Connected

Software Version 10.0.0

Upgrade Guide

For Connected Backup Customers

MICRO FOCUS®

Document Release Date: September 2021
Software Release Date: September 2021

Legal notices

Copyright notice

© Copyright 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit https://www.microfocus.com/documentation/connected/.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Manage software licenses and support contracts
- Submit and track service requests
- Contact customer support
- View information about all services that Support offers

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the Access Levels descriptions.

Contents

Upgrade overview

Micro Focus Connected 10.0 is the latest revision of our end point data protection service that offers many new features as well as additional capabilities that support an “upgrade” user experience for the Connected Backup SaaS customer. The upgrade experience will enable a fast and efficient transition to Connected 10.0 from both technology and business perspectives. Connected Backup SaaS Customers will gain new functionality and a new look and feel from both administrative and end user perspectives. The upgrade to Connected 10.0 is designed to expedite the deployment of a new Connected 10.0 agent and a Connected 10.0 administrative portal that is pre-populated with device, policies, user, and technician information from your existing Connected Backup Support Center. This is accomplished via automated processes that require minimal customer administrative effort and no end user involvement.

To ensure customer success, Micro Focus is delivering Connected 10.0 within a now SaaS data center tenant that, along with PC and Mac based agents will run in parallel with the customer’s existing Connected Backup SaaS tenant and agents. The temporary parallel deployment enables customers the ability to come up to speed with Connected 10.0 and perform any required acceptance testing before rolling out the upgrade enterprise wide.

In order to get started, we do require you to contact your Micro Focus Account Manager. Your Account Manager will be able to provide you access to your new Connected 10.0 tenant and schedule an introductory walk-through of the new capabilities available to your organization.

This section includes the following:

- Before you begin, on the next page

Before you begin

To upgrade to Connected 10.0, make sure the following prerequisites are met:

1. Contact your Support representative and initiate the Connected 10.0 upgrade process.
2. Make sure to uninstall the existing Connected MX agent.
3. The minimum DataCenter version of Connected Backup is 9.0.4.

   You can upgrade to Connected 10.0 from the following versions of Connected Backup Agents:

   a. 8.8.5.1a

   b. 8.10.1

   c. 8.11

   d. 8.11.2

   e. 9.0

   f. 9.0.3.1

   g. 9.0.4

Upgrade process

The following are the points to know during the upgrade process:

1. When you request for the upgrade to Connected 10.0, the Operations team will migrate your community, users, and metadata to the Connected 10.0 Data Center.
2. Technicians will receive a Connected 10.0 welcome email to set the password and personalize their account if these users are maintained by Connected 10.0. If you use your own identity provider (IdP) for authentication, technicians will not receive any welcome email.
3. From Connected Backup Support Center, you will be assigned to Connected Backup 9.0.5 agent configuration. The Connected Backup agent is upgraded to 9.0.5.
4. After the upgrade to Connected Backup 9.0.5, the next back up will download the Connected 10.0 MSI and will be installed.

   Once the upgrade is complete,

   a. the Connected 10.0 icon (C10) appears in the Windows system tray or macOS menu bar.

   b. the backup rules are migrated from Connected Backup but are not assigned. The Administrator will have to assign these rules. By default, the DataOnly policy is applied to the customer and other rules will be in Draft state. For details, see Assign policies, on page 8.
5. Once provisioned, the Connected 10.0 agent starts backing up every 15 minutes (default interval).
6. If you are not configured to use your own identity provider (IdP) for authentication, you can personalize and set the password through Connected 10.0 icon in the Windows system tray or macOS menu bar.
7. You can also access the Connected 10.0 web interface from the system tray.
8. You will get notification daily to set the password for 14 days unless notifications are suppressed or you are configured to your own identity provider (IdP) for authentication.

> **IMPORTANT:** Due to data protection measures introduced in macOS 10.15 (Catalina), the first time an Agent attempts to access a folder that contains either your documents or other personal files in your user profile, macOS prompts whether to allow access.
>
> The first of these prompts occurs during installation or upgrade to macOS Catalina when the Agent tries to create a shortcut on your desktop. Additional prompts occur during the Agent's initial scan whenever it attempts to access one of the protected folders for the first time. For the Agent to back up files, you must allow access. After granting access to a specific folder, you are not prompted again for that location unless you manually revoke access through the macOS Security & Privacy settings.
>
> For more information about this macOS security-related data protections feature, see https://www.apple.com/macos/catalina/features/.

Post upgrade

After the upgrade, the Administrator has to assign policies and / or might have to combine/merge the policies before assigning. This section includes the following:

- Assign policies, on the next page
- Export / import policies, on the next page
- Inheritance, on page 9

Assign policies

After upgrade, the Connected Backup rule sets (backup rules) are migrated to Connected 10.0. In Connected 10.0, the backup rules are referred as policies having **Draft** as the policy status. The Administrator needs to assign the policies to the customer and groups. By default, the DataOnly policy is applied to the customer and all the groups under the customer.

> **NOTE:** In Connected Backup, you have separate rule sets for Mac and PC. When you upgrade to Connected 10.0, all these rule sets will be migrated as policies with a **Draft** status. However, in Connected 10.0, a group can have only one policy applied to it. So to have all these rule sets applied to a group, either you can merge the rule sets using export and import policy options and manually editing them or create new policy with all the rules included for Mac and PC or update the default DataOnly policy which is applicable for the whole company.

