Upgrade Checklist for Expressway 15.5.20 and Later

Contents

Introduction

Components Used

Before Upgrade

- How to read the certificate
- What to do before the Maintenance Window

If the Upgrade Fails

- Readiness check stopped the upgrade
- Alarm after a node comes up
- Admin cannot sign in
- Certificate or peer-identity failure
- Cluster alarm during or just after upgrade
- Sign-in problems after the node is up
- Evidence to collect in case TAC case is needed

After the Upgrade

- On every node
- Cluster-only
- Service checks, by what the is in use

Introduction

This document describes how to prepare Expressway for an upgrade to X15.5.20 or X15.5.21. It lists each prerequisite and how to correct it.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: X15.5.21 is available to download. It contains the fix for the October 2026 PHP vulnerability, also called PHP2shell (CVE-2026-109618 and CVE-2026-109619, Cisco bug ID CSCwx37062.
X15.5.20 is the security-hardening release and does not include this PHP fix. Use the readiness checks in this document for an upgrade to X15.5.20 or to X15.5.21. The checks are the same for both releases. Download X15.5.21 from Cisco.com. Expressway Series, or Expressway Select for the uncapped image, then Expressway Core and Edge, release X15.5.21. The security advisory can

still list 15.5.21 as to be determined. The image is already posted on the software download page above.

Before Upgrade

⚠ **Caution**: Do not start a cluster upgrade until every peer passes the readiness checks. Set TLS verification to Enforcing and confirm the cluster is healthy. Use FQDN for each peer-identity. Each server certificate must contain that node's FQDN in the SAN, or in the CN only when the SAN is empty. An empty SAN can occur if OpenSSL was used to create the CSR. If a check fails, the upgrade stops without changing the existing cluster configuration.

Check	Standalone	Cluster	If it is not true
Upgrade path matches Appendix 3	Required	Required	Before X8.11.4, stop at X8.11.4 first. Convert X12 PAK licensing to Smart Licensing before X15.x.
Current backup, and a tested rollback plan	Required	Required on every node	Take the backup before the window. A later factory reset clears configuration.
Cluster healthy, no unexplained alarms, replication in sync	Not applicable	Required	Fix the cluster before upgrading. A rolling upgrade still uses the normal split-cluster behavior.
TLS verification is Enforcing and the cluster is healthy	Not applicable	Required before the upgrade	Change Permissive to Enforcing, fix the certificate, and confirm replication. Do not discover this during the window.
Every peer uses FQDN, and the peer list is not empty	Peer-identity check passes	Required. Mixed IP and FQDN is blocked before reboot	Standardize on all FQDNs, let the change replicate, and confirm the cluster is healthy. See Change Cluster to use FQDNs . Do not change the format during a rolling upgrade.
Server certificate contains the system FQDN in the SAN, or in the CN only when the SAN is empty	Required if the upgrade checks the certificate	Required. Upgrade stops and leaves the cluster configuration unchanged	Reissue the certificate. If a SAN exists, do not rely on the CN. Reject names that contain an embedded NUL.
Certificate is in date, trusted by peers, RSA 2048+ or P-256+, SHA-2 signature	Recommended	Required	SHA-1 signatures are already unsupported from X15.2. Reissue the certificate. A self-signed certificate is acceptable only when every peer is explicitly configured to trust it.
TCP 4371 allowed only from known peers	Recommended	Required	Restrict the firewall. This is defense in depth for ClusterDB; it is not a substitute for the upgrade.
Admin API clients reviewed	Required if APIs are used	Required if APIs are used	Expect tighter name and password validation, CSRF checks on FormPutXML writes, and no option-key API.
Maintenance window covers a rolling upgrade plus a possible short	Normal window	Required	Cookie re-encryption can raise a cluster communication alarm. It is expected to clear by itself.

Check	Standalone	Cluster	If it is not true
cluster alarm			

How to read the certificate

Export the server certificate and inspect it.

