



Migration Guide

CONTENTS

1. 25.x Migration	3
1.1. Prerequisites for Migration	4
2. Revision History	7
3. Migration 22.x to 25.x	8
4. Cluster Migration from 22.8Rx to 25.x	16

1. 25.x Migration

Introduction

This document describes about the guidelines and procedure for successfully migrating the ICS configurations from 22.x to 25.x. The ISA Appliance is the new next generation Secure Access Gateway with enhanced security and improved performance.

The recommended way to transfer the configuration and settings is through the export of **binary configurations** from 22.x to 25.x.

Assumptions

According to the guidelines in this document, it is assumed that you would migrate to the new environment concurrently and switching over to this once the migration steps have been completed. This method offers flexibility and allows for easy adoption of the new solution with minimal impact to existing production environments.

The following should be noted if the Administrator decides to migrate with the same network settings and certificates.

- When you migrate a cluster as-is, ensure that you form the new environment with the same cluster name and port definitions before importing the exported XML. Otherwise, , import will fail due to clashes in ports in use, existing cluster name on the same network and node hostnames.

Cluster Node Name Restriction: Cluster node names should not be configured as "localhost2". Using "localhost2" as a node name is not supported and may result in unexpected behavior.

- If you are using Active Directory or ACE authentication servers, there may be a need to recreate the computer objects. For ACE, there may also be a need to regenerate or re-import the SDCONF.REC file to the devices if authentication fails after import.

Please note that if the target environment is standalone, all cluster-related steps can simply be ignored.

1.1. Prerequisites for Migration

- **Software:** ISA Hardware or Virtual appliance should be available and online prior to starting the migration.
- **Deployment:** This is a server-to-server migration and cannot be performed in-place on the same hardware.
- **Licenses:** ISA Appliances require new licenses. Procure the new licenses and keep them handy.
 - ISA hardware would not require any additional core/CPU licenses.
- **Settings:** Identify the network settings for each of the configured ports for the target ISA gateway.
- **Configuration backup:** It is preferred to back up the system.cfg and user.cfg binary files, along with XML export of entire configuration immediately prior to migration. For more information, see [Exporting Configurations](#)
- **Upgrade:** It is recommended to upgrade your existing 22.8R2 ISA Appliance to 25.1.0.0 or later and import backup configure to ISA Appliance only, if required.
- **Configuration documentation:** Local settings that are mostly kept in system.cfg should be documented, as some of these may need to be manually re-entered to the ISA device.

Note down the following settings before migration:

- IP Pool filters
- Cluster configuration
- Virtual port configuration and certificates mapping
- SNMP configuration
- Log settings,
- Syslog can be configured in either cluster mode or individual nodes.
- Deprecated features are not supported in 25.1.0.0. Please refer to [Deprecated Features](#) for the list of deprecated features.

Connect Secure only: In an **Active/Active** cluster, attention should be given to the Network > VPN Tunneling > IP address filter and VPN Tunneling Profile IP pool settings. This is particularly important as the assumption of this guide is that both the existing and target deployment will be active at the same time. If the IP pools overlap, this may cause impact to production users if testing is done on the target deployment during production time. Specifically, the same IP may be leased to two independent users which will cause addressing clashes.

Some settings such as SNMP, Log settings, and the Syslog configuration can be set in either cluster mode or individual nodes.

Configuration Migration Path

The following table describes the tested migration paths.

