



Ivanti Neurons for Secure Access

MSP Portal Admin Guide

v22.3R4

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

© 2022, Ivanti, Inc. All rights reserved.

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

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

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

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

END USER LICENSE AGREEMENT

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

Contents

Preface	1
Document conventions	1
Text formatting conventions	1
Command syntax conventions	2
Code Block	2
Notes and Warnings	3
Requesting Technical Support	3
Self-Help Online Tools and Resources	3
Opening a Case with PSGSC	4
Reporting Documentation Issues	4
About This Guide	5
Logging in as a Tenant Administrator	7
Preparing to Login	7
Logging into the MSP Portal	8
Logging out of the MSP Portal	9
Using the MSP Portal	11
Using the Portal Interface	12
Using the All Tenants Dashboard	16
Creating Tenants in the MSP Portal	19
Introduction	19
Using the Add New Tenant Workflow	20
Editing the Details of an Existing Tenant	22
Generating Usage Data for Billing	25
Introduction	25
Viewing the Usage Summaries Page	25
Scheduling a Usage Report Generation	26
Configuring Administrator Access	29

Preface

- [Document conventions](#) (page 1)
- [Requesting Technical Support](#) (page 3)
- [Reporting Documentation Issues](#) (page 4)

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Ivanti technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
<i>italic text</i>	Identifies emphasis
	Identifies variables
	Identifies document titles
courier font	Identifies command output
	Identifies command syntax example

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member [member ...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Code Block

Following is an example of Python based code block in the html documentation:

```
def some_function():  
    interesting = False  
    print 'This line is highlighted.'  
    print 'This one is not...'  
    print '...but this one is.'
```

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

Note: This is an example of a note.

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

Attention: This is an example of an attention statement.

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

Caution: This is an example of a caution statement.

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit <https://support.pulsesecure.net/product-service-policies/>

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.pulsesecure.net>
- Search for known bugs: <https://support.pulsesecure.net>
- Find product documentation: <https://www.pulsesecure.net/techpubs>
- Download the latest versions of software and review release notes: <https://support.pulsesecure.net>
- Open a case online in the CSC Case Management tool: <https://support.pulsesecure.net>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://support.pulsesecure.net>

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: <https://kb.pulsesecure.net>
- Ask questions and find solutions at the Pulse Community online forum: <https://community.pulsesecure.net>

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at <https://support.pulsesecure.net>.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see <https://support.pulsesecure.net/support/support-contacts/>

Reporting Documentation Issues

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, contact Pulse Secure Technical Support (<https://support.pulsesecure.net>). Include a full description of your issue or suggestion and the document(s) to which it relates.

About This Guide

This guide introduces the Ivanti Neurons for Secure Access (nSA) MSP Portal and describes the processes and configuration options available in this release. It is intended for Managed Service Provider (MSP) administrators to enable them to create, manage, and monitor tenants within nSA.

It covers the following subject areas:

- Logging into the nSA Controller as a Tenant Admin. See [Logging in as a Tenant Administrator](#) (page 7).
- Using the portal dashboard. See [Using the MSP Portal](#) (page 11).
- Creating Tenants. See [Creating Tenants in the MSP Portal](#) (page 19).
- Generating tenant usage data. See [Generating Usage Data for Billing](#) (page 25).

Logging in as a Tenant Administrator

- [Preparing to Login](#) (page 7)
 - [Logging into the MSP Portal](#) (page 8)
 - [Logging out of the MSP Portal](#) (page 9)
-

Preparing to Login

As a Managed Service Provider (MSP), you can configure Ivanti Neurons for Secure Access (nSA) with details of the tenants for whom you want to provide access to nSA administrative services. An MSP can configure a tenant with an entitlement to use nZTA and/or ICS.

Through the MSP portal, a MSP Admin can:

- Create and edit tenants
- Delete tenants
- Block tenants
- Generate usage reports for billing

To log into the MSP portal, you require a MSP Admin login.

All MSP Admin accounts are set up by Ivanti. After your MSP Admin account has been created, you will receive an email which describes how to log into the MSP portal.

You can then proceed to login to the portal, see [Logging into the MSP Portal](#) (page 8).

