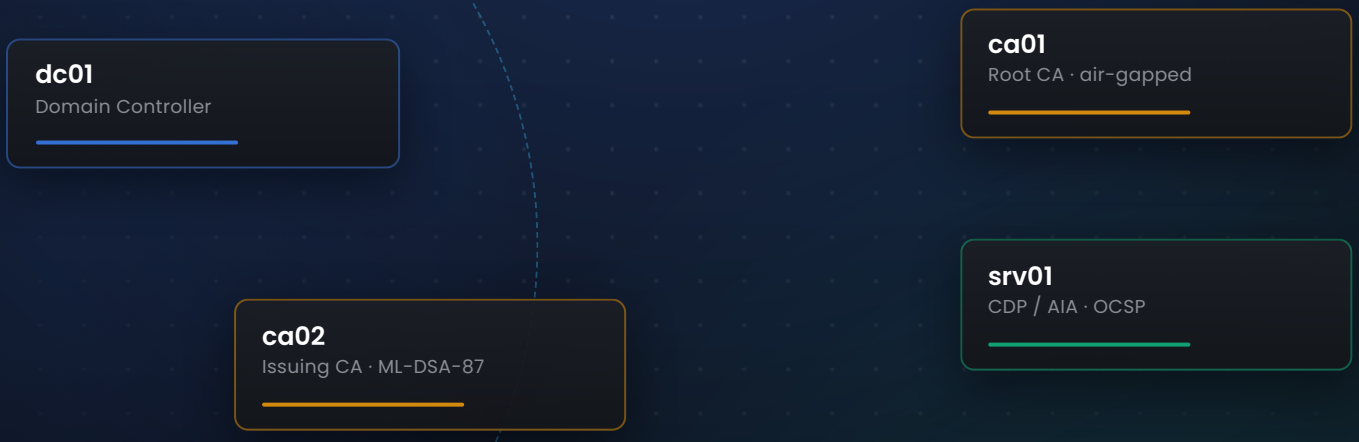
ENCRYPTION CONSULTING

GUEST GUIDE

PQC Playground

Design and deploy your own Post-Quantum Public Key Infrastructure

Describe your PKI Hierarchy on a canvas.
Deploy a full ADCS setup.



ENCRYPTION CONSULTING

Contents

ENCRYPTION CONSULTING

Before You Begin

The PQC Playground helps you construct a working public key infrastructure from a diagram. Place the machines you require on a canvas, complete their settings, draw the trust relationships between them, and click **Deploy**. After the deployment succeeds, real MS-PKI components will be running your design.

Common Applications

Evaluating post-quantum certificates	Set up an MS-PKI certificate authority that signs with a quantum-resistant algorithm, and observe its behavior before committing to a post-quantum migration plan.
Validating a design	Evaluate a decision about tiering, naming, or the placement of CDP and AIA endpoints on a live public key infrastructure.
Reproducing a problem	Rebuild a layout that is behaving incorrectly elsewhere, and investigate it in an isolated environment.
Evaluating Encryption Consulting's Products	Direct **CertSecure Manager**, **CBOM Secure**, or **CodeSign Secure** at an infrastructure built here, and evaluate them against your own tiering, algorithms, and certificate templates rather than against a fixed demonstration environment.

> **PRODUCT AVAILABILITY VARIES**
>
> The availability of CertSecure Manager, CBOM Secure, and CodeSign Secure varies, and the three are not necessarily available at the same time. Please contact Encryption Consulting regarding access to a product that you cannot see or deploy.

Requirements

A browser	A current version of Google Chrome, Microsoft Edge, or Mozilla Firefox.
The console address	Provided by Encryption Consulting.
An account	A username and a password, created on your behalf. Your projects and machines are private to your account unless you choose to share them.
Screen size	A resolution of 1440 × 900 or greater, so that the toolbox, the canvas, and the inspector are visible side by side.

What We Will Build

In this guide, we will set up a two-tier public key infrastructure consisting of a domain controller, an offline root certificate authority, an issuing certificate authority hierarchically beneath it, and a web server that publishes revocation information. The steps involve creating an empty project, drafting and staging the PKI architecture and deploying it.

MACHINE	ROLE	FUNCTION
dc01	Domain Controller	Creates the Active Directory domain and provides DNS. The remaining online machines join it.
ca01	Root CA	The top of the trust chain. It is kept offline and signs the issuing certificate authority and nothing else.
ca02	Issuing CA	Signs the routine certificates used by users, servers, and devices.
srv01	PKI Web Services	Publishes certificate revocation lists and certificate authority certificates over HTTP, and answers OCSP requests.

01

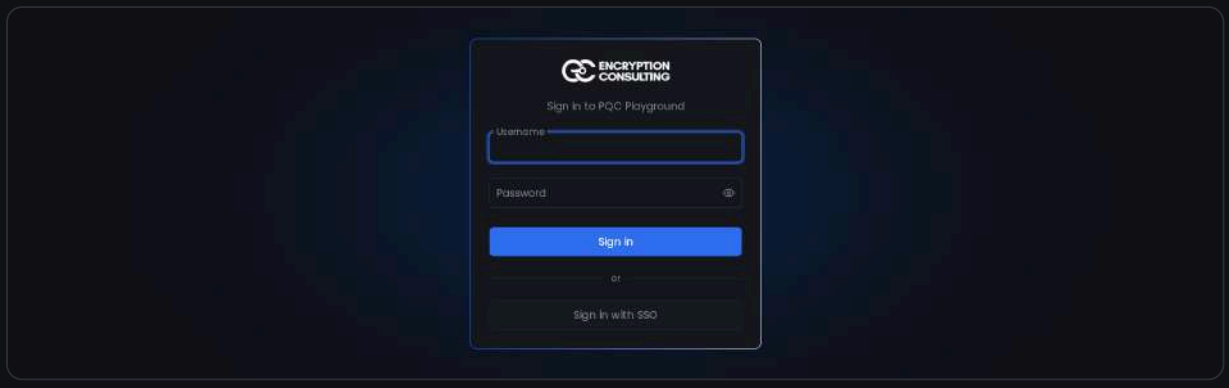
Start a Project

Choose Your Starting Point

Start a Project

1 Open the Console and Log In

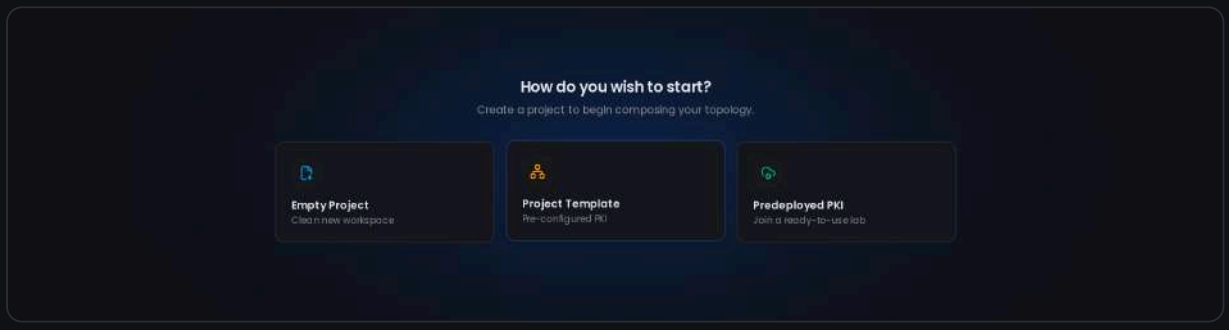
Navigate to the console address provided by Encryption Consulting.



The sign-in screen. A username and a password are required.

2 Choose How to Begin

Choose between empty project, starting from a template, or opening a predeployed PKI.



The start screen. Empty Project, Project Template, and Predeployed PKI. The green **Online** badge in the header indicates that the backend and its libraries are reachable. The **Guest** badge indicates the type of your account.

Empty Project

An empty canvas. The remainder of this guide uses this option, because constructing the environment by hand is how the purpose of each control becomes clear.

Project Template

A pre-configured topology that is already placed and already configured. Use this option when you want the completed diagram immediately and intend to adjust it rather than to draw it.

Predeployed PKI

Opens an environment that has already been deployed on your behalf, so that you may examine live machines without waiting for a deployment to complete.

