum: 90 days).

- **Display QR code during User Registration:** When selected, a QR code is displayed during user registration.
- **Disable Generation of Backup Codes:** When selected, the Controller does not generate TOTP backup codes.

6. To create an authentication method based on these settings, select **Add**.

The new TOTP user authentication method is added to the list of methods and the process is complete.

After you have created your TOTP authentication method, create or update your user sign-in authentication policies with the new method. nZTA supports using TOTP *only as secondary authentication*, so make sure you have previously configured a primary authentication method before continuing this process.

---

**Note:** Secondary authentication methods do not apply to *Enrollment User* type policies. The relevant field is hidden in this case.

---

Complete the following steps for your user sign-in authentication policy:

1. From the nZTA menu, select the **Secure Access** icon, then select **Manage Users > User Policies**.

The **User Policies** page appears. This page lists all existing user authentication policies.

Manage Users ⓘ									
User Groups		User Rules		User Policies			Authentication Servers		Create User Policy
<p><b>Note</b></p> <p>To create a User Policy, you need a prerequisite entity - <b>Authentication Servers</b>. User Policies which are <b>default</b> OR linked to any <b>User Group</b> will be disabled from selection.</p>									
14 TOTAL <span style="float: right;">SEARCH <input type="text"/></span> <span style="float: right;">Batch Delete</span>									
<input type="checkbox"/>	STATUS	NAME ↑	DEFAULT ↑	POLICY USER	ACCESS URL	SERVER	SERVER TYPE	DEVICE POLICY	
<input type="checkbox"/>	>	accounts-auth		user	*/login/accounts/	account-a...	SAML (Azu...	⋮	
<input type="checkbox"/>	>	accounts-enrollment		enroll	*/login/accountsenro...	account-e...	SAML (Azu...	⋮	
<input type="checkbox"/>		Admin Signin	☑	admin	*/login/admin/	Admin Auth	Local	⋮	
<input type="checkbox"/>		cxo		admin	*/login/cxo/	cxo	Local	⋮	
<input type="checkbox"/>		cxoics		admin	*/login/cxoics/	cxoics	Local	⋮	
<input type="checkbox"/>	>	Enrollment Signin	☑	enroll	*/login/enroll/	AzureAD-E...	SAML (Azu...	⋮	
<input type="checkbox"/>	>	kan_mfa		admin	*/login/QA/	kan-samls...	SAML (Azu...	⋮	
<input type="checkbox"/>		netadmin		admin	*/login/netadmin/	net-admin	Local	⋮	

FIGURE 2.32 : User Authentication Policies

To learn more about the policies on this page, see the *Tenant Admin Guide*.

2. Click the three dots adjacent to your desired user sign-in policy, then select **Edit**.

The **Edit Authentication Policy** form appears.

The screenshot shows the 'Edit Authentication Policy' form. The 'Policy Details' section includes fields for 'POLICY NAME' (User Signin), 'LOGIN URL' (\* /login/), 'DESCRIPTION' (User Auth), 'USER TYPE' (Users), and 'ENROLLMENT POLICY' (Enrollment Signin). The 'Policy Server Details' section includes 'PRIMARY AUTH SERVER' (AzureAD-Auth) and 'SECONDARY AUTH SERVER'. The 'SECONDARY AUTH SERVER' dropdown is open, showing a list of authentication methods: Aditi, cxo, cxoics, cxonew, net-admin, networkics, readonlyadmin, totpauth (highlighted with a red box), and User Auth. A 'Save' button is located to the right of the dropdown.

FIGURE 2.33 : Selecting a secondary TOTP authentication method for this policy

3. For **Secondary Auth Server**, select your new TOTP authentication method from the drop-down list (as indicated).

Alternatively, select *Add New Server* and create a new authentication method as per the steps described earlier in this section.

4. Select **Save** to update the policy.

**Note:** If you configure a secondary authentication method in a policy that is currently in use, any active user sessions must be disconnected and reconnected for the changes to take effect.



## Unlocking Locked User Accounts

After you have created a TOTP authentication method and assigned it to an active user authentication policy, you can use the authentication method configuration page to view users that have attempted authentication through TOTP. This information enables you to unlock locked user accounts, if required.

To access user attempt information, perform the following steps:

1. Select **Secure Access > Manage Users > Authentication Servers**.
2. Click the three dots adjacent to your TOTP authentication method, then select **Edit**.

At the bottom of the page, a Users table is presented:

USERS				
1 USER(S)				
SEARCH <input type="text"/>		UNLOCK		RESET
<input type="checkbox"/>	USER NAME ↑	LAST ATTEMPTED ↑	LAST SUCCESSFUL LOGIN ↑	STATUS ↑
<input type="checkbox"/>	user1	Thu, 23 Jun 2022 03:35:37 AM GMT	Thu, 23 Jun 2022 03:35:37 AM GMT	Active

FIGURE 2.34 : Viewing the list of users who attempted TOTP authentication through this method

This table lists each user who has attempted to authenticate a device through TOTP, including the last attempt and last successful login times.

3. (Optional) If a user account is locked through too many consecutive failed authentication attempts (that exceed the value configured in **No of Attempts**), unlock the account by selecting the checkbox adjacent to the user entry and selecting **UNLOCK**. The user is then free to re-attempt authentication using valid authentication codes.
4. (Optional) To remove a user from the list, select the checkbox adjacent to the user entry and select **RESET**. This means a user must then re-register their device with the TOTP policy.

---

**Note:** Reset and unlock operations of individual users are supported only when the TOTP authentication method is associated with a user authentication policy. To reset or unlock all users in a disassociated TOTP authentication method, delete the TOTP authentication method itself.

---

## Creating User Rules and User Groups

After your authentication policies and methods are established, you can set up any required **user rules**.

Each user rule identifies one or more users, either from a local authentication service or from an external SAML service.

You associate one or more user rules with an **authentication policy** to form a **user group**.

### Creating User Rules

nSA includes three default user rules:

- **ALLADMINUSERS**. This matches all users, and is referenced by the default **ADMINISTRATORS** user group, which associates it with the built-in *Admin Signin* authentication policy.
- **ALLENROLLMENTUSERS**. This matches all users, and is referenced by the default **ENROLLMENT** user group, which associates it with the built-in *Enrollment Signin* authentication policy.
- **ALLUSERS**. This matches all users, and is referenced by the default **USERS** user group, which associates it with the built-in *User Signin* authentication policy.

---

**Note:** To read more about default user groups or built-in authentication policies, see the *Tenant Admin Guide*.

---

This preset configuration of rules, groups, and policies is suitable for typical use cases involving whole-organization authorization needs. In other words, where you require only a single user authorization path that matches all users. For scenarios where you require more specific user authorization checks, you can create additional rules to match specific types of users.

When you create a rule, you select the user attribute with which you want this rule to test. nSA provides the following rule attribute types:

- **username**: For local authentication methods, choose this attribute type to match against locally-defined user names.
- **SAML (Azure AD)**: For SAML authentication methods, choose this attribute type to match against user names or groups provided by the SAML service.
- **Custom**: For SAML authentication methods, choose this attribute type to match against a custom SAML attribute expression.

To create a user rule:

1. From the nZTA menu, select the **Secure Access** icon, then select **Manage Users > User Rules**.

The *User Rules* page appears. This page lists all user rules.

2. Click **Create User Rule**.

The *Create User Rule* form appears.

FIGURE 2.35 : Create User Rule

---

**Note:** At any point during this process, you can reset the form data by clicking **Reset Fields**.

---

3. Enter a **Rule Name**.

4. Click **Select Attribute Type** and select one of the available options:

- **Username:** Matches user names in a local authentication method. When you select this option, you must then:
  - Select an **Expression** type, either *Matching* or *Not Matching*.
  - For the **User** value, enter a match expression for the selected **Expression** type. For the value:
    - \* A comma-separated list of items is supported where required.
    - \* Wildcard matches are supported.
    - \* Special characters are supported.
    - \* Single and double quotes are not supported.

---

**Note:** Ivanti recommends that a basic asterisk wildcard is not used when you intend to associate admin roles with user groups. Instead, a more-specific wildcard that only includes admin users is required in this case to prevent all users having total access rights.

---

- **SAML (Azure AD):** Matches user names or groups in a SAML authentication method. When you select this option, you must then:

- Select a **SAML Attribute Type**, either *Username* or *Group*.
- For **Attribute Value**, enter a match expression for the selected **SAML Attribute Type** as a SAML expression.
- *Custom*. Matches against a custom SAML attribute expression. When you select this option, use the **Type or Create an Expression** property to enter an attribute expression. Supported formats include:

- For simple user attribute key-value matching, use the syntax `userAttr.<attr-key> [=|!=] <attr-value>`. For example:

```
- userAttr.memberOf = "CN=sales,DC=example,DC=com"
- userAttr.mail = "user1@example.com"
- userAttr.realm = "Users"
- userAttr.department != "example_department"
```

- To match against attributes that can have multiple values associated with a single attribute key, use the syntax `samlMultiValAttr.<attr-key> [=|!=] (<list>)`. For example:

```
- samlMultiValAttr.memberOf = ("CN=Employee,CN=Users,
↪DC=example_demo,DC=com")
- samlMultiValAttr.memberOf = ("CN=Users,DC=example_demo,
↪DC=com")
```

- Use brackets and AND/OR operators to construct logical compound expressions:

```
- userAttr.groups = ("Group1" or "Group2")
- userAttr.realm = ("ztaqa") and samlMultiValAttr.memberOf
↪= ("CN=sales,DC=uisdp,DC=com")
- userAttr.realm = ("ztaqa") or samlMultiValAttr.memberOf
↪= ("CN=sales,DC=uisdp,DC=com")
- userAttr.realm != ("ztaqa") and samlMultiValAttr.
↪memberOf = ("CN=sales,DC=uisdp,DC=com")
```

5. Click **Create User Rule**.

The new user rule is added to the list of user rules.

6. Repeat steps 3-6 for each required user rule.

After you have created all required user rules, you can create user groups, see [Creating User Groups](#) (page 41).

## Creating User Groups

After you have created user rules (see [Creating User Rules](#) (page 38)), you associate one or more user rules with an authentication policy to form a user group.

nSA includes three default user groups:

- **ADMINISTRATORS.** This user group associates the default *ALLADMINUSERS* user rule with the built-in *Admin Signin* authentication policy.
- **ENROLLMENT.** This user group associates the default *ALLENROLLMENTUSERS* user rule with the built-in *Enrollment Signin* authentication policy.
- **USERS.** This user group associates the default *ALLUSERS* user rule with the built-in *User Signin* authentication policy.

---

**Note:** To read more about built-in authentication policies, see the *Tenant Admin Guide*.

---

This preset configuration of rules, groups, and policies is suitable for typical use cases involving whole-organization authorization needs. In other words, where you require only a single user authorization path that matches all users. For scenarios where you require more specific user authorization checks, you can create additional user groups to make different associations of user rules and custom authentication policies.

To create a user group:

1. From the nZTA menu, click the **Secure Access** icon, then select **Manage Users > User Groups**.

The *User Groups* page appears. This page lists all user rule groups.

2. Click **Create User Group**.

A form appears to enable you to create the user group.

FIGURE 2.36 : Create User Groups

3. Enter a **User Group Name** and an optional **Description**, then click **Next**.
4. Select each of the listed **User Rules** that are required in the user group, then click **Next**.
5. Select required authentication policy from the list, then click **Next**.
6. Review the summary and click **Create**.

The new user group appears in the **User Groups** list.

7. Repeat steps 2-7 to create all required user groups.

## Next Steps

After you have configured your authentication methods and policies, and added them to your user groups, proceed to configure your nZTA Gateways, see [Configuring Gateways](#) (page 43).

# Configuring Gateways

- [Introduction](#) (page 43)
  - [Workflow: Creating a Gateway in VMware vSphere](#) (page 47)
  - [Workflow: Creating a Gateway in Amazon Web Services](#) (page 53)
  - [Workflow: Creating a Gateway in Microsoft Azure](#) (page 59)
  - [Workflow: Creating a Gateway in KVM/OpenStack](#) (page 72)
  - [Workflow: Creating a Gateway in Google Cloud Platform](#) (page 84)
  - [Next Steps](#) (page 100)
- 

## Introduction

---

**Note:** This guide describes how to configure a ZTA Gateway for your secure applications and resources. To learn more about configuring Ivanti Connect Secure (ICS) Gateways, refer instead to the *ICS Tenant Admin Guide* available from the nZTA documentation portal.

---

A **Gateway** is a virtual machine instance that you use to control access to your applications. You deploy Gateway instances at each location your applications reside - at a physical datacenter, a private or public cloud-based service, or some hybrid combination. Each Gateway communicates with the Controller to ensure that application access requests received from end-user devices are authenticated.

Before you deploy a Gateway instance, you register a new *Gateway record* in the Controller through the Tenant Admin portal. This record contains all basic identification, type, and network details required to enable secure communication between the Controller and the Gateway instance. The registration process produces a package of settings, known as a Gateway definition, that you publish to the Gateway virtual machine instance during deployment. These settings enable the Gateway to establish communication back to the Controller.

**Note:** Make sure the Gateway virtual machine instance does not exist prior to registration with the Controller. Each ZTA Gateway must be deployed from the Controller directly. The Gateway definition file is designed to be published to a new virtual machine Gateway instance during its initial deployment.

You deploy a Gateway virtual machine instance from a supplied template. Each Gateway template is pre-configured to define the required virtual machine settings and network interfaces for the target platform. During deployment, you specify the values for each defined interface according to the public and private subnets configured in your network infrastructure.

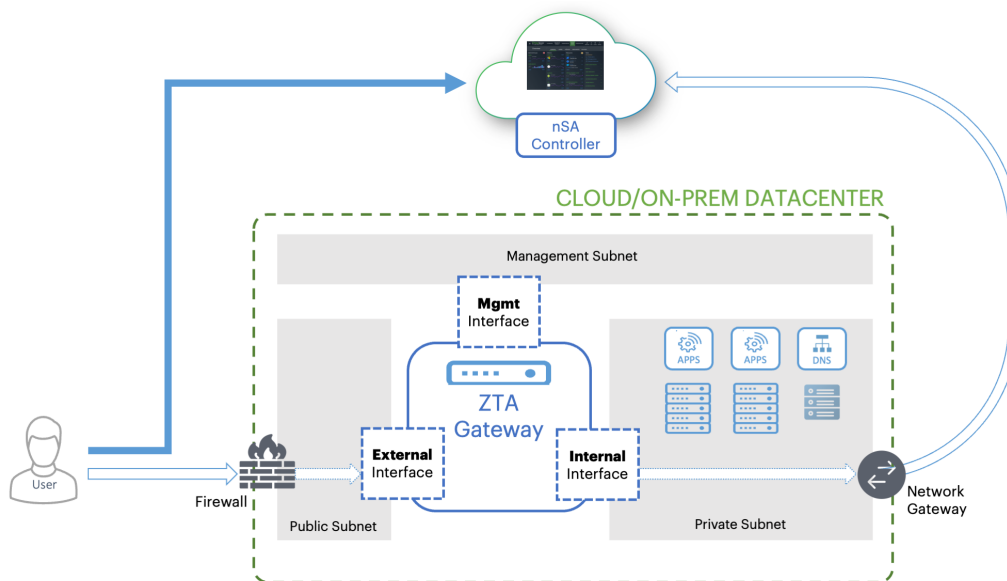


FIGURE 3.1 : Gateway network connections in your cloud and on-prem datacenter

Each ZTA Gateway virtual machine uses a number of network interfaces:

- **External network interface:** Configured with a public subnet IP address and used for external client access to the applications deployed in that datacenter. Use this IP address during the process of creating your Gateway record on the Controller.
- **Internal network interface:** Configured with a private subnet IP address and used for internal connections to the deployed applications, and for external communication with the Controller.
- (Optional) **Management network interface:** Configured with an IP address and port on a further, separate, network subnet for deployments where a specific management interface is required.

**Note:** When the management interface is enabled, the Gateway communicates with the Controller through this interface instead. In this scenario, the Gateway still uses the internal network interface for DNS resolution and NTP server communication. As such, the Gateway DNS server should resolve the Controller and



NTP server FQDNs through the internal interface (internet access is required).

---

To ensure communication between your Gateways, the Controller, and your client users, make sure the following network connections are enabled:

- Configure the firewall rules for the **Public Subnet** in which your ZTA Gateway **External Interface** resides is configured to accept inbound client connections on TCP port 443.
- Configure the **Network Gateway** serving your **Private Subnet** to allow outbound TCP traffic to the Controller on port 443.
- Configure the **Network Gateway** serving your **Private Subnet** to allow outbound UDP traffic to the following Network Time Protocol (NTP) services:
  - time.windows.com (port 123)
  - time.nist.gov (port 123)
- If you are planning to use your ZTA Gateway to serve SaaS (Software-as-a-Service) applications, configure the application to restrict inbound connections to your **network gateway** IP address. This ensures that your SaaS application can be reached only by clients connecting through the ZTA Gateway.
- If you maintain your own DNS service at the datacenter, use these details during Gateway record creation on the Controller.

### White-listing Required IP Addresses for your Services

The Controller service uses a series of IP addresses and ports to facilitate access to the admin and user web consoles, for user enrollment, and for connections to a ZTA Gateway. To ensure network access, make sure the following IP addresses and ports are white-listed (or added to the *allowed list*) in your network firewalls and routing infrastructure. Select the IP addresses and ports for your corresponding region only:

- **North America:**
  - 52.186.44.249 (port 443)
  - 52.188.33.186 (port 443)
- **Europe:**
  - 51.138.111.17 (port 443)
  - 20.50.150.82 (port 443)
- **APJ:**
  - 20.44.238.229 (port 443)
  - 20.44.237.67 (port 443)

## High Availability

nZTA allows you to deploy multiple Gateways at a single location to support high availability. This arrangement can be used to provide scaling, redundancy, and load distribution for your application delivery.

High availability is implemented in the Controller through **Gateway Groups**. You add individual Gateways to a group, and then associate the group with your Secure Access Policy.

To learn more about high availability and using Gateway Groups, see the *Tenant Admin Guide*.

## Configuring a Default Gateway

nZTA directs requests from each application towards the Gateway defined in the secure access policy for the application.

A default ZTA Gateway can be defined. This Gateway handles all requests from application that are not referenced by any secure access policy. This enables packet analysis to be conducted on requests passing through the Gateway to assess the validity of the requests. Two default Gateway scenarios are supported:

- Any single Gateway at v21.1 (or later) can be assigned to act as the default Gateway. This Gateway is exclusively used as the default Gateway.
- Alternatively, any Gateway Group whose Gateways are all at v21.1 (or later) can be assigned to act as the default Gateway. In this scenario, the Gateways are used exclusively as the default Gateway. The Gateway Group is typically fronted by a load balancer to enable the required distribution of requests across the Gateways in the group.

To configure a default ZTA Gateway, you must edit and update the built-in *Application discovery* secure access policy.

The default Gateway (or Gateway Group) then handles all requests from applications on enrolled devices that are not referenced by any other secure access policy.

To learn more about using a default Gateway, see the *Tenant Admin Guide*.

## Gateway Deployment Workflows

nZTA supports Gateway virtual machine instances deployed in the following environments:

- **VMware vSphere**: see [Workflow: Creating a Gateway in VMware vSphere](#) (page 47).
- **Amazon Web Services (AWS)**: see [Workflow: Creating a Gateway in Amazon Web Services](#) (page 53).
- **Microsoft Azure**: see [Workflow: Creating a Gateway in Microsoft Azure](#) (page 59).

- **KVM/OpenStack:** see [Workflow: Creating a Gateway in KVM/OpenStack](#) (page 72).
- **Google Cloud Platform:** see [Workflow: Creating a Gateway in Google Cloud Platform](#) (page 84).

## Workflow: Creating a Gateway in VMware vSphere

This workflow leads you through the process for setting up a Gateway in VMware vSphere. It contains two main procedures, in sequence:

- Creating the Gateway record in the Controller.
- Creating the Gateway virtual machine instance in VMware vSphere.

After these steps have been completed successfully, the Controller and Gateway establish communication with each other.

Before you start, make sure you have the following information and files for the Gateway:

- An identifying name for the Gateway
- The public IP address for the Gateway. This is the IP address at which clients can externally reach the Gateway instance.
- The Gateway geographic location
- (Optional) The name of the *Gateway Group* to which you want to add this new Gateway record. To learn more about Gateway Groups, see the *Tenant Admin Guide*.

