



nZTA Getting Started Guide
22.6R1

Copyright Notice

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

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

Copyright © 2023, Ivanti. All rights reserved.

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

Contents

| | |
|--|------------|
| Getting Started with Ivanti Neurons for Zero Trust Access | 4 |
| What is nZTA | 4 |
| Deploying and Using nZTA | 4 |
| Manually Configuring Your nZTA Deployment | 6 |
| What's New | 8 |
| Version 22.6R1 | 8 |
| Version 22.5R1 | 8 |
| Version 22.4R3 | 9 |
| Creating User Authentication Services | 10 |
| Workflow: Creating a Local Authentication Policy | 11 |
| Workflow: Creating a SAML Authentication Policy with Azure AD | 21 |
| Workflow: Creating a SAML Authentication Policy with On-Prem ICS | 38 |
| Workflow: Adding TOTP to an Authentication Policy | 58 |
| Creating User Rules and User Groups | 68 |
| Associating User Groups with Admin Roles | 73 |
| Role-based Access Control for Admin Users | 75 |
| Next Steps | 79 |
| Configuring Gateways | 80 |
| Introduction | 80 |
| Workflow: Creating a Gateway in VMware vSphere | 84 |
| Workflow: Creating a Gateway in Amazon Web Services | 93 |
| Workflow: Creating a Gateway in Microsoft Azure | 103 |
| Workflow: Creating a Gateway in KVM/OpenStack | 121 |
| Workflow: Creating a Gateway in Google Cloud Platform | 136 |
| Workflow: Creating a Gateway in Oracle Cloud Platform | 159 |
| Next Steps | 256 |
| Creating Device Policies and Device Rules | 257 |
| Introduction | 257 |
| Creating Device Policies | 259 |
| Creating Device Rules | 263 |
| Next Steps | 279 |
| Creating Applications and Application Groups | 280 |
| Introduction | 280 |
| Adding Applications to the Controller | 280 |
| Adding Application Groups to the Controller | 284 |
| Next Steps | 286 |
| Creating a Secure Access Policy | 287 |
| Introduction | 287 |
| Workflow: Creating a Secure Access Policy | 288 |
| Next Steps | 292 |

Getting Started with Ivanti Neurons for Zero Trust Access

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

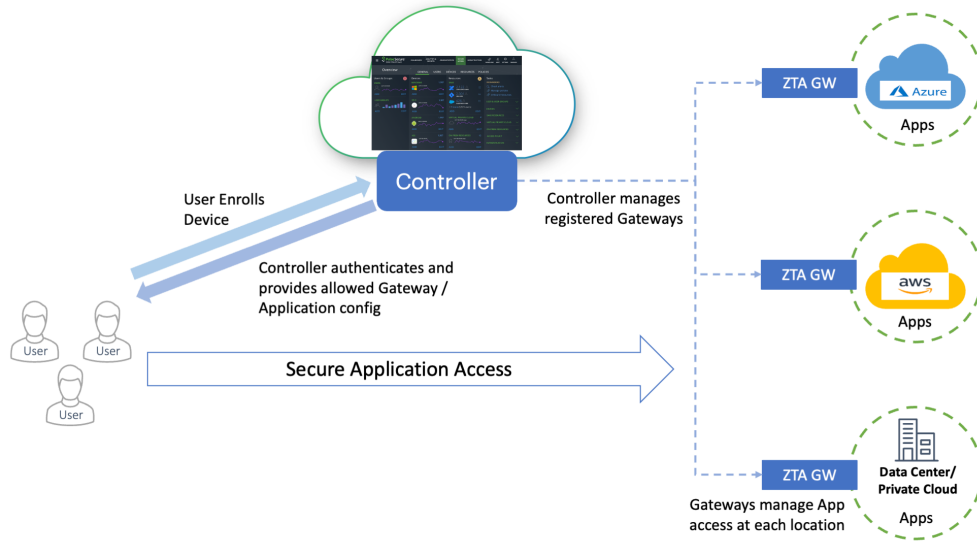
nZTA is a cloud-based SaaS (software as a service) application that provides fully-managed zero-trust authentication and access control for an organization's application infrastructure. nZTA enables administrators to define end-to-end authorization and authentication policies that control application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

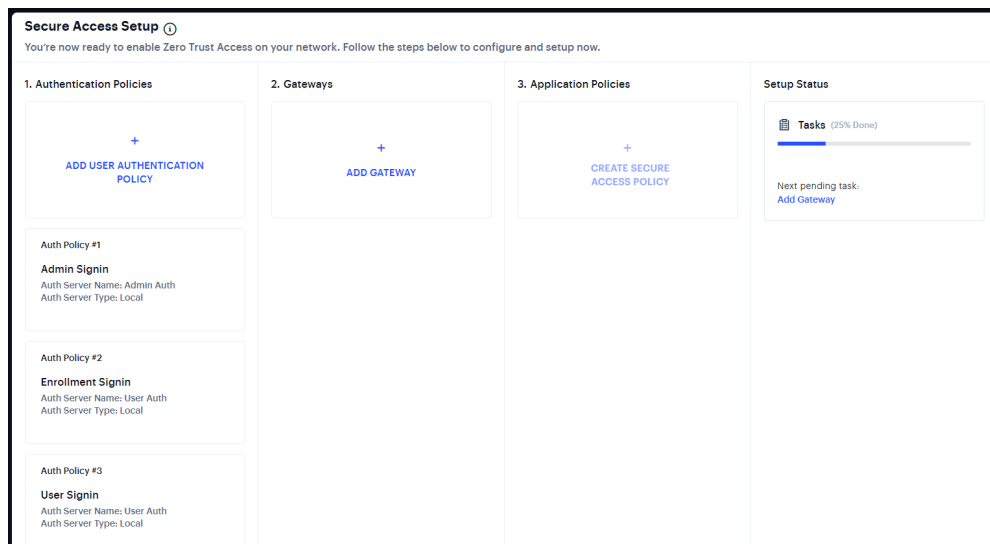
End-users install and run Ivanti Secure Access Client on their devices in order to manage secure and encrypted access to their organization's applications. Ivanti Secure Access Client works with the Controller and Gateways to assess authentication and authorization rights so applications that appear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



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.



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" on page 10](#).

- **Add Gateway.** This displays the Gateway Network Configuration dialog, see ["Configuring Gateways" on page 80](#).
- **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" below](#).

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**.



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



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" on page 10](#).
2. Create and deploy your application Gateways, see ["Configuring Gateways" on page 80](#).

3. Create your device rules and device policies, see ["Creating Device Policies and Device Rules"](#) on page 257
4. Create your applications and application groups, see ["Creating Applications and Application Groups"](#) on page 280
5. Create a secure access policy for an application and publish this policy to your Gateways, see ["Creating a Secure Access Policy"](#) on page 287.

What's New

Version 22.6R1

Oracle Cloud Platform support for ZTA Gateway

ZTA Gateway now supports deployment on Oracle Cloud Platform. For details see "[Workflow: Creating a Gateway in Oracle Cloud Platform](#)" on page 159.

Reusable custom icon to associate with application

The create application page provides an option to upload your own icon, which can be re-used to associate with more than one application. For details, see "[Creating Applications and Application Groups](#)" on page 280.

Simplifying Devices section and better correlation of data for Device Rules and Policies and Device Insights with a new workflow

Admin experience is enhanced by simplifying the device rules and policies. For details, see "[Creating Device Policies](#)" on page 259 and "[Creating Device Rules](#)" on page 263.

Version 22.5R1

Create another application option in Applications page

On Create Application page, admin can choose to continue to create one more application. For details, see "[Adding Applications to the Controller](#)" on page 280.

Gateway Creation Config UI Simplification

Create ZTA Gateway and Create ZTA Gateway Group options are grouped under Create. For details, see "[Workflow: Creating a Gateway in VMware vSphere](#)" on page 84.

Version 22.4R3

Role Based Access Control for Admin Users

With Role-based access control (RBAC), organizations can easily add admins and assign them specific roles, with differing levels of access to the nSA Admin Portal. In addition to an existing set of default roles, Administrators can now create custom granular roles for specific functions within the nSA admin portal.

For details, see ["Role-based Access Control for Admin Users" on page 75](#)

HTTP Proxy Support

Support Proxy configuration in gateway to connect to ZTA.

For details, see:

["Workflow: Creating a Gateway in VMware vSphere" on page 84](#)

["Workflow: Creating a Gateway in Amazon Web Services" on page 93](#)

["Workflow: Creating a Gateway in Microsoft Azure" on page 103](#)

["Workflow: Creating a Gateway in KVM/OpenStack" on page 121](#)

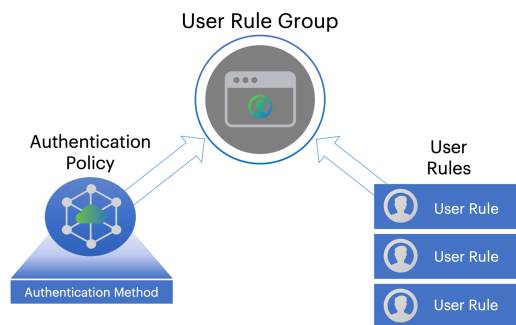
["Workflow: Creating a Gateway in Google Cloud Platform" on page 136](#)

Creating User Authentication Services

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](#)" on page 68.



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.
- *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.



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](#)" below.
- **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](#)" on page 21.
- **On-prem ICS 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](#)" on page 38.
- **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](#)" on page 58.



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

This process involves creating a local user authentication *method* and defining within it all user credentials necessary to identify and authenticate your end-users. You then configure this method as the primary authentication method in your *authentication policies*. If you are configuring Multi-Factor Authentication (MFA) in your deployment, you can configure local user authentication as either the primary or secondary authentication method.

Before you begin, make sure you have all user details (name and password) ready.

To configure a *new* local authentication method:

1. Log into the *Controller* as a Tenant Admin, see [Logging in as a Tenant 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 [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 | ⋮ |

User Authentication Methods

3. Select **Create Authentication Server**.

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

Adding a new local user authentication method



At any point during this process, you can reset the form data by selecting **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:

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.

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 [Using User Authentication Policies](#).

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

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.

| <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-saml... | SAML (Azu... | ⋮ |
| <input type="checkbox"/> | | netadmin | | admin | */login/netadmin/ | net-admin | Local | ⋮ |

User Authentication Policies

To learn more about the policies on this page, see [Viewing User Authentication Policies](#).

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

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

The **Create Authentication Policy** form appears.

The screenshot shows a web form titled "Create User Policies" with a sub-section "Create Authentication Policy". The form includes the following fields and sections:

- 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 larger text area with the placeholder "Add a description of the Authentication Policy".
- USER TYPE**: A dropdown menu currently showing "Users".
- DEVICE POLICY**: A dropdown menu showing "Select a Device Policy".
- ENROLL DEVICE POLICY**: A dropdown menu showing "Select a Enroll Device Policy".
- Auth Servers**: A section containing a **Note** and two dropdown menus:
 - PRIMARY AUTH SERVER***: A dropdown menu showing "Select from Local and SAML Auth Servers".
 - SECONDARY AUTH SERVER**: A dropdown menu showing "Select from Local and TOTP Auth Servers".

At the bottom right of the form, there are two buttons: "Cancel" and "Create User Policy".

Create Authentication Policy



To learn more about how custom policies are used for user login and enrollment, see [Adding Custom Authentication Policies](#).

- 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):

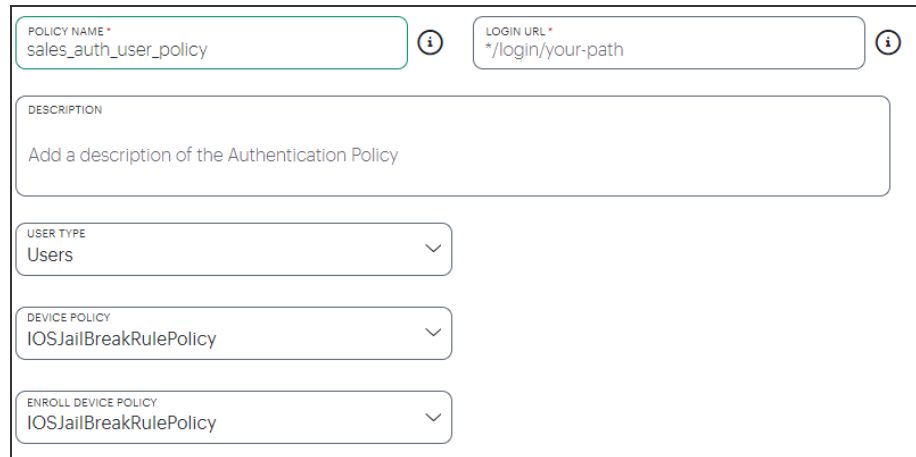
- In the case of user sign-in policies, this is the URL endpoint (appended to the tenant FQDN) to which new users are invited to connect to enroll or sign-in a device with the *Controller*. Example value: `*/login/saleslogin/`.
- In the case of user enrollment policies, this endpoint identifies the enrollment 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/`.



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 [Using User Authentication Policies](#).

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:
 - **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.

- (for policies with a **User Type** of "Users" only): Select an **Enroll Device Policy** from the drop-down list to be linked to this sign-in policy (as indicated):



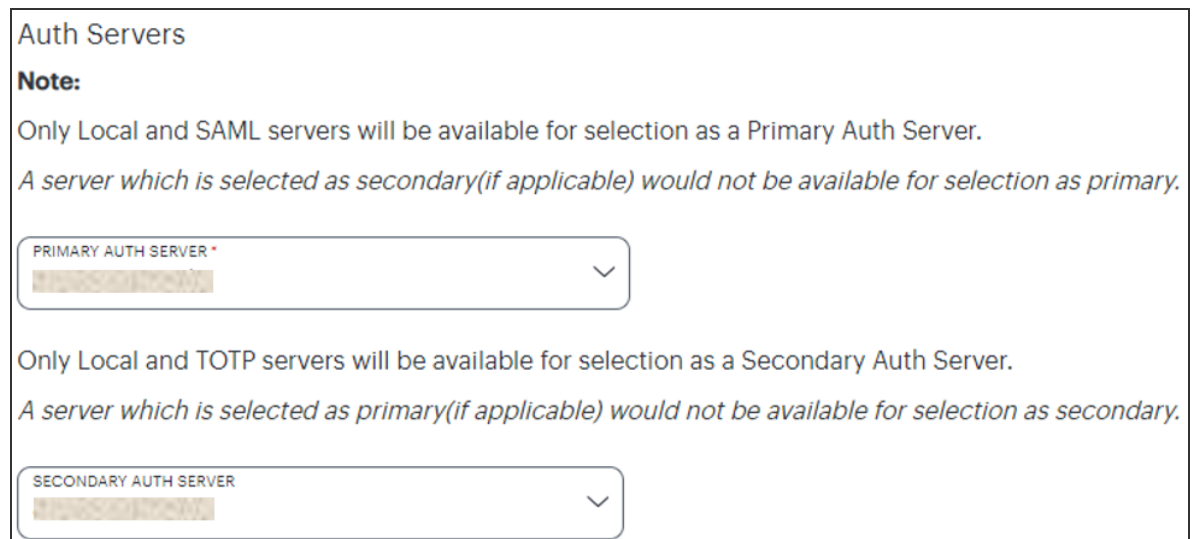
The screenshot shows a configuration form for an authentication policy. It includes the following fields:

- POLICY NAME ***: sales_auth_user_policy
- LOGIN URL ***: */login/your-path
- DESCRIPTION**: Add a description of the Authentication Policy
- USER TYPE**: Users
- DEVICE POLICY**: IOSJailBreakRulePolicy
- ENROLL DEVICE POLICY**: IOSJailBreakRulePolicy

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 [Using User Authentication Policies](#).

- Under **Policy Server Details**, select **Primary Auth Server** from the drop-down list:



The screenshot shows the 'Auth Servers' configuration section. It includes the following elements:

- Note:** 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.
- PRIMARY AUTH SERVER ***: A dropdown menu with a selected server.
- Note:** Only Local and TOTP servers will be available for selection as a Secondary Auth Server. A server which is selected as primary(if applicable) would not be available for selection as secondary.
- SECONDARY AUTH SERVER**: A dropdown menu with a selected server.

Selecting a primary authentication method for this policy

9. (Optional) Where a secondary method is required for Multi-Factor Authentication, select **Secondary Auth Server** from the drop-down list.



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

10. 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, then select **Edit**.

The **Edit authentication policy** form appears.



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):

Edit User Policies ⊙

Update Authentication Policy
Enter a name and description for the Authentication Policy

⊙
 ⊙

DESCRIPTION
 Add a description of the Authentication Policy

USER TYPE
 Administrators

DEVICE POLICY
 Select a Device Policy

Auth Servers

Note:
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.

PRIMARY AUTH SERVER*
 XDDDD

Only Local and TOTP servers will be available for selection as a Secondary Auth Server.
A server which is selected as primary (if applicable) would not be available for selection as secondary.

SECONDARY AUTH SERVER
 None

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):



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 **Update User Policy**.

The list of authentication policies updates.

4. Repeat until all required authentication policies are updated.

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/Editing Secure Access Policies](#).

For more information, see the *Tenant Admin Guide*.

Workflow: Creating a SAML Authentication Policy with Azure AD

nZTA supports the use of a cloud-based Active Directory (AD) SAML service to provide authentication for your users.

If you choose to use AD as a SAML Identity Provider (IdP), you do not create any users locally on the *Controller*. All users will already be present in your remote SAML service.

Configuring nZTA to use SAML authentication requires you to create separate SAML apps on the Azure AD platform for the following primary activities:

- User sign-in
- User enrollment

As part of hardening custom sign-in policies and login URLs, the following changes are implemented:

1. Instead of requiring administrators to configure enrollment policies, administrators will only need to configure user policies. As a default, all configured user policies support enrollment.
2. Single SAML authentication server for user authentication and enrollment.

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).

Configuring nZTA to Use SAML Authentication

Configure nZTA by performing the following steps:

1. Log into the *Controller* as a Tenant Admin, see [Logging in as a Tenant 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:

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 | ⋮ |

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](#)

Adding a user authentication method



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

4. Under **Choose Server Name and Authentication Type**:

- Select the **Authentication Type** as *SAML (Azure AD)*.

The form expands to show additional settings.

The screenshot shows the 'Manage Users' interface with the 'Authentication Servers' tab selected. The 'Create Authentication Server' form is displayed, featuring a 'Choose Server Name and Authentication Type' section. The 'Authentication Server Name' field is empty, and the 'Authentication Type' dropdown is set to 'SAML (Azure AD)'. Below this, there are options for 'Auth Metadata' (upload file or manual entry), 'Fields required for SAML Authentication Server' (allow unsigned metadata), and an 'Upload SAML Auth metadata' section with an 'Upload XML' button. A 'Single Logout URL' field is also present. At the bottom, there is an 'Enable Enrollment' toggle and 'Cancel' and 'Create Authentication Server' buttons.

Configuring SAML (Azure AD) authentication settings

- Specify an **Authentication Server Name**.

5. To provide your SAML IdP settings, select one of the following:

- Select **Upload SAML Auth metadata file** if not selected already. This is selected by default.

The **Download Auth Service Provider Metadata for IDP** link is enabled.

1. (Optional) Specify a **Single Logout URL**. For more information, see [Using SAML Single Logout to Force User Authentication](#).

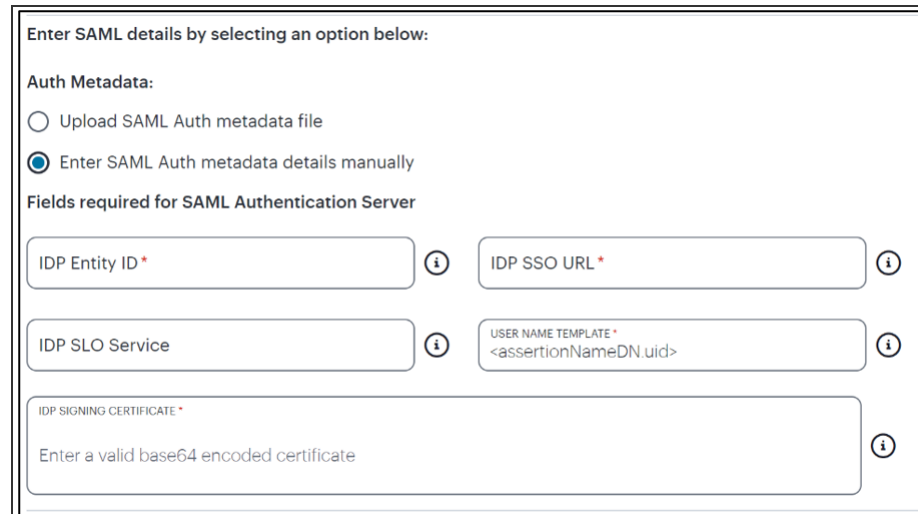


By default, the *Controller* expects a signed metadata definition file. To allow an unsigned metadata file, select **Allow Unsigned Metadata**.

2. Click the **Download Auth Service Provider Metadata for IDP** link. Retain the downloaded file for later use.

- Select **Enter SAML Auth metadata details 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:



The screenshot shows a configuration window titled "Enter SAML details by selecting an option below:". Under "Auth Metadata:", there are two radio buttons: "Upload SAML Auth metadata file" (unselected) and "Enter SAML Auth metadata details manually" (selected). Below this, the section "Fields required for SAML Authentication Server" contains four input fields, each with an information icon (i): "IDP Entity ID*" (required), "IDP SSO URL*" (required), "IDP SLO Service" (optional), and "USER NAME TEMPLATE*" (required) with the example value "<assertionNameDN.uid>". At the bottom, there is a large text area for "IDP SIGNING CERTIFICATE*" (required) with the instruction "Enter a valid base64 encoded certificate".

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 [Using SAML Single Logout to Force User Authentication](#).

- **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.

6. If this Auth server is used with User Policy of type "User", then click **Enable Enrollment**.

Enable Enrollment

You acknowledge that you have chosen to enroll metadata by checking this box.
If disabled, all enrollment configuration will be deleted and require reconfiguration.

Upload SAML Enroll metadata file
 Enter SAML Enroll metadata details manually

Fields required for SAML Authentication Server

Allow Unsigned Metadata

[Download Enroll Service Provider Metadata for IDP](#)

Upload SAML Enroll metadata

FILE
Upload XML file

Single Logout URL

Single Logout URL ?

Enable Enrollment

7. To provide your SAML IdP settings, select one of the following:

- Select **Upload SAML Enroll metadata file** if not selected already. This is selected by default.

1. (Optional) Specify a **Single Logout URL**. For more information, see [Using SAML Single Logout to Force User Authentication](#).

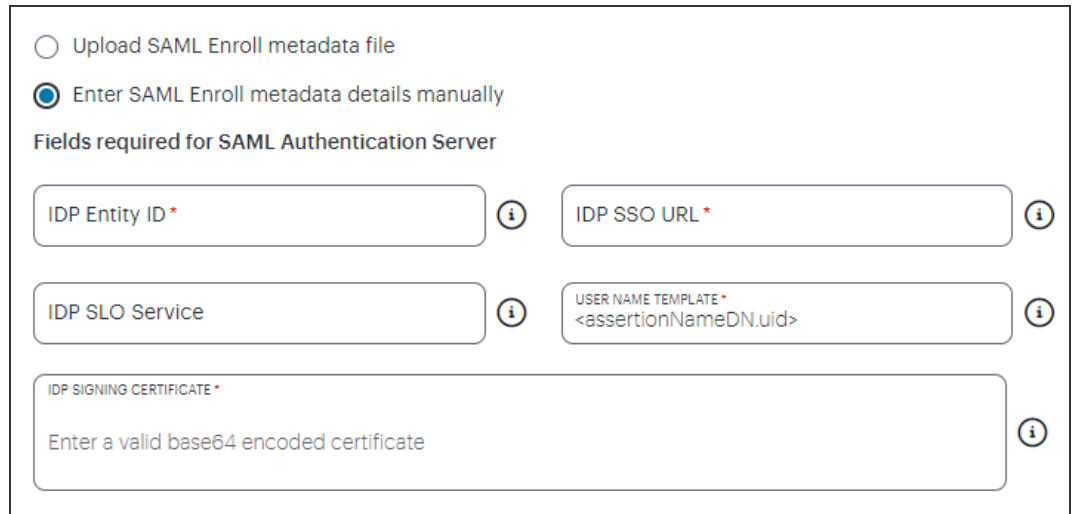


By default, the *Controller* expects a signed metadata definition file. To allow an unsigned metadata file, select **Allow Unsigned Metadata**.

2. Click the **Download Enroll Service Provider Metadata for IDP** link.

- Select **Enter SAML Enroll metadata details 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:



The screenshot shows a configuration form for SAML Enroll metadata details. At the top, there are two radio buttons: "Upload SAML Enroll metadata file" (unselected) and "Enter SAML Enroll metadata details manually" (selected). Below this, the section is titled "Fields required for SAML Authentication Server". There are four input fields, each with an information icon (i) to its right:

- IDP Entity ID ***: A text input field.
- IDP SSO URL ***: A text input field.
- IDP SLO Service**: A text input field.
- USER NAME TEMPLATE ***: A text input field containing the placeholder text "<assertionNameDN.uid>".

Below these fields is a larger text area for the **IDP SIGNING CERTIFICATE *** with the instruction "Enter a valid base64 encoded certificate".

