

Installation and Configuration Guide

Preparation and Prerequisites

Privileged Access Management Feature

The **Privileged Access Management (PAM) Active Directory optional feature** essentially unlocks two new capabilities in the AD Forest: Temporary time-based group memberships, and shadow principals. Both were introduced to allow the implementation of a Red (or bastion) Active Directory Forest, using a MIM (Microsoft Identity Manager) for requesting temporary privileged access. However, our JiT solution only leverages the former to ensure that after the specified time has elapsed, the user will be automatically removed from the security group (without administrator intervention).

Note! Enabling the PAM feature incurs some additional CPU overhead on the DCs in the forest where the feature is enabled. For most workloads in most environments, this CPU overhead is typically less than 1-2%. However, group member enumeration of very large security groups (for example, groups with more than 10K members) can become significantly (2 to 3 times) more expensive. For example, enumerating the group members of a security group with 20K members may take 200 milliseconds before enabling the PAM feature, and 400 milliseconds after enabling the PAM feature, depending on group size, the DC's hardware, etc. Administrators are advised to have an AD forest restore plan in place and ready to be executed prior to making any irreversible changes to their AD forest. Credits for this investigation go to our colleague [Ryan Ries](#).

The PAM feature in turn requires that the AD forest is running at **Windows Server 2016 forest function level (or higher)**.

You can run the following command to verify whether the PAM feature has been already enabled in your Forest:

```
Get-ADOptionalFeature -filter "name -eq 'privileged access management feature'"
```

In case the PAM feature is not enabled, the EnabledScope sections will be empty. In the screenshot below the PAM feature has already been enabled:

```
PS C:\Users\loc_admin> Get-ADOptionalFeature -filter "name -eq 'privileged access management feature'"
DistinguishedName : CN=Privileged Access Management Feature,CN=Optional Features,CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=contoso,DC=com
EnabledScopes      : {CN=NTDS Settings,CN=J-DC03-child,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,
DC=contoso,DC=com, CN=Partitions,CN=Configuration,DC=contoso,DC=com, CN=NTDS Settings,CN=J-DC01,CN
=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=contoso,DC=com}
FeatureGUID        : ec43e8/3-cce8-4b40-b4ab-0/77e4ab0bdc
FeatureScope       : {ForestOrConfigurationSet}
IsDisableable      : False
Name               : Privileged Access Management Feature
ObjectClass         : msDS-OptionalFeature
ObjectGUID         : 8dadcdce-f70c-4ed2-8357-e73cace5cd9f
RequiredDomainMode : 
RequiredForestMode : Windows2016Forest
```

The following command enables the PAM feature in the AD Forest:

```
Enable-ADOptionalFeature "Privileged Access Management Feature" -Scope  
ForestOrConfigurationSet -Target <ADEntity>
```

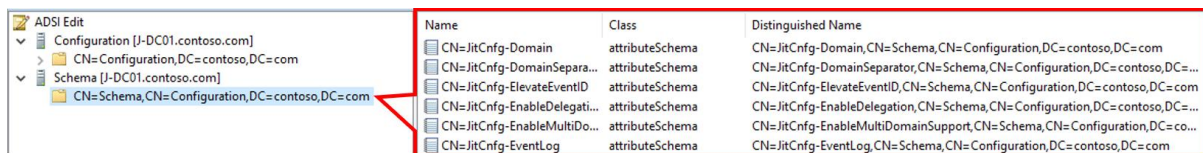
Note!

The command together with all the parameters required will be provided as part of the installation procedure.

AD Schema Update

The configuration for the JiT solution will be stored in Active Directory. To make this possible an Active Directory Schema extension must be implemented. Even though most AD admins do not enjoy schema updates, AD turned out to be the perfect location for storing the JiT configuration: it is highly available by default and is less likely to be messed up or even deleted than config files.