Additionally, if you want to *manually specify* Gateway network interface settings:

- The internal/private subnet IP address, subnet mask, and network gateway IP address.
- The primary (and optional secondary) DNS server IP address, and search domain.
- The external interface IP address, subnet mask, and network gateway IP address
- (Optional) The management interface IP address, subnet mask, and network gateway IP address.
- The Gateway OVF template: <https://pulsezta.blob.core.windows.net/gateway/ISA-V-VMWARE-ZTA-22.3R4-883.1.zip>

---

**Note:** Download a copy of the OVF template archive file and unpack to a local workstation. Make sure the resulting file set is accessible from the vSphere Console.

---

---

**Note:** You can also choose to download this file from the **Gateways Overview** page of the Tenant Admin Portal. The opportunity to do this occurs later in this process.

---

- Credentials for the vSphere Console.

---

**Note:** These credentials must include sufficient permissions to create a virtual machine from a template image.

---

To set up a ZTA Gateway in VMware vSphere, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:
  - On unconfigured nZTA systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
  - On configured nZTA systems, the **Network Overview** page appears. In this case:
    - From the nZTA menu, click the **Secure Access** icon, then select **Gateways > Gateway List**.

The *Gateways List* page appears, showing the full list of Gateway Groups and standalone Gateways currently configured on the Controller.

    - To add a new Gateway, select **Create** from the top-right:

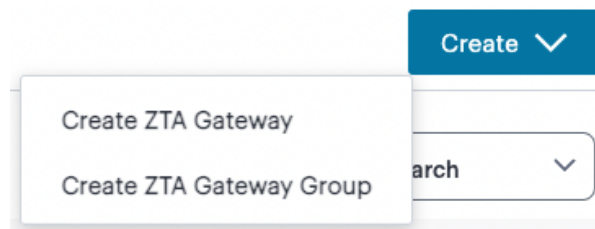


FIGURE 3.2 : Add a new Gateway or Gateway Group

- In the drop-down menu, click **create ZTA Gateway**.

In both cases, the **Gateway Network Configuration** dialog appears.

**Gateway Network Configuration**

View Gateways | Reset Fields

**Gateway Details**

GATEWAY PLATFORM: VMware vSphere  Use Manual Settings

**Gateway Information**

NAME:  PUBLIC ADDRESS or CNAME:

**Location**

COUNTRY:  STATE/REGION:  CITY:

**Add this Gateway to a group**  
Add gateway to any of the predefined gateway group or create a new gateway group

GATEWAY GROUP: Select a gateway group

**Gateway Network Settings**

Use Management Port  Use Dynamic Tunnel IP

FIGURE 3.3 : Gateway Network Configuration

**Note:** To learn more about the settings on this page, see the *Tenant Admin Guide*.

2. For **Gateway Platform**, select “VMware vSphere”.
3. (Optional) To enter your vSphere Gateway instance DNS and network interface settings manually, select **Use Manual Settings**. To instead allow nZTA to use DHCP-derived settings for DNS and network interfaces, leave **Use Manual Settings** un-selected.
4. Enter a **Name** for the Gateway.
5. Enter one or more **Public Address or CNAME** (Public IP address or CNAME) for the Gateway. Select **Add** to add each entry to the list.
6. Select a geographic **Location** for the Gateway.
7. (Optional) Select a Gateway **Group** to which the new Gateway is to be added.
8. (Optional) Select the **Use Management Port** check box to use management network ports for nZTA traffic rather than internal ports.


**Note:** When the management port is enabled, the Controller will still use the internal port for DNS resolution. If the internal DNS cannot resolve the Controller domain, the internal interface will require internet access.

9. (Optional) Select the **Use Dynamic Tunnel IP** check box to configure a pool of IP addresses that are dynamically mapped to client sessions with this Gateway, such that user traffic from the Gateway to an application can be identified as originating from a specific client.

The *Custom IP Pool* dialog appears:

Use Management Port     Use Dynamic Tunnel IP

Custom IP Pool



Example: x.x.x.x/netmask  
netmask would be in the range  
of 8-28

FIGURE 3.4 : Gateway Network Configuration - Custom IP Pool settings

---




**Note:** Dynamic Tunnel IP addresses are not supported in Gateway Groups.

---



Use the **Assignable Custom IPv4 Address** field to enter an IP address and subnet (in the range 8-28) in CIDR notation, then click **Add**. Repeat this step for each address/subnet you want to use.

10. If you elected to use manual settings, the following panel appears:




Internal IP

Internal Network / Private Subnet

External IP

Management IP

FIGURE 3.5 : Gateway Network Configuration - manual settings

Enter the following details:

- Specify the internal **IP Address** for the Gateway.
- Specify the internal **Subnet Mask** for the Gateway.
- Specify the internal network gateway IP address as the **Gateway** setting.
- Enter the **Primary DNS** IP address for the Gateway.
- (Optional) Enter the **Secondary DNS** IP address for the Gateway.
- Enter the **DNS Search Domain** for the Gateway.
- Specify the external **IP Address** for the Gateway.
- Specify the external **Subnet Mask** for the Gateway.
- Specify the external network gateway IP address as the **Gateway** setting.

---

**Note:** Management network settings are optional, unless the **Use Management Port** check box is selected.

---

- Specify the management **IP Address** for the Gateway.
- Specify the management **Subnet Mask** for the Gateway.
- Specify the management network gateway IP address as the **Gateway** setting.

11. To add a Gateway definition based on the settings you specified in this dialog, select **Create Configuration**.

After you complete this process, an unregistered Gateway record is created on the Controller. You can view this Gateway record on the **Gateways > Gateways List** page.

12. On the *Gateways List* page, select your vSphere Gateway and click the **Download** icon to obtain a copy of the Gateway definition file.



FIGURE 3.6 : The Download Icon

Retain this file for a later step.

---

**Note:** The Gateway definition file is valid for 24 hours. If this period expires, you must replace the Gateway to generate a new Gateway definition file.

---

13. (Optional) If you have not yet downloaded the latest version of your Gateway VM file, click the **Download** icon and select **Download gateway VM image**. Save the archive file and unpack to a local workstation. Make sure the resulting file set is accessible from the vSphere Console.
14. Access the *vSphere management interface*, either from a client or a web browser, and log in using your vSphere credentials.
15. In the vSphere console, start the *Deploy OVF Template* wizard to create a new virtual machine based on the nZTA vSphere Gateway template.
16. In the wizard:
  - Choose to deploy from a local file.
  - Locate and upload your ZTA Gateway OVF/VMDK template files.
  - Provide an identifying name and location for the new Gateway virtual machine.
  - Choose any required compute resource.

---

**Note:** For reference, the recommended minimum requirements for a Gateway virtual machine instance in vSphere are:

- 4 vCPU's and 8 GB memory, or
  - 8 vCPU's and 32 GB memory
- 

- Choose the required storage settings.
  - Customize the *vApp properties* of your virtual machine and, in the **VAIVE Configuration** parameter, paste the raw text of the Gateway definition file downloaded earlier.
  - Confirm all settings.
  - Finish the wizard to create the Gateway virtual machine.
17. Locate the new Gateway virtual machine in the hosts and clusters.
  18. Start the Gateway virtual machine by powering it on.  
Wait until the boot up process is complete.
  19. Return to the **Gateways List** page on the Controller.
  20. Locate the new Gateway record in the list and confirm that its **Connection Status** has updated to *Connected*.

---

**Note:** After you have registered a Gateway, you can configure it (or the Gateway Group to which it belongs) as the default Gateway if required. See the *Tenant Admin Guide* for details.

---



## Workflow: Creating a Gateway in Amazon Web Services

This workflow leads you through the process for setting up a Gateway in Amazon Web Services (AWS). It contains two main procedures, in sequence:

- Creating the Gateway record in the Controller.
- Creating the Gateway virtual machine instance in AWS.

After these steps have been completed successfully, the Controller and Gateway establish communication with each other.

Before you start, make sure you have the following information and files:

- An identifying name for the Gateway
- The public IP address for the Gateway. This is the IP address at which clients can externally reach the Gateway instance, typically an elastic IP address provided by AWS.
- The Gateway geographic location.
- (Optional) The name of the *Gateway Group* to which you want to add this new Gateway record. To learn more about Gateway Groups, see the *Tenant Admin Guide*.
- The primary (and optional secondary) DNS server IP address, and search domain.
- The Gateway template file. A ZTA Gateway can be deployed in a new VPC or an existing VPC, using **Nitro** hypervisor. Select the JSON template file that is applicable to your requirements:
  - To deploy in an existing VPC - Nitro hypervisor (M5-type instances):  
<https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-2-nics-existing-vpc.json>  
<https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-3-nics-existing-vpc.json>
  - To deploy in a new VPC - Nitro hypervisor (M5-type instances):  
<https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-2-nics-new-network.json>  
<https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-2-883/Nitro/ivanti-zta-3-nics-new-network.json>

---

**Note:** If you want to use a Management interface, you must download and use the 3 NIC template.

---

---

**Note:** You might not be able to specify the download location given here directly to AWS. In this case, download the Gateway template file first to your local workstation and specify this location instead.

---

---

**Note:** You can also choose to download this file from the **Gateways Overview** page of the Tenant Admin Portal. The opportunity to do this occurs later in this process.

---

- The Gateway AMI identifier. nZTA gateway AMIs are available in all AWS regions (except China). To obtain the AMI applicable to your region, follow these steps:
  1. Log into the AWS console.
  2. Navigate to **EC2 > Images > AMIs**.
  3. Select “Public Images”.
  4. Search for the image corresponding to your selected hypervisor:
    - Nitro: “ISA-V-NITRO-ZTA-22.3R4-883.1-SERIAL-nitro.img”
  5. Make a note of the corresponding AMI ID.
- Credentials for the AWS Management Console.

---

**Note:** These credentials must include sufficient permissions to create a stack.

---

- The SSH public key that you are using with the AWS Management Console.

To set up a ZTA Gateway in AWS, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:
  - On unconfigured nZTA systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
  - On configured nZTA systems, the **Network Overview** page appears. In this case:
    - From the nZTA menu, click the **Secure Access** icon, then select **Gateways > Gateway List**.

The *Gateways List* page appears, showing the full list of Gateway Groups and standalone Gateways currently configured on the Controller.

  - To add a new Gateway, select **Create** from the top-right:

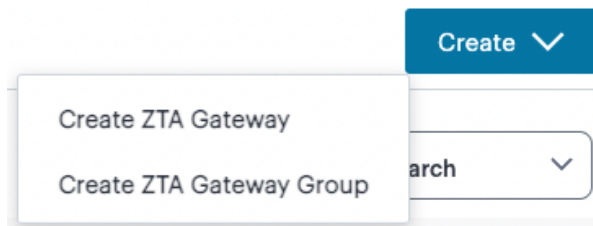


FIGURE 3.7 : Add a new Gateway or Gateway Group

- In the drop-down menu, click **Create ZTA Gateway**.

In both cases, the **Gateway Network Configuration** dialog appears.

The screenshot shows the 'Gateway Network Configuration' dialog box. At the top, it says 'Create ZTA Gateway' with a help icon. Below that, there are two tabs: 'View Gateways' and 'Reset fields'. The main content is organized into sections:

- Gateway Details:** A dropdown menu for 'GATEWAY PLATFORM' is set to 'Amazon Web Services'. There is a 'Use Manual Settings' checkbox.
- Gateway Information:** A 'NAME' field, a 'PUBLIC ADDRESS or CNAME' field, and an 'ADD' button.
- Location:** Three dropdown menus for 'COUNTRY', 'STATE/REGION', and 'CITY'.
- Add this Gateway to a group:** A dropdown menu for 'GATEWAY GROUP' is set to 'Select a gateway group'. There is a 'CREATE GATEWAY GROUP' button.
- Gateway Network Settings:** A 'Use Management Port' checkbox.
- Internal Network / Private Subnet:** Three input fields for 'PRIMARY DNS', 'SECONDARY DNS', and 'DNS SEARCH DOMAIN'.

At the bottom right, there are 'CANCEL' and 'Create Configuration' buttons.

FIGURE 3.8 : Gateway Network Configuration

**Note:** To learn more about the settings on this page, see the *Tenant Admin Guide*.

2. For **Gateway Platform**, select “Amazon Web Services”.
3. Enter a **Name** for the Gateway.
4. Enter one or more **Public Address or CNAME** (Public IP address or CNAME) for the Gateway. Select **Add** to add each entry to the list.
5. Select a geographic **Location** for the Gateway.
6. (Optional) Select a Gateway **Group** to which the new Gateway is to be added.
7. (Optional) Select the **Use Management Port** check box to use management network ports for nZTA traffic rather than internal ports.

**Note:** When the management port is enabled, the Controller will still use the internal port for DNS resolution. If the internal DNS cannot resolve the

Controller domain, the internal interface will require internet access.

---

8. Enter the Primary DNS IP address for the Gateway.
  9. (Optional) Enter the Secondary DNS IP address for the Gateway.
  10. Enter the DNS Search Domain for the Gateway.
- 

**Note:** Make sure the specified DNS service can resolve the IP address of your Controller. Issues here can cause registration of the Gateway with the Controller to fail.

---

11. To add a Gateway definition based on the settings you specified in this dialog, select **Create Configuration**.

After you complete this process, an unregistered Gateway record is created on the Controller. You can view this Gateway record on the **Gateways > Gateways List** page.

12. On the *Gateways List* page, select your new Gateway and click the **Download** icon to obtain a copy of the Gateway definition file.

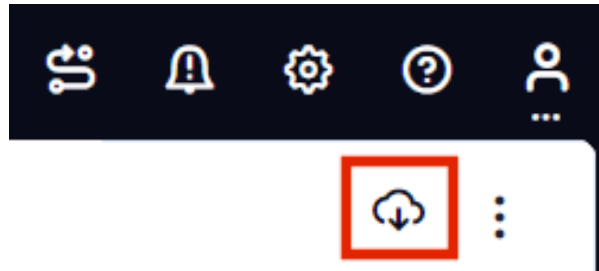


FIGURE 3.9 : The Download Icon

Retain this file for a later step.

---

**Note:** The Gateway definition file is valid for 24 hours. If this period expires, you must replace the Gateway to generate a new Gateway definition file.

---

13. (Optional) If you have not yet downloaded the latest version of your Gateway VM file, click the **Download** icon and select **Download gateway VM image**. Save the archive file and unpack to a local workstation. Make sure the resulting file set is accessible from the AWS Management Console.
14. Access the *AWS Management Console* and log in using your AWS credentials.
15. In the AWS **Services** menu, select **CloudFormation**.  
The **CloudFormation** home page appears.
16. Click **Create Stack** and then, from the sub-menu, select **With new resources (standard)**.

The **Specify template** step of the **Create Stack** wizard appears.

17. Under **Prerequisite - prepare template**, select the **Template is ready** option.
18. Under **Specify Template**, select the **Upload a template file** template source option.
19. Under **Upload a template file**, click **Choose File** and select the Gateway template file that you downloaded at the start of this process.

The file uploads, and the AWS S3 URL for the uploaded template file appears automatically.

20. Click **Next**.

The **Specify stack details** step of the **Create Stack** wizard appears. This page displays the details and parameters required by the Gateway template.

21. Enter a **Stack name**.
22. Specify the parameters as appropriate for your deployment:
  - If you are deploying the Gateway instance into a new VPC, you can accept the default values used for all parameters.
  - If you are deploying the instance into an existing VPC, you must manually specify the details of your existing VPC into the parameters on the page. For more information, contact Ivanti Technical Support.
23. Under **nZTA Configuration**, identify the required Gateway AMI using its **nZTA Gateway AMI ID**. Choose the designated AMI for the region in which you are deploying the Gateway instance.
24. For **Instance Type**, select the instance type that fits your hypervisor choice (Nitro) and minimum requirements, based on the following recommended types:

---

**Note:** For reference, the recommended minimum requirements for a Gateway virtual machine instance in AWS are:

For Nitro hypervisor-based instances, use M5 types:

- m5.large (2 vCPU, 8 GB Memory) (2NIC min)
  - m5.xlarge (4 vCPU, 16 GB Memory) (3NIC min)
  - m5.2xlarge (8 vCPU, 32 GB Memory)
  - m5.4xlarge (16 vCPU, 64 GB Memory)
- 

25. Under **nZTA Config Data**, paste in the raw text of the Gateway definition file downloaded earlier.
26. For **SSH Key Name**, specify your existing SSH key pair name.
27. For **Load Balancer Configuration**, If you plan to deploy multiple Gateways inside a Gateway Group, select "Yes" to deploy a new internet-facing network load balancer instance alongside the Gateway. Select "No" to launch only this Gateway instance.

---

**Note:** This option is applicable only for new VPC templates.

---

If you elect to launch a load balancer, the following pre-configuration is applied:

- An Elastic IP address is assigned to the load balancer.
- A TCP listener is configured on port 443.
- An IP-based Target Group is created and the private IP address of the deployed Gateway's external network interface is added as a target.
- A health-check is configured on TCP port 443.
- Stickiness is enabled on the Target Group.

After you have deployed the Gateway and Load Balancer, you must return to the Tenant Admin Portal on the Controller and update the Gateway Group **Load Balancer IP ADDRESS** setting to be the Load Balancer's public IP address.

If you want to configure the Load Balancer to balance across further Gateway instances from the Gateway Group, you must deploy each subsequent Gateway into an existing VPC and then update the Load Balancer Target Group.

---

**Note:** With new VPC templates, a NAT gateway is deployed for routing outbound Internet traffic from the Gateway's internal network interface in order for the Gateway to be able to reach the Controller.

---

---

**Note:** Public IP addresses are not automatically assigned to any of your Gateway's network interfaces. If you are deploying a Gateway into an existing VPC, in order for the Gateway to be able to reach the Controller from its internal network interface, make sure you allow outbound Internet traffic from the Private Subnet for the deployed Gateway.

---

To learn more about high availability and Gateway Groups, see the *Tenant Admin Guide*.

28. Click **Next**.

The **Configure stack options** step of the **Create Stack** wizard appears. All properties that were specified either in the template or in earlier steps are populated automatically.

No changes or new inputs are required.

29. Click **Next**.

30. The **Review** step of the **Create Stack** wizard appears.

31. Confirm all displayed details.

32. Click **Create stack**.

The **Stacks** page appears. The new stack is listed using the **Stack name** you specified during the wizard. The new stack has a status of `CREATE_IN_PROGRESS`.

33. Wait for the status of the new stack to reach `CREATE_COMPLETE`.
34. (This step is required only if you have not deployed your Gateway with a Load Balancer or NAT at the front-end) Elastic IP addresses are not automatically assigned to any of the Gateway's network interfaces. Therefore, before you can access the new Gateway instance from the Controller, you must associate a new Public IP address with the external interface of the Gateway. Then, return to the Tenant Admin Portal and update the *Gateway Public IP Address* setting to match this address.
35. In the Tenant Admin Portal **Secure Access > Gateways > Gateways List** page, locate the new Gateway record and confirm that its **Connection Status** has updated to *Connected*.

---

**Note:** You can directly access your AWS instance over SSH using *AWS EC2 Instance Connect*. To configure *AWS EC2 Instance Connect*, refer to the *Amazon Web Service Documentation*. You can then connect to the instance directly as a serial console using SSH from inside the *AWS Management Console*, refer to the *Amazon Web Service Documentation*.

---

---

**Note:** After you have registered a Gateway, you can configure it (or the Gateway Group to which it belongs) as the default Gateway if required. See the *Tenant Admin Guide* for details.

---

## Workflow: Creating a Gateway in Microsoft Azure

This workflow leads you through the process for creating and registering a ZTA Gateway in Microsoft Azure. It contains two main procedures, to be completed in sequence:

1. Create the Gateway record in the Controller.
2. Create the Gateway virtual machine instance in Azure and register it with the Controller.

Azure offers two methods for launching a Gateway virtual machine instance:

- Through the Azure Marketplace
- Using the provided template and image files

---

**Note:** ZTA Gateway instances in Azure Marketplace is limited to version 21.3R1. To use a Gateway version later than 21.3R1, either launch the Azure Marketplace version and upgrade in-place to the latest version, or use the

alternate procedure described below to launch a Gateway instance using the template and image files.

---

Before you start, make sure you have the following information and files:

- An identifying name for the Gateway
- The Gateway geographic location.
- (Optional) The name of the *Gateway Group* to which you want to add this new Gateway record. To learn more about Gateway Groups, see the *Tenant Admin Guide*.
- The primary (and optional secondary) DNS server IP address, and search domain.
- The SSH public key that you are using with the Azure Portal or Management Console.

