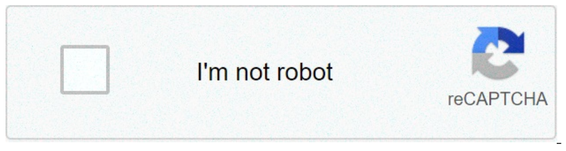

Continue

Perforce user guide

Perforce p4 user guide. Perforce swarm user guide. Perforce user guide pdf.

P4Admin tab in your opinia £ Perforce depot allows you to manage access write permissions to your project. You can create groups of Perforce usuÃ¡rios, set timeout off and edit the protections table.Navigate your space> Perforce Depot> P4Admin tab to manage groups and permissions.Creating usuÃ¡rios usuÃ¡rios GroupsAll with access Perforce the space is listed in the £ Ã ¢ usuÃ¡rios and seÃ§Ã £ ¢ the GroupsÃ. To create a new group click the Add Link + Ã ¢ ¢ GroupÃ: Then select the group name and Selecting the £ usuÃ¡rio users.Confirm Assign and click the button £ o Adda to create a usuÃ¡ river group.Manage in groupTo manage usuÃ¡rios within the selected group, click the ¢ Ã ¢ usersâ the Balkan £ next to the selected group name, and simply add or remove users.Set off timeoutsYou can set the end time-out Sessa the £ for each group, by clicking one timeoutÃ log ¢ next to the selected group. time to limit the £ Sessa can be set only for the group, and the individual £ users.Manage groups for usersYou Tamba © m can manage what groups sÃ £ o atribuÃdos the selected usuÃ¡rios. To do this, click the link group counter next to the usuÃ¡rio selected and select which groups the usuÃ¡rio should be part of.Manage Perforce depÃ³sito write permissions access tableThe £ seÃ§Ã the write permissions on P4Admin tab allows you write permissions to manage access to Top users and usuÃ¡rios groups. You can create access rules and gerenciÃ¡ them the protections table.Navigate your space> Perforce Depot> P4Admin> write permissions permission page.Creating the £ rulesTo create a new rule, click the button £ Ã ¢ o + Add write permissions ruleÃ ¢: you will be presented with a £ formulÃ¡rio of Creating the rule that allows you to define: Navel access, group or usuÃ¡rio, the path to the folder or file and £ observaÃ§Ã free to describe the rule if necessary. You can create rules vÃ¡rias to blend write permissions and set the dominant order that allows the most Creating £ avanÃ§ado combinations.Choose type levelSelect access access navel to the rule: write - Top users can send open filesOpen - Top users can open files to add, edit, delete and integrateRead - Top users can synchronize, diff, and print filesList - Top users can see the names, but in £ the contents of files; Top users can view all related metadata at the £ o-file (work spaces, usuÃ¡rios, changelists, jobs, etc.Review -. The permission granted to the special £ £ revision includes the daemons list and access reading, wing © m use the revision command £ P4 Ãºnico add comment daemons require this permission.No recording £ o -. in front of the access writeNo - usuÃ¡rios Cana t access allOnly read - If this right is denied, Top users £ nA can use the print £ P4, P4 diff, or synchronize P4 files.Only write - If this right is denied, Top users £ nA can send the open files.Read more about write permissions to access usuÃ¡rios or Guide.Select groups Perforce Server Administrator for Top users or groups ruleSelect this rule should apply to.Define the way to ruleFor each rule, you need to define the way the rule will be applied the path can include wildcards * - Matches all characters except bars within a ¢ directory.Ã | .. - Correspo node to all files in the directory of current job and all subdiretÃ³rios %% 1 - %% 9 - positional specifiers. for subsequÃªncia rearrangement FILENAM es when used in views.For example: usuÃ¡rio recording of the £ * / ... read Emily user group /elm_proj/%%1.%%2list DevOps /...list lisag user / constrÃ³i / * / user helpwrite lisag / elm_proj / doc / ... Read more in Guide and Perforce rules file Specifications.Set UsuÃ¡rio P4Admin orderYou Tamba © m can select what posiÃ§Ã £ on the list rule should be clicking the arrow correct buttons UPA and Ã ¢ downa. This allows the £ aplicaÃ§Ã the rules in the correct order to alcanÃ§ar more complex configurations.Simply click the The submit ¢ to create a new rule or apply changes to an existing already. If any of the rule conditions are not correct, you will see an error message. Edit or Remove an existing Ruleyou already can edit any of the existing rules by clicking the Edit Edit Icon or Removing it completely using the Ã ¢ trashcanÃ ¢ ¢ button button.if you have any doubts or need our help, Do not hesitate to contact us at support@assembla.com. Lice HÃ © Lice Service support for Core Helix clients and Helix Core clients, such as P4V, requires an extension of Helix Core Server. This extension, such as Node.js authentication service, can be run on Linux systems with enhanced SELINUX (SELinux) Linux enabled and in the execution mode. If you choose to activate the enhanced Security Linux (SELinux), the extension is performed in the run mode. For