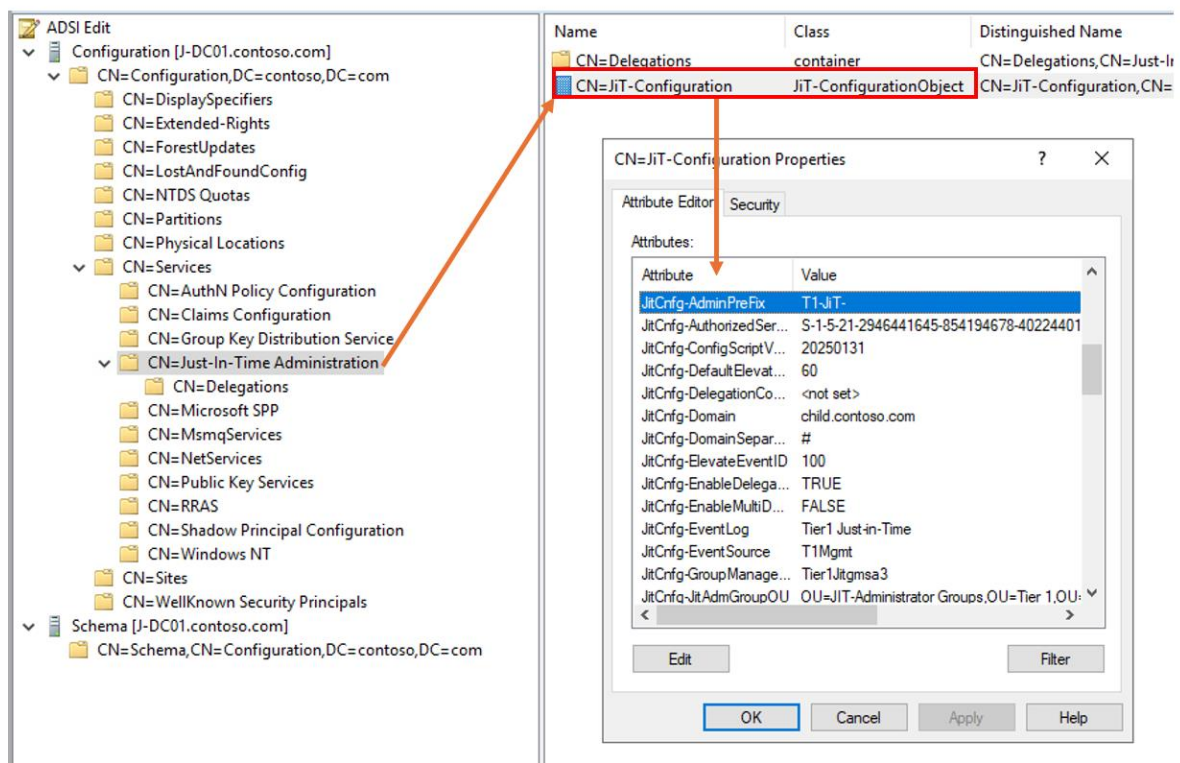
The changes related to the AD Schema Update can be reviewed in ADSI Edit:



Name	Class	Distinguished Name
CN=JitCfg-Domain	attributeSchema	CN=JitCfg-Domain,CN=Schema,CN=Configuration,DC=contoso,DC=com
CN=JitCfg-DomainSepar...	attributeSchema	CN=JitCfg-DomainSeparator,CN=Schema,CN=Configuration,DC=contoso,DC=...
CN=JitCfg-ElevateEventID	attributeSchema	CN=JitCfg-ElevateEventID,CN=Schema,CN=Configuration,DC=contoso,DC=com
CN=JitCfg-EnableDelegati...	attributeSchema	CN=JitCfg-EnableDelegation,CN=Schema,CN=Configuration,DC=contoso,DC=...
CN=JitCfg-EnableMultiDo...	attributeSchema	CN=JitCfg-EnableMultiDomainSupport,CN=Schema,CN=Configuration,DC=co...
CN=JitCfg-EventLog	attributeSchema	CN=JitCfg-EventLog,CN=Schema,CN=Configuration,DC=contoso,DC=com

JiT-ConfigurationObject

The actual configuration is stored in the attributes of the JiT-ConfigurationObject created for this purpose in CN=Just-In-Time Administration,CN=Services,CN=Configuration,DC=<domain>,DC=<tld>



Name	Class	Distinguished Name
CN=Delegations	container	CN=Delegations,CN=Just-In-Time Administration,CN=Services,CN=Configuration,DC=contoso,DC=com
CN=JiT-Configuration	JiT-ConfigurationObject	CN=JiT-Configuration,CN=Delegations,CN=Just-In-Time Administration,CN=Services,CN=Configuration,DC=contoso,DC=com

Attribute	Value
JitCfg-AdminPreFix	T1-JiT-
JitCfg-AuthorizedSer...	S-1-5-21-2946441645-854194678-40224401
JitCfg-ConfigScriptV...	20250131
JitCfg-DefaultElevat...	60
JitCfg-DelegationCo...	<not set>
JitCfg-Domain	child.contoso.com
JitCfg-DomainSepar...	#
JitCfg-ElevateEventID	100
JitCfg-EnableDelega...	TRUE
JitCfg-EnableMultiD...	FALSE
JitCfg-EventLog	Tier1 Just-in-Time
JitCfg-EventSource	T1Mgmt
JitCfg-GroupManage...	Tier1Jitgmsa3
JitCfg-JitAdmGroupOU	OU=JiT-Administrator Groups,OU=Tier 1,OU=...