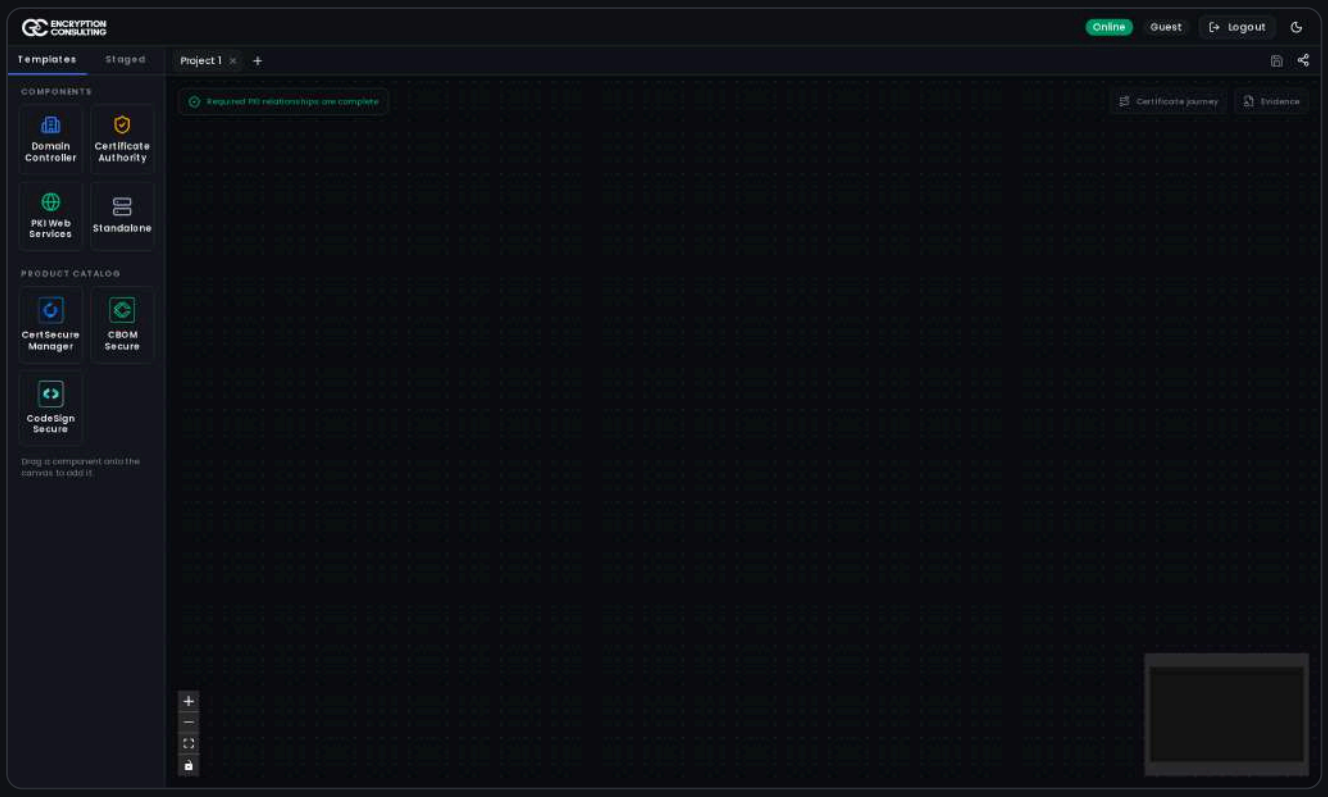
Select **Empty Project**.

02

The Workspace

Getting to Know the Playground

The Workspace



An empty project. The toolbox occupies the left edge, the project tabs run across the top, the canvas occupies the centre, and an inspector appears on the right once an item is selected.

Workspace Components

1. The Toolbox `left edge`

The **Templates** tab lists every server instance that may be placed on the canvas: Components (Domain Controller, Certificate Authority, PKI Web Services, and Standalone Server) and a Product Catalog (CertSecure Manager, CBOM Secure, and CodeSign Secure). The **Staged** tab lists the operations awaiting deployment.

2. The Project Tab Bar `top`

The bar contains one tab for each project. Click on the **+** button to create a new project. On the rightmost end, there is a save project icon and a share project icon. An asterisk after a project name indicates that the project has unsaved changes.

3. The Canvas `center`

The canvas is the area in which the topology is drawn. It is the interactive space where nodes are placed, relationships are drawn, and the topology is composed. The canvas may be zoomed and panned to accommodate large topologies.

4. Guidance and Lenses `canvas overlay`

The top left corner reports on the topology as a whole, stating either Required PKI relationships are complete or any errors encountered within the architecture. At the top right, there are two lenses, **Certificate journey** and **Evidence**. Certificate journey tracks the path of a certificate from its issuing authority to the PKI Web Services, and Evidence reports an audit snapshot of the topology, verifying every PKI path (each artifact - certificates, certificate request and CRL are downloadable).

Canvas Controls

CONTROL	LOCATION	EFFECT
Zoom In / Out	Bottom left	Adjusts the zoom level in steps. Scrolling on the canvas performs the same adjustment continuously.
Fit View	Bottom left	Frames every node within the viewport. This is the most direct way to restore an overview of the topology.
Toggle Interactivity	Bottom left	Locks the canvas so that nodes cannot be dragged unintentionally.
Minimap	Bottom right	Presents an overview of the entire topology, colour-coded by component type.

03

Compose the Topology

Design the PKI Architecture

Compose the Topology

1 Drag a Domain Controller onto the Canvas

Press and hold the **Domain Controller** tile in the toolbox, drag it onto the canvas, and release it. A node appears at the position where it was released, named `dc01` and marked as **draft**.

> **The first node.** A draft node is a placeholder: it has a name and a role, and nothing further. Names are assigned automatically according to role — `dc`, `ca`, `srv`, and `misc` — and are numbered in the order in which the nodes are placed.

2 Place the Remaining Three Components

Drag out a **Certificate Authority** for the root CA, a second **Certificate Authority** for the issuing CA, and a **PKI Web Services** node for the AIA/CDP endpoints.

The shape of the environment. Four draft nodes: `dc01`, `ca01`, `ca02`, and `srv01`. Both certificate authorities begin identically. What distinguishes a root authority from an issuing authority is its configuration, and not the tile from which it was created.

LAYOUT SUGGESTION

Consider placing the domain controller at the center, the root certificate authority at the top left, the issuing certificate authority below the root authority towards the right, and the web server to the right of the domain controller. This makes the completed diagram legible at a glance.

04

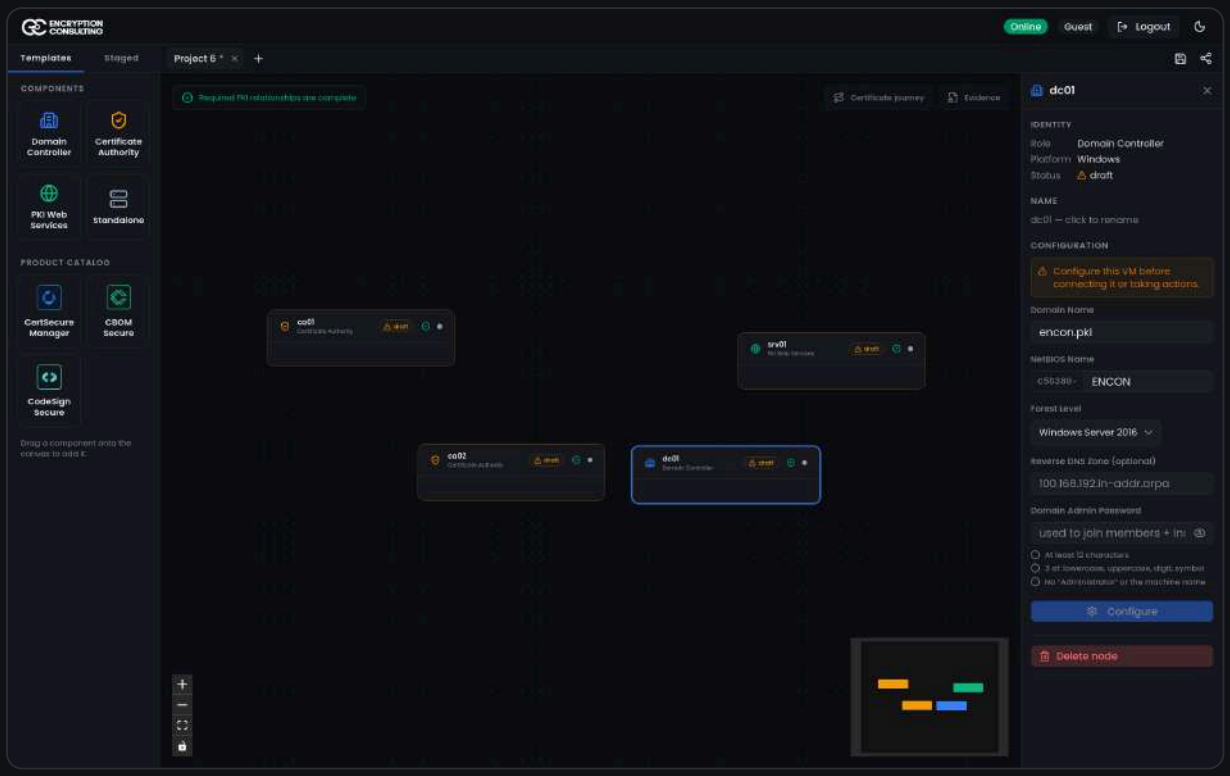
Configure Every Machine

Stage the Machines for Deployment.

Configure the Domain Controller

1 Select the Node

Select `dc01`. The Inspector opens on the right with three sections: **Identity** (role, platform, and status), **Name**, and **Configuration**.



An unconfigured machine. The amber banner — *Configure this VM before connecting it or taking actions* — conveys the same information as the draft badge. Below it are the fields specific to a domain controller.

