Onboard Azure tenant guest access

1. Prerequisites

- Representative with Global Administrator role access.
- Successfully completed "TSD SOP - 02 Register guest access synchronization application"

2. General information

Each step must be successfully implemented.

All operators work primarily as "Security Operators", they have no meaningful lower level of access. Cloud App Security Administrator is added to enable active remediation actions on identities.

3. Basic flow

- Create security groups used to manage Truesec guest access.
- (Optional) Enable privileged access management of the administrators group.
- Verify configuration

4. Tasks

4.1. Create security groups used to manage Truesec guest access.

- Visit https://portal.azure.com
- Go to “Microsoft Entra ID” →”Groups”
- Create the following five security groups
    - Use the specification listed in the table below
    - Bear in mind that the setting “Entra ID roles can be assigned to the group” cannot be changed after a group has been created.

Groups	
Group name:	Truesec SOC Readers
Group description:	Truesec MSS Detect and Respond Readers
AAD roles can be assigned to the group:	Yes
Owners:	Truesec Customer AAD Guest Access Sync EU (id: 650c28b2-db2e-4e95-8124-0d3410659df4)
Members:	-
Roles:	Security Reader
Group name:	Truesec SOC Operators
Group description:	Truesec MSS Detect and Respond Operators
AAD roles can be assigned to the group:	Yes
Owners:	Truesec Customer AAD Guest Access Sync EU (id: 650c28b2-db2e-4e95-8124-0d3410659df4)
Members:	-
Roles:	Security Operator, Cloud App Security Administrator
Group name:	Truesec SOC Privileged Operators
Group description:	Truesec MSS Detect and Respond Privileged Operators
AAD roles can be assigned to the group:	No
Membership type:	Assigned
Owners:	Truesec Customer AAD Guest Access Sync EU (id: 650c28b2-db2e-4e95-8124-0d3410659df4)
Members:	-
Group name:	Truesec SOC Live Responders
Group description:	Truesec MSS Detect and Respond Live Responders
AAD roles can be assigned to the group:	No
Membership type:	Assigned
Owners:	Truesec Customer AAD Guest Access Sync EU (id: 650c28b2-db2e-4e95-8124-0d3410659df4)
Members:	-
Group name:	Truesec SOC Admins
Group description:	Truesec MSS Detect and Respond Administrators
AAD roles can be assigned to the group:	No
Membership type:	Assigned
Owners:	Truesec Customer AAD Guest Access Sync EU (id: 650c28b2-db2e-4e95-8124-0d3410659df4)
Members:	-

5. (Optional) Enable privileged access management to the administrators group.

This option requires an Microsoft Entra ID P2 license.

5.1. Create security groups used to manage privileged access

- Visit https://portal.azure.com
- Go to "Microsoft Entra ID" →"Groups" → "New group"
- Use the specification listed in the table below

Group name:	Truesec SOC Admins PIM
Group description:	Truesec MSS Detect and Respond Administrators privileged access group
AAD roles can be assigned to the group:	Yes
Owners:	-
Members:	-
Roles:	-

5.2. Configure privileged access

- Navigate to the "Truesec SOC Admins PIM" group in Microsoft Entra ID
- Select "Privileged access (Preview)" in the menu to the left.
- Enable privileged access
- Click "Settings" → "Member" → "Edit" → "Assignment"
    - Click "Overview" and then back to "Privileged access (Preview)" if "Settings" aren't visible.
- Enable "Allow permanent eligible assignment" and click "Update"

- Navigate to the "Truesec SOC Admins PIM" group in Entra ID.
- Select "Privileged access (Preview)" in the menu to the left.
- Select the "Eligible Assignments" tab
- Click "+ Add assignment"
- Select role: "Member"
- Select member(s): "Truesec SOC Admins"
- Click "Next >"
- Verify that "Assignment type" is set to "Eligible" and that "Permanently eligible" is selected.
- Click "Assign"

6. Verify configuration

6.1. Check existence of Entra ID security groups:

- Truesec SOC Readers
- Truesec SOC Operators
- Truesec SOC Privileged Operators
- Truesec SOC Live Responders
- Truesec SOC Admins
- (Optional) Truesec SOC Admins PIM

6.2. Check group membership

- Check that the service principal is owner of the five non-optional Truesec SOC * groups
- (Optional) Check that the service principal is **not** owner of “Truesec SOC Admins PIM”
- Check that the “Truesec SOC Operators” group have:
    - Assigned role “Security Operator” AND “Cloud App Security Administrator”
- Check that the “Truesec SOC Readers” group have:
    - Assigned role “Security Reader”

Group Name	Owners	Assigned Role
Truesec SOC Readers	Truesec Customer AAD Guest Access Sync EU	Security Reader
Truesec SOC Operators	Truesec Customer AAD Guest Access Sync EU	Security Operator, Cloud App Security Administrator
Truesec SOC Privileged Operators	Truesec Customer AAD Guest Access Sync EU	-
Truesec SOC Live Responders	Truesec Customer AAD Guest Access Sync EU	-
Truesec SOC Admins	Truesec Customer AAD Guest Access Sync EU	-
Truesec SOC Admins PIM	-	-