SonicOSX 7 Multi-Instance

Administration Guide for the NSsp Series

SONICWALL®

Contents

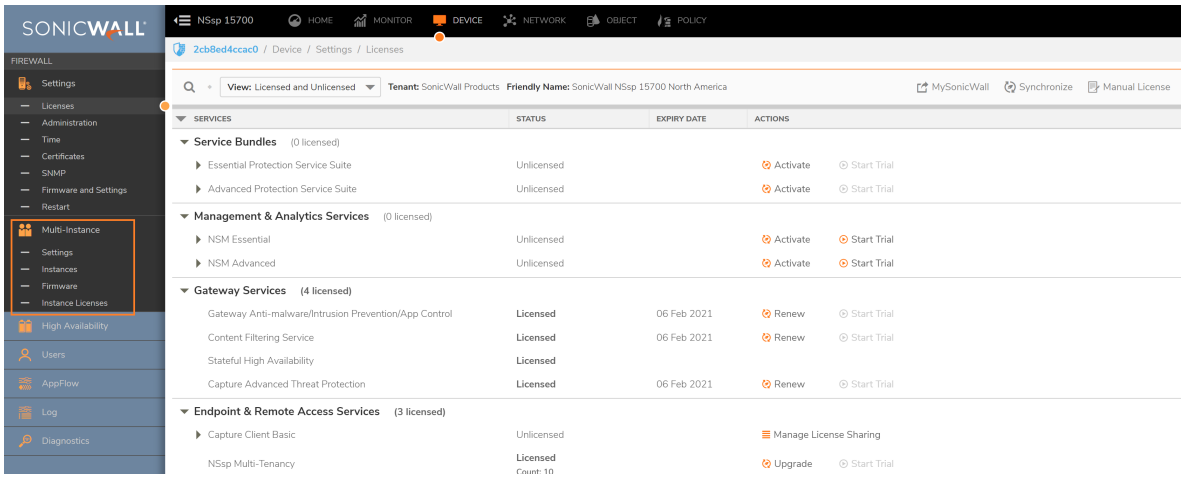
1

Multi-Instance (MI) Support

Topics:

This feature allows a security appliance to launch multiple instances of SonicOSX, each serving as an independent firewall. The Root Instance (RI) configures and launches each instance. Once the tenant instances are SonicOSX up and running, their X0…X7 interfaces allow access for detailed firewall configuration.

Navigate to **Device > Multi-Instance** to find configuration and monitoring screens.



Each tenant's X0, X1, X2… X7 interfaces will be mapped to a VLAN on the front panel port (X0 to X25) by the RI. Each tenant can be configured with up to 8 ports. Each tenant port can be mapped to a front panel port and tagged with a VLAN ID.

Enabling Multi-Instances

This feature is enabled on the GUI in the Settings screen and the number of logical blades allocated to supporting tenant instances needs to be set. Once configured, the NS_{sp} chassis will reboot and come up with Multi-Instances enabled.

This feature is enabled from the Settings screen. To enable Multi-instances, we first reserve logical blades and front panel ports that will be used for supporting tenant instances.

To select the number of logical blades, click and select up to two. Click Accept to save changes. This step requires the chassis to reboot for changes to take effect.

The next step is to reserve front panel ports for tenant instances. These ports are the ones available for tenant configuration.