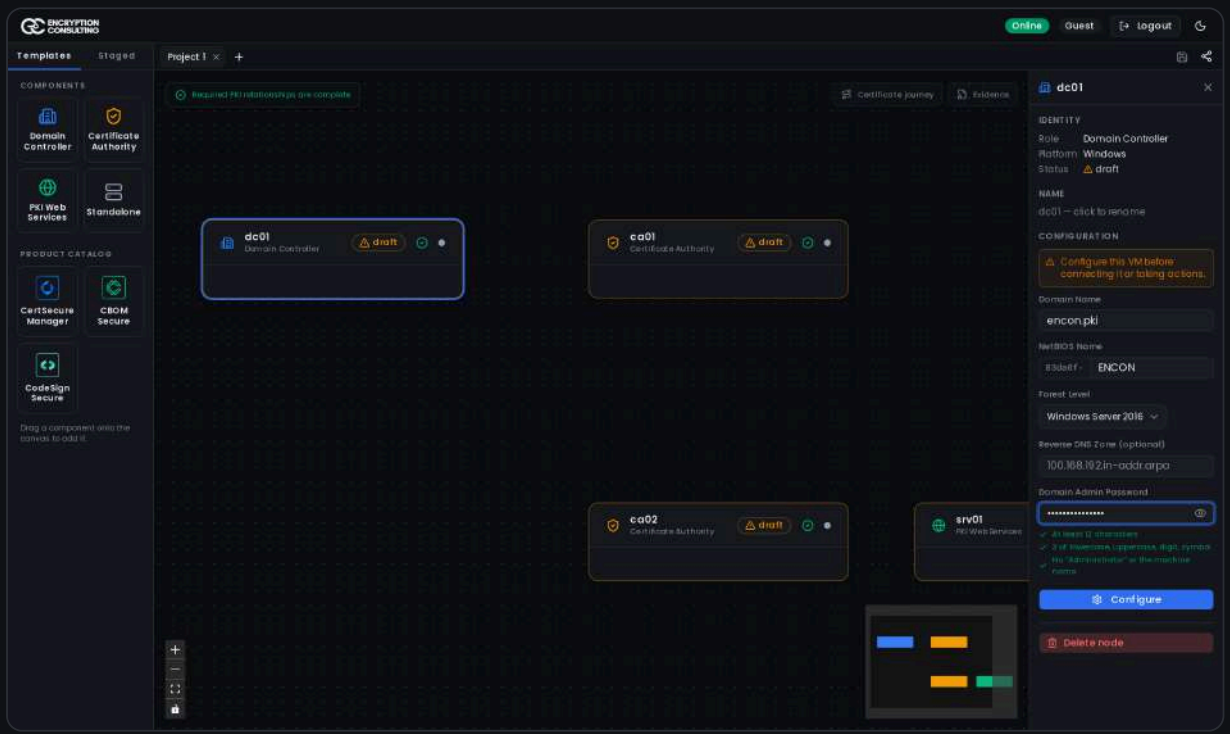
2 Rename the Machine

Select the name line, *dc01 — click to rename*, and enter a new name. Once a machine is configured, its name is fixed, because the name becomes the hostname of a real virtual machine.

3 Complete the Forest Settings

The domain controller creates the Active Directory forest in which the remainder of the environment resides.

FIELD	MEANING	SUGGESTED VALUE
Domain Name	The DNS name of the forest root domain.	`encon.pki`
NetBIOS Name	The short, case-insensitive domain identifier. It is displayed with your session prefix before it, which prevents concurrent environments from colliding.	`ENCON`
Forest Level	The forest functional level: Windows Server 2016, 2019, 2022, or 2025.	Windows Server 2016
Reverse DNS Zone	Optional. A reverse lookup zone, for example `100.168.192.in-addr.arpa`.	Leave empty
Domain Admin Password	The password for the built-in Administrator account of the domain. This field is required.	A password of your own choosing



The configuration completed. The password field carries a live checklist: a minimum of twelve characters, at least three of the four character classes (lower case, upper case, digit, and symbol), and no occurrence of "Administrator" or of the machine name. The **Configure** button remains disabled until all three conditions are satisfied.

RECORD THIS PASSWORD

The domain administrator password is the credential with which every subsequent step authenticates, including joining members to the domain, installing the issuing certificate authority, and removing the forest at the end. The Playground will not display it again.

4 Select Configure

The badge on the node changes from `draft` to `staged`, and a first operation is added to the Staged tab. Nothing has been created. *Staged* means that the machine will be created when the topology is deployed, which the Inspector now states explicitly.

A domain appears. Configuring a domain controller draws its **domain region**, the large dashed circle. The circle is dashed because the domain controller is still staged. Its labels report the forest functional level and a member count, which is currently zero.

Configure the Root CA

1 Select `ca01` and Review the Default Values

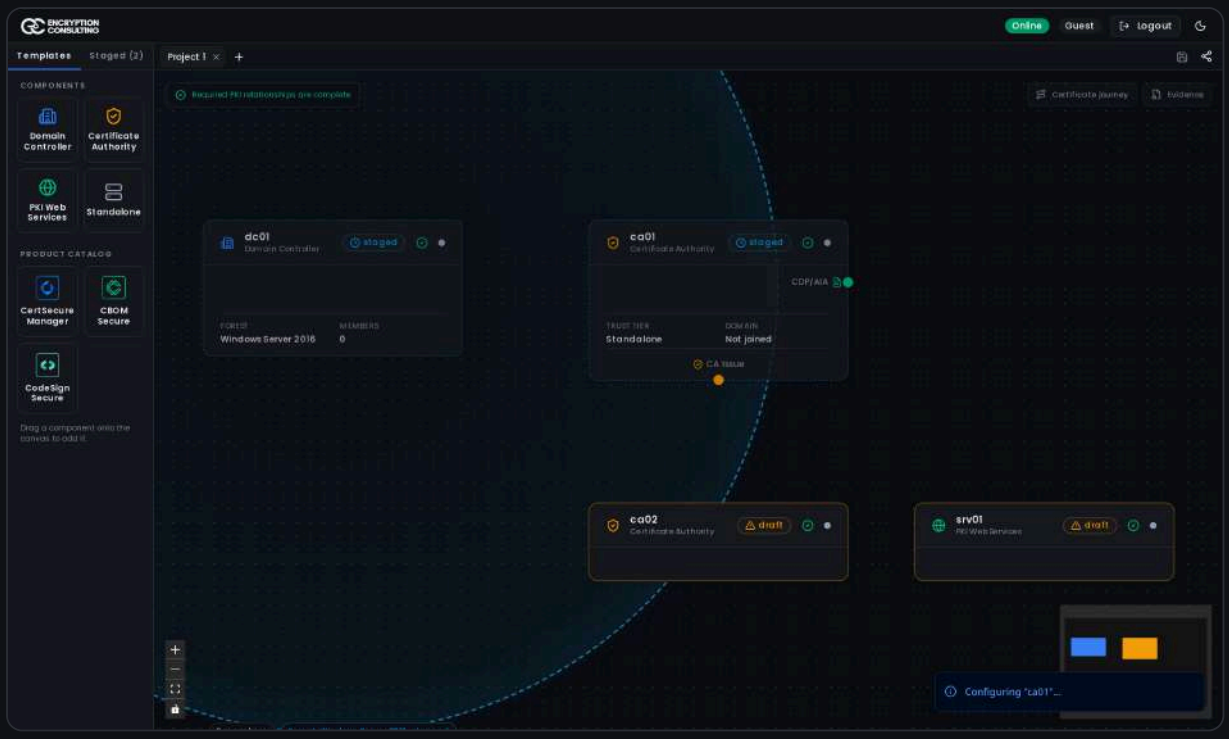
A certificate authority defaults to **Root**, which is the correct tier for this machine. Note the key algorithm. The Playground defaults to **ML-DSA-87**, the post-quantum signature scheme, and hides the key length and hash algorithm fields because ML-DSA-87 uses neither: its public key is a fixed 2,592 bytes, and it is a self-contained signature scheme with no separate hash selection. Selecting RSA or ECDSA instead restores both fields.

Root certificate authority configuration. Type, common name, publication directory, key algorithm, and validity period. A root authority has no CPS URL field, because that field belongs to an issuing authority.

FIELD	MEANING	DEFAULT
Type	Root or Issuing. Changing the type resets the common name and the validity period to values appropriate to that tier.	Root
Common Name	The subject name of the certificate authority. It must be unique within the topology.	`EC-Root-CA`
CA Publication Directory	The location on disk to which the certificate authority writes its certificate and its revocation list.	`C:\Windows\System32\CertSrv\CertEnroll`
Key Algorithm	RSA, ECDSA, or ML-DSA-87.	ML-DSA-87
Key Length	2048 or 4096. Hidden for ML-DSA-87, whose key size is fixed.	2,592 bytes
Hash Algorithm	SHA256, SHA384, or SHA512. Hidden for ML-DSA-87.	SHA256
Validity (years)	The lifetime of the certificate authority's own certificate.	20

2 Select Configure

`ca01` is staged, and the node now reports **Trust tier: Root** and **Isolation: Air-gapped**. Air-gapping is the defining characteristic of an offline root authority: it is not joined to a domain, and it communicates with exactly one other machine, the subordinate certificate authority.



The root certificate authority, staged. A configured authority presents sockets: **CDP/AIA** on its right edge and **CA Issue** at its lower edge. These are the connection points used in Part 5.

Configure the Issuing CA

1 Select `ca02` and Change Its Type to Issuing

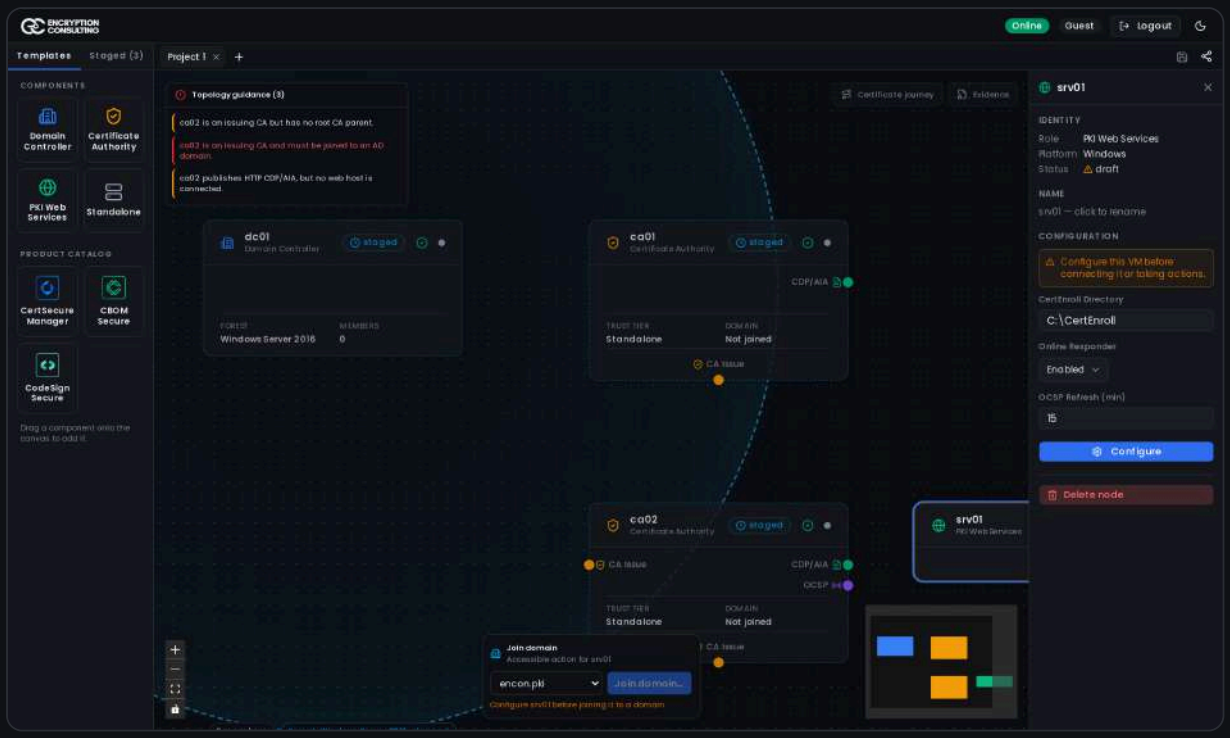
Open the **Type** list and select **Issuing**.