Logging into the MSP Portal

Before you can log in as a MSP Admin, you will receive an email from Ivanti detailing your subscription. This email contains:

- Your MSP Admin username.
- Your password.
- A hyperlink to start the login process. By default, this typically contains an endpoint URL in the form
`https://<yourMSPdomain>.pulsezta.net/login/msp.`

To log into your MSP Admin account:

1. Click the hyperlink in your email, or copy the URL into your web browser.
The MSP login page appears.

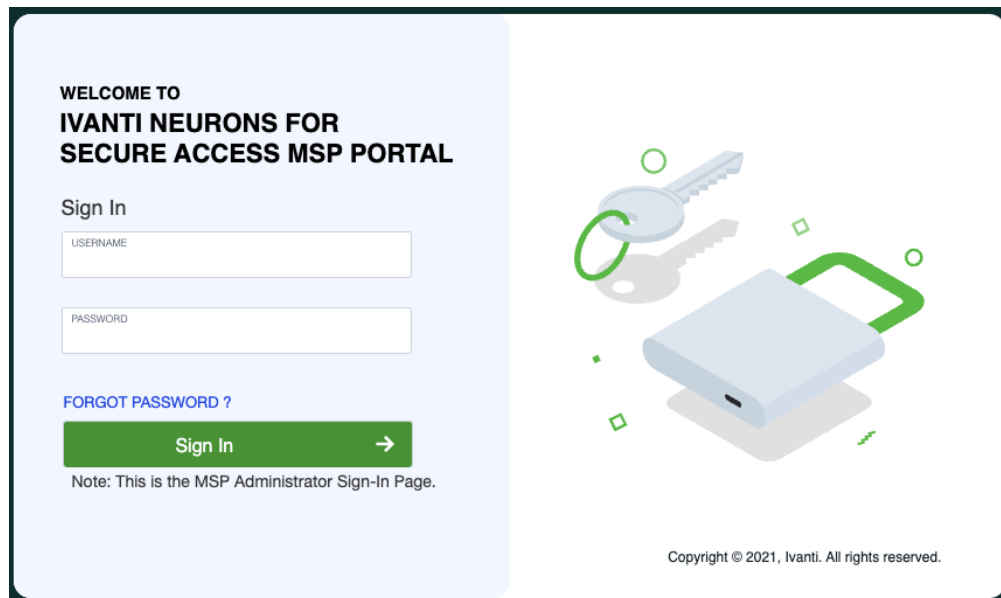


FIGURE 3.1 : MSP Admin Login Page

2. Log in using your supplied MSP Admin credentials.

The following default timeouts are used for all MSP admin sessions:

- The idle timeout is 10 minutes.
- The session timeout is 60 minutes.

3. If nSA requests it, specify a new password for your account.

Once this procedure is complete, you access the nSA portal interface as a MSP admin user. The main dashboard page appears.

Note: To reset a forgotten password, click **FORGOT PASSWORD**. This link presents a credentials form through which you enter a username and password. If the entered credentials match a registered MSP administrator account, nSA emails a

password reset link to the entered address allowing the recipient to create a new password.

Logging out of the MSP Portal

To log out of the nSA MSP portal and end the current session, click the *Profile* icon and select **Logout**.

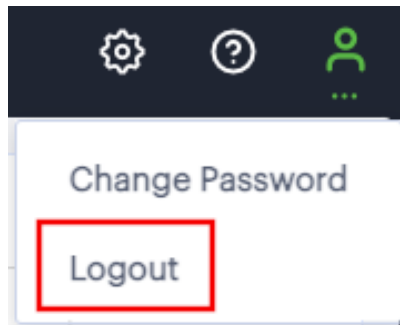


FIGURE 3.2 : Logging out of the portal

Using the MSP Portal

- [Using the Portal Interface](#) (page 12)
- [Using the All Tenants Dashboard](#) (page 16)

After you log in to the MSP Portal, nSA displays the **All Tenants** page. This serves as the *home page*, or dashboard, for your portal.