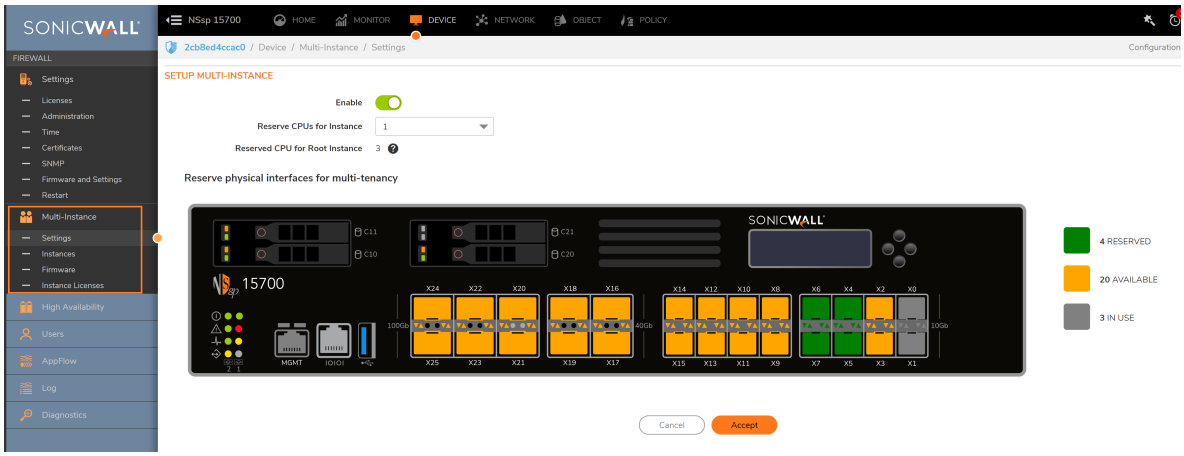
To select ports, click on ports that are orange. Selected ports turn green. The legend on the right provides details on the colors and the state of ports.

Click on Accept to save changes. This step does not require a reboot. Front panel port reservations can be modified anytime once multiple instances are enabled.

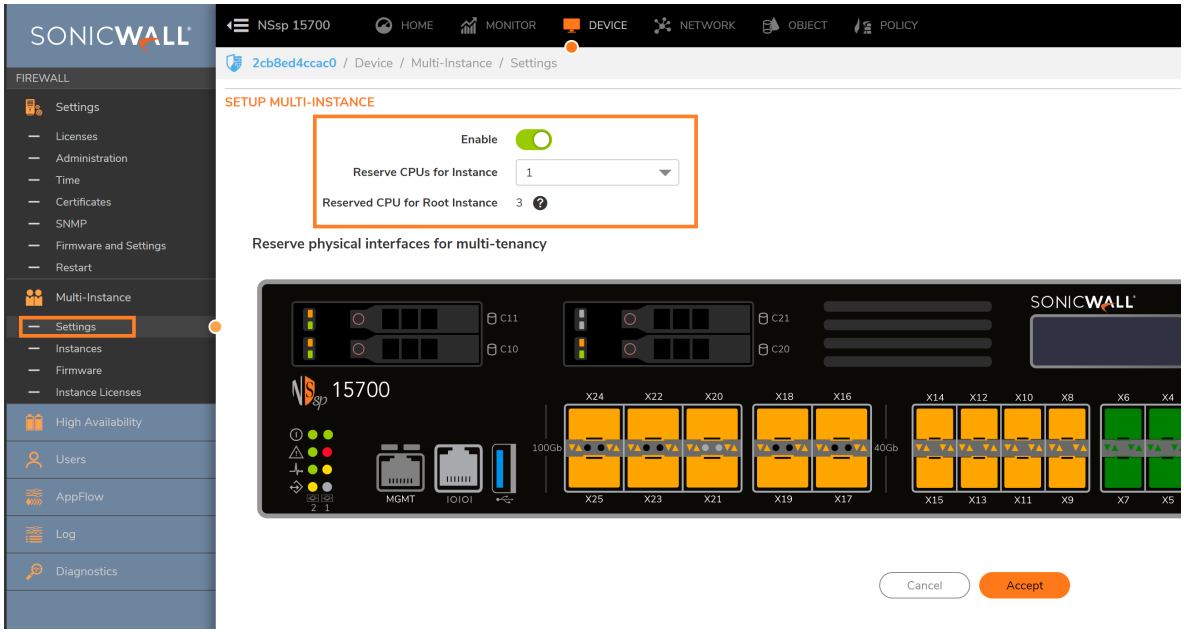
Ports reserved for the tenant instances are green, and ports available to tenant instances, but not reserved are orange. To reserve an orange port for tenant instances, simply click on it to turn it green.