Selecting the tier. Selecting Issuing rewrites the common name to `EC-Issuing-CA`, sets the validity period to ten years, and reveals the CPS URL field.

Configure the PKI Web Services

1 Select `srv01`

PKI Web Services is the host that publishes certificate revocation lists and certificate authority certificates over HTTP and that, optionally, answers OCSP requests.



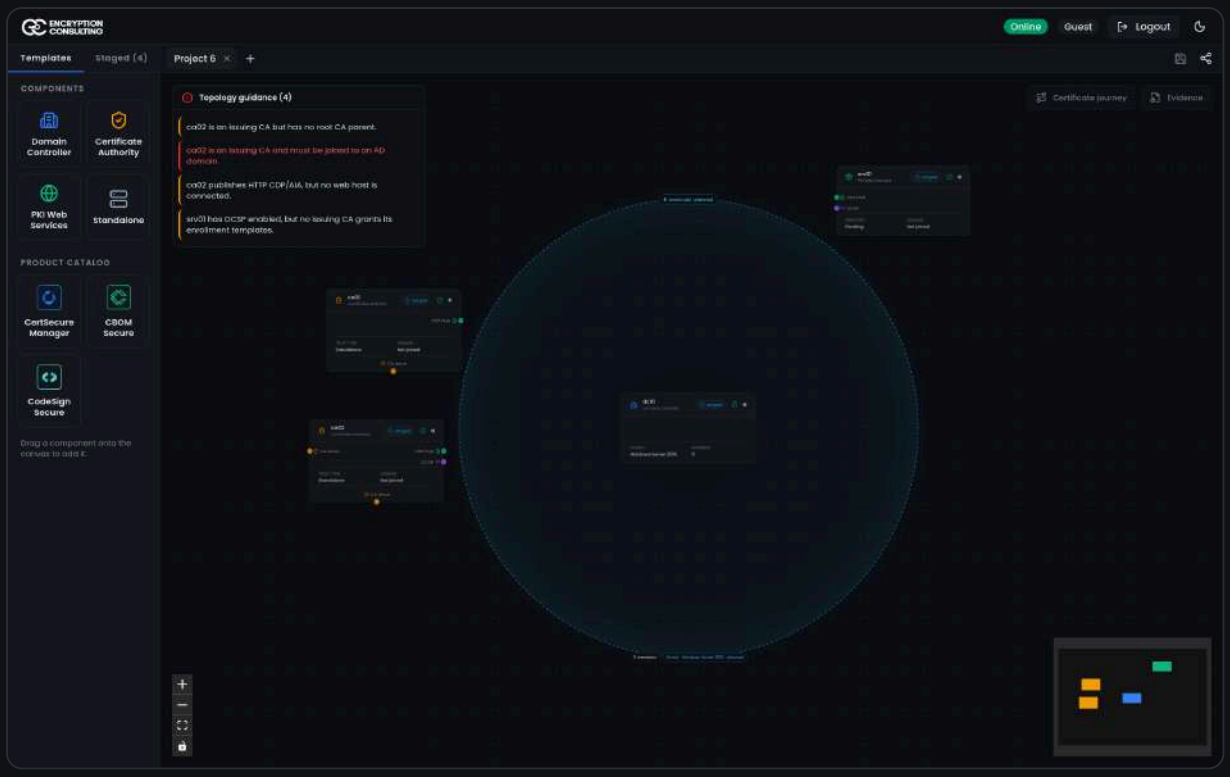
Web services configuration. Three fields, each with a usable default value.

FIELD	MEANING	DEFAULT
CertEnroll Directory	The IIS directory into which CDP and AIA artifacts are published.	`C:\CertEnroll`
Online Responder	Enables or disables the Online Responder role.	Enabled
OCSP Refresh (min)	The interval, in minutes, at which the responder refreshes revocation data. Hidden when the Online Responder is disabled.	15

Select **Configure**.

2 Review the Topology

All four machines are now staged. The Staged tab lists four operations, one for each machine. Nothing has been connected: every node reports **Domain: Not joined**, and the issuing certificate authority has no parent.



Four staged machines. Each configured node presents the sockets that its role supports, and each node summarises the configuration that is significant for it: forest level and member count, trust tier and isolation, and endpoint status.

05

Connect the Services

Connections Are Made between Sockets. Each One Is a Named Relationship with Defined Operations behind It.

Connect the Services

A configured node presents **sockets**, which are small labelled points on its edges. Each socket represents one kind of relationship within a public key infrastructure, and dragging between two compatible sockets stages the operations that establish that relationship.

The Three Sockets

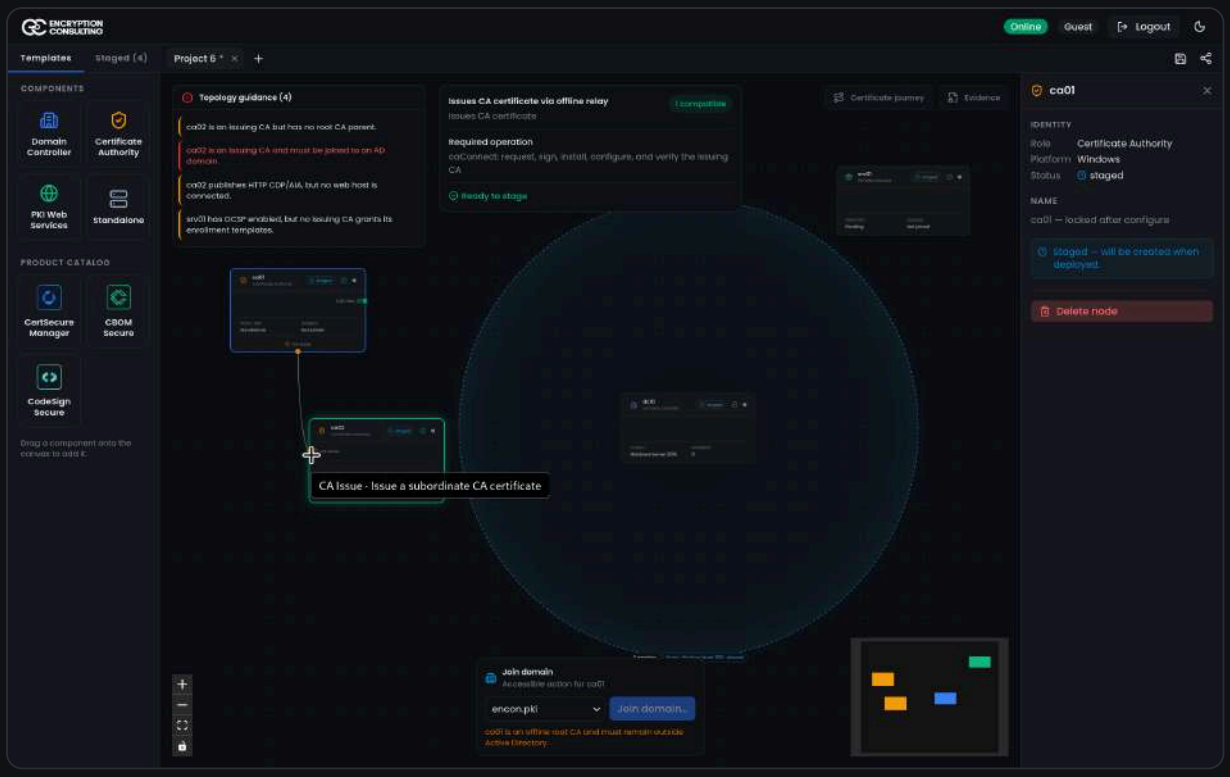
SOCKET	LOCATION	MEANING
CA Issue	The lower edge of every certificate authority, and the left edge of an issuing authority	Issues a subordinate certificate authority certificate. This runs the `caConnect` operation: request, relay, sign, install, and verify.
CDP/AIA	The right edge of a certificate authority, and the left edge of a web host	Publishes certificates and revocation artifacts. This runs the `webServerCert` operation: publish the CertEnroll directory and verify the artifacts over HTTP.
OCSP	The right edge of an issuing authority, and the left edge of a web host	Attaches an Online Responder path.

WHY A ROOT CERTIFICATE AUTHORITY HAS NO CA ISSUE INPUT

A root authority signs its own certificate, so it exposes CA Issue only as an output. An issuing authority exposes both: an input on its left edge, through which its parent signs it, and an output at its lower edge, through which it could sign a tier below it. The Playground does not render a socket for a relationship that would be invalid.

