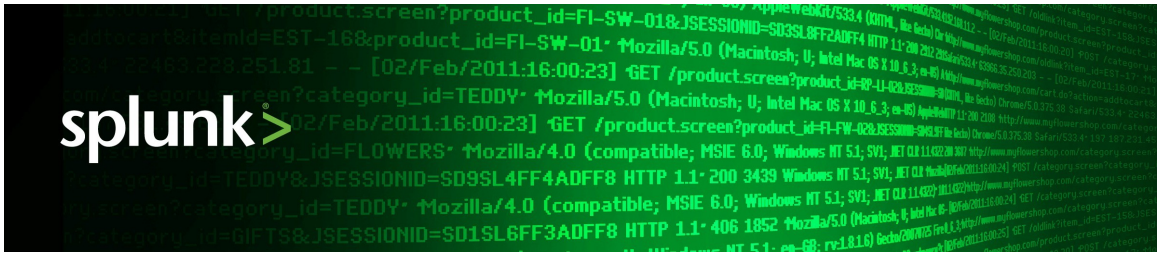

Splunk® Enterprise Installation Manual 7.1.0

Prepare your Windows network for an installation as a network or domain user

Generated: 5/18/2018 11:10 am

Prepare your Windows network for an installation as a network or domain user

You can prepare your Windows network to allow for Splunk Enterprise installation as a network or domain user other than the "Local System" user.

These instructions have been tested for Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, and might differ for other versions of Windows.

The rights you assign by using these instructions are the minimum rights that are necessary for a successful Splunk Enterprise installation. You might need to assign additional rights, either within the Local Security Policy or a Group Policy object (GPO), or to the user and group accounts that you create, for Splunk Enterprise to access the data you want.

Security requirements and ramifications of changing system defaults through Group Policy

This procedure requires full administrative access to the host or Active Directory domain you want to prepare for Splunk Enterprise operations. Do not attempt to perform this procedure without this access.

The low-level access requirements for Splunk Enterprise operations necessitate these changes if you want to run Splunk Enterprise as a user other than the Local System user. You must make changes to your Windows network to complete this procedure. Making these changes can present a significant security risk.

To mitigate the risk, you can prevent the user that Splunk Enterprise runs as from logging in interactively, and limit the number of machines from where the user can log in. Alternatively, on Windows Server 2008 R2 and later, you can set up managed user accounts (MSAs) that further limit risk.

If you are not comfortable with or do not understand the security risks that come with this procedure, then do not perform it.

Prepare Active Directory for Splunk installation as a domain user

Prepare your Active Directory for installations of Splunk Enterprise or the Splunk universal forwarder as a domain user.

To use PowerShell to configure your Active Directory for installation of Splunk Enterprise, see "Use PowerShell to configure your AD domain" later in this topic.

Prerequisites

You must meet the following requirements to perform this procedure:

- Your Windows environment runs Active Directory.
- You are a domain administrator for the AD domains that you want to configure.
- The installation hosts are members of this AD domain.

Create users

When you create users for running Splunk Enterprise, follow Microsoft best practices . See Microsoft Best Practices on MS TechNet.

1. Run the Active Directory Users and Computers tool by selecting **Start > Administrative Tools > Active Directory Users and Computers**.
2. Select the domain that you want to prepare for Splunk Enterprise operations.
3. Click **Action > New > User**
4. Enter the username for the new user and click **Next**.
5. Uncheck **User must change password at next logon**.
6. Click **Next**.
7. Click **Finish**.
8. (Optional) Repeat this procedure to create additional users.
9. (Optional) Quit Active Directory Users and Computers.

Create groups

This procedure creates the groups for users and machines that run Splunk Enterprise.

1. Run the Active Directory Users and Computers tool by selecting **Start > Administrative Tools > Active Directory Users and Computers**.
2. Select the domain that you want to prepare for Splunk Enterprise operations.
3. Double-click an existing container folder, or create an Organization Unit by selecting **New > Group** from the **Action** menu.

4. Select **Action > New > Group**.
5. Type a name that represents Splunk Enterprise user accounts, for example, Splunk Accounts.
6. Confirm that the **Group scope** is set to **Domain Local** and **Group type** is set to **Security**.
7. Click **OK** to create the group.
8. Create a second group and specify a name that represents Splunk Enterprise enabled computers, for example, Splunk Enabled Computers. This group contains computer accounts that receive permissions to run Splunk Enterprise as a domain user.
9. Confirm that the **Group scope** is **Domain Local** and the **Group type** is **Security**.