Once Multi-Instances are enabled and logical blades are selected and ports are reserved, the reserved ports for Multi-Instances are exclusive, not available for the rest of the sub-system.

Any time Multi-Instances is disabled and the chassis is rebooted, all the Multi-Instance port(s) will be un-reserved and will be available to the rest of the system while all instances or tenant(s) configured in the system will be lost.



Currently, a maximum of two logical blades may be configured to support tenant instances. With four logical blades in the system, two logical blades are used by the multi-bladed firewall while the other two can be used for tenant instances. However, the configuration is flexible, we could have three logical blades running in multi-bladed firewall mode with one logical blade configured to launch tenants.



The above screen shot shows the MI enabled settings in the **Device > Multi-Instances > Settings** screen. In this case, 4 logical blades are available and 1 is allocated to tenant instances, while 3 support multi-bladed firewall operation.

Once Multi-Instance operation is enabled on the GUI and the configuration is saved, the firewall will prompt for reboot before the settings can be applied. Once the reboot firewall confirmation button is clicked, the firewall comes up with one or two logical blades enabled for launching tenant instances. On the left hand Nav, the **Tenants** screen will be enabled only when MT is enabled. In order to change the number of logical blades selected to launch MI instances, the firewall has to go through the reboot processes. This means the currently running tenant-support blades will also be rebooted.

In order to revert back, with all the logical blades to work as one big multi-bladed firewall, the MI enabled settings have to be disabled and the firewall will have to go through reboot process again.

To reserve front panel ports for virtual firewall instances:

1. Identify available ports by looking for orange colored ports on the GUI.
2. Click on the port to turn it green.
3. Click on **Accept**.

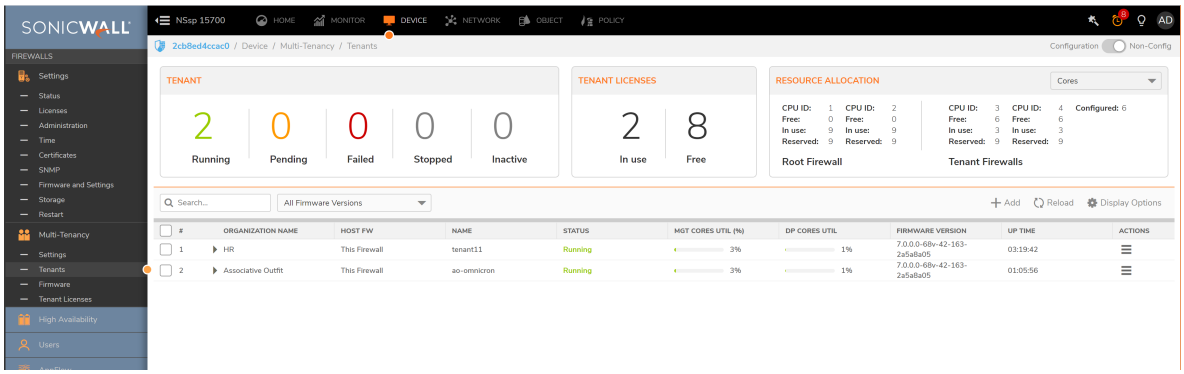
To allocate CPUs to instances:

1. Navigate to **Device | Multi-Instance > Settings** and locate the controls under **Setup Multi-Instance**.
2. Move the **Enable** switch to the right to turn on Multi-Instancre capability.
3. Determine the number of CPUs available to support instances.
4. Click on **Accept** and then reboot the system.

Multi-Instances

Once you have MI (Multi-Instances) enabled in the RI (Root Instance), then we can configure and launch the multiple instances. Each tenant instance is an independent virtual firewall with its own routing table, policy configuration, licenses and security services. Each tenant needs to be registered with the License Manager in order to enable the necessary licenses for Deep Packet Inspection (DPI). Each tenant can be configured with the required number of cores based on the use case. Currently, we support up to 8 Data Path (DP) cores max for each virtual firewall and 1 (Control Path) CP core per virtual firewall. Each tenant virtual firewall can be accessed through its DHCP-enabled X1 WAN interface. Tenant UI can be accessed via X0 as well, if tenant's X0 mapping is setup with accessible static IP, gateway and subnet and accessible to the RI front panel port, and VLAN mapping are properly set.