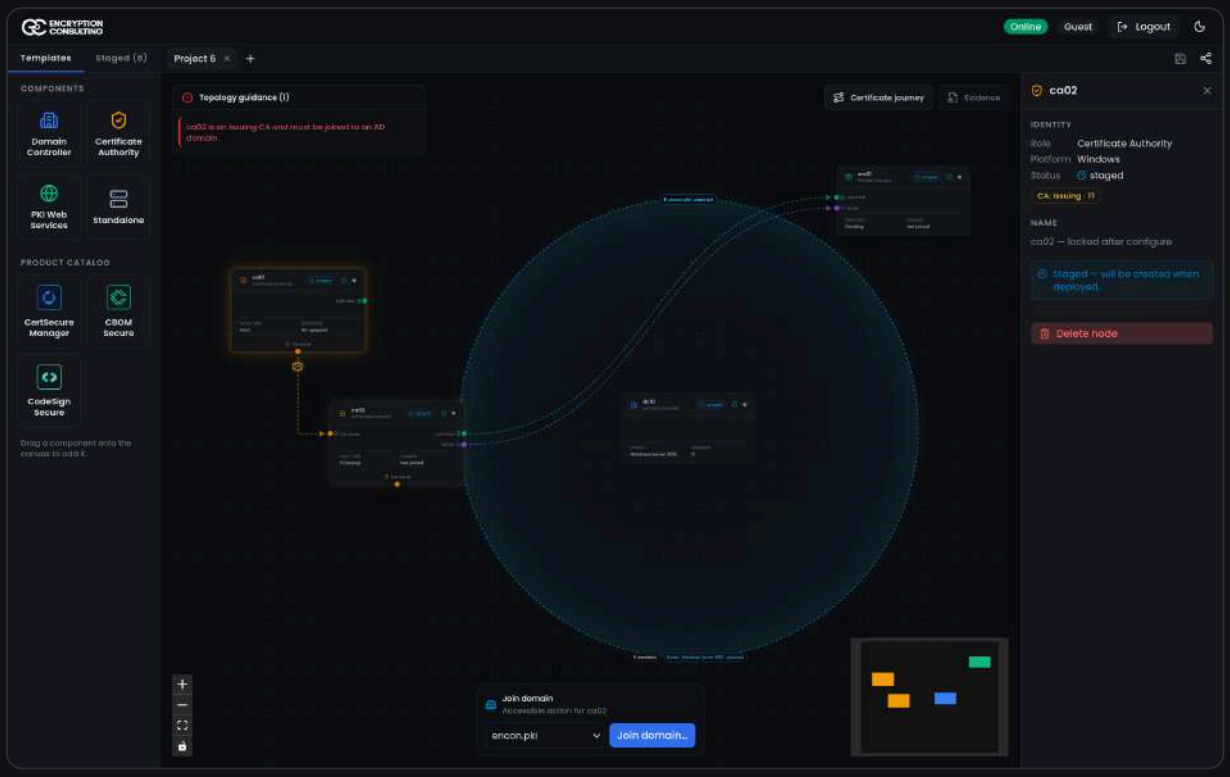
1 Connect the Root and Issuing Certificate Authorities

Press and hold the **CA Issue** socket on `ca01`, the amber point at the lower edge of the node, and drag. As soon as the drag begins, the canvas describes what is taking place: a panel names the relationship being created and the operation that it will generate, every compatible target is highlighted in green, and the guidance pill expands to list what remains outstanding.



> **A connection in progress.** *Issue a subordinate CA certificate · 1 compatible.* `ca02` is outlined in green because it is the only node that can accept this connection. Incompatible sockets are hidden entirely, rather than displayed and then refused.

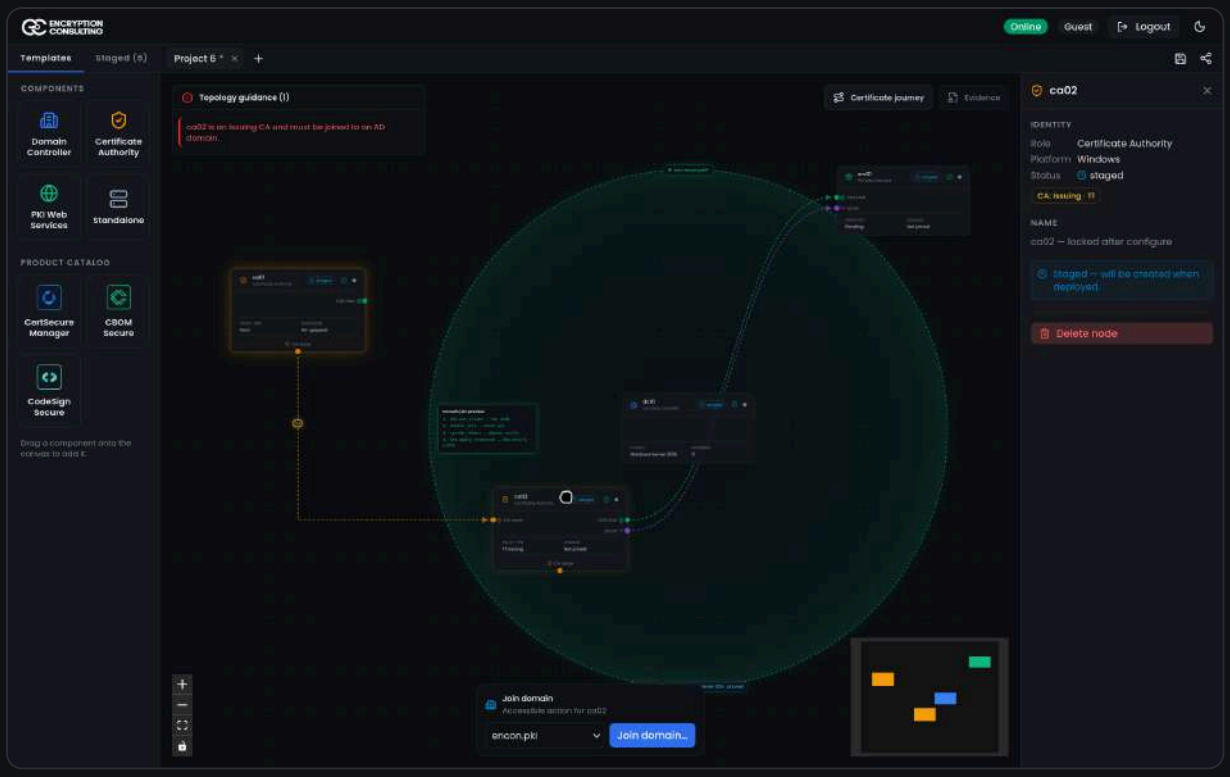
Release the pointer over the **CA Issue** socket on the left edge of `ca02`. An amber edge is drawn between the two nodes, carrying an envelope symbol that represents the certificate request travelling from the subordinate authority to the root authority, and the signed certificate returning.



Trust established. The trust tier of `ca02` changes from *Standalone* to *T1 issuing*. It now has a parent, and the topology has a hierarchy.

2 Connect CRL Publication and OCSP

Drag from the **CDP/AIA** socket on `ca02` to the **CDP/AIA** socket on `srv01`, and then from the **OCSP** socket on `ca02` to the **OCSP** socket on `srv01`. Two dashed edges appear: green for publication, and violet for OCSP.



Three relationships. Issuance in amber, publication in green, and OCSP in violet. Edges are dashed while they are planned, and become solid once the operation behind them has run.

One warning remains in the guidance pill: *ca02 is an Issuing CA and must be joined to an AD domain*. That condition is resolved in Part 6.

06

Join the Domain

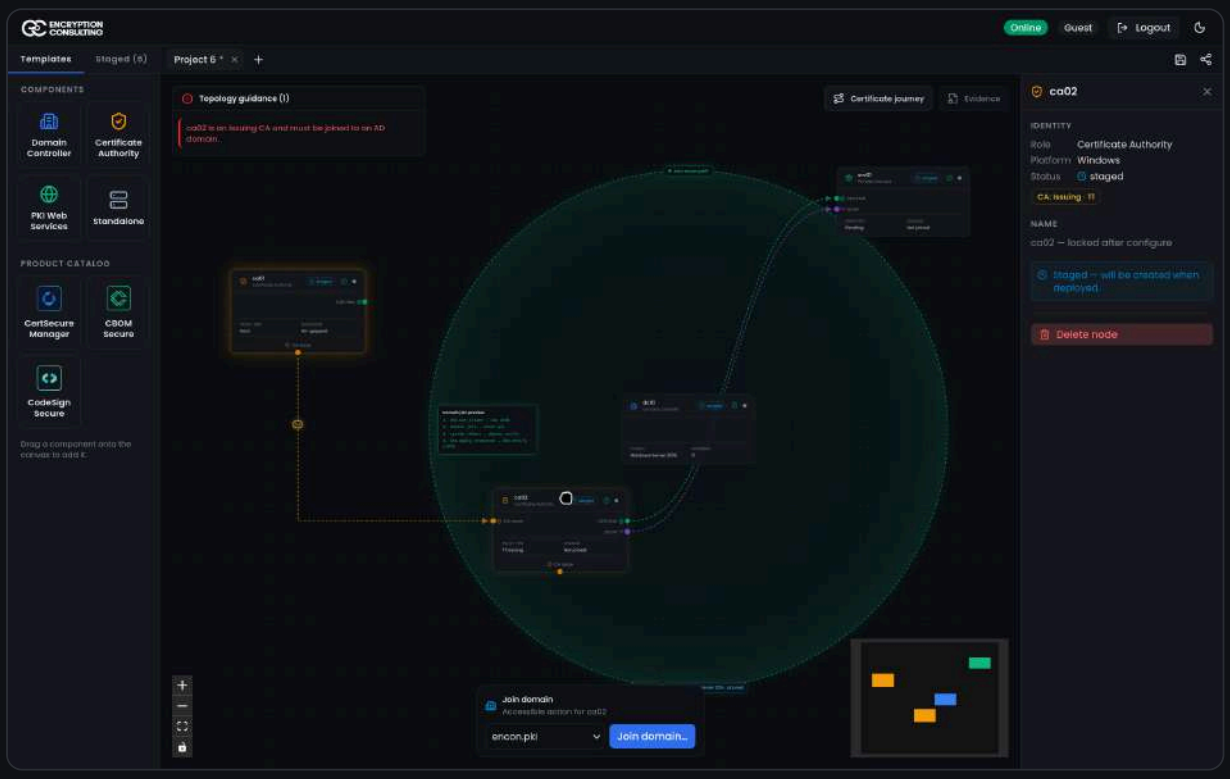
Domain Membership Is Expressed Spatially. A Machine Placed inside the Region Joins the Domain.