Assign users and computers to groups

This part of the procedure assigns users and computers that you created in the previous part.

1. Add the accounts to the **Splunk Accounts** group.
2. Add the computer accounts of the computers that will run Splunk Enterprise to the **Splunk Enabled Computers** group.
3. (Optional) Quit **Active Directory Users and Computers**.

Define a Group Policy object (GPO)

The Group Policy Object you create here will be distributed to all of the machines that run Splunk Enterprise. It assigns rights to the machines that make running Splunk Enterprise easier.

1. Run the **Group Policy Management Console (GPMC)** tool by selecting **Start > Administrative Tools > Group Policy Management**
2. In the tree view pane on the left, select **Domains**.
3. Click the **Group Policy Objects** folder.
4. In the **Group Policy Objects in <your domain>** folder, right-click and select **New**.
5. Type a name that describes the fact that the GPO will assign user rights to the servers you apply it to. For example, "Splunk Access."
6. Leave the **Source Starter GPO** field set to "(none)".
7. Click **OK** to save the GPO.
8. Remain in the GPMC. You will perform additional work there in the next section.

Add rights to the GPO

1. While still in the GPMC, right-click on the newly-created group policy object and select **Edit**.
2. In the **Group Policy Management Editor**, in the left pane, browse to **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment**.
    1. In the right pane, double-click on the **Act as part of the operating system** entry.
    2. In the window that opens, check the **Define these policy settings** checkbox.
    3. Click **Add User or Group?**
    4. In the dialog that opens, click **Browse?**
    5. In the **Select Users, Computers, Service Accounts, or Groups** dialog that opens, type in the name of the "Splunk Accounts" group you created earlier and click **Check Names?** Windows underlines the name if it is valid. Otherwise it tells you that it cannot find the object and prompts you for an object name again.
    6. Click OK to close the "Select Users?" dialog.
    7. Click OK again to close the "Add User or Group" dialog.
    8. Click OK again to close the rights properties dialog.
3. Repeat Steps 2a-2h for the following additional rights:
    - **Bypass traverse checking**
    - **Log on as a batch job**
    - **Log on as a service**
    - **Replace a process-level token**
4. Remain in the Group Policy Management Editor. You will perform additional work there in the next section.

Change Administrators group membership on each host

This procedure restricts who is a member of the Administrators group on the hosts to which you apply this GPO.

Confirm that all accounts that need access to the Administrators group on each host have been added to the Restricted Groups policy setting. Failure to do so can result in losing administrative access to the hosts on which you apply this GPO!

1. While still in the Group Policy Management Editor window, in the left pane, browse to **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups**.

1. In the right pane, right-click and select **Add Group?** in the pop-up menu that appears.
2. In the dialog that appears, type in **Administrators** and click OK.
3. In the properties dialog that appears, click the **Add** button next to **Members of this group:**.
4. In the **Add Member** dialog that appears, click **Browse?"**
5. In the **Select Users, Computers, Service Accounts, or Groups** dialog that opens, type in the name of the "Splunk Accounts" group you created earlier and click **Check Names?** Windows underlines the name if it is valid. Otherwise it tells you that it cannot find the object and prompts you for an object name again.
6. Click OK to close the **Select Users?** dialog.
7. Click OK again to close the "Add User or Group" dialog.
8. Click OK again to close the group properties dialog.

2. Repeat Steps 1a-1h for the following additional users or groups:
   - Domain Admins
   - any additional users who need to be a member of the Administrators group on every host to which you apply the GPO.
3. Close the Group Policy Management Editor window to save the GPO.
4. Remain in the GPMC. You will perform additional work there in the next section.

Restrict GPO application to select computers

This procedure controls which machines will actually receive the new GPO, and thus have their user rights assignments changed so that they can run Splunk Enterprise.

