



App Orchestration 2.0

Credentials Used in the App Orchestration Environment

Prepared by: Andy Zhu

Version: 1.0

Last Updated: December 9, 2013

Contents

Overview	3
App Orchestration configuration server installation/configuration credentials	3
Shared resource domain credentials	5
Shared user domain credentials	8
Migrated tenant resource domain credentials	9
Migrated tenant user domain credentials	10
Delivery Site credentials for the shared resource domain	11
Delivery Site credentials for the tenant resource domain	14
Delivery Site database creation credentials (XenDesktop)	16
Delivery Site database creation credentials (XenApp)	17
Citrix Product Depot access credentials	18
Product installation credentials	19

Overview

In a typical App Orchestration deployment, many different credentials are involved. There are the credentials used to install and configure the App Orchestration configuration server and the credentials used to migrate a Delivery Site into the App Orchestration environment. You could simply use a domain administrator account for all the credentials required in your App Orchestration deployment. However, as part of security best practice, we recommend you use the least privileged account necessary to perform each action.

App Orchestration requires credentials for the following operations.

- Installing and configuring the App Orchestration configuration server.
- Managing the shared resource domain and the tenant resource domain.
- Creating, migrating, and managing Delivery Sites.
- Creating Delivery Site databases.
- Accessing the Citrix Product Depot.
- Installing software on machines.

This document lists, for each set of credentials, the stage at which the credentials are introduced into the App Orchestration deployment process and the actions they are used to perform. In addition, recommendations on the minimum permissions required for each of these credentials are given.

App Orchestration configuration server installation/configuration credentials

Where specified

You use this domain account to log on to the App Orchestration configuration server locally to perform the installation and configuration.

Actions performed using these credentials

This account is used for the following functions.

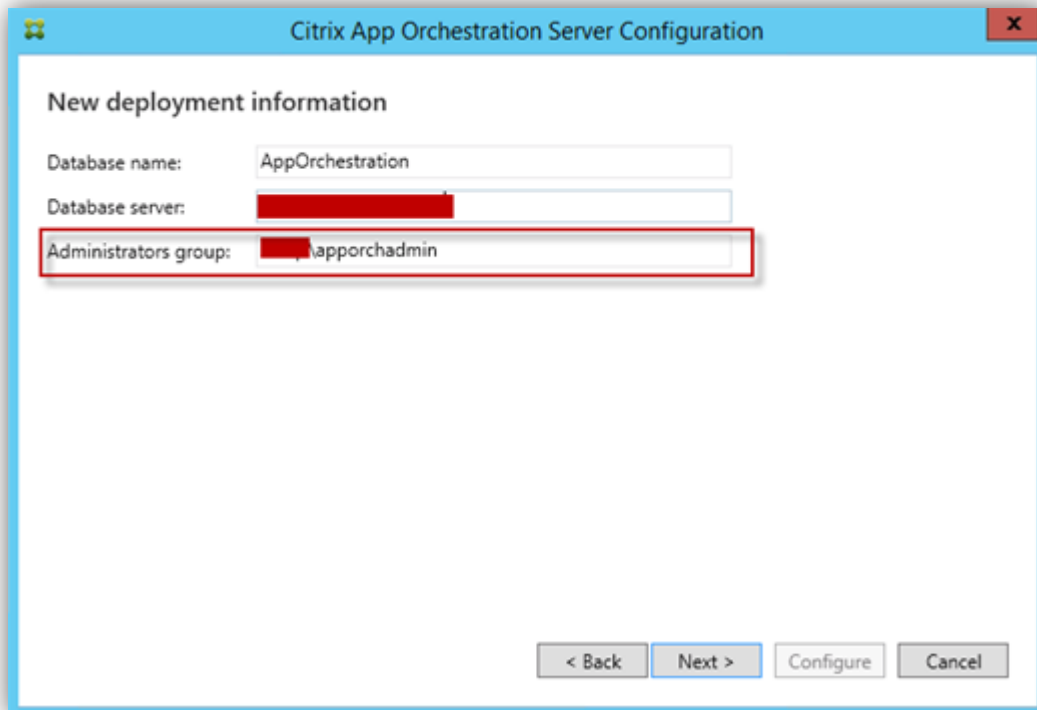
- Installing the App Orchestration configuration server binaries.
- Configuring the App Orchestration configuration server and creating the required Microsoft Internet Information Services (IIS) website.
- Reading the pre-installed SSL certificate so that it can be enabled on the IIS website.
- Creating the App Orchestration configuration server machine account on the database server so that the App Orchestration configuration server can communicate with the App Orchestration database.
- Creating the App Orchestration database on the database server.