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 [Using SAML Single Logout to Force User Authentication](#).

- **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.

- When editing an existing SAML Auth server, the 'Enable Enrollment' option can be enabled or disabled if the SAML Auth server is not being used in any 'User Policy'. If the SAML Auth server is being used in a 'User Policy', then Enable Enrollment button will be grayed out.



- If 'Enable Enrollment' is not selected, then while creation of 'User Policy' of type 'User', the server you have created (without Enable Enrollment) will not be listed.
 - When Enrollment is disabled, the enrollment SAML configuration will be deleted. To enable enrollment, you have to again provide enroll SAML auth server configuration.
-

8. Use the downloaded User Authentication and Enrollment SP Metadata files to create Sign-In and Enrollment SAML Apps in Azure AD. For details, see "[Creating Enrollment/Sign-in SAML App in Azure AD](#)" below.
9. Browse and upload the digitally-signed (or unsigned) federation metadata XML definition files downloaded from Azure AD.
10. Confirm that your settings are correct, then select **Create Authentication Server** 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.

11. (Optional) To edit a listed authentication method, click the adjacent three dots, then select **Edit**. Make any required updates and confirm.
12. (Optional) To delete one (or more) an *unused* authentication methods, select the check box for each, then select **Delete**. You must confirm the deletion.

Creating Enrollment/Sign-in SAML App in Azure AD

Perform the following steps in Azure AD:

1. Create a SAML app for the required activity (sign-in or enrollment).
2. Click **Upload Metadata File** and select the file from your download.

This defines 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.

The screenshot shows the Azure AD portal interface for configuring a SAML-based sign-on for an application named 'ZTA-Auth'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on), Provisioning, Application proxy, Self-service, Security (Conditional Access, Permissions, Token encryption), and Activity (Sign-ins, Usage & insights, Audit logs, Provisioning logs, Access reviews). The main content area is titled 'Set up Single Sign-On with SAML' and includes a link to 'Upload metadata file' (highlighted with a red box) and a 'Test this application' button. Below this, there are three numbered configuration sections:

- Basic SAML Configuration** (highlighted with a red box):

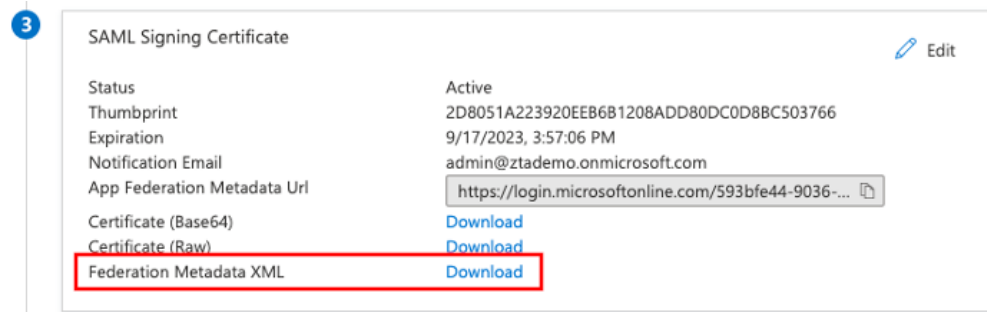
| | |
|--|---|
| Identifier (Entity ID) | https://pine1.pine.pzt.dev.perfsec.com |
| Reply URL (Assertion Consumer Service URL) | https://pine1.pine.pzt.dev.perfsec.com/dana-na/auth/saml-consumer.cgi |
| Sign on URL | Optional |
| Relay State | Optional |
| Logout Url | Optional |
- User Attributes & Claims**:

| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |
- SAML Signing Certificate**:

| | |
|-----------------------------|--|
| Status | Active |
| Thumbprint | 2D8051A223920EEB681208ADD80DC0D8BC503766 |
| Expiration | 9/17/2023, 3:57:06 PM |
| Notification Email | admin@ztademo.onmicrosoft.com |
| App Federation Metadata Url | https://login.microsoftonline.com/593bfe44-9036-... (Download) |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

Setting *Basic SAML Configuration* in Azure AD applications

- Download the Federation metadata XML definition for the SAML app to your local workstation. Retain this file for later use.



Downloading Federation Metadata XML files for user enrollment and user sign-in SAML applications

- Repeat these steps for each activity.



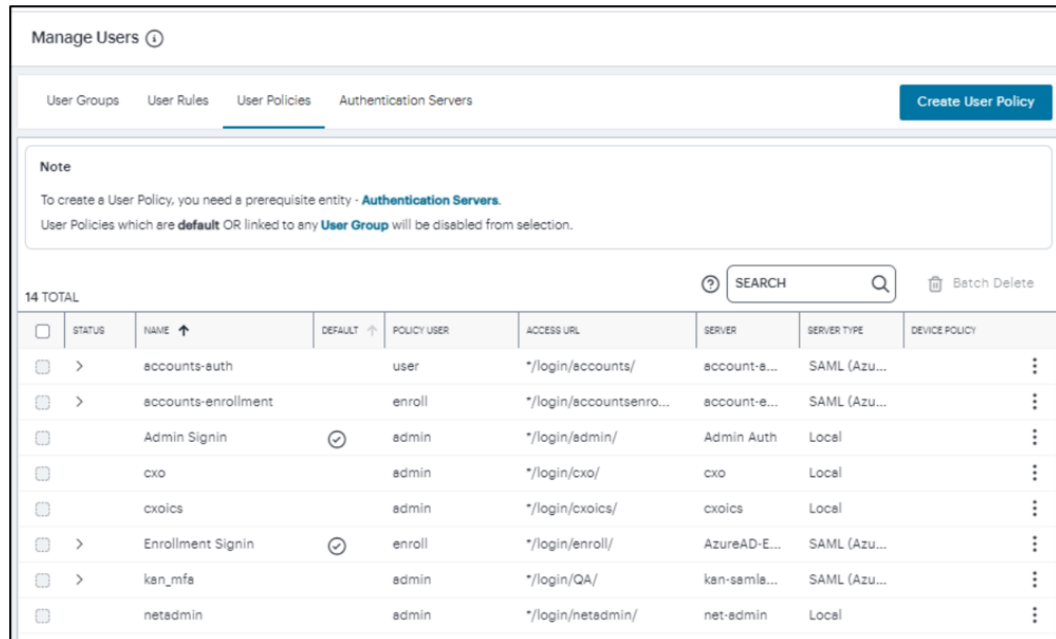
For details on how to create SAML apps in Azure AD, see the [Azure AD SAML documentation](#).

Creating/Updating Authentication Policies

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

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](#)

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-a... | SAML (Azu... | ⋮ |
| <input type="checkbox"/> | > | accounts-enrollment | | enroll | */login/accounsenro... | 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 | ⋮ |

User Authentication Policies

To learn more about the policies on this page, see [Viewing User Authentication Policies](#).

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

- To add a new custom policy, select **Create User Policy**.

The **Create Authentication Policy** form appears.

The screenshot shows a web form titled "Create User Policies" with a sub-section "Create Authentication Policy". The form includes the following fields and sections:

- 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 larger text area with the placeholder "Add a description of the Authentication Policy".
- USER TYPE**: A dropdown menu currently showing "Users".
- DEVICE POLICY**: A dropdown menu showing "Select a Device Policy".
- ENROLL DEVICE POLICY**: A dropdown menu showing "Select a Enroll Device Policy".
- Auth Servers**: A section with a **Note:** "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 for **PRIMARY AUTH SERVER *** with the placeholder "Select from Local and SAML Auth Servers".
- Below the primary server section, another note: "Only Local and TOTP servers will be available for selection as a Secondary Auth Server. A server which is selected as primary(if applicable) would not be available for selection as secondary." Below this is a dropdown menu for **SECONDARY AUTH SERVER** with the placeholder "Select from Local and TOTP Auth Servers".
- At the bottom right, there are two buttons: a solid "Cancel" button and a dashed "Create User Policy" button.

Create Authentication Policy

i At any point during this process, you can reset the form data by selecting **Reset Fields**.

i To learn more about how custom policies are used for user login and enrollment, see [Adding Custom Authentication Policies](#).

- 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/`.



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 [Using User Authentication Policies](#).

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:
 - **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. From the **Device Policy** list, select a device policy.
8. (for policies with a **User Type** of "Users" only): Select an **Enroll Device Policy** from the drop-down list to be linked to this sign-in policy (as indicated):

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 [Using User Authentication Policies](#).

9. Under **Auth Servers**, select **Primary Auth Server** and choose the required authentication method from the drop-down list. Only Local and SAML servers will be available for selection as a Primary Auth Server.

10. (Optional) Where a secondary method is required for Multi-Factor Authentication, select **Secondary Auth Server** and choose the required authentication method from the drop-down list. Only Local and TOTP servers will be available for selection as a Secondary Auth Server.
11. Click **Create User Policy** to create the new policy.

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

Existing User Policies

- For existing default user policies, admin can select either existing or new SAML or Local Auth Server.

Note: The Auth Server for enrollment will be added automatically.

- For existing custom user policies, user can update existing SAML Auth Server.

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

1. Click the three dots adjacent to the relevant policy, then select **Edit**.

The **Update Authentication Policy** form appears.



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

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

The screenshot shows the 'Edit User Policies' interface. At the top, it says 'Update Authentication Policy' and 'Enter a name and description for the Authentication Policy'. There are two input fields: 'POLICY NAME' with the value 'nevadadminpolicy' and 'LOGIN URL' with the value '/login/nadmin/'. Below these is a 'DESCRIPTION' field with the placeholder text 'Add a description of the Authentication Policy'. There are two dropdown menus: 'USER TYPE' set to 'Administrators' and 'DEVICE POLICY' set to 'Select a Device Policy'. Under the 'Auth Servers' section, there is a 'Note' stating that only Local and SAML servers are available for selection as a Primary Auth Server, and a server selected as secondary would not be available for selection as primary. The 'PRIMARY AUTH SERVER' dropdown is set to 'XPPDP'. Another note states that only Local and TOTP servers are available for selection as a Secondary Auth Server, and a server selected as primary would not be available for selection as secondary. The 'SECONDARY AUTH SERVER' dropdown is set to 'None'. At the bottom right, there are 'Cancel' and 'Update User Policy' buttons.

Editing the primary auth server

i 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**.

i 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.

- Select **Update User Policy**.

The list of authentication policies updates.

- 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. Select **Download** and save the metadata file.



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 the **User Authentication** workflow is complete, you can configure the Azure AD platform with the XML configuration of the *Controller*. For details on how to configure Azure AD, see [Configuring Azure AD with Service Provider Metadata from the Controller](#).

Finally, 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/Editing Secure Access Policies](#).

For more information, see the *Tenant Admin Guide*.

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

You can choose to use a configured *ICS* server (either remote or local) as an on-premises SAML AD authentication server for your *Controller*.



If you choose to use SAML authentication on your *Controller*, you do not create any users manually. All users will already be present on your remote SAML server.

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 includes the ability to create your own custom policies for separate authentication of specific groups. You create an authentication method referencing one of the 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.

To configure *nZTA* to use SAML authentication through *ICS*, perform the following steps:

1. Configure your on-premises *ICS* to act as a SAML AD authentication server:
 - Optionally, [Configuring Secondary Authentication for On-Premises ICS \(Optional\)](#).
 - [Configuring a SAML Identity Provider in Ivanti Connect Secure](#).
 - [Configuring a Metadata Provider in Ivanti Connect Secure](#).
2. Define an on-premises SAML authentication method, see [Defining an On-Premises SAML Authentication Method](#).
3. Configure an on-premises SAML authentication policy, see [Defining Authentication Policies for On-Premises SAML Authentication](#).
4. After you complete the User Authentication workflow, configure the SAML apps on the on-premises *ICS* server with the XML metadata configuration from the matching *nZTA* authentication policy, see [Configuring ICS with Controller Metadata](#).



You will need to repeat this process for each required SAML app on your *ICS* server.

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/Editing Secure Access Policies](#).

Configuring Secondary Authentication for On-Premises *ICS* (Optional)



This section describes an optional configuration activity for SAML User Authentication on an on-premises *ICS* server.

Multi-Factor Authentication (MFA) is an authentication method by which a computer user is granted access only after successfully presenting two (or more) pieces of evidence (or factors) to an authentication mechanism. The ICS platform supports a number of secondary authentication solutions, and can be configured so that two authentication factors are required by users using a single nZTA user authentication method. Before you configure the on-premises ICS server and Controller for SAML User Authentication, you can choose to configure MFA (secondary) support to ICS.



Before you start this procedure, you must have fully configured a secondary authentication server. For example, *Google OTP (One Time Password)* or *NAS OTP*. For the purposes of this example, an existing local *Google OTP* server is used, but different established secondary authentication methods are also supported.

To configure *ICS* for secondary authentication:

1. Log in to the on-premises *Ivanti Connect Secure* server.
2. On the **Authentication** menu, select **Auth. Servers**.

The **Authentication Servers** page appears.

3. Under **New**, select the required authentication server type. For example, select *Time based One Time Password (TOTP) Server*.
4. Select **New Server**.

The **New Time based One Time Password (TOTP) Server** page appears.

5. Enter the following parameters for the new server:
 - Add a **Name** for the server, for example *Google OTP*.
 - Select the **Allow Auto Unlock** check box, and set **Auto unlock period**. For example, 10 minutes.
 - Select the **Allow new TOTP user registration to happen via External Port** check box.
 - Select the **Allow TOTP authentication from Remote Pulse Secure Devices** check box.
 - Leave all other parameters as their default settings.
6. Select **Save Changes**.

The new server (Google OTP) is added to the list of **Authentication Servers**.

7. You must now add a new user to the local system. To do this:
 - In the **Authentication Servers** list, select the hyperlink for the *System Local* entry.
 - The **Settings** page for *System Local* appears.
 - Select the **Users** tab.
 - Select **New** to create a user.
 - The **New Local User** page appears.
 - Enter details for the user, and ensure that the **Enabled** check box is selected, and that other check boxes are clear.
 - Select **Save Changes** to create the user.
8. Select the **Users** menu, then select **User Realms**.

The **User Authentication Realms** page appears.

9. You must now enable secondary authentication. To do this:
 - In the **User Authentication Realms** list, select the hyperlink for the *Users* entry.

The **General** page for the *Users* realm appears.
 - Under **Additional authentication server**, select the **Enable additional authentication server** check box.
 - Set **Authentication #2** to *Google OTP*.
 - At the bottom of the page, select **Save Changes**.

You can now configure an Identity Provider in *ICS*, see [Configuring a SAML Identity Provider in Ivanti Connect Secure](#).

Configuring a SAML Identity Provider in *Ivanti Connect Secure*

This section describes the steps to configure a SAML Identity Provider (IdP) on an on-premises *Ivanti Connect Secure (ICS)* server. The metadata for the IdP is required by each SAML user method on *nZTA*.

To configure SAML IdP on the *Ivanti Connect Secure* server:

1. Log in to the on-premises *Ivanti Connect Secure* server that is identified as an Identity Provider.
2. Navigate to **System > Configuration > SAML > Settings**.
3. Configure the following Metadata Server Configuration:
 - **Timeout value for metadata fetch request** to 300.
 - **Host FQDN for SAML** to the Fully Qualified Domain Name, noting the host FQDN guidance below.

The host FQDN specified here is used in the SAML entity ID, used by browsers to connect to *ICS*, and used in the URLs for SAML services. Typically:

- If the *ICS* is standalone, the FQDN should resolve to the IP address of the external interface / internal interface, whichever is chosen.
 - If the *ICS* is an Active-Passive cluster, the FQDN should resolve to the external VIP / Internal VIP, whichever is chosen.
 - If the *ICS* is an Active-Active cluster behind an in-line load balancer, the FQDN should resolve to the load balancer's external VIP / Internal VIP, whichever is chosen.
4. Select **Save Changes**.
 5. Select **Update Entity IDs** and confirm this action on the warning page by selecting **Update Entity IDs**.
 6. Navigate to **System > Configuration > Certificates > Device Certificate**, create a new CSR, and import certificate and keys. Skip this step if the *ICS* external interface / internal interface (whichever is chosen) already provides a certificate that matches the host's Fully Qualified Domain Name.
 7. Navigate to **Authentication > Signing In > Sign In SAML > Identity Provider**.
 8. Locate the the **Basic Identity Provider (IdP) Configuration** section.
 9. Under **Protocol Binding to use for SAML Response**:
 - Select the **Post** check box.
 - Clear the **Artifact** check box.
 - Select the required **Signing Certificate**.

10. Under Other Configurations:
 - Select the **Accept unsigned AuthnRequest** check box.
 - Select **sha-256** for Signature Algorithm, if ICS is using 22.x version onwards.
11. Under Service-Provider-related IDP Configuration:
 - For **SignIn Policy**, select the */policy.
12. Under **User Identity**:
 - For **Subject Name Format**, select Email Address.
 - For **Subject Name**, enter <USERNAME>.
 - At the bottom of the page, select **Save Changes**.

You can now configure a Metadata Provider in ICS, see [Configuring a Metadata Provider in Ivanti Connect Secure](#).

Configuring a Metadata Provider in *Ivanti Connect Secure*

This section describes the steps to configure *Ivanti Connect Secure* to be a Metadata Provider, and to download metadata for use on the *Controller*.

To configure a Metadata Provider in the on-premises ICS server:

1. Log in to *Ivanti Connect Secure* server.
2. Navigate to **Authentication > Signing-In > Sign In SAML > Metadata Provider**.

The SAML Metadata Provider Entity Id property is pre-populated. It is generated by the system, based on the value for the Host FQDN for SAML setting on the **System > Configuration > SAML > Settings** page.

3. Set **Metadata Validity** to 365 days.
4. Clear the **Do Not Publish IdP in Metadata** check box.
5. Select **Save Metadata Provider**.
6. Select **Download Metadata** and save the file to your computer.

This definition file is required to enable on-premises SAML apps on the *Controller*.

You can then configure the *Controller* to use an on-premises SAML Server, see [Defining an On-Premises SAML Authentication Method](#).

Defining an On-Premises SAML Authentication Method

A minimum of two authentication methods are required:

- An authentication method for a SAML enrollment sign-in app.
- An authentication method for a SAML user sign-in app.

To create an on-premises SAML server authentication method for a specific activity, for example, device enrollment:

1. Log into the *Controller* as a Tenant Admin, see [Logging in as a Tenant 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:

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 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 | ⋮ |

User Authentication Methods

3. Select **Create Authentication Server**.

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

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

Creating a user authentication method



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

4. Under **Choose Server Name and Authentication Type**:

- Select the **Authentication Type** of *SAML (Custom)*.

The form expands to show additional settings:

The screenshot shows the 'Create Authentication Server' form. At the top, it lists authentication methods: Local, SAML (Azure AD), SAML (Custom) and TOTP. The 'Choose Server Name and Authentication Type' section has two input fields: 'AUTHENTICATION SERVER NAME' with the value 'sales_saml_custom' and 'AUTHENTICATION TYPE' with the value 'SAML (Custom)'. Below this, it asks to 'Enter SAML details by selecting an option below:' and provides two radio button options: 'Upload SAML Auth metadata file' (selected) and 'Enter SAML Auth metadata details manually'. There is also a checkbox for 'Allow Unsigned Metadata' which is unchecked, and a link to 'Download Auth Service Provider Metadata for IDP'. The 'Upload SAML Auth metadata' section has a file upload field with 'Upload XML' and a file icon. The 'Single Logout URL' section has a text input field. At the bottom, there is a toggle for 'Enable Enrollment' which is turned off. The form has 'Cancel' and 'Create Authentication Server' buttons at the bottom right.

Configuring SAML (Custom) authentication settings

- Specify an **Authentication Server Name**. For example: *Enrollment* or *SignIn*.

5. To provide your SAML IdP settings, select one of the following:

- Select **Upload SAML Auth metadata file** if not selected already. This is selected by default.

The **Download Auth Service Provider Metadata for IDP** link is enabled.

1. (Optional) Specify a **Single Logout URL**. For more information, see [Using SAML Single Logout to Force User Authentication](#).

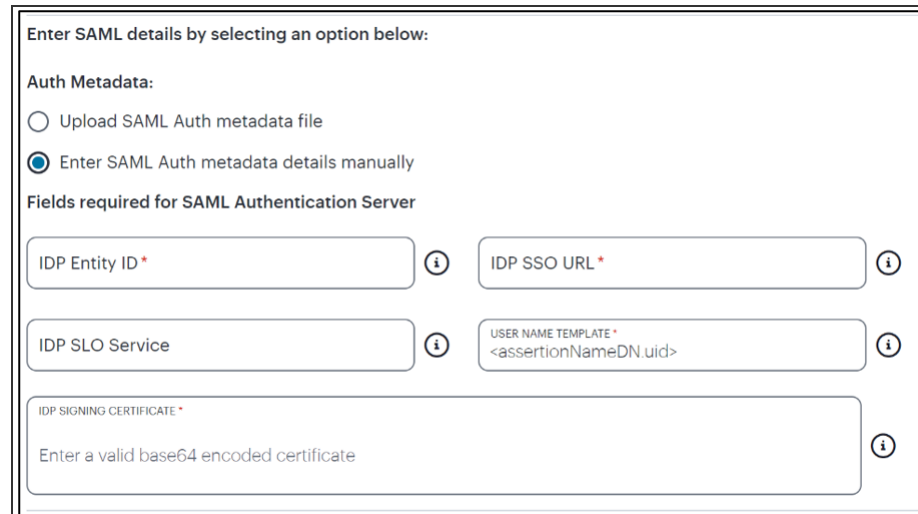


By default, the *Controller* expects a signed metadata definition file. To allow an unsigned metadata file, select **Allow Unsigned Metadata**.

2. Click the **Download Auth Service Provider Metadata for IDP** link. Retain the downloaded file for later use.

- Select **Enter SAML Auth metadata details 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:



The screenshot shows a configuration window titled "Enter SAML details by selecting an option below:". Under "Auth Metadata:", there are two radio buttons: "Upload SAML Auth metadata file" (unselected) and "Enter SAML Auth metadata details manually" (selected). Below this, the section "Fields required for SAML Authentication Server" contains several input fields, each with an information icon (i):

- IDP Entity ID ***: A text input field.
- IDP SSO URL ***: A text input field.
- IDP SLO Service**: A text input field.
- USER NAME TEMPLATE ***: A text input field containing the value "<assertionNameDN.uid>".
- IDP SIGNING CERTIFICATE ***: A large text area with the placeholder text "Enter a valid base64 encoded certificate".

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 [Using SAML Single Logout to Force User Authentication](#).

- **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.



- When editing an existing SAML Auth server, the 'Enable Enrollment' option can be enabled or disabled if the SAML Auth server is not being used in any 'User Policy'. If the SAML Auth server is being used in a 'User Policy', then Enable Enrollment button will be grayed out.
- If 'Enable Enrollment' is not selected, then while creation of 'User Policy' of type 'User', the server you have created (without Enable Enrollment) will not be listed.
- When Enrollment is disabled, the enrollment SAML configuration will be deleted. To enable enrollment, you have to again provide enroll SAML auth server configuration.

6. Confirm that your settings are correct, then select **Create Authentication Server** to create the authentication method.

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

7. (Optional) To edit a listed authentication method, click the adjacent three dots, then select **Edit**. Make any required updates and confirm.
8. (Optional) To delete one (or more) an *unused* authentication methods, select the check box for each, then select **Delete**. You must confirm the deletion.

You can now proceed to update the required authentication policy, see [Defining Authentication Policies for On-Premises SAML Authentication](#).

Defining Authentication Policies for On-Premises SAML Authentication

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

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](#)

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-samle... | SAML (Azu... | ⋮ |
| <input type="checkbox"/> | | netadmin | | admin | */login/netadmin/ | net-admin | Local | ⋮ |

User Authentication Policies

To learn more about the policies on this page, see [Viewing User Authentication Policies](#).

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

1. Select **Create User Policy**.


The **Create Authentication Policy** form appears.


The screenshot shows a web form titled "Create User Policies" with a sub-section "Create Authentication Policy". The form includes the following fields and sections:

- POICY 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 larger text area with the placeholder "Add a description of the Authentication Policy".
- USER TYPE:** A dropdown menu currently showing "Users".
- DEVICE POLICY:** A dropdown menu with the placeholder "Select a Device Policy".
- ENROLL DEVICE POLICY:** A dropdown menu with the placeholder "Select a Enroll Device Policy".
- Auth Servers:** A section containing a **Note** and two dropdown menus:
 - PRIMARY AUTH SERVER:** A dropdown menu with the placeholder "Select from Local and SAML Auth Servers".
 - SECONDARY AUTH SERVER:** A dropdown menu with the placeholder "Select from Local and TOTP Auth Servers".

At the bottom right of the form, there are two buttons: "Cancel" and "Create User Policy".

Add User Authentication

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

 To learn more about how custom policies are used for user login and enrollment, see [Adding Custom Authentication Policies](#).

