Configuring user Access Control for Virtualize Servers

This topic explains how to configure and work with user access controls that govern what actions each user can perform on the Virtualize Servers connected to his or her Virtualize Desktop installation. Sections include:

Note that this topic does not cover security access controls in the virtual assets or message proxies that are accessed by the application under test (AUT). That is addressed in Configuring for Services Deployed Over HTTPS.

About Virtualize Server User Access Control

User access control allows you to control what actions each user can perform on the Virtualize Servers connected to his or her Virtualize Desktop installation. This allows you to determine which users can view, provision, create, modify, delete, and deploy assets. For example, you can control which users can start and stop proxy recording, modify and activate data groups and performance profiles, create and modify message proxies, use JDBC controllers, and so forth.

Authentication

When user access control is in effect, a user must provide credentials when adding a remote Virtualize Server to his or her Virtualize desktop. Once the user is authenticated, he can perform only the operations that are allowed for his or her assigned role.

Roles

Available roles are *Admin, System*, and *Provision*. These roles are configured in CTP. They also control access to CTP operations.

In general:

- **Unspecified** (i.e., the user is authenticated, but not assigned a role via CTP): Users can view and monitor assets, but not provision, create, modify, delete, or deploy them. This is read-only access.
- **Provision**: Users can view and monitor assets as well as provision assets (e.g., change proxy configurations, performance profiles, and data groups).
- **System** and **Admin**: Users can view, monitor, provision, create, modify, delete, and deploy assets. This is full access. Note that both of these roles grant the same permissions on Virtualize Desktop; on CTP, the *Admin* role provides additional permissions (e.g., creating and configuring user accounts).

For a more detailed breakdown of the actions allowed for each role, see Understanding Role-Based Permissions.

How it Works: Details

Virtualize Server user access control takes effect whenever the server is configured to connect to a CTP installation. If such a connection is configured and user authentication succeeds, the user will be granted the appropriate level of access. If such a connection is configured but user authentication fails (e.g., because valid credentials were not supplied or because the Virtualize-CTP connection failed), the user will not be granted any access—even read-only access—to the Virtualize Server.

If any resource restrictions are specified in CTP, the same restrictions will be applied to operations performed from the Virtualize desktop. For example, assume that CTP restricts a certain Virtualize Server to only a small subset of users. In this case, only users who have access to that Virtualize Server AND have *Admin* or *System* roles will be able to create, modify, delete, and deploy assets on that server.

If a Virtualize Sever is not configured to connect to CTP, all users will have full access to all available operations and assets.

Virtualize Server caches access control roles for the credentials it receives from Virtualize Desktop with a lifespan of 1 minute. This means that if a role /user is modified in CTP, it can take up to a minute for the new access controls to be enforced by Virtualize Server. Also, due to caching on Virtualize Desktop, it can take up to a minute for connected Virtualize Desktops to update access control labels, enable right-click menu options, and enable controls within editors.

How it Works: Summary

CTP (EM)	Virtualize Server
Virtualize Server not configured to connect to EM	Full access
Admin role + successful EM authentication	Full access
System role + successful EM authentication	Full access
Provision role + successful EM authentication	Provision-only access

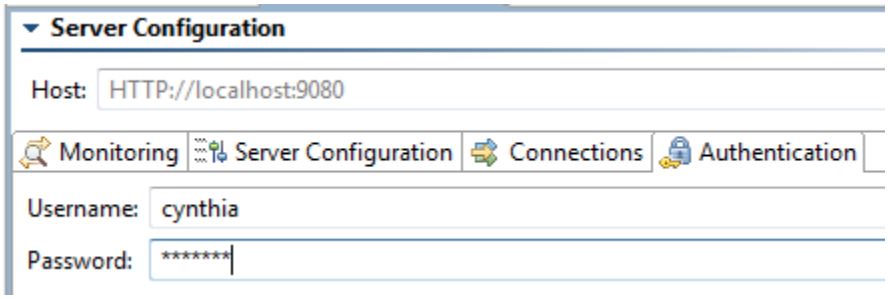
No assigned role + successful EM authentication	Read-only access
Unauthenticated (EM authentication failed)	No access
No credentials provided + Virtualize Server is configured to connect to EM	No access
Virtualize Server configured to connect to EM, but connection fails	No access
EM restricts access to the Virtualize Server	Access only for the selected list of users, based on their role. All other authenticated users have read-only access to that restricted resource
EM does not restrict access to the Virtualize Server	[Based on user role]

Migrating from Virtualize 9.5 or Earlier

If Virtualize Server 9.5 or earlier was configured to connect to CTP, then upgrading to Virtualize 9.6 or later will result in User Access Control being enabled on that server. Full access to the server will become restricted as a result of the upgrade.

To regain Virtualize Desktop access to an upgraded Virtualize Server:

1. Ensure that the desired roles and access controls for that server are configured in CTP.
2. For each Virtualize Desktop previously-connected to the Virtualize Server, re-connect with authentication (i.e., double-click the existing remote server node in the Virtualize Server view, specify a valid username/password, then save the Server Configuration editor)



Configuring User Access Controls for a Virtualize Server

To configure user access controls for a Virtualize Server:

1. Connect the Virtualize Server to CTP via **Preferences> CTP**. See CTP Settings for details.

   > **HTTPS Note**
   >
   > If CTP is deployed over an HTTPS connection (recommended), the Virtualize Server's CTP connection settings should use an HTTPS URL. This will ensure that the Virtualize Server will communicate with CTP securely over SSL.
   >
   > If the SSL certificate that CTP is configured with is not trusted by Virtualize Server (e.g., if it is self-signed), you will need to configure the Virtualize Server to trust all certificates—or add that particular CTP certificate to the Virtualize default Java cacerts file and select that option. This can be config-ured in the Preferences> Security settings (as described in Security Settings).