The following screen shot shows the Mult-Instance screen with two tenant instances in operation.



The Root Tenant (RI) serves as the console through which all the tenant instances are deployed. RT allows the user to add tenant instances, start the service, stop the service and delete the tenant. Each instance added through the Add Instance Dialog will be stored in the RI. This allows the user to add as many instances as possible, however there will be a limit on the number of instances that can be launched due to CPU core availability.

Adding an Instance

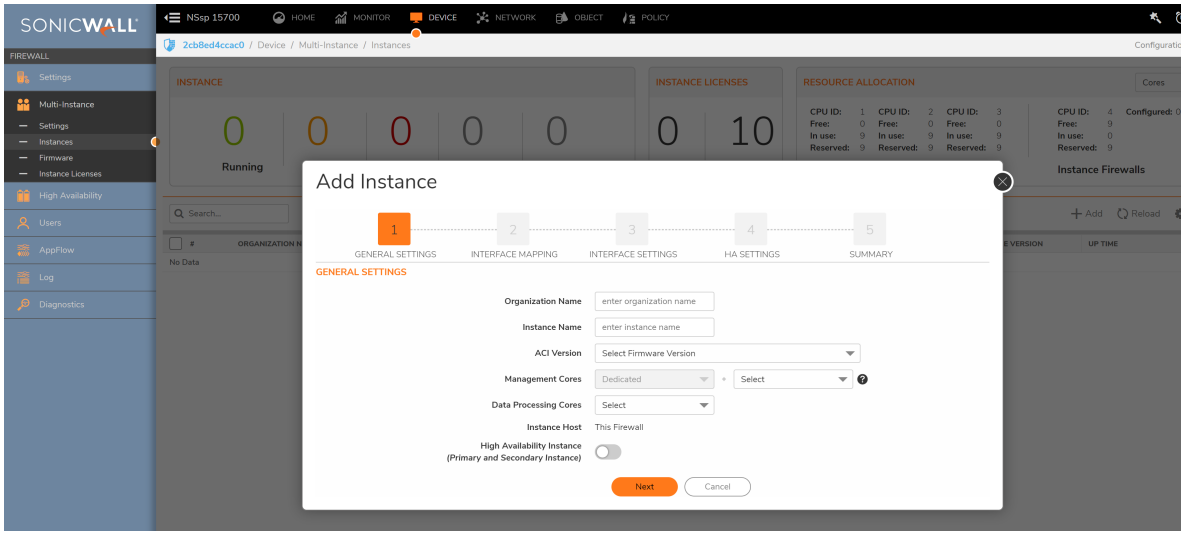
In order to add an instance, please click on the **Instance** tab on the left hand nav. On the Instance's page click on the add button and a dialog box will pop up.

There is a limit on the number of tenant instances that can be launched due to CPU core availability and total Instance Licenses available in the system.

Before this step is done, first Upload the Instance Firmware from the **Multi-Instance > Firmware** page. A typical Multi-Instance setup work flow would be:

1. Enable Multi-Instances, reserve Logical Blades, reserve port(s) and reboot chassis
2. Register the box, if not registered, to obtain instance instances
3. Verify that Tenant Instance(s) is available on the **Multi-Instance >Instance Licenses** page.
4. Upload tenant firmware from the **Multi-Instance > Firmware** page.
5. Add tenant(s), or start/stop/reboot/edit/deactivate/delete tenant(s).

Add Instance Dialog Box



In the add dialog, all the fields have to be populated.