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):

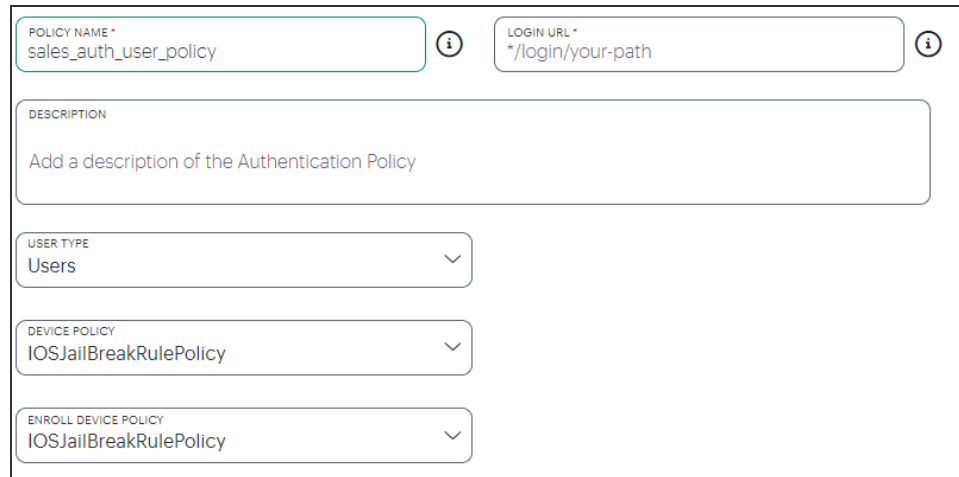
- In the case of user sign-in policies, this is the URL endpoint (appended to the tenant FQDN) to which new users are invited to connect to enroll or sign-in a device with the *Controller*. Example value: `*/login/saleslogin/`.
- In the case of user enrollment policies, this endpoint identifies the enrollment 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/`.



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 [Using User Authentication Policies](#).

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:
 - **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.

- (for policies with a **User Type** of "Users" only): Select an **Enroll Device Policy** from the drop-down list to be linked to this sign-in policy (as indicated):



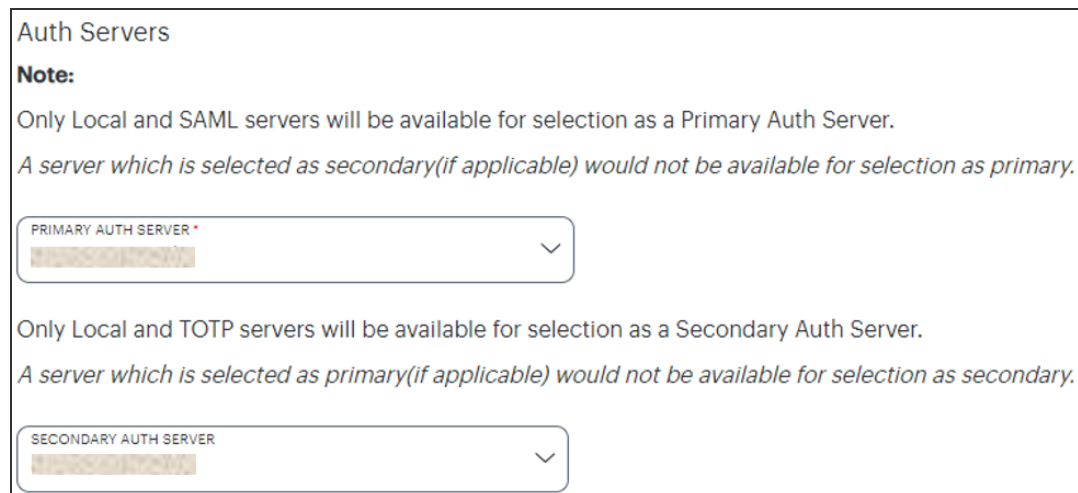
The screenshot shows a configuration form for an authentication policy. It contains the following fields:

- POLICY NAME ***: sales_auth_user_policy
- LOGIN URL ***: */login/your-path
- DESCRIPTION**: Add a description of the Authentication Policy
- USER TYPE**: Users
- DEVICE POLICY**: IOSJailBreakRulePolicy
- ENROLL DEVICE POLICY**: IOSJailBreakRulePolicy

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 [Using User Authentication Policies](#).

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



The screenshot shows the 'Auth Servers' configuration section. It includes a 'Note' and two dropdown menus:

Note:
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.

PRIMARY AUTH SERVER *

Only Local and TOTP servers will be available for selection as a Secondary Auth Server.
A server which is selected as primary(if applicable) would not be available for selection as secondary.

SECONDARY AUTH SERVER

Selecting a primary authentication method for this policy

Alternatively, select *Create Authentication 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**.



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

- Select **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:

- Click the three dots adjacent to the relevant policy, then select **Edit**.

The **Edit authentication policy** form appears.



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

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

The screenshot shows the 'Edit User Policies' interface. At the top, it says 'Update Authentication Policy' and 'Enter a name and description for the Authentication Policy'. There are two input fields: 'POLICY NAME' with the value 'newadminpolicy' and 'LOGIN URL' with the value '*/login/nadmin/'. Below these is a 'DESCRIPTION' field with the placeholder text 'Add a description of the Authentication Policy'. There are two dropdown menus: 'USER TYPE' set to 'Administrators' and 'DEVICE POLICY' set to 'Select a Device Policy'. The 'Auth Servers' section contains a 'Note' and two dropdown menus. The 'PRIMARY AUTH SERVER' dropdown is set to 'XPPDP' and the 'SECONDARY AUTH SERVER' dropdown is set to 'None'. At the bottom right, there are 'Cancel' and 'Update User Policy' buttons.

Editing the primary auth server

i 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**.

i 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.

- Select **Update User Policy**.

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:

- Refresh your browser until the **Download** action is visible for the relevant policy.
- Select the check box for the policy and clear all other check boxes.

3. Select **Download** and save the metadata file.



Repeat these procedures for each required SAML app on your On-Prem *ICS* server. That is, you require separate XML metadata files for your enrollment authentication policy and your sign-in authentication policy.

After you have configured a user authentication policy, you can configure your *ICS* SAML app with the SP Metadata configuration of the *Controller*, see [Configuring ICS with Controller Metadata](#).

Configuring *ICS* with *Controller* Metadata

Before the *Controller* can use a SAML server on an on-premises *ICS* server, you must enable communication between each separate SAML app on the *ICS* server and the *Controller*.

To do this, you must configure the SAML apps on the on-premises *ICS* server with the XML metadata configuration file for the *Controller*.

There are a minimum of two SAML apps:

- A SAML app for user enrollment. For example, called *Enrollment*.
- A SAML app during user sign-in. For example, called *Signin*.



You download the *Controller* XML configuration file when you selected an authentication policy. Alternatively, select the policy, then select **Download** on the **User authentication policies** page, see [Viewing User Authentication Policies](#).

To configure a SAML app on *ICS* with XML from the *Controller*:

1. Log into your *ICS* platform.
2. Navigate to **System > Configuration > SAML**.
3. Select **New Metadata Provider**.
4. Enter a **Name** for the metadata provider.

5. Under **Metadata Provider Location Configuration**:
 - For **Location**, select *Local*.
 - For **Upload Metadata File**, select **Browse** and select the metadata that you saved on your computer in the previous process (see above).
6. Under **Metadata Provider Verification Configuration**:
 - Select the **Accept Unsigned Metadata** check box.
7. Under **Metadata Provider Filter Configuration**:
 - For **Roles**, select the Service Provider check box.
8. Select **Save Changes**.
9. Navigate to **Authentication > Signing In > Sign-In SAML > Identity Provider**.
10. In the **Configuration** section, select **Add SP**.

The New Peer Service Provider page appears.
11. In the **Service Provider Configuration** and **Certificate Status Checking Configuration** sections, make the necessary service provider specific settings. For more details, refer to the "Configuring Sign-in SAML Identity Provider Settings" section in the "*Ivanti Connect Secure Administration Guide*".
12. In the **Customize IdP Behavior** section, select the **Override Default Configuration** check box.
13. Clear the **Reuse Existing NC (Pulse) Session** check box.
14. Select the **Accept unsigned AuthnRequest** check box.
15. At the bottom of the page, select **Save Changes**.

After the on-premises *ICS* SAML service is configured to connect to the *Controller*, you can then create a user group to apply the newly created authentication policy to your secure applications, see [Creating User Rules and User Groups](#).

For more information, see the *Tenant Admin Guide*.

Workflow: Adding TOTP to an Authentication Policy



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.

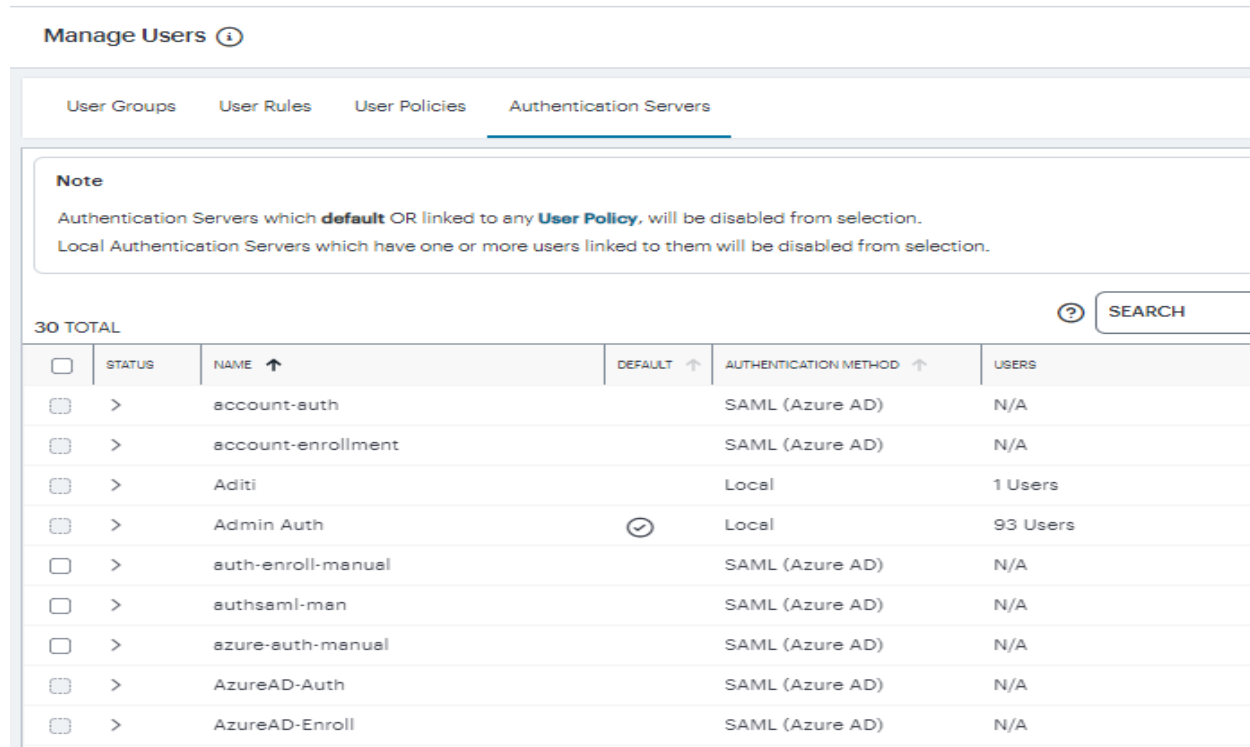
To use TOTP, first create a TOTP authentication method in nZTA and then associate it with your user sign-in authentication policies.

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](#)" on page 287.

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:



Manage Users ⓘ

User Groups User Rules User Policies **Authentication Servers**

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

| <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 |

3. Select **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. nZTA 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



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:

User Authentication

Add Authentication Method

Choose name and type

AUTHENTICATION SERVER NAME
totpauth 

AUTHENTICATION TYPE
TOTP 

Number of Attempts

Max number of consecutive wrong attempts allowed after which account will be locked

NO OF ATTEMPTS
3 

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 sign in 

Allow Auto Unlock

Locked account will be automatically unlocked after specified period (min: 10 minutes to max:90 days)

AUTO UNLOCK PERIOD
10 

Copyright © 2023, Ivanti. All Rights Reserved. [Privacy and Legal](#).

Minute(s) 

5. Enter the following settings:



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](#)" on page 67.
- **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.



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

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

? SEARCH

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

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.

User Policies

Edit Authentication Policy

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

AzureAD-Auth 

SECONDARY AUTH SERVER 

 Add new server

Aditi

cxo

cxoics

cxonew

net-admin

networkics

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.



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 | | | SEARCH  |
|---|---|--|---|
| 1 USER(S) | | | |
|  | USER NAME  | LAST ATTEMPTED  | LAST SUCCESSFUL LOGIN  |
|  | user1 | Thu, 23 Jun 2022 03:35:37 AM GMT | Thu, 23 Jun 2022 03:35:37 AM GMT |

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.



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.
- *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.



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.

< Create User Rule ⓘ

Create User Rule
Each user rule identifies one or more users, either from a local user authentication method or from a SAML user authentication method. nSA includes three built-in user rules: AllAdminUsers, AllEnrollmentUsers and AllUsers. [Reset Fields](#)

Rule Name* ⓘ

SELECT ATTRIBUTE TYPE
Username ⓘ

EXPRESSION MATCHING
User* ⓘ

[Cancel](#) [Create User Rule](#)



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.



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" on the next page](#).

Creating User Groups

After you have created user rules (see "[Creating User Rules](#)" on page 68), 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.
- **USERS.** This user group associates the default *ALLUSERS* user rule with the built-in *User Signin* authentication policy.

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.

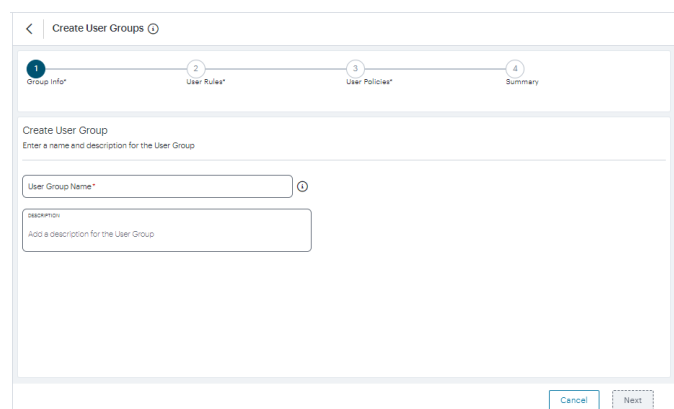
To create a user group:

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.



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.

Associating User Groups with Admin Roles

An admin role defines the elements of the user interface that an associated user group can access.

The current user can only access an individual user interface page/workflow if their user group is associated with an admin role that permits it. The tasks they can perform within that displayed element depends on the permissions set within the admin role.



When you are using admin roles, *Ivanti* recommends that any user rules for administrators does not use a basic asterisk wildcard, see [Creating User Rules](#). Instead, a more-specific wildcard that only includes admin users is required in this case to prevent all users having total access rights.



The default admin roles are not created by the tenant admin using the *nZTA* user interface. Rather, they are set up by the *Ivanti* DevOps team.

For example, the DevOps team might define the following admin roles:

- The *.Administrators* admin role has access to all user interface elements (full read, create, update, delete rights).
- The *.Read-Only Administrators* admin role has access to all user interface elements except workflows (read only).
- The *.Network Administrators* admin role has access to *ZTA Gateways* and *Insights* (read only).
- The *.CxOs* admin role has access to *Insights* only (read only).



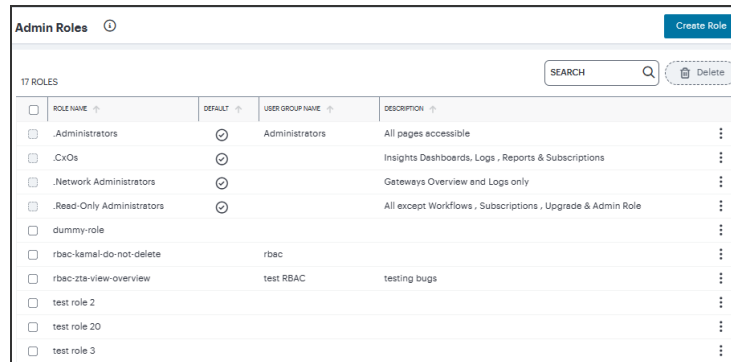
For more information about your assigned admin roles, please contact *Ivanti* DevOps.

The Tenant Admin can view admin roles in the **Administration > Admin Roles** page, and associate each role with a single user group.

To associate a user group with an admin role:

1. Log into the *Controller* as a Tenant Admin.
2. From the *nZTA* menu, select **Administration**, then select **Admin Roles**.

A list of Admin Roles appears. This includes default admin roles and custom admin roles (RBAC). For example:

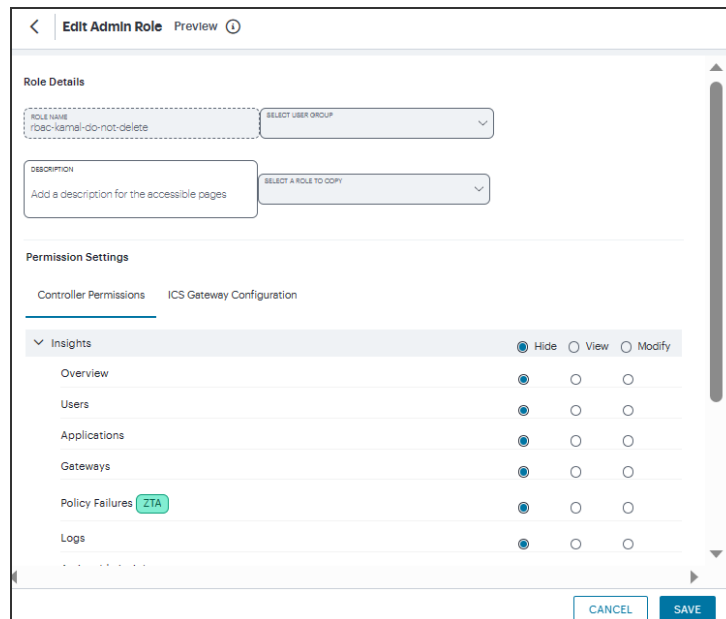


| ROLE NAME | DEFAULT | USER GROUP NAME | DESCRIPTION |
|---------------------------|-------------------------------------|-----------------|---|
| .Administrators | <input checked="" type="checkbox"/> | Administrators | All pages accessible |
| .CxOs | <input checked="" type="checkbox"/> | | Insights Dashboards, Logs , Reports & Subscriptions |
| .Network Administrators | <input checked="" type="checkbox"/> | | Gateways Overview and Logs only |
| .Read-Only Administrators | <input checked="" type="checkbox"/> | | All except Workflows , Subscriptions , Upgrade & Admin Role |
| dummy-role | <input type="checkbox"/> | | |
| rbac-kamal-do-not-delete | <input type="checkbox"/> | rbac | |
| rbac-zta-view-overview | <input type="checkbox"/> | test RBAC | testing bugs |
| test role 2 | <input type="checkbox"/> | | |
| test role 20 | <input type="checkbox"/> | | |
| test role 3 | <input type="checkbox"/> | | |

Admin Roles

3. Click the three dots adjacent to the role you want to update, then select **Edit Role**.

A dialog appears. For example:



Edit Admin Role Preview

Role Details

ROLE NAME: rbac-kamal-do-not-delete | SELECT USER GROUP: [Dropdown]

DESCRIPTION: Add a description for the accessible pages | SELECT A ROLE TO COPY: [Dropdown]

Permission Settings

Controller Permissions | ICS Gateway Configuration

Insights: Hide View Modify

| Permission | Hide | View | Modify |
|----------------------------|----------------------------------|-----------------------|-----------------------|
| Overview | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Users | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Applications | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Gateways | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Policy Failures ZTA | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Logs | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |

CANCEL SAVE

Edit Admin Roles

4. Under **Choose group**, select the user group that you want the admin group to be associated with.
5. Select **Save Changes**.
6. (Optional) Repeat steps 3 to 5 for each admin role.

Role-based Access Control for Admin Users

With Role-based access control (RBAC), organizations can easily add admins and assign them specific roles, with differing levels of access to the nSA Admin Portal. In addition to an existing set of default roles, Administrators can now create custom granular roles for specific functions within the nSA admin portal.

The following examples illustrate how an organization can leverage role-based administration for a variety of scenarios.

To create a custom admin role:

1. Log into the *Controller* as a Tenant Admin, see [Logging in as a Tenant Administrator](#).
2. From the *nZTA* menu, select **Administration**, then select **Admin Roles**.
3. In the Admin Roles page, click **Create Role**. The Create Admin Role page appears.

< **Create Admin Role** Preview ⓘ

Role Details

ROLE NAME SELECT USER GROUP
None

DESCRIPTION
Add a description for the accessible pages

SELECT A ROLE TO COPY

Permission Settings

Controller Permissions ICS Gateway Configuration

> Insights Hide View Modify

> Secure Access **ZTA** Hide View Modify

> Integrations **ZTA** Hide View Modify

> Administration Hide View Modify

CANCEL CREATE

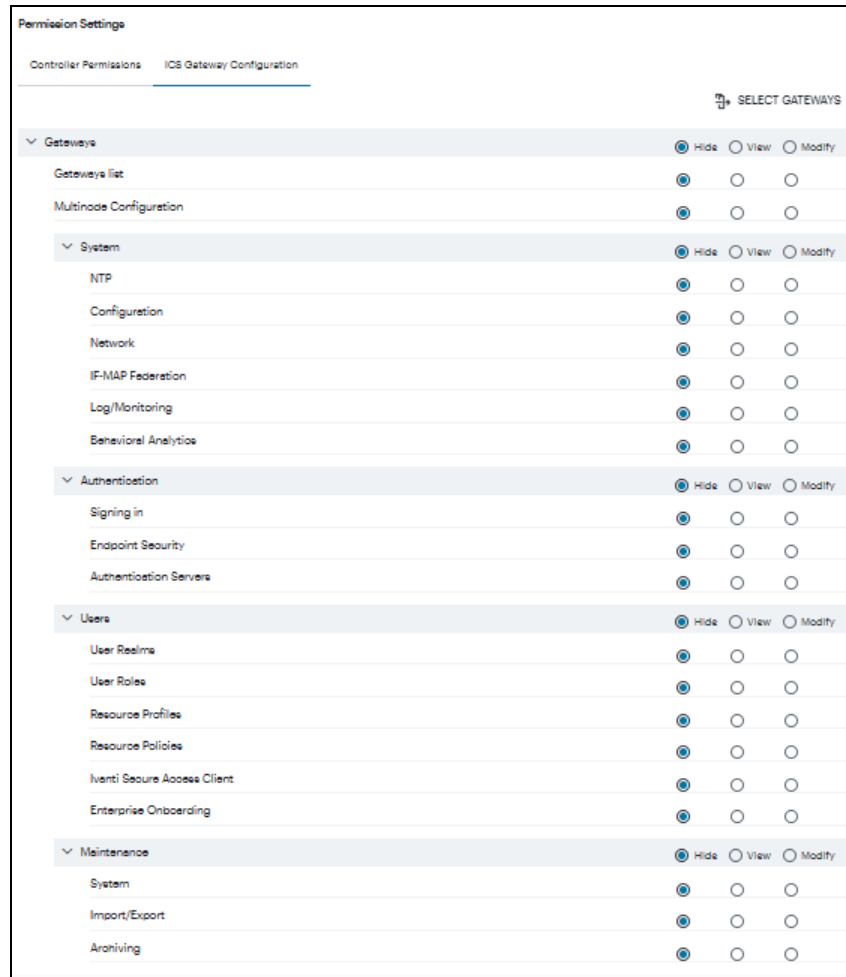
Create Admin Role

4. Enter a unique name for the role.
5. From the drop-down list, select the User Group that you want to associate with this role. For details, see ["Associating User Groups with Admin Roles" on page 73](#).
6. Optionally, enter a **Description**.
7. From the drop-down list, select an existing role that suits your requirements.
8. Under Permission Settings, the *Controller* Permissions list shows the list of resources. The resources specific to nZTA are tagged with **ZTA** and resources specific to ICS are tagged with **ICS**.

| Permission Settings | | | |
|-------------------------|-----|---------------------------------------|---|
| Controller Permissions | | ICS Gateway Configuration | |
| ▼ Insights | | <input checked="" type="radio"/> Hide | <input type="radio"/> View <input type="radio"/> Modify |
| Overview | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Users | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Applications | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Gateways | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Policy Failures | ZTA | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Logs | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Actionable Insights | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Reports | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Session Management | ICS | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| ▼ Secure Access | ZTA | <input checked="" type="radio"/> Hide | <input type="radio"/> View <input type="radio"/> Modify |
| Secure Access Policies | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Onboarding | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Manage Users | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Manage Devices | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Manage Applications | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Manage Gateways | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| ▼ Integrations | ZTA | <input checked="" type="radio"/> Hide | <input type="radio"/> View <input type="radio"/> Modify |
| CASB/SWG | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Enterprise Integrations | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| ▼ Administration | | <input checked="" type="radio"/> Hide | <input type="radio"/> View <input type="radio"/> Modify |
| Upgrade | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Admin Management | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Subscriptions | | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |
| Custom Geo IP | ZTA | <input checked="" type="radio"/> | <input type="radio"/> <input type="radio"/> |

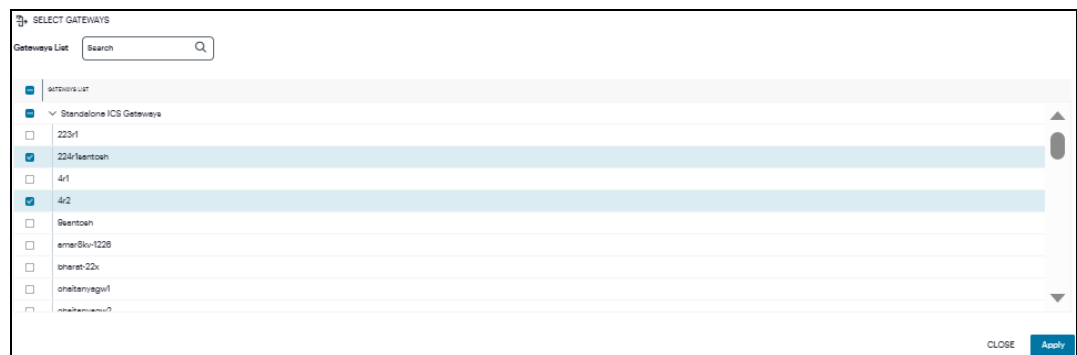
Controller Permissions

9. Select the Hide, View only, or Modify permissions for each resource and its attributes. This determines which pages to show and which actions to allow.
10. Under Permission Settings, the ICS Gateway Configuration list shows the list of ICS Gateway resources.