---

**Note:** SSH keys can be generated using sshkeygen on Linux and macOS, or PuTTYGen on Windows. For further details about generating SSH key pairs, see: \* For Windows: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows>  
\* For MacOS and Linux: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys>

---

- Credentials for the Azure Portal or Management Console.

---

**Note:** These credentials must include sufficient permissions to create a virtual machine.

---

Additionally, if you are deploying a Gateway instance directly from the template and image files (as opposed to using the Azure Marketplace):

- The Gateway template JSON file:

---

**Note:** A ZTA Gateway can be deployed in a new VNET or an existing VNET. Select the JSON template file applicable to your requirements.

---

- To deploy in a new VNET: <https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-2-nics.json>  
<https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-3-nics.json>
- To deploy in an existing VNET: <https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-2-nics-existing-vnet.json>  
<https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-2-883/ivanti-zta-3-nics-existing-vnet.json>



---

**Note:** If you want to use a Management interface, you must download and use the 3 NIC template.

---

- A link to the Gateway template image file. Choose from:
  - **Americas:** <https://pulsezta.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd>
  - **APJ:** <https://pulseztaapj1.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd>
  - **Europe:** <https://pulseztaeurope.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd>

Use the link most suitable for your geographic location. The instructions that follow include details of how to use *azcopy* to copy the VHD file into your storage account.

---

**Note:** You can also choose to download this file from the **Gateways Overview** page of the Tenant Admin Portal. The opportunity to do this occurs later in this process.

---

- A public IP address or CNAME for the Gateway. This is the IP address or CNAME at which client devices can externally reach the Gateway instance.

To create a Gateway record in the Controller, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:
  - On unconfigured nZTA systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
  - On configured nZTA systems, the **Network Overview** page appears. In this case:
    - From the nZTA menu, click the **Secure Access** icon, then select **Gateways > Gateway List**.

The *Gateways List* page appears, showing the full list of Gateway Groups and standalone Gateways currently configured on the Controller.

    - To add a new Gateway, select **Create** from the top-right:

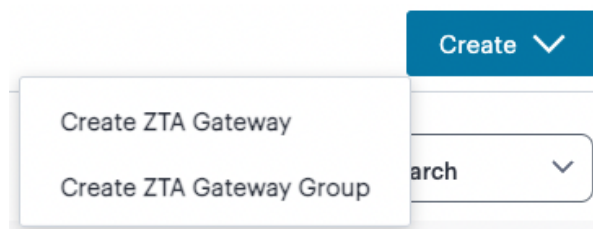


FIGURE 3.10 : Add a new Gateway or Gateway Group

– In the drop-down menu, click **Create ZTA Gateway**.

In both cases, the **Gateway Network Configuration** dialog appears.

The screenshot shows the 'Gateway Network Configuration' dialog box. At the top left, there is a back arrow and the title 'Create ZTA Gateway'. The dialog is divided into several sections:

- Gateway Details:** Includes a dropdown for 'GATEWAY PLATFORM' set to 'Azure' and a checkbox for 'Use Manual Settings'.
- Gateway Information:** Includes input fields for 'NAME', 'PUBLIC ADDRESS or CNAME', and an 'ADD' button.
- Location:** Includes dropdowns for 'COUNTRY', 'STATE/REGION', and 'CITY'.
- Add this Gateway to a group:** Includes a dropdown for 'GATEWAY GROUP' set to 'Select a gateway group' and a 'CREATE GATEWAY GROUP' button.
- Gateway Network Settings:** Includes a checkbox for 'Use Management Port'.
- Internal Network / Private Subnet:** Includes input fields for 'PRIMARY DNS', 'SECONDARY DNS', and 'DNS SEARCH DOMAIN'.

At the bottom right, there are 'CANCEL' and 'Create Configuration' buttons.

FIGURE 3.11 : Gateway Network Configuration

**Note:** To learn more about the settings on this page, see the *Tenant Admin Guide*.

2. For **Gateway Platform**, select “Azure”.
3. Enter a **Name** for the Gateway.
4. Enter one or more **Public Address or CNAME** (Public IP address or CNAME) for the Gateway. Select **Add** to add each entry to the list.

**Note:** For Azure Marketplace deployments, a public IP address or CNAME is typically allocated at deployment time through the Azure Portal. Therefore, if you do not yet know the expected address/CNAME, enter a dummy value in this field now and update the setting after you have deployed and registered the Gateway instance. For more details on this process, see [Creating a Gateway through Azure Marketplace](#) (page 64).

5. Select a geographic **Location** for the Gateway.
6. (Optional) Select a Gateway **Group** to which the new Gateway is to be added.
7. (Optional) Select the **Use Management Port** check box to use management network ports for nZTA traffic rather than internal ports.

---

**Note:** When the management port is enabled, the Controller will still use the internal port for DNS resolution. If the internal DNS cannot resolve the Controller domain, the internal interface will require internet access.

---

8. Enter the Primary DNS IP address for the Gateway.
9. (Optional) Enter the Secondary DNS IP address for the Gateway.
10. Enter the DNS Search Domain for the Gateway.

---

**Note:** Make sure the specified DNS service can resolve the IP address of your Controller. Issues here can cause registration of the Gateway with the Controller to fail.

---

11. To add a Gateway definition based on the settings you specified in this dialog, select **Create Configuration**.

After you complete the first part of this workflow, an unregistered Gateway record is created on the Controller. This Gateway record can be seen on the **Gateways > Gateways List** page.

12. On the *Gateways List* page, select your new Gateway and click the **Download** icon to obtain a copy of the Gateway definition file.

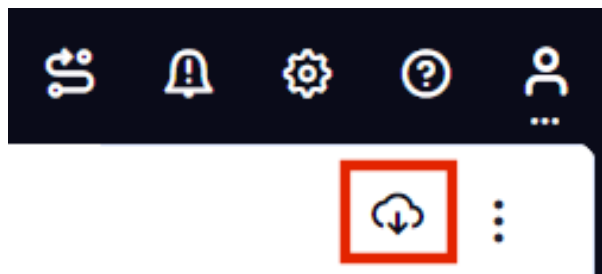


FIGURE 3.12 : The Download Icon

Retain this file for a later step.

---

**Note:** The Gateway definition file is valid for 24 hours. If this period expires, you must replace the Gateway to generate a new Gateway definition file.

---

13. (Optional) If you have not yet downloaded the latest version of your Gateway VM file, click the **Download** icon and select **Download gateway VM image**. Save the archive file and unpack to a local workstation. Make sure the resulting file set is accessible from the Microsoft Azure Console.

Next, decide which Azure deployment process you want to follow - launching an instance through Azure Marketplace, or creating an instance using the supplied template and image files.

- To launch an instance from Azure Marketplace, see [Creating a Gateway through Azure Marketplace](#) (page 64).
- To create an instance using the nZTA template and image files, see [Creating an Gateway using the Azure Template and Image Files](#) (page 68).

## Creating a Gateway through Azure Marketplace

---

**Note:** ZTA Gateway instances in Azure Marketplace are limited to version 21.3R1 at the present time. To use a Gateway version later than 21.3R1, either launch the Azure Marketplace version and upgrade in-place to the latest version (for more details, see the *Tenant Admin Guide*) or use the alternate procedure described in [Creating an Gateway using the Azure Template and Image Files](#) (page 68) to launch a Gateway instance using the template and image files.

---

To launch a Gateway virtual machine in Microsoft Azure from the Azure Marketplace, perform the following steps:

1. Log into the Microsoft Azure Portal (<http://portal.azure.com>).
2. Navigate to the Azure Marketplace by clicking **Create a resource**.
3. In the *Search the Marketplace* text box, enter “Ivanti”.  
Azure Marketplace presents the results relevant to your search term.
4. Locate *Ivanti Neurons Zero Trust Access Gateway* and click **Create**.
5. In the drop-down list, choose the option that is applicable to your needs:
  - **Ivanti Neurons Zero Trust Access Gateway - BYOL 3 NIC:** Includes 3 network interfaces (internal, external, and management)
  - **Ivanti Neurons Zero Trust Access Gateway - BYOL 2 NIC:** Includes 2 network interfaces (internal and external)

---

**Note:** To first learn more about *Ivanti Neurons Zero Trust Access Gateway*, click the product banner and view the associated information page. You can launch a new Gateway instance from this page.

---

The *Create Ivanti Neurons Zero Trust Access Gateway* process appears.

6. On the *Basics* tab, enter the following details:
  - **Subscription:** If you are using the “PZT\_Dev” subscription, leave this field as the default value. Otherwise, enter your subscription name.
  - **Resource Group:** Specify the resource group in which the Gateway needs to be deployed, or create a new resource group using the link

provided. An Azure Resource Group is a container for a collection of connected assets that you assign to a virtual machine. To learn more, see the Azure documentation (<https://docs.microsoft.com/azure>).

- **Region:** Specify the geographic region in which the Gateway instance is deployed.
- **Ivanti Neurons Zero Trust Access Gateway VM Name:** Enter a suitable name for your Gateway instance. This name must be 1-9 characters long, using only lowercase letters or numbers.
- **SSH Public Key Source:** Select “Use existing public key”.
- **SSH Public Key:** Copy and paste an RSA public key in a single-line format or the multi-line PEM format.

---

**Note:** SSH keys can be generated using `sshkeygen` on Linux and macOS, or PuTTYGen on Windows. For further details about generating SSH key pairs, see: \* For Windows: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows>  
\* For MacOS and Linux: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys>

---

To continue, click **Next: Network Settings >**.

7. On the *Network Settings* page, enter the following details:

- **Virtual Network:** A virtual network is a logical isolation of the Azure cloud dedicated to your services. The value you enter here affects the IP address and subnet allocations for all network interfaces shown on this page. Azure pre-populates this field with a new virtual network name, although you can select your own predefined virtual network as necessary.

To create a new virtual network, perform the following steps:

1. Click the **Create New** link under the Virtual Network setting.  
The *Create virtual network* dialog appears.
2. Enter a virtual network name.
3. Enter an address space in CIDR notation (for example, 192.0.2.0/24).
4. For each interface subnet, use the automatically-populated name and address values provided, or enter your own details. Each subnet must be contained by the address space entered in the previous setting.
5. To save your changes, click **OK**.

Your new virtual network settings are populated into the corresponding interface settings in the main *Network Settings* page.

- **Internal Subnet:** The subnet identifier for the Internal network, pre-populated by either the selected Virtual Network or your newly-entered virtual network settings.

- **External Subnet:** The subnet identifier for the External network, pre-populated by either the selected Virtual Network or your newly-entered virtual network settings.
- (For 3 NIC instances only) **Management Subnet:** The subnet for the Management network, pre-populated by either the selected Virtual Network or your newly-entered virtual network settings.
- **Public IP for Ivanti Neurons Zero Trust Access Gateway external interface LB:** The public IP address identifier at which clients can externally reach the Gateway instance, typically provided by Azure.

---

**Note:** Before you can connect to the new Gateway instance from the Controller, you must update the Controller with the Public IP address or CNAME assigned to the external interface of the Gateway load balancer. This process is described later.

---

- **DNS prefix for external interface LB:** The unique DNS name for the public IP address specified for the external interface load balancer.
- **Public IP for NAT Gateway:** The public IP address identifier of a NAT Gateway for the virtual machine to communicate with the Controller and other public resources.
- **DNS prefix for NAT Gateway public IP:** The unique DNS name for the public IP address specified for the internal interface NAT Gateway.
- **Deploy Ivanti Neurons Zero Trust Access Gateway with Load Balancer:** To deploy this Gateway with a load balancer, select “Yes” from the drop-down list. The front-end IP address of the load balancer is then used as the public IP address for your Gateway.

---

**Note:** If you select “No” to not deploy a load balancer, you must create and associate a public IP address to the external interface of your instance after deployment is complete.

---

In all cases, on completion of this process, you must update the Controller Gateway definition with the correct public IP address for your Azure Gateway instance.

To continue, click **Next: Instance Configuration >**.

8. On the *Instance Configuration* page, enter the following details:

- **Ivanti Neurons Zero Trust Access Gateway VM Size:** This is the specification of the virtual machine. Choose from:
  - For 2nic instances, select “1 x Standard DS2 v2”
  - For 3nic instances, select “1 x Standard DS4 v2”
- **Diagnostic storage account:** The storage account for the virtual machine diagnostics. The default value is a new account based on your VM name.

- **Ivanti Neurons Zero Trust Access Gateway Version:** Specify the version applicable to the current nSA version, or the version you require. Ivanti recommends you select the latest available version.
- **Ivanti Neurons Zero Trust Access Gateway Config Data:** Paste in the raw text of your Gateway definition file. To obtain the Gateway definition file, see the process described earlier in this section.

To continue, click **Next: Review + create >**.

9. On the *Review + create* page, verify the proposed configuration is validated successfully, and then click **Create** to create your new Gateway instance.

After a short wait, your instance is created and deployed.

10. Access the virtual machine settings for your new Gateway instance, and click **Networking** from the *Settings* menu.

The *Networking* dialog appears, showing your attached network interfaces (internal, external, and (optionally) management).

11. Click the tab that corresponds to the *external* network interface.

The settings for the external network interface appear.

12. Locate the **NIC Public IP** field and make a note of the IP address shown there. This is the public IP address you use to reconfigure the Controller record for this Gateway.

If no public IP address is shown, determine if a load balancer was deployed together with your Gateway instance by selecting the **Load balancing** tab.

- If a load balancer was deployed, make a note of the **Frontend IP address** displayed in this tab and use this as the Gateway public IP address on the Controller.
- If a load balancer was not deployed, create a public IP address and associate it with the *external* interface. Then, use this IP address as the Gateway public IP address on the Controller.

---

**Note:** To learn about configuring IP addresses in the Azure portal, see the Microsoft Azure documentation.

---

13. Return to the nZTA Tenant Admin Portal, and click **Secure Access > Gateways > Gateways List**.

The *Gateways List* page appears.

14. Make sure the new Azure Gateway instance is shown in the list of configured Gateways and is connected (Connection Status is *Connected*).
15. Select the new Gateway, then select **Secure Access > Gateways > Configuration** and locate *Gateway Network Settings*. Enter the Public IP address you noted from the Azure virtual machine settings. Make sure you remove any previously-entered dummy values.
16. To save your changes, click **Save Changes**.

This completes the Azure Gateway registration process. Your enrolled client devices should now be able to connect to the Gateway.

## Creating an Gateway using the Azure Template and Image Files

To create a Gateway virtual machine in Microsoft Azure from the nZTA template and image files applicable to this release, perform the following steps.

**Before you start**, you must complete the following prerequisites:

- Create a new *Azure Resource Group* in your desired location and subscription account.
- Create a new *storage account*, and create a new container in that account.
- Download the nZTA Azure VHD image file for your region and copy it to the storage account you created in the previous step.

Choose to download from the following regions:

- **Americas:** <https://pulsezta.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd>
- **APJ:** <https://pulseztaapj1.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd>
- **Europe:** <https://pulseztaeurope.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.3R4-883.1-SERIAL-hyperv.vhd>

For this process, you can use *azcopy*:

1. From the storage account, create a Shared Access Signature (SAS) token:



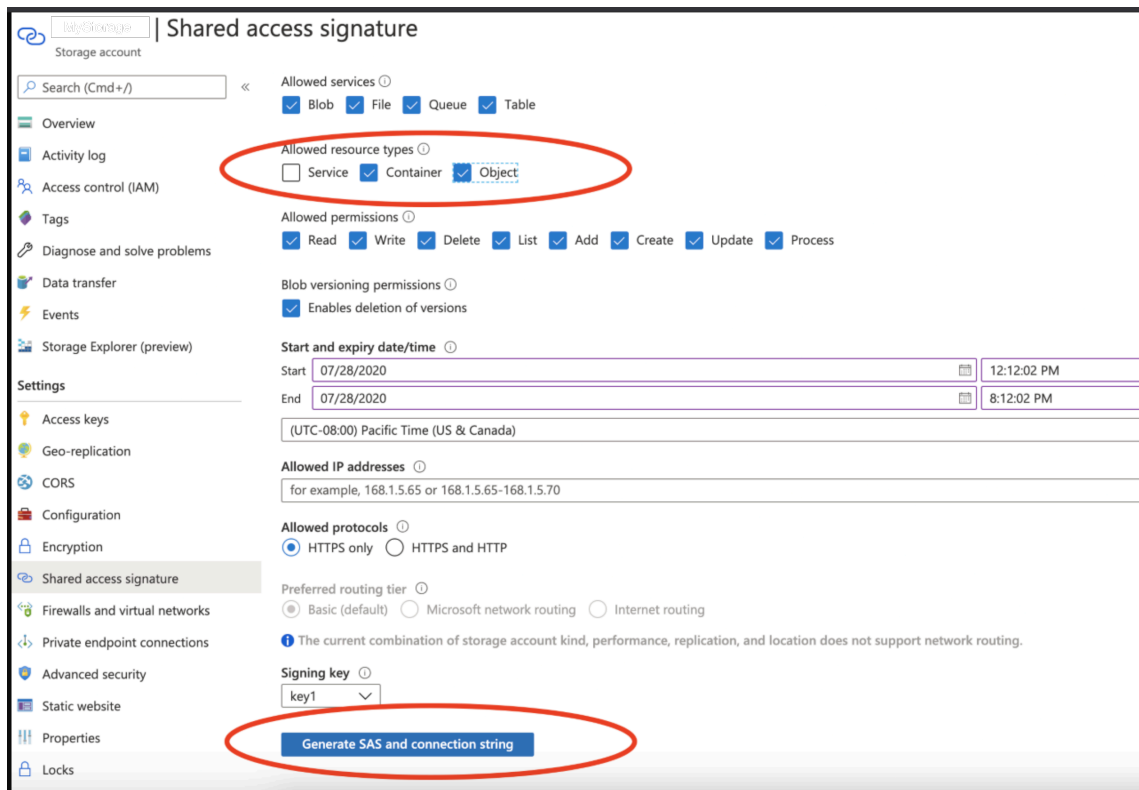


FIGURE 3.13 : Creating a SAS token from a storage account in Azure

2. Open the Azure Cloud Shell and start a bash shell:

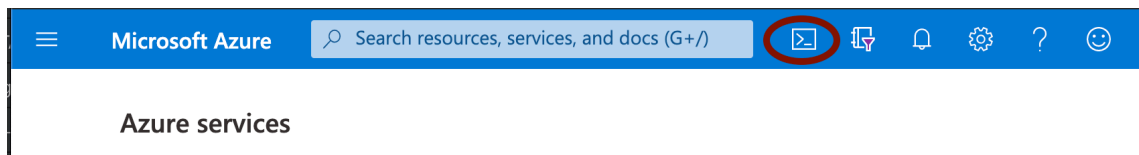


FIGURE 3.14 : Starting the Azure Cloud Shell

3. In the Azure Cloud shell, use `azcopy` to copy the Gateway VHD image file into your storage account. For example, use the following syntax:

```
azcopy copy '<URL to VHD file>' 'https://<MyStorageAccount>.
↵blob.core.windows.net/<Container_Name>/<VHD filename><SAS-
↵Token>'
```

Replace the angled-bracket elements with the details gathered in previous steps. For example:

```
azcopy copy 'https://pulseztaeurope.blob.core.windows.net/
↵gateway/PSA-V-HYPERV-ZTA-189.1-SERIAL-hyperv.vhd' 'https://
↵MyStorage.blob.core.windows.net/gateway/PSA-V-HYPERV-ZTA-189.
↵1-SERIAL-hyperv.vhd?sv=2018-11-12&ss=bfqt&srt=co&
↵sp=rwldacupx&se=2019-12-29T02:57:39Z&st=2020-07-28T18:57:39Z&
↵spr=https&sig=mJU7WNd9oNY7wcXNOqEOhbYshD9Sxv56rqE1%2FmEuCg4
↵%3D'
```

After you have completed the above prerequisites, create a Gateway instance using following steps:

---

**Note:** For reference, the recommended minimum requirements for a Gateway virtual machine instance in Azure are:

- Standard\_D2s\_v3 (2 vCPU, 8 GB Memory), or
  - Standard\_F4s (4 vCPU, 8 GB Memory)
- 

1. Access the Azure Management Console and log in using your credentials.
2. Access the **Home > Templates** page to view available templates.
3. Click "+ Add" to add a new template.
4. In the new template "General" section, enter a template name and description.
5. In the new template "ARM Template" section, remove the default data and replace with the raw text contents of the nZTA Azure Gateway template JSON file.

