Planning Your Upgrade to
HCL Notes and Domino 12.0

September 8, 2021

Please email corrections or comments to kendra.bowker@hcl.com

Table of Contents

Chapter 1 Introducing Domino and Notes 12.0

HCL Domino and Notes 12.0 introduces many new features for administrators, users, and developers alike. This guide will help you deploy this release so that you can take advantage of them. But first, read about what's new.

What's new for Domino administrators?

For the list of new features for the Domino Administrator and Domino server, see What's new in Domino 12? in the Domino documentation.

What's new for Notes users?

For the list of new features for Notes users, see What's new in Notes 12? In the Notes documentation.

For requirements for each new feature, see the article Requirements for new features in HCL Notes 12 on the HCL Software support site.

What's new for developers?

For the list of new features for developers, see What's new in Domino Designer 12? the Domino Designer documentation.

What's been removed?

The following components are no longer provided with Domino and Notes 12.0:

- Notes Client Single Logon. This feature, which synchronized Notes and Windows passwords, is no longer available and has been removed as an HCL Notes® client install option. Note that this is a different feature than Notes shared login, which continues to be supported.
- The Notes preloader is no longer included with the Notes install kit.
- The Web Administrator template, webadmin.ntf, is no longer included with Domino.
- The Notes 8 theme in the Notes client is deprecated. If you currently use it, after you upgrade to Notes 12, the Notes 11 theme is used.

Domino versions supported for upgrade to 12.0

HCL has tested upgrades from V10 to V12 and V11 to V12. Upgrades from V9.01 and earlier versions are expected to work but haven't been tested. If upgrading from a V9.0.1 or earlier release, see the requirements stated in this knowledge article KB00812302.

Domino directory changes in V12

The following changes were made to the Domino directory in V12. These changes are available after you upgrade the V12 Domino directory design.

- Several individual enhancements were made to the Domino directory that are not tied to larger features. For more information on each of these, see the section Stand-alone Domino directory enhancements in the Domino documentation.

- The following changes to the Domino directory support configuring the new feature time-based one-time password (TOTP) authentication:
    - Multi-Factor Authentication Certificates in the Certifiers view. For more information, see 1. Issuing a vault trust certificate for TOTP.
    - Multi-Factor Authentication section in the Security tab of the Configuration Settings document. For more information, see 2. Enabling TOTP authentication in the Configuration Settings document
    - Options for enabling TOTP in the Server document. For more information, see Enabling TOTP authentication for a server through a Server document.
    - Options for enabling TOTP in a Web Site document. For more information, see Enabling TOTP authentication for a server through a Web Site document
    - Options for enabling TOTP in a Virtual Server document. For more information, see Enabling TOTP authentication for a server through a Virtual Server document
    - Options for enabling secure mail for TOTP users with Notes IDs in a Security Settings document. For more information, see Enabling secure mail operations for TOTP.
- In the Security section of the Configuration Settings document, these new fields have been added to the **Enforce Internet Password Lockout** field: **Also enforce lockout based on IP address** and **Count user name failures also as IP address failures**. For more information, see Using Internet password lockout.
- The People view of the Domino directory now includes the option **Upload ID files to ID vault**. For more information, see Uploading user IDs to a vault manually.
- The Server document, Web Site document, and Web SSO Configuration document have the new field **SameSite cookie attribute**. For more information, see Configuring the SameSite cookie attribute.
- The DAOS tab of the Server document includes a new field **DAOS object encryption** used to choose whether to encrypt DAOS attachments with a shared key (new in V12) or a private key. For more information, see Encrypting DAOS attachment files.
- In the Mail > Basics tab of a Mail Settings policy, there are new options to control the behavior of the **Set outgoing limits** settings. For more information, see Prevent or allow messages that exceed outgoing limits.
- To support the new feature Active Directory password synchronization, the Server document and the Configuration settings document have a new tab **Active Directory Password Sync** with configuration fields. For more information, see Configuring password synchronization.
- References to SSL in the Domino directory interface have been changed to TLS.
- Fields and their embedded help referencing obsolete features and technologies were deleted on several forms.
- All applet use was discontinued in the web interface. This makes some things work in a web browser that weren't working before (though not everything).
- A view and some forms to support the integrated panagenda Marvel Client Essentials were added.

- In several end-user facing views that display Person documents, form formulas were deleted because they only applied to Notes/Domino versions long out of support. This corrected an issue with composing non-Person documents from those views.
- No significant changes were made to existing hidden views.

Chapter 2 Security considerations prior to upgrading

It's important to review your security practices before upgrading, especially if you are upgrading from an old version. Now is a good time to meet with your security team and understand any new security requirements or guidelines for your industry or organization. Review the security section of the Domino documentation.

This chapter describes of some of the security changes and features introduced since version 9.0.1 to consider using in your environment. Domino V12 introduces many security enhancements. Most are described here, but for a complete listing see the section New security features and enhancements in the Domino 12 documentation.

Certificate management with CertMgr

Domino V12 introduces a new server task, Certificate Manager (CertMgr), that works with a new database, Certificate Store (certstore.nsf) to manage TLS certificates in your Domino environment. You use CertMgr and certstore.nsf to completely automate requesting, configuring, and renewing free, widely trusted TLS certificates from the Let's Encrypt® certificate authority (CA). You can also process certificate signing requests for other third-party CAs. In this case, you manually submit the generated CSR to the CA, and paste the certificates received into certstore.nsf.

Certificates generated through Certificate Manager are securely stored directly in TLS Credentials documents in certstore.nsf rather than in keyring files on disk as was done previously.

Note: An Internet site document still needs to have a value specified in the Key file name field when CertMgr is used. This value should typically be the server host name.

For more information on CertMgr, see Managing TLS certificates with Certificate Manager in the Domino documentation.

Important: If you upgrade a Web server and don't use CertMgr

If you upgrade a Web server that stores TLS certificates in keyring files on disk and don't run CertMgr, if client certificate authentication is enabled on the server, after the upgrade, web users will be unable to log in. For more information and steps to correct the issue, see the knowledge article KB0092163 on the HCL Software support site.

Time-based one-time password authentication (TOTP)

Domino V12 introduces TOTP for multi-factor authentication for web users. Time-based one-time password (TOTP) authentication provides an extra layer of security when users authenticate to a Domino web server. When TOTP is enabled, users are required to provide a time-based one-time password (token) in addition to their names and passwords. Session time-out that is configured on the Domino server controls how often users are prompted to log in and provide both credentials. For more information, see the section Time-based one-time password (TOTP) authentication in the Domino documentation.

Ciphers

In Domino V12, the TLS 1.2 ciphers that use Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) for forward secrecy now support two new curves for forward secrecy: X25519 and X448. These offer better performance and space efficiency than the equivalent NIST Prime curves and are simpler to implement in an error-free fashion. For more information, see Two new curves supported for TLS 1.2 ciphers that use ECDHE for forward secrecy.

In addition, a Domino V12 server configured to use an ECDSA keyring file ECDSA credentials via CertMgr or kyrtool supports the following two TLS 1.2 cipher suites, which are supported by most current browsers and devices:
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC02B)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC02C)

Note: If you are upgrading from V9.0.1, carefully evaluate your cipher settings. If you currently use the notes.ini setting SSLCipherSpec, after you upgrade to V12, these settings are moved to the server document or Internet Sites document (depending on configuration). SSLCipherSpec notes.ini setting is ignored.

Review the list of ciphers that were deprecated in V11 and their impact on server configuration, see KB0074597.

SameSite cookie attribute

Domino V12 introduces support for use of the SameSite cookie attribute to reduce the risk of cross-site request forgery (CSRF). You can configure the SameSite cookie in these documents in the Domino directory: Server document, Web Site document (single server), or Web SSO Configuration document (multiple servers). Alternatively, you can configure the attribute through a notes.ini server setting. For more information, see Configuring the SameSite cookie attribute in the Domino documentation.

Internet password lockout based on IP address

Domino V12 extends the internet password lockout feature. By default, lockouts are enforced for users in the Domino directory. You can now also enforce lockouts for users who are not in the directory according to IP addresses. If you enable this option, you can also require that to access a server, IP addresses with X-Forwarded-For headers must be included in a trusted proxies list in the Server document. For more information, see Using Internet password lockout.