Migrate to	ISA Hardware device Migrate From (Supported Versions)	VA Migrate From (Supported Versions)
Connect Secure		
25.1.3.1	25.1.3.0 , 25.1.2.2, 25.1.1.1, 22.7R2.14	25.1.3.0 , 25.1.2.2, 25.1.1.1, 22.7R2.14
25.1.3.0	25.1.2.2, 25.1.2.1, 25.1.2.0, 25.1.1.1, 25.1.1.0, 22.8R2.4, 22.7R2.14	25.1.2.2, 25.1.2.1, 25.1.2.0, 25.1.1.1, 25.1.1.0, 22.8R2.4, 22.7R2.14
25.1.2.2	25.1.2.1, 25.1.1.1, 25.1.0.1, 25.1.1.0, 22.8R2.4, 22.8R2.3, 22.7R2.13, 22.7R2.12	NA
25.1.2.1	25.1.0.1, 25.1.1.0, 22.8R2.3, 22.7R2.12	NA
25.1.2.0	25.1.1.0, 22.8R2.3, 22.7R2.12	NA
25.1.1.1	25.1.1.0, 22.8R2.3	25.1.1.0, 22.8R2.3
25.1.1.0	25.1.0.1, 25.1.0.0, 22.8R2.3, 22.8R2.2, 22.8R2.1, 22.7R2.12, 22.7R2.11	25.1.0.1, 25.1.0.0, 22.8R2.3, 22.8R2.2, 22.8R2.1, 22.7R2.12, 22.7R2.11
25.1.0.1	25.1.0.0, 22.8R2 and 22.7R2.8	25.1.0.0, 22.8R2 and 22.7R2.8
25.1.0.0	22.8R2, 22.7R2.8, and 22.7R2.7	22.8R2, 22.7R2.8, and 22.7R2.7

Upgrade the servers to the nearest matching version per the table to proceed with Migration if the exact versions are not listed.

Deprecated Features

To improve stability and overall security posture in new ICS, Ivanti has decided to deprecate old set of features. For Ivanti Connect Secure: Features and Options Becoming Unsupported or Deprecated in 22.7Rx, 22.8Rx, and 25.x, refer to [article](#).

Configs with deprecated features will be upgraded or imported to 25.x but will not be qualified. Please refer the [KB](#) for more details

Refer to [Prerequisites for Migration](#) and Supported [Configuration Migration Path](#) before starting the migration.

Post Migration Activities

After performing the migration steps, it is recommended that the following settings be checked and validated manually:

1. **System > Network > Overview settings** (set in cluster or individual nodes).
2. **System > Network > Routes** (for internal, external and other ports).
3. **System > Network > Hosts** (set in cluster or individual nodes).
4. **System > Network > Internal Port/ External Port>Virtual Ports** (if clustered, set this up in cluster "Entire Cluster").
5. **System > Network > VLANs** (if clustered, set this up in cluster "Entire Cluster").
6. ICS only- **System > Network > VPN Tunneling** (set in cluster or individual nodes).

7. **System > Log/Monitoring > SNMP** (set in cluster or individual nodes).
8. **System > Configuration > Certificates > Device Certificates** (and its ports bindings).
9. ICS only - **Users > Resource Policies > VPN Tunneling > Connection Profiles** (if configured).
10. **System > Configuration > Licensing** - License client-server settings (if used as license client in Enterprise Licensing Server environment), proper licenses installed.

2. Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
5.0	August 2026	Update config migration path
4.0	July 2026	Update config migration path
3.0	May 2026	Update config migration path
2.0	April 2026	Update config migration path
1.0	September 2025	Initial Publication

3. Migration 22.x to 25.x

On the existing 22.x ICS. Log in to the standalone device or the primary node of the cluster (where the cluster was first formed) and export its binary configs (system.cfg and user.cfg), and the XML Network settings configurations.

Refer to [Prerequisites for Migration](#) and Supported [Configuration Migration Path](#) before starting the migration.