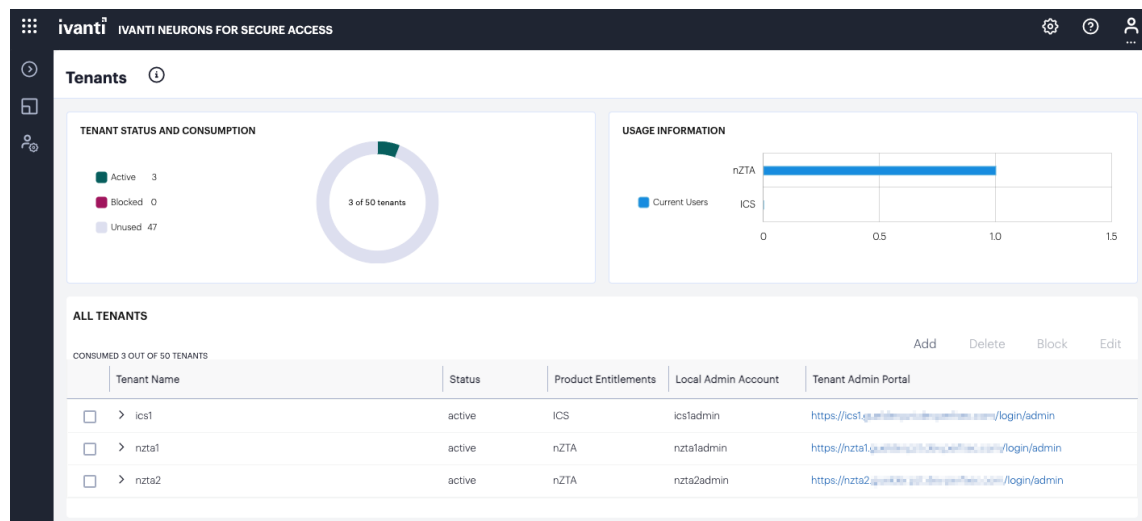


FIGURE 4.1 : The MSP Portal

Note: To return to this page any time, click the menu icon in the left-hand menu bar and select **Tenants > All Tenants**. Alternatively, click the banner at the top.

From this page, you can view and configure all functions and capabilities allowed through your subscription.

To learn more about the portal interface, see [Using the Portal Interface](#) (page 12).

To learn more about the graphs and data shown in this page, see [Using the All Tenants Dashboard](#) (page 16).

Using the Portal Interface

When you log in to the MSP portal for the first time, or at any point where you have no tenants defined in your deployment, nSA presents a banner recommending you create a new tenant:

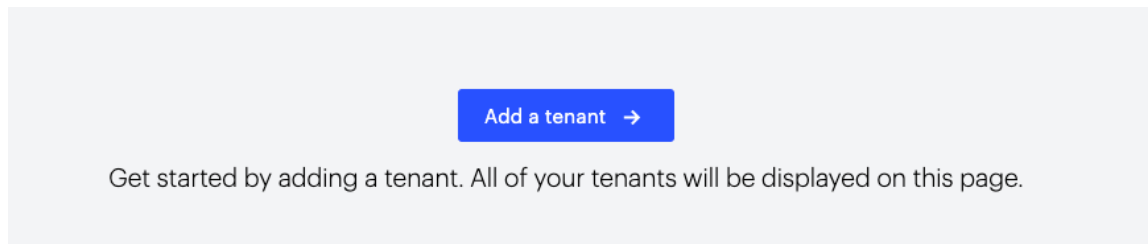


FIGURE 4.2 : Getting started in the MSP portal

To add a new tenant, select **Add a tenant**. Then, to learn more about the process of creating tenants, refer to [Creating Tenants in the MSP Portal](#) (page 19).

For all subsequent login sessions, nSA displays the *Tenant Dashboard*. This serves as the home page for your portal, and provides an overview of tenant activity across your deployment.