Server Name Indication (SNI) Support

Support for SNI was introduced in V11.0.1. SNI is an extension to the TLS protocol. It enables Domino to support multiple virtual hosts over HTTPS when you have multiple hostnames mapped to a single IP address. For more information, see the Enabling support for Server Name Indication (SNI).

Note: ENABLE_SNI=1 enables the 11.0.1 SNI functionality that is only used as a fallback in V12 if the certstore.nsf is being used. It is still supported in V12 to avoid breaking compatibility on upgraded servers, but is obsolete if the server's TLS credentials are stored in certstore.nsf instead of keyring files.

Authenticating web users against Notes ID passwords in the ID Vault

When enabled, this feature (introduced in V11.0.1) allows HCL Verse, HCL iNotes and other web users with Notes IDs to provide their web name and Notes ID password to authenticate to the Domino server. This allows the users to remember one password, the Notes ID password. Without this feature the web users must use their HTTP password, and then are prompted for the Notes ID password when performing secure mail operations if their Notes ID password is different than their HTTP password. For more information, see Authenticating web users against the Notes ID passwords in the ID vault.

Cross Origin Resource Sharing (CORS)

This feature was introduced in V10.0.1 and allows a web application from another origin to access resources on the Domino web server. For security reasons, most browsers comply with the same-origin policy rule. This rule restricts a web page loaded from one origin from accessing the resources on a different server or origin. CORS allows you to define exceptions to the same-origin policy. For more information on using CORS, see Configuring cross-origin resource sharing (CORS).

Improved DAOS object encryption

Beginning with Domino V12, you can create a shared key that multiple servers that are enabled for DAOS can use to encrypt objects. In addition, when you encrypt objects with the server ID file, you can now choose AES-128 or AES-256 bit encryption.

Note: If you anticipate needing to revert a Domino 12 server to a pre-11.0.1 version, before upgrading the server to Domino 12, add the following notes.ini setting to force Domino to use the legacy encryption for DAOS objects: DAOS_NLO_ENCRYPTION_METHOD=0.

When the Server document field DAOS object encryption is set to **Private to this server**, this notes.ini setting causes the "DAOS encryption strength" to be "Domino classic". Without this change, Domino 12 or later will default to AES-128 instead.

For more information on this feature, see Improved DAOS encryption security.

NRPC port encryption enhancement

In Domino V12, support for forward secrecy (https://en.wikipedia.org/wiki/Forward_secrecy) using X25519 (https://en.w ikipedia.org/wiki/Curve25519) has been added to NRPC port encryption. In addition, the default algorithms are upgraded. For more information, see NRPC port encryption supports forward secrecy using X25519.

Notes IDs

The minimum key size for newly registered Notes IDs was increased to 1024 bits in V11.0.1 and the default key size for newly registered Notes IDs was increased to 2048 bits in V12.0. Existing IDs with smaller keys that were created by older versions of Notes and Domino can still be used with V12, but for improved security we recommend using the "User Key Rollover" and "Server Key Rollover" features to upgrade existing ID files with smaller keys to 2048 bits.

ID Vault – maintaining ID file synchronization

When passwords on Notes client IDs become different from the passwords on the IDs in the ID vault, synchronization of ID information between clients and the ID vault stops. Starting with V10.0.1, you can enable automatic restarting of synchronization when the passwords get out of sync.

SAML and federated login

Notes and Web Federated Login is a feature that has been around for a long time, however it has had great improvements in both versions 10 and 11. In earlier versions of Domino, only two specific IdPs were supported. Starting in Domino V10, Domino supports AuthnRequests for SAML requests, meaning any SAML 2.0 provider that supports AuthnRequests is expected to be compatible.

Starting in V11.0.1, when using Notes Federated Login or Web Federated Login is used to extract the ID file from the ID vault, the value for the ID Vault policy setting “Allow automatic ID downloads” is now ignored.

For the latest instructions, see the topic Using Security Assertion Markup Language (SAML) to configure federated-identity authentication in the Domino documentation.

Database encryption

Starting with V11.0.1, Domino supports encrypting databases with AES 128-bit encryption.
See KB0079874 for details.

Whitelist Active Content Filter (ACF) for iNotes and Verse

Starting with V10.0.1, an ACF can be used to remove potentially harmful active content from HTML messages such as JavaScript™, Java™, and ActiveX. A whitelist filter removes all entities except those in the whitelist. A blacklist filter (used in previous releases and still the default in this release) retains all entities except those in the blacklist. Blacklist filters need to be continuously maintained to guard against threats from new markup patterns. Whitelist filters are considered a best practice because they are explicit about the patterns that are allowed. ACF is available for iNotes and Verse, it does not apply to the Notes client. See the topic Enabling the whitelist Active Content Filter in the Domino documentation for details.

Chapter 3 Preparing your environment for the Domino 12 upgrade

Time spent doing a thorough evaluation of your environment prior to upgrading is time well spent. Capturing baselines of your existing server infrastructure allows you to compare how the upgraded environment is performing.

Prepare your production environment before you upgrade

Before upgrading to Domino 12 perform these steps:

1. Normalize your environment. Resolve any major issues or crash/hang conditions before you upgrade. Don't assume the upgrade will fix these issues, unless documented.
2. Investigate the compatibility of vender-supplied applications and companion products with Domino 12.

If you are performing an upgrade from a version of Domino that is pre-V9.0x then it is a best practice to perform pre-upgrade maintenance on your Domino applications to ensure the smoothest upgrade process possible.

If there is a need to view the console information before, during, or after the upgrade process you can access what was displayed in the Domino Server Console by accessing the “console.log” file located on the Domino server in the ***Data\IBM_TECHNICAL*_SUPPORT** directory.

If you are using a version of the Domino server prior to V9.0.1 the “console.log” file is not automatically created. Instead, you can configure your Domino server to create a debug file. To do this, add the following value to the Domino server’s “notes.ini” configuration file: ***DEBUG_OUTFILE=filename.txt***

When adding this value, change the ***filename.txt*** to be a recognizable file name that you can easily locate. You can also include a directory name within that value (e.g. ***c:\temp\filename.txt***) if you would like to store the file in a specific location. If the directory name is not included the file will be created in the Domino server’s ***Data\IBM_TECHNICAL_SUPPORT*** directory.

Once this has been done, run the following process on your Domino applications:

Fixup task

The Fixup task ensures that there is no corruption within your Domino applications. This will ensure that all of your Domino applications will be accessible once the upgrade to the Domino server is complete.

If the Domino server is currently running the Fixup command to run is as follows:

```
load fixup -f -j -v
```

If the Domino server is **NOT** running the Fixup command to run is as follows:

For Windows OS:

```
nfixup -f -j -v
```

For Linux/Unix:

```
fixup -f -j -v
```

Command Notes:
-f Exhaustive fixup, all documents are checked.
-j Include transaction-logged databases if you have transaction logging enabled. Without this option, fixup does not repair logged databases.
-v Exclude database views (faster). Views will be rebuilt later during the Domino V11.0 upgrade

For more information on running maintenance tasks on your Domino server see **Domino Server Maintenance Tasks** in this document.

Check the "console.log" file or the DEBUG_OUTFILE for any errors, possibly indicating data corruption. Query the HCL Support site and/or work with HCL Support to get them resolved.

Note: If you don't have time to run fixup on all databases, at a minimum, run fixup on your system databases. Verify all system databases have inheritance enabled:

- NAMES.NSF (StdR4PublicAddressBook)
- LOG.NSF (StdNotesLog)
- EVENTS4.NSF (StdR4Events)
- ADMIN4.NSF (StdR4AdminRequests)

Database design inheritance must be enabled to allow the design task to refresh the database designs while the Domino server is down. If you fail to do this now, the design will need to be replaced manually using the Domino Administrator client.

For more information on enabling design inheritance please visit the website Linking a database to a template.

Plan your deployment Sequence

The following table and the information that follows describe the deployment sequence. This sequence does not account for organizational, demographic, or other constraints in your environment. Use this information as a guiding principle while taking other factors of your business into account.