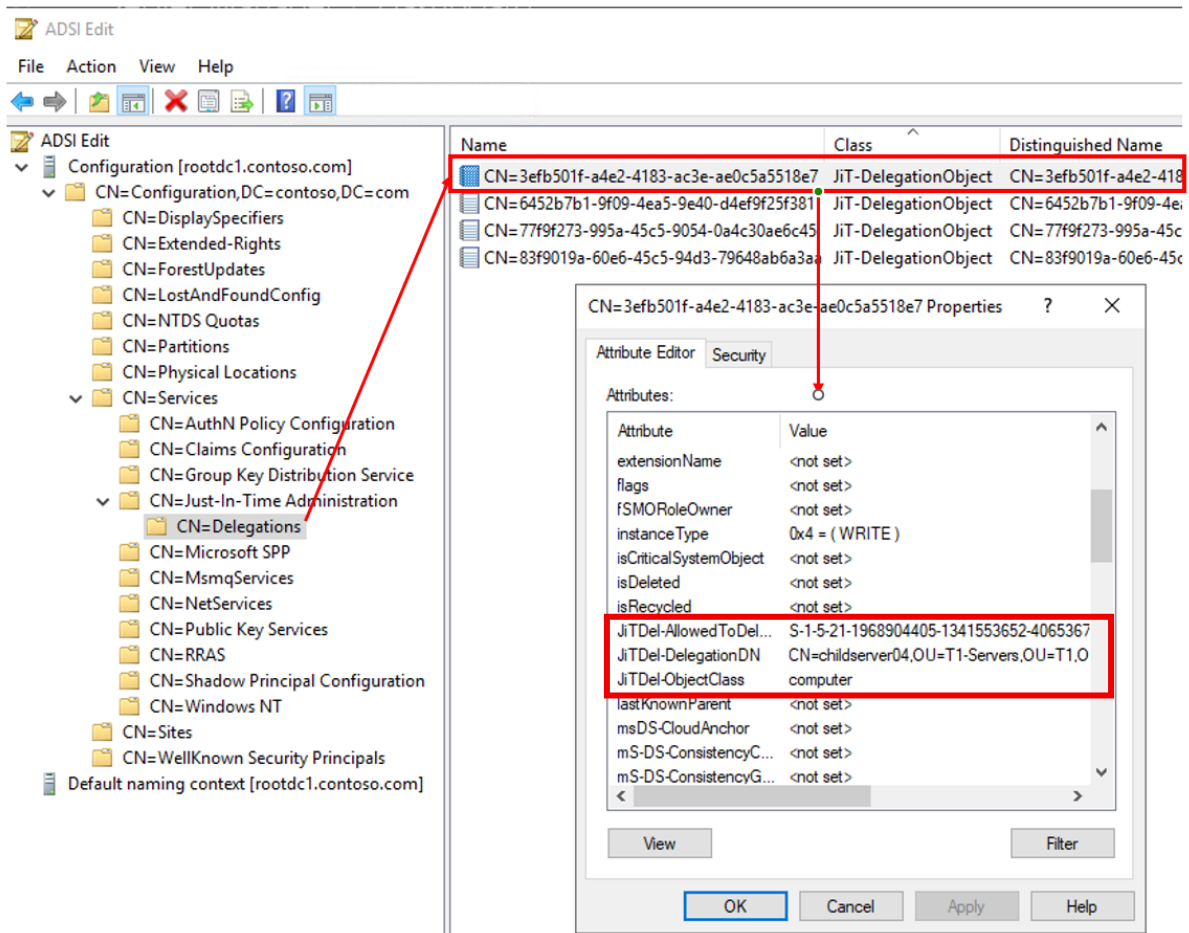
Note

The JiT-Configuration object is filled with default values during creation.

Delegations Container

This container is used for configuring server- or OU-based permissions. In simple terms: which T1-Admin account is allowed to request elevation on which server or OU holding T1-servers.

A separate object storing the relevant information as attributes is created in this container for each delegation:



Monitoring

The configuration procedure creates an Event Log (Default name = Tier1 Just-in-Time) in Windows Event Viewer.