Join the Domain

The domain is drawn on the canvas as a circular region, and membership is determined placing a machine inside the region. Dragging a machine out of it causes the Playground to propose a domain departure.

1 Drag the Issuing Certificate Authority into the Domain Region

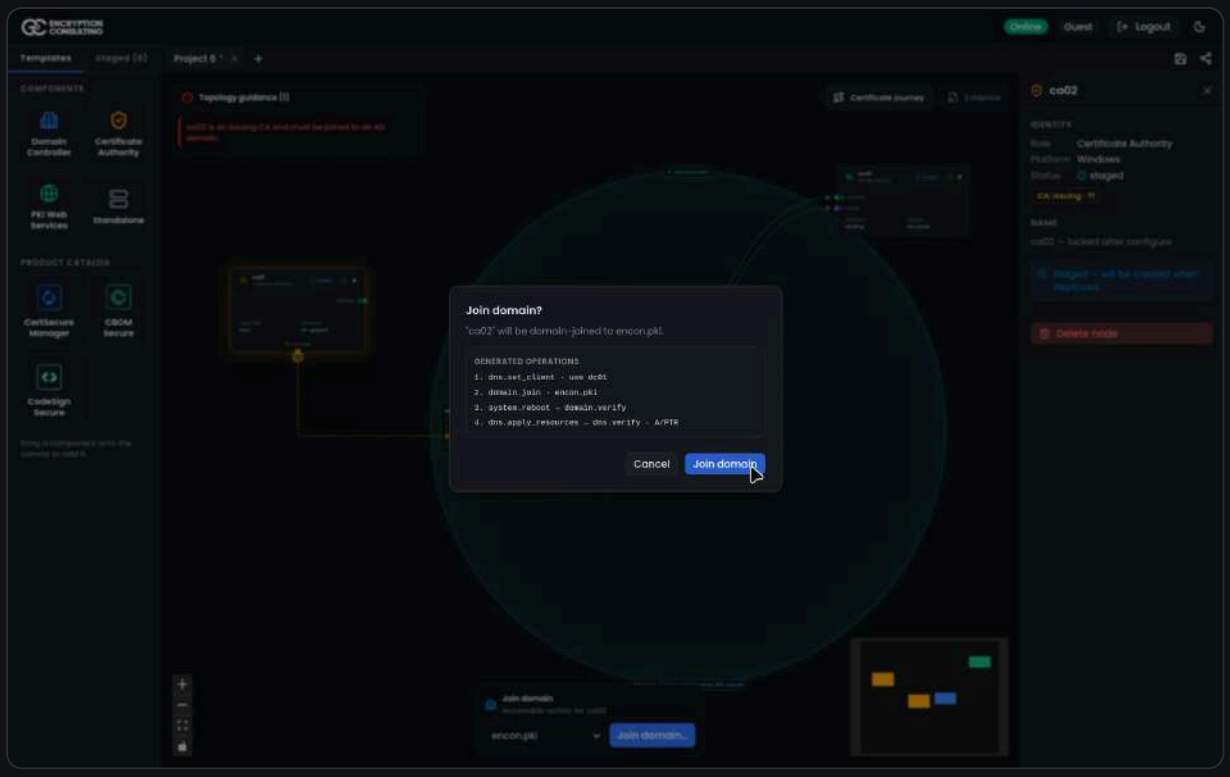
Take hold of `ca02` by its header and drag it inside the dashed circle surrounding `dc01`. While the node is positioned over the region, the circle is highlighted to indicate that the placement will be accepted.



Crossing the boundary. The region turns green while it holds a node that is eligible to join it. A placement that would not be valid, such as an unconfigured node, or a domain controller dragged into another domain, is refused, and the reason is stated.

2 Confirm the Join

Release the node, and the Playground requests confirmation before committing the change. The dialog merits reading, because it lists, in order, the **generated operations** that the join will perform.

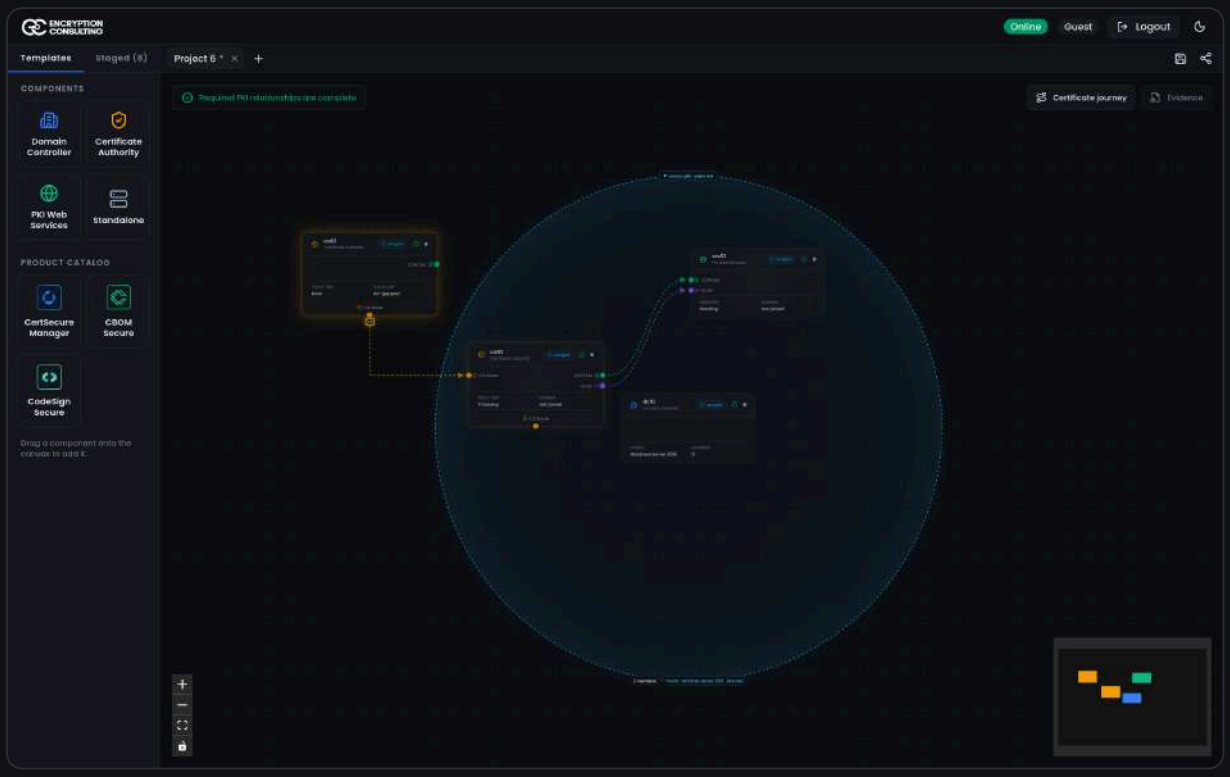


Join domain. Four operations: direct DNS to `dc01`, join `encon.pki`, restart the machine and verify membership, and then apply and verify the A and PTR records. This is the level of detail that the Playground compiles behind each gesture.

Select **Join domain**. Selecting **Cancel** returns the node to its previous position, so that the diagram and the actual membership can never disagree.

3 Domain Join the PKI Web Services

Repeat the same operation for `srv01`. The same dialog appears, listing the same four operations.