---

**Note:** Use either the *new VNET* template JSON file or the *existing VNET* template JSON file as per your requirements.

---

6. Save the new template.
7. On the **Home > Templates** page, locate the new Azure Gateway template.
8. On the context menu for the template, click **Deploy**.  
The **Custom Deployment** page appears.
9. On the **Custom Deployment** page, enter any required details for the Gateway deployment.
  - **Resource Group:** Specify the resource group name in which the Gateway needs to be deployed, or create a new group.
  - **Location:** Specify the region in which the Gateway instance is deployed.
  - **nZTA Storage Account Name:** Specify the storage account you created earlier where the Gateway image is held.
  - **nZTA Storage Account Resource Group:** Specify the resource group you created earlier.
  - **nZTA Image Location URI:** Enter the full URI for the Gateway template image VHD file you copied to your storage account earlier.
  - **nZTA VM Name:** Enter a suitable name for your Gateway instance. Pulse recommends matching the Gateway name used during the process of creating the Gateway record on the Controller.
  - **nZTA Config:** Paste in the raw text of your Gateway definition file. To obtain the Gateway definition file, see the process described earlier in this section.

- **SSH Public Key:** Specify your SSH key pair name.
10. If required, update the labels for the instance:
    - Update the **Dns Label Prefix Ext** if required. For example, “azuregwext”.
    - Update the **Dns Label Prefix Mgmt** if required. For example, “azuregwmgmt”.
    - Update the **Existing Vnet Name** if required.
    - Update the **Existing Internal Subnet** if required. For example: “InternalNW”.
    - Update the **Existing External Subnet** if required. For example: “ExternalNW”.
    - Update the **Existing Management Subnet** if required. For example: “ManagementNW”.
  11. For **Load Balancer Configuration**, If you plan to deploy multiple Gateways inside a Gateway Group, select “Yes” to deploy a new internet-facing Public Standard Load Balancer instance alongside the Gateway. Select “No” to launch only this Gateway instance.

---

**Note:** This option is applicable only for new VNET templates.

---

If you elect to launch a load balancer, the following pre-configuration is applied:

- A Standard SKU Public IP address is assigned to the Load Balancer.
- A Backend Pool is created and the deployed Gateway is associated with the pool through its external network interface.
- A health probe is configured on TCP port 443.
- Load balancing rules are configured.

After you have deployed the Gateway and Load Balancer, you must return to the Tenant Admin Portal on the Controller and update the Gateway Group **Load Balancer IP ADDRESS** setting to be the Load Balancer’s public IP address.

If you want to configure the Load Balancer to balance across further Gateway instances from the Gateway Group, you must deploy each subsequent Gateway into the same Resource Group through the use of existing VNET templates and then update the Load Balancer’s Backend Pool.

---

**Note:** With new VNET templates, a NAT gateway is deployed for routing outbound Internet traffic from the Gateway’s internal network interface in order for the Gateway to be able to reach the Controller.

---

---

**Note:** Public IP addresses are not automatically assigned to any of your Gateway’s network interfaces. If you are deploying a Gateway into an existing

VNET, in order for the Gateway to be able to reach the Controller from its internal network interface, make sure you allow outbound Internet traffic from the Private Subnet for the deployed Gateway.

---

To learn more about high availability and Gateway Groups, see the *Tenant Admin Guide*.

12. Agree to the terms and conditions.
13. Click **Purchase** to start the creation of the Gateway.

A window displays the status of the process, starting with **Deployment in Progress**.

(Optional) Click the **Deployment in Progress** hyperlink to view a status page for the process.

14. Wait until the process completes.
15. Ensure that your Azure Security Groups support the IP addresses allocated to the Gateway instance. Please refer to Azure's own documentation for full details.
16. *(This step is required only if you have not deployed your Gateway with a Load Balancer or NAT at the front-end)* Public IP addresses are not automatically assigned to any of the Gateway's network interfaces. Therefore, before your client devices can connect to the new Gateway instance from the Controller, you must associate a new Public IP address with the external interface of the Gateway. Then, update the Controller's Gateway Public IP address setting to match this address (in the **Secure Access > Gateways Overview** page, select your new Gateway, then click the **Configuration** tab and locate *IP Settings*).
17. In the **Secure Access > Gateways > Gateways List** page, make sure the new Gateway has a confirmed status of *Connected*.

This completes the Azure Gateway registration process. Your enrolled client devices should now be able to connect to the Gateway.

---

**Note:** After you have registered a Gateway, you can configure it (or the Gateway Group to which it belongs) as the default Gateway if required. See the *Tenant Admin Guide* for details.

---

## Workflow: Creating a Gateway in KVM/OpenStack

This workflow leads you through the process for setting up a KVM Gateway in OpenStack. It contains two main procedures, in sequence:

- Preparing to create a KVM gateway, see [Preparing to Create a KVM Gateway](#) (page 73).
- Creating the gateway record in the Controller, see [Adding a KVM Gateway in nSA](#) (page 74).

- Preparing Metadata for OpenStack, see [Preparing Metadata for OpenStack](#) (page 77).
- Creating the KVM Gateway virtual machine instance in OpenStack, see [Creating the KVM Gateway Virtual Machine Instance in OpenStack](#) (page 79).

After these steps have been completed successfully, the Controller and Gateway establish communication with each other.

## Preparing to Create a KVM Gateway

Before you start, make sure you have the following information and files:

- An identifying name for the Gateway
- The public IP address for the Gateway. This is the IP address at which clients can externally reach the Gateway instance.
- The Gateway geographic location
- (Optional) The name of the *Gateway Group* to which you want to add this new Gateway record. To learn more about Gateway Groups, see the *Tenant Admin Guide*.

Additionally, to manually specify KVM Gateway network interface settings:

- The primary (and optional secondary) DNS server IP address, and search domain.
- The required internal/private subnetworks must already be defined on OpenStack. Please refer to the OpenStack documentation for details.
- The required external subnetworks must already be defined on OpenStack. Please refer to the OpenStack documentation for details.
- (Optional) Any required management subnetwork must already be defined on OpenStack. Please refer to the OpenStack documentation for details.
- The Gateway KVM template: <https://pulsezta.blob.core.windows.net/gateway/ISA-V-KVM-ZTA-22.3R4-883.1.zip>

---

**Note:** Download a copy of the KVM template ZIP file. Then fully unpack the ZIP file, including any compressed .gz files inside, it to a local workstation. Make sure that the resulting file set is accessible from the OpenStack Console.

---

---

**Note:** You can also choose to download this file from the **Gateways Overview** page of the Tenant Admin Portal. The opportunity to do this occurs later in this process.

---

- Credentials for the OpenStack Console.

---

**Note:** These credentials must include sufficient permissions to create a virtual machine from a template image.

---

After you have all required information, you can set up a nZTA KVM gateway, see [Adding a KVM Gateway in nSA](#) (page 74).

## Adding a KVM Gateway in nSA

To set up a nZTA KVM Gateway, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:
  - On unconfigured nZTA systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
  - On configured nZTA systems, the **Network Overview** page appears. In this case:
    - From the nZTA menu, click the **Secure Access** icon, then select **Gateways > Gateway List**.

The *Gateways List* page appears, showing the full list of Gateway Groups and standalone Gateways currently configured on the Controller.

- To add a new Gateway, select **Create** from the top-right:

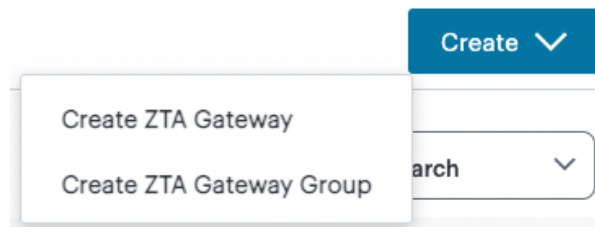


FIGURE 3.15 : Add a new Gateway or Gateway Group

- In the drop-down menu, click **Create ZTA Gateway**.

In both cases, the **Gateway Network Configuration** dialog appears.

**Gateway Network Configuration**

Gateway Details

GATEWAY PLATFORM  
KVM  Use Manual Settings

Gateway Information

NAME PUBLIC ADDRESS or CNAME ADD

Location

COUNTRY STATE/REGION CITY

Add this Gateway to a group  
Add gateway to any of the predefined gateway group or create a new gateway group

GATEWAY GROUP  
Select a gateway group CREATE GATEWAY GROUP

Gateway Network Settings

Use Management Port  Use Dynamic Tunnel IP

Internal Network / Private Subnet

PRIMARY DNS SECONDARY DNS DNS SEARCH DOMAIN

CANCEL Create Configuration

FIGURE 3.16 : Gateway Network Configuration

**Note:** To learn more about the settings on this page, see the *Tenant Admin Guide*.

2. For **Gateway Platform**, select “KVM”.
3. Enter a **Name** for the Gateway.
4. Enter one or more **Public Address or CNAME** (Public IP address or CNAME) for the Gateway. Select **Add** to add each entry to the list.
5. Select a geographic **Location** for the Gateway.
6. (Optional) Select a Gateway **Group** to which the new Gateway is to be added.
7. (Optional) Select the **Use Management Port** check box to use management network ports for nZTA traffic rather than internal ports.

**Note:** When the management port is enabled, the Controller will still use the internal port for DNS resolution. If the internal DNS cannot resolve the Controller domain, the internal interface will require internet access.

8. (Optional) Select the **Use Dynamic Tunnel IP** check box to configure a pool of

IP addresses that are dynamically mapped to client sessions with this Gateway, such that user traffic from the Gateway to an application can be identified as originating from a specific client.

The *Custom IP Pool* dialog appears:

Use Management Port     Use Dynamic Tunnel IP

Custom IP Pool



ASSIGNABLE CUSTOM IPV4 ADDRESS   Example: x.x.x.x/netmask  
netmask would be in the range  
of 8-28

FIGURE 3.17 : Gateway Network Configuration - Custom IP Pool settings

---

**Note:** Dynamic Tunnel IP addresses are not supported in Gateway Groups.

---

Use the **Assignable Custom IPv4 Address** field to enter an IP address and subnet (in the range 8-28) in CIDR notation, then click **Add**. Repeat this step for each address/subnet you want to use.

9. Enter the Primary DNS IP address for the Gateway.
10. (Optional) Enter the Secondary DNS IP address for the Gateway.
11. Enter the DNS Search Domain for the Gateway.

---

**Note:** Make sure the specified DNS service can resolve the IP address of your Controller. Issues here can cause registration of the Gateway with the Controller to fail.

---

12. To add a Gateway definition based on the settings you specified in this dialog, select **Create Configuration**.

After you complete the first part of this workflow, an unregistered Gateway record is created on the Controller. This Gateway record can be seen on the **Gateways > Gateways List** page.

You can now prepare your metadata, see [Preparing Metadata for OpenStack](#) (page 77).



## Preparing Metadata for OpenStack

The preparation of metadata for use on OpenStack currently requires some manual steps:

1. Log into nZTA and access the **Gateways > Gateways List** page.
2. On the *Gateways List* page, select your new Gateway and click the **Download** icon to obtain a copy of the Gateway definition file.

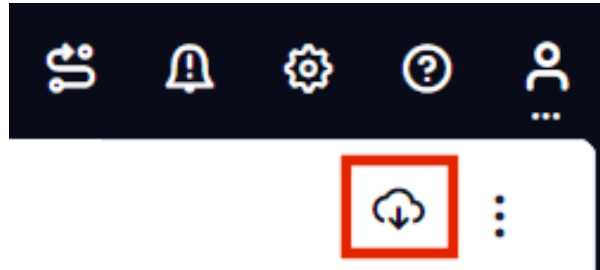


FIGURE 3.18 : The Download Icon

3. Specify a save location for your Gateway definition file.

---

**Note:** The Gateway definition file is valid for 24 hours. If this period expires, you must replace the Gateway to generate a new Gateway definition file.

---

4. (Optional) If you have not yet downloaded the latest version of your Gateway VM file, click the **Download** icon and select **Download gateway VM image**. Save the archive file and unpack to a local workstation. Make sure the resulting file set is accessible from the OpenStack Management Console.
5. View the gateway definition file in a text editor.
6. Start a separate text editor file, and paste the following template text block into it:

```
<pulse-config>
  <config-download-url>
    '<insert vaConfigURL value here>'
  </config-download-url>
  <appliance-id>
    <insert vaApplianceID value here>
  </appliance-id>
  <secondary-dns>
    <insert vaSecondaryDNS here>
  </secondary-dns>
  <primary-dns>
    <insert vaPrimaryDNS here>
  </primary-dns>
  <dns-domain>
    <insert vaDnsSearchDomain here>
  </dns-domain>
</pulse-config>
```

(continues on next page)

(continued from previous page)

```

    <insert vaCommonName value here>
  </cert-common-name>
  <accept-license-agreement>
    y
  </accept-license-agreement>
  <controller-enrolled-hostname>
    <insert vaControllerEnrolledHostname value here>
  </controller-enrolled-hostname>
  <dns-search-domain>
    <insert vaDnsSearchDomain value here>
  </dns-search-domain>
  <controller-hostname>
    <insert vaControllerHostname value here>
  </controller-hostname>
</pulse-config>

```

7. For each parameter block in the template text block file:

- Locate the required metadata property for the line.

For example, in the following block:

```

<appliance-id>
  <insert vaApplianceID value here>
</appliance-id>

```

You require the **vaApplianceID** value from the gateway definitions file.

- Locate the required value in the gateway definitions file.

For example, the **vaApplianceID** value is  
*99ce3aa3c9494cbabb51c085c9c3f6ad*.

- Copy and paste this value from the gateway definitions file into the template text file.

For example, the <appliance-id> block will now read as follows:

```

<appliance-id>
  99ce3aa3c9494cbabb51c085c9c3f6ad
</appliance-id>

```

---

**Note:** You do not need to change the <accept-license-agreement> block, and can retain its y setting.

---

8. After you have added all required text to the template text file, save that file for use in the next section.

You can now create a KVM gateway VM in Openstack, see [Creating the KVM Gateway Virtual Machine Instance in OpenStack](#) (page 79).

## Creating the KVM Gateway Virtual Machine Instance in OpenStack

To create a KVM VM instance in OpenStack:

1. Access the *OpenStack Management Portal*, either from a client or a web browser, and log in using your OpenStack credentials.

In the OpenStack console, the **Overview** page appears.

2. In the left menu, click **Compute > Images**.

The **Images** page appears. This shows a list of images.

3. Above the list of images, click **Create Image**.

The **Create Image** wizard appears. In this wizard, you upload a KVM gateway image for use.

4. Under **Image Details**:

- Enter an **Image Name**. Typically, this incorporates a version number. For example, *ZTA\_GWY\_100*.
- Enter an **Image Description**. For example: *ZTA KVM Image*.
- Under **Image Source**, click **Browse** and select the unpacked KVM disc image file. Then, click **Format** and select *QCOW2 - QEMU Emulator*.
- Under **Image Requirements**, set **Minimum Disk (GB)** to *40* and **Minimum RAM (KB)** to *2048*.
- Set **Visibility Setting** as required. *Public* will enable the image to be used in other projects. *Private* will not.
- Set **Image Sharing** as required.
- Use the default settings for all other properties.

5. Click **Next**.

The **Metadata** page of the wizard appears. No action is required on this page, all properties can use their default settings.

6. Click **Create Image**.

The wizard closes, and the new KVM gateway image is added to the **Images** page.

7. Wait until the image has been uploaded and processed and shows as *Active*.

---

**Note:** The upload image process typically takes 15-20 minutes.

---

8. After the image has uploaded and is *Active*, click its **Launch** button.

The first page of the **Launch Instance** wizard appears. In this wizard, you create a KVM gateway instance.

9. Under **Details**:

- Enter an **Instance Name**. This will be the displayed name of the gateway in nZTA.
- Enter a **Description** for the KVM gateway. For example *ZTA KVM Gateway*.
- Use the default settings for all other properties.

10. Click **Next**.

The **Source** page of the wizard appears. This page lists the selected disk image and selected/default settings for the instance. No action is required on this page, all properties can use their displayed settings.

11. Click **Next**.

The **Flavor** page of the wizard appears. This page lists the available types of gateway you can create.

12. Locate the *PSA3000-V* entry and click its “up arrow” button to select it.

13. Click **Next**.

The **Networks** page of the wizard appears. This page lists the available networks (and associated subnetworks) for the gateway. It enables you to select the required subnetworks for your gateway.

14. In the available list, locate the required subnetworks.

For example, you may require a subnetwork for internal ports and a subnetwork for external ports, but not a subnetwork for management interfaces.

---

**Note:** If the required subnetworks do not yet exist, you must define them. Please refer to the OpenStack documentation for details of this process.

---

15. Click the “up arrow” button for each subnetwork to select it.

---

**Note:** For each selected subnetwork, a fixed IP address is added automatically to the gateway. These appear later in this process, so that they can be assigned to floating IP addresses.

---

16. Click **Next**.

The **Network Ports** page of the wizard appears. No action is required on this page, all properties can use their displayed settings.

17. Click **Next**.

The **Security Groups** page of the wizard appears. No action is required on this page, all properties can use their displayed settings.

18. Click **Next**.

The **Security Groups** page of the wizard appears. No action is required on this page, all properties can use their displayed settings.

---

**Note:** If there is no default security group defined, you must define one. Please refer to the OpenStack documentation for details of this process.

---

19. Click **Next**.

The **Key Pair** page of the wizard appears. No action is required on this page, all properties can use their displayed settings.

20. Click **Next**.

The **Configuration** page of the wizard appears. This page enables you to configure the gateway instance using metadata you prepared earlier, see [Adding a KVM Gateway in nSA](#) (page 74).

21. Open your template text file and copy the entire text block that starts with `<pulse-config>` and ends with `</pulse-config>`.
22. Paste the text block into the **Customization Script** block.

---

**Note:** You cannot directly paste metadata for your gateway from nZTA. You must prepare a suitable text block from the metadata, see [Adding a KVM Gateway in nSA](#) (page 74).

---

23. Enable the **Configuration Drive** check box.

24. Click **Launch Instance**.

The wizard closes, and the new KVM gateway instance is added.

25. Access the **Instances** page.

The new KVM gateway instance is listed on this page.

26. Wait until the **Power State** of the gateway instance is *Running*.

---

**Note:** This process may take several minutes.

---

27. After the instance state changes to *Running*, make a note of the subnetworks and their automatically-assigned fixed IP addresses in the **IP Address** column for the instance. For example:

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor
<input type="checkbox"/>	kvmgw3	ZTA_GW_68	ext-port-2 5.5.10.64 int-port-2 4.4.10.83	PSA3000-V

FIGURE 3.19 : Unassociated KVM Ports

In this example, floating IP addresses are listed after the fixed IP addresses, so all are unassociated:

- The fixed IP address on the *int-port-2* subnetwork is 4.4.10.83.
- The fixed IP address on the *ext-port-2* subnetwork is 5.5.10.64.

28. Access the **Network > Floating IPs** page.

The **Floating** IPs page shows the floating IP addresses associated with your account. Both associated and unassociated floating IP addresses are listed.

---

**Note:** Associated floating IPs have a **Mapped Fixed IP Address** listed.

---

29. Identify an unassociated floating IP address that you want to associate with a fixed IP address.

30. Click the **Associate** button for the fixed IP address.

The **Manage Floating IP Associations** dialog appears.

31. Select a fixed **port to be associated** for the selected floating IP address.

32. Click **Associate** to conform the association.

33. Repeat the association process until each of the fixed IP addresses for your gateway instance is associated with a floating IP address.

34. Wait until the status of these floating IP addresses all show as *Active*.

35. Return to the **Compute > Instances** page.

This page now shows a fixed IP address associated with floating IP address for each port. For example:

<input type="checkbox"/>	Instance Name	Image Name	Address	Flavor
<input type="checkbox"/>	kvmgw3	ZTA_GW_68	<b>ext-port-2</b> 5.5.10.64, 10.96.145.196 <b>int-port-2</b> 4.4.10.83, 10.96.145.156	PSA3000-V

FIGURE 3.20 : Associated KVM Ports

36. Click the **Console** tab.

A console monitor view shows the ongoing boot-up process for the instance.