Minimum permissions

Ensure that the account you use has the following permissions.

- Membership of the local administrators group on the App Orchestration configuration server.
- Membership of the domain group which acts as the administrators group for the App Orchestration deployment.

This administrators group must be specified when you first configure the App Orchestration configuration server and must be created before you run the Citrix App Orchestration Server Configuration wizard.



The screenshot shows a window titled "Citrix App Orchestration Server Configuration" with a close button (X) in the top right corner. The window contains a section titled "New deployment information" with three input fields: "Database name:" containing "AppOrchestration", "Database server:" containing a redacted value, and "Administrators group:" containing "apporchadmin". The "Administrators group" field is highlighted with a red rectangular border. At the bottom of the window, there are four buttons: "< Back", "Next >", "Configure", and "Cancel".

- Membership of the system administrator group on the App Orchestration database server.

Shared resource domain credentials

Where specified

You specify this domain administrator account during initial configuration of App Orchestration.

Global Settings

Domain Settings

Shared resource domain
Contains machines that host resources for multiple tenants. This is the primary and default resource domain.

Shared resource domain: [REDACTED] [Edit](#)
Once saved, this field cannot be changed.

Root OU:
This OU must already exist in Active Directory.

User name:
The orchestration service account for this domain. Requires elevated domain permissions.

Password:

Orchestration service group:

After initial configuration, you can update the shared resource domain credentials on the **Edit Domain** screen of the App Orchestration web management console.

Edit Domain

General

Credentials

Domain Credential

Update domain administrator credential

Domain administrator username:

Domain administrator password:

Product Installation Credential ⓘ

This domain has been previously configured with product install credentials.

Update product installation credentials

Product install administrator username:

Product install administrator password:

Actions performed using these credentials

This account is used for the following functions.

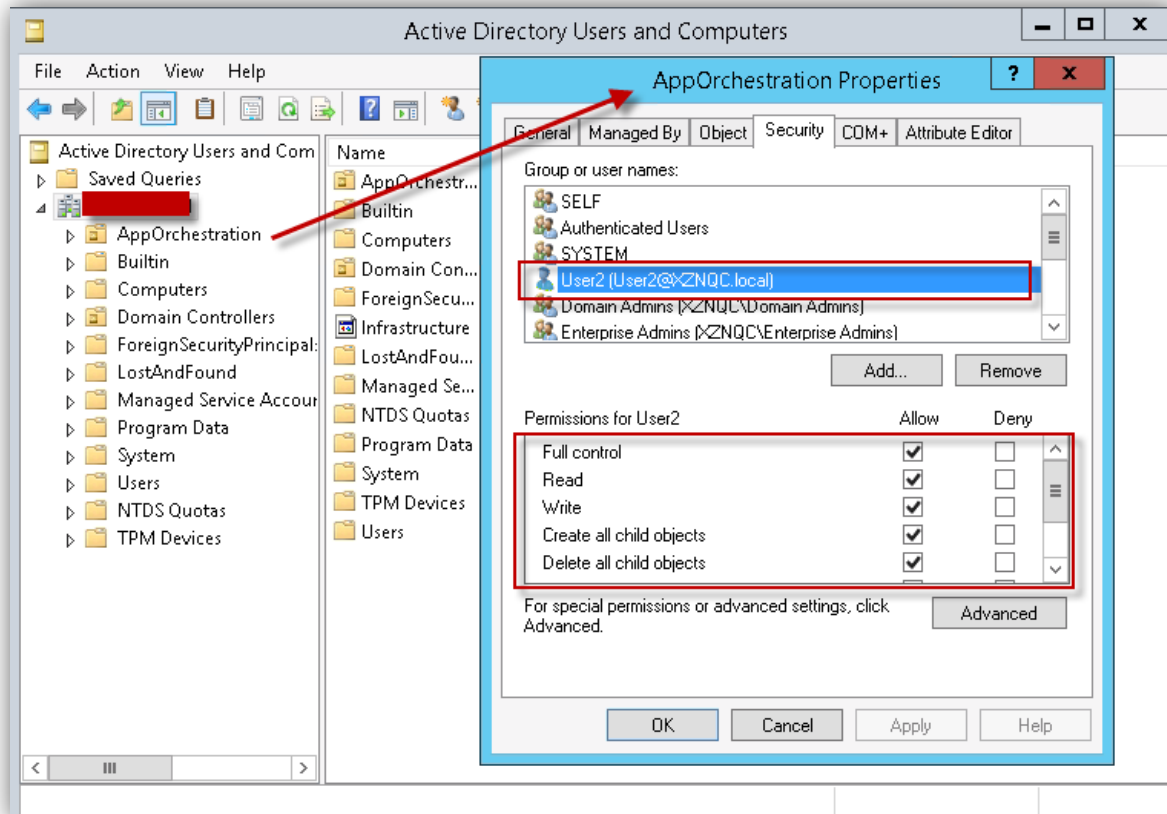
- Microsoft Active Directory organizational unit (OU) operations:
 - Verifying that the App Orchestration root OU exists.
 - Creating the DecommissionedServers OU after initial configuration of App Orchestration global settings.
 - Creating all necessary OUs during subscription creation operations.
- Machine operations:
 - Moving Delivery Controllers to the correct OU.
 - Moving Session Machines to the correct Delivery Group OU.
- User verification (if the shared user domain is the same as the shared resource domain):
 - Verifying that the specified user group exists during subscription.
 - Verifying that the specified groups are user groups and not just users.
 - Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.
- Creating the compute resources to support integrated provisioning.
- Remotely accessing the base VM to create the integrated provisioning template.