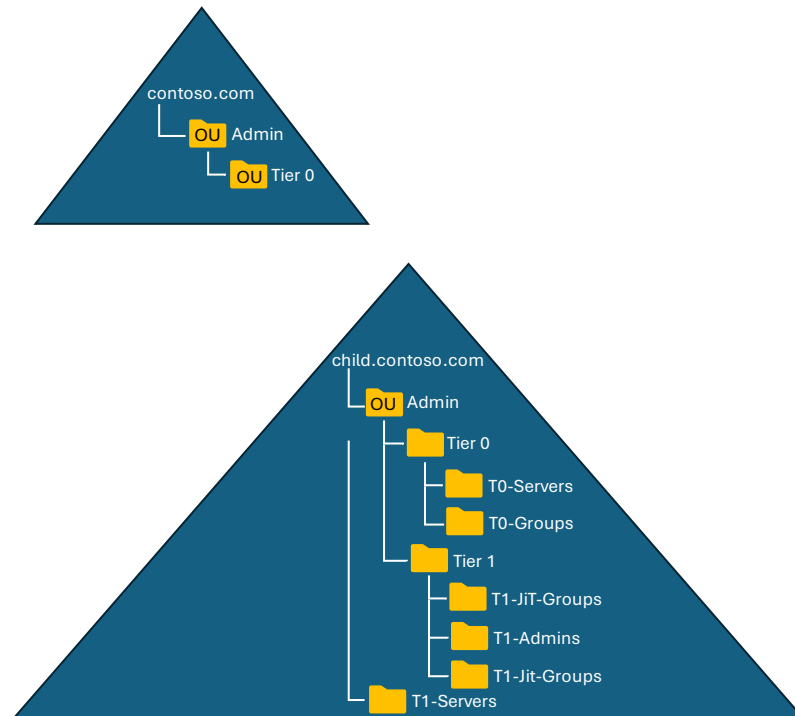
The event source (default = T1Mgmt) and the event ID written when an elevation is performed (default event ID = 100) can be configured during initial setup.

Events are written under the following circumstances:

- JiT configuration complete with/without errors.
- A new JiT (admin) group is created/creation failed.
- Elevation is requested
- Elevation is performed (event details include user to be elevated, Jit admin group, T1 server's domain in case the tool is operated in multi domain mode, elevation time, user requesting elevation.

Sample Walkthrough of JiT Implementation in a Multi-Domain Forest

The sample Active Directory Forest consists of a root domain (contoso.com) and a child domain (child.contoso.com). As Tier 1 servers only exist in the child domain, the JiT solution will be implemented only in child.contoso.com (aka “single-domain support”).



Step 1: Schema Update

The easiest way of performing the AD Schema Update is by running the installation script as follows:

1. Log on to a Domain Controller in the root domain (contoso.com) with an account which is member in the Schema Admins and Enterprise Admins groups.
2. Copy and extract the JiT files into a folder on the local disk.
3. Open an **elevated** PowerShell prompt and run install-JiT.ps1 with the parameter - ExtendSchema: **.\install-JiT.ps1 -ExtendSchema**

Note!

Adding the parameter-**CustomOidPrefix** allows to specify a registered OID prefix for the new Active Directory schema objects:

```
.\install-JiT.ps1 -ExtendSchema -CustomOidPrefix  
1.3.6.1.4.1.[customer PEN].[sub trail AD].[sub trail schema]
```

The script will verify if the **Privileged Access Management (PAM)** Feature is enabled for the forest and if not will provide the exact command to enable it. Please follow the instructions to enable the PAM feature before running **.\install-JiT.ps1 - ExtendSchema** again.

Step 2: JiT-ConfigurationObject

Still on the Domain Controller in the root domain (contoso.com) with the same permissions as described in step 1, run:

.\install-JiT.ps1 -CreateADStructure

This will create the **Just-In-Time Administration** and the **Delegations** container, as well as the **JiT-ConfigurationObject** in the Active Directory configuration partition.

Step 3: Installation of the JiT Tools on JiT Management Server

The T1-JiT solution must be a Tier 0 service and therefore administered by Tier 0 and protected accordingly. This solution will be provided to Tier 1 as a service, which results in the T1-Jit-Management server(s), the Jit-Administrative groups and the according GPO will be Tier 0 and part of the Tier 0 administrative structure.

1. Log on the T1 Management server (in child.contoso.com in our scenario) with an account with membership in the **Enterprise Admins group**.
2. Open an **elevated** PowerShell prompt and run **.\install-JiT.ps1**
3. Provide a custom installation directory or accept the default (C:\Program Files\Just-In-Time).