Sequence #	Description
1	Upgrade / Install Domino V12 Administrator client(s)
2	Upgrade Primary Domino administration server to V12
3	Upgrade Domino directory design based on new template within primary Domino Administration server
4	Upgrade Domino Hub and Directory servers to V12
5	Upgrade the Domino Mail and Application servers to V12
6	Upgrade users' Notes clients to V12
7	Upgrade the design of Notes Mail and Standard System applications using V12 templates to enable the new functionality included in Domino V12
8	Update all Domino applications to use latest On Disk Structure (ODS)

Steps 1 - 2

These steps need to occur regardless of the overall strategy and sequence of server/client upgrades.

Step 3

Once the Primary Domino Administration server has been upgraded to V12 you should also update the design of the Domino Directory on that server.

Another option is to upgrade the design of the Domino directory along with other system database designs when you upgrade the primary Domino Administration server.

For information about changes in this release, See Domino directory changes in V12 in this document.

Important Note: Some customers, especially enterprise customers with thousands of users in their Domino Directory, may want to control the flow of the new Domino Directory design out into the domain. For more information, see Control the flow of the Domino Directory design in this document.

Steps 4 - 5

These steps can be achieved in various ways. The table indicates that all non-user facing Domino servers be upgraded before those that users' access. In larger organizations, it may make more sense to upgrade all Domino servers in a location before moving to the next location in which case some infrastructure and some user-accessed Domino servers will be upgraded at the same time.

Most Domino upgrades are relatively straightforward and cause minimal disruption to your production environment. However, you are strongly encouraged to plan the order and pace of Domino Hub and Mail Server upgrades. Planning these steps wisely can minimize risk of service problems or disruptions, while still maintaining your upgrade schedule. When upgrading software, many enterprises follow the principle of stepwise upgrade. The basic idea is to at each step of the process, preserve the opportunity to back off to the previous step, until you are confident in the current step.

HCL recommends choosing a single, or small number of Domino servers for the first step of the process. The server(s) should be chosen based on a tradeoff between being representative of your production environment but also involving less business risk, if possible. This allows you to ensure configuration and tuning of the upgraded environment is optimal for the broader deployment. Criteria for success should be set for this and each subsequent step. It is recommended that one of the criteria be delta change in key parameters you monitor routinely, but especially these parameters should include CPU, virtual memory usage, and storage operations (reads and writes). Compare CPU, virtual memory and storage operations for a period of several days before and after upgrade and investigate significant differences unaccounted for by component changes in the upgrade. Enterprises with passive (fail over) Domino servers should consider deploying one of these as a first step to further reduce risk.

Subsequent steps should be small enough (for example involve the appropriate level of change, say the number of Domino servers) to enable the ability to back out to the previous step, if necessary, at least in the earlier stages of a deployment. Again, providing an opportunity for additional optimizations for your specific environment. As more Domino servers are upgraded, and confidence increases, enterprises usually increase the rate of change and size of particular steps.

HCL also recommends wise use of any failover architecture you may have implemented to reduce risk during upgrades. Some enterprises, for example, delay upgrading both pairs in two-way clusters until all of one side is upgraded. If a problem occurs with an upgraded server, failover to a clustermate is a possibility with high probability of success. Consider upgrade of the Active side of Active/Passive pairs first. This enables deployment on production loads, while preserving the failover opportunity. Larger enterprises also do well to consider a production failover test to validate previous hardware sizing assumptions for clustermates. Failover test criteria should also include monitoring.

Steps 6 - 8

These steps are important to take advantage of the new features in Notes and Domino V12. Depending on the size of your Notes client base, communication needed, training required, etc. these steps are often carried out weeks after the server upgrades. This allows time for production testing before rolling out to hundreds or thousands of users.

The Domino V12 On Disk Structure level (ODS 55) increases the number of entries allowed in database ACLs and the maximum size allowed for individual fields. Be sure to read the topic Enhancements introduced in ODS 55 in Domino 12 in the Domino documentation for important details.

Chapter 4 Upgrading to Domino V12

Time spent doing a thorough evaluation of your environment prior to upgrading is time well spent. Capturing baselines of your existing server infrastructure allows you to compare how the upgraded environment is performing.

Evaluate and monitor your current environment

Evaluate

As a starting point, do a thorough investigation of the state of your current environment. Use tools to capture data about the following aspects:

- Server infrastructure (including baseline stats, performance, etc)
- Clients / workstations
- Applications
- 3rd party Products

Document pre-existing conditions and problems:

- Try to resolve outstanding issues and problems prior to upgrading.
- No matter how tenuous the link, an upgrade can be held responsible for any problem whether old or new.

Document things you want or need to address while you have the opportunity, focus, and resources available:

- There is always clean-up that can be done ahead of time

Monitor

Monitoring your current environment is a critical part of any upgrade, even an upgrade to a point release. The goal is to understand the cost of running the current environment and to predict a problem before it happens in the new environment. Monitoring is particularly important when you are moving users and/or consolidating servers

1. Capture the available raw data from the servers:
    - Operating system capacity and performance metrics
    - CPU, memory (usage, paging), disk (usage, I/O rates, performance), network
    - Domino server specific statistics
    - Other components (for example, SAN switches and disk metrics)
2. Interpret/analyse the data and create baselines for your current environment:
    - What are the typical operating parameters for your servers?
    - What is the data telling you about your environment?

3. Monitor your user baselines.
4. Create daily/weekly/monthly reports based on your baselines.
5. Create a remediation process to address results that exceed baselines.

Evaluate operating system and hardware requirements for Domino V12

Evaluate system requirements. Then, ask these questions:

- Is a hardware refresh required? It is time for a hardware update?
- Is the current platform still supported?
- Does the current platform fit the strategic needs?
- Do you need more or different storage?
- Can you or should you consolidate?
- Do workstations need upgrades?
- What is the support position of each vendor of third-party products?

For links to system requirements, see System requirements in this document.

Are you moving from a 32-bit operating system to a 64-bit operating system?

If so, the following things will happen:

- All existing full text indexes will be discarded and rebuilt
- On Windows, all existing views currently built will be discarded and rebuilt

Because of the two items mentioned above, if the UPDALL process is used during upgrading it will take much longer to run so you should plan for it. This is a one-time occurrence.

See the following link for additional information:
Knowledge Article #KB0030213 Steps to upgrade a 32-bit Domino server to 64-bit server on Windows platform

Evaluate coexistence of features across versions

Understand what you need to consider if operating Domino and Notes V12 in an environment that includes earlier versions.

Certificate management with CertMgr

The new certificate management feature requires Domino V12, on both the CertMgr server that requests certificates and the servers for which the certificates are requested. A new TLS cache reads the encrypted credentials and the TLS cache is available only with Domino V12.

Clustered servers

Upgrading Domino servers in a cluster at different times is supported, so that you can have a mixed Domino server cluster with V12 and earlier versions during the coexistence period of your project.

Cluster replication does not restrict the replication of design elements. The Domino V12 Directory design (pubnames.ntf) is backward compatible with earlier Notes and Domino versions. However other databases may cause issues on earlier Domino servers and Notes clients. This is important to keep in mind if you have custom templates.

Additional resources

See Release interoperability information in this document.

Plan HCL Traveler Upgrades

If upgrading a Domino server that runs Traveler, keep the following points mind:

- If you plan to upgrade Domino and Traveler at the same time, upgrade Domino first.
- You can install and run Traveler on any version of Domino that Traveler supports. Best practice is to use the latest maintenance level of the Domino version you choose.
- If you upgrade the Domino server major version, you must re-run the HCL Traveler installation to ensure the proper binary files are installed. For example, if running Traveler V12 on Domino V10.0.1 and you upgrade to Domino V12, re-run the HCL Traveler V12 installer.

For additional information and steps, see the topic Upgrade considerations and overview in the Traveler documentation. For Traveler system requirements, see System requirements for Traveler 12.x.

Determine best upgrade process for your Domino Servers

As part of the Domino server upgrade, you have a good opportunity to make some other changes to your Domino infrastructure. There are some choices you need to make at this point, such as if you want to upgrade an existing server, install a new server with a new identity or install a new server and inherit identities. Here are some things to consider at this point in the process:

Will this be an upgrade or a new installation? After defining your server requirements, you should determine if servers should...

