CHECKLIST

Secure ICA Readiness Checklist for Citrix Virtual Apps

A practical checklist to validate Secure ICA settings, compatibility, logging, and rollout readiness before enabling encryption changes in production.

Secure ICA Readiness Checklist

Use this checklist before enabling or tightening Secure ICA settings in a Citrix Virtual Apps environment.

1) Define the scope

- [ ] Identify every access path in scope:
- [ ] Internal LAN
- [ ] VPN
- [ ] Remote access gateway
- [ ] Partner or contractor network
- [ ] Branch office or shared network
- [ ] List the delivery groups affected by the change.
- [ ] Identify which published apps are sensitive enough to require encrypted ICA traffic.
- [ ] Confirm whether the policy will be global, per-delivery group, or per-access path.
- [ ] Document any exceptions and the business reason for each one.

2) Confirm the security objective

- [ ] Decide whether the goal is:
- [ ] Encrypt ICA traffic only
- [ ] Require encryption for all sessions
- [ ] Use different rules for internal and external access
- [ ] Confirm the control is being used to protect session transport, not endpoint security.
- [ ] Verify that the chosen setting aligns with the organization?s risk tolerance and compliance requirements.
- [ ] Confirm clipboard, authentication, and application-layer risks are addressed separately if needed.

3) Inventory client compatibility

- [ ] Identify the oldest supported client version in production.
- [ ] List all client types in use:
- [ ] Managed desktops and laptops
- [ ] Thin clients
- [ ] Shared workstations
- [ ] BYOD or unmanaged endpoints
- [ ] Mobile clients
- [ ] Verify each client type supports the intended Secure ICA behavior.
- [ ] Check whether any legacy clients will generate warnings, disconnects, or session failures.
- [ ] Confirm support status for reconnect, seamless app launch, and session handoff scenarios.
- [ ] Remove or isolate clients that cannot meet the target policy.

4) Validate delivery and gateway paths

- [ ] Confirm the Secure ICA setting is applied consistently across the intended path.

- [ ] Check whether access through gateways, brokers, or delivery groups changes the effective policy.
- [ ] Verify that external sessions and internal sessions behave as expected.
- [ ] Confirm there are no conflicting policies that could create mixed encryption behavior.
- [ ] Validate behavior over each relevant network path:
- [ ] Office network
- [ ] Home internet
- [ ] VPN
- [ ] Wi-Fi
- [ ] Third-party transit

5) Test a representative session

- [ ] Launch a published app session from each major client type.
- [ ] Confirm the session connects successfully under the intended policy.
- [ ] Verify the effective encryption state from the endpoint or session logs.
- [ ] Check for fallback to weaker settings or unexpected warnings.
- [ ] Test logon, reconnect, and disconnect/reconnect behavior.
- [ ] Validate performance under normal and peak conditions.

6) Review operational impact

- [ ] Measure whether encryption introduces noticeable latency or user experience degradation.
- [ ] Confirm that application responsiveness remains acceptable.
- [ ] Verify that support teams know what errors to expect if a client is incompatible.
- [ ] Prepare a response path for users who cannot connect after the change.
- [ ] Confirm help desk and operations teams have the rollout schedule and rollback steps.

7) Check logging and monitoring

- [ ] Confirm logs capture policy application and session behavior.
- [ ] Verify you can identify:
- [ ] Encryption enabled sessions
- [ ] Rejected or incompatible clients
- [ ] Warnings and fallback behavior
- [ ] Reconnect issues after policy changes
- [ ] Establish a baseline before rollout.
- [ ] Define what constitutes an alert versus an expected failure during testing.
- [ ] Make sure monitoring can distinguish policy issues from general connectivity issues.

8) Prepare the rollout plan

- [ ] Start with a pilot group.
- [ ] Prefer external or higher-risk access paths for early enforcement.
- [ ] Expand only after client compatibility is confirmed.
- [ ] Set a clear rollback condition.
- [ ] Communicate the change window to application owners and support staff.
- [ ] Keep a record of the exact policy values in use.

9) Document exceptions and acceptance

- [ ] Record any legacy or unsupported endpoints.
- [ ] Document why an exception is required.
- [ ] Define when the exception will be removed.
- [ ] Get business and security approval for any non-standard posture.

- [ ] Revisit exceptions on a scheduled basis.

10) Final go-live decision

Before production rollout, confirm all of the following:

- [ ] The intended Secure ICA policy is defined and approved.
- [ ] Compatible client versions have been verified.
- [ ] A representative session test succeeded.
- [ ] Logs confirm the expected encryption behavior.
- [ ] Support teams are ready for user issues.
- [ ] Rollback criteria are documented.
- [ ] Exceptions are tracked and approved.
- [ ] The rollout scope is limited enough to reduce blast radius.

Quick pass/fail summary

Ready to proceed if:

- [ ] You can state exactly which sessions will be encrypted.
- [ ] You have tested the oldest supported client.
- [ ] You have validated internal and external access paths.
- [ ] You know how to detect failures or fallback behavior.
- [ ] You have a rollback plan.

Not ready if:

- [ ] The effective policy is unclear.

- [ ] Legacy clients were not tested.
- [ ] Logs do not show session transport behavior clearly.
- [ ] Support is unaware of the change.
- [ ] No rollback path has been defined.

Rollout notes

- Owner: _____
- Environment: _____
- Delivery groups in scope: _____
- Client versions tested: _____
- Approved exceptions: _____
- Rollout date: _____
- Rollback trigger: _____

Outcome

If the checklist above is complete, you should have enough evidence to decide whether Secure ICA settings can be enabled safely, where enforcement should start, and what must be monitored after rollout.