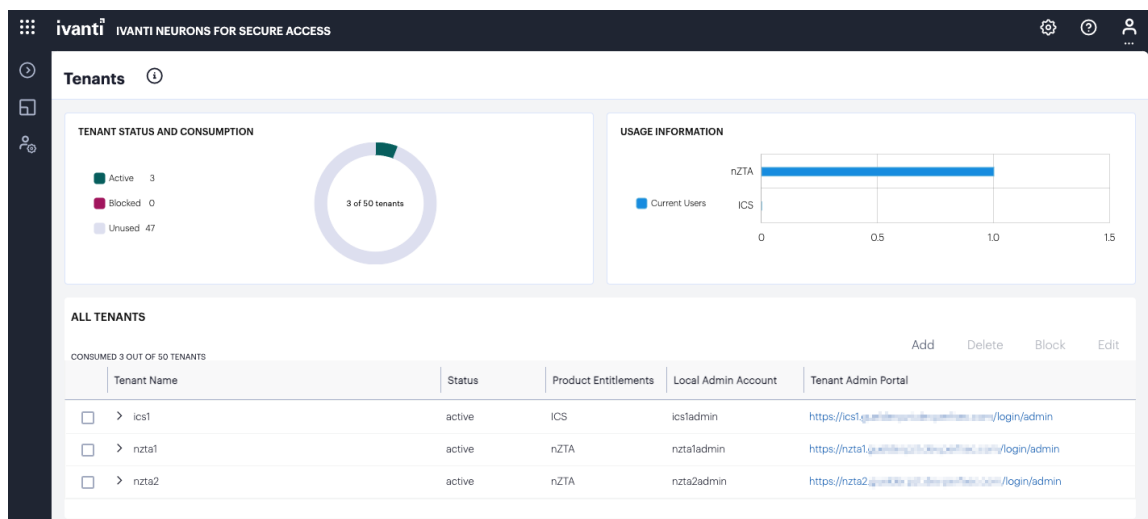


FIGURE 4.3 : The Tenant Dashboard

Note: To return to this page any time, click the menu icon in the nSA menu and select **Tenants > All Tenants**. Alternatively, click the banner at the top.

From this page, you can view and configure all functions and capabilities allowed through your subscription and role. Using the nSA menu at the left-hand side, choose from:

- The **Show/Hide** menu icon, providing the ability to show or collapse the nSA menu tree:

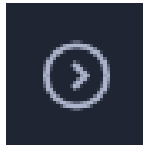


FIGURE 4.4 : Showing or hiding the nSA menu system

- The **Tenants** menu icon, providing access to the main configuration screens of the MSP portal:



FIGURE 4.5 : Accessing the Tenants menu

Through this menu, you can select:

- **Tenants > All Tenants**: See [Using the MSP Portal](#) (page 11).
- **Tenants > Usage Summary**: See [Generating Usage Data for Billing](#) (page 25).
- The **Administrator** menu icon, providing options to configure administrator access to the MSP portal:

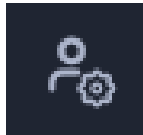


FIGURE 4.6 : Accessing the Administrator menu

To learn more, see [Configuring Administrator Access](#) (page 29).

In addition to the nSA menu, the following controls can be used to configure the appearance and functionality of the portal:

- Portal settings:



FIGURE 4.7 : Accessing the portal settings menu

The Settings dialog appears:

Settings [X]

White Labeling [^]
Use your logo across the system

Color Scheme [^]
Choose the color mode for the app

☐ Light ☐ Dark

Timezone [^]
Set Timezone

CHOOSE TIMEZONE
Choose your option [v]

CANCEL APPLY

FIGURE 4.8 : Configuring portal settings

Use this dialog to configure your portal interface. Select from:

– **White Labeling:**

Use this feature to configure a common branding across all of your deployed tenants. Select the text **White Labeling** to view the *White Labeling* dialog:

FIGURE 4.9 : The White Labeling dialog

In this dialog you can configure:

- * The **Application Name** applied to your tenants.
- * The **Logo** that appears on the tenant's nSA portal.
- * The **Favicon** used in the browser.
- * The **Colors** used to brand the tenant's nSA portal.

– **Color Scheme:**

Select **Light** or **Dark** to switch between themes:

– **Timezone:**

Configure the default timezone for this admin login account. The configured timezone affects the display of data across all pages. Changes to the timezone persist across login sessions, and the default setting is *UTC (Coordinated Universal Time)*.

Note: Changing the timezone can affect the analytics and usage data displayed in the portal.

- **Help and Documentation:**

nSA documentation for administrators is available from the MSP portal. If you are a MSP admin, login to the portal using the URL provided in your welcome email. To access product help and documentation links, click the help icon in the navigation bar:



FIGURE 4.10 : Getting help and documentation

- **MSP Admin account options:**



FIGURE 4.11 : Admin account options

From this option, you can reset the account password or log out of the portal (see also [Logging out of the MSP Portal](#) (page 9)).