- be upgraded in place?
- be replaced with new servers?
- be some combination of these approaches?
    - Should new servers inherit existing identities or have new ones?
    - Consider what impacts there could be on the client configuration.

There are a range of options depending on the answers to those questions above. For all options, the upgrade process and configuration testing should always be done in a test environment first.

For all upgrade processes you will first need to obtain the latest installation files from within the HCL Flexnet system. Please be sure to have these files available prior to performing any upgrade processes.

The following outlines the three main scenarios for upgrading your Domino server:

Option 1 In-place upgrade (simple install)

This is the easiest and most common method for upgrading your Domino server. Use this method if the following apply to your Domino server environment:

- Your current version of Domino server is V10.0 or above.
- The operating system on the server is compatible with Domino V12.0.
- The hardware meets the minimum requirements for Domino V12.0.
- Baseline monitoring indicates that the Domino server is currently performing well.
- You are keeping the existing directory structure on the Domino server.
- The Domino server's identity will remain the same.

If your Domino server environment meets these criteria, then use the in-place upgrade scenario. Follow these steps:

1. Shut down the Domino server (via Domino Administrator or Domino Server Console application)
2. Launch installer application.
3. Follow on-screen prompts.
4. Restart entire Domino server.

If you have clustered Domino servers, you must upgrade all Domino servers in the cluster. This ensures that all Domino servers use the same version of Domino and the same set of Domino templates. You can upgrade one Domino server at a time in the cluster. Remember that ACLs and replication settings do not prevent designs from propagating in a cluster.

Option 2 In-place upgrade (Pre-V10 environments)

When upgrading your Domino server from a pre-10 version of the platform, it is highly recommended that you first uninstall the current version prior to installing the latest release. This ensures that there are no conflicts with the latest version of the files that are deployed and that there are no residual files left within your environment that are no longer used.

Prior to performing the uninstall process, first make a complete backup of the following files:

File name	Location
NOTES.INI	Domino program directory (...\Domino)

NAMES.NSF	Domino\Data directory
Any other directory databases (if your environment uses them): • Directory Assistance • Extended Directory Catalog • Condensed Directory Catalog • Schema database	Domino\Data directory
LOG.NSF	Domino\Data directory
CERTLOG.NSF	Domino\Data directory
*.NTF (ONLY templates you have modified)	Domino\Data\*.NTF
*.ID	Domino\Data\*.ID
Mail Files	Domino\Data\Mail\*.*
Diagnostic Files	\Domino\Data\IBM_TECHNICAL_SUPPORT\*.*

After confirming the backup files are acceptable, proceed with uninstalling Domino using the uninstaller. Reboot the server before performing an in place upgrade as outlined in option 1 previously.

Once the upgrade process has completed it is recommended to run the **fixup** task outlined in the **Fixup task** section of this document on the Domino server again. This ensures that any updates to the **fixup** task that have been released in the latest version of the Domino server are applied to your environment.

After the upgrade is complete and you have verified Domino is operating as expected, you can optionally remove the backup files. If there is a need to recover a file from the backup, you should first shut down the Domino server, recover the files from the backup and then restart your Domino server to determine if the issue is resolved.

Option 3 Parallel upgrade with hardware and/or operating system update

In some environments, there may be a need to update the operating system and/or the hardware to support the Domino V12 server platform.

Special Note: Upgrading hardware and the Domino server program at the same time is not recommended. You should upgrade the hardware before or after the Domino server upgrade, but not at the same time unless you have no other choice. Upgrading them separately makes it much easier to troubleshoot when problems arise, isolating the issue to the hardware upgrade versus the Domino server upgrade.

If the operating system on the hardware to be used can easily be upgraded to support the minimum Domino V12 requirements, then you should upgrade the operating system first, then test to make sure that your operating system and existing Domino server function as expected.

If there are no issues with the operating system updates you can then proceed to perform the Domino server upgrade based on the upgrade options 1 or 2 described previously.

If the hardware to be used can easily be updated to support the minimum Domino V12 requirements (e.g. additional RAM memory or hard drive space), update the hardware first, then test to make sure that your hardware and existing Domino server function as expected. If there are no issues with the hardware updates you can then proceed to perform the Domino server upgrade based on the upgrade options 1 or 2.

If the hardware cannot support either an updated operating system or cannot accommodate the required hardware resources needed to run Domino V12, then you will need to migrate your Domino server environment onto new hardware. In this scenario you must perform a parallel upgrade. In this scenario you first configure the new hardware and operating system. Once that has been done, you then perform the following steps:

Special Note: the following actions assume that the identity of the Domino server will not change. If this is not the case, then proceed to **Option 4** in the following section.

1. Shut down the existing Domino server on the older hardware.
2. Make note of the existing Domino server's deployment location for the Domino Program, Data and Transactional Logs (if enabled) directories.
3. Make note of the existing hardware's network configurations (IP addresses, host file, etc.)
4. On the new hardware, connect to the existing hardware's file system.
5. Move the Domino Program, Data and Transactional Logs (if enabled) directories onto the new hardware, placing them in the identical spot as they were on the existing hardware. **Special Note:** If you are changing file locations and directory structure during this move, refer to the Support article: Changing directory locations when moving a Domino server to new hardware for more information.

Special Note: Once you start the copy of the files to the new hardware, you should never bring up the Domino server on the existing machine.

6. Run installation of the latest version of the Domino server and point to all of the same file locations to mirror your previous configurations.
7. Switch the server host and network identities to that of the existing server.
8. Run this configuration for a few days to make sure everything runs correctly. If there are no issues, you can safely discard the existing Domino server

Once the upgrade process has completed it is recommended to run the **fixup** task outlined in the **Fixup task** section of this document on the Domino server again. This ensures that any updates to the **fixup** task that have been released in the latest version of the Domino server are applied to your environment.

Option 4 – Install new Domino server (new identity)

You can install a new Domino server with a new name rather than upgrading. This approach:

- Builds a new server independently.

- Creates a new server identity.
- Permits change of underlying hardware and operating system.
- Permits testing of the configured state before cut-over.
- For mail users, requires some migration of users and client configurations from existing to new server.
- Permits monitoring as you ramp up users to verify that you don't overload the "new" server.
- For applications, requires migration of applications to new server and redirection from old server.
- If clustered...
    - Creates new servers and new cluster
    - Migrates users and client configurations to distribute users across the members
    - Migrates applications to the new cluster

Special note for Domino Servers with transactional Logging

If you currently have transactional logging enabled on your Domino server, you cannot change the location of where your Domino server is already installed during the upgrade process. There are many files contained within the transactional logging system that list the existing Domino server location. If you change the Domino server location before or after the upgrade process, the Domino server will not restart.

Domino Attachment and Object Service (DAOS) considerations

If you plan on moving the location of where DAOS stores the files for any reason (e.g. if the current drive is running low in physical space) then complete these steps:

1. Specify the new location in the **DAOS base path** field in the DAOS tab of the Server document.
2. Stop the Domino server.
3. Move the DAOS repository to the new location.
4. Restart the server.

Domino detects the new location.

Post upgrade process to improve Domino server performance

After you complete the Domino server upgrade, there is an additional process that you can perform that will improve the overall performance of your newly upgraded Domino server. This process entails purging the existing configuration settings contained within the notes.ini file so that any redundant or legacy settings are removed, thus allowing the Domino server to operate more efficiently.

There are a number of values stored in the notes.ini file that are either specific to the previous version(s) of the Domino server and / or are no longer required. By purging the notes.ini file of all values and allowing the Domino server to start with a fresh file, the legacy values will not inhibit the Domino server from operating properly.

Although this post upgrade step is optional, to ensure that your Domino server is running at peak performance it is highly recommended to go through this process.

This process involves creating strategic file backups, making modifications to your notes.ini file, and re-running the post-installation Domino Server Configuration process.

Step 1: Back up strategic files

The following files in your Domino environment will need to have backup **COPIES** made in the event that there are any issues:

- notes.ini
- names.nsf
- server.id
- admin.id (if available)
- cert.id (if available)

Step 2: Modify the notes.ini

In order for the Domino server program to recognize your environment as a supposed new installation you will need to modify the notes.ini file.