ICS Gateway Permissions

- Click **Select Gateways**. In the Select Gateways dialog, select one or more Gateways / Clusters from the list and click **Apply**.



Select Gateways/Clusters

- Select the Hide, View only, or Modify permissions for each resource and its attributes. This determines which pages to show and which actions to allow.

13. Click **Create**. The newly created custom admin role is displayed in the Admin Roles page.
14. (Optional) Edit an existing admin role by clicking the adjacent three dots, and then selecting **Edit**. Make any required updates and save the changes.
15. (Optional) Delete an unused custom admin rule by clicking the adjacent three dots, and then selecting **Delete**. You must confirm the deletion.

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](#)" on the next page.

Configuring Gateways

- ["Introduction" below](#)
- ["Workflow: Creating a Gateway in VMware vSphere" on page 84](#)
- ["Workflow: Creating a Gateway in Amazon Web Services" on page 93](#)
- ["Workflow: Creating a Gateway in Microsoft Azure" on page 103](#)
- ["Workflow: Creating a Gateway in KVM/OpenStack" on page 121](#)
- ["Workflow: Creating a Gateway in Google Cloud Platform" on page 136](#)
- ["Workflow: Creating a Gateway in Oracle Cloud Platform" on page 159](#)

Introduction



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.

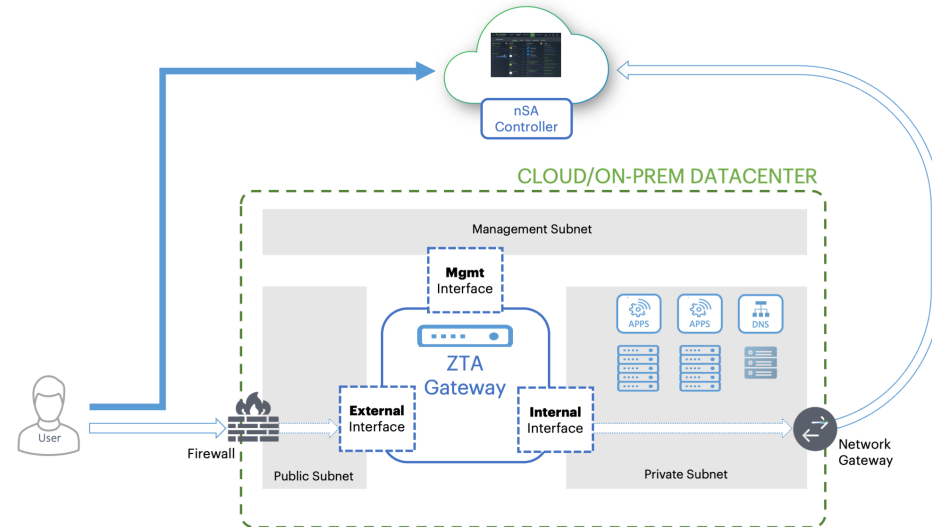
A **Gateway** is a virtual machine instance that you use to control access to your applications. You deploy Gateway instances at each location your applications reside - at a physical datacenter, a private or public cloud-based service, or some hybrid combination. Each Gateway communicates with the controller 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.



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.



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.



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)

- **UAE**

20.233.40.108 (port 443)

20.233.41.69 (port 443)

- **Canada:**

20.220.157.85 (port 443)

20.220.157.158 (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"](#) below.
- **Amazon Web Services (AWS):** see ["Workflow: Creating a Gateway in Amazon Web Services"](#) on page 93.
- **Microsoft Azure:** see ["Workflow: Creating a Gateway in Microsoft Azure"](#) on page 103.
- **KVM/OpenStack:** see ["Workflow: Creating a Gateway in KVM/OpenStack"](#) on page 121.
- **Google Cloud Platform:** see ["Workflow: Creating a Gateway in Google Cloud Platform"](#) on page 136.

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-22.6R1.2-569.1.zip>



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.



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.



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

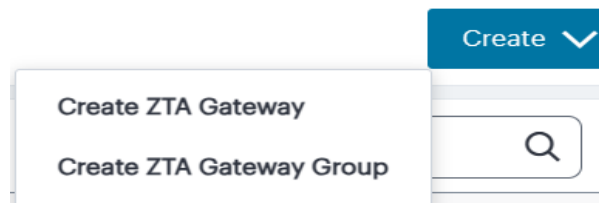
To set up a ZTA Gateway in VMware vSphere, perform the following steps:

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:



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

In both cases, the **Gateway Details** dialog appears.

Manage Gateways i

Gateways List
Gateway Selectors

Gateway Details

Gateway Information

Use Manual Settings

Gateway Network Settings

Use Management Port Use Dynamic Tunnel IP

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

Use Proxy Server for communication i

Proxy Server Settings

Add this Gateway to a group

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



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

2. (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.
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. For **Gateway Platform**, select "VMware vSphere".
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.



When the management port is enabled, the will Controller 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:

Gateway Network Settings

Use Management Port Use Dynamic Tunnel IP

Use Proxy Server for communication ⓘ

Proxy Server Settings

HOST: _____ PORT: 8080

USERNAME: _____ PASSWORD: _____

Custom IP Pool

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



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. (Optional) Select the **Use proxy server for communication** check box to enable nZTA to Controller communication via proxy server. Proxy is supported on both internal and management interfaces of the Gateway. Once enabled, enter host name and port. Optionally, if your proxy server requires further authentication, enter a username and password to log in to the proxy server.



Admin can configure proxy for existing Gateway after upgrading it to 22.4R3 version or later.

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

The image shows a network configuration panel with four main sections, each containing three input fields:

- Internal IP:** IP ADDRESS, SUBNET MASK, GATEWAY. Each field has a warning icon.
- Internal Network / Private Subnet:** PRIMARY DNS, SECONDARY DNS, DNS SEARCH DOMAIN. Each field has a warning icon.
- External IP:** IP ADDRESS, SUBNET MASK, GATEWAY. Each field has a warning icon.
- Management IP:** IP ADDRESS, SUBNET MASK, GATEWAY. No warning icons are present.

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.



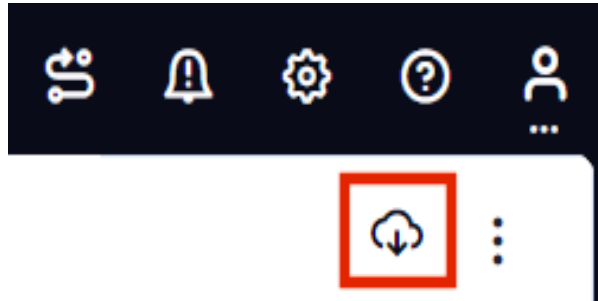
Management network settings are optional, unless the **Use Management Port** check box is selected.

- 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.

12. 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.

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



Retain this file for a later step.



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.

14. (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.
15. Access the *vSphere management interface*, either from a client or a web browser, and log in using your vSphere credentials.
16. In the vSphere console, start the *Deploy OVF Template* wizard to create a new virtual machine based on the nZTA vSphere Gateway template.

17. 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.

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 **VA IVE 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.

18. Locate the new Gateway virtual machine in the hosts and clusters.

19. Start the Gateway virtual machine by powering it on.

Wait until the boot up process is complete.

20. Return to the **Gateways List** page on the Controller.

21. Locate the new Gateway record in the list and confirm that its **Connection Status** has updated to *Connected*.



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/23-11-569/Nitro/ivanti-zta-2-nics-existing-vpc.json>
<https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-11-569/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/23-11-569/Nitro/ivanti-zta-2-nics-new-network.json>
<https://pulsezta.blob.core.windows.net/gateway/templates/AWS/23-11-569/Nitro/ivanti-zta-3-nics-new-network.json>



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



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.



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-22.6R1.2-569.1-SERIAL-nitro.img"
 5. Make a note of the corresponding AMI ID.

- Credentials for the AWS Management Console.



These credentials must include sufficient permissions to create a stack.

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

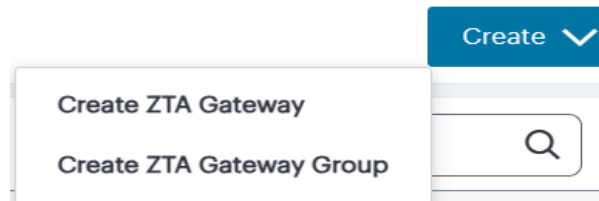
To set up a ZTA Gateway in AWS, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:

- On nZTA unconfigured systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
- On nZTA configured 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:



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

In both cases, the **Gateway Details** dialog appears.

Manage Gateways ?

Gateways List Gateway Selectors

Gateway Details

Gateway Information

NAME

PUBLIC ADDRESS or CNAME

COUNTRY STATE/REGION CITY

GATEWAY PLATFORM Use Manual Settings

Internal Network / Private Subnet

PRIMARY DNS SECONDARY DNS DNS SEARCH DOMAIN

Gateway Network Settings

Use Management Port

Use Proxy Server for communication ?

Proxy Server Settings

HOST PORT

USERNAME PASSWORD

Add this Gateway to a group

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

GATEWAY GROUP

CANCEL

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

2. Enter a **Name** for the Gateway.
3. 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.
4. Select a geographic **Location** for the Gateway.

5. For **Gateway Platform**, select "Amazon Web Services".
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.



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 proxy server for communication** check box to enable nZTA to Controller communication via proxy server. Proxy is supported on both internal and management interfaces of the Gateway. Once enabled, enter host name and port. Optionally, if your proxy server requires further authentication, enter a username and password to log in to the proxy server.



Admin can configure proxy for existing Gateway after upgrading it to 22.4R3 version or later.

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.

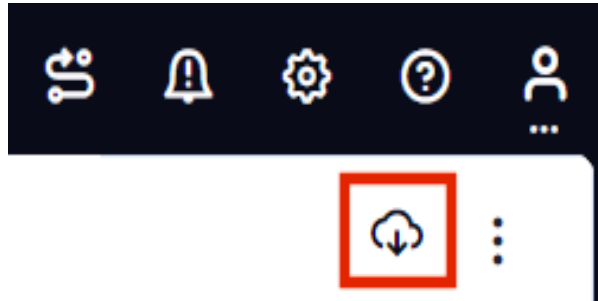


Make sure the specified DNS service can resolve the IP address of your Controller. Issues here can cause registration of the Gateway with the Controller to fail.

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

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

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



Retain this file for a later step.



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.

14. (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.
15. Access the *AWS Management Console* and log in using your AWS credentials.
16. In the AWS **Services** menu, select **CloudFormation**.

The **CloudFormation** home page appears.
17. Click **Create Stack** and then, from the sub-menu, select **With new resources (standard)**.

The **Specify template** step of the **Create Stack** wizard appears.
18. Under **Prerequisite - prepare template**, select the **Template is ready** option.
19. Under **Specify Template**, select the **Upload a template file** template source option.
20. 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.

21. 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.

22. Enter a **Stack name**.

23. 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 Technical Support.

24. 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.

25. For **Instance Type**, select the instance type that fits your hypervisor choice (Nitro) and minimum requirements, based on the following recommended types:

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)

26. Under **nZTA Config Data**, paste in the raw text of the Gateway definition file downloaded earlier.

27. For **SSH Key Name**, specify your existing SSH key pair name.

28. 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.


 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.

 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.

 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*.

29. 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.

30. Click **Next**.

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

32. Confirm all displayed details.

33. 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`.

34. Wait for the status of the new stack to reach `CREATE_COMPLETE`.

35. *(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.

36. 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*.



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*.



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



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.



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.



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:



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/23-11-569/ivanti-zta-2-nics.json>

<https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-11-569/ivanti-zta-3-nics.json>

To deploy in an existing VNET:

<https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-11-569/ivanti-zta-2-nics-existing-vnet.json>

<https://pulsezta.blob.core.windows.net/gateway/templates/Azure/23-11-569/ivanti-zta-3-nics-existing-vnet.json>



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-22.6R1.2-569.1-SERIAL-hyperv.vhd>
 - **APJ:** <https://pulseztaapj1.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.6R1.2-569.1-SERIAL-hyperv.vhd>
 - **Europe:** <https://pulseztaeurope.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.6R1.2-569.1-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.



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.

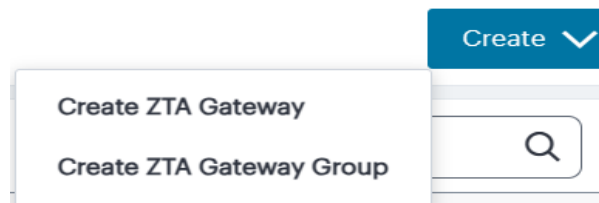
To create a Gateway record in the Controller, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:

- On nZTA unconfigured systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
- On nZTA configured 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:



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

In both cases, the **Gateway Details** dialog appears.

Manage Gateways ⓘ

Gateways List Gateway Selectors

Gateway Details

Gateway Information

NAME

PUBLIC ADDRESS or CNAME

COUNTRY STATE/REGION CITY

GATEWAY PLATFORM Use Manual Settings

Internal Network / Private Subnet

PRIMARY DNS SECONDARY DNS DNS SEARCH DOMAIN

Gateway Network Settings

Use Management Port

Use Proxy Server for communication ⓘ

Proxy Server Settings

HOST PORT

USERNAME PASSWORD

Add this Gateway to a group

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

GATEWAY GROUP

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

2. Enter a **Name** for the Gateway.

3. 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.



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](#)" on [page 110](#).

4. Select a geographic **Location** for the Gateway.
5. For **Gateway Platform**, select "Azure".
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.



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 proxy server for communication** check box to enable nZTA to Controller communication via proxy server. Proxy is supported on both internal and management interfaces of the Gateway. Once enabled, enter host name and port. Optionally, if your proxy server requires further authentication, enter a username and password to log in to the proxy server.



Admin can configure proxy for existing Gateway after upgrading it to 22.4R3 version or later.

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

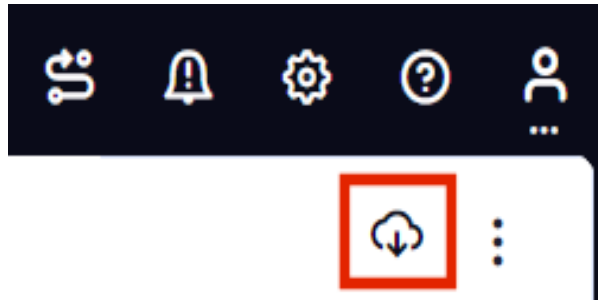
11. Enter the DNS Search Domain for the Gateway.

 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.

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



Retain this file for a later step.


 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.

14. (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](#)" on the next page.
- To create an instance using the nZTA template and image files, see "[Creating a Gateway using the Azure Template and Image Files](#)" on page 115.

Creating a Gateway through Azure Marketplace

 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 a Gateway using the Azure Template and Image Files](#)" on page 115 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)

 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.

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.



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.



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.



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 a 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.

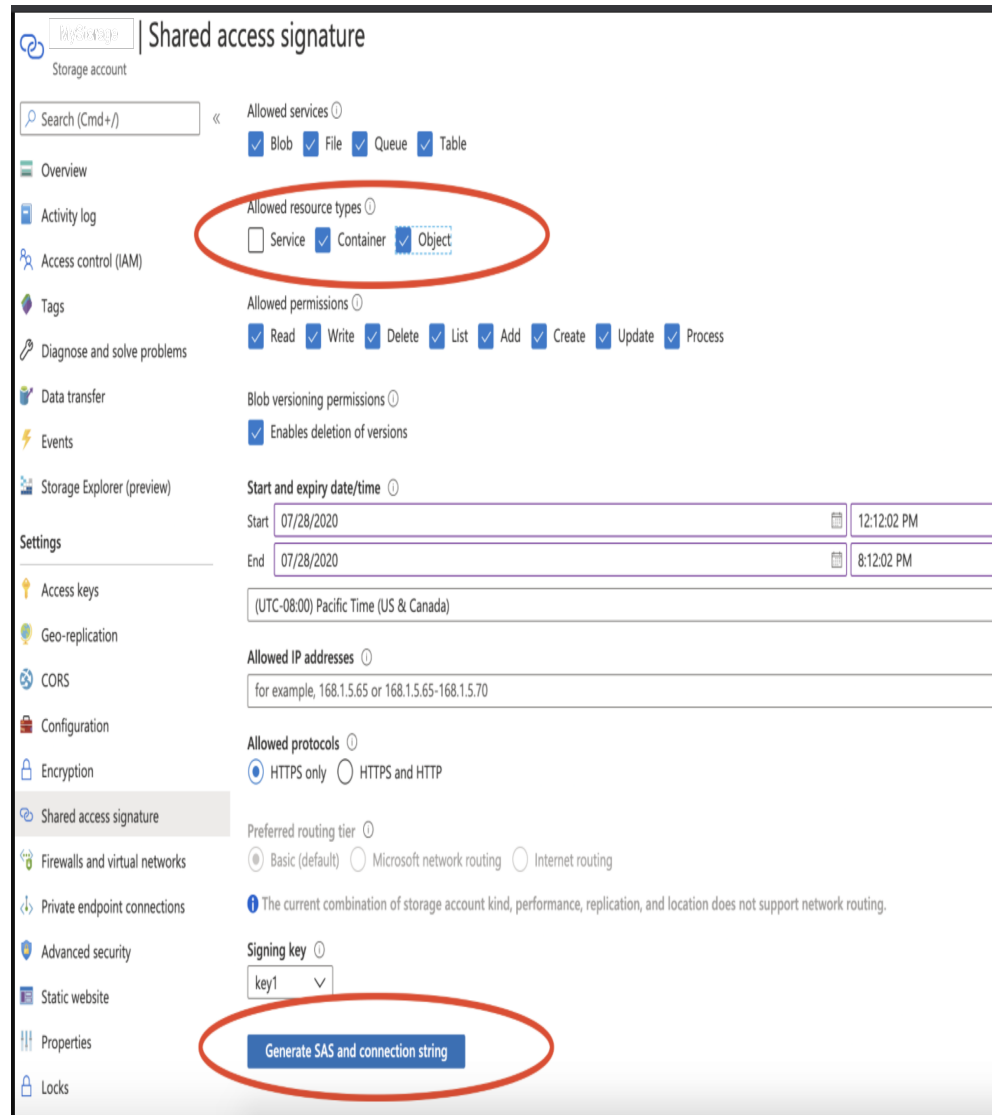
- Download the nZTA Azure VHD image file for your region and copy it to the storage account you created in the previous step.

Choose to download from the following regions:

- **Americas:** <https://pulsezta.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.6R1.2-569.1-SERIAL-hyperv.vhd>
- **APJ:** <https://pulseztaapj1.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.6R1.2-569.1-SERIAL-hyperv.vhd>
- **Europe:** <https://pulseztaeurope.blob.core.windows.net/gateway/ISA-V-HYPERV-ZTA-22.6R1.2-569.1-SERIAL-hyperv.vhd>

For this process, you can use *azcopy*:

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



The screenshot shows the 'Shared access signature' configuration page for a storage account. The 'Allowed resource types' section is circled in red, showing 'Container' and 'Object' selected. The 'Generate SAS and connection string' button at the bottom is also circled in red.

Storage account

Search (Cmd+/) «

Allowed services ○

- Blob
- File
- Queue
- Table

Allowed resource types ○

- Service
- Container
- Object

Allowed permissions ○

- Read
- Write
- Delete
- List
- Add
- Create
- Update
- Process

Blob versioning permissions ○

- Enables deletion of versions

Start and expiry date/time ○

| | | |
|-------|------------|-------------|
| Start | 07/28/2020 | 12:12:02 PM |
| End | 07/28/2020 | 8:12:02 PM |

(UTC-08:00) Pacific Time (US & Canada)

Allowed IP addresses ○

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ○

- HTTPS only
- HTTPS and HTTP

Preferred routing tier ○

- Basic (default)
- Microsoft network routing
- Internet routing

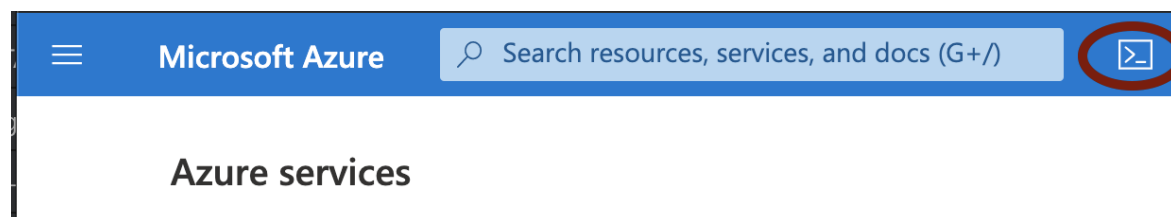
The current combination of storage account kind, performance, replication, and location does not support network routing.

Signing key ○

key1

Generate SAS and connection string

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



Microsoft Azure

Search resources, services, and docs (G+)

Azure services

Open 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/ISA-V-
HYPERV-ZTA-22.6R1.2-569.1-SERIAL-hyperv.vhd'
'https://MyStorage.blob.core.windows.net/gateway/ISA-V-HYPERV-
ZTA-22.6R1.2-569.1-SERIAL-hyperv.vhd?sv=2023-09-
12&ss=bfqt&srt=co&sp=rwldacupx&se=2019-12-29T02:57:39Z&st=2020-
07-
28T18:57:39Z&spr=https&sig=mJU7WNd9oNY7wcXNOqEOhbYshD9Sxv56rqE1%2
FmEuCg4%3D'
```

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



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.



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.


 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.

 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.

 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 *ZTA 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 Process** 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.



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](#)" on [the next page](#).
- Creating the gateway record in the Controller, see "[Adding a KVM Gateway in nSA](#)" on [page 123](#).
- Preparing Metadata for OpenStack, see "[Preparing Metadata for OpenStack](#)" on [page 127](#).

- Creating the KVM Gateway virtual machine instance in OpenStack, see "[Creating the KVM Gateway Virtual Machine Instance in OpenStack](#)" on page 130.

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-22.6R1.2-569.1.zip>



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.



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.



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" below](#).

Adding a KVM Gateway in nSA

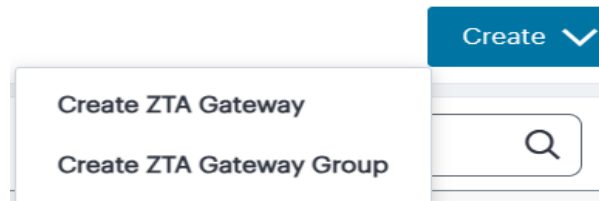
To set up a nZTA KVM Gateway, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:

- On nZTA unconfigured systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
- On nZTA configured 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:



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

In both cases, the **Gateway Details** dialog appears.

Manage Gateways ?

Gateways List
Gateway Selectors

Gateway Details

ADD

Use Manual Settings

Internal Network / Private Subnet

Gateway Network Settings

Use Management Port
 Use Dynamic Tunnel IP

ADD

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

Use Proxy Server for communication ?

Proxy Server Settings

Add this Gateway to a group

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

[CREATE GATEWAY GROUP](#)

[CANCEL](#)



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

2. Enter a **Name** for the Gateway.
3. 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.
4. Select a geographic **Location** for the Gateway.

5. For **Gateway Platform**, select "KVM".
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.



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:

Gateway Network Settings

Use Management Port Use Dynamic Tunnel IP

Use Proxy Server for communication ⓘ

Proxy Server Settings

HOST PORT 8080

USERNAME PASSWORD

Custom IP Pool

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



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. (Optional) Select the **Use proxy server for communication** check box to enable nZTA to Controller communication via proxy server. Proxy is supported on both internal and management interfaces of the Gateway. Once enabled, enter host name and port. Optionally, if your proxy server requires further authentication, enter a username and password to log in to the proxy server.



Admin can configure proxy for existing Gateway after upgrading it to 22.4R3 version or later.

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



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.

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

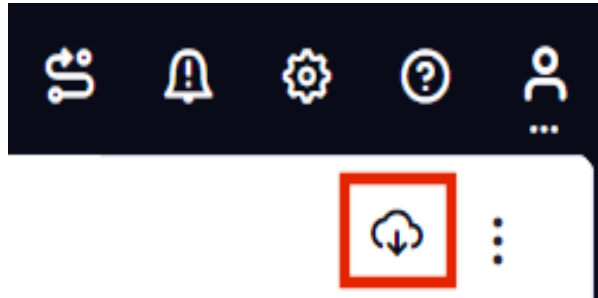
After you complete the first part of this workflow, an unregistered Gateway record is created on the Controller. This Gateway record can be seen on the **Gateways > Gateways List** page.

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

Preparing Metadata for OpenStack

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

1. Log into and nZTA 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.



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



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>
<secondary-dns>
<insert vaSecondaryDNS here>
</secondary-dns>
<primary-dns>
<insert vaPrimaryDNS here>
</primary-dns>
<dns-domain>
<insert vaDnsSearchDomain here>
</dns-domain>
</appliance-id>
<cert-common-name>
<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>
```



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](#)" below.