37. Wait until the instance shows a screen similar to the following:

```

Welcome to the Pulse Zero Trust Access Serial Console!

Current version: 20.10R1 (build 68)
Reset version: 20.10R1 (build 68)

Licensing Hardware ID: UASPHYI7PLEU7F0MS

Please choose from among the following options:
0. Start shell
100. mount root rw and start rsync...
101. mount root rw and chpax /home/bin...
102. modify platform code...
103. validate files...
104. Start sshd for debugging ...
105. Manage fault injection scenarios
1. Network Settings and Tools
2. Create admin username and password
3. Display log/status
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Maintenance
8. Reset allowed encryption strength for SSL
Choice:

```

FIGURE 3.21 : KVM Instance Console Monitor

38. Return to the **Gateways List** page on the Controller.
39. Locate the new Gateway record in the list and confirm that its status has updated to *Connected*. For example:

ALL GATEWAYS				
Search				
Add				
Gateways List				
	GATEWAYS	CONNECTION STATUS	VERSION	STATUS
>	GCP			
∨	Standalone NZTA Gateways			
	aws265	Disconnected	21.3R3-265	
	awsnew171	Connected	21.6R1-171	
	esxgw111	Connected	21.3R3-265	
	gcp195	Connected	21.6R1-169	
	gcpnew	Not registered		
	kvmgw3	Connected	21.6R1-171	
	skaws	Not registered		
	vsphere01	Connected	21.6R1-169	

FIGURE 3.22 : KVM Gateway Connected

**Note:** After you have registered a Gateway, you can configure it (or the Gateway Group to which it belongs) as the default Gateway if required. See the *Tenant Admin Guide* for details.

## Workflow: Creating a Gateway in Google Cloud Platform

This workflow leads you through the processes for setting up a Gateway on the Google Cloud Platform (GCP). These processes must be performed in sequence:

- Preparing to create a GCP gateway, see [Preparing to Create a GCP Gateway](#) (page 84).
- Creating the gateway record in the Controller, see [Adding a GCP Gateway in nSA](#) (page 87).
- Downloading Metadata for Google Cloud Platform, see [Downloading Metadata for Google Cloud Platform](#) (page 90).
- Uploading the GCP Image onto the Google Cloud Platform, see [Uploading the GCP Virtual Machine Image onto the Google Cloud Platform](#) (page 90).
- Creating a VM Instance of the GCP image. Either:
  - Creating a VM Instance of the Uploaded GCP Image Manually, see [Creating a VM Instance of the Uploaded GCP Image Manually](#) (page 92).
  - Creating a VM Instance of the Uploaded GCP Image Using a Script/Template, see [Creating a VM Instance of the Uploaded GCP Image Using a Script/Template](#) (page 97).
- Completing the Configuration of the Controller, see [Completing the Configuration of the Controller](#) (page 99).

After these steps have been completed successfully, the Controller and Gateway establish communication with each other.

### Preparing to Create a GCP Gateway

Before you start, make sure you have the following information and files:

- An identifying name for the Gateway.
- The public IP address for the Gateway. This is the IP address at which clients can externally reach the Gateway instance, such as an LB/NAT or Datacenter network forward rules.

---

**Note:** If you want Google Cloud platform to allocated a public IP address automatically, you can use a dummy IP address (for example, *1.1.1.1*) when you create the Gateway on nZTA. You must then update the Controller with the allocated public IP address afterwards.

---

- The Gateway geographic location.
- (Optional) The name of the *Gateway Group* to which you want to add this new Gateway record. To learn more about Gateway Groups, see the *Tenant Admin Guide*.



**Note:** A Gateway Group may have a defined public IP address, which you can specify during the creation of the Gateway.

Additionally, to manually specify GCP Gateway network interface settings:

- The primary (and optional secondary) DNS server IP address, and search domain.
- The required internal/private subnetworks must already be defined on Google Cloud Platform, including firewall settings. All required firewall settings for this interface are shown below.

The screenshot shows the Google Cloud Platform console for a project named 'pcs-project'. The page title is 'Network interface details'. Under the 'Firewall and routes details' section, the 'FIREWALL RULES' tab is selected and highlighted with a red box. Below the tabs, there is a 'Filter' section with a 'Filter table' dropdown. The main content is a table of firewall rules.

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network ↑	Logs
fw-backend-svr	Ingress	Apply to all	IP ranges	tcp:80,443,22,5001 icmp	Allow	1000	vpc-network-private-darumuga	Off
fw-pcs-int-port	Ingress	Apply to all	IP ranges	tcp:80,443,830,11000-11099,4808-4809,4900-4910 udp:4803-4804,4500 icmp	Allow	1000	vpc-network-private-darumuga	Off
ingress-pzt-int-port	Ingress	ingress-pzt-i	IP ranges	tcp:6667	Allow	1000	vpc-network-private-darumuga	Off

FIGURE 3.23 : Internal/Private Firewall Rules

Refer to the Google Cloud Platform documentation for details.

- The required external/public subnetworks must already be defined on Google Cloud Platform, including firewall settings. All required firewall settings for this interface are shown below.

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network ↑	Logs
egress-pcs-ext-port	Ingress	egress-pzt-ε	IP ranges: 12	all	Deny	1000	vpc-network-public-darumuga	Off
egress-pzt-ext-port	Ingress	egress-pzt-ε	IP ranges: 12	all	Deny	1000	vpc-network-public-darumuga	Off
a-firewall-rule	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:80,7001,443,6667,22	Allow	1000	vpc-network-public-darumuga	Off
default1-allow1-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:6666	Allow	1000	vpc-network-public-darumuga	Off
fw-pcs-ext-port	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:80,443 udp:4500 icmp	Allow	1000	vpc-network-public-darumuga	Off
ingress-pzt-ext-port	Ingress	ingress-pzt-ε	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	vpc-network-public-darumuga	Off

FIGURE 3.24 : External/Public Firewall Rules

Refer to the Google Cloud Platform documentation for details.

- (Optional) Any required management subnetwork must already be defined on Google Cloud Platform, including firewall settings. All required firewall settings for this interface are shown below.

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network ↑	Logs
fw-pcs-mgmt-port	Ingress	Apply to all	IP ranges	tcp:80,443,830,22 icmp	Allow	1000	vpc-network-mgmt-darumuga	Off
ingress-pzt-mgmt-port	Ingress	ingress-pzt-r	IP ranges	tcp:6667	Allow	1000	vpc-network-mgmt-darumuga	Off

FIGURE 3.25 : Management Firewall Rules

Refer to the Google Cloud Platform documentation for details.

- The ZTA Gateway GCP virtual machine image: <https://pulsezta.blob.core.windows.net/gateway/ISA-V-GCP-ZTA-22.3R4-883.1.tar.gz>

---

**Note:** Download a copy of the GCP Gateway image as a compressed TAR archive file, then decompress the archive to a local workstation. Make sure that the resulting file set is accessible from the Google Cloud Platform Console.

---

---

**Note:** You can also choose to download the Gateway image through the **Gateways Overview** page of the Tenant Admin Portal after you have defined the Gateway record. The opportunity to do this occurs later in this process.

---

- (Optional) GCP Gateway YAML templates, suitable for automating the creation of your GCP VM instances. Choose from:
  - To deploy in an existing VPC: <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-2-nics-existing-vpc.zip>  
<https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-3-nics-existing-vpc.zip>
  - To deploy in a new VPC: <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-2-nics-new-vpc.zip>  
<https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-3-nics-new-vpc.zip>

---

**Note:** You can also choose to download Gateway templates through the **Gateways Overview** page of the Tenant Admin Portal after you have defined the Gateway record. The opportunity to do this occurs later in this process.

---

- Credentials for the Google Cloud Platform Console.

---

**Note:** These credentials must include sufficient permissions to create a virtual machine from a template image.

---

After you have all required information, you can set up a nZTA GCP gateway, see [Adding a GCP Gateway in nSA](#) (page 87).

## Adding a GCP Gateway in nSA

To set up a nZTA GCP Gateway, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:
  - On unconfigured nZTA systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
  - On configured nZTA systems, the **Overview of Network** page appears. In this case:

- From the nZTA menu, click the **Secure Access** icon, then select **Gateways > Gateway List**.

The *Gateways List* page appears, showing the full list of Gateway Groups and standalone Gateways currently configured on the Controller.

- To add a new Gateway, select **Create** from the top-right:

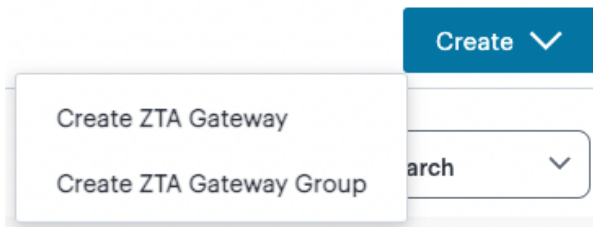


FIGURE 3.26 : Add a new Gateway or Gateway Group

- In the drop-down menu, click **Create ZTA Gateway**.

In both cases, the **Gateway Network Configuration** dialog appears.

FIGURE 3.27 : Gateway Network Configuration

---

**Note:** To learn more about the settings on this page, see the *Tenant Admin Guide*.

---

2. For **Gateway Platform**, select “Google Cloud Platform”.
3. Enter a **Name** for the Gateway.
4. Enter one or more **Public Address or CNAME** (Public IP address or CNAME) for the Gateway. Select **Add** to add each entry to the list.

---

**Note:** If you want Google Cloud Platform to allocate a public IP address automatically, you can use a dummy IP address (for example, 1.1.1.1) at this point. You must then update the Controller with the allocated public IP address after the GCP VM instance is created.

---

5. Select a geographic **Location** for the Gateway.
6. (Optional) Select a Gateway **Group** to which the new Gateway is to be added.

---

**Note:** A Gateway Group may have a defined public IP address, which you can specify as the **Public Address**, see above.

---

7. (Optional) Select the **Use Management Port** check box to use management network ports for nZTA traffic rather than internal ports.

---

**Note:** When the management port is enabled, the Controller will still use the internal port for DNS resolution. If the internal DNS cannot resolve the Controller domain, the internal interface will require internet access.

---

8. Enter the Primary DNS IP address for the Gateway.
9. (Optional) Enter the Secondary DNS IP address for the Gateway.
10. Enter the DNS Search Domain for the Gateway.

---

**Note:** Make sure the specified DNS service can resolve the IP address of your Controller. Issues here can cause registration of the Gateway with the Controller to fail.

---

11. To add a Gateway definition based on the settings you specified in this dialog, select **Create Configuration**.

By completing the **Gateway Network Configuration** workflow, an unregistered Gateway record is created on the Controller. You can view this Gateway record on the **Gateways > Gateways List** page.

You can now download your metadata, see [Downloading Metadata for Google Cloud Platform](#) (page 90).

## Downloading Metadata for Google Cloud Platform

The preparation of metadata for use on Google Cloud Platform currently requires some manual steps:

1. Log into nZTA and access the **Gateways > Gateways List** page.
2. Select your GCP Gateway and click the **Download** icon to obtain a copy of the Gateway definition file.

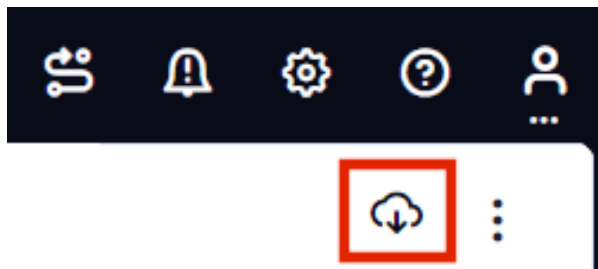


FIGURE 3.28 : The Download Icon

3. Specify a save location for your Gateway definition file.

---

**Note:** The Gateway definition file is valid for 24 hours. If this period expires, you must replace the Gateway to generate a new Gateway definition file.#

---

4. (Optional) If you have not yet downloaded the latest version of your Gateway VM image and optional YAML templates, click the **Download** icon and select **Download gateway VM image**. Save the archive file and unpack to a local workstation. Make sure the resulting file set is accessible from the Google Cloud Platform Management Portal.

You can now create a GCP gateway VM in Google Cloud Platform, see [Uploading the GCP Virtual Machine Image onto the Google Cloud Platform](#) (page 90).

## Uploading the GCP Virtual Machine Image onto the Google Cloud Platform

To upload a GCP Gateway virtual machine image into Google Cloud Platform:

1. Access the *Google Cloud Platform Management Portal*, either from a client or a web browser, and log in using your Google Cloud Platform credentials.
2. In the Google Cloud Platform console, select your required project from the pull-down list on the title bar. For example:

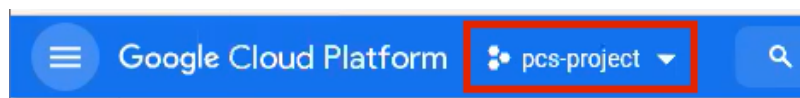


FIGURE 3.29 : GCP Select Project

3. Click the **Navigation** menu, and then select **Cloud Storage > Browser**.  
A list of GCP storage buckets appears.
4. Select the bucket into which you wish to place the GCP image.  
A page listing the current contents of the bucket appears.
5. (Optional) Navigate to the required folder within the bucket.
6. Click **Upload Files**. For example:

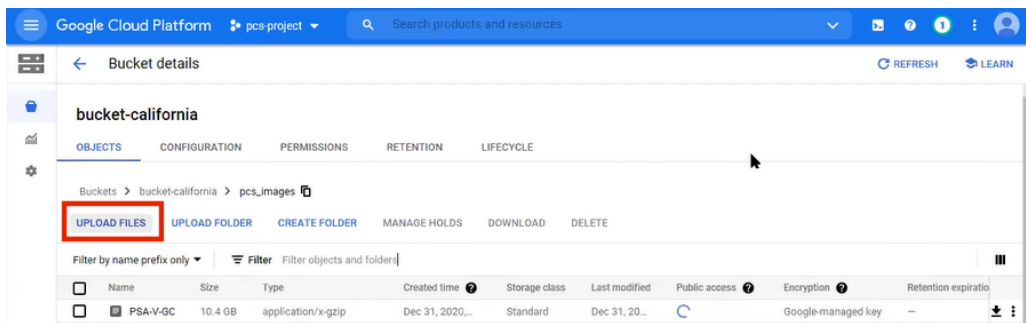


FIGURE 3.30 : GCP Upload Files

An upload dialog appears.

7. Select the .tar image file archive downloaded from <https://pulsezta.blob.core.windows.net/gateway/ISA-V-GCP-ZTA-22.3R4-883.1.tar.gz>, and click **Open**.

---

**Note:** If you want to use the provided YAML templates to automate the creation of your VM instance (see *Creating a VM Instance of the Uploaded GCP Image Using a Script/Template* (page 97)), select these in addition to the image archive.

---

The image archive and any selected template files are added to the bucket.

8. Wait until the upload completes. This may take several minutes.
9. Start a command line session from the title bar. For example:

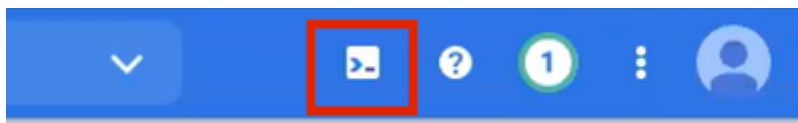


FIGURE 3.31 : GCP Upload Files

A command line session starts.

10. Navigate to the project folder.
11. Create an image from the ZTA Gateway image archive using the following command:

```
gcloud compute images create <instance_name> --source-uri=gs://
↪<bucket_name>/<optional_path>/<image_name>.tar --guest-os-
↪features MULTI_IP_SUBNET
```

For example:

```
gcloud compute images create ztagcp152 --source-uri=gs://bucket-
↪california/pcs_images/PSA-V-GCP-ZTA-153.1-SERIAL-gcp.tar --guest-
↪os-features MULTI_IP_SUBNET
```

You can now create a VM instance of the uploaded GCP image. To do this, either:

- Perform the task manually, see [Creating a VM Instance of the Uploaded GCP Image Manually](#) (page 92).
- Perform the task with a script/template, see [Creating a VM Instance of the Uploaded GCP Image Using a Script/Template](#) (page 97).

## Creating a VM Instance of the Uploaded GCP Image Manually

This section describes how to manually create a virtual machine instance of the ZTA Gateway image inside Google Cloud Platform. You can also perform this process automatically using a script/template, see [Creating a VM Instance of the Uploaded GCP Image Using a Script/Template](#) (page 97).

1. Click the **Navigation** menu, and then select **Compute Engine > Images**.

The **Images** page appears. For example:

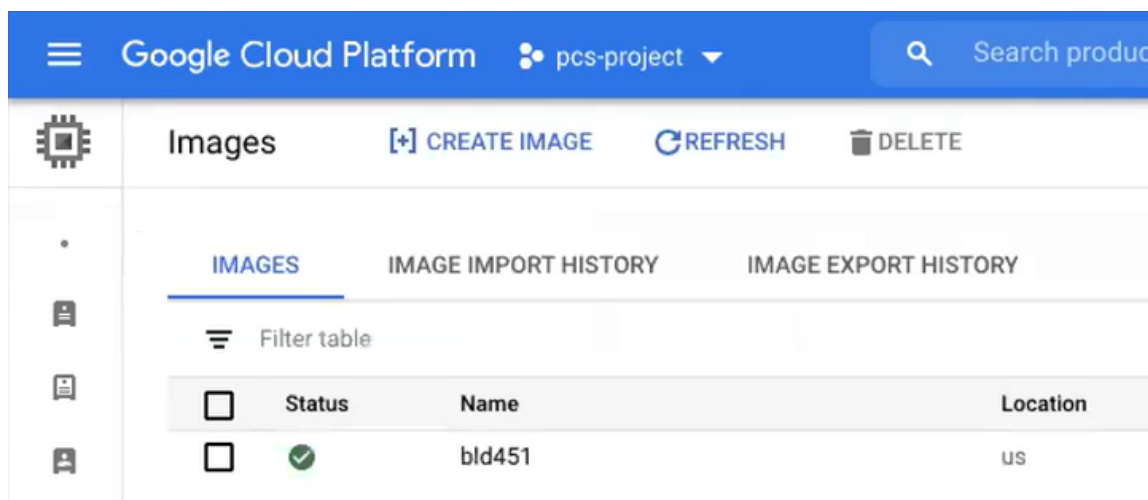


FIGURE 3.32 : GCP Images Page

2. Locate the new image in the list of images.
3. At the end of the image entry, click the action menu and select **Create Instance**.

The **Create Instance** page appears. For example:



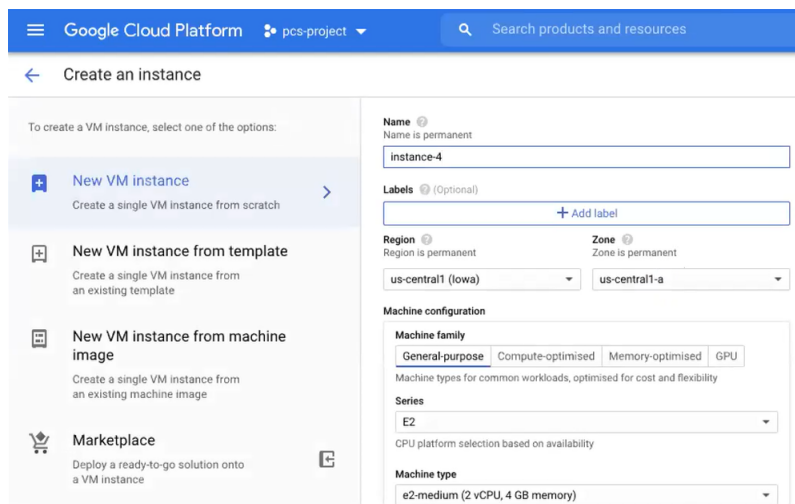


FIGURE 3.33 : GCP Create Instance

4. On the **Create Instance** page:

- Enter a **Name** for the new instance.
- Select a **Region** and **Zone**.
- Under **Machine configuration**:
  - For **Series**, select *N1*.
  - For **Machine Type**, select a minimum of *n1-standard-2*.
  - For **Boot Disk**, confirm that the correct image is already selected.
  - For **Firewall**, select the required HTTP/HTTPS options.
- Expand the **Management, security, disks, networking, sole tenancy** options.
- Select the **Management** tab.
- Under **Metadata**:
  - For **Key**, enter *pulse-config*.
  - For **Value**, paste the text of the metadata file you downloaded earlier.
- Select the **Networking** tab.
- Under **Network interfaces**, click the **Edit** icon to change the default network interface selection.

The **Network interface** options appear.