The script will perform the following tasks:

- Copy all JiT related files to the installation directory specified.
- Copy the JiT PowerShell module to C:\Program Files\WindowsPowerShell\Modules\Just-In-Time
- Checks for JiT AD schema extensions.
- Updates AD schema cache.
- Checks for Jit administration AD structure.
- Registers the computer (its SID) in the JiT configuration object in AD (see step 2).

Step 4: Configuration of JiT on JiT Management Server

1. For the initial configuration: Still in the **elevated** PowerShell prompt, run **.\config-JiT.ps1**

Note: run **.\config-JiT.ps1 -UpdateConfig** to load (and change) a previous configuration. See "Update existing configuration" section later in this document for a list of parameters which cannot be changed.

2. Go through the questions marked as **open** one by one

Decision table

Nr	Configuration item	
1	JiT schema extension	Done Schema update was performed in step 1.
2	JiT AD structure	Done JiT AD structure was created in step 2.
3	Enable/disable multi-domain support	No This setting defines whether the T1-JiT solution will be applied in only one domain or multiple domains in the AD forest. As in our scenario we only have T1 servers in child.contoso.com, we set this <i>No</i> . If set to Yes, the scope of search for servers and groups will be extended to the full AD forest. For multi-domain support, the group prefix for the JiT groups will include the <i>domainFQDN</i> .
4	Define OU for JiT-(admin)groups	Specify the OU in which the JiT-specific groups will be created. OU=T1-JiT-Admin-Groups,OU=T1,OU=Admin,DC=child,DC=contoso,DC=com
5	Define prefix for JiT-groups	T1-JiT In our scenario, this will result in T1-Jit-child.contoso.com#[T1-Server-Name] as a group name.
6	Set default domain for JiT mgmt servers	child.contoso.com
7	Set Name(s) of Tier0 computer group(s) -> multiple Tier0 groups are allowed	T0-Servers The tool needs to identify Tier 1 servers and ensure that no T0 computers are included in the JiT configuration unintentionally. Note! Multiple entries allowed.
8	Define LDAP filters to Tier1 systems	Done Filters for all Windows Server computer objects, excluding gMSA, DCs and RODCs to ensure that these account types are not included in the configuration unintentionally. In almost all cases, there is no need to change something here.
9	Set Tier1 computers OUs (optional)-if not specified, whole domain will be searched	OU=T1-Servers,DC=child,DC=contoso,DC=com Note! Multiple entries allowed.

10	Set Max elevation time allowed for JiT	Default = 600 minutes
11	Set default elevation time used by JiT	Default = 60 minutes
12	Set max. number of systems where users can be elevated in parallel	Default = 10
13	Define name of gMSA running JiT tasks	Provide the name for a gMSA to be created according to your naming convention. Default = T1JiTgMSA-R
14	Define task run interval (minutes)	This setting defines the interval the scheduled tasks will run in.
15	Define central task script directory	A central script directory for the scheduled tasks can be configured in case multiple JiT Management servers will be used. Default = C:\Program Files\Just-In-Time
16	Define Just-in Time event log	Default = Tier1 Just-in-Time The Eventlog will be created on the JiT Management Server, under <i>Application and Services Logs</i> .
17	Define Just-in Time event source	A new event source will be registered. T1Mgmt by default. See the <i>Monitoring</i> section for more details.
18	Set JiT elevation event ID	Event ID 100 by default.
19	Set AD Principals allowed to request on behalf of other identities	Reserved for later use.
20	Enable/disable delegation mode	Default = no Setting to Yes allows restricting the T1-Admins who can elevate themselves to specific T1 servers or T1 servers OUs. We will set this to Yes to demonstrate the feature.
21	Start configuration	
0	Exit configuration	