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*.



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 *ISA4000-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.



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.



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.



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" on page 123](#).

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.



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" on page 123](#).

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*.

 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 | |

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.

 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 | ext-port-2 5.5.10.64, 10.96.145.196 int-port-2 4.4.10.83, 10.96.145.156 | |

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)

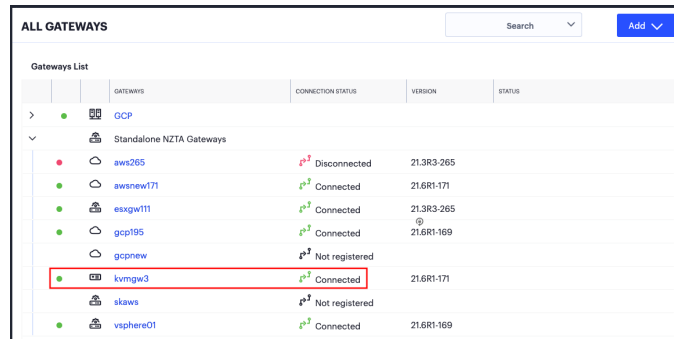
Licensing Hardware ID: UASPHYI7PLEU7F0MS

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:

```

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 | | |
| | lvmgw3 | Connected | 21.6R1-171 | |
| | skaws | Not registered | | |
| | vsphere01 | Connected | 21.6R1-169 | |



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 *ICS 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" on the next page](#).
- Creating the gateway record in the Controller, see ["Adding a GCP Gateway in nSA" on page 141](#).
- Downloading Metadata for Google Cloud Platform, see ["Downloading Metadata for Google Cloud Platform" on page 145](#).
- Uploading the GCP Image onto the Google Cloud Platform, see ["Uploading the GCP Virtual Machine Image onto the Google Cloud Platform" on page 146](#).
- 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" on page 148](#).
 - 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" on page 155](#).

- Completing the Configuration of the Controller, see "[Completing the Configuration of the Controller](#)" on page 158.

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.



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 with the Controller allocated public IP address afterwards.

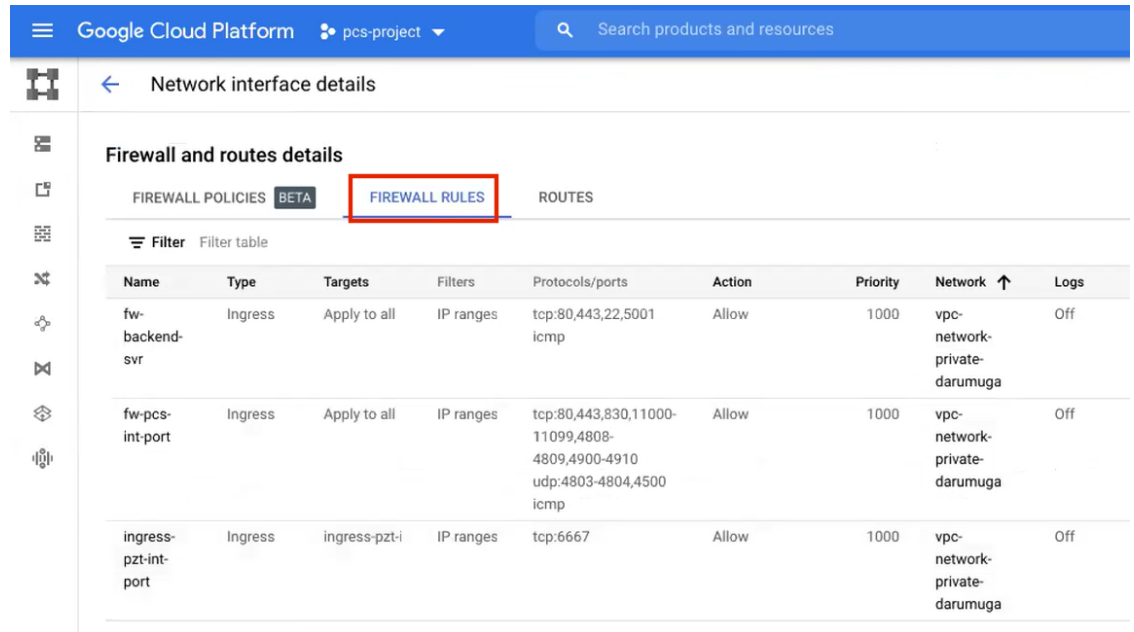
- The Gateway geographic location.
- (Optional) The name of the *Gateway Group* to which you want to add this new Gateway record. To learn more about Gateway Groups, see the *Tenant Admin Guide*.



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.

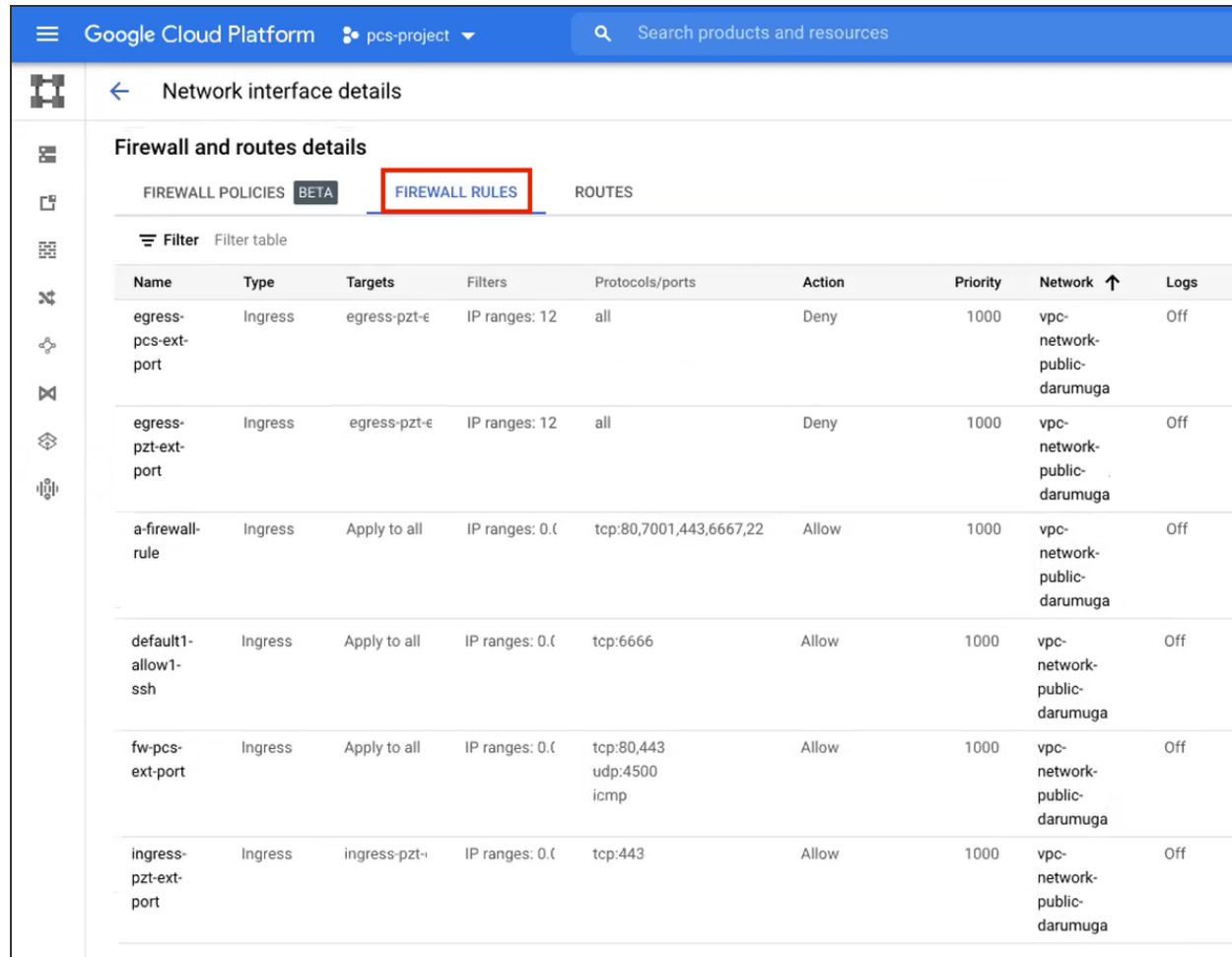


The screenshot shows the Google Cloud Platform interface for configuring Firewall Rules. The page title is "Network interface details". Under the "Firewall and routes details" section, the "FIREWALL RULES" tab is selected and highlighted with a red box. Below the tabs, there is a "Filter" button and a "Filter table" link. A table lists three 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 |

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.

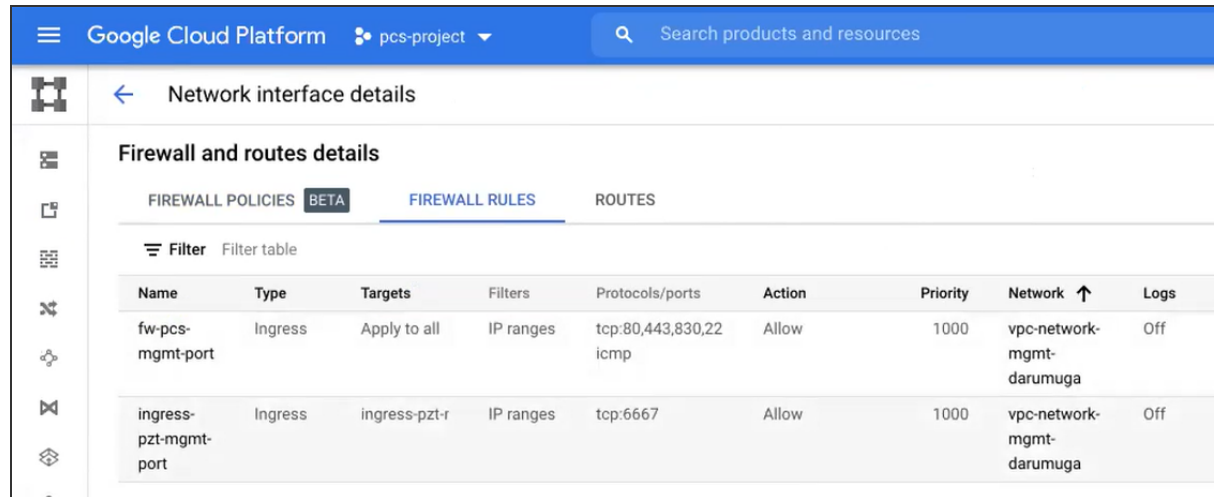


The screenshot shows the Google Cloud Platform console for a network interface. The 'Firewall and routes details' section is active, with 'FIREWALL RULES' highlighted. A table lists several firewall rules with columns for Name, Type, Targets, Filters, Protocols/ports, Action, Priority, Network, and Logs.

| Name | Type | Targets | Filters | Protocols/ports | Action | Priority | Network | Logs |
|----------------------|---------|---------------|----------------|--------------------------------|--------|----------|-----------------------------|------|
| egress-pcs-ext-port | Ingress | egress-pzt-e | IP ranges: 12 | all | Deny | 1000 | vpc-network-public-darumuga | Off |
| egress-pzt-ext-port | Ingress | egress-pzt-e | IP ranges: 12 | all | Deny | 1000 | vpc-network-public-darumuga | Off |
| a-firewall-rule | Ingress | Apply to all | IP ranges: 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 | tcp:6666 | Allow | 1000 | vpc-network-public-darumuga | Off |
| fw-pcs-ext-port | Ingress | Apply to all | IP ranges: 0.0 | tcp:80,443 udp:4500 icmp | Allow | 1000 | vpc-network-public-darumuga | Off |
| ingress-pzt-ext-port | Ingress | ingress-pzt-i | IP ranges: 0.0 | tcp:443 | Allow | 1000 | vpc-network-public-darumuga | Off |

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.



The screenshot shows the Google Cloud Platform console interface for a network interface. The main section is titled "Firewall and routes details" and has three tabs: "FIREWALL POLICIES BETA", "FIREWALL RULES", and "ROUTES". The "FIREWALL RULES" tab is active. Below the tabs is a "Filter" section with a "Filter table" link. A table lists two firewall 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 |

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-22.6R1.2-569.1.tar.gz>



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.



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/23-11-569/ivanti-zta-2-nics-existing-vpc.zip> <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-11-569/ivanti-zta-3-nics-existing-vpc.zip>
 - To deploy in a new VPC:
<https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-11-569/ivanti-zta-2-nics-new-vpc.zip>
<https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-11-569/ivanti-zta-3-nics-new-vpc.zip>
-



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.
-



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](#)" below.

Adding a GCP Gateway in nSA

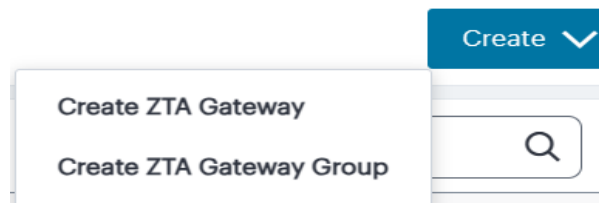
To set up a nZTA GCP Gateway, perform the following steps:

1. Log into the Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:

- On nZTA unconfigured systems, the **Secure Access Setup** (Onboarding) wizard appears. In this case, click **Add Gateway**.
- On nZTA configured 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:



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

In both cases, the **Gateway Details** dialog appears.

Manage Gateways ⓘ

Gateways List Gateway Selectors

Gateway Details

Gateway Information

NAME

PUBLIC ADDRESS or CNAME

COUNTRY STATE/REGION CITY

GATEWAY PLATFORM Use Manual Settings

Internal Network / Private Subnet

PRIMARY DNS SECONDARY DNS DNS SEARCH DOMAIN

Gateway Network Settings

Use Management Port

Use Proxy Server for communication ⓘ

Proxy Server Settings

HOST PORT

USERNAME PASSWORD

Add this Gateway to a group

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

GATEWAY GROUP

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

2. Enter a **Name** for the Gateway.

3. 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.



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.

4. Select a geographic **Location** for the Gateway.
5. For **Gateway Platform**, select "Google Cloud Platform".
6. (Optional) Select a Gateway **Group** to which the new Gateway is to be added.



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.



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 proxy server for communication** check box to enable nZTA to Controller communication via proxy server. Proxy is supported on both internal and management interfaces of the Gateway. Once enabled, enter host name and port. Optionally, if your proxy server requires further authentication, enter a username and password to log in to the proxy server.



Admin can configure proxy for existing Gateway after upgrading it to 22.4R3 version or later.

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.



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**.

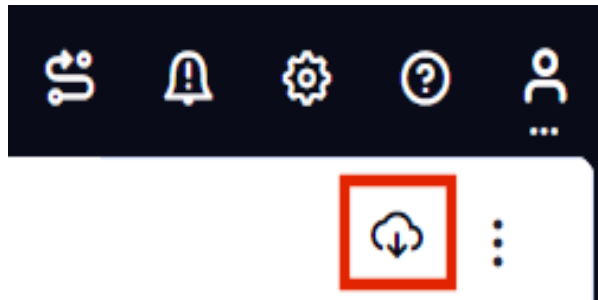
By completing the **Gateway Details** workflow, an unregistered Gateway record is created on the Controller. You can view this Gateway record on the **Gateways > Gateways List** page.

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

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.



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



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](#)" below.

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:



3. Click the **Navigation** menu, and then select **Cloud Storage > Browser**.

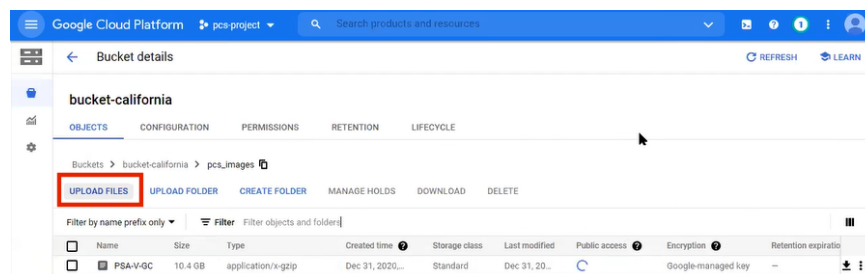
A list of GCP storage buckets appears.

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:



An upload dialog appears.

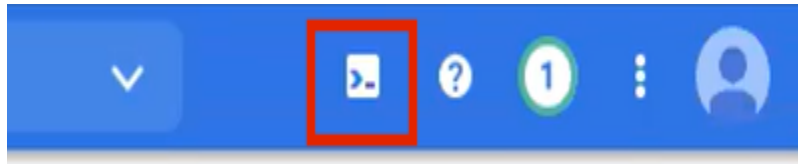
7. Select the `.tar` image file archive downloaded from <https://pulsezta.blob.core.windows.net/gateway/ISA-V-GCP-ZTA-22.6R1.2-569.1.tar.gz>, and click **Open**.



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"](#) on page 155), 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:



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
```

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

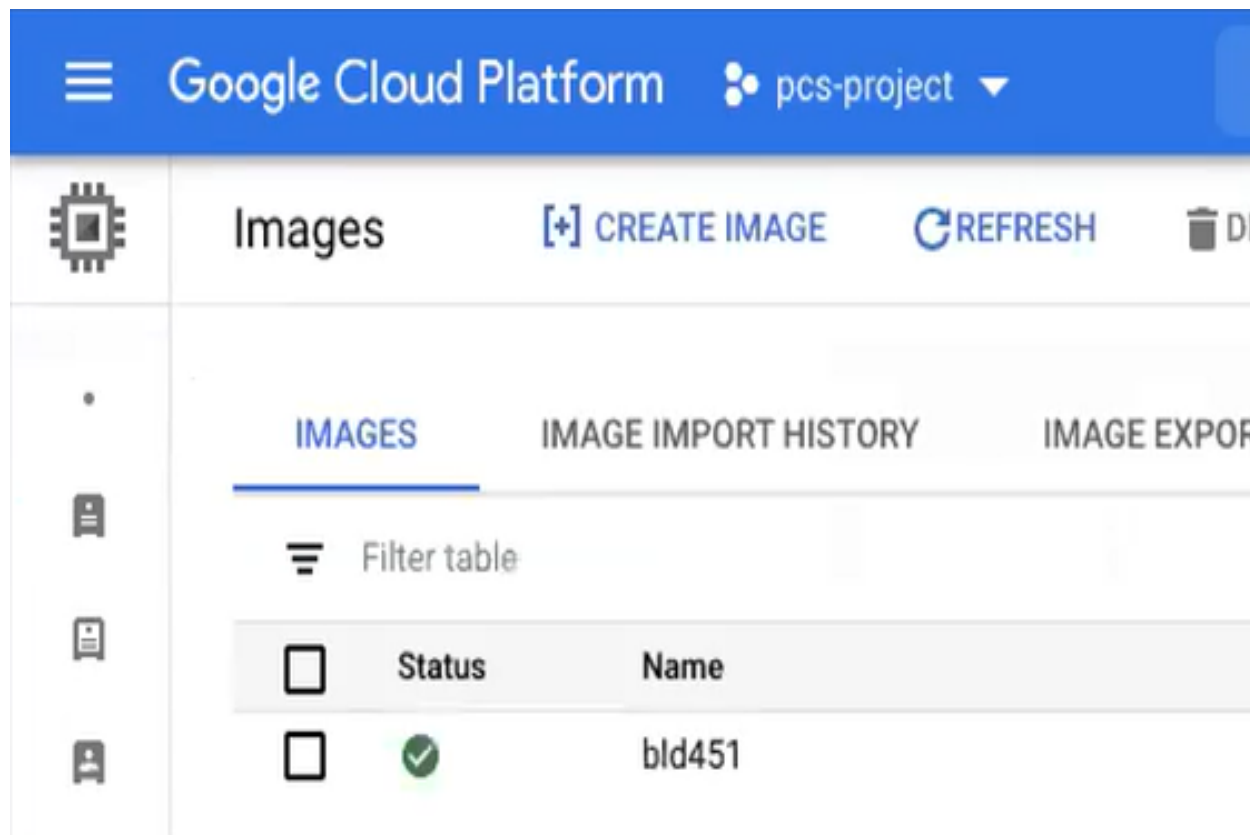
- Perform the task manually, see ["Creating a VM Instance of the Uploaded GCP Image Manually"](#) on the next page.
- Perform the task with a script/template, see ["Creating a VM Instance of the Uploaded GCP Image Using a Script/Template"](#) on page 155.

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"](#) on page 155.

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

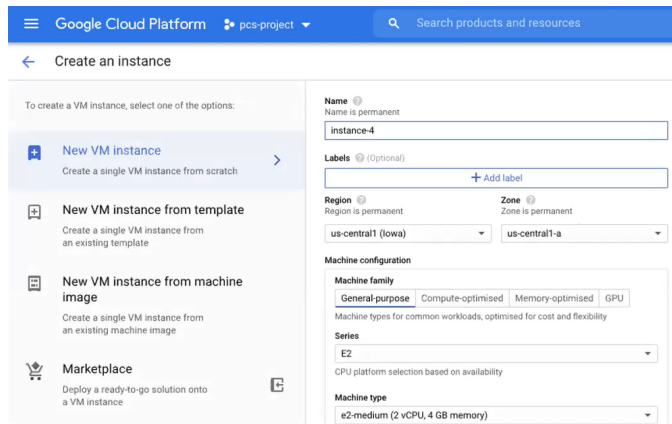
The **Images** page appears. For example:



2. Locate the new image in the list of images.

- At the end of the image entry, click the action menu and select **Create Instance**.

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



The screenshot displays the Google Cloud Platform interface for creating a VM instance. The top navigation bar includes the Google Cloud Platform logo, the project name 'pcs-project', and a search bar. The main heading is 'Create an instance'. On the left, there are four options: 'New VM instance' (highlighted), 'New VM instance from template', 'New VM instance from machine image', and 'Marketplace'. The right-hand side shows the configuration details for the selected 'New VM instance' option. The 'Name' field is 'instance-4'. The 'Region' is 'us-central1 (Iowa)' and the 'Zone' is 'us-central1-a'. Under 'Machine configuration', the 'Machine family' is 'General-purpose', the 'Series' is 'E2', and the 'Machine type' is 'e2-medium (2 vCPU, 4 GB memory)'.

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.

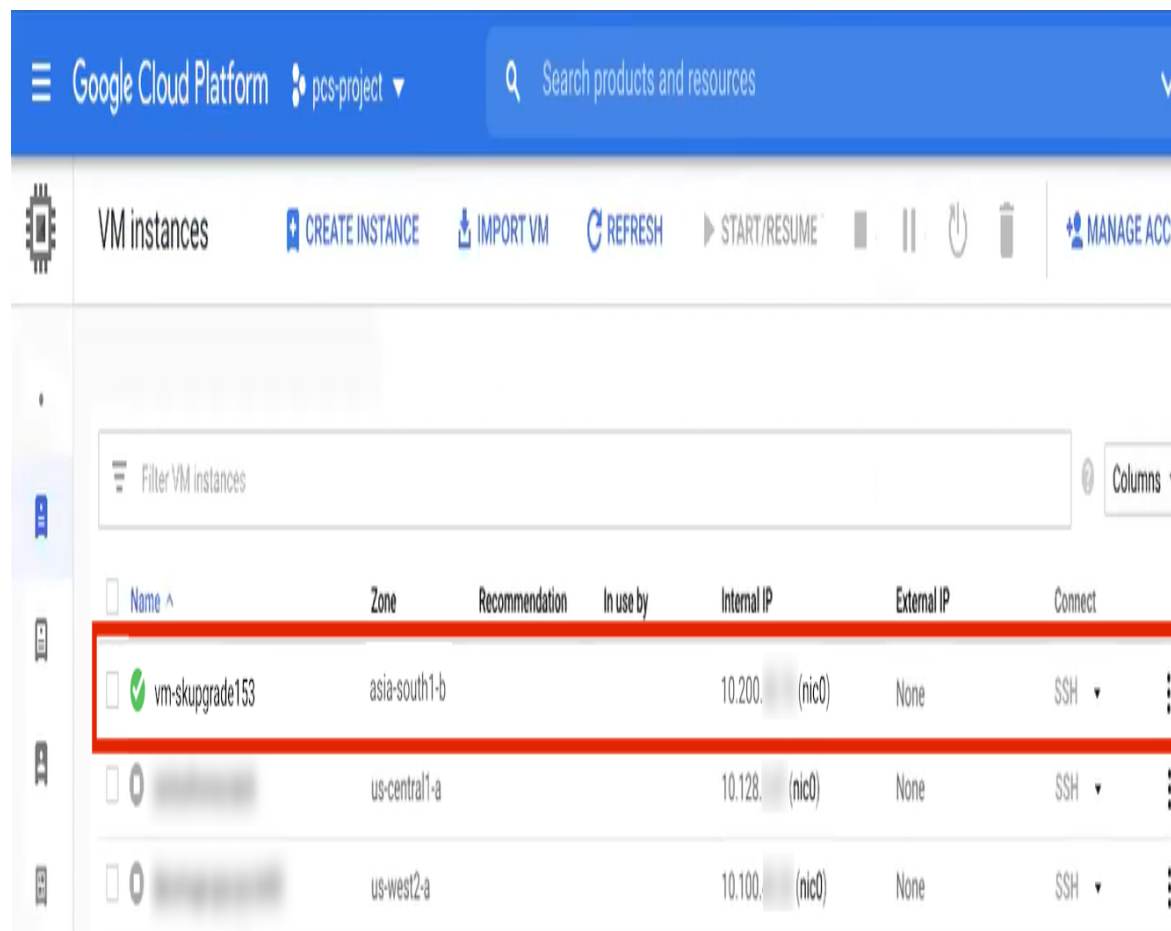
The **Network interface** options appear.