Using the All Tenants Dashboard

The **All Tenants** page contains the following components:

- **Tenant Status and Consumption:**

MSPs are typically provided with a default initial allowance of 50 tenants. This dashboard contains a chart showing deployed tenants as a proportion of the total allowance.

Defined tenants are indicated as either **Active** or **Blocked**, with the remainder of the allowance indicated as **Unused**.

Note: As you approach the limit of your allowance, nSA presents an **Increase Operation Limit** dialog. Confirming this dialog sends a message to Ivanti to indicate that you wish to increase your maximum tenant allowance.

- **Usage Information:**

This dashboard contains a usage chart showing the total number of enrolled and licensed end-users, per nSA service, across all tenants.

• **All Tenants:**

This section contains a table listing all of your tenant definitions. Each entry lists the following details:

- **Tenant Name:** The designated name for this tenant.
- **Status:** The status of this tenant deployment, “active” (for fully active tenants) or “pending” (for tenants in a mid-deployment state).
- **Product Entitlements:** The nSA services this tenant is entitled to use.
- **Local Admin Account:** The tenant admin account username specified during tenant creation.
- **Tenant Admin Portal:** The FQDN of this tenant’s default Tenant Admin Portal endpoint, in the form `https://<yourMSPsubdomain>.pulsezta.net/login/admin`.

Note: The Tenant Admin Portal displayed here is the default endpoint for the tenant admin. The tenant admin might modify this endpoint later; however, this field is not updated to reflect such changes and only ever shows the default endpoint.

Select the arrow indicator adjacent to the tenant name to view a drop-down panel containing a summary of **Current Users** versus **Maximum Users** for each of this tenant’s product entitlements:

Tenant Name		Status	Product Entitlements	Local Admin Account	Tenant Admin Portal
<input type="checkbox"/>	▼ doctest1	active	ICS, nZTA	doctest1	https://doctest1.pulsezta.net/login/admin
Product		Current Users		Max Users	
ICS		0		50	
nZTA		0		50	

FIGURE 4.12 : Viewing a summary of a tenant’s service usage

To add a new tenant, select **Add**. To edit an existing tenant, select the checkbox adjacent to the tenant name, then select **Edit**. To learn more about adding and editing tenants, see *Creating Tenants in the MSP Portal* (page 19).

To permanently remove a tenant and all their data, select the checkbox adjacent to the tenant name, then select **Delete**. Confirm the operation in the subsequent dialog.

Note: Deleting a tenant is a permanent operation and cannot be reversed.

To temporarily suspend the operation of a tenant without removing any configuration, select the checkbox adjacent to the tenant name, then select **Block**. Confirm the operation in the subsequent dialog.

Blocking a tenant does not deny access for the tenant admin to the Tenant Admin Portal. However, nSA does then disallow any further connection attempts by the end users in the tenant subscription.

A blocked tenant is indicated accordingly in the *All Tenants* MSP dashboard, and the *Tenant Status and Consumption* dashboard **Blocked** counter is incremented.

Creating Tenants in the MSP Portal

- [Introduction](#) (page 19)
 - [Using the Add New Tenant Workflow](#) (page 20)
 - [Editing the Details of an Existing Tenant](#) (page 22)
-

Introduction

This chapter describes how to use the MSP portal to create and edit tenants. Before you begin, make sure you have the following information for a prospective tenant:

- The tenant name
- The nSA services required (nZTA and/or ICS), including the maximum potential end-user count required in each case
- The subdomain you want to configure for the tenant, in the form `https://<subdomain>.pulsezta.net`.
- The username and email address of a tenant administrator. This is the individual who can login to the nSA Tenant Admin Portal and configure the *Secure Access Policies* governing access to an organization's applications and resources.

To learn more about adding new tenants to the MSP portal, see [Using the Add New Tenant Workflow](#) (page 20). To learn more about editing an existing tenant, see [Editing the Details of an Existing Tenant](#) (page 22).