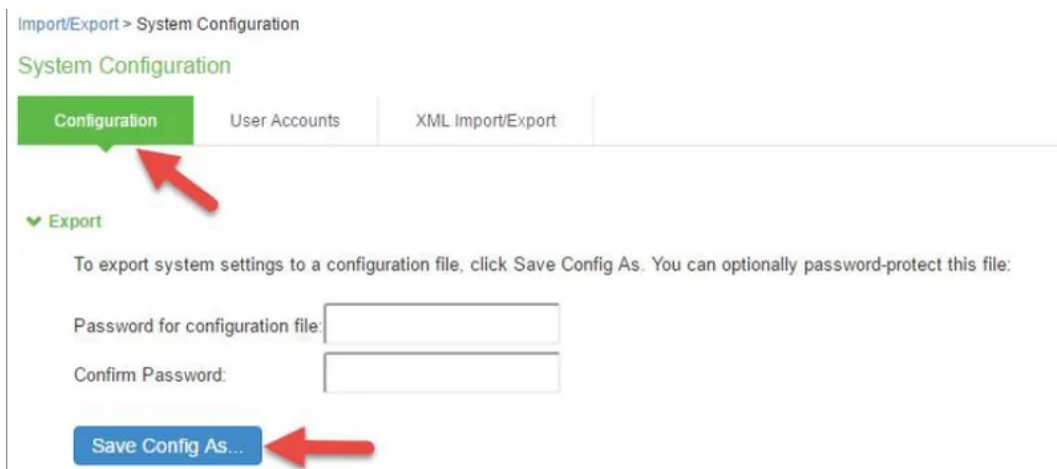
Migration procedure explained in this document applies to both ISA and ISA-V Appliance.

Exporting Configurations

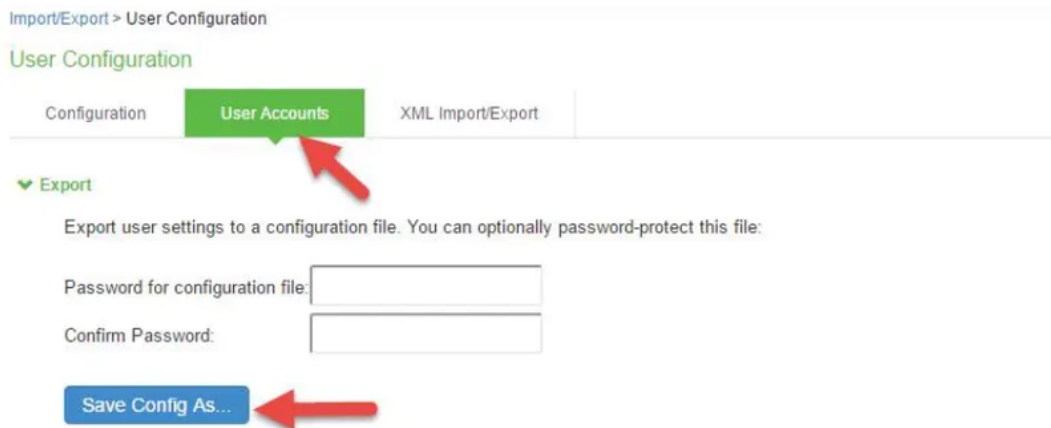
Ivanti recommends that you export the System and User binary config and the entire XML configuration. This provides you with the greatest possibilities for restoring or migrating the configuration. However, using the binary exports in the first instance is recommended when importing.

To export the binary configurations from the 22.x:

1. From the 22.x Admin UI, select **Maintenance > Import/Export > Configuration**.
2. Under Export, enter a password if you'd like to password-protect the configuration file.
3. Click **Save Config As** to save the file. The default filename is *system.cfg*.



4. Select **Maintenance > Import/Export > User Accounts**.
5. Under **Export**, enter a password if you would like to password-protect the configuration file.
 - If you choose to password-protect the file, ensure that the password is stored in a long-term sustainable location. There is no way to recover the password or decrypt the file if the password is lost.
6. Click **Save Config As** to save the file. The default filename is *users.cfg*.



To export the XML Network configuration:

1. Select **Maintenance > Import/Export > XML Import/Export**.
2. Under **Export**, expand **System Settings** and select **Select All System Settings**.
3. Click **Export** and save the XML file.



Make notes of all the local settings for both nodes (if not yet done during preparation stage): IP information, clustering, virtual ports, VLANs, hosts, routes, DNS settings, SNMP (if configured) and Syslog settings.