To start this process, open the notes.ini file in a text editor. Once opened, remove all but the top five (5) lines form the file. You should be left with something similar to below:

```
[Notes]
NotesProgram=C:\HCL\Domino
Directory=C:\HCL\Domino\data
KitType=2
InstallType=4
```

The specific location where the Domino server is installed, the “KitType” and “InstallType” values may vary from what is listed above. Retain the lines that contain these values.

Once you have removed all other lines from the file, save and close the notes.ini.

Step 3: Start Domino to relaunch Server Setup

Now you can start your Domino server. Once started, the Domino server will believe that this is a newly installed Domino server. The “Domino Server Setup” process will launch. This is the same process that started when you first installed the Domino server.

Once the “Domino Server Setup” process begins, follow these recommended options:

Screen “First or Additional Server?”

- Select “Set up first server or stand-alone server”

Screen “Provide a server name and title”

- On this screen, select the bottom option “I want to use an existing server ID file”. If the server ID file is in the Domino Data folder it will be already listed. If you store your server ID file in another location, use the “Browse button to locate and select the server ID file

Screen “Choose your organization name”

- On this screen, select the bottom option “I want to use an existing certifier ID file”. If the certifier ID file is in the Domino Data folder it will be already listed. If you store your certifier ID file in another location, use the “Browse” button to locate and select the server ID file
- If you do not have the certifier ID on your Domino server, you will need to provide values for the other fields on this screen. This will create a new certifier ID file that can be disposed of after this process is completed

Screen “Choose the Domino domain name”

- On this screen you can enter any value into the field. The process requires a value, but this will not be used in the Domino environment.

Screen “Specify an Administration name and password”

- On this screen, select the bottom option “I want to use an existing Administrator ID file”. If the Administrator ID file is in the Domino Data folder it will be already listed. If you store your Administrator ID file in another location, use the “Browse” button to locate and select the server ID file
- If you do not have the Administrator ID on your Domino server, you will need to provide values for the other fields on this screen. This will create a new Administrator ID file that can be disposed of after this process is completed

Screen “What internet services should this Domino Server provide?”

- On this screen you can use the default values. Later in this section we will reset the configured Server Tasks within the notes.ini file

Screen “Domino network settings”

- On this screen you can use the default values. Later in this section we will be replacing the modified Domino Directory (names.nsf) with the instance that was backed up previously

Screen “Secure your Domino Server”

- On this screen you can use the default values. This will ensure that your existing Domino applications are not vulnerable to any security issues

Screen “Please review and confirm your chosen server setup options”

- On this screen you can review the previously selected values. Once you are comfortable with this information, press the “Setup” button

The setup process will run very rapidly due to the fact that many of the settings that this process would normally configure are already in place on your Domino server.

Step 4: Restore names.nsf from backup

Once the setup is completed, restore the Domino Directory (names.nsf) from the backup files created earlier in this process. Locate the backup of the Domino Directory (names.nsf) and overwrite the same file that is located in the Domino data directory on the Domino server.

Step 5: Remove new Certifier and Administrator IDs

If during the “Domino Server Setup” process you needed to create either the Certifier ID or the Administrator ID, you will need to remove those files. The files that were created will have different certificates than the official IDs that were created during the original Domino server installation. The temporary ID files will reside within the Domino Data directory and have the default file names “cert.id” and “admin.id”.

Step 6: Adjust the server tasks in the new notes.ini file

Before restarting the Domino server, adjustments must be made to the new notes.ini file that was set up during the "Domino Server Setup" process. Specifically, we will need to adjust which Server Tasks are configured on the Domino server.

The values in the notes.ini file that we need to compare are as follows:

- ServerTasks=
- ServerTasksAt***x***= (these may be multiple entries, where "x" is the hour)

The "ServerTasks" values are what tell the Domino server which tasks you want running. These values must be copied from the original notes.ini that was backed up at the beginning of this process and used to replace the values in the new notes.ini. Save and close the notes.ini file once you have updated these values.

Step 7: Restart the server

Restart your Domino server to ensure that the adjustments to the Server Tasks launch correctly based on the modifications made to the notes.ini file.

Step 8: Reinstall add-on programs

If you have add on programs installed within your Domino server environment you will need to reinstall them with a compatible version from the vendor and re-install the add on program(s).

Create a Domino Server Test Environment

If you do not have a test environment, it is highly recommended that you create one. You will want to incorporate all the decisions that you have made up to this point and create a test environment that is representative of your current and target platforms, including hardware and software resources. Creating this environment is very important if you want to do any kind of performance or capacity planning.

For your basic test environment:

- Install Domino V12.
- Create copies of applications.
- Use test IDs and access applications just as you would in production.
- Customization work is done during testing. Get access to all the templates and applications from your test server and customize them as needed.

Pilot the upgrade in the production environment

Pilot the upgrade in the production environment, considering the following as you do:

- Document EVERYTHING during your pilot upgrade. For example, record in detail the operations, commands, the hours required to perform the upgrade, and any error messages you encounter.
- Imaging: Because some testing should focus on sets of steps that are to be executed, imaging saves time by enabling you to reset your environment to a known position. For example, VMWare with its snapshot capability can be a useful tool for this purpose. If VMWare is not ideal for your specific platform, implementing a robust backup and restore program is another way to achieve this.
- Determine the feedback needed from pilot users and determine success criteria.
- Choose pilot groups carefully. Start with immediate IT staff, then add lowest risk user populations. Grow the pilot population over time, adopting new audiences. Target diverse roles: technical, power user, assistants, application users.
- Perform the upgrades necessary for the pilot. Start with Administration servers, Hubs and SMTP Gateways with no users. Begin your pilot with one Domino mail server. Once working properly, continue to add/upgrade more mail servers.
- Run a steady state environment for a defined pilot duration.
- Review and update procedures after pilot feedback.
- Leverage clustering. If there are any issues during upgrading, your users can fail back over to the "down-level" server

Chapter 5 Upgrading applications

Start planning and testing application upgrades at the outset of your Domino upgrade planning.

Create an inventory of applications

Creating an inventory of your applications allows you to get an understanding of your application landscape as input for requirements and architectural discussions. It also gives you an opportunity to clean up your application environment.

As you create the inventory, identify the following information:

- The current user population: executives, managers, entire organization, small groups of people.
- Nature of the applications: template-based, custom, back-end integration and connectivity, level of complexity.
- Any current issues. After an upgrade, it is important to know if the upgrade caused an issue in an application or if the issue existed prior.

Follow best practices for application upgrades

- If there are current application issues, decide if any need to be fixed before the upgrade, and if so, plan for the resources needed to do so. Concentrate your efforts on issues that are simple and easy to fix.

- Notify users in advance and provide training on any application changes.
- Upgrade applications that are based on standard templates
- Change the design of applications to incorporate new features in the new release, if appropriate.

Testing application upgrades

Before fully testing your applications, review the list of features that have been removed from the Domino server platform in recent releases. For a list of these features, see the following topics in the Domino product documentation:

- Components no longer included in Domino 12
- Components no longer included in Domino 11
- Components no longer included in Domino 10

For information about the OpenJDK included in the Domino 12 server, see the following topic in the product documentation: New Java Runtime Environment.

Test an upgrade of a sampling of applications

Include in your upgrade testing:

- Mission-critical applications that are based on different designs
- Applications used by executives
- Complex or custom applications that include:
  - back-end integration
  - reliance on third-party software
  - undocumented functions and features
  - extensions or add-in tasks using nsf_hooks, ext_mgr, and home-grown APIs
  - use recompile all (LotusScript) to check for LotusScript issues
- Sample of applications that use a common or standard template

Documents the results

Document the results of testing and convey them to the application developers.

Resolve issues

Resolve issues found based on your priorities and testing results:

- Decide which application problems to fix before deploying to production.
- Create a small team to address problems that arise after deploying to production.
- Put applications into the pilot test environment for acceptance testing.
- On successful testing, archive copies of new templates.