- **Organization Name** identifies operating enterprise, a name which is a string.
- **Tenant Name** field requires a name which is a string.
- **ACI Version**. This is a drop down list and the user has to pick one of the ACI versions that needs to be running on the instance. In order to upload an ACI, please follow the instructions mentioned under Uploading Tenant SWI.
- **Management Cores** At this point, only 2 Control Plane cores can only be dedicated to a particular tenant. Select the number from the right hand pull-down.
- **Data Processing Cores**, Allows the user to select the number of DP Cores. Please limit this allocation to 8 for this release. Ideal max would be 4.
- **High Availability Tenant** Sets up redundant tenant instance: Primary (active) and Secondary (standby). At this point, only HA pairs within a single NS_{sp} are supported.

When you are complete, click on **Next**, the dialog will move to the interface mapping stage:

Setup interfaces for the tenant instance by mapping each X0, X1, X2…X7 to a physical interface from the drop down list. The drop down shows only those front panel ports that were reserved for tenants. For each interface, provide a unique VLAN. In setting VLAN IDs:

- VLAN should be in the range 65 .. 4094
- For a given instance, VLAN configured on X0 .. X7 should be unique, two or more instances of Xn can't have same VLAN.

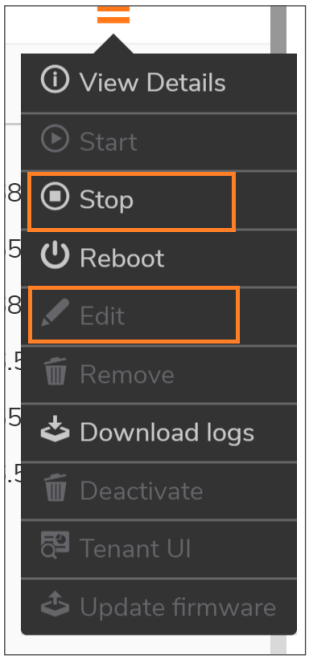
Each instance can be configured with a default X0 IP address.

Once configuring is complete, click on **Next**.

In order to launch the instance, click on the **Start** button on the Actions drop-down menu. The instance can be stopped with **Stop** button and restarted using the **Reboot** button.

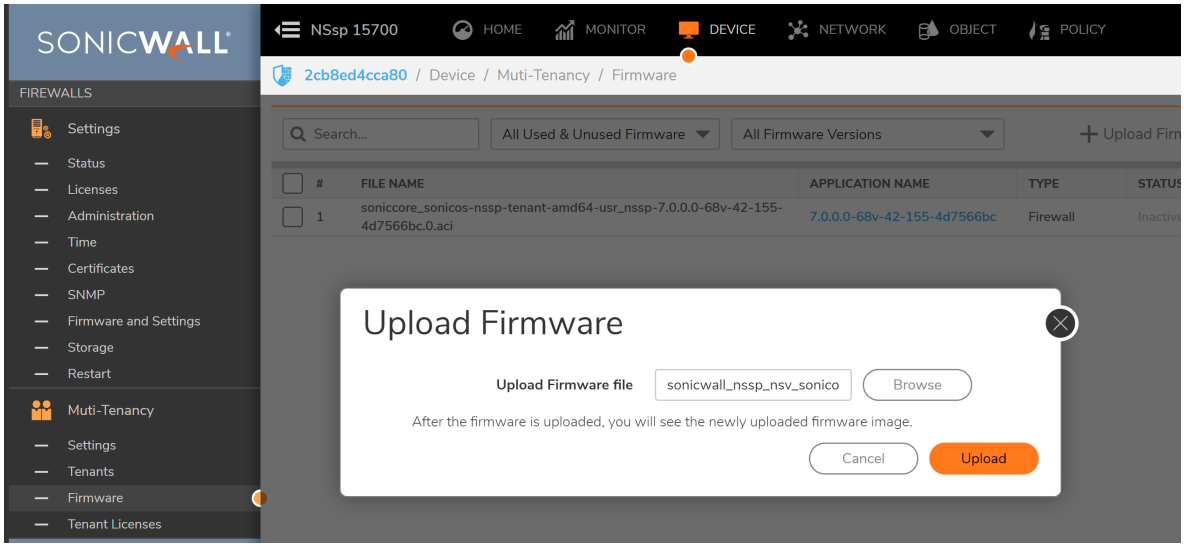
Editing an Instance

To change the configuration of an instance, click on the Action icon at the far right of the tenant instance row in the Instance page. When the menu appears choose **Stop**. Wait until the status of the tenant changes to "Stopped". This could take up to 5 minutes. Click again on the Action icon and click **Edit**.