Configuring Devices

1. Configure the new devices with the network settings identified in the [Prerequisites](#) section.

The settings to configure are:

- Internal Virtual Ports
 - External Virtual Ports
 - Management Ports
 - VLANs
 - Static Routes
 - Port settings
2. Apply the entitled/purchased licenses to the individual GW or Cluster or connect to the license server through Gateway licensing Mode.

If you are migrating a non-clustered device, skip next 4 steps and proceed.

3. In the new ISA device (first device), manually create a new cluster and ensure that this does not conflict in settings or naming with your existing production cluster.

Clustering > Create New Cluster

Create New Cluster

Join

Create

Type:

Cluster Name:

Cluster Password:

Confirm Password:

Member Name:

GEC1

Create Cluster

Confirm Create Cluster

Are you sure you want to create a new cluster *GEC_CLUSTER* ?

Please click **Create** to create a new cluster and add this appliance with member name *GEC1* to the cluster.
Click **Cancel** if you do not want to create a cluster.

Create

Cancel

4. Add the second device to the cluster in the primary node cluster configuration and save the settings.

a. Click **Add Members** to add a member.

Clustering > Cluster Status

Cluster Status

Status Properties

Cluster Name:

Type: Configuration Active/Active

Add Members Enable Disable Remove

10 records per page

Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
GEC1	10.209.69.44/22		Leader		0	

Previous 1 Next

b. Enter member node name and IP and check netmask and gateway, then click **Add**.

c. Click **Save Changes**.

Clustering > Cluster Add

Cluster Add

Cluster: --

Delete

Node Name	Internal IPv4 address	Internal IPv4 Netmask	Internal IPv4 Gateway	Add
GEC2	10.209.69.44	255.255.252.0	10.209.71.254	

Note: after the changes are saved, you must click "Network" on the left panel to check and ensure the network settings for all new nodes are fully configured prior to their joining. Keep in mind that the entire state currently on the new nodes will be completely overwritten during the joining process.

Save Changes Cancel

d. Check cluster **status**.

The status turns **transitioning** for short period, then the first node becomes enabled, and the status turns as **Leader**. The second node remains **Enabled, Unreachable** until it joins the cluster.

Clustering > Cluster Status

Cluster Status

Status Properties

Cluster Name:

Type:

Configuration: Active/Passive

Internal VIP on GEC1:

IPv4: 10.209.69.55

IPv6: not defined

Add Members... Enable Disable Remove Fail-Over VIP?

10 records per page

Search:

Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
GEC1	10.209.69.45/22		Leader		0	
GEC2	10.209.69.44/22		Enabled, Unreachable		0	

← Previous 1 Next →

For full clustering guidance, please refer to the [Clustering Configuration Guide](#) which handles this topic in-depth.

5. If the XML config is exported from an **Active/Passive** Cluster, following needs to be done prior to XML Import:

- Configure External Port for the Cluster Members (if external ports are configured in cluster).
- Go to **Clustering > Cluster Properties** page. Change the Cluster Type from **Active/Active** to **Active/Passive** and add the cluster VIP address/es (the example here does not use external port

Clustering > Cluster Properties

Cluster Properties

Status Properties

Type:

Cluster Name:

Cluster Password:

Confirm Password:

Configuration Settings

☒ Active/Passive configuration

This is a high-availability failover mode, in which one node is active while the other is held as backup.

Internal VIP:

IPv4: 10.209.69.55

×

IPv6:

External VIP:

IPv4:

IPv6:

☐ Active/Active configuration

c. Save the cluster configuration settings.

Advanced Settings

☐ Enable Advanced Settings

Save Changes

Delete Cluster...

d. Change confirmation will appear confirming change from **Active/Active** to **Active/Passive**.