Minimum permissions

Ensure that the account you use has the following permissions.

- **Full control** permissions for the App Orchestration root OU.

You define the root OU during initial configuration of App Orchestration and it must exist in the shared resource domain before starting initial configuration.



- Membership of the orchestration service group.

Global Settings

Domain Settings

Shared resource domain
Contains machines that host resources for multiple tenants. This is the primary and default resource domain.

Shared resource domain: [REDACTED] [Edit](#)
Once saved, this field cannot be changed.

Root OU:
This OU must already exist in Active Directory.

User name:
The orchestration service account for this domain. Requires elevated domain permissions.

Password:

Orchestration service group:

Member of

- Membership of the local administrators group on the App Orchestration configuration server.
- Membership of the local administrators group on the integrated provisioning base VM.

Shared user domain credentials

Where specified

As with the shared resource domain credentials, you specify this account during initial configuration of App Orchestration and can update the credentials on the **Edit Domain** screen of the App Orchestration web management console.

Actions performed using these credentials

This account is used for the following functions.

- Verifying that the specified user group exists during subscription.
- Verifying that the specified groups are user groups and not just users.
- Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.

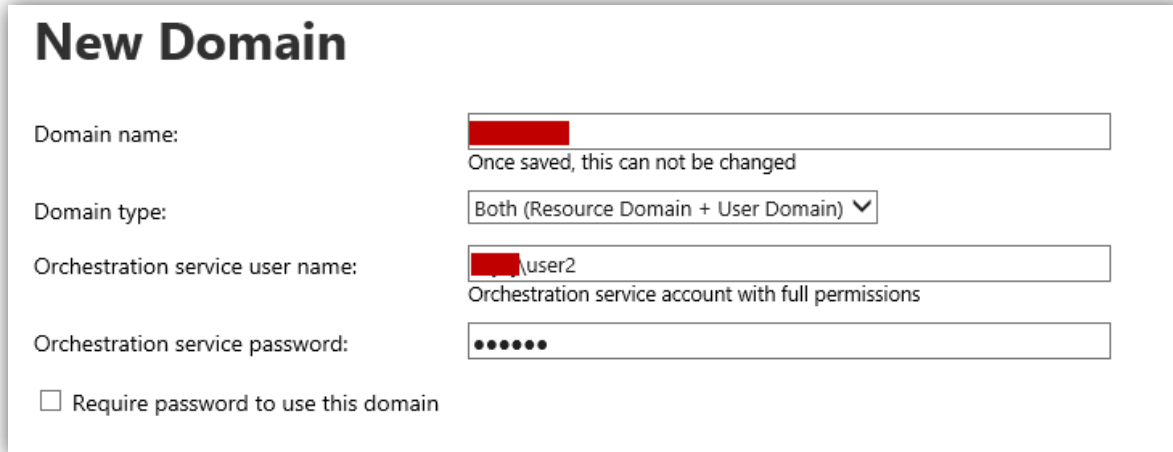
Minimum permissions

Ensure that the account you use has read permissions on the Active Directory deployment.