Using the Add New Tenant Workflow

To add a new tenant:

1. Log into nSA as a MSP Admin, see [Logging into the MSP Portal](#) (page 8).
2. From the main Dashboard page, activate the *Add New Tenant* workflow by selecting **Add** from the *All Tenants* panel:

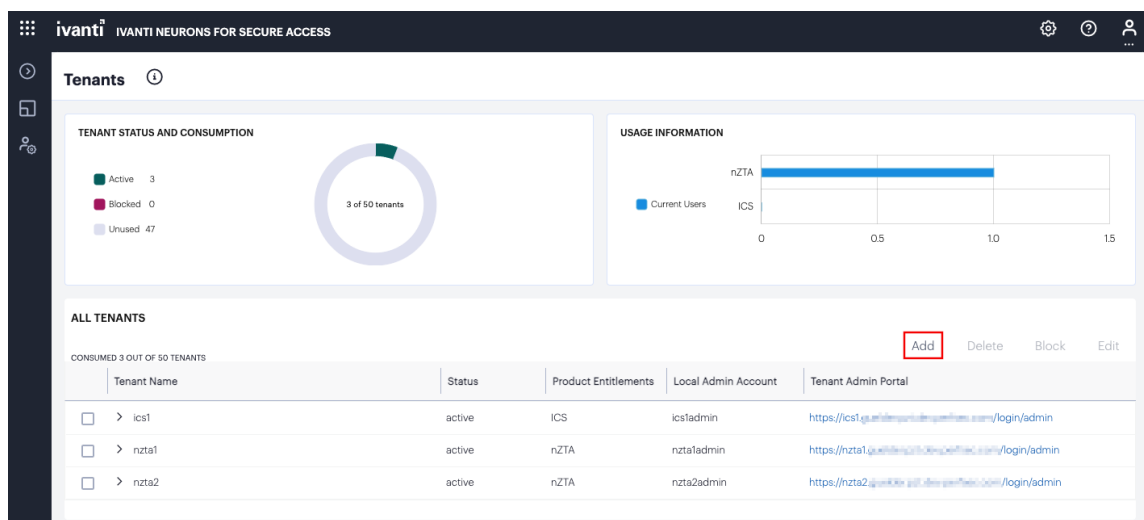


FIGURE 5.1 : Activating the *Add New Tenant* workflow

The *Add New Tenant* workflow dialog appears:

Add New Tenant USING 2 OF 60 TENANT

Tenant Details

Tenant Name

☐ nZTA

☐ ICS

Subdomain Information

The Subdomain is where the tenant's user will access the product

<https://> [CHECK AVAILABILITY](#) [.pulsezta.net](#)

Create Username

Contact Information

The tenant administrator will be sent a one-time use password that they can use to set their own password

[CANCEL](#) [CREATE TENANT](#)

FIGURE 5.2 : The Add New Tenant workflow

3. In the *Tenant Details* section:

- Enter a **tenant name**.
- Use the checkboxes to select the nSA services to which this tenant is entitled to access.
- For each selected service, enter the **Max Users** allowed to access the service. This is a soft limit that does not restrict additional users from enrolling to the relevant service. Instead, a tenant exceeding this limit receives a warning in the Tenant Admin Portal enabling them to take action without any reduction in service. Furthermore, the MSP Portal dashboard is updated to indicate to a MSP Admin any tenants that have breached their user limit.

4. In the *Subdomain Information* section:

- Enter the unique **Subdomain** you want to allocate for this tenant. This forms part of the FQDN to which all users enroll or sign-in their devices.
- Your tenant FQDN must be unique and unused. To check the availability of the FQDN, enter the **Subdomain** and select **CHECK AVAILABILITY**.

nSA presents an error if the domain is unavailable:

Subdomain Information

The Subdomain is where the tenant's user will access the product

https:// .pulsezta.net

Subdomain is taken. Please try another

FIGURE 5.3 : nSA showing that the subdomain you specify is not available

5. In the *Create Username** section:

- Enter the **Username** of the initial tenant administrator account.

6. In the *Contact Information* section:

- Enter the **Tenant administrator Email** to which you want to send the invitation email. The recipient receives an email containing credentials and a link to login to the *default* nSA Tenant Admin Portal endpoint (based on the subdomain you specify for this tenant, the default endpoint is `https://<subdomain>.pulsezta.net/login/admin`). This includes a one-time use password that must be changed upon login.