[Clustering](#) > Cluster Properties

Cluster Properties

Status

Properties

i info: Internal(IPv4) VIP changed to 10.209.69.55



i info: Cluster Pair switched to Active/Passive mode



Type:

Cluster Name:

Cluster Password:

Confirm Password:

e. Log in to the second device and join this node to the cluster by **Clustering > Join Cluster**.

Clustering > Join Existing Cluster

Join Existing Cluster

Join

Create

Cluster Name:

Name of the cluster to join

Cluster Password:

••••••••

Existing Member Address:

10.209.69.45

Internal IP address of any existing cluster member

Join Cluster

f. Click **Join**.

Confirm Join Cluster

This node will next contact the cluster member '10.209.69.45' and ask to join the cluster *GEC_CLUSTER*. If this succeeds, the node will join as member of the cluster.
WARNING: This host's entire state will be overwritten with the current cluster configuration, including bookmarks, IP address, netmask etc.

Please click **Join** to join the cluster.
 Click **Cancel** to return to the previous page.

Join

Cancel

6. Log in to primary node and check cluster status and it should stabilize in a few minutes.

Clustering > Cluster Status

Cluster Status

Status

Properties

Cluster Name:

Type:

Configuration: Active/Passive

Internal VIP on GEC1:

IPv4: 10.209.69.55

IPv6: not defined

Add Members...

Enable

Disable

Remove

Fail-Over VIP

10

records per page

Search:

	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
☐		10.209.69.45/22		●	Leader	0	
☐		10.209.69.44/22		●	Enabled	0	

Importing existing ISA configurations

To import the ISA configurations:

1. From the ISA Appliance Admin UI, select **Maintenance > Import/Export > Configuration**.
2. Select **Import Everything except network settings, cluster settings, and licenses** to import all configurations except network, cluster and license settings.
3. Browse to the configuration file, system.cfg. Enter the password if specified.
4. Click **Import Config**.

Import/Export > System Configuration

System Configuration

Configuration	User Accounts	XML Import/Export
----------------------	---------------	-------------------

Export

To export system settings to a configuration file, click Save Config As. You can optionally password-protect this file:

Password for configuration file:

Confirm Password:

Save Config As...

Import

To import system settings from a configuration file, select the configuration file and which settings to bring in, and click Import Config. A Options:

☐ Import Device Certificate(s)?
Note: Checking this will overwrite the existing Device Certificate(s).

Other Import Options: ☐ Import everything (except Device Certificate(s))

☐ Import everything but the IP address

Preserves the IP address, netmask, default gateway, VIPs, ARPs and routes of the network interfaces on this device.

Note: Use this option only if the exported configuration file is from a standalone node.

☒ Import everything except network settings, cluster settings and licenses

Leaves everything in Network Settings, Clustering Properties, Licensing sections and Onboarding Profile UUID unchanged.

Note: Always use this option if configuration file was exported from a node that is part of a cluster.

☐ Import only Device Certificate(s)

Imports the Device Certificate(s) only.

Note: You must check the Import Device Certificate(s) checkbox above.

Config File: **Browse** No file chosen

Password: Use this if the configuration file was password-protected

Import Config

5. Select **Maintenance > Import/Export > User Accounts** and browse to the users.cfg file.

6. Click **Import Config**.

Import/Export > User Configuration

User Configuration

Configuration	User Accounts	XML Import/Export
---------------	----------------------	-------------------

Export

Export user settings to a configuration file. You can optionally password-protect this file:

Password for configuration file:

Confirm Password:

Save Config As...

Import

Import user settings by selecting the configuration file and clicking Import Config. Import User Accounts will invalidate all existing End-User and Administrators sessions.

Browse No file chosen

Password. Use this if the configuration file was password-protected

Import Config

Import XML

ConfigurationUser AccountsAdministrative NetworkXML Import/Export

ExportExport UniversalImport

Schema Files

Download the [Schema files](#)

To import data, select a valid XML data file, then click Import.

* XML data file: Browse No file chosen

Import

7. Check cluster status (if clustered) and test operation by logging in to the cluster VIPs (or the standalone device IP).