- **FQDN in the SAN.** The release notes require the system FQDN in a SAN. The CN is checked only when the SAN extension is empty.
- **No CN fallback.** If a SAN is present and does not match, verification fails even when the CN is correct. Put every required DNS name in the correct SAN type.
- **NUL characters.** A certificate name that contains an embedded NUL is rejected.
- **Dates.** `notBefore` must be in the past and `notAfter` must be in the future.
- **Key.** RSA at least 2048 bits, or an EC key on P-256 or stronger.
- **Signature.** SHA-2 family. From X15.2, `sha1WithRSAEncryption` and `ecdsa-with-SHA1` are not supported.
- **Issuer.** If Subject and Issuer are the same, it is self-signed. Peers must already trust it.

What to do before the Maintenance Window

- Before the window, set cluster TLS verification to Enforcing, restart the cluster (starting from publisher first) and confirm the cluster is healthy. Permissive mode is not supported. A legacy Permissive value could remain visible, but it does not bypass ClusterDB certificate trust or peer identity validation.
- Peer identities must all be FQDNs. Do not change that format while a rolling upgrade is in progress.
- An authenticated H.323 endpoint with more than one alias could need a credential alias map for every alias, or credential alias binding turned off on the subzone. Turning binding off weakens the security posture.
- Local admin password expiry stays off when `PasswordExpiryDays` is 0. When it is enabled, expiry is calculated at 00:00 UTC, not local midnight.
- Password history depth defaults to 12. The training range is 3 to 24. Empty administrator passwords are rejected, and a recently used password can be rejected.
- LDAP administrator-role mapping requires an exact group-name match. A group name that only contains the configured name no longer grants the role.
- A new install, factory reset, or unattended deployment cannot reuse a factory-default root password. An upgrade does not wipe the current administrator password.
- A read-only administrator can no longer change SAML IdP trust.
- Email that cannot complete STARTTLS is not sent in the clear.
- Smart Licensing is the only licensing mode. PAK option keys were removed in X14.2. The standard Expressway image allows 2500 encrypted signaling sessions; Expressway Select is the uncapped image.

If the Upgrade Fails

Leave the cluster as it is. A failed readiness check does not change the existing cluster configuration. Do not factory-reset a node to get past the failure.

Readiness check stopped the upgrade

The installer stops before reboot when the certificate, TLS verification, or peer-identity requirement fails. Standalone nodes pass the peer-identity check.

Alarm after a node comes up

A burst of cluster-database re-encryption can raise a cluster communication failure alarm. Give it time to finish. Escalate if it stays up.

Admin cannot sign in

Treat this separately from an install failure. Expired, reused, or first-login passwords block the session. They do not mean the image failed.

Certificate or peer-identity failure

1. Download a full system snapshot from the node that stopped. Open **installimage.log** in that snapshot's **tmp** directory.
2. If the message is about peer identity, check for a mix of IP addresses and FQDNs, or an empty peer list. Make every peer use one format, wait for replication, confirm the cluster is healthy, and retry. Do not change the identity format in the middle of a rolling upgrade.
3. If the message is about the certificate, compare it with the release-note rule: the system FQDN must be in the SAN, or in the CN only when the SAN is empty. A present SAN is not allowed to fall back to the CN.
4. Reissue the certificate with every required DNS name in the correct SAN type. Reject a name that contains an embedded NUL.
5. Confirm the new certificate is in date, trusted, RSA 2048+ or P-256+, and signed with SHA-2. Do not attach the private key to the case.
6. Set TLS verification to Enforcing, confirm the cluster is healthy, and retry the upgrade on the node that stopped.
7. Continue the rolling upgrade only after that node is healthy. Do not upgrade the remaining nodes while one node is halted on this check.

Cluster alarm during or just after upgrade

1. Confirm the upgrade itself finished and the node is on the intended build, X15.5.20 or X15.5.21.
2. Look in the event log for developer.upgrade messages about re-encrypting ClusterDB fields, then "Saving migrated data to CDB."
3. Wait for the alarm to clear. The training material says it clears when re-encryption finishes.
4. If it remains, collect cluster status, alarms, and a snapshot from each peer. Do not copy cluster cookies or key material into the case notes.

Sign-in problems after the node is up

- **Web UI redirects to a password change.** The current password must be entered, and the new password must be different. This is expected on first GUI login after an install or factory reset, and when a local password has expired.
- **SSH says keyboard-interactive / PAM failed and never opens a shell.** An expired local password has to be changed. The old session is not granted.
- **REST returns 401.** Expected for an expired local administrator. Event log can show `Password Mismatch` or `taa-chkpasswd` failure for the API realm. Change the password, then retry.