7. Make sure your tenant details are correct. A deployed tenant can only be edited to update basic details - the product entitlement and admin account details are not amendable through the MSP Admin Portal.

Note: A Tenant Admin is entitled to modify their administrative user details at any point through the Tenant Admin Portal. For more details, see the Ivanti Neurons for Secure Access Tenant Admin documentation.

- To create the tenant, select **Create Tenant**.

The Dashboard page reappears and your new tenant is added to the *All Tenants* list with a status of “Initializing”. After the creation process completes, the status updates to “Active”.

Note: This process can take a few minutes to complete. If your tenant status remains as “Initializing” for some time, contact Ivanti Support for help.

Editing the Details of an Existing Tenant

To edit an existing tenant:

- Log into nSA as a MSP Admin, see [Logging into the MSP Portal](#) (page 8).
- From the main Dashboard page, select the checkbox adjacent to a tenant entry in the *All Tenants* panel, then select **Edit**:

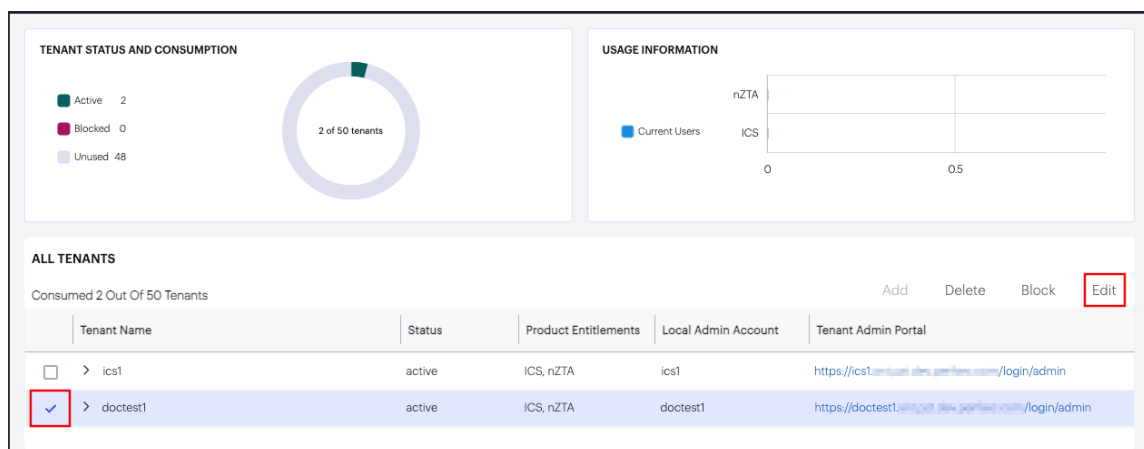


FIGURE 5.4 : Editing a tenant

The *Edit Tenant* dialog appears:

Edit Tenant

Tenant Details

TENANT NAME
doctest1 ⓘ

✓ nZTA MAX USERS
100 ⓘ

✓ ICS MAX USERS
200 ⓘ

Subdomain
<https://doctest1.iam.pam.digipartner.com/login/admin>

Username
doctest1

Contact Information
support@ivanti.com

CANCEL SAVE

FIGURE 5.5 : The Edit Tenant dialog

3. In the *Tenant Details* section, you can edit:

- The **Tenant Name**
- The **Max Users** amount for each service entitlement

Note: You cannot change the remaining details for an existing deployed tenant.

4. To save your changes, select **Save**.

Generating Usage Data for Billing

- [Introduction](#) (page 25)
 - [Viewing the Usage Summaries Page](#) (page 25)
 - [Scheduling a Usage Report Generation](#) (page 26)
-

Introduction

This page provides the ability to generate usage reports for tenant billing purposes. Each report contains a breakdown, per tenant, of the user counts in each service a tenant is entitled to use, calculated at the time the report is generated.

You can generate a report immediately, set up a repeating schedule, or delete unneeded reports.

Viewing the Usage Summaries Page

To access the usage summaries page:

1. Log into nSA as a MSP Admin, see [Logging into the MSP Portal](#) (page 8).
2. From the main menu, select **Tenants > Usage Summary**.