1. While still in the GPMC, in the GPMC left pane, select the GPO you created and added rights to, if it is not already selected. The GPMC displays information about the GPO in the right pane.
2. In the right pane, under **Security Filtering**, click **Add?**
3. In the **Select User, Computer, or Group** dialog that appears, type in "Splunk Enabled Computers" (or the name of the group that represents Splunk-enabled computers that you created earlier.)
4. Click **Check Names**. If the group is valid, Windows underlines the name. Otherwise, it tells you it cannot find the object and prompts you for an object name again.
5. Click OK to return to the GPO information window.
6. Repeat Steps 2-5 to add the "Splunk Accounts" group (the group that represents Splunk user accounts that you created earlier.)
7. Under **Security Filtering**, click the **Authenticated Users** entry to highlight it.

8. Click **Remove**. GPMC removes the "Authenticated Users" entry from the "Security Filtering" field, leaving only "Splunk Accounts" and "Splunk Enabled Computers."
9. Remain in the GPMC. You will perform additional work there in the next section.

Apply the GPO

Active Directory controls when Group Policy updates occur and GPOs get applied to hosts in the domain. Under normal circumstances, replication happens every 90-120 minutes. You must either wait this amount of time before attempting to install Splunk as a domain user, or force a Group Policy update by running `GPUPDATE /FORCE` from a command prompt on the host whose Group Policy you want to update.

1. While still in the GPMC, in the GPMC left pane, select the domain that you want to apply the GPO you created.
2. Right click on the domain, and select **Link an Existing GPO?** in the menu that pops up.

   If you only want the GPO to affect the OU that you created earlier, then select the OU instead and right-click to bring up the pop-up menu.
3. In the **Select GPO** dialog that appears, select the GPO you created and edited, and click **OK**. GPMC applies the GPO to the selected domain.
4. Close GPMC by selecting **File > Exit** from the GPMC menu.

Install Splunk with a managed system account

Alternatively, you can install Splunk Enterprise with a managed system account.

You can use the instructions in "Prepare your Active Directory to run Splunk Enterprise services as a domain account" earlier in this topic to assign the MSA the appropriate security policy rights and group memberships.

When you grant file permissions to the MSA after installation, you might need to break NTFS permission inheritance from parent directories above the Splunk Enterprise installation directory and explicitly assign permissions from that directory and all subdirectories.

Windows grants the "Log on as a service" right to the MSA automatically if you use the Services control panel to make changes to Splunk services.

1. Create and configure the MSA that you plan to use to monitor Windows data.
2. Install Splunk from the command line and use the `LAUNCHSPLUNK=0` flag to keep Splunk Enterprise from starting after installation has completed.
3. After installation completes, use the Windows Explorer or the `ICACLS` command line utility to grant the MSA "Full Control" permissions to the Splunk Enterprise installation directory and all its sub-directories.
4. Change the default user for the `splunkd` and `splunkweb` service accounts, as described in the topic Correct the user selected during Windows installation.

   You must append a dollar sign ($) to the end of the username when completing this step for the MSA to work. For example, if the MSA is `SPLUNKDOCS\splunk1`, then you must enter `SPLUNKDOCS\splunk1$` in the appropriate field in the properties dialog for the service. You must do this for both the `splunkd` and `splunkweb` services.
5. Confirm that the MSA has the "**Log on as a service**" right.
6. Start Splunk Enterprise. It runs as the MSA configured above, and has access to all data that the MSA has access to.

Use PowerShell to configure your AD domain

You can use PowerShell to configure your Active Directory environment for Splunk Enterprise services. This option is available when you do not want to use the GUI-based administrative applications.

Create the Splunk user account

1. Open a PowerShell window.
2. Import the ActiveDirectory PowerShell module, if needed:

```
> Import-Module ActiveDirectory
```

3. Create a new user:

```
> New-ADUser ?Name <user> `
-SamAccountName <user> `
-Description ?Splunk Service Account? `
-DisplayName ?Service:Splunk? `
-Path ?<organizational unit LDAP path>? `
-AccountPassword (Read-Host ?AsSecureString ?Account Password?) `
-CannotChangePassword $true `
-ChangePasswordAtLogon $false `
-PasswordNeverExpires $true `
-PasswordNotRequired $false `
-SmartcardLogonRequired $false `
```

```
-Enabled $true `
-LogonWorkstations ?<server>? `
```

In this example:

- The command creates an account whose password cannot be changed, is not forced to change after first logon, and does not expire.
- *<user>* is the name of the user you want to create.
- *<organizational unit LDAP path>* is the name of the OU in which to put the new user, specified in X.500 format, for example: `CN=Managed Service Accounts,DC=splk,DC=com`.
- *<server>* is a single host or comma-separated list which specifies the host(s) that the account can log in from.