- Under **Network interface**, specify a *private* (internal) network interface:
  - For **Network**, select the required private VPC.
  - For **Subnetwork**, select the required subnetwork.
  - Click **Done** to confirm the settings for the private network interface.

- Under **Network interfaces**, click **Add network interface**.  
The **Network interface** options appear.
- Under **Network interface**, specify a *public* (external) network interface:
  - For **Network**, select the required public VPC.
  - For **Subnetwork**, select the required subnetwork.
  - Click **Done** to confirm the settings for the public network interface.
- (Optional) Click **Add network interface** and specify a management network interface.
- Click **Create** to confirm the settings and instantiate a VM instance of the image.  
The **VM Instances** page appears. This page shows the new VM instance of the image. For example:

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
vm-skupgrade153	asia-south1-b			10.200. (nic0)	None	SSH
	us-central1-a			10.128. (nic0)	None	SSH
	us-west2-a			10.100. (nic0)	None	SSH

FIGURE 3.34 : GCP Create Instance

5. On the **VM Instances** page, wait until the creation of the VM instance completes. This may take several minutes.
6. After the VM instance is created, click on it in the list of VM instances.  
The **VM instance details** page appears for the instance.
7. Confirm the details for the VM instance, including the number of network interfaces.
8. Make a note of the public IP address of the EXT interface (typically, this is *nic1*. This is required inside nZTA.
9. Under **Network interfaces**, confirm that the firewall settings from your VPCs are present for your specified network interfaces:
  - Click *nic0*. A summary page for this network interface appears.  
Under **Firewall and route details**, click the **Firewall Rules** tab and confirm that the following firewall rules are defined.

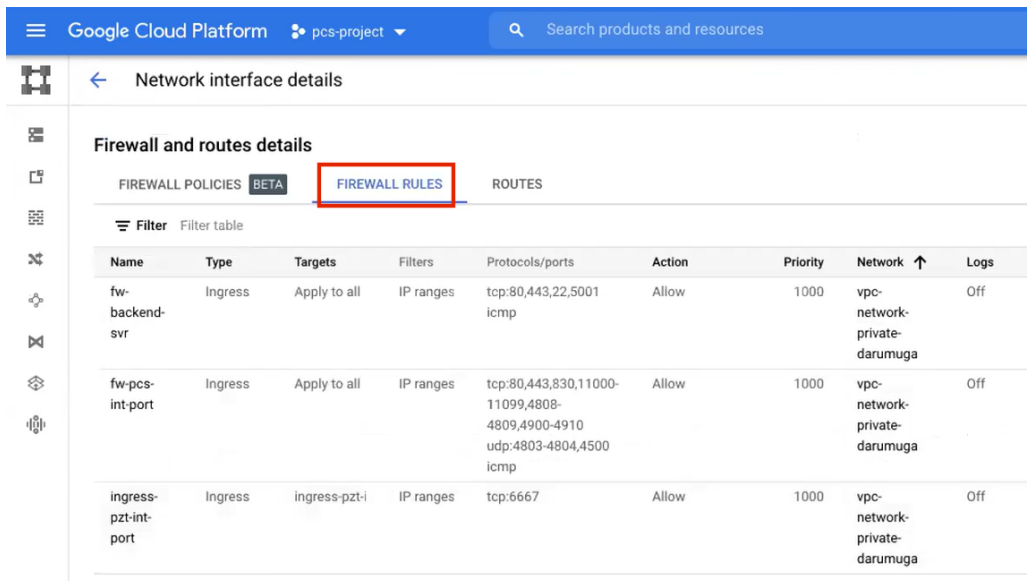


FIGURE 3.35 : NIC0 Firewall Rules

- Click *nic1*. A summary page for this network interface appears. Under **Firewall and route details**, click the **Firewall Rules** tab and confirm that the following firewall rules are defined.

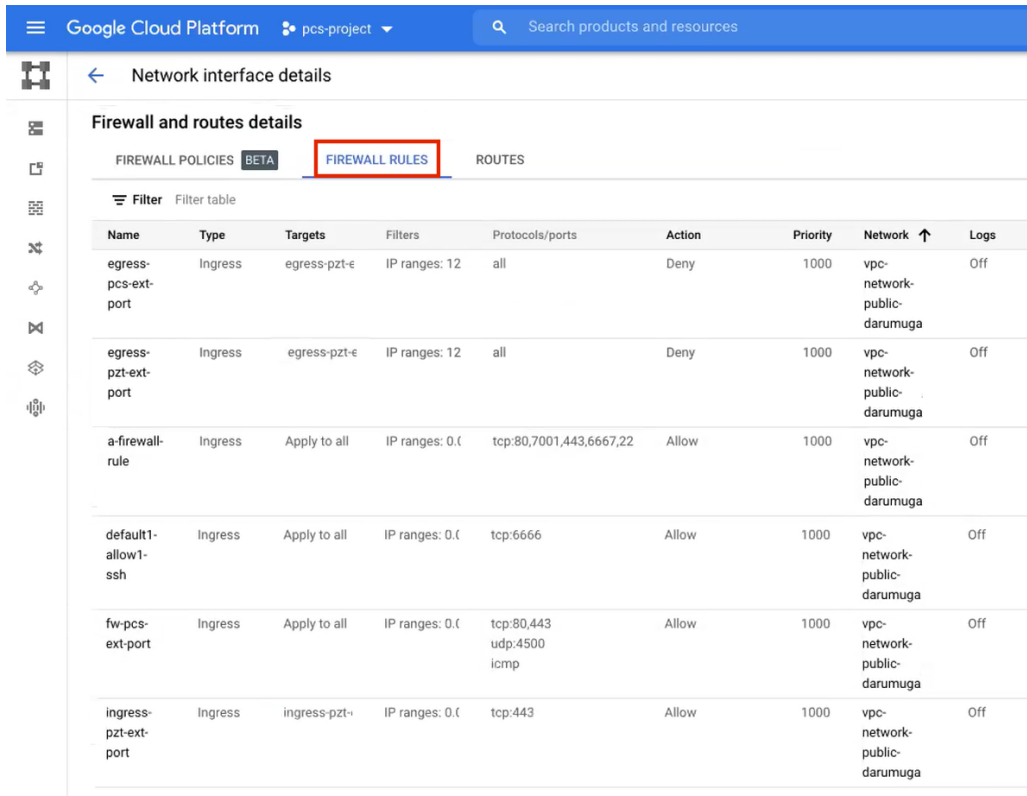
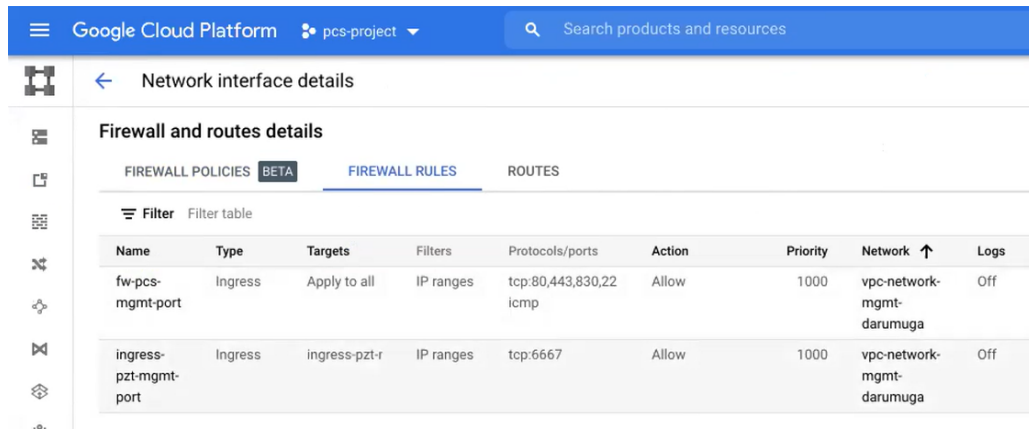


FIGURE 3.36 : NIC1 Firewall Rules

- (Optional) Click *nic2*. A summary page for this optional network interface

appears.

Under **Firewall and route details**, click the **Firewall Rules** tab and confirm that the following firewall rules are defined.



The screenshot shows the Google Cloud Platform interface for Firewall Rules. The 'FIREWALL RULES' tab is selected. A table lists the following rules:

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network	Logs
fw-pcs-mgmt-port	Ingress	Apply to all	IP ranges	tcp:80,443,830,22 icmp	Allow	1000	vpc-network-mgmt-darumuga	Off
ingress-pzt-mgmt-port	Ingress	ingress-pzt-r	IP ranges	tcp:6667	Allow	1000	vpc-network-mgmt-darumuga	Off

FIGURE 3.37 : NIC2 Firewall Rules

10. The *VM instance details\** page, click **Connect to serial console**

A console monitor view (in a separate browser tab) shows the ongoing boot-up process for the instance.

11. Wait until the instance boot up is complete, and shows a screen similar to the following:

```

Welcome to the Pulse Zero Trust Access Serial Console!

Current version: 21.2R1 (build 153)
Rollback version: 21.2R1 (build 107)
Reset version: 21.2R1 (build 107)

Licensing Hardware ID: VASPH80EQ02HBPTES

Please choose from among the following options:
 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log/status
 4. System Operations
 5. Toggle password protection for the console (Off)
 6. Create a Super Admin session.
 7. System Maintenance
 8. Reset allowed encryption strength for SSL
Choice:

```

FIGURE 3.38 : GCP Instance Console Monitor

You can then complete this process by updating the Gateway details on the Controller, see [Completing the Configuration of the Controller](#) (page 99).

## Creating a VM Instance of the Uploaded GCP Image Using a Script/Template

This section describes how to automatically create a virtual machine instance of the ZTA Gateway image inside Google Cloud Platform using a script/template. You can also perform this process manually, see [Creating a VM Instance of the Uploaded GCP Image Manually](#) (page 92).

Ivanti provides YAML-based templates to create an instance of the ZTA Gateway image in the following configurations:

- Two network interfaces in an *existing* VPC.
- Three network interfaces in an *existing* VPC.

Download: <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-2-nics-existing-vpc.zip>  
<https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-3-nics-existing-vpc.zip>

- Two network interfaces in a *new* VPC.
- Three network interfaces in a *new* VPC.

Download: <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-2-nics-new-vpc.zip> <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-2-883/ivanti-zta-3-nics-new-vpc.zip>

---

**Note:** You can obtain these templates through the links given here, or as part of the archive file set provided through the *Download* link on the **Gateways Overview** page in the Tenant Admin Portal after you have defined a Gateway record.

---

To use a template:

1. Download the required template archive file to your local workstation.
2. Unpack the downloaded archive file to a location that is accessible from Google Cloud Platform. Each archive contains three files. For example, for the two-interface (existing VPC) version of the archive:

```
pulsesecure-zta-2nics-existing-vpc.jinja
pulsesecure-zta-2nics-existing-vpc.jinja.scheme
pulsesecure-zta-2nics-existing-vpc.yaml
```

3. Edit the YAML file `properties` section to reflect your project and instance requirements, including the `user_data` property.

An example of an *existing* VPC YAML file is provided here:

```
imports:
  - path: pulsesecure-zta-2-nics-existing-vpc.jinja
resources:
  - name: my-vm
    properties:
      project: zta-gw-263035
```

(continues on next page)

(continued from previous page)

```
email: admin@example.com
region: asia-south1
zone: asia-south1-b
image: ztagcp123
machine_type: n1-standard-2
int_network:
ext_network:
int_subnetwork:
ext_subnetwork:
user_data:
type: pulsesecure-zta-2-nics-existing-vpc.jinja
```

An example of a *new VPC* YAML file is provided here:

```
imports:
  - path: pulsesecure-zta-2-nics-new-vpc.jinja
resources:
  - name: my-vm
    properties:
      deploy_with_lb: yes
      project: zta-gw-263035
      email: admin@example.com
      region: asia-south1
      zone: asia-south1-b
      image: ztagcp123
      machine_type: n1-standard-2
      user_data: <pulse-config><primary-dns>8.8.8.8<\primary-
↪dns> ...
      int_cidr: 192.0.2.0/24
      ext_cidr: 192.0.2.0/24
      type: pulsesecure-zta-2-nics-new-vpc.jinja
```

---

**Note:** Where you are specifying a new VPC for your virtual machine instance, make sure you use properties (for example, networking settings) that do not conflict with an existing VPC.

---

1. Save the YAML file.
2. On the Google Cloud Platform, start a command line session from the title bar. For example:



FIGURE 3.39 : GCP Upload Files

A command line session starts.

3. Select the required project:

```
gcloud config set project <project-name>
```

4. Within the project folder, create a *deploymentmanager* folder.
5. Copy the three script files to this folder.
6. Create a VM instance from the ZTA Gateway image archive file using the following command:

```
gcloud deployment-manager deployments create <vm-name> --config
↔<yaml_file>
```

For example:

```
gcloud deployment-manager deployments create vm-gcp-123 --config
↔pulsesecure-zta-3-nics-existing-vpc.yaml
```

7. Wait until the command completes.
8. On the **VM Instances** page, click on the new VM in the list of VM instances. The **VM instance details** page appears for the instance.
9. Confirm the details for the VM instance, including the number of network interfaces.
10. Make a note of the public IP address of the EXT interface (typically, this is *nic1*. This is required inside nZTA.

You can now complete this process by updating the Gateway details on the Controller, see [Completing the Configuration of the Controller](#) (page 99).

## Completing the Configuration of the Controller

If you specified a dummy public IP address (for example, *1.1.1.1*) when you created the Gateway on the Controller, you now need to update the Controller with the allocated public IP address for the Gateway VM instance on Google Cloud Platform.

---

**Note:** You do not need to perform the following procedure if you specified the correct public IP address when you created the Gateway on the Controller, see [Adding a GCP Gateway in nSA](#) (page 87).

---

1. Return to the **Gateways List** page in the nZTA Tenant Admin Portal.

2. Locate the new Gateway record in the list and confirm that its status has updated to *Connected*.
3. Select the Gateway, and then select **Secure Access > Gateways > Configuration**.
4. Under **Gateway Network Settings**, delete the current public IP setting and replace it with the public IP address if the nic1 (external) interface for the VM instance.

---

**Note:** After you have registered a Gateway, you can configure it (or the Gateway Group to which it belongs) as the default Gateway if required. See the *Tenant Admin Guide* for details.

---

## Next Steps

After you have defined your user authentication policies, move on to create your device policies. See [Creating Device Policies and Device Rules](#) (page 101).



# Creating Device Policies and Device Rules

- [Introduction](#) (page 101)
  - [Creating Device Rules](#) (page 103)
  - [Creating Device Policies](#) (page 116)
  - [Next Steps](#) (page 119)
- 

## Introduction

**Device Policies** define the minimum standard a device must meet to be considered compliant with Ivanti Neurons for Zero Trust Access (nZTA). Device Policies are used when defining a nZTA **Secure Access Policy** for an application.

You create one or more **Device Rules** and then group them together to form a complete **Device Policy**.

## Device Policy

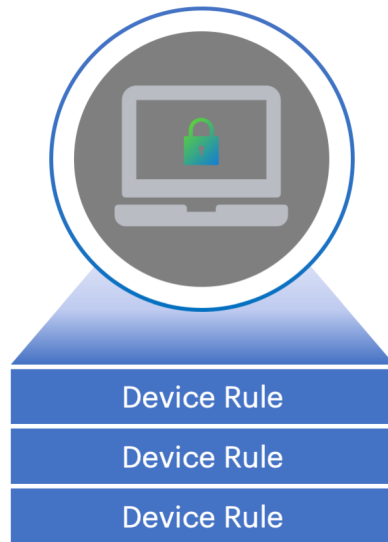


FIGURE 4.1 : Grouping device rules to create a device policy

Rules are created as one of the following types:

- *Antispyware*: Checks compliance to designated anti-spyware requirements.
- *Antivirus*: Checks compliance to designated anti-virus requirements.
- *Command*: Runs a command on the client device to check against an expected value (macOS client devices only).
- *CVE check*: Checks for protection against a list of publicly disclosed Common Vulnerability and Exposure (CVE) notices (Windows client devices only).
- *File*: Checks for the existence of a known file on the client.
- *Firewall*: Checks compliance to designated firewall requirements.
- *Hard Disk Encryption*: If encryption software is installed on the client device, this rule type checks the device's hard disks for applied encryption.
- *Location*: Checks the client device's geographic location matches, or avoids, a list of defined locations.
- *Mac Address*: Checks the client device's MAC address.
- *Netbios*: Checks the client device's Netbios domain name.
- *Network*: Checks the client device complies with a defined IP address and netmask range.
- *OS*: Checks the client device's Operating System meets a defined minimum standard.
- *Process*: Checks for the existence of a known process on the client.
- *Port*: Checks the client device's network interface ports.
- *Patch Management*: If patch management software is installed on a client device, this rule type checks for the existence of missing software patches.

- *Registry*: Checks for a value in a registry key (Windows client devices only).
- *Risk Sense*: Supports Allow access, Block access and Notify based on the risk level.
- *System Integrity*: Checks the system integrity of the client device (macOS client devices only).
- *Time of day*: Checks resource access requests against compliance with a time-based access schedule.

---

**Note:** Restrictions exist for rule type availability on the following Ivanti Secure Access Client platform variants:

- Android clients are limited to rules based on *jail\_break\_root* and OS.
  - iOS clients are limited to rules based on *jail\_break\_root*, OS, and *Time of day*.
  - Linux clients are limited to rules based on *File*, *Port*, and *Process*.
- 

nZTA includes a number of built-in device rules and policies relating to antivirus software, suitable for general use. To learn more, see the *Tenant Admin Guide*.

## Creating Device Rules

Before you begin, decide what kind of rule you want to create. For each rule type, make sure you have the supporting parameters. For example, if you are creating a *Network* rule, make sure you know the IP address and netmask range you want to apply. To learn more, see [Introduction](#) (page 101).

To create a device rule:

1. Log into the Controller as a Tenant Admin.
2. From the nZTA menu, select the **Secure Access** icon, then select **Manage Devices > Device Rules**.

The *Device Rules* page appears. This page lists all device rules.

<input type="checkbox"/>	RULE TITLE ↑	DEFAULT ↑	RULE TYPE ↑	SECURITY LEVEL ↑	ATTRIBUTES
<input type="checkbox"/>	> Android-Rule		os		Platform: android, Comparator: above, Vers...
<input type="checkbox"/>	> AndroidRootRule	✓	jail_break_root	high	Description: Checks whether android device...
<input type="checkbox"/>	> custom_tod		date_time		Mode: deny, Start Time: 03:00:00 End Time...
<input type="checkbox"/>	> cve		cve_check		Platform: windows, CVE Check all: true,
<input type="checkbox"/>	> India_allow		location		Location: India => Mode: allow, Descriptio...
<input type="checkbox"/>	> India_Bangalore-allow		location		Location: Bengaluru(India, Karnataka) => M...
<input type="checkbox"/>	> India_bangalore-Deny		location		Location: Bengaluru(India, Karnataka) => M...
<input type="checkbox"/>	> India_deny		location		Location: India => Mode: deny, Descriptio...
<input type="checkbox"/>	> iOS-Rule		os		Platform: ios, Comparator: above, Version:...
<input type="checkbox"/>	> IOSJailBreakRule	✓	jail_break_root	high	Description: Checks whether ios device is ...
<input type="checkbox"/>	> linux-Ajay-client		file		Mode: allow, File Name: /home/qa1/file1.tx...
<input type="checkbox"/>	> Linux_file_allow		file		Mode: allow, File Name: /home/subham/requi...

FIGURE 4.2 : Device Rules Page

3. Click **Create** and then select **Create Device Rules**.

The **Add Device Policy Rules** form appears.

**Add Device Policy Rules**

View Device Rules Reset fields

RULE TYPE  
Network

RULE NAME

Rule Details

RULE DESCRIPTION

IP ADDRESS NETMASK

MODE  
Choose your option

Cancel Add

FIGURE 4.3 : Add a Device Rule

**Note:** At any point during this process, you can reset the form data by selecting **Reset Fields**. You can also view existing device rules in a pop-up dialog by selecting **View Device Rules**.

4. Select **Rule Type** and select one of the following options:

- *Antispyware*
- *Antivirus*
- *Command*
- *CVE check*

- *File*
- *Firewall*
- *Hard Disk Encryption*
- *Location*
- *Mac Address*
- *Netbios*
- *Network*
- *OS*
- *Process*
- *Port*
- *Patch Management*
- *Registry*
- *Risk Sense*
- *System Integrity*
- *Time of day*

5. Enter a **Rule Name** for your device rule.

6. (Optional) Enter a **Rule Description** for your device rule.