Chapter 6 Deploying Domino V12 servers

Depending on the size of your organization and the number of Domino servers involved, an organization upgrade schedule may range from a few hours to a few weeks or months. An organization with a small number of users and a handful of Domino servers can easily be upgraded in a single day and even in a matter of hours. However, an enterprise with hundreds of thousands of users in multiple domains on hundreds of Domino servers located throughout the world will implement an upgrade plan that spans several months. Fortunately, one of the great strengths of Notes & Domino is that it maintains a very strong interoperability story between releases that makes this all possible.

The number of ways to perform a Notes and Domino upgrade is almost limitless. This document will cover only a few of these ways and hopefully give administrators several ideas they may decide to incorporate in their own upgrade plans. This chapter discusses best practices for upgrading small and medium businesses as well as how large enterprises may go about it.

It is always highly recommended, as time permits within your organization, to keep as close to the most current release of Notes and Domino as possible. Keeping up with maintenance releases (MRs) and FixPacks (FPs) for each major release as they become available is also recommended.

Review your deployment planning

Note: When upgrading Domino servers from V10 or an earlier release, the data directories from the previous version are retained, for example C:\Program Files\IBM\Domino and C:\Program Files\IBM\Domino\Data. On fresh installations, the default directories are C:\Program Files\HCL\Domino and C:\Program Files\HCL\Domino\Data.

Before upgrading servers as described in this chapter, it is VERY important that you read and follow the steps in Chapter 2 – Preparing your Environment for the Domino V11 Upgrade in this document. There is a lot of prerequisite information covered there that positions you for success during this phase of the deployment.

If you have already followed the steps in Chapter 2, you should feel comfortable at this point because you have tested the upgrade in a test environment and you have completed an upgrade pilot. The following things cannot be stressed enough:

- Make backups of all files (ID files, notes.ini files, system databases, applications, etc.) and validate the integrity of the backups if you have not done this already.
- Although it can be time consuming, performing maintenance on your databases before or during the upgrade process is very important. Repairing any database corruption before you upgrade is the best way to avoid big headaches later. Ideally, you run at least **Fixup -j** and possibly **dbmt** on ALL of your databases when instructed to. If you don't have the time to do that, you should try to run the maintenance tasks on at least your system databases. You can use indirect files to save time in this process.
- To have the least end-user impact, upgrade your environment during off-hours or over a weekend.

Domino Server Maintenance Tasks

Here are tips for performing Domino database maintenance during the upgrade.

Running maintenance tasks when the Domino server is shut down

The upgrade sections in this chapter include steps for running maintenance tasks while the Domino server is shut down. Here is information on how to do that.

UNIX: "Running compact, fixup, and updall on AIX or Linux when a Domino server is down"

Windows: To run maintenance tasks while the Domino server is shut down (offline), add the letter "n" to the beginning of the Domino server command (required when Domino is shut down, Windows platforms only).

1. Open a command window (Start -> Run -> type "cmd" -> click Enter).
2. Navigate to the file system folder where the Domino server is installed (same directory where nserver.exe is located).
3. From that path, type the Domino server command in the command window, adding the letter "n" before the name of the Domino server task. For example:
   - x:\HCL\Domino\nfixup.exe names.nsf -f -j -v
   - x:\HCL\Domino\ncompact.exe names.nsf -c
   - x:\HCL\Domino\nupdall.exe admin4.nsf -R
   - x:\HCL\Domino\nupdall.exe admin4.nsf -X

Use indirect files to save time running maintenance tasks

To save time, you can use multiple indirect files to run the same maintenance task multiple times concurrently. **Fixup, Compact, Updall, Design, Convert,** and **Replicate** tasks all support using indirect files. Additionally, you can create batch/scripts that run several maintenance tasks serially against different indirect files to help complete them more quickly.

Article: Using indirect files to run maintenance tasks

Upgrading small and medium business environments

Small and medium businesses (SMBs) are generally defined as ones having 10,000 users or less and 50 Domino servers or less.

SMB deployment sequence

The recommended deployment sequence for this type of environment is:

1. Upgrade the Notes clients that administrators will use to edit and operate on the Domino directory.
2. Upgrade the administration server of the Domino directory.
3. Allow the new Domino directory design to replicate freely to the other servers.
4. Upgrade hub servers.
5. Upgrade Resource and Reservations (R&R) servers.
6. Upgrade Domino mail servers.
7. Upgrade SMTP servers.
8. Upgrade application and web servers.
9. Upgrade third-party and companion product servers.
10. Upgrade the general population to Notes V12.
11. Replace design of mail files with MAIL12.NTF
12. Upgrade the On-Disk Structure (ODS) to the latest format of ODS 55. See the topic Domino On-disk structure in the Domino documentation for more information on how to perform this task.

Upgrading Domino servers

1. Make sure the Domino server to be upgraded is shut down “cleanly” (no errors or hangs).

If the Domino server does not shut down cleanly:

   a) Run nsd -kill
   b) With the Domino server shut down, run a Domino maintenance task against a non-existent database name. This step flushes the transactional logs to disk and essentially simulates a clean Domino server shutdown.

Below is an example maintenance task and resulting output:

```
c:\domino> nfixup.exe fred.nsf
Restart Analysis (117 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Recovery Manager: Recovery being performed for DB d:\notefile\mail.box
Recovery Manager: Recovery being performed for DB d:\notefile\names.nsf
Recovery Manager: Recovery being performed for DB d:\notefile\log.nsf
Restart Replay (116 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
04/22/2018 04:33:03 PM Recovery Manager: Restart Recovery complete.
(3/2 databases needed full/partial recovery)
04/22/2018 04:33:07 PM Informational, rebuild view needed - collection
object was deleted (reading d:\notefile\names.nsf view note
Title:'($Servers)')
04/22/2018 04:33:08 PM Informational, rebuilding view - container
integrity lost (reading d:\notefile\names.nsf view note
Title:'($Servers)')
04/22/2018 04:33:08 PM Informational, rebuild view needed - collection
object was deleted (reading d:\notefile\names.nsf view note
Title:'($Servers)')
04/22/2018 04:33:10 PM Database Fixup: Started
```

```
04/22/2018 04:33:10 PM Database Fixup: The pathname 'd:\notefile\fred'
was not found: File does not exist
04/22/2018 04:33:10 PM Database Fixup: Shutdown
```

2. Install Domino V11 following the guidance in the section Determine best upgrade process for your Domino Servers in this document.
3. Copy customized templates into place.
4. Run the design task to refresh the design of system Domino applications.
   Note: Ensure that inheritance is enabled on the system Domino applications. See Preparing your production environment before you upgrade in Chapter 2 of this document for more information.
5. Run the **Updall** task to rebuild views with design or collation changes.
   Note: Use indirect files to save time.
6. Restart the Domino server.
7. Upgrade the On-Disk Structure (ODS) to the latest format of ODS 55. See the topic Domino On-disk structure in the Domino documentation for more information on how to perform this task.
8. Repeat the steps for the next server to be upgraded.

Upgrading enterprise environments

An enterprise business is generally defined as one having more than 10,000 users and more than 50 servers. It can easily take many weeks or even months to upgrade all servers while end-users are anxious to use the new V12 interface as soon as possible.

Important information about design changes to the Domino directory

Two critical views, ($USERS) and ($SERVERACCESS), are used when a Notes client or a Domino server attempts to authenticate with a Domino server. The design upgrade causes these views to be rebuilt from scratch when first opened. If a Domino server is running when the views are being rebuilt, all authentication attempts to that server are blocked. Users attempting to access a Domino server in this state can experience significant delays or hangs. Domino clustering is also unavailable during view rebuilding. However, if the views are rebuilt with the Domino server down, the Notes client can take advantage of Domino clustering and fail over.

Rebuilding of the ($USERS) and ($SERVERACCESS) views takes longer in enterprise environments due to the many more users in the Domino directory, especially if the Domino server is running and the view rebuilds are competing for cycles. Therefore, it is important to allow the new Domino directory design to replicate out during off-hours and/or on the weekend so that the views can be rebuilt with limited end-user impact. Or, you can control the flow of the new Domino Directory design within the domain and only upgrade to the new Domino directory design as you upgrade each individual Domino server and assure all critical views are rebuilt prior to restarting the newly upgraded Domino server.