Uploading Instance Firmware

The firmware for launching the instances has to be pre-loaded using the RT. On the **DEVICE | Multi-Instance > Firmware** page upload the SWI file as shown.



Once uploaded, the firmware appears as a choice in the **Add/Edit Instance** dialog.

NOTE: The instance firmware is not the same Root Firewall firmware. These instance firmware is exclusive to tenant(s) only.

To Upgrade Instance Firmware:

The steps for upgrading firmware for an instance are:

1. Download the firmware as described above.
2. Stop the instance.
3. Use the edit process to select new firmware.
4. Restart the instant.

Licenses for Multiple Instances

Topics

- Instance Registration
- Instance license update

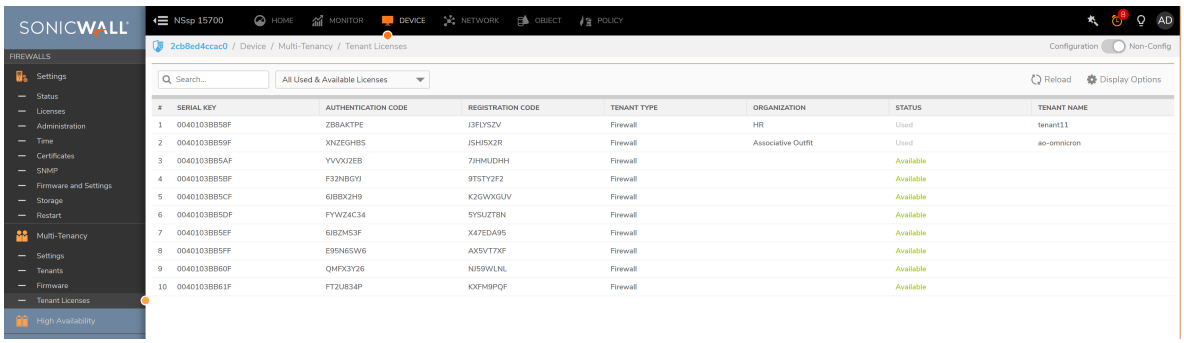
Multiple Instances

Instance licenses are required for spawning instances. The NS_{sp} Multi-Instance licenses will be fetched onto the system once the device is registered with the license manager. The licenses are then managed by the Root Tenant for spawning instances. The root tenant takes care of assigning an available instance to a tenant once it is started.

The licenses are assigned to an instance and marked as in use only when the tenant is started. The license assigned to a tenant will remain in use until an instance is deleted. Stopping an instance does not release its license.

Once all instances are consumed, a request to start a new instance would fail owing to insufficient licenses.

The Instances page will display the list of instance licenses and their status (used/available) and also the name of the instance (for licenses in use).



Instance Registration

The instance, once spawned, automatically registers itself with the license manager upon boot-up. In order for this to work fine, the VLAN for the tenant's X1 (WAN interface) should be configured properly so that it has access to WAN/internet to reach the license manager over the network. That is, the X1 interface of the tenant instance must be linked to a front panel port that has access to WAN/internet.

For further information on setting up a WAN internet connection for tenants. see "Network Configuration".

Instance license update

If a customer has purchased additional tenant instances, the licenses can be updated or upgraded by re-registering the device with license manager. The NS_{sp} Multi-Instance licenses are always designed to be bundle of previous + new tenant license. Once licenses are updated, the SonicOSX Root tenant identifies the newer set of licenses and updates the licenses shown as available on the **Instance** page.

Deactivating an Instance

Stopping an instance and removing it from the **Instance** page strips off the instance with all its resources (instance license, physical and logical resource) and renders itself into Inactive status.

2

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOSX Multi-Instance Administration Guide for the NSsp Series
Updated - August 2020
Software Version - 7
232-005401-30 Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035