Migrated tenant resource domain credentials

Where specified

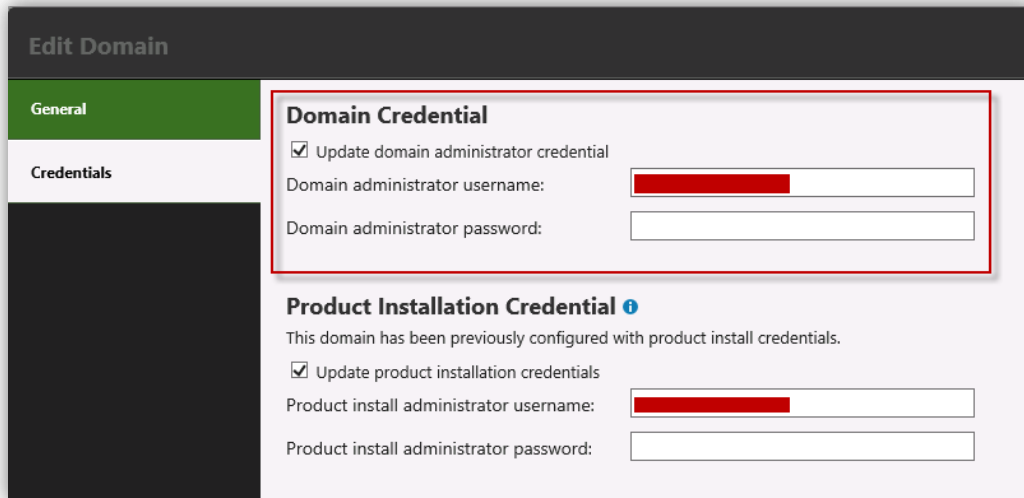
You specify these credentials when you create a new domain.



The 'New Domain' form contains the following fields:

- Domain name:** A text input field with a redacted value. Below it, the text reads: "Once saved, this can not be changed".
- Domain type:** A dropdown menu with the selected option: "Both (Resource Domain + User Domain)".
- Orchestration service user name:** A text input field with the value: "user2". Below it, the text reads: "Orchestration service account with full permissions".
- Orchestration service password:** A password input field with six dots representing the masked password.
- Require password to use this domain

You can update the migrated tenant resource domain credentials on the **Edit Domain** screen of the App Orchestration web management console.



The 'Edit Domain' console shows two sections:

- Domain Credential** (highlighted with a red border):
 - Update domain administrator credential
 - Domain administrator username: [Redacted]
 - Domain administrator password: [Empty]
- Product Installation Credential** ⓘ
 - This domain has been previously configured with product install credentials.
 - Update product installation credentials
 - Product install administrator username: [Redacted]
 - Product install administrator password: [Empty]

Actions performed using these credentials

This account is used for the following functions.

- OU operations:
 - Verifying that the App Orchestration root OU exists.
 - Creating all necessary OUs during subscription creation operations.
- Machine operations:
 - Moving Delivery Controllers to the correct OU.
 - Moving Session Machines to the correct Delivery Group OU.