Rebuilding ($Users) and ($Server Access) can be time consuming for a very large Domino directory. Therefore it is not uncommon in an enterprise to do all this work once on the directory of the first server upgraded. Then, copy the updated directory on each subsequent server being upgraded after installation of Domino V12.

Control the flow of the Domino directory design

As with almost everything in Notes and Domino, there are several ways to control the flow of the Domino directory design. Here are a couple of ways: Domino directory design. Here a couple of ways:

Enterprise deployment sequence #1

1. Remove all instances of the Domino directory template (PUBNAMES.NTF) from your domain(s).
2. Upgrade the Notes clients that administrators will use to edit and operate on the Domino directory
3. Prohibit Domino directory Design elements from replicating to Domino servers:
   - From the Domino directory choose File -> Replication -> Options for this Application.
   - Select the Advanced Tab.
   - In the "Receive these elements from other replicas" section, uncheck "Design elements."

   Note: After you upgrade a Domino server, be sure to allow (check) Design elements to be received for the replica of the Domino directory on this server.
4. Upgrade Domino Administration server of the Domino directory.
5. Upgrade Domino Hub servers.
6. Upgrade Domino Resource and Reservations (R&R) servers.
7. Upgrade Domino Mail servers.
8. Upgrade Domino SMTP servers.
9. Upgrade Domino Application and Web servers.
10. Upgrade third-party and companion product servers.
11. Upgrade the general population to Notes Client V12.x.
12. Replace design of mail files with MAIL12.NTF.
13. Upgrade the On-Disk Structure (ODS) to the latest format of ODS 55. See the topic Domino On-disk structure in the Domino documentation for more information on how to perform this task.

Enterprise Deployment Sequence #2

1. Remove all instances of the Domino directory template (PUBNAMES.NTF) from your domain(s).
2. Configure the Domino directory ACL so that a new design can only flow in the following direction:

Domino Administration Server of Domino Directory -> Domino Hub Servers -> Domino Spoke Servers.

This ensures there is no backflow of Domino Directory changes as you upgrade first Domino Spoke servers, then Domino Hub servers, and finally the Domino Administration server of the Domino Directory.

3. Upgrade the Notes Clients that administrators will use to edit and operate on the Domino Directory.
4. Upgrade Domino SMTP servers.
5. Upgrade Domino Mail servers.
6. Upgrade Domino Resource and Reservations (R&R) servers.
7. Upgrade the general population to Notes Client V12.
8. Replace design of mail files with MAIL11.NTF.
9. Upgrade Domino Application and Web servers.
10. Upgrade third-party and companion product servers.
11. Upgrade Domino Hub servers.
12. Upgrade the Domino Administration server of the Domino Directory.
13. Upgrade the On-Disk Structure (ODS) to the latest format of ODS 55. See the topic Domino On-disk structure in the Domino documentation for more information on how to perform this task.

Upgrading the first Domino server in an enterprise

1. Make sure the Domino server to be upgraded is shut down cleanly (no errors or hangs).

If the Domino server does not shut down cleanly:

a) Run nsd -kill to clean up.

b) While the Domino server is down, run a Domino maintenance task against a non-existent database name which will flush the transactional logs to disk and essentially simulate a clean Domino server shutdown.

Below is an example maintenance task and resulting output:

```
c:\domino> nfixup.exe fred.nsf
Restart Analysis (117 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Recovery Manager: Recovery being performed for DB d:\notefile\mail.box
Recovery Manager: Recovery being performed for DB d:\notefile\names.nsf
Recovery Manager: Recovery being performed for DB d:\notefile\log.nsf
Restart Replay (116 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
04/22/2018 04:33:03 PM Recovery Manager: Restart Recovery complete. (3/2 databases needed full/partial recovery)
04/22/2018 04:33:07 PM Informational, rebuild view needed - collection object was deleted (reading d:\notefile\names.nsf view note Title:'($Servers)')
```

```
04/22/2018 04:33:08 PM Informational, rebuilding view - container integrity lost (reading
d:\notefile\names.nsf view note Title:'($Servers)')
04/22/2018 04:33:08 PM Informational, rebuild view needed - collection object was deleted
(reading d:\notefile\names.nsf view note Title:'($Servers)')
04/22/2018 04:33:10 PM Database Fixup: Started
04/22/2018 04:33:10 PM Database Fixup: The pathname 'd:\notefile\fred' was not found: File
does not exist
04/22/2018 04:33:10 PM Database Fixup: Shutdown
```

2. Install Domino V12 following the guidance in the section Determine Best Upgrade Process for your Domino Servers in this document
3. Copy customized templates into place.
4. Run the design task to refresh the design of system databases

Note: Ensure that inheritance is enabled on the system databases. See Preparing your production environment before you upgrade in Chapter 2 for more information.

5. Run the **Updall** task to rebuild views with design or collation changes.

Note: Use indirect files to save time.

6. Copy the Domino directory and full-text Index where they can later be copied to the next Domino server being upgrade.
7. Restart the Domino server
8. Upgrade the On-Disk Structure (ODS) to the latest format of ODS 55. See the topic Domino On-disk structure in the Domino documentation for more information on how to perform this task.
9. Proceed to Upgrading the next Domino server.

Upgrading the next Domino servers in an enterprise

1. Make sure the Domino server to be upgraded is shut down cleanly (no errors or hangs).
2. Install Domino V12 following the guidance in the section Determine Best Upgrade Process for your Domino Servers in this document
3. Copy customized templates into place.
4. Copy the Domino directory and full-text index, if enabled, saved from the "Administration Server" upgrade.
5. Run the updall task to rebuild views with design or collation changes.

Note: Use indirect files to save time.

6. Restart the Domino server.
7. Upgrade the On-Disk Structure (ODS) to the latest format of ODS 55. See the topic Domino On-disk structure in the Domino documentation for more information on how to perform this task.
8. Repeat to upgrade the next Domino server.

Enabling new features

For information on new features, see Chapter 1. Before enabling new features, review the topic Evaluate coexistence of features across versions.

Chapter 7 Deploying Notes V12 clients

System requirements

Before performing any Notes client upgrade, review the System requirements later in this document.

MarvelClient Essentials

Domino includes MarvelClient Essentials by Panagenda. This product can assist you in deploying and managing your Notes clients. In V12, improvements have been made to enabling and configuring Domino to use it. For more information, see the Marvel Client documentation.

Before you begin the Notes client upgrade

Before you upgrade, take the opportunity to do some client cleanup and maintenance so that you can begin on the right foot with Notes V12.

Automate and standardize

- Relocate client code on the desktop. If data is in a non-standard location, consider moving it to the recommended location for multi-user installs. For users who frequently change machines, consider a roaming user deployment.
- Set or reset mail quotas.
- Update configuration settings.
- Enforce consistency using policies. For example, use consistent install choices, bookmarks, preferences, certification schemes, hierarchies, etc.
- Improve load balancing of users across your environment.

Clean, tighten, and fix

- Remove unneeded applications from desktops.
- Remove notes.ini settings that are no longer required.
- Remove hard-coded server IP addresses from address books.
- Fix any issues with your current deployment.
- Run maintenance on local system databases.
- Defragment user workstations.

Overall upgrade order

The following upgrade order is supported:

1. Domino servers
2. Notes clients
3. Application templates

Notes client install best practices

Follow these install best practices.

Multi-user installs

Multi-user installs are ideal for most Notes users. The exception is users who use Domino Designer or Domino Administrator, which are available for single-user installs only.

A multi-user install provides the following benefits:

- Leverages operating system multi-user profiles.
- Leverages user-independent settings.
- Allows administrators to lock-down control of installed programs by installing in read-only directories.
- Allows multiple Notes users to share a computer while keeping their work stored securely in separate personal data directories.

To switch from single-user to multi-user, see the following topic: Upgrading from Notes single user to Notes multi-user in the Domino documentation.

Standard client installation

Use the standard client rather than the basic client unless hardware is inadequate. If you need to use the basic client, install the standard client but launch the basic client. To launch the basic client, add the setting UseBasicNotes=1 to the client notes.ini file or configure the installer to use the "-sa" or "-basic" switch in the shortcut.