- 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:



5. On the **VM Instances** page, wait until the creation of the VM instance completes. This may take several minutes.

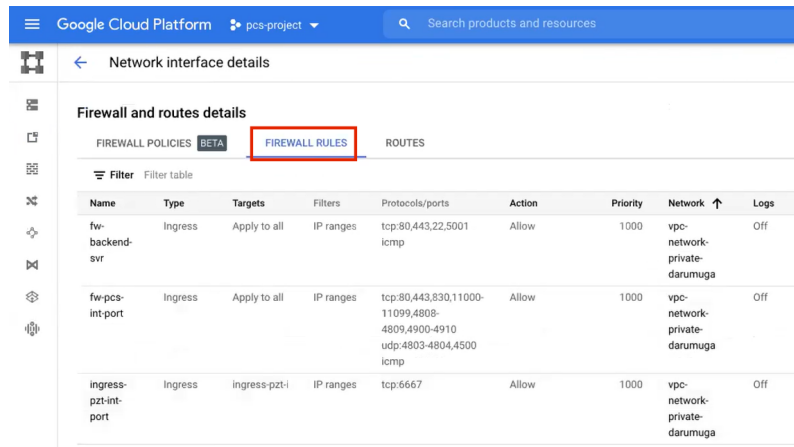
6. After the VM instance is created, click on it in the list of VM instances.

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.

- 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.

The screenshot shows the Google Cloud Platform interface for a network interface. The 'Firewall and routes details' section is active, with the 'FIREWALL RULES' tab selected and highlighted by a red box. Below the tabs is a table of firewall rules. The table has columns for Name, Type, Targets, Filters, Protocols/ports, Action, Priority, Network, and Logs. Three rules are listed: 'fw-backend-svr', 'fw-pcs-int-port', and 'ingress-pzt-int-port'.

| 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-l | IP ranges | tcp:6667 | Allow | 1000 | vpc-network-private-darumuga | Off |

- 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.

The screenshot shows the Google Cloud Platform interface for network interface details. The 'Firewall and routes details' section is active, with the 'FIREWALL RULES' tab selected. A table lists several firewall rules:

| Name | Type | Targets | Filters | Protocols/ports | Action | Priority | Network | Logs |
|----------------------|---------|---------------|----------------------|--------------------------------|--------|----------|-----------------------------|------|
| egress-pcs-ext-port | Ingress | egress-pzt-e | IP ranges: 12 | all | Deny | 1000 | vpc-network-public-darumuga | Off |
| egress-pzt-ext-port | Ingress | egress-pzt-e | 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-e | IP ranges: 0.0.0.0/0 | tcp:443 | Allow | 1000 | vpc-network-public-darumuga | Off |

- (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 network interface details. The 'Firewall and routes details' section is active, with the 'FIREWALL RULES' tab selected. A table lists several firewall 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 |

- 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: VASPH80EQ02HBPTE$

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:
```

You can then complete this process by updating the Gateway details on the Controller, see "[Completing the Configuration of the Controller](#)" on page 158.

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](#)" on page 148.

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/23-11-569/ivanti-zta-2-nics-existing-vpc.zip> <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-11-569/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/23-11-569/ivanti-zta-2-nics-new-vpc.zip> <https://pulsezta.blob.core.windows.net/gateway/templates/GCP/23-11-569/ivanti-zta-3-nics-new-vpc.zip>



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  
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
```



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:



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" below](#).

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.



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" on page 141](#).

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.



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 *ICS Tenant Admin Guide* for details.

Workflow: Creating a Gateway in Oracle Cloud Platform

This workflow leads you through the processes for setting up a Gateway on the Oracle Cloud Platform (OCI).

These processes must be performed in sequence:

- Preparing to create an Oracle gateway, see "[Preparing to Create an Oracle Gateway](#)" below.
- Creating the gateway record in the Controller, see "[Adding an Oracle Gateway](#)" on the next page.
- Downloading Metadata for Oracle Cloud Platform, see "[Downloading Metadata for Oracle Cloud Platform](#)" on page 163.
- Uploading the Oracle Image onto the Oracle Cloud Platform, see "[Uploading the Oracle Virtual Machine Image onto the Oracle Cloud Platform](#)" on page 164.
- Creating a VM Instance of the OCI image:
 - Creating a VM Instance of the Uploaded Oracle Image Using a Script/Template, see "[Creating a VM Instance of the Uploaded OCI Image Using Terraform Script](#)" on page 168.
 - Refer Terraform Configurations for details on the configuration, see "[Terraform Configurations](#)" on page 170.
- Creating a VM Instance of the Uploaded OCI Image Using any Other Methods, see "[Creating a VM Instance of the Uploaded OCI Image Using any Other Methods](#)" on page 256

Preparing to Create an Oracle 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.

If you want Oracle Cloud platform to allocate 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.

- 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 "[Configuring Gateways](#)" on page 80.

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

- The ZTA Gateway Oracle virtual machine image:
<https://pulsezta.blob.core.windows.net/gateway/ISA-V-OCI-ZTA-22.6R1.2-569.1.zip>

Download a copy of the Oracle Gateway image as a compressed zip archive file, then decompress the archive to a local workstation. Make sure that the resulting file set is accessible from the Oracle Cloud Platform Console.

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

- (Optional) Oracle Gateway deployment scripts, suitable for automating the creation of your Oracle VM instances.

Template files: <https://pulsezta.blob.core.windows.net/gateway/templates/OCI/Terraform.zip>

- Credentials for the Oracle Cloud Platform Console.

These credentials must include sufficient permissions to create a virtual machine using terraform scripts.

- The primary (and optional secondary) DNS server IP address, and search domain.

Adding an Oracle Gateway

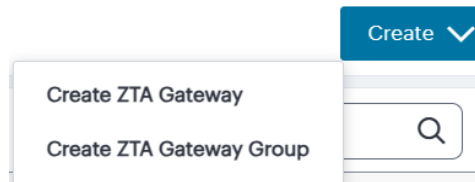
To register a Gateway on your Controller, use the Gateway Details dialog. To begin, log into the Controller Tenant Admin Portal using the credentials provided in your welcome email. Two outcomes are possible:

- On unconfigured nZTA systems, the Secure Access Setup Onboarding wizard appears (see [Working with the Onboarding Wizard](#)). In this case, click **Add Gateway**.

- On configured nZTA systems, the Network Overview page appears. In this case:
 1. From the nZTA menu, click the Secure Access icon, then select **Manage Gateways**.

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

2. To add a new Gateway, select **Create** from the top-right.
3. From the drop-down menu, click **Create ZTA Gateway**.



The Gateway Details dialog appears.

A screenshot of the Gateway Details dialog in the Manage Gateways interface. The dialog is titled 'Gateway Details' and contains the following sections:

- Gateway Information**: Includes input fields for NAME, PUBLIC ADDRESS or CNAME (with an ADD button), and dropdown menus for COUNTRY (Select a Country), STATE/REGION (Select a State/Region), and CITY (Select a City).
- Gateway Platform**: Includes a dropdown menu for GATEWAY PLATFORM (Oracle Cloud Platform) and a checkbox for Use Manual Settings.
- Internal Network / Private Subnet**: Includes input fields for PRIMARY DNS, SECONDARY DNS, and DNS SEARCH DOMAIN.
- Gateway Network Settings**: Includes checkboxes for Use Management Port and Use Proxy Server for communication (with a help icon).
- Add this Gateway to a group**: Includes a sub-section with the text 'Add gateway to any of the predefined gateway group or create a new gateway group'.

Enter the following details:

1. Enter a **Name** for the Gateway.
2. Enter one or more **Public Address or CNAME** (Public IP address or CNAME) for the Gateway.

3. Select **Add** to add each entry to the list. To learn more about this setting, see "[Configuring Gateways](#)" on page 80.

If you want Oracle 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 Oracle VM instance is created (if it is not updated automatically).

4. Select the geographic location details for the Gateway.
5. For Gateway Platform, select **Oracle Cloud Platform**.
6. Enter the Primary DNS IP address for the Gateway.
7. (Optional) Enter the Secondary DNS IP address for the Gateway.
8. Enter the DNS Search Domain for the Gateway.
9. (Optional) Select the **Use Management Port** check box to use management network ports for nZTA traffic rather than internal ports.

When the management port is enabled, Gateway will use management interface to communicate with Controller and NTP Server.

The Gateway will still use the internal port for DNS resolution and NTP server name resolution.

If the internal DNS cannot resolve the Controller domain, the internal interface will require internet access.

10. (Optional) Select the **Use proxy server for communication** check box to enable nZTA to Controller communication via proxy server.

Proxy is supported on both internal and management interfaces of the Gateway. Once enabled, enter host name and port.

Optionally, if your proxy server requires further authentication, enter a username and password to log in to the proxy server.

11. (Optional) Select a Gateway Group to which the new Gateway is to be added. To learn more about Gateway Groups, see "[Configuring Gateways](#)" on page 80.

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

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

You can now download your metadata, see "[Downloading Metadata for Oracle Cloud Platform](#)" below.

In case of registration failure due to Gateway configuration mistakes in firewall rules, DNS, etc., you can re-register the gateway. It does not require re-deploying of Gateway.

Downloading Metadata for Oracle Cloud Platform

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

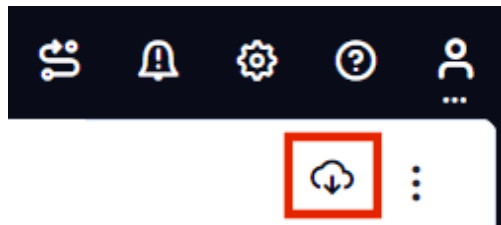
1. Log into the Controller as a Tenant Admin, see [Logging in as a Tenant Administrator](#).
2. From the nZTA menu, click the Secure Access icon, then select **Manage Gateways > Gateways List**.

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

3. Locate and select your Oracle cloud Gateway.

The Gateways Overview page appears.

4. Click the Download icon, then choose **Download gateway init config** to obtain a copy of the Gateway definition file.



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

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.

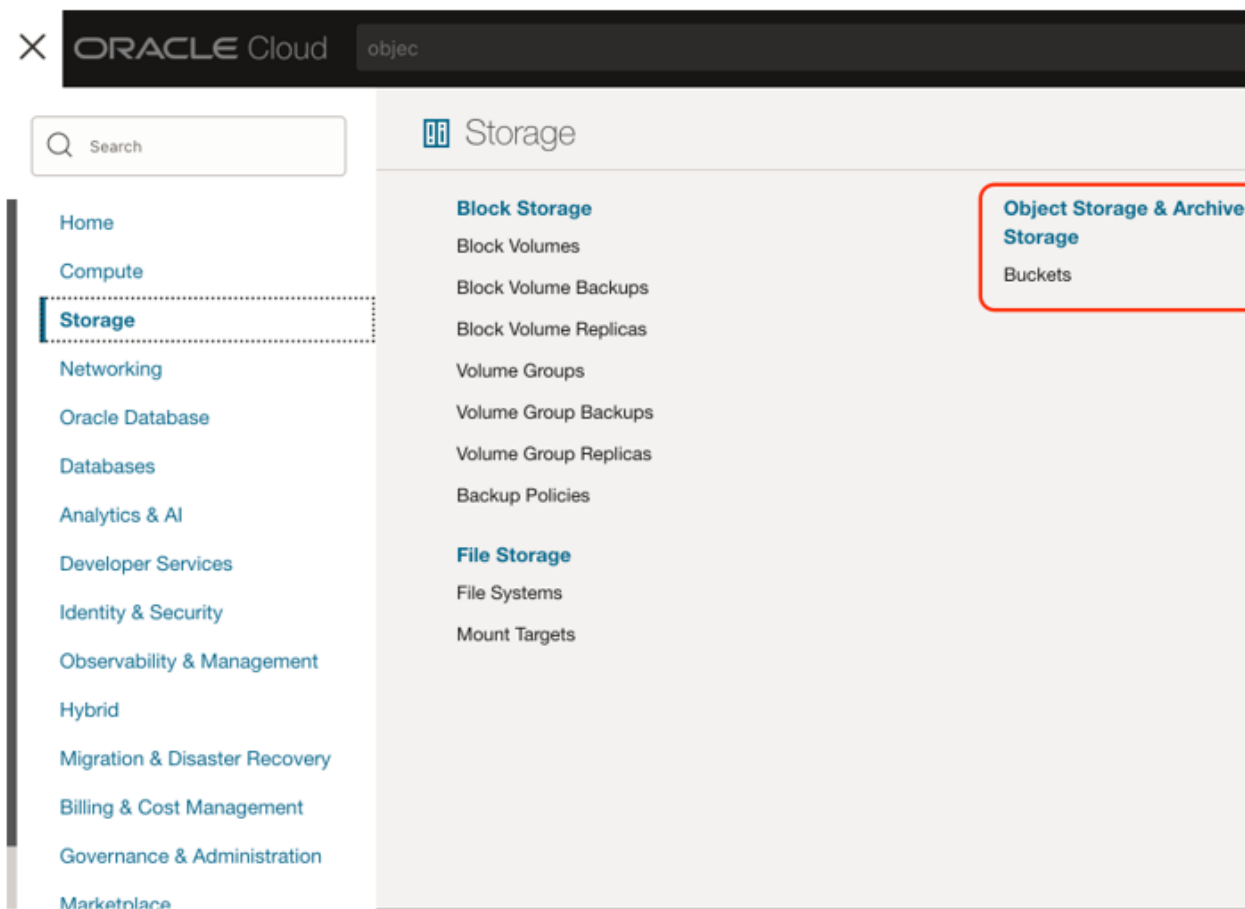
6. (Optional) If you have not yet downloaded the latest version of your Gateway VM image and optional YAML templates, click the Download icon and select **Download gateway VM image**. Save the archive file and unpack to a local workstation. Make sure the resulting file set is accessible from the Oracle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

You can now create an Oracle cloud gateway VM in Oracle Cloud Platform, see "[Uploading the Oracle Virtual Machine Image onto the Oracle Cloud Platform](#)" below.

Uploading the Oracle Virtual Machine Image onto the Oracle Cloud Platform

To upload a Oracle Gateway virtual machine image into Oracle Cloud Platform:

1. Access the Oracle Cloud Platform Management Portal, either from a client or a web browser, and log in using your Oracle Cloud Platform credentials.
2. Click the Navigation menu, and then select **Storage > Buckets**.

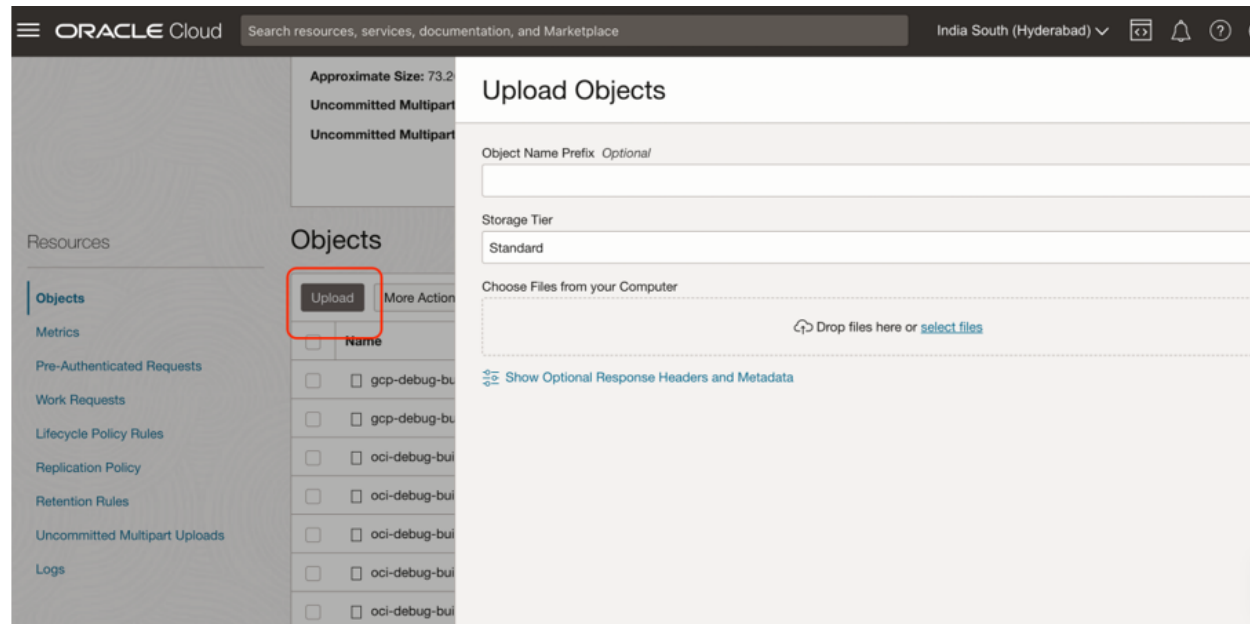


3. Select the right compartment and then the list of OCI storage buckets appears as below.
4. Select the bucket into which you wish to place the OCI image.

A page listing the current list of the files from the bucket appears.

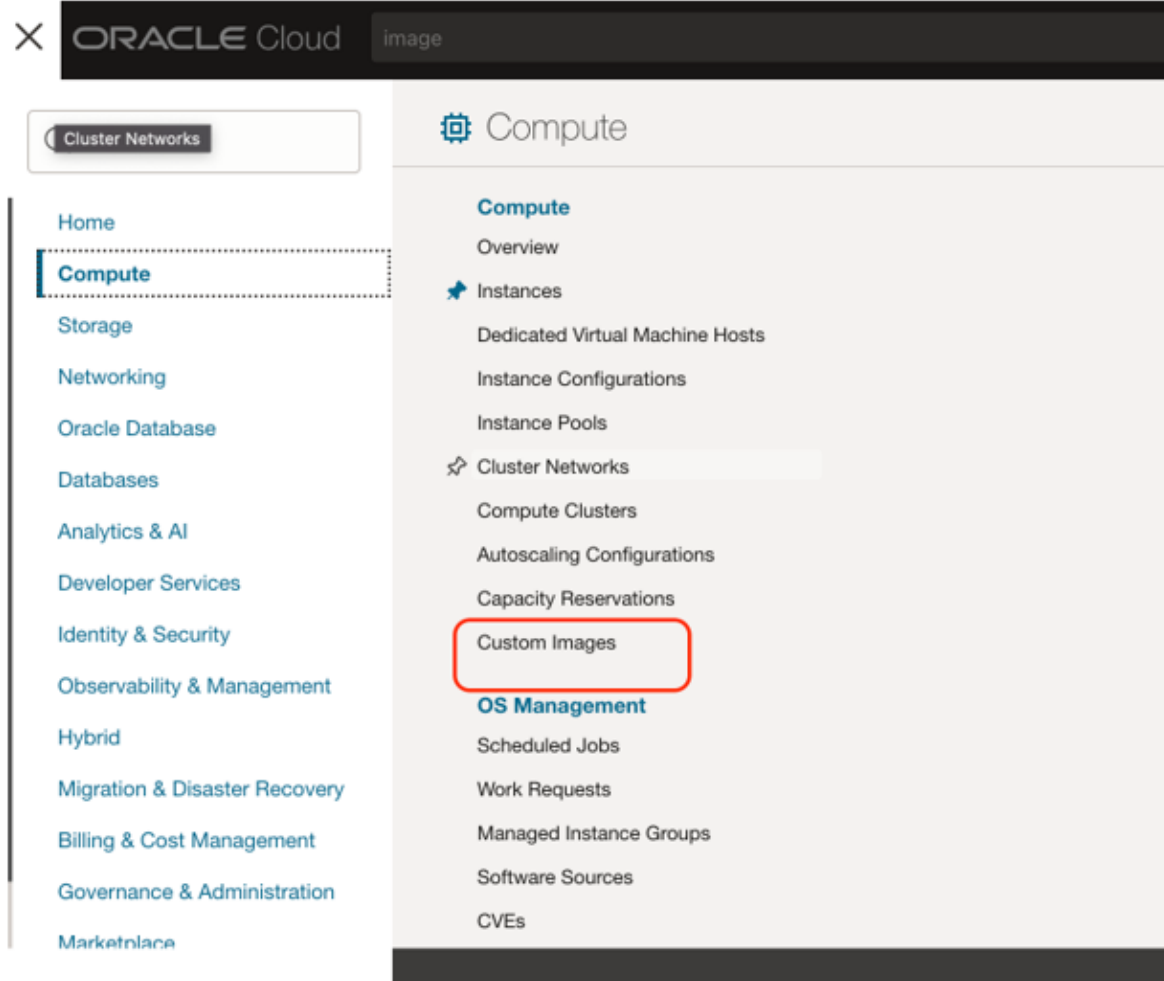
5. Click **Upload**.

An upload dialog appears.

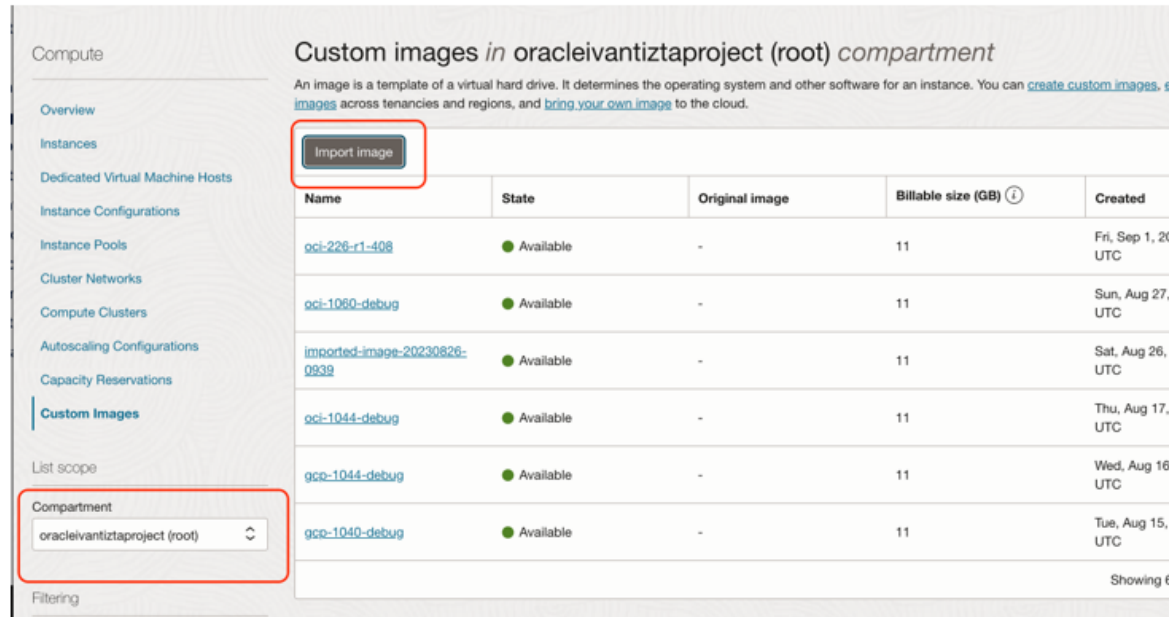


6. Select the *ZTA Gateway* OCI virtual machine image.tar file from your local workstation and click **Open**.
7. Wait until the upload completes. This may take several minutes.
8. Once upload completes. Create an image from the bucket using the following method:

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



2. Select the right compartment and then the list of current images appears.



Compute

Custom images in oracleivantzproject (root) compartment

An image is a template of a virtual hard drive. It determines the operating system and other software for an instance. You can [create custom images](#), [import images](#) across tenancies and regions, and [bring your own image](#) to the cloud.

Import image

| Name | State | Original image | Billable size (GB) ⓘ | Created |
|--|-----------|----------------|----------------------|-----------------------------|
| oci-226-r1-408 | Available | - | 11 | Fri, Sep 1, 2023 10:00 UTC |
| oci-1080-debug | Available | - | 11 | Sun, Aug 27, 2023 10:00 UTC |
| imported-image-20230826-0939 | Available | - | 11 | Sat, Aug 26, 2023 09:39 UTC |
| oci-1044-debug | Available | - | 11 | Thu, Aug 17, 2023 10:00 UTC |
| gcp-1044-debug | Available | - | 11 | Wed, Aug 16, 2023 10:00 UTC |
| gcp-1040-debug | Available | - | 11 | Tue, Aug 15, 2023 10:00 UTC |

Compartment: oracleivantzproject (root)

Filtering

3. Click on **Import image**. An import dialog will appear and then choose the .tar file that was uploaded in the bucket. Refer to the below screenshots.
 - Ensure the OS is selected as CentOS.
 - Ensure Launch mode is chosen as Paravirtualized mode.
 - Ensure Image type is chosen as QCOW2.