Based on the information provided, the script will

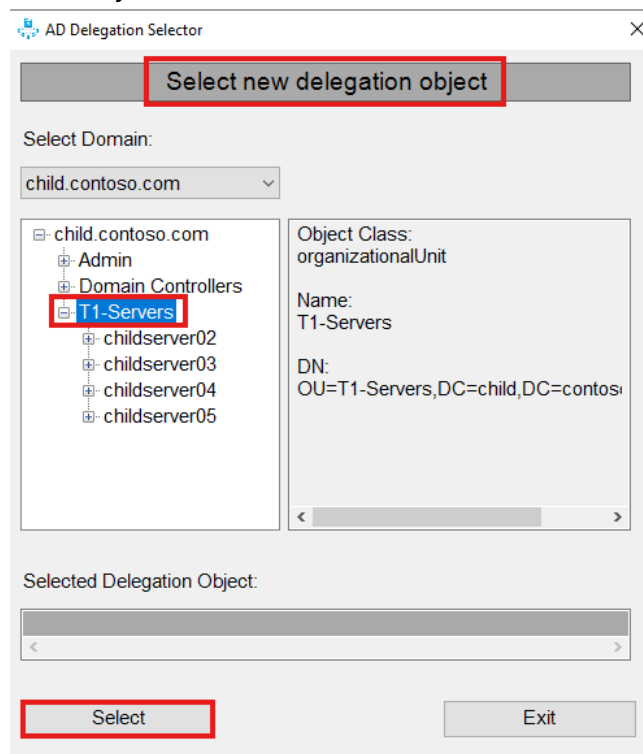
- store the JiT configuration in the [JiT-ConfigurationObject](#) in Active Directory
- define the scope of analysis. In other words: Whether the (search for servers, groups etc.) will be performed in only a single domain or all domains in the forest.
- Create and configure a gMSA for running the Scheduled Tasks on the JiT-Management Server.
- Grant permissions to the gMSA to create and manage group objects in defined OU in Active Directory.
- Create and configure two Scheduled Tasks on the JiT Management Server.
 - Elevate User
 - Tier 1 Local Group Management
- Create the Eventlog and register the event source.

Step 5: Configure Delegation

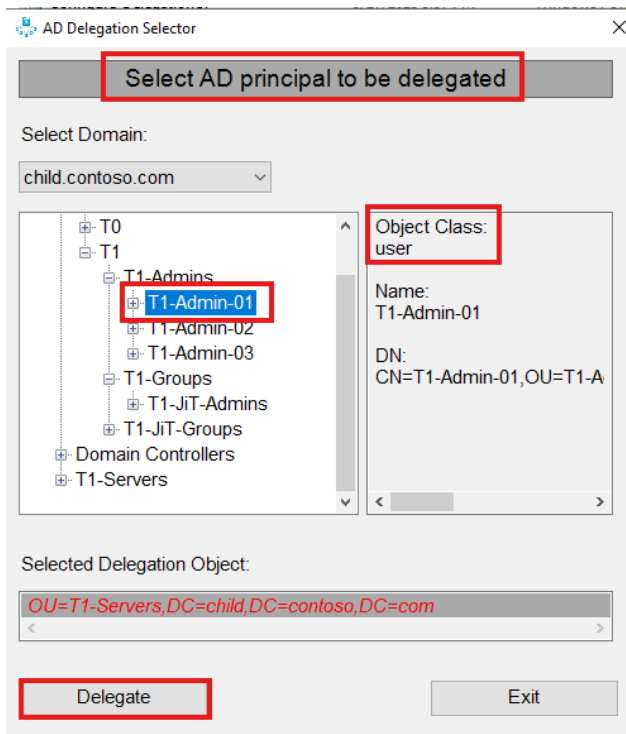
As we enabled delegation mode in the previous step (step 3/21), we can now configure delegation. In simple words: We will configure **which group of users/individual users will be allowed to request elevation to the servers in a specific OU/individual servers**.

1. Still in the **elevated** PowerShell prompt, run **.\config-DelegationUI.ps1**
2. Click **New Delegation**.
3. In the *Select new delegation object* window, your default JiT domain will be already pre-selected.
4. **Note! Delegation can be configured on OU level or on single computer accounts only.**

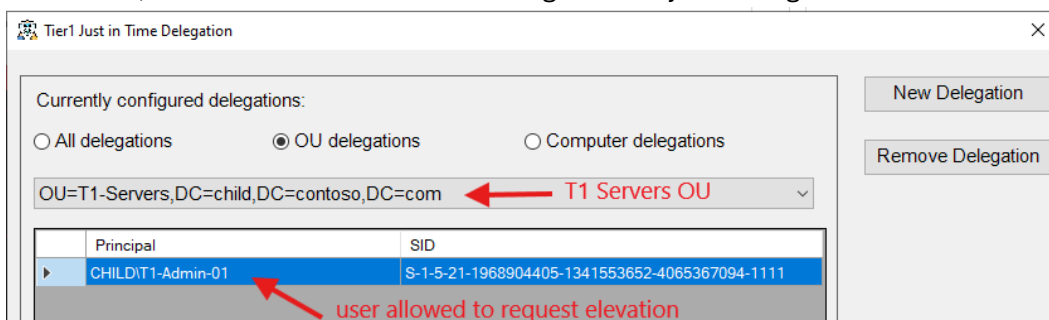
Either choose an OU or a single T1 server like in the screenshot below. Press *Select* to confirm your selection:



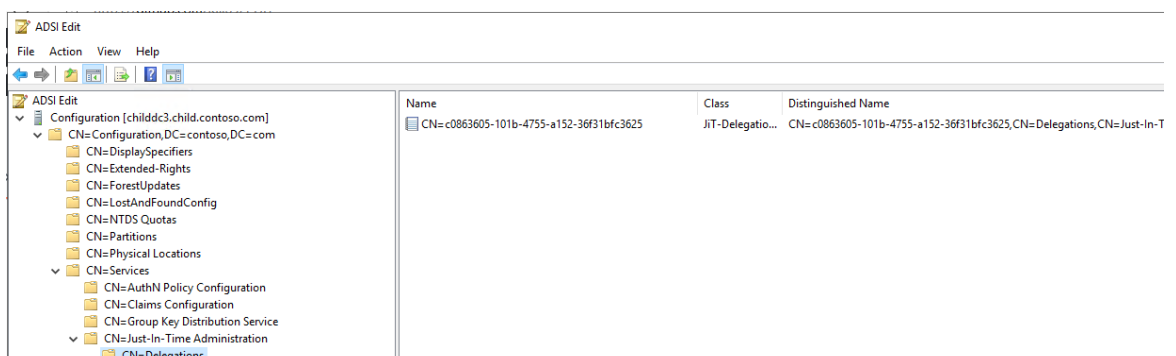
5. **Note! Delegation can be configured for groups or single user accounts only.**
On the *Select AD principal to be delegated* page, choose which individual user (or group of users) will be allowed to request elevation:



6. Press *Delegate* to confirm your selection.
7. As a result, the overview will show the delegation we just configured:



The configuration we just created results in a corresponding object being created in Active Directory:



Step 6: Create Group Policy

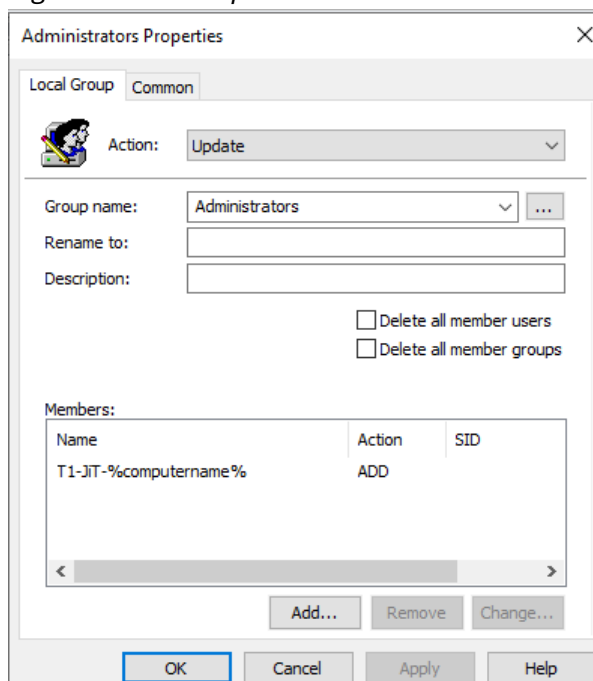
Finally, we need a Group Policy which performs the task of adding the group created individually for each server to the server's (local) *Administrators* group.

1. Create a Group Policy.
2. Edit the Group Policy. Navigate to Preferences → Control Panel Settings.
3. Right-click Local Users and Groups → New → Local Group.
4. Group name = Administrators

Note! Do not browse for the group name. Just type it.

Note! In case you are using different languages you have to add a separate configuration for every single language (e.g. Administratoren, Administrateurs etc.)

5. Press Add and type the name of the group as follows:
[JiT prefix exactly written as in Step 3/5]%computername%
e.g.: *T1-JiT-%computername%*