information about the extensions of Helix Core Server, see the Developer's Guide Extensions of the Extensions. Preme - Rechositos support the Helix authentication service setting to work with the Identity Provider (IDP) and the Perforce Server product requires an experienced security administrator. This effort may require performing support assistance. Preparing for installation before installing the extension of authentication, there are some steps to be taken. Update customers that are useful so that the final users have upgraded HELIX clients. Updated customers direct the user to the web browser during login progress. Older customers can print only the URL on the screen and do not open the browser automatically. See the Readme.md file for the list of supported customer versions. Testing the extension to test the extension with a limited set of users, before activating the SSO for all users, you can set the SSO-users or SSO-group configurations, as described in the test section below. With any of these configurations, only users listed in SSO users or are members of one of the groups listed in SSO groups, are authenticated using the extension. After the appropriate operation of the extension has been established, you can clear these settings to activate SSO for all users. Deleting some SSO users see the below-mentioned section allowing non-SSO users for details. It is recommended to have at least one administrative user called between non-SSO users. Administrative users should use a database password to avoid being blocked in the case that the SSO mechanism is not operational (for example, the identity provider is temporarily inaccessible). Installing Extension The extension can be installed using the configuration script provided or manually for non-system supported by the script. This section will describe how to use the configuration script, while the manual installation section describes the detailed steps for the construction, installation and Configuration of extension. In both assisted procedures and install manuals, the last step will involve restarting the Helix Core server. Configuration Script The configuration script is a Linux-based bash script named Configure-Login-hook.sh in the BIN directory. As the script requires a Linux system, it does not support the installation of a Windows system. Helix Core Server may be in execution on a Windows system, but the configuration script must be run from a Linux system. The script can run without requesting input by providing all the required command-line options, including -n to signal the script to run not interactively. When you run without options, the script requests the required information. The script will use the information provided to create, install and configure the extension. It will also restart the Helix Core server, if given the permission to do so. Invoke the script with the --help option to learn the details of the options and use of the script. Manual Installation Building Extension If you already have the LoginOk.p4 extension file, you will go for the installation section. If you want to create the LoginOK extension in the source code, open a terminal window and issue the following command: $ P4 extension - Package LoginOK The result will be a zip file named loginok.p4-extension installing the extension To install the extension, run the following command in Terminal Window: $ P4 Extension - LoginOK.p4-Extension -y Extension 'Auth :: Loginhook # 1.0' Installed successfully. If this is not the first time you are installing installing Extension, remove the existing extension before reinstalling it. See the removal of the extension. Configuring the extension the extension is configured both on the global level and on the level of the instance. To learn about these levels, refer to the topical "Extension Configuration of the Server (Global and Instance Specifications)" in the History Developer's Developer's Guide. The extension has specific configurations for the global and instance configuration as described below. Both the global and instance configuration is defined using pierce forms, in which fields consist of a label, a cholon, a tab character and a value. Fields that allow several values to start in a new line, with each value in a separate row and all lines are prefixed by a tab character. Within the Estrconfig section, the field rotles are prefixed by a character of a tab and values are started in a new line and are prefixed with two tab characters. Specific for this extension, any value that begins with ... It means that the value is left indefinite and the standard behavior will come into effect if any. By setting a value for a configuration, remove the ... and all that follows in this line and insert the desired value. Global Initio When defining the overall extension extension setting: $ P4 Extension - Confinfigure Auth :: LoginOK [Snip] Extp4User: SampleExtensionSususer EXTCONFIG: Authentication protocol: ... Protocol Authentication, SAML or OIDC. Authority-Cert: ... Path to Public Key Certification Authority, Patterns for ./ca.crt Cert: ... Path to the Public Key Client, Patterns for ./client.crt Client Key : ... Path to Private Customer Key, Patterns for ./client.key Service-URL: ... The URL of the authentication service base. Check-preer: ... Make sure the service certificate is true if "true". Verify that: ... Make sure that the name of the service host matches the certificate, if "true". Where [Snip] means that some information has been omitted. The first field to change is Extp4User, which must be the user of the perforce that will have this extension, usually a "super" or administrative user. Of the configurations in EXTCONFIG, only the SERVICE-URL configuration is required. The other configurations have standard values as described below. Global Settings Name Description Auth-protocol can be any value supported by the authentication service. This determines the authentication protocol for SSO users to authenticate. This setting is optional because the authentication service will use your own configurations to determine the protocol. Patterns for any authentication service decide. Cert Authority Path for the Public Key of the Certificate Authority. See section certificates for more information. Standards for the CA.CRT file in the extension directory. Cert Client Path for the Public Key of the Extension Customer Certificate. See section certificates for more information. Patterns for the client.crt file in the extension directory. Client key path for the Private Key of the Extension Client Certificate. See section certificates for more information. Standards for the client.key file in the extension directory. Service-URL The address of the authentication service by which the Helix server can make a connection no verify-peer if set to true, then the extension will check if the Authentication service is using a SSL / TLS cable certificate. FALSE VERIRIFY-HOST If set to True, then the extension will check if the host name of the Authentication Service matches the SSL / TLS certificate returned by the service. False example In this example below, each level of indentation represents a single tab character. Rotters are prefixed with a character of a tab and values are all with two tab characters. [Snip] EXTP4User: SUPER EXTCONFIG: AUTH-PROTOCOL PROTOCOL: SAML AUTHORITY-CERT: /etc/ssl/trusted-ca.crt Certifier: /p4/1/ssl/loginhook-client.crt Key: / p4 / 1 / SSL / loginOK-client.key service-url: Verify-peer: ... Make sure the service certificate is true if " real". Verify-Host: ... Make sure your service name matches service if it's true'. Instance to set up a single instance of the extension, include the --name option along with the --configure option. This example uses loginOk-a1 only as an example; You are free to use a more descriptive name. P4 Extension - CumPrigure Auth :: LoginOK - Name LoginOK-A1 -O [snip] Exconfig: Enable-log: ... The extension will write debugging messages to a log if "true". Name identifier: ... field within the IDP response containing unique user identifier. Nao-sso-groups: ... These groups whose members will not be using SSO. User-sso: ... the users who will not be using SSO. SSO-groups: ... These groups whose members should authenticate using SSO. SSO-Users: ... those users who should authenticate using SSO. User-Identifier: ... variable trigger used as the exclusive user identifier. Where [Snip] means that some information has been omitted. All these settings have sensitive patterns. However, for the extension to be activated, we must configure it. You may want to change the non-SSO-group or not-ssos fields for a list of perforce and users who are not participating in the integration of SSO authentication . Instance Settings Name Description The unimpressive extension of activity of the activation will write debugging messages to a log if true false nao-sso -Groups of these groups that will not use SSO. This is a field of several values, with each value, starting in a new line and prefixed by two tab characters. No non-SSO-users can not be using SSO. This is a field of several values, with each value, starting in a new line and prefixed by two tab characters. No SSO-groups These groups whose members should authenticate using SSO. If this field is set to the name one or more groups, the NO-SSOS-groups field will be ignored. See the test section below. This is a field of several values, with each value, starting in a new line and prefixed by two tab characters. No SSO-Users these users who should authenticate using SSO. If this field is set to the name one or more users, the NO-SSO User field will be ignored. See the test section below. This