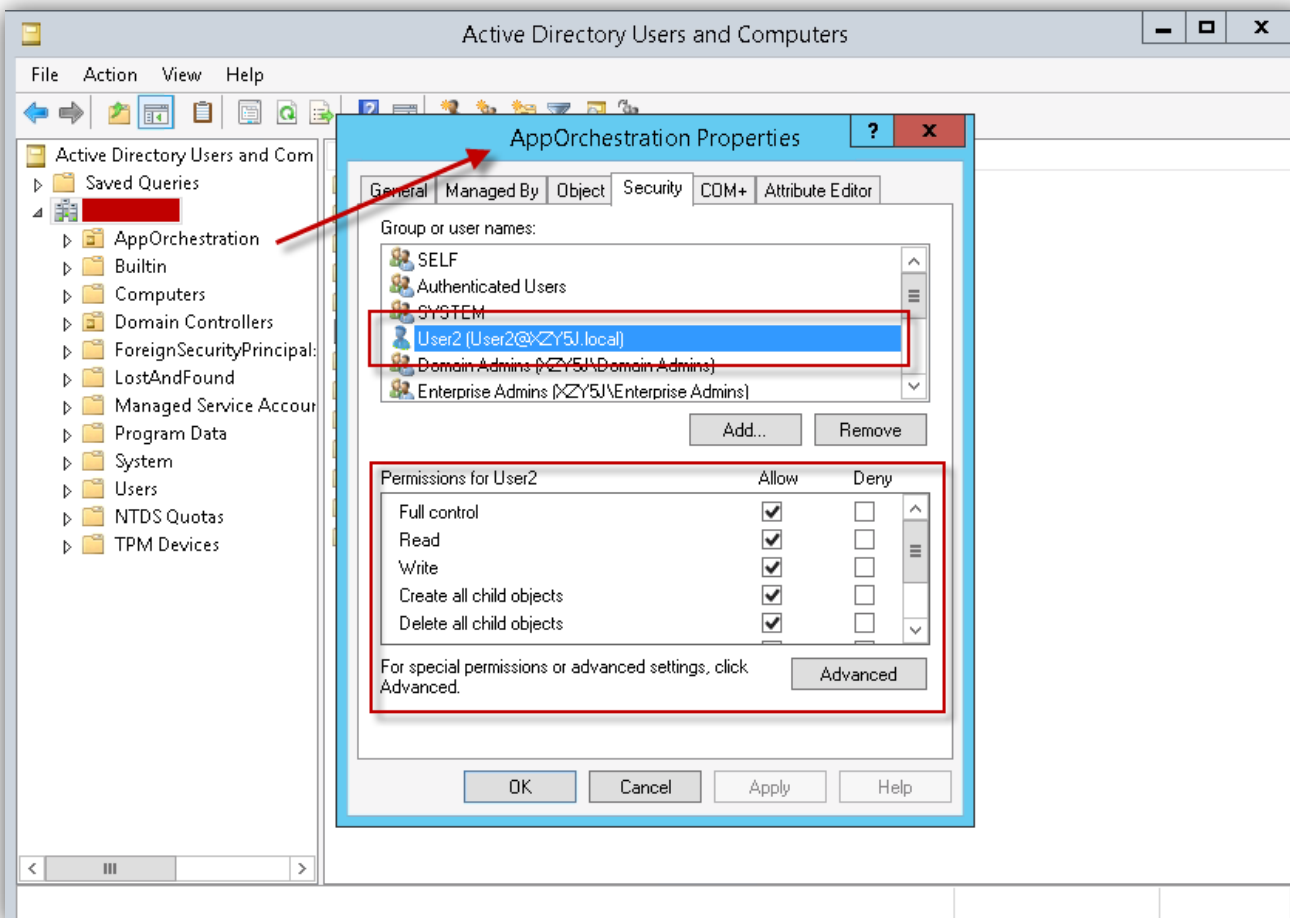
App Orchestration 2.0: Credentials Used in the App Orchestration Environment

- User verification (if the tenant user domain is the same as the tenant resource domain):
 - Verifying that the specified user group exists during subscription.
 - Verifying that the specified groups are user groups and not just users.
 - Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.

Minimum permissions

Ensure that the account you use has **Full control** permissions for the App Orchestration root OU.

You must create the root OU in the tenant resource domain before you migrate the domain to the App Orchestration environment.



Migrated tenant user domain credentials

Where specified

As with the migrated tenant resource domain credentials, you specify this account when you create a new domain and can update the credentials on the **Edit Domain** screen of the App Orchestration web management console.

Actions performed using these credentials

This account is used for the following functions if the tenant user domain is the same as the tenant resource domain.

- Verifying that the specified user group exists during subscription.
- Verifying that the specified groups are user groups and not just users.
- Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.

Minimum permissions

Ensure that the account you use has read permissions on the Active Directory deployment.