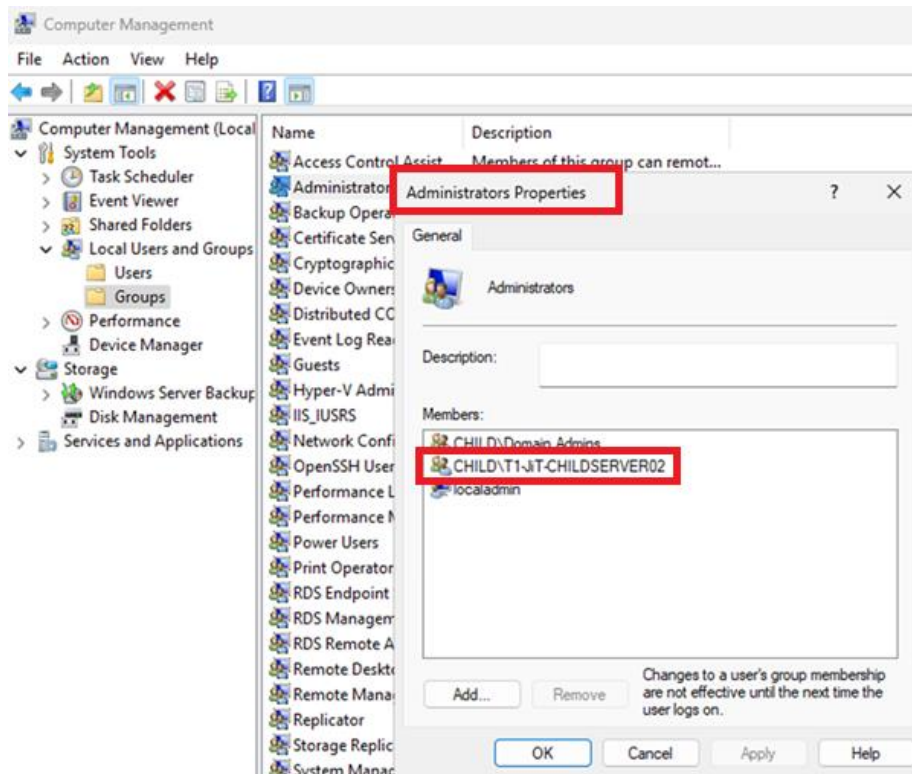


Note: if multi-domain support is enabled, the JiT group names will include the domain FQDN followed by a domain separator (#) to differentiate identical computer names across different domains,
e.g.: *T1-JiT-**child.contoso.com**#%computername%*

- Assign it to the OUs where the T1 servers are located (OU=T1-Servers,DC=child,DC=contoso,DC=com in our scenario)

Once the Group Policy has been applied successfully, the individual JiT group created for each server will be added to the (local) Administrators group.

E.g. the group *T1-JiT-Childserver02* was added to the (local) Administrators group on *childserver02*.



Step 7: Elevation

While all the previous tasks required Enterprise Administrator permissions and local Administrator permissions on the JiT Management Server and therefore required a Tier 0 account, the following tasks will be performed by an unprivileged T1 user.

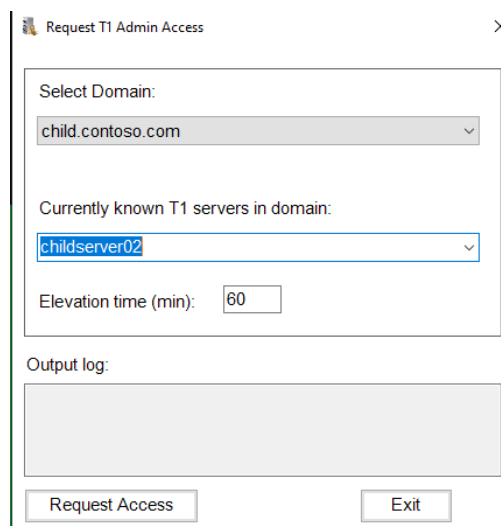
1. **T1-Admin-01** logs on to the **JiT Management Server**.

Note! No Admin permissions of any kind are needed for this step.

Note! To log on to the JiT Management Server T1-Admin-01 must be *member of the Remote Desktop Users* and have the *Allow log on through Terminal Services* User Right assigned.

2. Start **Request-AdminAccessUI.ps1**.
3. The UI will provide a list of all servers for which a JiT group exists in the JiT group OU as well as the default elevation time configured:

Note: new servers might not show up until the "Tier 1 Local Group Management" scheduled task has been run and a proper JiT group has been created for that server.



4. Press *Request Access* to start the elevation process.

The Scheduled Task will add the T1-Admin-01 user account to the T1-JiT-childserver02 group in the background. **T1-Admin-01 is now an indirect member of the local Administrators group on T1-JiT-childserver02.**

Thanks to the Privileged Access Management Feature, the **T1-Admin-01 account will be automatically removed from the group** after elevation time has been exceeded.

Optional: Update existing Configuration

Run **.\config-JiT.ps1 -UpdateConfig** to load (and change) a previous configuration.

Please note that the following items cannot be changed due to dependencies of sharing the configuration between multiple servers:

- Multi-domain support
- JiT-GROUP NAMING
- JiT-Group OU
- Default domain for JiT server
- gMSA
- JiT Eventlog
- JiT Elevation EventID
- Scheduled Tasks settings