is a field of several values, with each value, starting in a new line and prefixed by two tab characters. None User-Identifier Variable Trigger used as unique user identifier, one of: FullName, e-mail or user. E-mail name identifier field in the user profile of the identity provider containing unique user identifier. E-mail example In this example below, each level of indentation represents a single tab character. Rotters are prefixed with a character of a tab and values are all prefixed with two tab characters. [Snip] EXTCONFIG: Enable-log: True name-identifier: Name Não-SSO-groups: Admins SUPERS SSO-User: Bruno Ssusan SSO-groups: ... (none) SSOUS: ... (None)) User identifier: Send several instance configurations The extension is not designed to support several instance configurations. To find out which settings have been set, use the P4 Extension -List command as well: $ P4 Extension --List --Type Configs ... Foobar Config ... Extension Auth :: LoginOk ... UUID 117E9283- 732B -45A6-9993-ae64c354f1c5 ... Review 1 ... Super owner ... type auth-check-sso ... arg auth ... config foobar ... extension auth :: loginhook ... uuid 117E9283-732b -45a6-9993-ae64c354f1c5 ... Review 1 ... super ... type auth-pre-sso ... arg auth ... config loginhook ... extension Auth :: loginhook ... uuid 117e9283-732b -45a6-9993-ae64c354f1c5 ... Review 1 ... Super Owner ... Type Global-Extcfg ... Config logoSOK-ALL ... extension the auth :: loginhook ... uuid 117e9283-732b-45a6-9993- ae64c354f1c5 ... Review 1 ... super ... type auth-check-sso Arg auth ... config loginok-all ... extension auth :: loginhook ... uuid 117e9283-732b-45A6- 9993-ae64c354f1c5 ... Review 1 ... Super Owner ... Type AUTH-PRE-SSO ... Arg Auth of the example Sample above, we see two instances set up rations, one of which is named Foobar. To remove this strange setting, use the P4 Extension - Delete Delete As shown in the example below: $ p4 extension --delete Auth :: loginhook - name foobar would erase extension 'auth :: loginhook # 1, foobar'. This was the report mode. Use -y to run the operation. $ Extension P4 --Delete Auth :: loginhook - Name foobar -y extension 'Auth :: loginhook # 1, foobar' erased successfully. This command will remove the named instance setting, leaving the other configurations and the extension itself. Applying the changes After installing and configuring the authentication extension, the Normal Helix server must be restarted so that the changes have effect. Reinitium is required because Helix Node prepares the authentication mechanisms during initialization. This is true when adding or removing auth- related triggers as well as installing or removing the loginOK extension. Next steps tests for the purpose of testing the authentication integration with a limited number of users, you can change the SSO field to users a list of perforce users who must Authenticate using the SSO authentication integration. When this value is configured with one or more users, then the non-SSO-users and non-SSO-group lists will be ignored by the extension. Likewise, users are not included in this list will not be authenticated using the extension. To clear the SSO User field, replace the list of users with ... to indicate that the field is to be ignored. When the SSO user field begins with ... then no-SSO-users and non-SSO-groups fields will be considered by extension during authentication that of the user. Similar to the SSO User field is the field-group SSO, in which Perforce group names are given. All users who are members of any of the named groups will be required to authenticate using the integration of SSO authentication. When this value is configured with one or more groups, then the non-SSO-groups and non-SSO-user lists will be ignored by the extension. Likewise, users who are not members of any of the groups will not be authenticated using the extension. To clear the SSO group field, replace the list of groups with ... to indicate that the field is to be ignored. When field groups begin with ... then no-sso-groups and non-SSO-users are considered by the extension during authentication of user. The debug registration when enabled, the extension writes debugs logs to a formatted JSON file that will appear in the directory identified by the DATA-dir extension attribute. You can find the value for data-dir by searching the installed extensions using P4 extension as a privileged user. $ Extension P4 --List --TYPE = Extensions ... extensions Auth :: Loginhook ... [Snip] ... Data-dir Server.Extensions.dir / 117E9283-732b-45A6-9993-ae64c354f1c5 / 1-dice where [snip] means some information has been omitted. User profile mapping for user specifications Perforce User Helix has several fields that can be used - correspondence with the information of the returned profile of the identity provider . The extension uses the variables â €