Delivery Site credentials for the shared resource domain

Where specified

You specify these credentials when you create a Delivery Site.

Location Settings

Machine Name(s):

+

A minimum of 2 machine names are required. Additional can be added if desired.

Network:

Domain:

Datacenter: ▾

Delivery Site Admin Group:

User name:

Install administrator

Password:

Actions performed using these credentials

This account is used for the following functions.

- Installing Delivery Controllers.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the shared resource domain or tenant resource domain so that the Session Machine can be joined to the Delivery Site.
- Verifying users when hosted applications are created.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the shared resource domain or tenant resource domain so that the Session Machine can be removed from the Delivery Site.
- Group Policy operations:
 - Creating the license server Group Policy Object.
 - Linking the license server Group Policy to the App Orchestration OU.
 - Creating the Delivery Controller Group Policy.
 - Linking the Delivery Controller Group Policy to a specific workload/Delivery Group OU.
- Integrated provisioning support:
 - Creating Session Machine accounts under the App Orchestration root OU in the shared resource domain and tenant resource domain.
 - Removing Session Machine accounts from the shared resource domain and tenant resource domain.
 - Moving Session Machine accounts to Delivery Group OUs in the shared resource domain and tenant resource domain.

Minimum permissions

Ensure that the account you use has the following permissions.

- **Full control** permissions for the App Orchestration root OU in the shared resource domain.
- Permission to create Group Policy Objects.
- **Full control** permissions for the App Orchestration root OU in the tenant resource domain.

This means that you must create a two-way trust relationship between the shared resource domain and the tenant resource domain.

- Membership of the local administrators group on all of the Desktop Controllers.
- Membership of the local administrators group on the Session Machines in the shared resource domain.
- Membership of the local administrators group on the Session Machines in all the tenant resource domains if these Session Machines need to be added to the Delivery Site in the shared resource domain, such as when creating private Delivery Group subscriptions.
- Membership of the system administrator group on all the XenDesktop database servers.
- Membership of the Delivery Site administrators group.

Location Settings

Machine Name(s):
 +

A minimum of 2 machine names are required. Additional can be added if desired.

Network:

Domain:

Datacenter:

Delivery Site Admin Group: **Member of**

User name:
Install administrator

Password:

Cancel Back Next

Delivery Site credentials for the tenant resource domain

Where specified

You specify these credentials when you migrate a Delivery Site from the tenant resource domain.

Location Settings

Machine Name(s):
 +
A minimum of 2 machine names are required. Additional can be added if desired.

Network:

Domain:

Datacenter:

Delivery Site Admin Group:

User name:
Install administrator

Password:

Cancel Back Next

Actions performed using these credentials

This account is used for the following functions.

- Installing Delivery Controllers in the tenant resource domain.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the tenant resource domain so that the Session Machine can be joined to the Delivery Site when creating a private Delivery Site subscription or private Delivery Group.
- Verifying users when hosted applications are created.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the tenant resource domain so that the Session Machine can be removed from the Delivery Site.

App Orchestration 2.0: Credentials Used in the App Orchestration Environment

- Group Policy operations:
 - Creating the license server Group Policy Object.
 - Linking the license server Group Policy to the App Orchestration OU.
 - Creating the Delivery Controller Group Policy.
 - Linking the Delivery Controller Group Policy to a specific workload/Delivery Group OU.

Minimum permissions

Ensure that the account you use has the following permissions.

- Permission to create Group Policy Objects.
- **Full control** permissions for the App Orchestration root OU in the tenant resource domain.
- Membership of the local administrators group on all of the Desktop Controllers.
- Membership of the local administrators group on the Session Machines in all the tenant resource domains.
- Membership of the system administrator group on all the XenDesktop database servers.
- Membership of the Delivery Site administrators group.

Location Settings

Machine Name(s):
 +

A minimum of 2 machine names are required. Additional can be added if desired.

Network:

Domain:

Datacenter: ▼

Delivery Site Admin Group: **Member of**

User name:
Install administrator

Password:

Delivery Site database creation credentials (XenDesktop)

Where specified

You specify these credentials when you create a Delivery Site.