The *Usage Summaries* page appears:




Usage Summaries			Schedule	Generate Now	Delete
3 Usage Summaries Found					
Generated On	Usage Summary Details				
<input type="checkbox"/> Jan 06, 2022	usage_report_2022-01-06T16:32:28Z.csv				
<input type="checkbox"/> Jan 03, 2022	usage_report_2022-01-03T01:17:58Z.csv				
<input type="checkbox"/> Dec 27, 2021	usage_report_2021-12-27T01:17:56Z.csv				

FIGURE 6.1 : The Usage Summaries page

From this page, you can:

- View previously generated reports, and download each report as a CSV text file to your local workstation.

To download a report, select the download icon adjacent to the report entry:



FIGURE 6.2 : Downloading a usage report

- Schedule a regular report generation, see [Scheduling a Usage Report Generation](#) (page 26).
- Generate a usage summary report immediately by selecting **Generate Now**.
- Delete one or more usage summary reports by selecting the checkbox adjacent to each applicable report entry, then selecting **Delete**.

Scheduling a Usage Report Generation

To set up a usage report schedule, or to cancel an existing schedule, select **Schedule**.

The *Schedule* dialog appears:

The screenshot shows a 'Schedule' dialog box with a clock icon in the top left. It contains a toggle switch for 'Schedule usage summary reports' which is turned on. Below this are two dropdown menus: 'FREQUENCY' set to 'Weekly' and 'SELECT A DAY' set to 'Monday'. Both dropdowns have an information icon (i) to their right. Below the dropdowns, it says 'Next summary will be generated on Mar 14, 2022'. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

🕒 Schedule

Schedule usage summary reports ☒

FREQUENCY ▼ i
Weekly

SELECT A DAY ▼ i
Monday

Next summary will be generated on Mar 14, 2022

CANCEL SAVE

FIGURE 6.3 : Setting up a usage report schedule

In this dialog, you can:

- Switch on or off scheduled reporting.
- Set a schedule duration based on a frequency of *Daily*, *Weekly* (with a selected day of the week), or *Monthly* (with a selected date in each month).

To apply your changes, select **SAVE**.

Configuring Administrator Access

To access and use the MSP admin portal, you require a MSP Admin account. The initial MSP Admin login is set up by Ivanti and provided to the nominated email account when the MSP subscription is created. The initial MSP Admin account can create and manage further admin accounts as required to access the portal.

The MSP Portal uses **Admin Groups** to represent the group of admin users entitled to access the portal. An admin group combines an **Authentication Policy**, **Authentication Method**, and a set of one or more **Authentication Rules**.

You can view each of these elements through the **Administrator** menu.

Note: Editing policies, rules, and groups is not possible. These sections are read-only and included for information purposes.

A MSP admin can create and edit a defined list of admin user accounts managed locally in the MSP portal. Login requests are authenticated against this list to determine access rights.

To add a new admin user:

1. Log into the MSP admin portal, see [Logging into the MSP Portal](#) (page 8).
2. From the menu, select **Administrator > Admin Authentication**.
3. Select the checkbox adjacent to the “Admin Auth” method, then select **Edit**.
A form appears that enables you to update the authentication method.

Admin Authentication ⓘ

Edit Authentication Method

View Auth Methods

Reset

Choose name and type

AUTHENTICATION SERVER NAME

Admin Auth ⓘ

AUTHENTICATION TYPE

Local ▾

USER NAME ⓘ

FULL NAME ⓘ

PASSWORD ⓘ

EMAIL ⓘ

CONFIRM PASSWORD ⓘ

☐ Temporary password (require user to change password at next sign in)

ADD TO USERS LIST

🔍

EDIT

DELETE

<input type="checkbox"/>	USERNAME ↑	FULL NAME ↑	PASSWORD	CHANGE PASSWORD	EMAIL
<input type="checkbox"/>	msp	Administrator	N/A	NO	admin@ivanti.com
<input type="checkbox"/>	msp2	MSP 2	N/A	NO	admin@ivanti.com

Cancel

Update Admin Authentication

FIGURE 7.1 : Editing the Admin Auth method to add a new admin user

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

4. Enter the following settings:

- Specify a **User Name**, **Full Name**, and **Email** for the new admin 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.
- Select **Add To Users List**.

The user is added to the list of admin users.

5. Repeat the previous step for each required admin user.

6. Select **Update Admin Authentication**.