To assign policies, perform the following:

1. Log on to the Connected 10.0 Web Application.
2. Click the **POLICIES** tab. List of available policies along with their status and other options are displayed.
3. Click the policy name that you want to assign. The policy details are displayed.
4. Click **EDIT AS DRAFT**.

   You can modify the backup settings and add new rules to the policy.
5. Specify the group name for the **Apply to** option.
6. Click **SAVE & PUBLISH** to assign the policy to the group.

For details, see *Policy overview* section in Connected 10.0 *Help Center* for Web Application.

Export / import policies

You can export a backup policy to an XML file, modify its rules manually using a text editor, and then import the policy back into Connected 10.0. The ability to export and import a policy enables you to perform the following tasks:

- Create a custom backup policy template containing common corporate rules.

  This template can then serve as a base for all future backup policies.
- Duplicate a specific backup policy, and then customize it for another group of users.
- Replicate a backup policy across various Connected 10.0 hierarchies or geographical Connected 10.0 instances.
- Combine or merge one or more policies.

After exporting a backup policy, you can import it into any Connected 10.0 hierarchy you manage or send it to other Connected 10.0 administrators for import into groups under their administrative control.

For more details, see *Manually edit an exported backup policy*, *Export a backup policy*, *Import a backup policy*, and *Tips for creating a backup policy* sections in Connected 10.0 *Help Center* for Web Application.

Inheritance

In Connected 10.0, the policies are inherited, meaning, any policy applied at company level is inherited to all its groups and sub groups. So you can create common corporate-level policies that is applied to whole company and create subsets that is applied to groups and sub groups.

For details, see *Policy scope* section in Connected 10.0 *Help Center* for Web Application.

Troubleshooting

This section includes the following scenario:

- Registration failure, on the next page

Registration failure

Issue

Every time you login, the Connected 10.0 Agent displays the login prompt.

Workaround

This might happen for one of the following reasons:

- if the user is a technician,
- if the registration has failed.

If the user is a technician, then the user should set password with one of the earlier sent welcome email and use that email to login and proceed with the next steps.

If the user is a technician, but never received a welcome email, or if the registration has failed, then one of the Customer Admins or your Support representative should log on to the Connected 10.0 Web application. In the Edit user profile page of the user, update email address, if needed, and use **SET/RESET PASSWORD** to send the welcome email. Once the user sets the password, follow the steps to complete the registration.

If the user is a technician and the authentication is configured to have through their own identity provider (IdP), then enter the email address in the email prompt. It will auto login if the identity provider (IdP) is configured with windows integrated authentication and the machine is in the same domain. Else, the user needs to provide the password associated with that email address.

The login prompt is not displayed the next time you try to login to the system.

Mapping

The following table provides the mapping between Connected Backup and Connected 10.0:

Connected Backup	Connected 10.0
Community	Customer
Sub community	Group
Account	User
Technician	Admin user **NOTE:** Based on corresponding technician permissions, the Admin user can be a Customer Admin, Customer Data Admin, Group Admin, Group Data Admin, or ReadOnlySupport. For more details, see User overview, on the next page.
Backup rules	Policies

> **NOTE:** Since Connected 10.0 is user centric, email address should be unique within the customer.

This section includes the following:

- Mapping in detail, on the next page
- User overview, on the next page

Mapping in detail

- Based on the corresponding permissions in Connected Backup, the technicians at root community are mapped as Customer Admin or Customer Data Admin.
- Remaining technicians in the sub communities are mapped as Group Admin or Group Data Admin.
- If the Connected Backup technician has permission ONLY for reports, then that technician is mapped as ReadOnlySupport.
- If Connected Backup has technicians at multiple communities with same email address, they will be created in the root with Group Admin, Group Data Admin, or ReadOnlySupport based on the corresponding Connected Backup permissions.

User overview

Connected10.0 roles include the following:

- **Customer Data Admin ( ).** A data administrator who can access and migrate the data of any user in your company. This person can also manage groups and users, create policies, and run reports for any group in your company. Additionally, a Data Admin can perform typical User functions on their own files.
- **Customer Admin ( ).** An administrator who can manage groups and lower-ranked users (except Group Data Admins), create policies, and run reports for any group in your company. An Admin can also perform typical User functions on their own files.
- **Read Only Support ( ).** An administrator who can view groups, users, and policies, and who can run reports for any group in your company. This view-only permission on Connected10.0 information helps the Support user investigate and resolve end-user issues. A Support user can also perform typical User functions on their own files.
- **Group Data Admin** ( ). A data administrator who can access and migrate the data of lower-ranked users in their own group or any of its subgroups. Within this same scope, this person can also manage groups and lower-ranked users, create policies, and run reports. Additionally, a Group Data Admin can perform typical user functions on their own files.
- **Group Admin** ( ). An administrator who can manage groups and lower-ranked users, create policies, and run reports for their own group or any of its subgroups. A Group Admin can also perform typical user functions on their own files.

For more details on Connected10.0 roles, see *User overview* section in *Connected10.0 Help Center* for Web Application.