The `LogonWorkstations` argument is not required, but lets you limit which workstations a managed service account can use to log into the domain.

Configure the Splunk Enterprise server

After you have configured a user account, use PowerShell to configure the server with the correct permissions for the account to run Splunk Enterprise.

This is an advanced procedure. Improper changes to your AD can render it unusable. Perform these steps only if you feel comfortable doing so and understand the ramifications of using them, including problems that can occur due to typos and improperly-formatted files.

In the following examples:

- *<user>* is the name of the user you created that will run Splunk Enterprise.
- *<domain>* is the domain in which the user resides.
- *<computer>* is the remote computer you want to connect to in order to make changes.

To configure local security policy from PowerShell:

1. Connect to the machine that you wish to configure.
   - If you use the local machine, log in and open a PowerShell prompt, if you have not already.
   - If you connect to a remote machine, create a new `PSSession` on the remote host, as shown in the following examples.

- You might need to disable Windows Firewall before you can make the remote connection. To do so, see Need to Disable Windows Firewall on MS TechNet (for versions of Windows Server up to Server 2008 R2, and Firewall with Advanced Security Administration with Windows PowerShell, also on MS TechNet.

```
> Enter-PSSession -Computername <computer>
```

2. Add the service account to the local Administrators group.

```
> $group = [ADSI]?WinNT://<server>/Administrators,group?
> $group.Add(?WinNT://<domain>/<user>?)
```

3. Create a backup file that contains the current state of user rights settings on the local machine.

```
> secedit /export /areas USER_RIGHTS /cfg OldUserRights.inf
```

4. Use the backup to create a new user rights information file that assigns the Splunk Enterprise user elevated rights when you import it.

```
> Get-Content OldUserRights.inf `
| Select-String ?Pattern `
?(SeTcbPrivilege|SeChangeNotify|SeBatchLogon|SeServiceLogon|SeAssignPrimaryToken|
`
| %{ ?$_,<domain>\<user>? }
| Out-File NewUserRights.inf
```

5. Create a header for the new policy information file and concatenate the header and the new information file together.

```
> ( ?[Unicode]?, ?Unicode=yes? ) | Out-File Header.inf
> ( ?[Version]?, ?signature=`?`$CHICAGO`$`??, ?Revision=1?) |
Out-File ?Append Header.inf
> ( ?[Privilege Rights]? ) | Out-File ?Append Header.inf
> Get-Content NewUserRights.inf | Out-File ?Append Header.inf
```

6. Review the policy information file to ensure that the header was properly written, and that the file has no syntax errors in it.
7. Import the file into the local security policy database on the host.

```
> secedit /import /cfg Header.inf /db C:\splunk-lsp.sdb
> secedit /configure /db C:\splunk-lsp.sdb
```

Prepare a local machine or non-AD network for Splunk Enterprise installation

If you do not use Active Directory, follow these instructions to give administrative access to the user you want Splunk Enterprise to run as on the hosts on which you want to install Splunk Enterprise.

1. Give the user Splunk Enterprise should run as administrator rights by adding the user to the local Administrators group.
2. Start Local Security Policy by selecting **Start > Administrative Tools > Local Security Policy**.
3. In the left pane, expand **Local Policies** and then click **User Rights Assignment**.
    1. In the right pane, double-click on the **Act as part of the operating system** entry.
    2. Click **Add User or Group?**
    3. Click **Browse?**
    4. Type in the name of the "Splunk Computers" group you created earlier, and click **Check Names...** Windows underlines the name if it is valid. Otherwise it tells you that it cannot find the object and prompts you for an object name again.
    5. Click **OK**.
    6. Click **OK**.
    7. Click **OK**.
4. Repeat Steps 3a-3g for the following additional rights:
    - **Bypass traverse checking**
    - **Log on as a batch job**
    - **Log on as a service**
    - **Replace a process-level token**

After you have completed these steps, you can then install Splunk Enterprise as the desired user.