Database Settings

Database Name:

Database Server Name:

User name:

Password:

Use default Config Logging database settings

Config Logging Database Server:

Config Logging Database Name:

Use default Monitoring database settings

Monitoring Database Server:

Monitoring Database Name:

Actions performed using these credentials

This account is used for the following functions.

- Creating the XenDesktop database and tables.
- Creating Delivery Controller machine accounts.

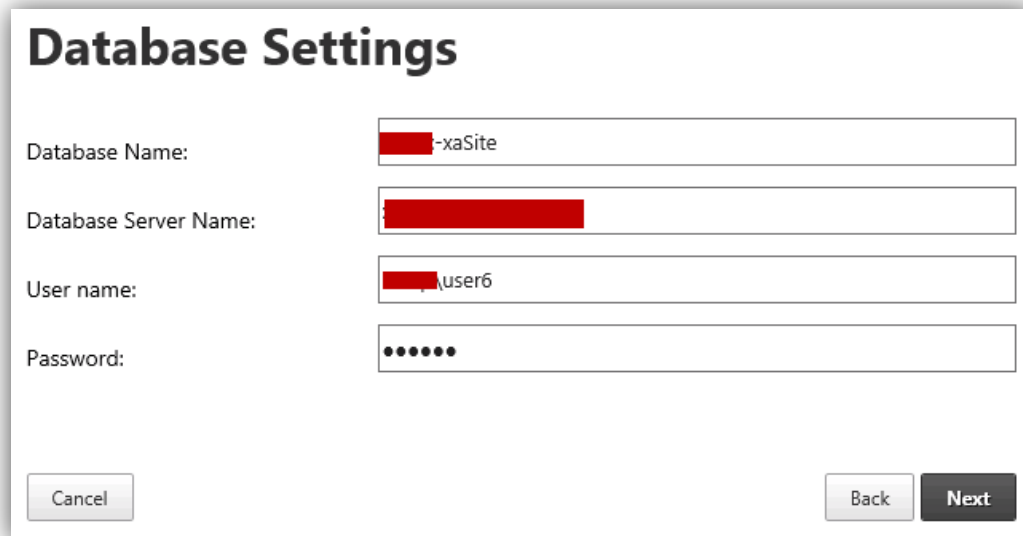
Minimum permissions

Ensure that the account you use is a member of the system administrator group on the XenDesktop database server.

Delivery Site database creation credentials (XenApp)

Where specified

You specify these credentials when you create a Delivery Site.



Database Settings

Database Name: [redacted]-xaSite

Database Server Name: [redacted]

User name: [redacted]user6

Password: [redacted]

Cancel Back Next

Actions performed using these credentials

This account is used to create the XenApp database and tables.

Minimum permissions

Ensure that the account you use is a member of the system administrator group on the XenApp database server.

Citrix Product Depot access credentials

Where specified

You specify this account during initial configuration of App Orchestration.

Global Settings

Product depot settings

Network file share containing installation software for your deployment. App Orchestration uses this location when installing software on remote machines.

Depot location:

User name:

Account used to access the product depot from remote machines. Configure with read-only permissions to the product depot.

Password:

External DNS suffix

DNS suffix used to configure netscaler gateway address.

External DNS suffix:

Actions performed using these credentials

This account is used to read the installation package.

Minimum permissions

Ensure that the account you use has read permissions on the Citrix Product Depot.

Product installation credentials

Where specified

You specify this account during initial configuration of the shared resource domain.

Product installation credential

Account used to install Citrix software on externally provisioned machines.

User name:

The product install account for the shared resource domain. Requires permissions to install software on remote machines in the domain.

Password:

You also enter the product installation credentials during domain migration to the tenant resource domain.

New Domain

Domain name:
Once saved, this can not be changed

Domain type:

Orchestration service user name:
Orchestration service account with full permissions

Orchestration service password:

Require password to use this domain

Product Installation Credential

Account used to install Citrix software on externally provisioned machines

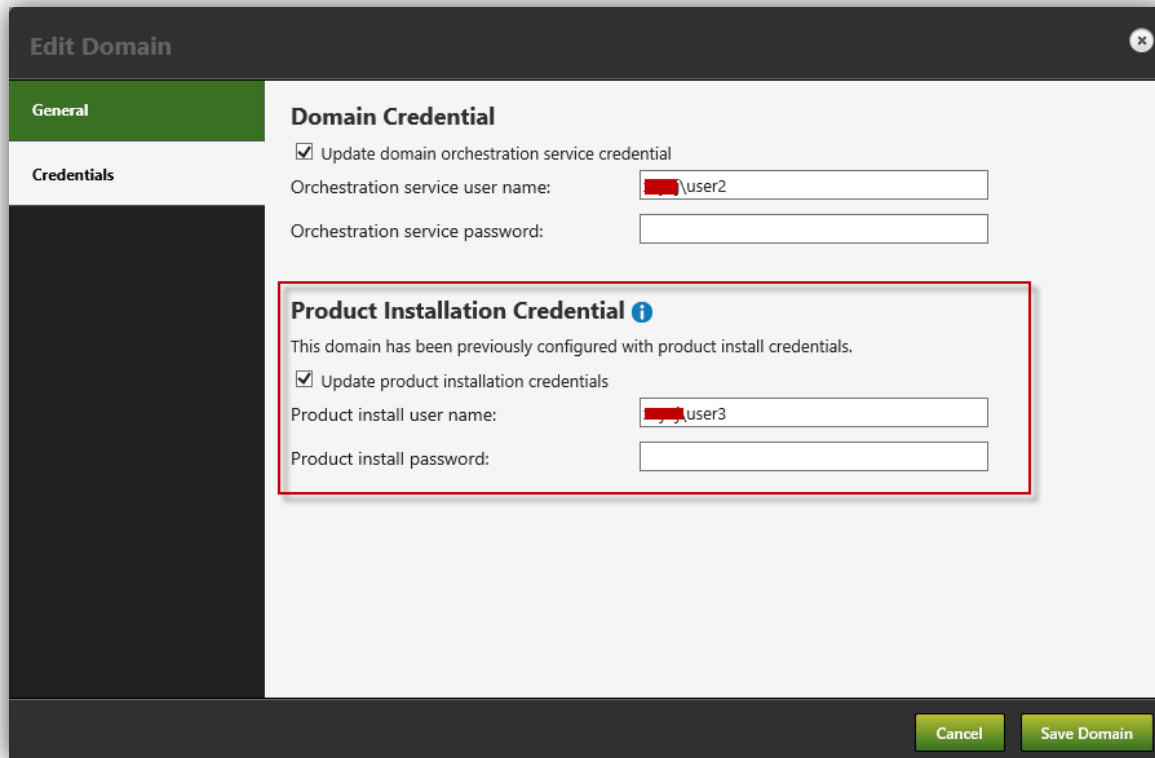
Update product installation credentials

Product install user name:
Requires permissions to install software on remote machines in the domain

Product install password:

App Orchestration 2.0: Credentials Used in the App Orchestration Environment

You can update these credentials on the **Edit Domain** screen of the App Orchestration web management console.



The screenshot shows the 'Edit Domain' interface. On the left, there is a navigation menu with 'General' (highlighted in green) and 'Credentials'. The main content area is titled 'Domain Credential' and contains a checked checkbox for 'Update domain orchestration service credential'. Below this are two input fields: 'Orchestration service user name' (containing '\user2') and 'Orchestration service password'. A red box highlights the 'Product Installation Credential' section, which includes an information icon, a message stating 'This domain has been previously configured with product install credentials.', a checked checkbox for 'Update product installation credentials', and two input fields: 'Product install user name' (containing '\user3') and 'Product install password'. At the bottom right, there are 'Cancel' and 'Save Domain' buttons.

Actions performed using these credentials

This account is used for the following functions.

- Installing the Citrix App Orchestration Agent service on Delivery Controllers.
- Installing the Citrix App Orchestration Agent service on StoreFront server group machines.
- Installing XenApp on Session Machines.
- Installing the Virtual Desktop Agent and configuring Microsoft Remote Desktop Services on Session Machines.
- Installing StoreFront and configuring the StoreFront server group.
- Performing image analysis on Session Machines to determine the operating system and obtain application information.

Minimum permissions

Ensure that the account you use has the following permissions.

- Membership of the local administrators group on all of the Desktop Controllers.
- Membership of the local administrators group on all of the Session Machines.
- Membership of the local administrators group on all of the StoreFront server group machines.