Roaming users

Enable Notes users to roam so that settings and key Notes files (names.nsf, notes.ini, bookmarks, desktop, journal) stay synchronized across multiple clients. For more information, see the following topics in the Domino documentation:

- Roadmap for registering and configuring Notes roaming users
- Considerations for changing roaming user status

ID vault

If you don't already, store Notes IDs in an ID vault. An ID vault makes recovery of damaged ID files easy and enables administrators to reset passwords when users forget them. In addition, some security features, for example time-based one-time password (TOTP) authentication introduced in V12, require an ID vault. For more information, see the Notes ID vault section of the Domino documentation.

Standardized notes.ini Settings

Standardizing notes.ini settings across clients is recommended when possible by deploying the settings through policies. An exception is settings that are needed as part of launching Notes: these you can specify through a custom installer.
For more information, see the following topics in the Domino documentation:

- Assigning Notes.INI settings through user policies
- Creating a customized add-on installer

Replicate notes.ini settings via roaming user functionality

Enable roaming user functionality to push notes.ini settings replicated after an upgrade. Then, you can delete user notes.ini settings locally and roaming functionality restores them upon next launch.

Uninstalling before upgrading

Uninstalling a prior version of Notes before upgrading is not required. However, you might want to do so for the following reasons:

- To remove files no longer needed.
- To standardize settings and configuration.

"Low touch" installation and setup

Customize Notes installation and setup so that users aren't required to input information into the install and setup panels (other than passwords). This practice streamlines and standardizes the upgrade across your environment. The following topics in the Domino documentation provides information on options for custom installs:

- Setting up Notes installation using scriptable setup
- Using Notes Smart Upgrade
- Notes Auto Update (Available for upgrading from Notes 10.0.1 or later version).
- Automating a customized or default Notes deployment using silent install

Steps to deploy Notes V12 clients

Note: When you upgrade a Notes V10x or earlier client V12, the Program and Data directories from the previous version are retained, for example C:\Program Files\IBM\Notes and C:\Program Files\IBM\Notes\Data. On fresh installations, the default directories are C:\Program Files\HCL\Notes and C:\Program Files\HCL\Notes\Data.

Phase 1: Plan the deployment

- Set realistic goals about how long deploying Notes V12 will take.
- Take an inventory of the applications that must be tested with the new version of Notes. Factor in time to test the applications and to respond to any issues.
- Develop a plan to carefully pilot the client. Collect feedback from the pilot to help create a realistic deployment roll-out plan.
- Develop a plan for training and communicating upgrade information to end-users. Goal is to ensure you have user acceptance and that they are prepared for new client.
- Develop a training and support plan for help desk staff.
- Review system requirements
- Review what maintenance releases are scheduled near your planned deployment time.
- Plan to follow the recommended upgrade order: servers first, clients second, templates third.

Phase 2: Download and customize the install kit

For information on the install customization features described here, see the topic Customizing Notes installation in the Domino documentation.

- To install translated versions of the Notes Standard client on Windows, download the cascaded Multilingual User Interface (MUI) pack installer kit. This installer is new in V12 and allows you to install any translated version of the Notes client from one kit. For more information, see the topic Using the cascaded Multilingual User Interface (MUI) pack installer (Windows).
- To install translated version of Notes on MacOS, see the topic Using the Native Language (NL) packs (Mac OS).
- Customize which features to install, add, or remove.
  - Edit the install manifest to control which features are available and what the user sees on the installation panel.
  - If notes.ini settings must be run before the user initially launches Notes, you can configure a transform file to accomplish this. Otherwise, rely on recommended best practices for standardized notes.ini settings described earlier.
  - Remove default components not used by your company. For example, if your company is not integrating Connections or Sametime with the Notes client, remove those components from the install kit.
  - Add custom plug-ins used by your company. If your company integrates custom plug-ins with the Notes client, add the plug-ins to install kit.
- Set run-time settings for notes.ini, Domino policies, and plugin_customization.ini.
  - Whenever possible, use Domino policies to manage notes.ini settings
- Configure Notes "Scriptable Setup"
  - Use a "Scriptable Setup" (or Setup Response file) to limit user intervention during both the install and the initial setup of Notes. During the install, the wizard displays only the panels that users need to set up the Notes client.
- Pre-populate cross certificates in deploy.nsf
  - You can prevent users from having to respond to cross-certificate prompts by pre-populating the deploy.nsf with admin-generated cross certificates.
  - Admin-generated certificates are copied to users’ address books at first launch.

Phase 3: Build and test the deployment package

- Use a "push" tool to automate the deployment.
- Consider uninstalling earlier clients for a reportedly smoother experience and the added benefit of being able to change the location of install directories.
- Code scripting to shut down client if not already shut down and also reboot the machine before starting the install.
- Use verbose install logging for the pilot.
- Run maintenance on local databases & defragment machine.

Phase 4: Pilot the upgraded client

- Determine pilot length & ideal participants.
    - At minimum, you should allow a month for customer feedback but preferably longer if possible.
    - At least 100 users distributed 80% in main site, 20% in remote site, preferably not all IT users.
    - Target diverse roles such as technical, power user, assistants, specific application users; consider a separate pilot for Notes Citrix users.
- Determine feedback required from pilot users and success criteria.
    - Look for user feedback on issues with the new release.
    - Make sure to check Release Notes for known issues, etc.
    - Use pilot experience to estimate support cost to final rollout.
- Collect ADC fault statistics before and after the pilot and compare the statistics. For more information, see Setting up automatic diagnostic data collection on clients.
- Certify that custom apps work with new release.

Phase 5: Roll out the deployment

- Plan the roll-out based on bandwidth.
    - Consider how many desktops must be upgraded and plan your roll- out based on network bandwidth as well as your IT support capabilities.
    - In case of low WAN bandwidth, consider alternatives such as LAN storage devices or Smart Upgrade Governor
- Provide the support plan to help desk staff.
    - Use the feedback and lessons learned during the pilot to determine how much deskside support may be needed.
- Monitor the deployment.
    - Throughout the deployment, monitor the progress by using the tracking features of the tool in use.
    - Considering using MarvelClient Essentials to help monitor the deployment. For more information, see the Marvel Client documentation.

- Push out initial policy settings.
    - Configure hierarchical policy settings document to control the desktop configuration. The settings are detected automatically at first client launch.
- Update mail templates
    - After the server and client have been upgraded, then upgrade mail templates.
- Update folder designs
    - The mail file folder design is not automatically updated with a template change. You must use a Desktop policy to update the folder design.
    - Prior to updating the folder design, have users empty their Trash folders.

Phase 6: Manage the desktop

- Apply the latest Fix Pack.
- Use Policies to manage desktops.
- If necessary, modify desktops by re-running the Installer in Modify mode.
- Use the Add-On Installer toolkit to build installers for 3rd-party apps.
- As needed, deploy new widgets via the Widget Catalog.

Maintaining Notes clients

Upgrading Notes to the latest maintenance release and Fix Pack is a better choice than applying hotfixes:

- Maintenance releases and fix packs are maintenance deliverables for Notes and Domino that are planned, scheduled, well-tested, and manageable.
- Hotfixes have the following disadvantages:
    - Limited customer eligibility.
    - Intended for only the most critical issues.
    - Extensive testing by customers in their environments is required as they are minimally tested by HCL.

For information about the fixes provided in each release and Fix Pack, see the Fix List.

Chapter 8 Upgrade resources

System requirements

For requirements, see the following links:

- Domino 12.0 system requirements
- Domino 12.0 for IBM i Software Requirements
- Traveler 12.0 system requirements
- Domino support for virtualization platforms
- Notes 12.0. system requirements
- iNotes 12.0 browser requirements

Release interoperability information

- Requirements for new features in HCL Notes 12

Download information

- HCL License and Delivery Portal

Known issues

- HCL Customer Support

Fix list

- By release

Product documentation

- Domino
- Notes
- Nomad
- iNotes
- Domino Designer
- AppDev Pack
- Verse
- Traveler
- HCL Traveler mail support for Microsoft Outlook (end-user)
- HCL Client Application Access (ICAA)