7. The remaining options are dependent on the **Rule Type** you selected:

For *Antispyware* and *Firewall* rules, see [Options for Antispyware and Firewall Rules](#) (page 106).

For *Antivirus* rules, see [Options for Antivirus Rules](#) (page 107).

For *Command* rules, see [Options for Command Rules](#) (page 108).

For *CVE check* rules, see [Options for CVE Check Rules](#) (page 108).

For *File* rules, see [Options for File Rules](#) (page 108).

For *Hard Disk Encryption* rules, see [Options for Hard Disk Encryption Rules](#) (page 109).

For *Location* rules, see [Options for Location Rules](#) (page 109).

For *Mac Address* rules, see [Options for MAC Address Rules](#) (page 110).

For *Netbios* rules, see [Options for Netbios Rules](#) (page 110).

For *Network* rules, see [Options for Network Rules](#) (page 110).

For *OS* rules, see [Options for OS Rules](#) (page 111).

For *Process* rules, see [Options for Process Rules](#) (page 111).

For *Port* rules, see [Options for Port Rules](#) (page 112).

For *Patch Management* rules, see [Options for Patch Management Rules](#) (page 112).

For *Registry* rules, see [Options for Registry Rules](#) (page 113).

For *Risk Sense* rules, see [Options for Risk Sense Rules](#) (page 114).

For *System Integrity* rules, see [Options for System Integrity Rules](#) (page 115).

For *Time of day* rules, see [Options for Time of Day Rules](#) (page 115).

8. Select **Add** to create the device rule.

The new rule is added to the list of device rules.

Individual device rules cannot be referenced by a *secure access policy*. After you have created all required rules, you must organize them into **device policies**, see [Creating Device Policies](#) (page 116).

## Options for Antispyware and Firewall Rules

1. Select **Platform** and select one of the following options:

- *windows*
- *mac*

Using the selected platform, nZTA populates the lists of *Vendors* and *Products* that can be selected for this rule.

2. (Optional) Select **Select Vendors** and use the drop-down list to select or deselect one or more product vendors. When done, select anywhere outside of the list.

Each selected vendor is added to the panel below the drop-down list. To remove a selection, select the corresponding **X** indicator.

3. (Optional) Select **Select Products** and use the drop-down list to select or deselect one or more products. When done, select anywhere outside of the list.

Each selected product is added to the panel below the drop-down list. To remove a selection, select the corresponding **X** indicator.

---

**Note:** While both *Vendor* and *Product* fields are optional, you must select at least one vendor or product for your rule.

---

4. (Optional) To set advanced options for this rule, select **Advanced Configuration**.

The following options are provided:

- Enable monitoring of this rule in Ivanti Secure Access Client.

## Options for Antivirus Rules

1. Select **Platform** and select one of the following options:

- *windows*
- *mac*

Using the selected platform, nZTA populates the lists of *Vendors* and *Products* that can be selected for this rule.

2. (Optional) Select **Select Vendors** and use the drop-down list to select or deselect one or more product vendors. When done, select anywhere outside of the list.

Each selected vendor is added to the panel below the drop-down list. To remove a selection, select the corresponding **X** indicator.

3. (Optional) Select **Select Products** and use the drop-down list to select or deselect one or more products. When done, select anywhere outside of the list.

Each selected product is added to the panel below the drop-down list. To remove a selection, select the corresponding **X** indicator.

---

**Note:** While both *Vendor* and *Product* fields are optional, you must select at least one vendor or product for your rule.

---

4. Select **Enforcement Level** and select one of the following options:

- *high*
- *moderate*
- *low*

5. (Optional) To set advanced options for this rule, select **Advanced Configuration**.

The following options are provided:

- Add a maximum allowed time limit since the last successful system scan, in days.
- Add a maximum allowed age limit for the most recent virus definition file update, either by number of available updates or by number of days.
- Enable monitoring of this rule in Ivanti Secure Access Client.

## Options for CVE Check Rules

---

**Note:** This rule type is applicable to Windows devices only.

---

1. Select one of the following options:
  - To check all supported CVEs, select **Require all supported CVE checks**.
  - To check a list of specific CVEs, select **Check for specific CVE**, then use the **Select CVE Checks** drop-down control to select or deselect CVEs to be included.

---

**Note:** To remove a selected CVE from the list, select the “X” button adjacent to the CVE tag.

---

## Options for Command Rules

---

**Note:** This rule type is applicable to macOS devices only.

---

In this release, Command Type is limited to “Defaults Read Command” only. This runs the `/usr/bin/defaults read` command on the client device.

1. Enter a value in **Argument1** to represent the path of the *Property List* file to read. For example, `/Applications/Utilities/Terminal.app/Contents/Info.plist`.
2. Enter a value in **Argument2** to represent the property key name. For example, `CFBundleShortVersionString`.
3. Enter one or more **Expected Values** to be returned by the command, as a comma-separated list. “\*” (wildcard) values are also accepted.

## Options for File Rules

---

**Note:** This rule type is applicable to Windows and macOS devices only.

---

1. Select **Platform** and select one of the following options:
  - *windows*
  - *mac*
  - *linux*
2. Enter a full file name and path in **File Name**. For example, “c:test.txt” or “/Users/exampleuser/Downloads/test.txt”.



3. Select **Checksum Type** and select one of the following options:
  - *md5*
  - *sha256*
4. Enter the **Checksum** value for the file.
5. Select **Mode** and select one of the following options:
  - *allow*. Select this to allow access where the file exists and is valid.
  - *deny*. Select this to deny access if the file does not exist or is invalid.

### Options for Location Rules

1. Select **Mode** and select one of the following options:
  - *allow*. Select this to enable access for devices identified as being present at one of the set locations in the rule.
  - *deny*. Select this to disallow access for devices identified as being present at one of the set locations in the rule.
2. Use the “Add a location” section to define one or more geographic locations to which the current **Mode** applies:
  - Select a **Country**, **State** (optional), and **City** (optional).
  - To add the location, select **Add**.
3. Repeat the above steps for each location you want to add to the rule. Multiple “allow” and “deny” locations are possible in a single rule, with each added location identified by a green (allow) or red (deny) tag in the list.

---

**Note:** To remove a location, select the “X” button adjacent to the location tag.

---

### Options for Hard Disk Encryption Rules

---

**Note:** This rule type is applicable to Windows and macOS devices only.

---

1. Select the device **Platform** to which this rule applies.
2. Select the **Vendors** and associated encryption **Products** you want this rule to check.
3. Choose which hard drives you want the rule to check:
  - To check all drives detected on the client device, select **All Drives**.
  - To check specific drives on the client device, select **Specific Drives**, then enter the drive identifiers required.
4. Select **Advanced Configuration** to provide additional rule configuration:

- (Specific drives only) To ensure the rule does not trigger a failure where one or more of the specified drives are not detected, select **Consider policy as passed if the drives are not detected**.
- To ensure the rule does not trigger a failure where detected drives are currently undergoing encryption, but are not yet fully encrypted, select **Consider policy as passed if the drive encryption is in progress**.

### Options for MAC Address Rules

1. Select **Platform** and select one of the following platform options:
  - *windows*
  - *mac*
2. Enter the **MAC address** as a comma-separated list (without spaces) of MAC addresses in the form HH:HH:HH:HH:HH:HH where the HH is a two-digit hexadecimal number. Duplicate MAC addresses are not supported.
3. Select **Mode** and select one of the following options:
  - *allow*. Select this to enable access from a listed MAC address.
  - *deny*. Select this to disallow access from a listed MAC address.

### Options for Netbios Rules

1. Select **Platform** and select one of the following platform options:
  - *windows*
  - *mac*
2. Enter the Netbios domain **Names** as a comma-separated list (without spaces) of domain names. Each name can be 15 characters. Duplicate names are not supported.
3. Select **Mode** and select one of the following options:
  - *allow*. Select this to enable access from a listed Netbios domain name.
  - *deny*. Select this to disallow access from a listed Netbios domain name.

### Options for Network Rules

1. Enter the **IP Address** and **Netmask** from which you want to either allow or deny access.
2. Select **Mode** and select one of the following options:
  - *allow*. Select this to enable access for the given IP address and netmask.
  - *deny*. Select this to disallow access for the given IP address and netmask.

## Options for OS Rules

1. Select **Platform** and select one of the following options:
  - *windows*
  - *mac*
  - *ios*
  - *android*
2. The remaining fields are dependent on your choice of **Platform**:
  - Where you selected a platform of *windows* or *mac*, select **OS Name** and select an Operating System edition. For example, "Windows 2008" or "macOS Mojave".  
  
Then, select **OS Version** and select the version number or service pack associated with that edition of the Operating System. For example, "SP2" or "10.14.3". To not enforce the version number, select "Ignore".
  - Where you selected a platform of *ios* or *android*, select **Equality** and select one of the following options pertaining to how you want to enforce Operating System versions numbers:
    - *above*
    - *below*
    - *equal*  
Then, select **OS Version** and select the version number you want to check against.

## Options for Process Rules

---

**Note:** This rule type is applicable to Windows and macOS devices only.

---

1. Select **Platform** and select one of the following options:
  - *windows*
  - *mac*
  - *linux*
2. Enter a **Process Name**. For example, "explorer.exe".
3. Select **Checksum Type** and select one of the following options:
  - *md5*
  - *sha256*
4. Enter the **Checksum** value for the process executable.
5. Select **Mode** and select one of the following options:

- *allow*. Select this to allow access where the process exists and is valid.
- *deny*. Select this to deny access if the process does not exist or is invalid.

## Options for Port Rules

1. Select **Platform** and select one of the following platform options:
  - *windows*
  - *mac*
  - *linux*
2. Enter the **Ports** as a comma-separated list (without spaces) of ports. Port ranges are supported. Duplicate ports are not supported.
3. Select **Mode** and select one of the following options:
  - *allow*. Select this to enable access from a listed port.
  - *deny*. Select this to disallow access from a listed port.

## Options for Patch Management Rules

---

**Note:** This rule type is applicable to Windows and macOS devices only.

---

1. Select the device **Platform** to which this rule applies.
2. Select the **Vendors** and associated patch management **Products** you want this rule to check the presence of.
3. (Optional) Select **Advanced Configuration** to view more options:
  - Choose the **Severity** levels of missing patches you want to check in this rule:
    - *Critical*
    - *Important*
    - *Moderate*
    - *Low*
    - *Unspecified/Unknown*

---

**Note:** For some products, the patch severity level might not be detectable. In this case, select *Unspecified/Unknown* to detect missing patches.

---

- Choose the **Category** types of missing patches you want to check in this rule:
  - *Security Update*

- *Rollup Update*
- *Critical Update*
- *Regular Update*
- *Driver Update*
- *Service Pack Update*
- *Unknown*

---

**Note:** For some products, the patch category might not be detectable. In this case, select *Unknown* to detect missing patches.

---

## Options for Registry Rules

---

**Note:** This rule type is applicable to Windows devices only.

---

1. Select **Rootkey** and select one of the following options:
  - *HKEY\_LOCAL\_MACHINE*
  - *HKEY\_USERS*
  - *HKEY\_CURRENT\_USER*
  - *HKEY\_CURRENT\_CONFIG*
  - *HKEY\_CLASSES\_ROOT*
2. Enter a **Subkey** for the registry path.
3. Select **Key Type** and select one of the following key types:
  - *string*
  - *dword*
  - *binary*
4. Enter a **Key** name.
5. Enter a **Value** for the registry key.
6. Tick the **64-bit** checkbox to use the 64-bit registry store. Leave this checkbox unticked to use the 32-bit registry store.

The following example values would create a rule to ensure the client device contained a registry key `HKEY_LOCAL_MACHINE\SOFTWARE\pzt a` with a value 123:

Field	Value
Rootkey	HKEY_LOCAL_MACHINE
Subkey	SOFTWARE
Key Type	string
Key	zta
Value	123
64-bit	<i>ticked</i>

### Options for Risk Sense Rules

RiskSense provides vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk based scoring, analytics to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness.

Integrating RiskSense's Vulnerability Risk Rating (VRR) scores with nZTA provides an additional layer of security by isolating and preventing vulnerable devices from connecting to the ZTA network thereby protecting enterprise resources.

---

**Note:** This rule type is applicable to Windows only.

---

1. Enter the **Rule Name**.
2. Enter the **Rule Details**.
3. Select **Risk Level** and select one of the following options:
  - Low
  - Medium
  - High
  - Critical
4. Select **Action** and select one of the following options:
  - Allow: Select this to allow access when the risk level is low or medium.
  - Block: Select this to block the access based on the risk level.
  - Notify: Select this to notify the user about the risk identified.

## Options for System Integrity Rules

---

**Note:** This rule type is applicable to macOS devices only.

---

1. To enable this rule type, select **Enable**.

## Options for Time of Day Rules

This rule type applies a resource restriction (allow or deny access) based upon a specified period frequency within a defined date and time range. Enter the following parameters:

1. Select the frequency with which you want the rule to apply inside the date range you specify:
  - **Custom:** Apply the rule for the whole period continuously between the start date/time and end date/time.
  - **Daily:** Apply the rule for the specified days in each month. Enter a comma-separated list of numerical days (1-31), for example: "1,5,19,28".
  - **Weekly:** Apply the rule for the specified days of each week. For **Select Days**, select the checkbox for each day on which you want the rule to apply.
  - **Monthly:** Apply the rule for all days in the specified months. For **Month**, select one or more months from the drop-down list.
2. Enter the **Start Date** and **End Date** to apply to the selected period frequency. For custom rules, the date range entered here is continuous. For daily, weekly, and monthly rules, each day in the range is executed individually according to the selected times and frequency.

---

**Note:** Start and end date values are optional for **Daily**, **Weekly**, and **Monthly** frequencies. If not specified, the rule applies indefinitely.

---

3. Enter the **Start Time** and **End Time** to apply to the selected period frequency. For custom rules, the times are applied with the corresponding start and end date to provide a continuous period within which the rule applies. For daily, weekly, and monthly rules, the times are applied for each day in the schedule.

---

**Note:** All times are applied as UTC timezone values. Your ZTA Gateways must also use UTC time for the rule schedule to apply.

---

---

**Note:** Time periods for daily, weekly, and monthly rule frequencies are restricted to the 24 hours in a single day, such that you cannot enter an end time that is earlier than the start time. Therefore, in cases where you want to apply a rule allowing access for a time period that spans across midnight into

the next day, add separate rules for each day in the range covering the time period for that day only. For example, to allow access during the period 21:00 Monday until 12:00 Tuesday, configure the following rules:

Rule 1: **Period:** *weekly*, **Days:** *Monday*, **Start Time:** *21:00*, **End Time:** *23:59*, **Mode:** *allow*  
 Rule 2: **Period:** *weekly*, **Days:** *Tuesday*, **Start Time:** *00:00*, **End Time:** *11:59*, **Mode:** *allow*

4. Choose the **Mode** that should apply during the specified times:

- **allow:** Devices accessing resources to which this policy is applied are *authorized only* during the selected days and times.
- **deny:** Devices accessing resources to which this policy is applied are *not authorized* during the selected days and times.

## Creating Device Policies

You can create **Device policies** and attach to them one or more **Device Rules** as required. To learn more on creating device rules, see [Creating Device Rules](#) (page 103).

To create a device policy:

1. Log into the Controller as a Tenant Admin.
2. From the nZTA menu, select the **Secure Access** icon, then select **Manage Devices > Device Policies**.

The *Device Policies* page appears. This page lists all current device policies.

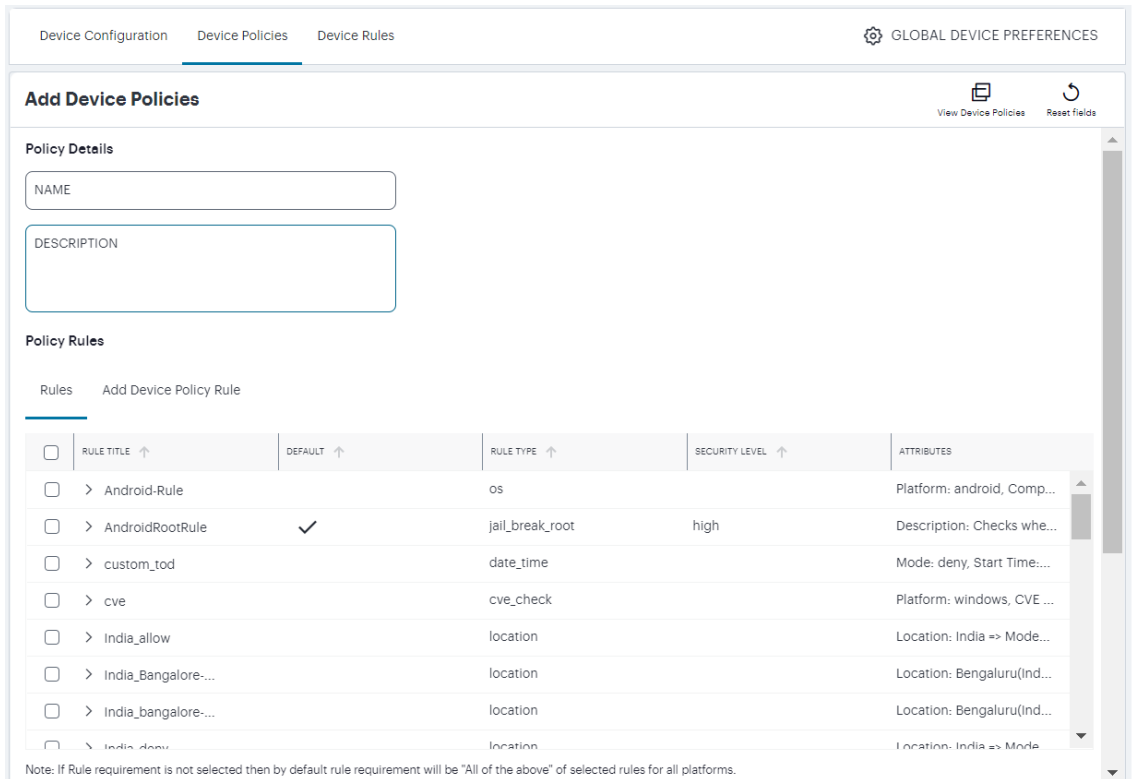
Manage Devices ⓘ			Create
Device Configuration		Device Policies	Device Rules
			GLOBAL DEVICE PREFERENCES
DEVICE POLICIES			EDIT
13 DEVICE POLICIES			DELETE
<input type="checkbox"/>	NAME ↑	DEFAULT ↑	DESCRIPTION
<input type="checkbox"/>	BlockIPRange		
<input type="checkbox"/>	Common-Device-Policy		Common-Device-Policy
<input type="checkbox"/>	McAfeeAVHigh	✓	McAfee AntiVirus Check (High)
<input type="checkbox"/>	McAfeeAVLow	✓	McAfee AntiVirus Check (Low)
<input type="checkbox"/>	McAfeeAVMedium	✓	McAfee AntiVirus Check (Medium)
<input type="checkbox"/>	RiskSenseCriticalNotify	✓	Risk Sense Critical Notification Device Po...
<input type="checkbox"/>	SymantecAVHigh	✓	Symantec AntiVirus Check (High)
<input type="checkbox"/>	SymantecAVLow	✓	Symantec AntiVirus Check (Low)
<input type="checkbox"/>	SymantecAVMedium	✓	Symantec AntiVirus Check (Medium)
<input type="checkbox"/>	TrendMicroAVHigh	✓	TrendMicro AntiVirus Check (High)
<input type="checkbox"/>	TrendMicroAVLow	✓	TrendMicro AntiVirus Check (Low)
<input type="checkbox"/>	TrendMicroAVMedium	✓	TrendMicro AntiVirus Check (Medium)

FIGURE 4.4 : Add a new Device Policy

3. Click **Create** and then select **Create Device Policy**.



A form appears to enable you to create the device policy.