- **New password rejected.** It is in the history (default last 12), or it failed the current complexity rules.
- **LDAP administrator lost the expected role.** Compare the configured group with the exact group name returned by LDAP. A partial or substring match no longer grants the role. A read-only admin cannot edit SAML IdP trust.
- **There is no factory-default root password** on a new install or factory reset. Do not search for or distribute a default credential. An upgrade does not clear the current administrator password.

⚠ **Caution**: Factory reset is not the upgrade-recovery step. It deletes cluster identity and cluster cookies. A system-triggered reset after de-clustering or an inconsistent cluster database keeps the IP address and the admin and root passwords, clears other configuration and logs, and returns the node to its temporary certificate. Use it only when the release notes call for it, and only after a backup exists.

Evidence to collect in case TAC case is needed

1. Software version and role of every node, plus which node stopped.
2. Full system snapshot from the failed node, including **tmp/installimage.log**.
3. Server certificate text (openssl x509 -text -noout). No private key.
4. Cluster status, alarms, and whether xConfiguration Cluster TlsVerify shows Permissive or Enforce.
5. Event log lines for the upgrade and, if relevant, sshd or httpd authentication failures. Redact passwords and cookies.
6. Whether using local, LDAP, or SAML administrators, Smart Licensing, and any API automation.

After the Upgrade

On every node

1. Version is the intended build. Use X15.5.21 when the upgrade is for the October 2026 PHP vulnerability. X15.5.20 does not include that fix.
2. Node is reachable on its management address and the Web UI loads.
3. No new hardware, disk, or application alarm is left raised. (A cluster communication alarm clears after re-encryption.)
4. A fresh backup is taken after the cluster is stable.

Cluster-only

1. Every peer is up, in the cluster, and replication is healthy.
2. Peers communicate with mutual TLS on TCP 4371 and 4372. (A connection without a valid client certificate must fail.)
3. Cluster TlsVerify is Enforcing.

Permissive is not supported. A legacy Permissive value could still be visible, but it does not bypass validation. Set Enforcing and confirm the cluster stays healthy.

4. Firewall still allows TCP 4371 only from the peer addresses.

5. No cluster cookie or diagnostic secret appears in logs or the snapshot notes you upload.

Service checks, by what the is in use

If using	What good looks like	If it fails
Local administrators	GUI, SSH, and API accept the current password. Expired accounts are pushed to a password change or receive HTTP 401.	Confirm expiry is at 00:00 UTC and that the new password is outside the history window.
LDAP administrators	An administrator signs in only when the LDAP group name matches the configured group exactly.	Compare the directory group with the Expressway group. Do not broaden the match to force a login.
SIP or B2B calls	A test call connects in both directions.	Collect call history and a snapshot.
Authenticated H.323 registration	The endpoint registers with every alias it uses, including an H.323 ID and an E.164 number.	Add a credential alias map for each alias. The release notes use `xConfiguration Registration CredentialAliasMap` with pattern type Exact. Turning `CredentialAliasBinding` off on the subzone also restores registration, and it weakens the security posture. H.323 itself is not removed.
MRA or device registration	A known endpoint registers and places a call. UC client certificate SANs are specific DNS names, not overly broad or malformed values.	Compare certificates, traversal credentials, and DNS with the pre-upgrade backup. Reissue a certificate whose SAN is too broad.
Email alerts	A test message leaves the node using STARTTLS.	If STARTTLS cannot complete, delivery fails closed. Fix the mail server trust or TLS. Do not expect cleartext fallback.
Smart Licensing	Registration and authorization match the Web UI. The standard image stays within 2500 encrypted signaling sessions, or the node is Expressway Select.	Check transport and CSSM. The CSSM “allow export-controlled functionality” checkbox does not apply to Expressway. Revoking the token and deleting the product instance sets the node to Deregistered. Option keys are not a workaround.
REST or configuration scripts	Account names match the new length and character limits. Configuration writes include the CSRF protection the GUI uses.	Update the client against the shipping API schema. A removed `/provisioning/optionkey` call is expected to fail.