Import image

Create in compartment
oracleivantztaproject (root)

Name
imported-image-20230903-1512

Operating system
CentOS

Import from an Object Storage bucket
 Import from an Object Storage URL

Bucket in **oracleivantztaproject (root)** [\(Change compartment\)](#)

✓ ztaproject

Object name
oci-debug-build-1062ISA-V-OCI-ZTA-22.5R1-1062.1.tar.gz

Image type
 VMDK
Virtual machine disk file format. For disk images used in virtual machines.
 QCOW2
For disk image files used by QEMU.

- Wait until the import completes. This may take several minutes.

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

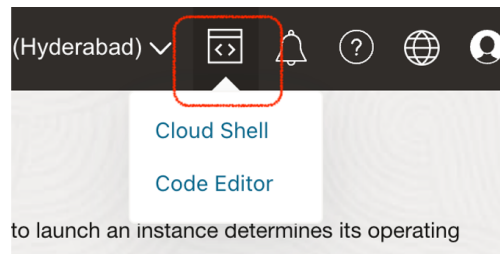
- Perform the task manually, see ["Configuring Gateways" on page 80](#).
- Perform the task with a script, see ["Creating a VM Instance of the Uploaded OCI Image Using Terraform Script" below](#).

Creating a VM Instance of the Uploaded OCI Image Using Terraform Script

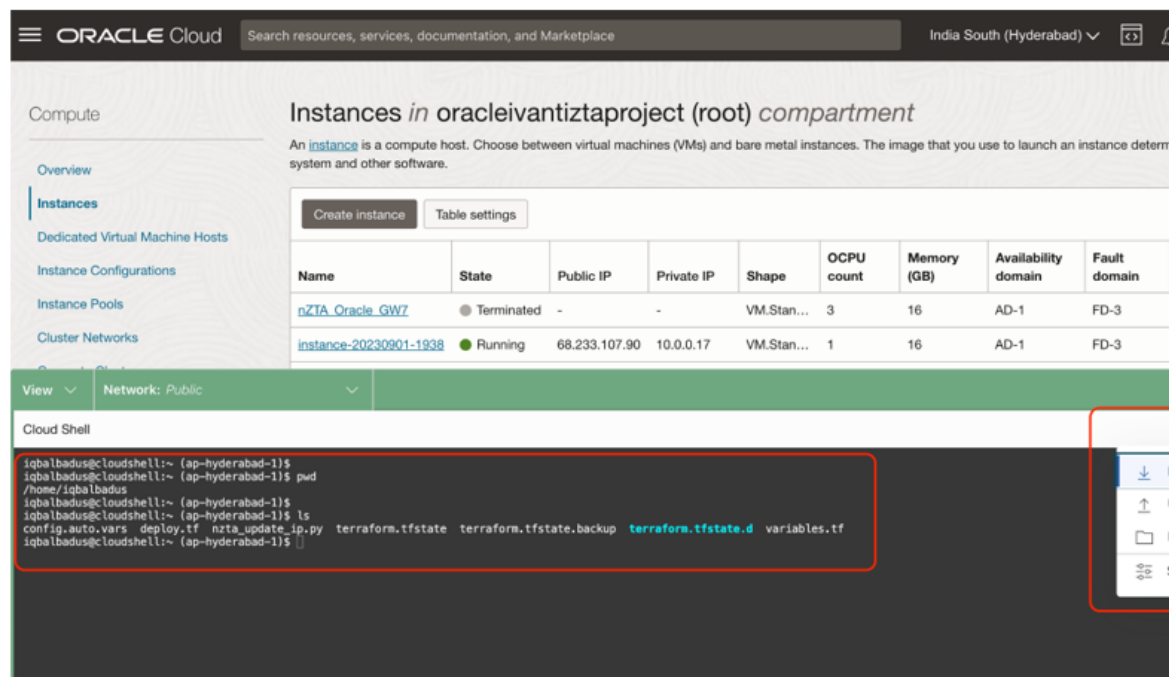
Pre-requisites: Ensure OCI configurations required for CLI access is enabled. This is one-time process. Please see here for details:

1. Download the required template archive file to your local workstation.
2. Upload all the scripts to Oracle cloud shell as below:

1. Open the cloud shell using the option as shown below.



2. Upload the terraform scripts using the upload option from the cloud shell settings as shown below. Once it is uploaded, the scripts will be present in the user's home directory.



3. Edit the `config.auto.vars` file as per the intended deployment. Refer "[Terraform Configurations](#)" on the next page for details on the configuration.
3. Run **terraform init**.
4. Run **terraform validate**. This will let the admin know if there are any issues with the configurations.
5. Run **terraform apply**. This will trigger the deployment process.
6. If any resource deployment fails, retry running the command **Terraform apply** again.

Terraform Configurations

| Description | Sample Value |
|--|--------------------------|
| 1e T n h a i b s l e d e m f a i n n a e g s e , m e i n f t n Z T | enable_management = true |

| | |
|------------------------|--------------|
| Description | Sample Value |
| Additional Information | |

| | |
|---|---------------------|
| <p style="writing-mode: vertical-rl; transform: rotate(180deg);">Description</p> | <p>Sample Value</p> |
| <p style="writing-mode: vertical-rl; transform: rotate(180deg);">Interface</p> | |
| <p style="writing-mode: vertical-rl; transform: rotate(180deg);">21 This is the internal existing_vcn = false</p> | |

| Description | Sample Value |
|---|--------------|
| if n g n e + y s c, n i f e x i s t i n | |

| Description | Sample Value |
|--|--------------|
| o b e u s e d f o r i n t e | |

| Description | Sample Value |
|--|--------------|
| e , t h e n w e n e e d t o p r | |

| Description | Sample Value |
|--|-------------------------------|
| 3e T x h t i e s r n d a e l f i e n x e i s , t i i n f g + v c n | external_existing_vcn = false |

| Description | Sample Value |
|--------------|--------------|
| existing VCN | to be |

| Description | Sample Value |
|-------------------------------|--------------|
| Final interface . . . if true | |

| Description | Sample Value |
|-------------|--------------|
| Signature | External - |

| Description | Sample Value |
|---------------------|---------------------------------|
| Management Existing | management_existing_vcn = false |

| Description | Sample Value |
|--------------|--------------|
| Existing VCN | to be |

| Description | Sample Value |
|--------------------|--------------|
| Element identifier | |

| Description | Sample Value |
|--------------------------|--------------|
| Configuration Management | |

| Description | Sample Value |
|---|----------------------------------|
| 5uT show settings and the configuration | use_internal_vcn_for_all = false |

| Description | Sample Value |
|-------------------------|--------------|
| Internal VCN to be used | |

| Description | Sample Value |
|----------------------|--------------|
| external/management) | |

| Description | Sample Value |
|--|--------------|
| 6) This indicates that the default configuration is false. | |

| Description | Sample Value |
|---|----------------------------------|
| 7e This external existing subnet is defined as follows: \$, t i n f g e s x u i b s n t e i t n g s u b n | external_existing_subnet = false |

| Description | Sample Value |
|----------------------------|------------------------------------|
| Management Existing Subnet | management_existing_subnet = false |

| Description | Sample Value |
|----------------------------------|------------------------------|
| 9c The information that needs to | create_management_nat = true |

| Description | Sample Value |
|---|----------------------------|
| 1c T Or h e i a s t e d - e i f n i t n e e r s n , a l i - f n a N t A T n e e d s t o | create_internal_nat = true |

| Description | Sample Value |
|--|---------------------------|
| 1c T 1r h e i a s t e d e t e f e x i t n e e r s n , a i f i g i n t e r n e t e g a t e | create_external_ig = true |

| Description | Sample Value |
|---|--------------------------------|
| 1. This is a sample configuration for the use_static_external_ip parameter. | use_static_external_ip = false |

| Description | Sample Value |
|---|--------------------------------|
| 1uT 3sh eis +s \$ td ae tf ii cn +e +s n, te ef n as lt +a it pic p ri v a t | use_static_internal_ip = false |

| Description | Sample Value |
|--|----------------------------------|
| 1uT4\$heis\$tdaefticnemea,naifgemesetnaatticppri v a t | use_static_management_ip = false |

| Description | Sample Value |
|--|---------------------------|
| 1uT 5sh eis +s lod ae df +i bn ae ls a, n ci ef r l oa d | use_load_balancer = false |

| | |
|--------------|--------------|
| Description | Sample Value |
| Availability | |

| Description | Sample Value |
|--------------|--------------|
| Availability | |

| Description | Sample Value |
|--|-------------------------------------|
| 1uT 6sh eis +s e xd ie \$f tin ne gs + b +f oe rx +s xt +n ng i cl o ad | use_existing_lb_for_ext_nic = false |

| Description | Sample Value |
|--|--------------|
| 1uT use_existing_bs_for_ext_nic = false 7\$ h e i + s e x d i e \$ f t i i n n e g s + , b \$ i + f f o e r x + i e s x t t i + n n g i c b a c k | |

| Description | Sample Value |
|--|-------------------------------------|
| 1uT8\$heisxdiesftinnesgs',siffoerxiesttinnngiclist | use_existing_ls_for_ext_nic = false |

| Description | Sample Value |
|--|---|
| 1c T 9o h me p a O r C t l m D e n o t f i t d h e c o m p a r t m e n t | compartment_id = "ocid1.tenancy.oc1..aaaaaaaarod5yc3653ujwgvjbbqui3s6r6ntfbs3d4uwxlkitku5flcbkrety" |

| Description | Sample Value |
|---|--------------------------------|
| 2v D 0mi + s d p i l s a p y l a n y a + m n e a m f e o r t h e n Z T A g a t e | vm_display_name = "skrn-new-2" |

| Description | Sample Value |
|---|--|
| 21 1mC al gD e + o if d t h e i m a g e t o u s e f o r t i | image_id = "ocid1.image.oc1.ap-hyderabad-1.aaaaaaapw7vnd4fqbp3heuk5kikfhlmhpcxjhcr17tz7a3ln52gg7jr3h |

| Description | Sample Value |
|--|--------------|
| 2s VM shape = "VM.Standard.E4.Flex" 2h M a p s e h a p e f o r t h e n Z T A g a t e w a y | |

| Description | Sample Value |
|--|----------------------|
| 2t N 3o u t m a b l e + r f l o e f x + r O e C q P u U i s r e d O C P U . s f o r | total_flex_OCPUs = 3 |

| Description | Sample Value |
|---|---------------------|
| 2t R 4o A t M a l s i f z l e e x f o R r A Mt h e f l e x V M | total_flex_RAM = 16 |

| Description | Sample Value |
|------------------------|--|
| 2a Availability Domain | availability_domain = "bsUY:AP-HYDERABAD-1-AD-1" |

| Description | Sample Value |
|--|---|
| 216nntee r r n n a a l l y C c l n D t R c i b d l r o t c b k l l o f c o k r t h e | internal_vcn_cidr_block = "10.0.0.0/16" |

| Description | Sample Value |
|--|--|
| 217n i t s e p r l n a y l n y a c m n e t d f i o s r p l t a h y e t n i a n m t e e r n a l | internal_vcn_display_name = "ZTA_internal_vnc_2" |

| Description | Sample Value |
|---|---|
| 21 8n C t l e D r n o a f t y h c e n e i x d i s t i n g v c n t o | internal_vcn_id = "ocid1.vcn.oc1.ap-hyderabad-1.amaaaaaatgkbhxyaia3zy75gt3cqxtgdagfsw7vdy2sylscjvavm2 |

| Description | Sample Value |
|--|---|
| 219n C t l e D r n o a f t t s h u e b n s e u t b n i e d t t o u s e f o r | internal_subnet_id = "ocid1.subnet.oc1.ap-hyderabad-1.aaaaaaafscfn7nzwsnv5xgjscybresi55fyxreqrqu67umi |

| Description | Sample Value |
|--|--|
| 31 On Internal network subnet identifier for calculation | internal_subnet_cidr_block = "10.0.0.0/18" |

| Description | Sample Value |
|--|--|
| 31 1 n i t s e p r l n a y l n s a u m b e n e f t o r d i t s h p e l a i y n t n e a r m n e a l | internal_subnet_display_name = "internal_Subnet_2" |

| Description | Sample Value |
|--|---------------------------------------|
| 31 2n t s e p r l n a a y l n r a t m e n a o mf e t h e r o u t i n g t a t | internal_rt_name = "internal_rt_name" |

| Description | Sample Value |
|--|---|
| 3n i t s e p r l n a y l n a m t e n o a f m e t h e n a t f o r t h | internal_nat_name = "internal_nat_name" |

| Description | Sample Value |
|------------------------------|--------------|
| 3) internal_nic_display_name | internal" |

| Description | Sample Value |
|--|----------------------------------|
| 31 S 5n t t a e t r i n c a l l P i p a d a d d r d e r s e s \$ \$ o f t h e i n t e r | internal_ip_address = "10.1.1.2" |

| Description | Sample Value |
|---|---------------------------------------|
| 31 T 6n h t i e s r n d a e l f i n s e s p, u b i l f i c w e i p n e e e n d a b t l o e d s s . | internal_is_public_ip_enabled = false |

| Description | Sample Value |
|---|---|
| 317 This deployment name is the name of the network segment. | internal_nsg_name = "internal_nsg_name" |

| Description | Sample Value |
|---|--|
| 31 8n t e r n a l i n g r e s s | protocol = "6"//TCP destination = "0.0.0.0/0" source = "0.0.0.0/0" min_dstport = 6667 max_dstport = 6667 min_srcport = 0 max_srcport = 0 description = "internal ingess" direction = "INGRESS" |

| Description | Sample Value |
|---|--------------|
| 3e External_vcn_cidr_block = "10.0.0.0/16" 9x t e r n a l C I D R c i b d r c b k o f c o k r t h e | |

| Description | Sample Value |
|--|--|
| 4e D 0x i t s e p r l n a a y l n y a c m n e + d f i o s r p l t a h y e + n e a x m t e e r n a l v | external_vcn_display_name = "ZTA_external_vnc_2" |

| Description | Sample Value |
|---|--------------|
| external_vcn_id = "ocid1.vcn.oc1.ap-hyderabad-1.amaaaaaatgkbhxyaia3zy75gt3cqotgdagfsw7vdy2sylvscjvavm | |

| Description | Sample Value |
|---|--------------|
| external_subnet_id = "ocid1.subnet.oc1.ap-hyderabad-1.aaaaaaafscfn7nzwsnv5xgjscybresi55fyxreqrqu67umi | |

| Description | Sample Value |
|----------------------------|--|
| external_subnet_cidr_block | external_subnet_cidr_block = "10.0.0.0/18" |

| Description | Sample Value |
|------------------------------|--|
| external_subnet_display_name | external_subnet_display_name = "external_Subnet_2" |

| Description | Sample Value |
|--|---------------------------------------|
| 4e D 5x i t s e p r l n a a y l n r a t m e n a o mf e t h e r o u t i n g t a l | external_rt_name = "external_rt_name" |

| Description | Sample Value |
|---------------------------------------|--------------|
| external_ig_name = "external_ig_name" | |

| Description | Sample Value |
|---------------------------|--------------|
| external_nic_display_name | external |

| Description | Sample Value |
|--|----------------------------------|
| external_ip_address of the external IP address | external_ip_address = "10.1.1.2" |

| Description | Sample Value |
|--------------------------------------|--------------|
| external_is_public_ip_enabled = true | |

| Description | Sample Value |
|---|---|
| 5e D 0x i t s e p r l n a a y l n n a s m g e n o a f m e t h e n e t w o r k s e | external_nsg_name = "external_nsg_name" |

| Description | Sample Value |
|----------------------|--|
| 5e1xtetehnaingstrues | protocol = "6"//TCP destination = "0.0.0.0/0" source = "0.0.0.0/0" min_dstport = 6667 max_dstport = 6667 min_srcport = 0 max_srcport = 0 description = "external ingess" direction = "INGRESS" |

| Description | Sample Value |
|---------------------------|---|
| Management_vcn_cidr_block | management_vcn_cidr_block = "10.0.0.0/16" |

| Description | Sample Value |
|--|--|
| 5mD 3a i n s a p g l e a m y e n n t a + m y e c n f + o d r i s t p h l e a y m + a n n a a m g e e m e n . | management_vcn_display_name = "ZTA_management_vnc_2" |

| Description | Sample Value |
|---|---|
| 5mC 4aC nI aD g e o mf e nt th + e y ce nx + i i s dt i n g v c n t o | management_vcn_id = "ocid1.vcn.oc1.ap-hyderabad-1.amaaaaatgkbhxyaia3zy75gt3cqxtgdagfsw7vdy2sylscj |

| Description | Sample Value |
|---|---|
| 5mC 5a C n l a D g e o mf e nt th e s us bu nb en te t i dt o u s e f o r | management_subnet_id = "ocid1.subnet.oc1.ap-hyderabad-1.aaaaaaafscfn7nzwsnv5xgjscopybresi55fyxreqrqeu6" |

| Description | Sample Value |
|---|--|
| 5mC 6a I n D a R g e b ml e o n c t k + s f u o b r n e t t h - e c i m d a r n - a b g l e o m c e k n t | management_subnet_cidr_block = "10.0.0.0/18" |

| Description | Sample Value |
|--|--|
| 5mD 7a i n s a p g l e a m y e n n t a + m s e u b f n o e r t + t d h i e s p m l a a n y a + g n e a m m e e n . | management_subnet_display_name = "management_Subnet_2" |

| Description | Sample Value |
|--|---|
| 5mD 8a i n s a p g l e a m y e n n t a + m r e t + o n f a m t e h e r o u t i n g t a t | management_rt_name = "management_rt_name" |

| Description | Sample Value |
|-------------|--------------|
|-------------|--------------|

5mD
9a i
n s
a p
g l
e a
m y
e
n n
t a
+ m
n e
a
t o
+ f
n
a t
m h
e e

n
a
t

f
o
r

management_nat_name = "management_nat_name"

| Description | Sample Value |
|--|--|
| 6mD 0a i n s a p g l e a m y e n n t a + m n e i c f + o d r i s t p h l e a y m + a n n a a m g e e m e n . | management_nic_display_name = "management" |

| Description | Sample Value |
|--|------------------------------------|
| 6mS 1a t n a a t g i e c m e l n P t + a i d p d + r a e d s d s r e o s f s t h e m a n a g | management_ip_address = "10.1.1.2" |

| Description | Sample Value |
|--|---|
| 6mT 2a h n i a s g e d me e f n i t n + e + s \$, + p i u f b w i e c + n i e p e + d e n t a o b l s e s t : | management_is_public_ip_enabled = false |

| Description | Sample Value |
|--|---|
| 6mD 3a i n s a p g l e a m y e n n t a + m n e \$ g o + f n a t m h e e n e t w o r k | management_nsg_name = "management_nsg_name" |

| Description | Sample Value |
|--------------------|--|
| Management ingress | <pre> protocol = "6"//TCP destination = "0.0.0.0/0" source = "0.0.0.0/0" min_dstport = 6667 max_dstport = 6667 min_srcport = 0 max_srcport = 0 description = "management ingress" direction = "INGRESS" </pre> |

| Description | Sample Value |
|---|---|
| 6 5 i t t + c o n n f i g t h a t n Z T A w i l l p i c t | <pre> init_config = "PHB1bHNILWNvbmZpZz48cHJpbWFyeS1kbnM+OC44LjguODwvcHJpbWFyeS1kbnM+PHNIY29uZGFyeS1kbnM pbj48Y2VydC1jb21tb24tbnFtZT5za3JuLW9jaS5nLmUyZTluZS5qdW5pcGVyLnB6dC5kZXYucGVyZnNIYy5jb208L2 W5zZS1hZ3JlZW1lbnQ+PGNvbmZpZy1kb3dubG9hZC11cmw+J2h0dHBzOi8vZTJlMi5qdW5pcGVyLnB6dC5kZXY UzNDMzYi9vcml0aHRhbnR0cmF0aW9uL2luaXRpYWwtY29uZmlnP3Q9Z0FBQUFBQmstQUFmYXlwYjgtNXowMXo4aV QWp2c2JEWGUzcnA1X2VmU3Joc1ISWTM1SU96WmE3dlZsaDRXalNSQ3ZXa3JFVkkVek5mOTdqeDI1T1A1VktxQ pYWDdOa2Y5STZlWUctUWI0aHRENzNOZnZyYjhzNmRYZGo0WUllaXltdXA0YnJ5d1I0dUdiVThuZ20zR3ZWanFPa ZTUFmY1E4YTM5MmRFUIQ1OVhWM3p4QkRvaklQQ1I1RINtbExCd2NKckRjZC1oTVMwSmpxYUE1NHhLMDNsM UF4TT0nPC9jb25maWctZG93bmxvYWQtdXJsPjxhcHBsaWFuY2UtaWQ+MGNhM2U2ZTBmZjEyNDUxN2FhNjNjO XlucHp0LmRldi5wZXJmc2VjLmNvbTwvY29udHJvbGxlc1ob3N0bmFtZT48Y29udHJvbGxlc1lbnJvbGxlc1ob3N0b bGVkLWwhvc3RuYW1lPjxkbmMtc2VhcmNoLWRvbWFpbj5wc2VjdXJlM5ldDwvZG5zLXNIYXJjaC1kb21haW4+PGN PjwvcHVsc2UtY29uZmlnPg==" </pre> |

| Description | Sample Value |
|-----------------|--------------------------------------|
| 6b Display name | lb_display_name = "external_lb_name" |

| Description | Sample Value |
|---|--------------|
| 67 listener_display_name = ["external_ls_name_443" , "external_ls_name_80"] | |

| Description | Sample Value |
|--|--|
| 6b D 8\$ i + s d p i l s a p y l a n y a + m n e a m o e f t h e b a c k e n d | bs_display_name = ["external_bs_name_443","external_bs_name_80"] |

| Description | Sample Value |
|---|---|
| 6e09x C t l e r i n d a l o f b t h i e d e x t e r n a l l o a d b a l | external_lb_id = "ocid1.networkloadbalancer.oc1.ap-hyderabad-1.amaaaaaatgkbhxyanzrjec4irpjuumytyuk5qugc |

| Description | Sample Value |
|---|--------------|
| 7b L ports = [443,80] 0p o r a t d s b a l a n c e r p o r t s f o r t h e l i | |

| Description | Sample Value |
|---|--------------------------|
| 7b B 1\$ a + c p k o e l n i d c y s e t p o l i c y t h a t s h o u l d | bs_policy = "FIVE_TUPLE" |

| Description | Sample Value |
|--|------------------|
| 7b T 2r C o P t o i c s o l o n l y p r o t o c o l s u p p o r t e d | protocol = "TCP" |

Creating a VM Instance of the Uploaded OCI Image Using any Other Methods

Deploy a VM with nZTA gateway image uploaded to the OCI, with following requisites:

1. Configure 2 nic's in the order Internal, External, if the Management port is not required for the nZTA gateway deployment.
2. Configure 3 nic's in the order Internal, External and Management. If management port is configured for the nZTA gateway deployment.
3. Ensure custom metadata "pulse-config" is configured for the VM. The value of pulse-config metadata needs to be taken from the init file downloaded from the nZTA controller interface as explained in admin guide section "[Downloading Metadata for Oracle Cloud Platform](#)" on [page 163](#).
4. Ensure internal NIC can access the controller present in the azure cloud and application resources.
5. Ensure external NIC public ip is reachable by the ISAC clients over the port 443.
6. Ensure management NIC can access the controller present in the azure cloud , if management port is enabled for controller communication.
7. Ensure load balancer ip is reachable by the ISAC clients over port 443, if load balancer is used for gateway deployment.
8. Recommended Firewall rules:
 - Internal - INGRESS (TCP: 6667), EGRESS (TCP: ANY, UDP: ANY)
 - External - INGRESS (TCP: 443)
 - Management - INGRESS (TCP: 6667), EGRESS (TCP: ANY, UDP: ANY)

Next Steps

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

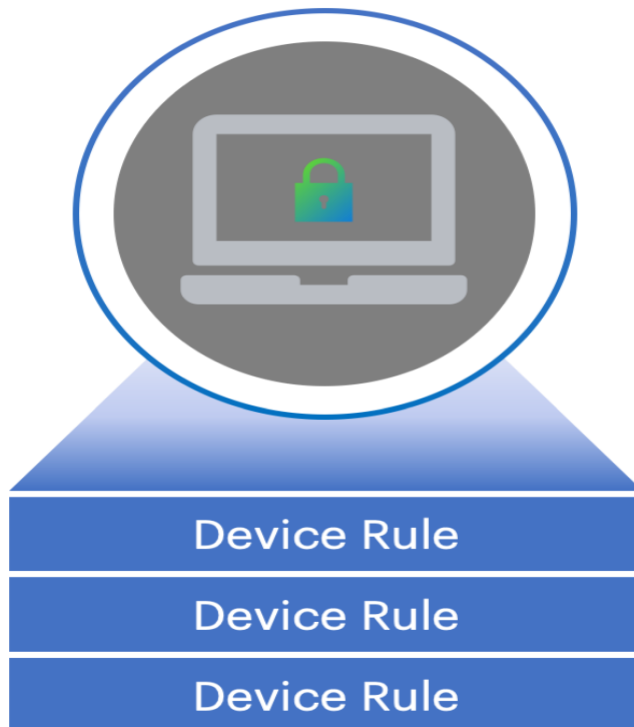
Creating Device Policies and Device Rules

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 can create **Device policies** and attach to them one or more **Device Rules** as required.