Device Configuration    Device Policies    Device Rules    GLOBAL DEVICE PREFERENCES

**Add Device Policies**    View Device Policies    Reset Fields

**Policy Details**

NAME

DESCRIPTION

**Policy Rules**

Rules    Add Device Policy Rule

<input type="checkbox"/>	RULE TITLE ↑	DEFAULT ↑	RULE TYPE ↑	SECURITY LEVEL ↑	ATTRIBUTES
<input type="checkbox"/>	> Android-Rule		os		Platform: android, Comp...
<input type="checkbox"/>	> AndroidRootRule	✓	jail_break_root	high	Description: Checks whe...
<input type="checkbox"/>	> custom_tod		date_time		Mode: deny, Start Time:...
<input type="checkbox"/>	> cve		cve_check		Platform: windows, CVE ...
<input type="checkbox"/>	> India_allow		location		Location: India => Mode...
<input type="checkbox"/>	> India_Bangalore-...		location		Location: Bengaluru(Ind...
<input type="checkbox"/>	> India_bangalore-...		location		Location: Bengaluru(Ind...
<input type="checkbox"/>	> India_deny		location		Location: India => Mode...

Note: If Rule requirement is not selected then by default rule requirement will be "All of the above" of selected rules for all platforms.

FIGURE 4.5 : Add a new Device Policy

**Note:** At any point during this process, you can reset the form data by selecting **Reset Fields**. You can also view existing device policies in a pop-up dialog by selecting **View Device Policies**.

4. Enter a **Name** for the device policy.
5. Add a **Description** for the device policy.
6. Select each of the listed **Policy Rules** that are required in the device policy.
7. (Optional) In the *Rule Requirement* section: Specify for each end-user device **Platform** how you want to enforce your policy rules by choosing one of the following **Rule Requirement** options:
  - **All of the above rules:** The end-user device must comply with all rules defined in the policy.
  - **Any of the above rules:** The end-user device must comply with at least one of the defined rules in the policy.
  - **Custom:** The end-user device must comply with the conditions specified in a custom expression. Use the **Custom Expression** field to define an expression for the rules defined in this policy and how they should be evaluated. You can use the Boolean operators AND, OR and NOT, and also use parentheses to group or nest conditions.

The following is a list of sample custom expressions:

- *customExpr*
- (*customExpr*)
- *NOT customExpr*
- *customExpr OR customExpr*
- *customExpr AND customExpr*

As an example, where a policy has associated with it the rules "Rule1", "Rule2", and "Rule3", the following expression is valid: *Rule1 AND (NOT Rule2 OR (NOT Rule3))*

When using custom expressions, consider the following points:

- Using NOT: When using "*NOT expr*", the negated expression evaluates to true if the outcome of *expr* is false and evaluates to false if the outcome of *expr* is true.
- AND, OR, NOT precedence: These operators are evaluated from highest to lowest precedence in this order: NOT (from right), AND (from left), OR (from left).
- A combination of any device rule is allowed in an expression, except location, time of day, and network rules. For example, the following expressions are not allowed:
  - \* *Windows\_Process AND Locationrule*
  - \* *Windows\_Process AND Networkrule*
  - \* *Windows\_Process AND Time-of-Day\_Rule*

After you have set a platform and rule requirement, select **Apply** to add the entry. Then, repeat this procedure if you want to add any rule requirements for other device platforms.

---

**Note:** If you intend to add multiple rules of varying types to a device policy, be aware that individual rules might not by themselves guarantee allowed or denied access to an application depending on the outcome of other evaluated rules in a device policy, and the rule requirements settings configured here.

---

8. (Optional) To provide custom remediation instructions for the policy, tick **Enable Custom Instruction** and enter your remediation text into **Custom Instruction**. This option also requires selection of a target **Platform**.

These instructions are presented through Ivanti Secure Access Client when a device compliance check fails based on this policy.

---

**Note:** This feature is applicable to Windows, Mac, and Linux device policies only. Note also that custom instructions are restricted to a 500 byte limit and can contain only plain text or an HTML document with HREF links.

---

9. Select **Add**.

The new device policy appears in the list of **Device Policies**.

10. Repeat steps 3-7 to create all required device policies.

## Next Steps

After you have created your device policies, move on to define your applications. See [Creating Applications and Application Groups](#) (page 121).



# Creating Applications and Application Groups

- [Introduction](#) (page 121)
  - [Adding Applications to the Controller](#) (page 122)
  - [Adding Application Groups to the Controller](#) (page 125)
  - [Next Steps](#) (page 127)
- 

## Introduction

Application publishing is central to the configuration of your Ivanti Neurons for Zero Trust Access (nZTA) services.

A nZTA application definition can be created to refer to on-premise applications, web pages, or network locations served from your datacenter and cloud infrastructure. nZTA can also publish resources based on Software-as-a-Service (SaaS) applications such as Microsoft O365 and Salesforce.

You publish your application definitions to the Gateways that reside at the corresponding locations, and your Gateways ensure that access requests are authenticated and authorized according to the rules defined in your *Secure Access Policies* (see [Creating a Secure Access Policy](#) (page 129)).

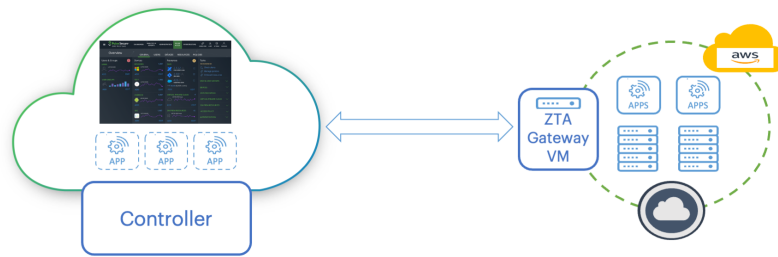


FIGURE 5.1 : Creating definitions for deployed apps you want to make available to your users

The Controller enables you to:

- Create definitions of applications to which your end users require access, see [Adding Applications to the Controller](#) (page 122).
- Group together multiple applications for which a single secure access policy is required, see [Adding Application Groups to the Controller](#) (page 125).

---

**Note:** An application, or application group, can be associated with only one secure access policy.

---

## Adding Applications to the Controller

Before you begin, make sure you have the following information:

- The name of your application
- A suitable description for your application
- The URL, FQDN, or IPv4 address you use to access the application.

To create an application definition:

1. Log into the Controller as a Tenant Admin.
2. From the nZTA menu, click the **Secure Access** icon, then select **Applications > Applications**.

The *Applications* page appears. This page lists all applications defined on the Controller.



5. Enter the **Application Details**. That is, the URL, FQDN or IPv4 address of the application you want to add.

---

**Note:** You can only access each application using the addressing method specified when registering it. That is, if you registered the app using an IP address, you cannot access it using its FQDN, even via DNS that resolves to the correct IP. Similarly, if you registered the app using an FQDN, you cannot access it using its IP address.

---

6. For scenarios that require one or more additional domains to be associated with an application, select **Add Allowed Domains**.

Then, add your domains through one of the following methods:

- Individually, by entering valid domains in the **Add Domain** text box, then selecting **Add** to add the domains to the list. You can add several domains at the same time by using a comma (,) separator. Repeat this step for each domain, or group of domains, you want to add.
- In bulk, by uploading a Comma-Separated Value (CSV) text file containing the full list of your domains.

Domains added to this list must conform to the same scheme rules as the URI used in the **Application Details** field. To view a complete list of valid domain schemes, see the *Tenant Admin Guide*.

In the list of added domains, remove individual entries by selecting the **X** indicator adjacent to the domain name. To remove all domains, select **Clear All**.

7. For HTTP/HTTPS applications, the **SAML Access** option appears:
  - Disable this setting if you are using an application-level login for the application.
  - Enable this setting if you are using SAML single sign-on for the application. Then:
    - Under **Download IdP Metadata**, click **Download** and save the IdP metadata file.
    - Log into the application and upload the IdP metadata file. Refer to the product documentation for the third-party application for details of this process.
    - In the application, download its SAML metadata as a file. Refer to the product documentation for the third-party application for details of this process.
    - Under **Upload SAML Metadata**, upload the SAML metadata file from the application.
8. (Optional) If you want to add custom SAML attributes, use **Attribute** and **Value** to add key-value pairs. Select **Add** to add an attribute pair, then repeat as required.



Added attributes are displayed beneath the input fields. Click the corresponding **X** indicator to remove an attribute.

9. To associate an icon with this application, either:
  - Select a **Application Icon** from the list of supported icons. This field auto-populates based on the scheme you use in **Application Details**.
  - Use **Upload Icon** to upload a bespoke image file as the icon for this application. Make sure your icon is in JPEG format using the maximum dimensions 48 x 48 pixels (maximum file size 1 MB). Ivanti recommends you use only square images for your application icons.
10. Enter a **Description** for the application.
11. (Optional) If you want a bookmark for this application, select the **Create bookmark for application** check box.
12. (Optional) If you want to enable application discovery, select the **Enable Application Discovery** check box.
13. (Optional) If you want to add the new application to an application group, select the **Add to Application Group** check box, and then select the required application group.

---

**Note:** When using SAML authentication, make sure you add to a single application group only those applications that use the same SAML authentication source.

---

14. Click **Create Application**.

The new application appears in the list of applications.

After you have defined your applications in the Controller, you can publish the definitions to your ZTA Gateway, see [Workflow: Creating a Secure Access Policy](#) (page 131).

## Adding Application Groups to the Controller

Multiple applications can be referenced from an *application group*.

When you select an application group during any subsequent process, all applications in the group are included automatically.

---

**Note:** For SAML authentication, make sure you add to a single application group only those applications that use the same SAML authentication source. A secure access policy can associate an application group with only one authentication method. Therefore, all applications added to the group must use the same SAML metadata for authentication.

---

To create an application group:

1. Log into the Controller as a Tenant Admin.
2. From the nZTA menu, click the **Secure Access** icon, then select **Applications > Application Groups**.

The *Applications Groups* page appears. This page lists all application groups defined on the Controller.

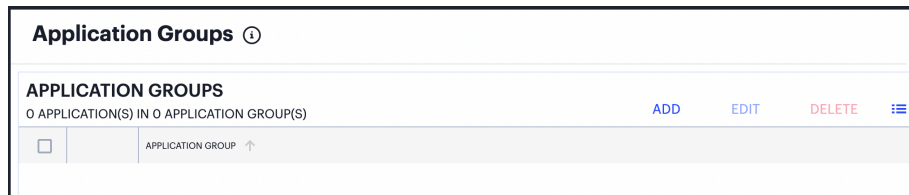


FIGURE 5.4 : Application Groups Page

3. Click **Add**.

The **Add Application Group** form appears.

Applications	NAME	TYPE	APPLICATION DETAIL	DESCRIPTION
<input type="checkbox"/>	Application Discovery	application	https://www.applicationdiscovery.com...	
<input type="checkbox"/>	Drivezy	application	https://www.drivezy.com	
<input type="checkbox"/>	flipkart	application	https://www.flipkart.com	
<input type="checkbox"/>	SBI	application	https://www.onlinesbi.c...	
<input type="checkbox"/>	shopclues	application	https://www.shopclues.c...	
<input type="checkbox"/>	sshapp	network	10.20.1.5	
<input type="checkbox"/>	tataaia	application	https://www.tataaia.com	
<input type="checkbox"/>	vogo	application	https://vogo.in/	

CANCEL CREATE

FIGURE 5.5 : Add an Application Group

---

**Note:** At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing application groups in a pop-up dialog by clicking **View Application Groups**.

---

4. Enter the **Group Name**.
5. Select the applications you want to include in the group.

---

**Note:** You cannot add the *Application discovery* application to a group.

---

6. Click **Create** to create the group.

The application group is added to the list.

## Next Steps

After you have created your application definitions on the Controller and deployed them to your cloud or datacenter locations, move on to create your Secure Access Policies. See [Creating a Secure Access Policy](#) (page 129).

---

**Note:** Before you create a Secure Access Policy, make sure you have created all required definitions for Gateways, Users, Devices, and Applications.

---



# Creating a Secure Access Policy

- [Introduction](#) (page 129)
  - [Workflow: Creating a Secure Access Policy](#) (page 131)
  - [Next Steps](#) (page 134)
- 

## Introduction

A *Secure Access Policy* is central to the configuration of your Ivanti Neurons for Zero Trust Access (nZTA) services.

The Controller enables you to create and publish complete Secure Access Policies to a ZTA Gateway. Each policy is based on four main components:

- **Applications:** The application (or application group) to which this policy applies.
- **User Rule Groups:** The user rule group you want to apply to access requests for this application.
- **Device Policies:** The device policy you want to apply to access requests for this application.
- **Gateways:** The ZTA Gateway governing access to the application, and to which this policy is to be published.

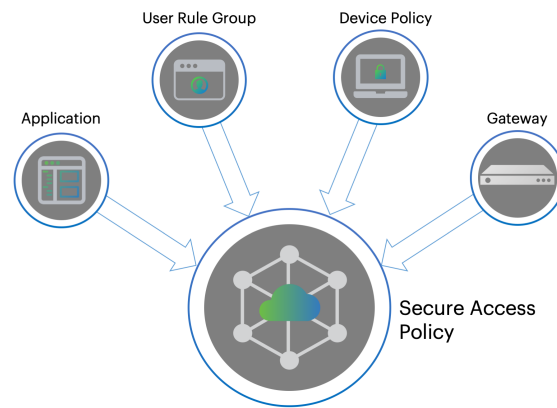


FIGURE 6.1 : Creating a secure access policy

**Note:** nZTA has one built-in secure access policy, *Application discovery*. This policy, when enabled and configured, directs any request from an application that is not referenced by a secure access policy to a *default Gateway*. See the *Tenant Admin Guide* for details.

Through this page, you can:

- Create a new secure access policy (see [Workflow: Creating a Secure Access Policy](#) (page 131)).
- Edit an existing secure access policy.
- Enable or disable a secure access policy. Use the checkboxes at the left to select the policies you want to enable/disable, then select the corresponding link at the top of the page.
- Delete a secure access policy. Use the checkboxes at the left to select the policies you want to delete, then select the **Delete** link at the top of the page.
- Perform Search term highlighting for occurrences of named applications, application groups, gateways, gateway groups, device policies, user groups and enabled status (yes/no) for the policies listed on this page.
- Filter the policies displayed on the page by application/application group, gateway, user, device policy, or status. When you select the *Filter* icon, a side panel dialog appears within which you can select specific criteria to filter the display to show only matching policies. Applied filters remain in place until you select **Clear All** from the side-panel, or until you leave the page.

To find more details about nZTA, including full descriptions of each feature, function and ability, see the *Tenant Admin Guide*.

## Workflow: Creating a Secure Access Policy

Before you begin creating your Secure Access Policy, make sure you have completed all tasks required in creating the policy components. Each chapter in this guide is dedicated to providing an overview of, and instructions in creating, each element.

To learn more about creating user rules, see [Creating User Authentication Services](#) (page 5).

To learn more about registering Gateways, see [Configuring Gateways](#) (page 43).

To learn more about creating device policies, see [Creating Device Policies and Device Rules](#) (page 101).

To learn more about defining applications, see [Creating Applications and Application Groups](#) (page 121).

To see an overview of nZTA, see [Getting Started with Ivanti Neurons for Zero Trust Access](#) (page 1).

After you have created all your application definitions, user authentication rules, device policies, and registered your Gateways, you can proceed to create a Secure Access Policy. Each policy publishes one or more applications with the associated users rules and device policies to the selected Gateway, ready for use by your organization's end-users.

To create a Secure Access Policy:

1. Log into the Controller as a Tenant Admin.
2. From the nZTA menu, select the **Secure Access** icon, then select **Secure Access Policies**.

The *Secure Access Policies* page appear. This lists all current secure access policies.

STATUS	APPLICATION / APPLICATION GROUP	GATEWAY / GATEWAY GROUP/ GATEWAY SELECTOR	USER GROUP	DEVICE POLICY	ENABLED
<input type="checkbox"/>	10.204.88.244_telnet	blackthorn-bng-2	sj group		on
<input type="checkbox"/>	10.96.75.63_rdp	blackthorn-bng-2	sj group	RiskSenseCriticalNot...	on
<input type="checkbox"/>	3liftWildcard	aws-blackthorn	sj group		on
<input type="checkbox"/>	54.159.47.183_ipv4	aws-blackthorn	sj group	notepad_reqd	on
<input type="checkbox"/>	ad.doubleclick.net_wik	blackthorn-debug	bng group		on
<input type="checkbox"/>	Adobe	blackthorn-bng-2	bng group	Time_Of_Day_Policy_B...	on
<input checked="" type="checkbox"/>	Adp	az-bkthrn-eastus	bng group	OnlyIP	on
<input type="checkbox"/>	Amazon	blackthorn-bng-2	bng group		on
<input type="checkbox"/>	Application discovery	blackthorn-bng-3	default group		on
<input type="checkbox"/>	Atlassian	blackthorn-bng-2	bng group	Antivirus	on
<input checked="" type="checkbox"/>	BambooHR	az-bkthrn-eastus	mac group		on
<input checked="" type="checkbox"/>	BIGIP-F5	blackthorn-bng-4	bng group	OnlyIP	on

FIGURE 6.2 : Viewing the list of existing Secure Access Policies

3. Click **Create**:

**Create Secure Access Policy**

Create Secure Access Policy  
 A Secure Access Policy defines how end users can connect to nSA to access applications.  
 To create a Secure Access Policy, user has to define Application/Application Group, Device Policy, User Group and Gateway/Gateway Group/Gateway Selector.  
 Optional Selection: Device Policy

1 Applications/Application Groups (dailymotion) | 2 Device Policies (actionable-insight) | 3 User Groups (accounts-auth) | 4 Gateways/Gateway Groups/Gateway Selectors (esxi-21-12r1-95) | 5 Summary

**APPLICATIONS AND APPLICATION GROUPS**  
 10 APPLICATIONS AND APPLICATION GROUPS

NAME	TYPE	APPLICATION DETAILS	APPLICATION GROUP
amazon	single	*.amazon.com	
Bamboo	single	https://dev.pulsesecure.net/bamboo	Onprem,OnPrem Apps
Confluence	single	https://dev.pulsesecure.net/confli...	Onprem,OnPrem Apps
<input checked="" type="radio"/> dailymotion	single	https://www.dailymotion.com	
Dropbox	single	https://www.dropbox.com/login	
Eng Portal	single	https://eng-portal.psecure.net/	Onprem,OnPrem Apps
Flipkart	single	*.flipkart.com	
G1	single	*.google.com	Google
G2	single	*.googleapis.com	Google
G3	single	*.googleusercontent.com	Google

Rows per page: 10

Navigation: << < 1 2 3 > >>

Buttons: Cancel, Next

FIGURE 6.3 : Creating a new Secure Access Policy



---

**Note:** At any point during this process, you can reset the form data by selecting **Reset**. You can also view existing secure access policies in a pop-up dialog by selecting **View Secure Access Policies**.

---

4. Select the application, or application group, for the policy. Click **Next**.

---

**Note:** An application, or application group, can be associated with only one secure access policy.

---

5. From the Device Policies list, select the device policy to apply to your Secure Access Policy. Click **Next**.
6. From the User Groups list, select the user group to apply to your Secure Access Policy. Click **Next**.
7. From the Gateways, Gateway Groups and Gateway Selectors list, select the ZTA Gateway/Gateway Group to which you want to publish your Secure Access Policy. Click **Next**.
8. Verify the Summary details and then click **Create**.  
The policy is created and added to the list of secure access policies.
9. (Optional) To edit a listed secure access policy, select the adjacent three dots and then select **Edit**. After the secure access policy is updated, it is automatically applied to the ZTA Gateway that it references.
10. (Optional) To enable a disabled secure access policy, use the toggle button. After the secure access policy is enabled, it is automatically applied to the ZTA Gateway that it references.
11. (Optional) To disable an enabled secure access policy, use the toggle button.
12. (Optional) To delete an *unused* secure access policy, select the adjacent three dots and then select **Delete**. Confirm the deletion in the subsequent dialog.

After the secure access policy is created, it is automatically downloaded and applied to the ZTA Gateway that it references.

---

**Note:** Secure Access Policies can take several minutes to reach their destination Gateway(s). If an entered policy contains configuration that fails to apply properly due to a compatibility or validation problem, nZTA displays an error message that the applied configuration is incorrect. nZTA attempts to re-apply the configuration in the policy at 15 minute intervals, and repeats this process until such a time as the policy is corrected or deleted.

---

After you have published applications to your Gateways, users can enroll their desktop and mobile devices. For more details, see the *Tenant Admin Guide*.

## Next Steps

After you have created your Secure Access Policies and deployed them to your Gateways, you can enroll your end-user devices. To learn more, see the *Tenant Admin Guide*.

---

The Ivanti product that is the subject of this technical documentation consists of (or is intended for use with) Ivanti software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <https://www.ivanti.com/company/legal/eula>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.