Clustering > Cluster Status

Cluster Status

StatusProperties

Cluster Name:

Type:

Configuration: Active/Active

Add Members...EnableDisableRemove

10 records per page

Search:

	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
☐	* c62	10.209.113.62/20	10.30.113.62/16		Enabled	0	
☐	c92	10.209.113.92/20	10.30.113.92/16		Leader	0	

← Previous1Next →

4. Cluster Migration from 22.8Rx to 25.x

ICS deployments in a cluster running Active/Passive or Active/Active configurations cannot be upgraded directly from version 22.8Rx to version 25.x. Each node must be individually disabled or removed from the cluster and upgraded separately. This process applies to both ISA hardware and ISA-V virtual appliances. Review the steps below to perform a step-by-step upgrade with a planned downtime.

Known Limitations

Cluster Node Name Restriction: Cluster node names should not be configured as "localhost2". Using "localhost2" as a node name is not supported and may result in unexpected behavior.

You must perform one of the following approaches for migrating from 22.8Rx to 25.x:

- [Option1: Delete and Recreate the Cluster](#)
- [Option2: Disable one Node](#)

Option1: Delete and Recreate the Cluster

To delete and recreate the cluster perform the following:

1. **Review Cluster Status**, Navigate to **System > Clustering > Cluster Status** to verify the current status of the cluster.

Cluster Name: Test
Type: ISA-V
Configuration: Active/Active

Buttons: Add Members..., Enable, Disable, Remove

Member Name	Internal Address	External Address	Status	Notes	Sync Rank
Node-12	10.34.109.12/24		Enabled		0
Node-48	10.34.109.48/24		Leader		9

* Indicates the node you are currently using

2. **Delete the Cluster**, Navigate to **System > Clustering > Properties** tab and click **Delete Cluster** to remove the current cluster.



3. **Upgrade Nodes Individually**, Upgrade **each node** in the cluster to the ICS 25.x package. Follow standard upgrade procedures for your platform.

System Maintenance > Install Service Package

Install Service Package

Platform **Upgrade/Downgrade** Options Installers

Installing a service package can take several minutes and requires the system to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your **system log** before trying to install a service package.

Note: Browsing away from this page while uploading the package will abort the installation.

Install Service Package

☐ From File

Browse No file chosen (**WARNING:** Please ensure that the steps recommended in KB44877 have been performed without fail before initiating upgrade.)

☐ From Staged Package

Choose this option if you want to install the staged service package.

☐ **DELETES** all system and user configuration data before installing the service package, restoring the member to an unconfigured state. Use this option if you want to downgrade to an older service package than the currently installed package. **Do NOT check this box** if you want to retain existing settings and data during a system upgrade to a newer service package.

Note: This option does not change the factory image.

Install

4. **Recreate the Cluster**, After all nodes are upgraded, re-create the cluster by following the standard cluster creation steps.

System Authentication Administrators Users Maintenance Wizards

Clustering > Join Existing Cluster

Join Existing Cluster

Join Create

Cluster Name: Name of the cluster to join

Cluster Password:

Existing Member Address: Internal IP address of any existing cluster member

Join Cluster

Options2: Disable one Node

Important Notes:

- When upgrading clustered nodes, after disabling and upgrading the second node (N2), it cannot rejoin the cluster until the first node (N1) is also upgraded to the same version.
- Upgrading N1 will result in both nodes being unavailable, causing complete downtime until the upgrade is completed.
- Recommendation: Plan your upgrade window carefully, as downtime cannot be avoided in this scenario. Breaking the cluster will also result in both nodes being offline. Ensure stakeholders are informed about the expected service interruption.

To disable the node and then to upgrade perform the following:

1. **Disable a Node**, Navigate to **System > Clustering > Cluster Status**, select the **node** you want to upgrade, and click **Disable**.