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.

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*.

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*.

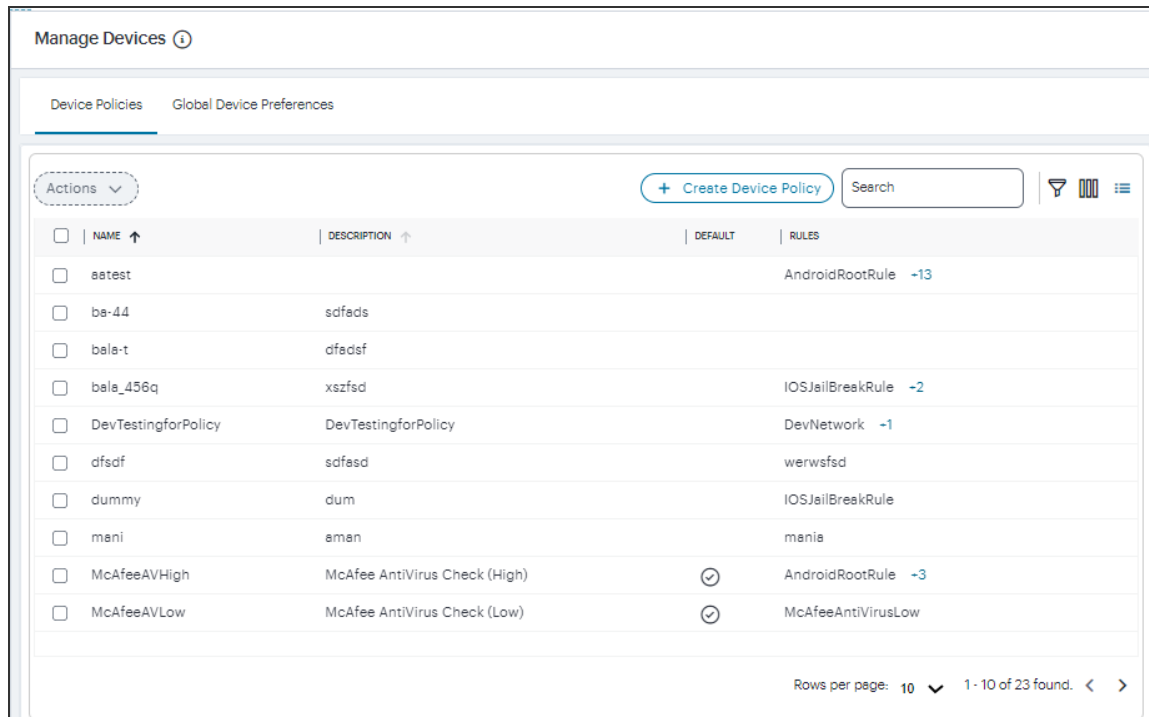
Creating Device Policies

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](#)" on page 263.

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.



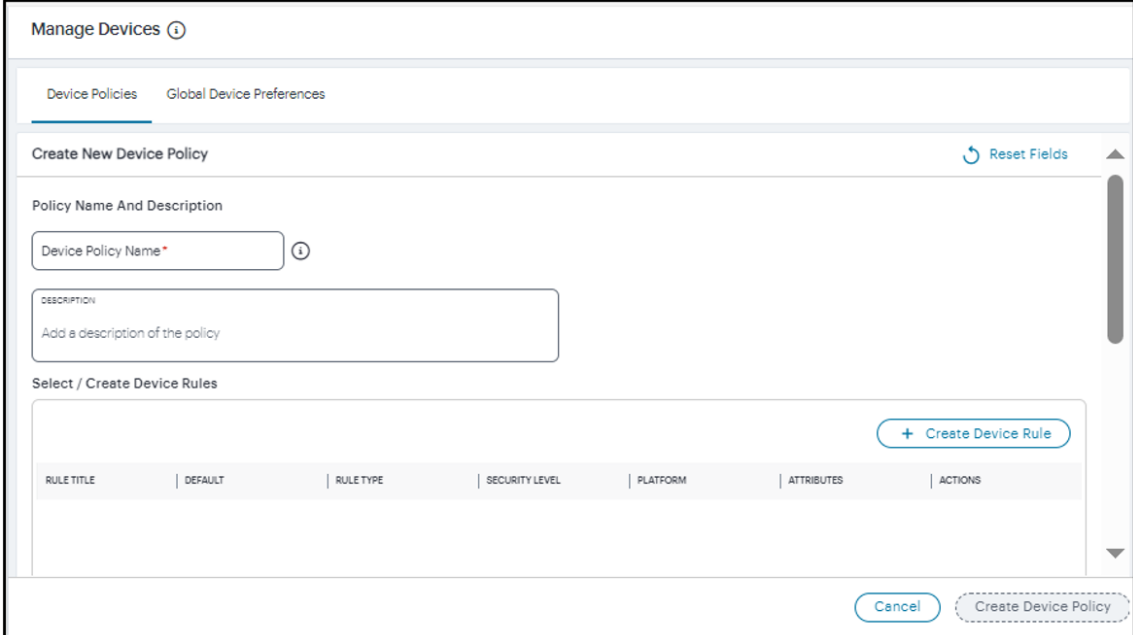
The screenshot shows the 'Manage Devices' interface with a sub-tab for 'Device Policies'. The table below lists various device policies with their names, descriptions, default status, and associated rules.

| <input type="checkbox"/> | NAME ↑ | DESCRIPTION ↑ | DEFAULT | RULES |
|--------------------------|---------------------|-------------------------------|-------------------------------------|---------------------|
| <input type="checkbox"/> | estest | | | AndroidRootRule -13 |
| <input type="checkbox"/> | ba-44 | sdfads | | |
| <input type="checkbox"/> | bala-t | dfadfs | | |
| <input type="checkbox"/> | bala_456q | xszfds | | IOSJailBreakRule -2 |
| <input type="checkbox"/> | DevTestingforPolicy | DevTestingforPolicy | | DevNetwork -1 |
| <input type="checkbox"/> | dfsdf | sdfads | | werwsfsd |
| <input type="checkbox"/> | dummy | dum | | IOSJailBreakRule |
| <input type="checkbox"/> | mani | eman | | menis |
| <input type="checkbox"/> | McAfeeAVHigh | McAfee AntiVirus Check (High) | <input checked="" type="checkbox"/> | AndroidRootRule -3 |
| <input type="checkbox"/> | McAfeeAVLow | McAfee AntiVirus Check (Low) | <input checked="" type="checkbox"/> | McAfeeAntiVirusLow |

At the bottom right of the table, it indicates 'Rows per page: 10' and '1 - 10 of 23 found'.

3. Click **Create Device Policy**.

A form appears to enable you to create the device policy.



The screenshot shows the 'Manage Devices' interface with the 'Create New Device Policy' form. The form is titled 'Create New Device Policy' and includes a 'Reset Fields' button. The form is divided into two main sections: 'Policy Name And Description' and 'Select / Create Device Rules'. The 'Policy Name And Description' section contains a 'Device Policy Name*' field and a 'DESCRIPTION' field with the placeholder text 'Add a description of the policy'. The 'Select / Create Device Rules' section contains a '+ Create Device Rule' button and a table with columns: RULE TITLE, DEFAULT, RULETYPE, SECURITY LEVEL, PLATFORM, ATTRIBUTES, and ACTIONS. At the bottom of the form, there are 'Cancel' and 'Create Device Policy' buttons.

i At any point during this process, you can reset the form data by selecting **Reset Fields**.

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, or select **Create Device Rule** to use the in-line rule creation form. To learn more about this process, see "[Creating Device Rules](#)" on page 263.

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.



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.



- This feature is applicable to Windows and Mac device policies only.
- Also note 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 **Create Device Policy**.

The new device policy appears in the list of **Device Policies**.

10. Repeat steps 3-7 to create all required device policies.

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 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 Policies**.

The *Device Policies* page appears. This page lists all device policies and the associated rules.

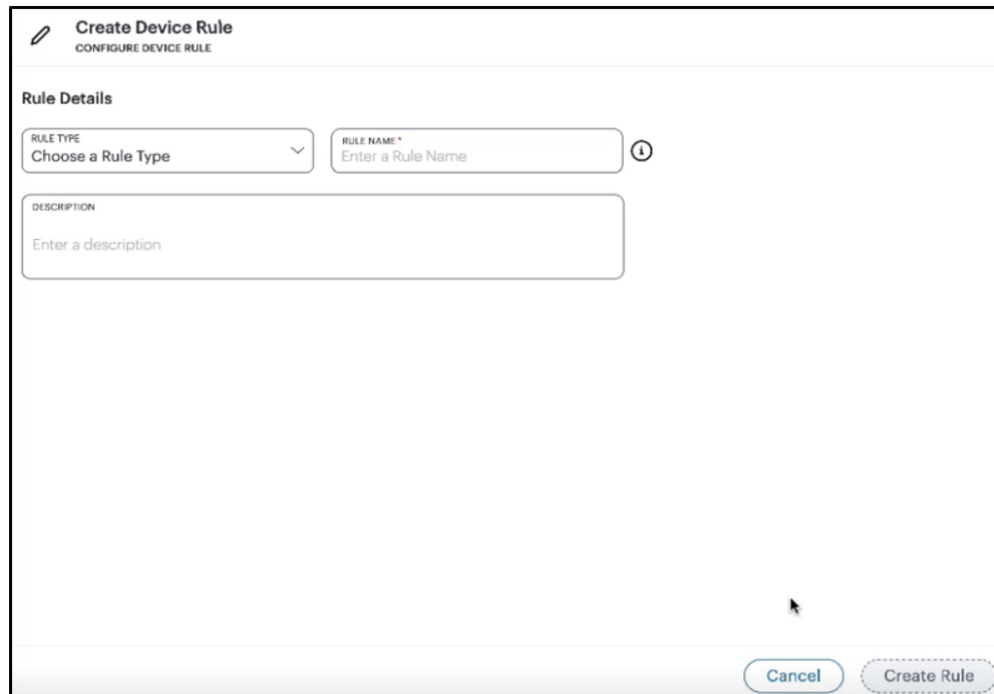
3. Click **Create Device Policy**. Fill the Create Device Policy form that appears. For details, see ["Creating Device Policies" on page 259](#).



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

4. Click **Create Device Rule**.

The **Create Device Rule** form appears.



The screenshot shows a web form titled "Create Device Rule" with the subtitle "CONFIGURE DEVICE RULE". The form is divided into a "Rule Details" section and a footer. In the "Rule Details" section, there are three input fields: a dropdown menu for "RULE TYPE" with the text "Choose a Rule Type", a text input for "RULE NAME*" with the placeholder "Enter a Rule Name" and a help icon, and a text area for "DESCRIPTION" with the placeholder "Enter a description". At the bottom right of the form, there are two buttons: "Cancel" and "Create Rule".

Create Device Rule

5. 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*

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

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

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

For *Antispyware* and *Firewall* rules, see ["Options for Antispyware and Firewall Rules"](#) on the next page.

For *Antivirus* rules, see ["Options for Antivirus Rules"](#) on the next page.

For *Command* rules, see ["Options for Command Rules"](#) on page 269.

For *CVE check* rules, see ["Options for CVE Check Rules"](#) on page 268.

For *File* rules, see ["Options for File Rules"](#) on page 269.

For *Hard Disk Encryption* rules, see ["Options for Hard Disk Encryption Rules"](#) on page 270.

For *Location* rules, see ["Options for Location Rules"](#) on page 270.

For *Mac Address* rules, see ["Options for MAC Address Rules"](#) on page 271.

For *Netbios* rules, see ["Options for Netbios Rules"](#) on page 272.

For *Network* rules, see ["Options for Network Rules"](#) on page 272.

For *OS* rules, see ["Options for OS Rules"](#) on page 272.

For *Process* rules, see ["Options for Process Rules"](#) on page 273.

For *Port* rules, see ["Options for Port Rules"](#) on page 274.

For *Patch Management* rules, see ["Options for Patch Management Rules"](#) on page 274.

For *Registry* rules, see ["Options for Registry Rules"](#) on page 275.

For *Risk Sense* rules, see ["Options for Risk Sense Rules"](#) on page 277.

For *System Integrity* rules, see ["Options for System Integrity Rules"](#) on page 277.

For *Time of day* rules, see ["Options for Time of Day Rules"](#) on page 278.

9. Select **Create Rule** to create the device rule.

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

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.



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.



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



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.



To remove a selected CVE from the list, select the "X" button adjacent to the CVE tag.

Options for Command Rules



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




This rule type is applicable to Windows and macOS devices only.

1. Select **Platform** and select one of the following options:
 - *windows*
 - *mac*
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.

 To remove a location, select the "X" button adjacent to the location tag.

Options for Hard Disk Encryption Rules

 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



This rule type is applicable to Windows and macOS devices only.

1. Select **Platform** and select one of the following options:

- *windows*
- *mac*

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*
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



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*
-



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*
-



For some products, the patch category might not be detectable. In this case, select *Unknown* to detect missing patches.

Options for Registry Rules



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\pzta` 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.

 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

 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.

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.



All times are applied as UTC timezone values. Your ZTA Gateways must also use UTC time for the rule schedule to apply.

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.

Next Steps

After you have created your device policies, move on to define your applications. See "[Creating Applications and Application Groups](#)" on the next page.

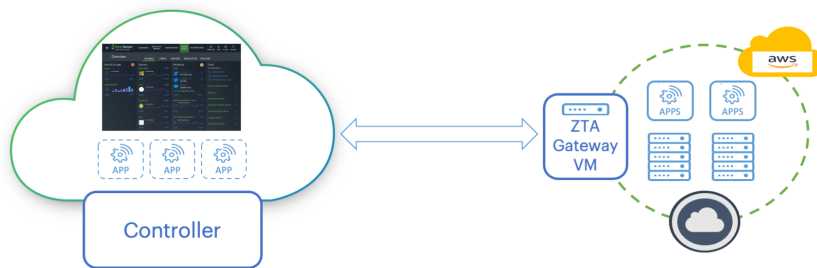
Creating Applications and Application Groups

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" on page 287](#).



The enables Controller you to:

- Create definitions of applications to which your end users require access, see ["Adding Applications to the Controller" below](#).
- Group together multiple applications for which a single secure access policy is required, see ["Adding Application Groups to the Controller" on page 284](#).



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 **Manage Applications > Applications**.

The *Applications* page appears. This page lists all applications defined on the Controller.

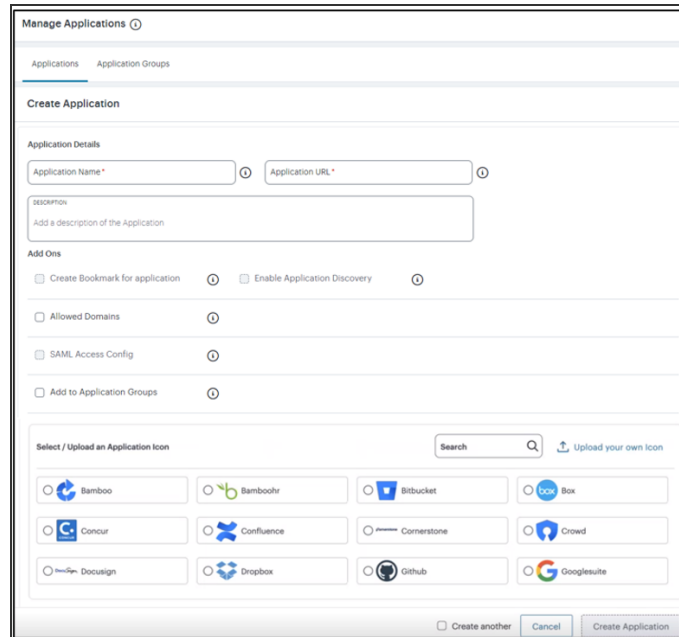
| STATUS | NAME | TYPE | APPLICATION DETAIL | APPLICATION GROUP(S) |
|--------------------------|------------------------|-------------|---------------------------|---|
| <input type="checkbox"/> | 10.90.6.11 | application | ssh://10.90.6.11 | bookmarked |
| <input type="checkbox"/> | 1_app_con_adp_bookmark | application | https://1_app.com | |
| <input type="checkbox"/> | Application discovery | application | *.* | |
| <input type="checkbox"/> | FQDN_port1 | application | www.example.com:9090 | |
| <input type="checkbox"/> | FQDN_portA_portB | application | www.example.com:9090-9099 | |
| <input type="checkbox"/> | IP_path | application | http://1.1.1.1 | bookmarked, nw-group, combined_grp, pe... |
| <input type="checkbox"/> | aajtak | application | aajtak.in | perftest_apps3, combined_grp, allowd_g... |
| <input type="checkbox"/> | about | application | about.google | perftest_apps, perftest_apps4, allowd_... |
| <input type="checkbox"/> | abplive | application | abplive.com | perftest_apps5, allowd_group, perftest... |
| <input type="checkbox"/> | academia | application | academia.edu | perftest_apps2, perftest_apps5, perfte... |



The list includes a built-in application called *Application discovery*. The **Application Detail** for this application is ".*", indicating that all applications that it applies to all unlisted applications. This application is used by the nZTA application discovery feature, and cannot be deleted.

3. Click **Create Application**.

A form appears enabling you to create the application.



The screenshot shows the 'Manage Applications' interface. At the top, there are tabs for 'Applications' and 'Application Groups'. Below this is the 'Create Application' section. It includes an 'Application Details' section with fields for 'Application Name*' and 'Application URL*', and a 'Description' field. Below that is an 'Add Ons' section with checkboxes for 'Create Bookmark for application', 'Enable Application Discovery', 'Allowed Domains', 'SAML Access Config', and 'Add to Application Groups'. At the bottom, there is a 'Select / Upload an Application Icon' section with a search bar and a grid of application icons including Bamboo, BambooHR, Bitbucket, Box, Concur, Confluence, Cornerstone, Crowd, DocuSign, Dropbox, GitHub, and Google Suite. At the very bottom, there are buttons for 'Create another', 'Cancel', and 'Create Application'.

i At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing application definitions in a pop-up dialog by clicking **View Applications**.

4. Enter the **Application Name**.

5. Enter the **Application Details**. That is, the URL, FQDN or IPv4 address of the application you want to add.

i 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**.
 - Click **Upload your own icon** to upload a bespoke image file as the reusable custom icon. Then select the icon from the list to associate to 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. You can edit or remove the uploaded custom icon.
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.



When using SAML authentication, make sure you add to a single application group only those applications that use the same SAML authentication source.

14. To save this application and create another application, select the **Create another** check box.
15. 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](#)" on page 288.

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.



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 **Manage Applications > Application Groups**.

The *Applications Groups* page appears. This page lists all application groups defined on the Controller.

| STATUS | NAME | NO OF APPS | FQDN APPS | URL APPS | NETWORK APPS |
|--------|----------------|------------|-----------|----------|--------------|
| | 67_apps | 44 | 43 | 1 | 0 |
| | allowed_group | 6 | 5 | 1 | 0 |
| | bookmarked | 21 | 4 | 16 | 1 |
| | combined_grp | 24 | 9 | 15 | 0 |
| | mw-group | 6 | 2 | 1 | 3 |
| | perftest_apps | 88 | 85 | 3 | 0 |
| | perftest_apps1 | 35 | 35 | 0 | 0 |
| | perftest_apps2 | 44 | 44 | 0 | 0 |
| | perftest_apps3 | 35 | 35 | 0 | 0 |
| | perftest_apps4 | 26 | 26 | 0 | 0 |

- Click **Create Application Group**.

The **Create Application Group** form appears.

The screenshot shows the 'Create Application Group' form. At the top, there is a text input field for 'Application Group Name'. Below it is a search bar. The main part of the form is a table of applications. The table has the following columns: 'status', 'name', 'type', 'application detail', and 'application group'. The table contains the following rows:

| status | name | type | application detail | application group |
|--------------------------|-----------------------|-------------|-----------------------------|-------------------|
| <input type="checkbox"/> | s1app | application | http://s1df.com | |
| <input type="checkbox"/> | s2app | application | http://s2df.com | |
| <input type="checkbox"/> | enc | application | http://ecn.com | s1 |
| <input type="checkbox"/> | Application discovery | application | ** | |
| <input type="checkbox"/> | confluence | application | https://ire.cam.zeus.com/ | s1 |
| <input type="checkbox"/> | Duo | application | https://www.duo.google.com/ | s1 |
| <input type="checkbox"/> | Facebook | application | https://www.facebook.com/ | s1 |

At the bottom of the form, there are two buttons: 'Cancel' and 'Create Application Group'.

- Enter the **Group Name**.
- Select the applications you want to include in the group.



You cannot add the *Application discovery* application to a group.

- Click **Create Application Group** 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" on the next page](#).



Before you create a Secure Access Policy, make sure you have created all required definitions for Gateways, Users, Devices, and Applications.

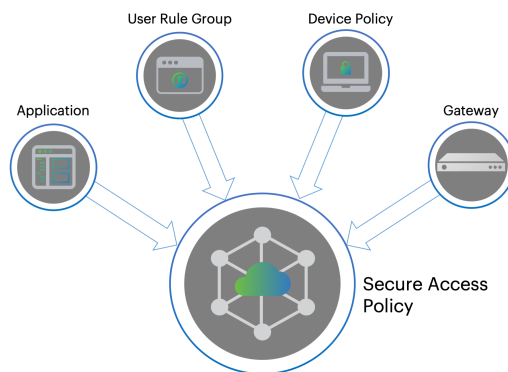
Creating a Secure Access Policy

Introduction

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.



i 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](#)" on the next page).
- *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 Applications and Application Groups](#)" on page 280.

To learn more about registering Gateways, see "[Configuring Gateways](#)" on page 80.

To learn more about creating device policies, see "[Creating Device Policies and Device Rules](#)" on page 257.

To learn more about defining applications, see "[Creating Applications and Application Groups](#)" on page 280.

To see an overview of nZTA, see "[Getting Started with Ivanti Neurons for Zero Trust Access](#)" on page 4.

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.

| Secure Access Policies ⓘ | | | | | |
|--------------------------|--------|---------------------------------|--|---------------|-------------------------|
| SECURE ACCESS POLICIES | | | | | |
| 54 POLICIES - 0 SELECTED | | | | | |
| SEARCH | | | | | |
| <input type="checkbox"/> | STATUS | APPLICATION / APPLICATION GROUP | GATEWAY / GATEWAY GROUP / GATEWAY SELECTOR | USER GROUP | DEVICE POLICY |
| <input type="checkbox"/> | | 10.204.88.244_telnet | blackthorn-bng-2 | sj group | |
| <input type="checkbox"/> | | 10.96.75.63_rdp | blackthorn-bng-2 | sj group | RiskSenseCriticalNot... |
| <input type="checkbox"/> | | 3liftWildcard | aws-blackthorn | sj group | |
| <input type="checkbox"/> | | 54.159.47.183_ipv4 | aws-blackthorn | sj group | notepad_reqd |
| <input type="checkbox"/> | | ad.doubleclick.net_wilc | blackthorn-debug | bng group | |
| <input type="checkbox"/> | | Adobe | blackthorn-bng-2 | bng group | Time_Of_Day_Policy_B... |
| <input type="checkbox"/> | | Adp | az-bkthrn-eastus | bng group | OnlyIP |
| <input type="checkbox"/> | | Amazon | blackthorn-bng-2 | bng group | |
| <input type="checkbox"/> | | Application discovery | blackthorn-bng-3 | default group | |
| <input type="checkbox"/> | | Atlassian | blackthorn-bng-2 | bng group | Antivirus |
| <input type="checkbox"/> | | BambooHR | az-bkthrn-eastus | mac group | |
| <input type="checkbox"/> | | BIGIP-F5 | blackthorn-bng-4 | bng group | OnlyIP |

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.

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

APPLICATIONS AND APPLICATION GROUPS

10 APPLICATIONS AND APPLICATION GROUPS

| | NAME | TYPE | APPLICATION DETAILS | AI |
|----------------------------------|-------------|--------|-------------------------------------|----|
| <input type="radio"/> | amazon | single | *.amazon.com | |
| <input type="radio"/> | Bamboo | single | https://dev.pulsesecure.net/bamboo | O |
| <input type="radio"/> | Confluence | single | https://dev.pulsesecure.net/conf... | O |
| <input checked="" type="radio"/> | dailymotion | single | https://www.dailymotion.com | |
| <input type="radio"/> | Dropbox | single | https://www.dropbox.com/login | |
| <input type="radio"/> | Eng Portal | single | https://eng-portal.psecure.net/ | O |
| <input type="radio"/> | Flipkart | single | *.flipkart.com | |
| <input type="radio"/> | G1 | single | *.google.com | G |
| <input type="radio"/> | G2 | single | *.googleapis.com | G |
| <input type="radio"/> | G3 | single | *.googleusercontent.com | G |

Rows per page: 10 ▼



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**.



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.



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*.