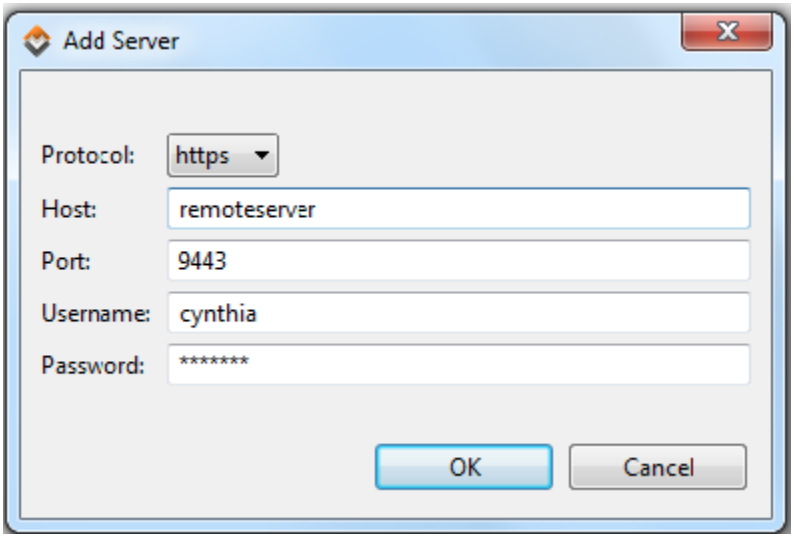
2. If you have not already done so, use CTP to configure user accounts and permissions. For details, see the CTP User's Guide.

Working with User Access Control

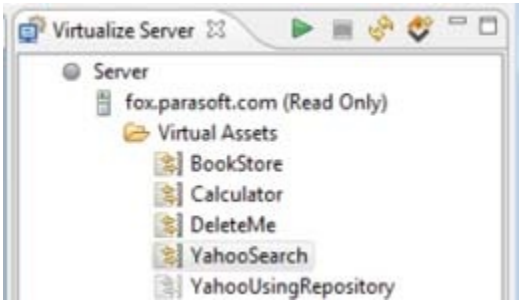
The following sections explains how Virtualize Server user access control impacts Virtualize Desktop users.

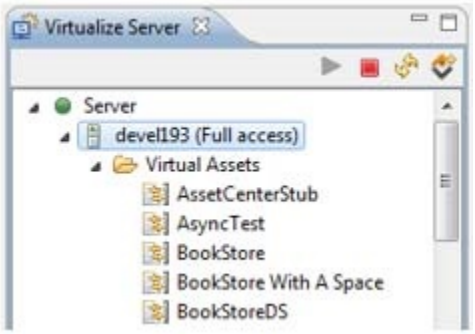
Adding a Remote Server

When adding a remote server, users need to enter a valid username and password in the Add Server dialog.

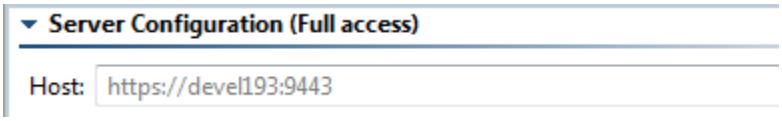


Note that access levels (Read Only, Full Access, Provision Only) will be indicated with labels in the Virtualize Server view. For example:



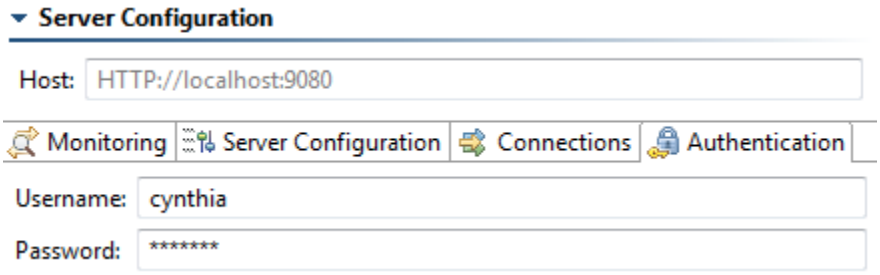


Additionally, access levels will be indicated in the server configuration page:



Re-Entering Credentials for an Existing Server

If users need to re-enter credentials (e.g., if their roles were changed via CTP), they can provide this data in the Virtualize Server's Authentication tab:



Understanding Role-Based Permissions

The following table is designed to help you understand which capabilities are associated with the available roles:

Capability	Full Access (Server /Admin)	Provision-Only Access	Read-Only Access
View assets (virtual assets, proxies, files)	X	X	X
Start/stop monitoring	X	X	X
Enable/disable assets	X	X	
Configure JDBC Controller settings	X	X	
Change Parasoft JDBC Driver modes	X	X	
Start/stop recording	X	X	
Change active data groups	X	X	
Change active performance profiles	X	X	
Modify settings in the server's configuration panel (Monitoring, Server Configuration, Connections, etc.)	X		
Refresh a server	X		
Add assets	X		
Delete assets	X		
Re-deploy all assets	X		