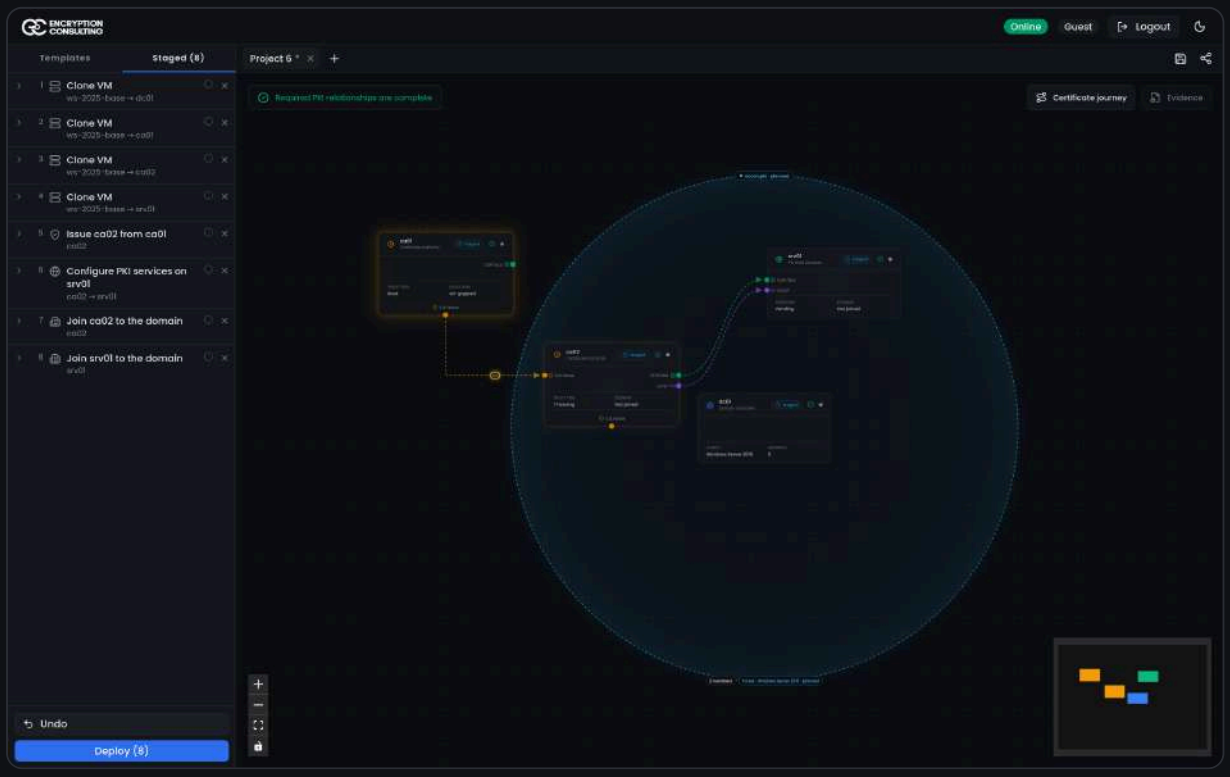


Inside the boundary. A joined member is drawn with a link back to its domain controller, and the member count of the domain increases.

> **LEAVE THE ROOT CERTIFICATE AUTHORITY OUTSIDE THE REGION**
>
> Do not drag `ca01` into the circle. An offline root authority is air-gapped by design. It is not a domain member, and it does not need to be one. Its only relationship is the issuance edge drawn in Part 5.

4 Check the Guidance on the Top Left

With the issuing certificate authority joined to the domain, the final warning clears and guidance returns to green, reporting that *Required PKI relationships are complete*. The topology is ready to be deployed.



The completed topology. A domain controller and its region, an air-gapped root authority signing a domain-joined issuing authority, and a web host publishing CDP, AIA, and OCSP on its behalf.

07

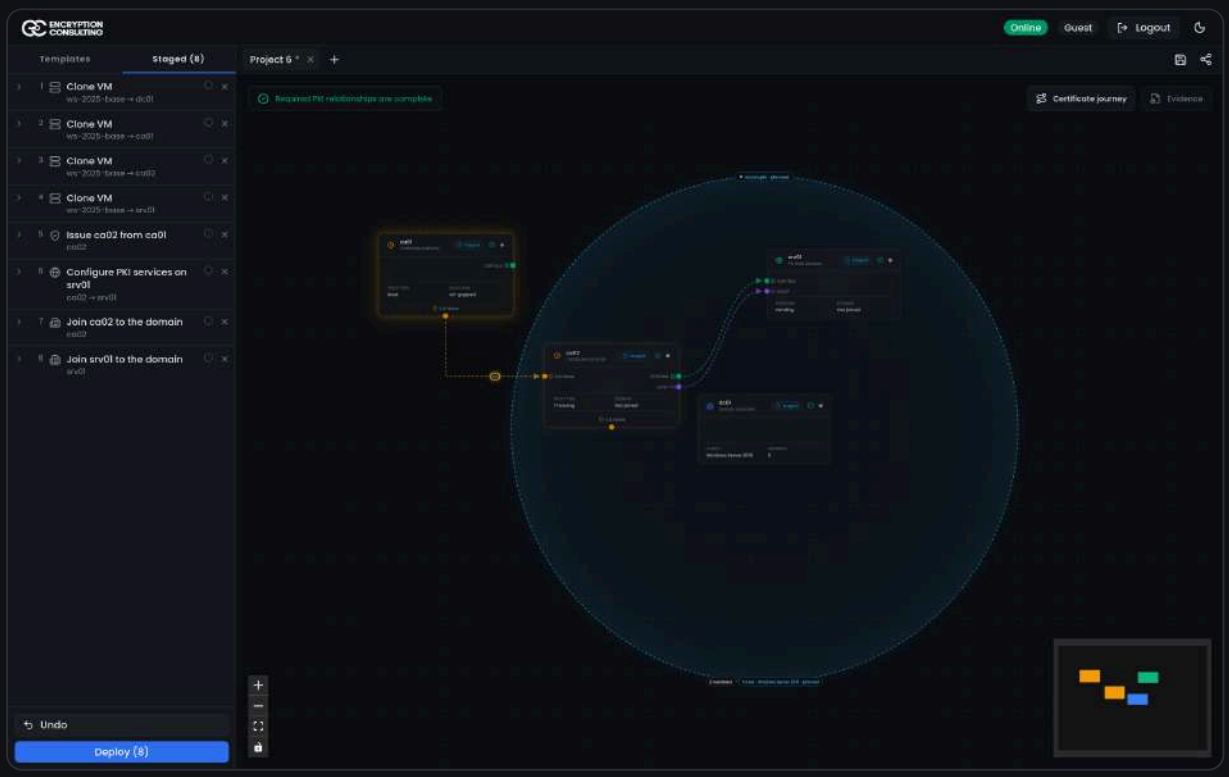
Review and Deploy

Everything That Has Been Staged, Compiled into an Ordered Plan, and Then Executed.

Review What You Have Staged

1 Open the Staged Tab

Select **Staged** at the top of the toolbox. The panel widens and lists every operation that has been created, in the order in which the operations will run. For the environment built in this guide, there are eight rows: four machines to create, two domain joins, one issuance relationship, and one publication relationship.



The staged operations. Four machines to create, one issuance relationship, one publication relationship, and two domain joins, with the **Deploy** button and its count at the foot of the panel.

Each row carries an icon indicating its kind, a description, and a status symbol. Before a deployment, every row is shown as a hollow circle, denoting the staged state.

2 Remove or Undo an Operation

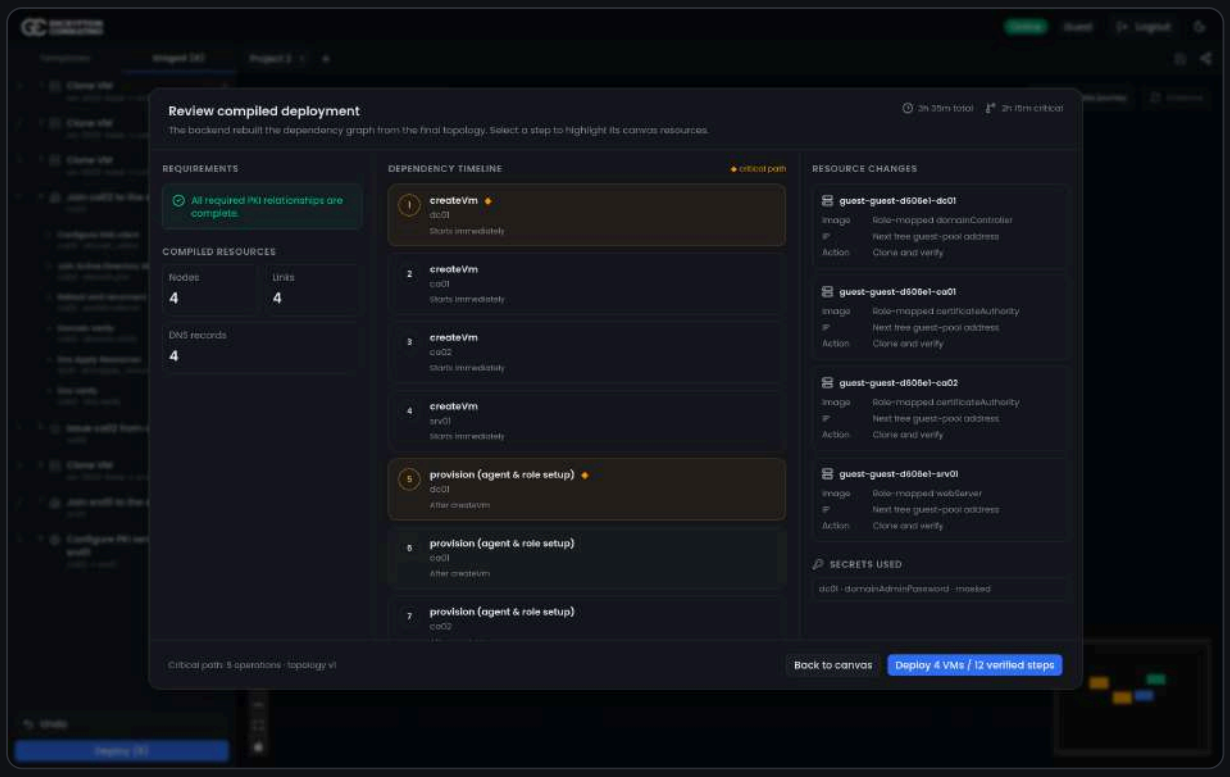
Each row carries a ✕ control. Because later operations can depend on earlier ones — a domain join depends on the existence of the machine — removing one row may require the removal of others. When that is the case, the Playground names precisely which operations are affected, and requests confirmation before removing anything.

The **Undo** button, and `Ctrl` + `Z`, remove the most recent operation. Because the list is always maintained in dependency order, the most recent operation never has dependents, which is what makes a simple undo safe.

Deploy

1 Select Deploy

The **Deploy** button at the foot of the Staged panel carries a count of the operations that it will run. Selecting it does not begin the deployment immediately. The topology is first sent to the backend to be compiled, and the result is returned as a plan for you to review.