System Authentication Administrators Users Maintenance Wizards

Clustering > Cluster Status

Status Properties

Cluster Name: cluster-debug

Type: ISA000-V

Configuration: Active/Passive

Internal VIP on node-128: IPv4: 10.34.26.21 IPv6: 1070:1034:24::7221

External VIP on node-128: IPv4: 10.34.127.221 IPv6: 1070:1034:127::7221

Add Members... **Enable** **Disable** **Remove** **Fail-Over VIP**

20 records per page

	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
☐	node-128	10.34.24.128/22	10.34.127.44/24	Leader		0	
☒	node-129	10.34.24.129/22	10.34.127.45/24	Enabled		0	

* Indicates the node you are currently using

Previous 1 Next

2. **Upgrade the Disabled Node**, Upgrade the disabled node to the ICS 25.x package.

The screenshot shows the Ivanti Connect Secure web interface. At the top, there's a navigation bar with the Ivanti logo and several tabs: System, Authentication, Administrators, Users, Maintenance (which is highlighted), and Wizards. Below the navigation bar, the breadcrumb trail reads "System Maintenance > Install Service Package". The main heading is "Install Service Package". There are three tabs below the heading: Platform, Upgrade/Downgrade (which is active and highlighted in green), and Options. A note states: "Installing a service package can take several minutes and requires the system to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your [system log](#) before trying to install a service package." Another note says: "Note: Browsing away from this page while uploading the package will abort the installation." Under the heading "Install Service Package", there are two radio button options: "From File" and "From Staged Package". The "From File" option is selected. It includes a "Browse" button and a warning message: "[WARNING: Please ensure that the steps recommended in KB44877 have been performed without fail before initiating upgrade.]". The "From Staged Package" option has a checkbox labeled "DELETES all system and user configuration data before installing the service package, restoring the member to an unconfigured state. Use this option if you want to downgrade to an older service package than the currently installed package. Do NOT check this box if you want to retain existing settings and data during a system upgrade to a newer service package." A final note at the bottom says: "Note: This option does not change the factory image." At the very bottom, there is a blue "Install" button.

3. **Repeat for Each Node**, If applicable, repeat the disable/upgrade process for all nodes in the cluster.
4. **Enable Upgraded Nodes**, After upgrading, navigate to **System > Clustering > Cluster Status**, select the upgraded node, and click Enable.

Cluster Status

Cluster Name: cluster-debug
 Type: ISA4000 V
 Configuration: Active/Passive

Internal VIP on node-128:
 IPv4: 10.34.26.21
 IPv6: fdf7:1034:24::f221

External VIP on node-128:
 IPv4: 10.34.127.221
 IPv6: fdff:1034:127::f221

Action	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
☐	node-128	10.34.24.128/22	10.34.127.44/24	●	Leader	0	[Update]
☒	node-129	10.34.24.129/22	10.34.127.45/24	○	Disabled	0	[Update]

* Indicates the node you are currently using

5. **Verify Cluster Status**, Once all nodes are enabled and upgraded, verify the cluster status in **System > Clustering > Cluster Status**.

Cluster Status

Status

Properties

Cluster Name:

cluster-debug

Type:

ISA1000-V

Configuration:

Active/Passive

Internal VIP on node-128:

IPv4: 10.34.26.21

IPv6: fd70:10:34:24::7221

External VIP on node-128:

IPv4: 10.34.127.221

IPv6: fd70:10:34:127::7221

Add Members...

Enable

Disable

Remove

Fail-Over VIP

20

records per page

Search:

	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
☐	* node-128	10.34.24.128/22	10.34.127.44/24	●	Leader	0	
☒	node-129	10.34.24.129/22	10.34.127.45/24	●	Enabled	0	

* indicates the node you are currently using

← Previous

1

Next →

Ensure you have appropriate backups before beginning the upgrade.

Carefully plan the upgrade to avoid downtime, especially for clusters in production environments.

Post-upgrade, verify that cluster operations and failover functionality are working as expected.