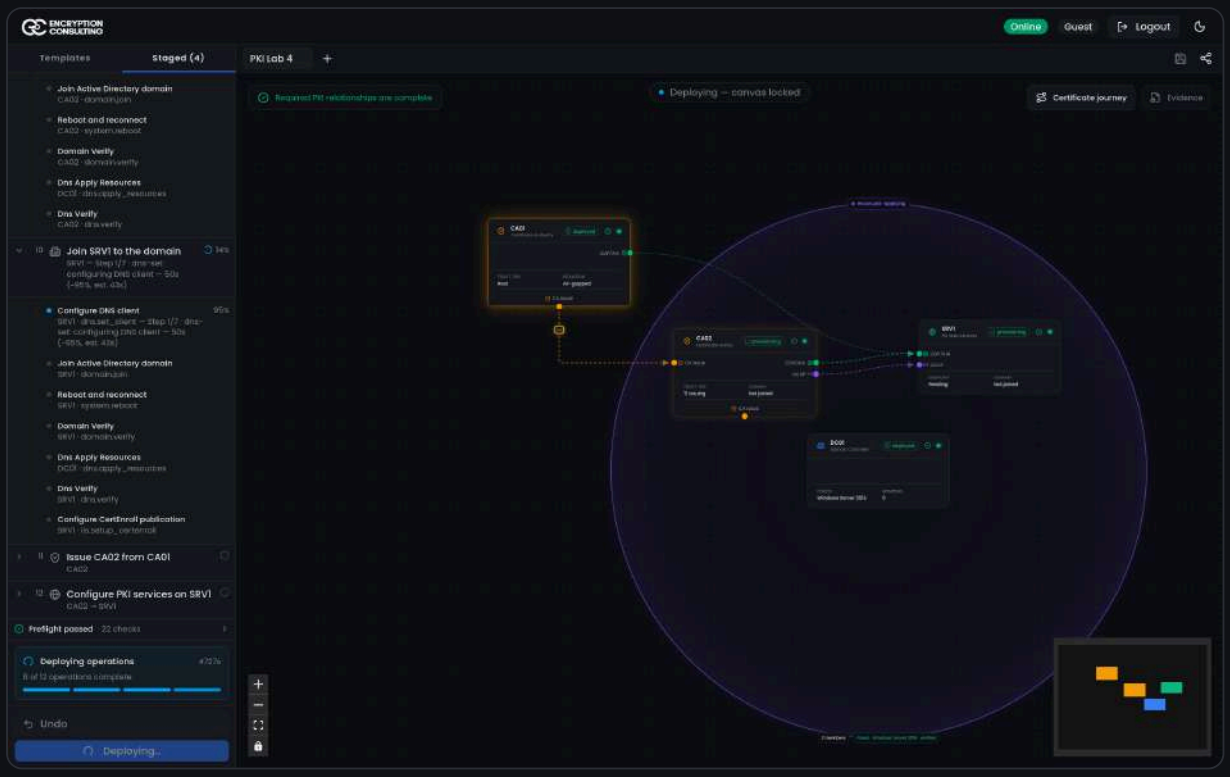
The compiled plan. The operations that the backend derived from the topology, the groups that may run in parallel, the critical path, and an estimated duration.

The review presents the compiled operations, the execution groups that may run in parallel, the critical path, and an estimated duration. It states what is about to happen, and in what order.

> **THIS IS THE POINT OF NO RETURN**
>
> Confirming enqueues a real job: virtual machines are cloned on the shared host, addresses are allocated from a finite pool, and the machines are started. Cancelling at this point has no cost and changes nothing.

2 Confirm the Plan, and Observe the Run

Once the plan is confirmed, the canvas is locked, because a topology that is being built cannot be edited, and progress is streamed back as it occurs. Each staged row acquires a progress indicator and a percentage, and then a green check mark. On the canvas, nodes move from `staged` to `deploying`, and their domain regions change from dashed to solid.



The run in progress. Each staged row acquires a progress indicator and a percentage, and then a green check mark. On the canvas, the nodes leave the *staged* state and the domain region changes from dashed to solid.

3 In the Event of a Failure

A failed operation turns red, and its error message is readable from the row itself. A failure does not abort the plan: operations that depended on the failed operation are marked cancelled and skipped, and every operation independent of it continues. Rows that have already succeeded remain listed for context.

WHEN YOU HAVE FINISHED

A deployed environment holds real machines and real addresses drawn from a pool shared with everyone else using the Playground. When you have finished with an environment, please inform Encryption Consulting, and the environment will be reclaimed. No shutdown procedure is required of you.

08

Projects

Saving, Sharing, Starting Again, and Signing Out.

Working with Projects

Tabs

Each project is represented by a tab across the top of the canvas. The **+** control creates another project, the **×** on a tab deletes that project after a confirmation, and double-clicking a tab name renames the project. Projects are private to you: the console displays only the projects that your account owns.

Saving

Projects are saved automatically. Changes are written back shortly after you stop making them, and an asterisk after the project name indicates that something has not yet been saved. The save icon, or `Ctrl` + `S`, forces a checkpoint immediately.

> **A DEPLOYMENT SAVES FIRST**
> Clicking deploy always checkpoints the project first. A deployment names real machines after the project, so the project must exist on the server before the machines do.

Sharing

The share icon publishes a read-only link to the current project. Anyone who opens that link receives a copy of the topology on their own canvas, marked as collaborative and kept separate from their own projects.

Starting from a Template

Project Template, on the start screen and in the **+** menu, creates a project in which the two-tier public key infrastructure is already drawn and already configured. It is the most direct route to a deployable environment, and it serves as a reference against which a topology of your own construction may be compared.

Signing Out

Logout in the header ends the session and returns you to the sign-in screen. Your projects remain on the server. The local copy held by the browser is detached and cleared, so that the next person to use the machine begins with none of your data.

Reference

Components, Badges, Guidance Messages, and Shortcuts.

Appendix A · Component Reference

Components

COMPONENT	PLATFORM	PROVIDES	AUTOMATIC NAME
Domain Controller	Windows	AD DS · DNS	`dc01`
Certificate Authority	Windows	AD CS, root or issuing	`ca01`
PKI Web Services	Windows	IIS publication · CDP/AIA · OCSP	`srv01`
Standalone	Windows	A Windows Server with no role installed	`misc01`

Product Catalog

PRODUCT	PLATFORM	BASE IMAGE
CertSecure Manager	Linux	Ubuntu 22.04
CBOM Secure	Linux	Ubuntu 22.04
CodeSign Secure	Linux	Ubuntu 22.04

Configuration Fields

Domain Controller

FIELD	TYPE	DEFAULT
Domain Name	text	`encon.pki`
NetBIOS Name	text	`ENCON`
Forest Level	select	Windows Server 2016 / 2019 / 2022 / 2025
Reverse DNS Zone	text, optional	—
Domain Admin Password	password, required	—

Certificate Authority

FIELD	TYPE	DEFAULT
Type	select	Root / Issuing
Common Name	text	`EC-Root-CA` / `EC-Issuing-CA`
CA Publication Directory	text	`C:\Windows\System32\CertSrv\CertEnroll`
Key Algorithm	select	RSA / ECDSA / **ML-DSA-87**
Key Length	select	2048 / 4096 — fixed at 2,592 bytes for ML-DSA-87
Hash Algorithm	select	SHA256 / SHA384 / SHA512 — not used by ML-DSA-87
Validity (years)	text	20 (root) / 10 (issuing)
CPS URL	text	Issuing authorities only

PKI Web Services

FIELD	TYPE	DEFAULT
CertEnroll Directory	text	`C:\CertEnroll`
Online Responder	select	Enabled / Disabled
OCSP Refresh (min)	text	15

Appendix B · Lifecycle Badges

BADGE	MEANING	NEXT ACTION
draft	Placed, but not configured. It cannot be connected, joined to a domain, or deployed.	Configure it.
staged	Configured. It will be created when the topology is deployed.	Deploy the topology.
deploying	Its operation is running within an active plan.	Wait.
provisioning	The machine has started, but its in-guest agent has not yet reported.	Wait.
deployed	Live, reachable, and with its agent connected.	Use the machine.
drifted	Deployed, but its configuration has been edited since deployment.	Informational only.
failed	Its operation did not succeed.	Read the error message on the staged row.

Appendix C · Topology Guidance

The pill at the top left of the canvas is a continuous check on the topology. Green indicates that every required relationship exists. A red count expands into the specific errors. The errors listed below are those encountered most frequently.

MESSAGE	RESOLUTION
"…is an issuing CA but has no root CA parent."	Drag from the CA Issue socket of the root authority to the corresponding socket on the issuing authority.
"…is an issuing CA and must be joined to an AD domain."	Drag the issuing authority into the region of the domain controller, and confirm the join.
"…publishes HTTP CDP/AIA, but no web host is connected."	Connect the CDP/AIA socket of the authority to a PKI Web Services node.
"…has OCSP enabled, but no issuing CA grants its enrollment templates."	Connect the OCSP socket of an issuing authority to the web host, or disable the Online Responder.
"Configure the node before placing it inside a domain."	Configure the node first. A draft node cannot be a domain member.
"A domain controller defines its own boundary and cannot join another domain."	This is expected. Leave the domain controller where it is.
"This CA common name is already used by…"	Change the common name, or change the type of the authority. Changing the type to Issuing renames it automatically.

Appendix D · Shortcuts

KEYS	EFFECT
`Ctrl` + `Z`	Undoes the most recent staged operation. Ignored while text is being entered in a field.
`Ctrl` + `S`	Saves the active project immediately.
`Shift` + drag	Selects several nodes at once.
Scroll	Zooms the canvas.
Drag empty canvas	Pans the canvas.
Click empty canvas	Deselects the current node and closes the Inspector.